ΜΙΚΡΟΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

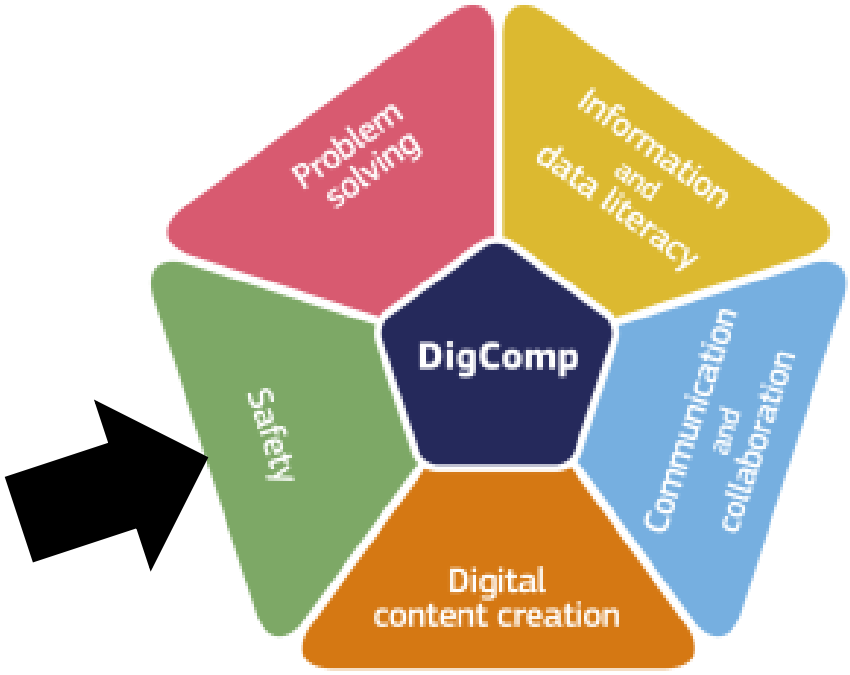
Ικανότητα 4.2:

ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ

DSW
DIGITAL SKILLS WALLET

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

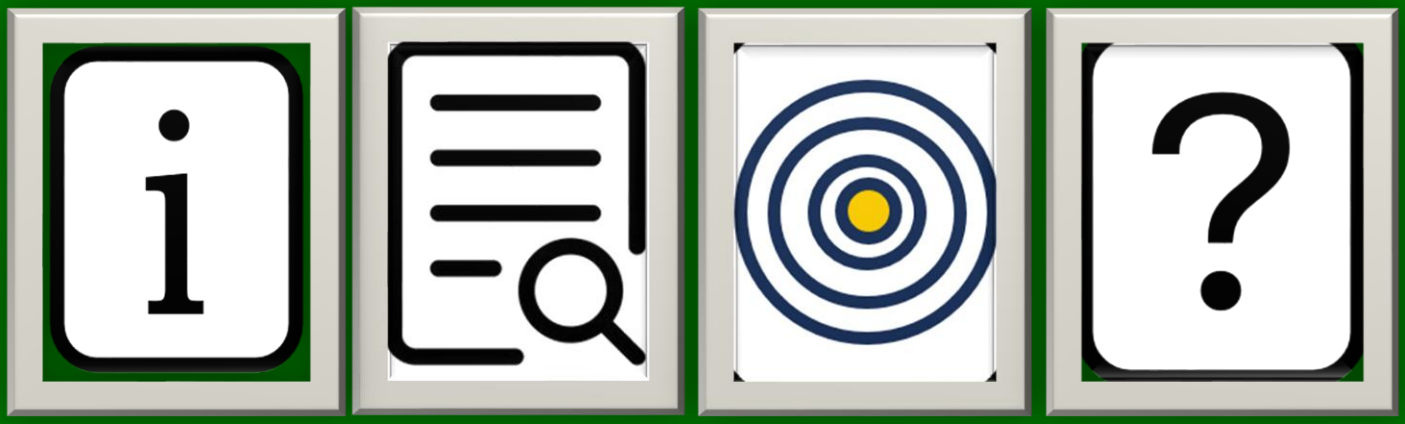
Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις


Problem solving
Information and data literacy
DigComp
Communication and collaboration
Safety
Digital content creation

Περιεχόμενα

ΕΠΙΠΕΔΟ ΘΕΜΕΛΙΩΣΗΣ

(Επίπεδο 1 και επίπεδο 2)



Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	**Ολοκληρωμένη κατανόηση της ψηφιακής ασφάλειας και της ασφάλειας των συναλλαγών** **Κωδ: A.1: MC 4.2. A.1**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΙΔΡΥΜΑ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16 - 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.1 και 4.2.2):

- Αναγνωρίζουν τη σημασία της ασφαλούς ηλεκτρονικής ταυτοποίησης για την ασφαλέστερη ανταλλαγή προσωπικών δεδομένων στις συναλλαγές.
- Προσδιορίστε τα στοιχεία που συνήθως εξηγούνται στην "πολιτική απορρήτου" των εφαρμογών.

Περιγραφή

Καθώς ο ψηφιακός κόσμος επεκτείνεται, η σημασία των μέτρων ψηφιακής ασφάλειας και προστασίας κλιμακώνεται, ιδίως όσον αφορά την ανταλλαγή και τη διαχείριση προσωπικών δεδομένων. Αυτό το Micro Credential επικυρώνει τη βαθιά κατανόηση του κρίσιμου ρόλου της ασφαλούς ηλεκτρονικής ταυτοποίησης και την ολοκληρωμένη κατανόηση των πολιτικών απορρήτου που χρησιμοποιούνται από διάφορες εφαρμογές και υπηρεσίες. Η γνώση και η ευαισθητοποίηση είναι τα πρώτα βήματα για τη διασφάλιση ασφαλέστερων ηλεκτρονικών συναλλαγών και ενός ασφαλούς ψηφιακού περιβάλλοντος.

Η πρώτη σημαντική πτυχή της ψηφιακής ασφάλειας είναι η ασφαλής ηλεκτρονική ταυτοποίηση. Αυτή αποτελεί μια ψηφιακή "απόδειξη" ταυτότητας που χρησιμεύει ως αξιόπιστο εργαλείο επικύρωσης για τις ηλεκτρονικές συναλλαγές. Η ουσία αυτής της διαδικασίας είναι η διασφάλιση της ασφάλειας των κοινών δεδομένων, που εγγυάται την ανταλλαγή τους με τον προοριζόμενο παραλήπτη. Παίζει ιδιαίτερα σημαντικό ρόλο στις συναλλαγές που αφορούν προσωπικά, ευαίσθητα ή εμπιστευτικά δεδομένα. Οι συναλλαγές αυτές κυμαίνονται από οικονομικές συναλλαγές έως ανταλλαγές δεδομένων υγειονομικής περίθαλψης και επαγγελματικές επικοινωνίες. Ως εκ τούτου, η χρήση ασφαλούς ηλεκτρονικής ταυτοποίησης αποτελεί σημαντική πτυχή της ευρύτερης ψηφιακής οικονομίας και διαμορφώνει την εμπιστοσύνη των χρηστών στις ψηφιακές συναλλαγές. Επιπλέον, η ασφαλής ηλεκτρονική ταυτοποίηση αποτελεί το θεμέλιο για πολιτικές προστασίας της ιδιωτικής ζωής που προστατεύουν τα δεδομένα των χρηστών και προασπίζουν τα δικαιώματα. Οι πολιτικές προστασίας της ιδιωτικής ζωής είναι κεντρικής σημασίας για τη διατήρηση της εμπιστοσύνης στον ψηφιακό κόσμο, διασφαλίζοντας ότι τα δεδομένα των χρηστών αντιμετωπίζονται με προσοχή, σεβασμό και νομική συμμόρφωση. Πρόκειται για νομικά έγγραφα που περιγράφουν λεπτομερώς τον τρόπο με τον οποίο οι εφαρμογές ή οι υπηρεσίες συλλέγουν, αποθηκεύουν, προστατεύουν και μοιράζονται προσωπικά δεδομένα. Η ισχυρή κατανόηση αυτών των πολιτικών απορρήτου οδηγεί σε τεκμηριωμένες αποφάσεις σχετικά με τη χρήση εφαρμογών ή υπηρεσιών και βοηθά στη διατήρηση της ψηφιακής αυτονομίας.

Μεταξύ των στοιχείων μιας πολιτικής απορρήτου, η κατανόηση των τύπων δεδομένων που συλλέγονται από μια εφαρμογή ή υπηρεσία είναι ζωτικής σημασίας. Αυτά θα μπορούσαν να περιλαμβάνουν προσωπικές πληροφορίες, λεπτομέρειες συσκευής ή δεδομένα συμπεριφοράς του χρήστη. Οι χρήστες που κατανοούν αυτό το στοιχείο μπορούν να διασφαλίσουν ότι αισθάνονται άνετα με τους τύπους πληροφοριών που συλλέγονται. Μπορούν επίσης να εκτιμήσουν κατά πόσον η συλλογή αυτή ευθυγραμμίζεται με την προβλεπόμενη χρήση της εφαρμογής ή της υπηρεσίας, μειώνοντας έτσι τις πιθανότητες ανεπιθύμητης έκθεσης δεδομένων.

Εξίσου σημαντική είναι η κατανόηση του λόγου για τον οποίο συλλέγονται τα δεδομένα, δηλαδή του σκοπού της συλλογής δεδομένων. Αυτός μπορεί να περιλαμβάνει λόγους όπως η βελτίωση της εμπειρίας του χρήστη, η παροχή εξατομικευμένου περιεχομένου ή η παροχή υπηρεσιών. Η κατανόηση αυτών των λόγων βοηθά στην αξιολόγηση του κατά πόσον η συλλογή δεδομένων εξυπηρετεί τα συμφέροντα των χρηστών ή αν γίνεται κυρίως προς όφελος του παρόχου υπηρεσιών. Μια άλλη κρίσιμη πτυχή είναι οι πρακτικές επεξεργασίας και

κοινής χρήσης δεδομένων. Το στοιχείο αυτό αναλύει τη διαδρομή των δεδομένων που συλλέγονται, περιγράφοντας λεπτομερώς τον τρόπο με τον οποίο γίνεται η επεξεργασία, η αποθήκευση και η πιθανή κοινοποίησή τους σε τρίτους. Περιλαμβάνει επίσης πληροφορίες σχετικά με τις διεθνείς διαβιβάσεις δεδομένων και τη διασυνοριακή επεξεργασία. Η γνώση αυτών των πρακτικών δίνει τη δυνατότητα στους χρήστες να αξιολογούν τους δυνητικούς κινδύνους και να κάνουν συνειδητές επιλογές σχετικά με την κοινοποίηση προσωπικών δεδομένων.

Η συγκατάθεση αποτελεί ακρογωνιαίο λίθο των κανονισμών προστασίας δεδομένων. Ως εκ τούτου, είναι ζωτικής σημασίας να κατανοήσετε πώς λαμβάνεται η συγκατάθεση για τη συλλογή και την επεξεργασία δεδομένων από την εφαρμογή ή την υπηρεσία. Αυτό μπορεί να γίνεται μέσω ρητών μεθόδων, όπως τα πλαίσια ελέγχου, ή μέσω σιωπηρών μεθόδων, όπως η συνεχής χρήση της εφαρμογής. Οι χρήστες που κατανοούν αυτές τις διαδικασίες μπορούν να ελέγχουν καλύτερα τη συγκατάθεσή τους, ενισχύοντας τη δύναμή τους επί των προσωπικών δεδομένων.

Τα δικαιώματα των χρηστών αποτελούν αναπόσπαστο μέρος των πολιτικών προστασίας δεδομένων και απορρήτου. Συνήθως περιλαμβάνουν το δικαίωμα πρόσβασης, διόρθωσης, διαγραφής ή περιορισμού της επεξεργασίας προσωπικών πληροφοριών. Η γνώση αυτών των δικαιωμάτων επιτρέπει στους χρήστες να ασκούν έλεγχο στα δεδομένα τους, γεγονός που μπορεί να οδηγήσει σε μεγαλύτερη εμπιστοσύνη στην ψηφιακή σφαίρα.

Μια άλλη κρίσιμη πτυχή μιας πολιτικής απορρήτου είναι η περιγραφή των μέτρων ασφαλείας που λαμβάνονται για την προστασία των δεδομένων των χρηστών από μη εξουσιοδοτημένη πρόσβαση ή κατάχρηση. Η σαφής κατανόηση αυτών των μέτρων μπορεί να βοηθήσει τους χρήστες να αξιολογήσουν την ευρωστία του πλαισίου ασφαλείας της υπηρεσίας ή της εφαρμογής και την επάρκειά του για τις συγκεκριμένες ανάγκες τους. Η κατανόηση των περιόδων διατήρησης δεδομένων, οι οποίες καθορίζουν το χρονικό διάστημα για το οποίο η υπηρεσία ή η εφαρμογή διατηρεί τα δεδομένα των χρηστών πριν από τη διαγραφή ή την ανωνυμοποίησή τους, είναι επίσης ζωτικής σημασίας. Διαφορετικοί χρήστες μπορεί να έχουν διαφορετικά επίπεδα άνεσης με τη διάρκεια διατήρησης των δεδομένων τους, γεγονός που καθιστά αυτό σημαντικό παράγοντα στην επιλογή ψηφιακών υπηρεσιών ή εφαρμογών.

Εάν η εφαρμογή ή η υπηρεσία συνεργάζεται με τρίτους, η πολιτική απορρήτου θα πρέπει να περιγράφει λεπτομερώς τη φύση αυτών των συνεργασιών. Οι χρήστες θα πρέπει να γνωρίζουν αυτές τις συνεργασίες, καθώς συχνά συνεπάγονται πρόσθετη κοινή χρήση και επεξεργασία δεδομένων. Σε περιπτώσεις όπου η εφαρμογή ή η υπηρεσία απευθύνεται σε παιδιά ή συλλέγει δεδομένα από παιδιά, η τήρηση των νόμων περί προστασίας της ιδιωτικής ζωής των παιδιών καθίσταται ζωτικό στοιχείο της πολιτικής απορρήτου. Η γνώση αυτής της συμμόρφωσης μπορεί να βοηθήσει τους χρήστες να λαμβάνουν πιο τεκμηριωμένες αποφάσεις σχετικά με τις εν λόγω εφαρμογές ή υπηρεσίες.

Τέλος, η κατανόηση του τρόπου με τον οποίο οι αλλαγές ή οι ενημερώσεις της πολιτικής απορρήτου κοινοποιούνται στους χρήστες και η γνώση του τρόπου με τον οποίο μπορούν να απευθύνονται στην υπηρεσία ή την εφαρμογή για ερωτήσεις ή ανησυχίες σχετικά με το απόρρητο των δεδομένων είναι θεμελιώδους σημασίας.

Αυτό το Πιστοποιητικό Micro πιστοποιεί την προηγμένη κατανόηση ενός ατόμου για την ψηφιακή ασφάλεια και προστασία στις συναλλαγές δεδομένων. Αναγνωρίζει τις γνώσεις του σχετικά με την ασφαλή ηλεκτρονική ταυτοποίηση και την ικανότητά του να αναγνωρίζει και να κατανοεί στοιχεία που συνήθως εξηγούνται στις πολιτικές απορρήτου. Ο αποδέκτης αυτού του Micro Credential είναι έτσι καλά εξοπλισμένος για να προστατεύει τα προσωπικά του δεδομένα, να περιηγείται με αυτοπεποίθηση στον ψηφιακό κόσμο και να συμβάλλει σε ένα ασφαλέστερο ψηφιακό περιβάλλον.

Ερωτήσεις

1. Τι είναι η ασφαλής ηλεκτρονική ταυτοποίηση και γιατί είναι ζωτικής σημασίας στις συναλλαγές προσωπικών δεδομένων;
2. Πώς συμβάλλει η ασφαλής ηλεκτρονική ταυτοποίηση στην εμπιστοσύνη των χρηστών στις ψηφιακές συναλλαγές;
3. Γιατί είναι απαραίτητη η πλήρης κατανόηση των πολιτικών απορρήτου στο πλαίσιο της ψηφιακής ασφάλειας και προστασίας;
4. Ποιοι είναι ορισμένοι τυπικοί τύποι δεδομένων που μπορεί να συλλέγονται από εφαρμογές ή υπηρεσίες στο πλαίσιο της πολιτικής απορρήτου τους;
5. Γιατί η κατανόηση του σκοπού της συλλογής δεδομένων είναι σημαντική για τους χρήστες ψηφιακών εφαρμογών ή υπηρεσιών;
6. Τι περιλαμβάνει συνήθως το στοιχείο των πρακτικών επεξεργασίας και κοινοχρησίας δεδομένων σε μια πολιτική απορρήτου; Γιατί είναι σημαντικό να το κατανοήσουν οι χρήστες;
7. Πώς μπορεί μια εφαρμογή ή υπηρεσία να λάβει συνήθως τη συγκατάθεση ενός χρήστη για τη συλλογή και επεξεργασία δεδομένων; Γιατί η κατανόηση αυτού του ζητήματος είναι ζωτικής σημασίας για τους χρήστες;
8. Ποια είναι μερικά από τα δικαιώματα του χρήστη που συνήθως επισημαίνονται σε μια πολιτική απορρήτου; Γιατί είναι σημαντικό να τα γνωρίζουν και να τα κατανοούν οι χρήστες;
9. Ποια είναι η σημασία της κατανόησης των μέτρων ασφαλείας που περιγράφονται σε μια πολιτική απορρήτου;
10. Γιατί είναι σημαντική η γνώση των περιόδων διατήρησης δεδομένων για τους χρήστες και πώς μπορεί να επηρεάσει τις αποφάσεις τους σχετικά με τη χρήση ορισμένων ψηφιακών υπηρεσιών ή εφαρμογών;
11. Πώς συμβάλλει η κατανόηση των συνεργασιών με τρίτους και των ειδοποιήσεων ενημέρωσης πολιτικής στην τεκμηριωμένη λήψη αποφάσεων ενός χρήστη σχετικά με τη χρήση εφαρμογών ή υπηρεσιών;

Επαρκής γνώση της ασφάλειας προσωπικών δεδομένων και της αξιολόγησης κινδύνων (MC 4.2.A.2)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Επαρκής γνώση της ασφάλειας προσωπικών δεδομένων και της αξιολόγησης κινδύνων **Κωδ: A.2.A.2**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΙΔΡΥΜΑ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16 - 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.3 και 4.2.4):

- Προσδιορίστε τους διάφορους τύπους προσωπικών δεδομένων που ενδέχεται να διατρέχουν κίνδυνο (π.χ. όνομα, ηλεκτρονικό ταχυδρομείο, διεύθυνση, αριθμός τηλεφώνου, αριθμός ασφάλισης ασθενείας ΕΕ).
- Υπολογίστε τα οφέλη και τους κινδύνους προτού επιτρέψετε σε τρίτους να επεξεργάζονται προσωπικά δεδομένα.

Περιγραφή

Η πλοήγηση στο ψηφιακό τοπίο έχει γίνει κανόνας στον σύγχρονο κόσμο. Κάθε κλικ, like και share συμβάλλει στο ψηφιακό αποτύπωμα ενός ατόμου, ενισχύοντας έτσι τη σημασία της ασφάλειας των προσωπικών δεδομένων. Η οριοθέτηση των διαφόρων τύπων προσωπικών δεδομένων που διατρέχουν κίνδυνο, ιδίως στις πλατφόρμες των μέσων κοινωνικής δικτύωσης, και η αξιολόγηση των πλεονεκτημάτων και των κινδύνων της επεξεργασίας δεδομένων από τρίτους αποτελούν κρίσιμες δεξιότητες στο πεδίο της ιδιωτικότητας και της ασφάλειας των δεδομένων. Αυτό το Micro Credential επικυρώνει την επάρκεια ενός ατόμου στην κατανόηση αυτών των κρίσιμων πτυχών και την ικανότητά του να λαμβάνει τεκμηριωμένες αποφάσεις που προάγουν ένα ασφαλέστερο ψηφιακό περιβάλλον.

Τα δεδομένα προσωπικού χαρακτήρα αποτελούν ένα ευρύ φάσμα πληροφοριών που μπορούν να ταυτοποιήσουν ή να αφορούν ένα άτομο. Περιλαμβάνει γενικά αναγνωριστικά στοιχεία όπως ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, διευθύνσεις κατοικίας και αριθμούς τηλεφώνου. Τα πιο ευαίσθητα δεδομένα μπορεί να περιλαμβάνουν αριθμούς ασφάλισης ασθενείας της ΕΕ, ημερομηνίες γέννησης, οικονομικές πληροφορίες και στοιχεία απασχόλησης. Με την άνοδο των πλατφορμών κοινωνικής δικτύωσης, ακόμη και τα προσωπικά ενδιαφέροντα, οι δραστηριότητες και τα δεδομένα συμπεριφοράς έχουν γίνει μέρος αυτού του μείγματος. Κάθε κομμάτι δεδομένων, όταν μοιράζεται ή αποθηκεύεται ψηφιακά, είναι ευάλωτο σε πιθανούς κινδύνους και απειλές ασφαλείας.

Η σημασία της ασφάλειας των προσωπικών δεδομένων γίνεται ιδιαίτερα εμφανής στις πλατφόρμες κοινωνικής δικτύωσης. Αυτές οι πλατφόρμες χρησιμεύουν ως ένα στάδιο όπου οι χρήστες μπορούν να εκφράζονται, να αλληλεπιδρούν με άλλους και να έχουν πρόσβαση σε πληθώρα υπηρεσιών. Ωστόσο, με τον τρόπο αυτό, οι χρήστες συχνά αποκαλύπτουν πληθώρα προσωπικών δεδομένων. Ένα απλό "like" σε μια ανάρτηση μπορεί να υποδείξει τις προτιμήσεις ενός ατόμου, ενώ ένα "check-in" μπορεί να εκθέσει δεδομένα τοποθεσίας. Η κοινοποίηση γενεθλίων, οικογενειακών στοιχείων ή ακόμη και φωτογραφιών μπορεί να αποκαλύψει ακούσια ευαίσθητες πληροφορίες, καθιστώντας τους χρήστες ευάλωτους σε παραβιάσεις της ιδιωτικής ζωής ή ακόμη και σε κλοπή ταυτότητας.

Η κατανόηση των τύπων προσωπικών δεδομένων που κινδυνεύουν στις πλατφόρμες κοινωνικής δικτύωσης και των πιθανών επιπτώσεων της έκθεσής τους αποτελεί την πρώτη γραμμή άμυνας για την ψηφιακή ασφάλεια. Για παράδειγμα, ενώ η αποκάλυψη μιας διεύθυνσης ηλεκτρονικού ταχυδρομείου μπορεί να οδηγήσει σε ανεπιθύμητες επικοινωνίες, η αποκάλυψη οικονομικών πληροφοριών μπορεί να έχει σοβαρότερες συνέπειες, όπως η οικονομική απάτη. Η γνώση αυτών των κινδύνων υπογραμμίζει την ανάγκη για συνετή κοινοποίηση και προσεκτική διαχείριση των προσωπικών δεδομένων στις πλατφόρμες κοινωνικής δικτύωσης.

Ωστόσο, η ευθύνη για την ασφάλεια των προσωπικών δεδομένων εκτείνεται πέραν του ατόμου. Αφορά επίσης τους οργανισμούς και τις υπηρεσίες που χειρίζονται τα δεδομένα αυτά. Ως εκ τούτου, η σημασία των πολιτικών προστασίας της ιδιωτικής ζωής, των ασφαλών πρακτικών χειρισμού δεδομένων και της ασφαλούς ηλεκτρονικής ταυτοποίησης μεγεθύνεται. Η γνώση αυτών των μέτρων επιτρέπει στους χρήστες να

διασφαλίζουν ότι τα προσωπικά τους δεδομένα αντιμετωπίζονται με την απαραίτητη προσοχή και σεβασμό. Το σύγχρονο ψηφιακό οικοσύστημα περιλαμβάνει συχνά επεξεργασία δεδομένων από τρίτους, όπου τα δεδομένα μοιράζονται με εξωτερικές οντότητες για διάφορους σκοπούς, συμπεριλαμβανομένης της βελτίωσης της ποιότητας των υπηρεσιών, της εξατομίκευσης της εμπειρίας των χρηστών ή της διενέργειας αναλύσεων δεδομένων. Ενώ αυτές οι συνεργασίες μπορούν να ενισχύσουν τις δυνατότητες των ψηφιακών υπηρεσιών και να προσφέρουν βελτιωμένες εμπειρίες, ενέχουν επίσης κινδύνους που οι χρήστες πρέπει να γνωρίζουν.

Η πιθανότητα παραβίασης δεδομένων αυξάνεται με κάθε πρόσθετη οντότητα που χειρίζεται τα δεδομένα. Κάθε εξωτερική συνεργασία αποτελεί ένα ακόμη πιθανό σημείο τρωτότητας όπου η ασφάλεια των δεδομένων μπορεί να τεθεί σε κίνδυνο. Επιπλέον, η επεξεργασία από τρίτους συχνά οδηγεί σε έναν βαθμό απώλειας του ελέγχου των προσωπικών δεδομένων. Λαμβάνοντας υπόψη αυτές τις εκτιμήσεις, η ικανότητα αξιολόγησης των οφελών και των κινδύνων πριν από την έγκριση της επεξεργασίας δεδομένων από τρίτους αποτελεί κρίσιμη δεξιότητα για τη διατήρηση της ασφάλειας των προσωπικών δεδομένων.

Η αξιολόγηση αυτή περιλαμβάνει την κατανόηση των πρακτικών χειρισμού δεδομένων, των πολιτικών απορρήτου και των μέτρων ασφαλείας του τρίτου μέρους. Απαιτεί επίγνωση των συγκεκριμένων δεδομένων που κοινοποιούνται, του τρόπου χρήσης τους και των εφαρμοζόμενων μεθόδων προστασίας.

Η εξοικείωση με τα δικαιώματα των χρηστών, συμπεριλαμβανομένου του δικαιώματος πρόσβασης, διόρθωσης, διαγραφής ή περιορισμού της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, είναι επίσης απαραίτητη.

Συχνά, η επεξεργασία δεδομένων από τρίτους περιλαμβάνει διασυνοριακές διαβιβάσεις δεδομένων, εισάγοντας την πρόσθετη πολυπλοκότητα των διαφορετικών κανονισμών προστασίας δεδομένων σε διάφορες περιοχές.

Ως εκ τούτου, η σαφής κατανόηση αυτών των πτυχών είναι ζωτικής σημασίας για τη λήψη τεκμηριωμένων αποφάσεων σχετικά με την επεξεργασία δεδομένων από τρίτους και τη διασφάλιση της ασφάλειας των δεδομένων προσωπικού χαρακτήρα.

Εν κατακλείδι, αυτό το Micro Credential αναγνωρίζει την επιδεξιότητα ενός ατόμου στην ασφάλεια των προσωπικών δεδομένων και στην αξιολόγηση των κινδύνων. Σηματοδοτεί την ικανότητά του να εντοπίζει διάφορους τύπους προσωπικών δεδομένων που διατρέχουν κίνδυνο, ιδίως στις πλατφόρμες κοινωνικής δικτύωσης, και την ικανότητά του να αξιολογεί τα οφέλη και τους κινδύνους πριν εγκρίνει την επεξεργασία δεδομένων από τρίτους. Εφοδιασμένος με αυτές τις γνώσεις, ο κάτοχος αυτού του Micro Credential μπορεί να διαχειρίζεται ενεργά τα προσωπικά του δεδομένα, να περιηγείται στον ψηφιακό κόσμο με αυτοπεποίθηση και να συμβάλλει στην προώθηση ενός ασφαλέστερου ψηφιακού περιβάλλοντος.

Ερωτήσεις

1. Ποιοι είναι οι διάφοροι τύποι προσωπικών δεδομένων που μπορεί να κινδυνεύουν στις πλατφόρμες κοινωνικής δικτύωσης;
2. Ποιοι πιθανοί κίνδυνοι για την ιδιωτικότητα και την ασφάλεια μπορεί να προκύψουν από την κοινοποίηση ευαίσθητων προσωπικών πληροφοριών δημοσίως σε πλατφόρμες κοινωνικής δικτύωσης;
3. Ποιες μπορεί να είναι οι πιθανές επιπτώσεις εάν εκτεθούν στα μέσα κοινωνικής δικτύωσης πιο ευαίσθητα δεδομένα, όπως οι αριθμοί ασφάλισης ασθενείας της ΕΕ ή οικονομικά δεδομένα;
4. Πώς μπορεί η επεξεργασία δεδομένων από τρίτους να ενισχύσει τις δυνατότητες των ψηφιακών υπηρεσιών;
5. Ποιοι είναι ορισμένοι από τους κινδύνους που συνδέονται με την επεξεργασία δεδομένων από τρίτους;
6. Γιατί είναι σημαντικό να αξιολογούνται τα οφέλη και οι κίνδυνοι προτού επιτραπεί η επεξεργασία δεδομένων από τρίτους;
7. Πώς η επεξεργασία δεδομένων από τρίτους αυξάνει δυνητικά την ευπάθεια σε παραβιάσεις

δεδομένων;

8. Τι σημαίνει απώλεια του ελέγχου των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της επεξεργασίας δεδομένων από τρίτους;
9. Πώς βοηθά η κατανόηση των πρακτικών χειρισμού δεδομένων, των πολιτικών προστασίας προσωπικών δεδομένων και των μέτρων ασφαλείας του τρίτου μέρους στην αξιολόγηση των πλεονεκτημάτων και των κινδύνων της επεξεργασίας δεδομένων από τρίτους;
10. Ποια είναι τα δικαιώματα των χρηστών όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και πώς παίζουν ρόλο στην επεξεργασία δεδομένων από τρίτους;
11. Πώς οι διασυνοριακές διαβιβάσεις δεδομένων προσθέτουν πολυπλοκότητα στην επεξεργασία δεδομένων από τρίτους;
12. Πώς μπορεί ένα άτομο να διασφαλίσει την ασφάλεια των προσωπικών του δεδομένων κατά την αλληλεπίδρασή του σε πλατφόρμες κοινωνικής δικτύωσης;
13. Ποια είναι μερικά από τα μέτρα που μπορούν να λάβουν οι οργανισμοί και οι υπηρεσίες για να διασφαλίσουν την ασφάλεια των προσωπικών δεδομένων, ιδίως όταν πρόκειται για επεξεργασία δεδομένων από τρίτους;

Δεξιοτεχνία στην προσαρμογή εφαρμογών Antivirus και ρυθμίσεων προσωπικής ιδιωτικότητας (MC 4.2.A.3)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος του μικροπιστοποιητικού	Δεξιοτεχνία στην εφαρμογή Antivirus και στην προσαρμογή των προσωπικών ρυθμίσεων απορρήτου Κωδ: A.3: MC 4.2.A.3
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΙΔΡΥΜΑ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.5 και 4.2.6):

- Συζητήστε το ρόλο του λογισμικού προστασίας από ιούς στην προστασία από κακόβουλο λογισμικό και εξασκηθείτε στην εκτέλεση τακτικών σαρώσεων από ιούς στις συσκευές σας.
- Εξατομικεύστε τις ρυθμίσεις απορρήτου στους λογαριασμούς σας στα μέσα κοινωνικής δικτύωσης για να περιορίσετε τις πληροφορίες που είναι δημόσια ορατές.

Περιγραφή

Στη διαρκώς εξελισσόμενη ψηφιακή εποχή, η διατήρηση της ασφάλειας δεν αφορά μόνο τη διαφύλαξη των φυσικών πτυχών της ζωής μας, αλλά και την προστασία της εικονικής μας ύπαρξης. Η παρουσία λογισμικού προστασίας από ιούς στις συσκευές και η εξατομίκευση των ρυθμίσεων απορρήτου στους λογαριασμούς των μέσων κοινωνικής δικτύωσης έχουν γίνει αναπόσπαστα στοιχεία ολοκληρωμένων στρατηγικών κυβερνοασφάλειας. Το Πιστοποιητικό Micro Credential in Mastery in Antivirus Application and Personal Privacy Setting Customization πιστοποιεί την επάρκεια ενός ατόμου στην αξιοποίηση αυτών των εργαλείων για την ασφάλεια των ψηφιακών του χώρων.

Το λογισμικό προστασίας από ιούς διαδραματίζει καθοριστικό ρόλο στην προστασία των ψηφιακών συσκευών από διάφορες μορφές κακόβουλου λογισμικού, γνωστού επίσης ως κακόβουλο λογισμικό. Αυτό το λογισμικό λειτουργεί με τη σάρωση, τον εντοπισμό και την εξάλειψη απειλών που ενδέχεται να θέσουν σε κίνδυνο την ακεραιότητα, τη λειτουργικότητα και την ασφάλεια της συσκευής. Οι ιοί, τα σκουλήκια, το ransomware, το spyware, το adware και τα Trojans είναι συνηθισμένοι τύποι κακόβουλου λογισμικού που μπορούν να προκαλέσουν σημαντικές ζημιές στις ψηφιακές συσκευές, από τη διαφθορά και την κλοπή δεδομένων έως την ολική αποτυχία της συσκευής.

Το άτομο πρέπει να κατανοήσει ότι η τακτική εκτέλεση σαρώσεων antivirus στις συσκευές του αποτελεί θεμελιώδη πτυχή της ψηφιακής ασφάλειας. Οι τακτικές σαρώσεις βοηθούν να διασφαλιστεί ότι οι πιο πρόσφατες απειλές εντοπίζονται και αντιμετωπίζονται άμεσα, γεγονός ιδιαίτερα σημαντικό δεδομένης της συνεχούς εμφάνισης νέων τύπων κακόβουλου λογισμικού. Οι προγραμματισμένες σαρώσεις, μαζί με τις λειτουργίες προστασίας σε πραγματικό χρόνο που προσφέρουν πολλά προγράμματα προστασίας από ιούς, δημιουργούν ένα πολυεπίπεδο σύστημα άμυνας που μπορεί να ανατρέψει μια μεγάλη ποικιλία επιθέσεων κακόβουλου λογισμικού, προστατεύοντας έτσι τα δεδομένα του ατόμου, την ιδιωτική ζωή και τη συνολική υγεία των συσκευών του.

Πέρα από τη χρήση του λογισμικού προστασίας από ιούς, η ικανότητα προσαρμογής των ρυθμίσεων απορρήτου στους λογαριασμούς των μέσων κοινωνικής δικτύωσης είναι μια άλλη κρίσιμη ικανότητα που συμβάλλει στην ψηφιακή ασφάλεια ενός ατόμου. Οι πλατφόρμες μέσων κοινωνικής δικτύωσης αποτελούν κοινούς στόχους για τους εγκληματίες του κυβερνοχώρου λόγω του τεράστιου όγκου προσωπικών δεδομένων που κατέχουν. Ως εκ τούτου, οι ρυθμίσεις απορρήτου σε αυτές τις πλατφόρμες πρέπει να αντιμετωπίζονται με μεγάλη προσοχή, ώστε να περιορίζονται οι πληροφορίες που είναι δημόσια ορατές και συνεπώς δυνητικά προσβάσιμες σε κακόβουλους φορείς.

Η εξατομίκευση των ρυθμίσεων απορρήτου στις πλατφόρμες κοινωνικής δικτύωσης περιλαμβάνει την κατανόηση και την προσαρμογή μιας σειράς ελέγχων που υπαγορεύουν την ορατότητα και την

προσβασιμότητα των προσωπικών πληροφοριών, των αναρτήσεων, των δεδομένων τοποθεσίας και των συνδέσεων του χρήστη. Το άτομο πρέπει να γνωρίζει ότι αυτές οι ρυθμίσεις συχνά προκαθορίζουν την ευρεία κοινοποίηση πληροφοριών, οπότε πρέπει να διαχειρίζεται προληπτικά αυτές τις ρυθμίσεις για να περιορίσει τη διάδοση των προσωπικών πληροφοριών. Ο περιορισμός του κοινού των αναρτήσεων, η αναθεώρηση των ετικετών από τους φίλους, η διαχείριση των ρυθμίσεων τοποθεσίας και ο έλεγχος της ορατότητας της λίστας φίλων είναι μερικές από τις ενέργειες που μπορούν να ενισχύσουν σημαντικά την ιδιωτικότητα στις πλατφόρμες κοινωνικής δικτύωσης.

Ως εκ τούτου, το Πιστοποιητικό πιστοποίησης Micro για την απόκτηση Mastery in Antivirus Application and Personal Privacy Setting Customization συμβολίζει την κατανόηση και την εφαρμογή κρίσιμων πρακτικών κυβερνοασφάλειας από ένα άτομο. Αυτό περιλαμβάνει την αποτελεσματική χρήση λογισμικού antivirus για την προστασία από κακόβουλο λογισμικό και την εξατομίκευση των ρυθμίσεων απορρήτου στα μέσα κοινωνικής δικτύωσης για τον περιορισμό της δημόσιας προβολής προσωπικών πληροφοριών.

Η απόκτηση αυτών των δεξιοτήτων δίνει στα άτομα τα εφόδια για να περιηγηθούν καλύτερα στον ψηφιακό κόσμο, προάγοντας την ασφάλεια και την ιδιωτική τους ζωή σε ένα τοπίο που συχνά είναι γεμάτο με απειλές κυβερνοασφάλειας.

Ερωτήσεις

1. Τι ρόλο παίζει το λογισμικό προστασίας από ιούς στην προστασία των ψηφιακών συσκευών;
2. Προσδιορίστε και περιγράψτε ορισμένους κοινούς τύπους κακόβουλου λογισμικού από τους οποίους μπορεί να προστατεύσει το λογισμικό προστασίας από ιούς.
3. Γιατί είναι απαραίτητο να εκτελείτε τακτικές σαρώσεις antivirus στις συσκευές σας;
4. Εξηγήστε την έννοια της προστασίας σε πραγματικό χρόνο στα προγράμματα προστασίας από ιούς και πώς συμβάλλει σε ένα πολυεπίπεδο σύστημα άμυνας.
5. Πώς συμβάλλει η εξατομίκευση των ρυθμίσεων απορρήτου στις πλατφόρμες κοινωνικής δικτύωσης στην ψηφιακή ασφάλεια ενός ατόμου;
6. Ποιοι τύποι πληροφοριών μπορούν να γίνουν δημόσια ορατοί εάν δεν γίνεται σωστή διαχείριση των ρυθμίσεων απορρήτου των μέσων κοινωνικής δικτύωσης;
7. Περιγράψτε ορισμένα μέτρα που μπορούν να ληφθούν για την ενίσχυση της ιδιωτικότητας στις πλατφόρμες κοινωνικής δικτύωσης.
8. Γιατί είναι σημαντικό να περιορίσετε το κοινό των αναρτήσεων στις πλατφόρμες κοινωνικής δικτύωσης;
9. Πώς συμβάλλει η διαχείριση των ρυθμίσεων τοποθεσίας στα μέσα κοινωνικής δικτύωσης στην προστασία της ιδιωτικής ζωής των χρηστών;
10. Εξηγήστε τους πιθανούς κινδύνους που συνδέονται με τον μη έλεγχο της ορατότητας της λίστας φίλων στις πλατφόρμες κοινωνικής δικτύωσης.

Εμπειρία στη διαχείριση κωδικών πρόσβασης και στη χρήση των χαρακτηριστικών ασφαλείας των smartphone (MC 4.2.A.4)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Εμπειρογνωμοσύνη στη διαχείριση κωδικών πρόσβασης και στα χαρακτηριστικά ασφαλείας smartphone **Κωδικός** χρήσης: **A.4 ΚΩΔΙΚΟΣ ΧΡΉΣΗΣ: MC 4.2.A.4**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΙΔΡΥΜΑ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.7 και 4.2.8):

- Ελέγξτε την ισχύ των κωδικών σας χρησιμοποιώντας εργαλεία διαχείρισης κωδικών πρόσβασης.
- Δείξτε πώς να χρησιμοποιείτε τις ενσωματωμένες λειτουργίες ασφαλείας του smartphone σας, όπως το κλείδωμα οθόνης, για να προστατεύετε τα προσωπικά σας δεδομένα.

Περιγραφή

Ο ταχέως αυξανόμενος ρυθμός ψηφιοποίησης έχει καταστήσει αναγκαία την εφαρμογή ολοκληρωμένων μέτρων ασφαλείας για την εξασφάλιση της ασφάλειας των προσωπικών δεδομένων. Με την πρόοδο της τεχνολογίας, η διασφάλιση των προσωπικών δεδομένων δεν περιορίζεται πλέον σε εξωτερικούς φυσικούς παράγοντες, αλλά επεκτείνεται και σε εσωτερικούς εικονικούς παράγοντες. Το Micro Credential in Expertise in Password Management and Smartphone Security Features Usage επικυρώνει τις δεξιότητες ενός ατόμου στη διαχείριση κωδικών πρόσβασης με τη χρήση εργαλείων διαχείρισης κωδικών πρόσβασης και τη χρήση των ενσωματωμένων χαρακτηριστικών ασφαλείας των smartphones για τη διασφάλιση των προσωπικών δεδομένων.

Η ισχύς του κωδικού πρόσβασης είναι ένας βασικός παράγοντας που καθορίζει την ασφάλεια των ηλεκτρονικών λογαριασμών ενός ατόμου και, κατ' επέκταση, των προσωπικών του δεδομένων. Οι αδύναμοι κωδικοί πρόσβασης μπορούν εύκολα να παραβιαστούν από εγκληματίες του κυβερνοχώρου, καθιστώντας τους λογαριασμούς και τα προσωπικά δεδομένα ενός ατόμου ευάλωτα σε μη εξουσιοδοτημένη πρόσβαση και κατάχρηση. Ως εκ τούτου, είναι σημαντικό για τα άτομα να ελέγχουν την ισχύ των κωδικών πρόσβασης, εργασία που μπορεί να διευκολυνθεί με τη χρήση εργαλείων διαχείρισης κωδικών πρόσβασης.

Τα εργαλεία διαχείρισης κωδικών πρόσβασης εκτελούν διάφορες λειτουργίες που ενισχύουν την ασφάλεια των κωδικών πρόσβασης. Δημιουργούν σύνθετους και μοναδικούς κωδικούς πρόσβασης για κάθε λογαριασμό, αποθηκεύουν τους κωδικούς αυτούς με ασφάλεια και τους συμπληρώνουν αυτόματα κατά τη διάρκεια της σύνδεσης, ελαχιστοποιώντας έτσι τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης. Οι περισσότεροι διαχειριστές κωδικών πρόσβασης διαθέτουν επίσης ένα τεστ αντοχής κωδικών πρόσβασης, επιτρέποντας στο άτομο να ελέγξει την ανθεκτικότητα των κωδικών του έναντι πιθανών επιθέσεων στον κυβερνοχώρο. Η κατανόηση και η αξιοποίηση αυτών των εργαλείων αποτελεί βασική δεξιότητα στο σημερινό ψηφιακό περιβάλλον, όπου η ασφάλεια των προσωπικών δεδομένων εξαρτάται σε μεγάλο βαθμό από την ισχύ των κωδικών πρόσβασης.

Παράλληλα, το άτομο θα πρέπει να είναι έμπειρο στη χρήση των ενσωματωμένων χαρακτηριστικών ασφαλείας των smartphones του για την προστασία των προσωπικών του δεδομένων. Σε μια εποχή όπου τα smartphones αποτελούν αποθήκη τεράστιου όγκου προσωπικών δεδομένων, η μη επαρκής ασφάλισή τους μπορεί να οδηγήσει σε σημαντικές παραβιάσεις της ιδιωτικής ζωής. Τα ενσωματωμένα χαρακτηριστικά ασφαλείας, όπως οι μηχανισμοί κλειδώματος οθόνης, προσφέρουν μια πρώτη γραμμή άμυνας έναντι μη εξουσιοδοτημένης πρόσβασης.

Οι μηχανισμοί κλειδώματος οθόνης περιλαμβάνουν διάφορες μορφές ελέγχου ταυτότητας, όπως PIN, μοτίβα, κωδικούς πρόσβασης, αναγνώριση προσώπου και δακτυλικά αποτυπώματα. Ένα άτομο πρέπει να κατανοήσει τα οφέλη και τους περιορισμούς κάθε τύπου μεθόδου ελέγχου ταυτότητας για να επιλέξει αυτόν που ταιριάζει καλύτερα στις ανάγκες του και προσφέρει μέγιστη προστασία. Για παράδειγμα, ενώ η αναγνώριση προσώπου

και οι σαρωτές δακτυλικών αποτυπωμάτων προσφέρουν υψηλά επίπεδα ασφάλειας και ευκολίας, ενδέχεται να μην λειτουργούν βέλτιστα σε όλες τις συνθήκες. Αντίθετα, οι κωδικοί PIN, τα μοτίβα και οι κωδικοί πρόσβασης είναι καθολικά λειτουργικοί, αλλά μπορεί να είναι ευάλωτοι εάν είναι αδύναμοι ή εύκολα μαντεύσιμοι.

Εν κατακλείδι, το Πιστοποιητικό Micro Credential in Expertise in Password Management and Smartphone Security Features Usage πιστοποιεί τη γνώση και την εφαρμογή βασικών πρακτικών ασφαλείας από ένα άτομο. Αυτό περιλαμβάνει τη χρήση εργαλείων διαχείρισης κωδικών πρόσβασης για την ενίσχυση της ασφάλειας των κωδικών πρόσβασης και την αποτελεσματική χρήση των ενσωματωμένων χαρακτηριστικών ασφαλείας των smartphone για την προστασία των προσωπικών δεδομένων. Η κατοχή αυτών των δεξιοτήτων ενισχύει την ικανότητα του ατόμου να περιηγείται στον ψηφιακό κόσμο με ασφάλεια και αυτοπεποίθηση. Η αναγνώριση των πιθανών τρωτών σημείων και η εφαρμογή ισχυρών μέτρων προστασίας είναι ζωτικής σημασίας για τη διατήρηση της ασφάλειας των προσωπικών δεδομένων στην ψηφιακή εποχή.

Ερωτήσεις

1. Ποιος είναι ο ρόλος της ισχύος του κωδικού πρόσβασης στην ασφάλεια των ηλεκτρονικών λογαριασμών και των προσωπικών δεδομένων ενός ατόμου;
2. Πώς συμβάλλουν τα εργαλεία διαχείρισης κωδικών πρόσβασης στην ενίσχυση της ασφάλειας των κωδικών πρόσβασης;
3. Ποιες είναι ορισμένες βασικές λειτουργίες των εργαλείων διαχείρισης κωδικών πρόσβασης;
4. Εξηγήστε πώς λειτουργεί η δοκιμή ισχύος κωδικού πρόσβασης σε εργαλεία διαχείρισης κωδικών πρόσβασης.
5. Γιατί είναι σημαντικό να αξιοποιείτε τα ενσωματωμένα χαρακτηριστικά ασφαλείας των smartphones για την προστασία των προσωπικών δεδομένων;
6. Πώς ένας μηχανισμός κλειδώματος οθόνης χρησιμεύει ως γραμμή άμυνας κατά της μη εξουσιοδοτημένης πρόσβασης σε smartphones;
7. Προσδιορίστε και περιγράψτε τους διάφορους τύπους μεθόδων ελέγχου ταυτότητας που είναι διαθέσιμοι στους μηχανισμούς κλειδώματος οθόνης smartphone.
8. Συζητήστε τα πλεονεκτήματα και τους περιορισμούς της χρήσης της αναγνώρισης προσώπου ως μεθόδου ελέγχου ταυτότητας για το κλείδωμα οθόνης smartphone.
9. Πώς συμβάλλουν τα PIN, τα μοτίβα και οι κωδικοί πρόσβασης στην ασφάλεια των smartphone και ποια είναι τα πιθανά τρωτά σημεία τους;
10. Πώς η χρήση μοναδικών και σύνθετων κωδικών πρόσβασης για κάθε λογαριασμό ενισχύει την ασφάλεια των προσωπικών δεδομένων;
11. Ποιοι είναι οι κίνδυνοι που συνδέονται με τη χρήση αδύναμων ή εύκολα μαντεύσιμων PIN, μοτίβων και κωδικών πρόσβασης για τον έλεγχο ταυτότητας κλειδώματος οθόνης smartphone;

Γνώση της συντήρησης κωδικών πρόσβασης και κατανόηση της ασφάλειας δημόσιων δικτύων Wi-Fi (MC 4.2.A.5)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Γνώση της συντήρησης κωδικών πρόσβασης και κατανόηση της ασφάλειας δημόσιου δικτύου Wi-Fi **Κωδ: A.5**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΙΔΡΥΜΑ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.9 και 4.2.10):

- Τροποποιείτε περιοδικά τον κωδικό πρόσβασής σας για να αποφύγετε πιθανές παραβιάσεις δεδομένων.
- Συμπεραίνετε τους κινδύνους από τη χρήση μη ασφαλών δημόσιων δικτύων Wi-Fi για συναλλαγές που αφορούν προσωπικά δεδομένα.

Περιγραφή

Καθώς οι ψηφιακές πλατφόρμες συνεχίζουν να ενσωματώνονται σε κάθε πτυχή της σύγχρονης ζωής, η έμφαση στη διατήρηση της ασφάλειας στον κυβερνοχώρο έχει αυξηθεί σημαντικά. Το Micro Credential in Proficiency in Password Maintenance and Understanding Public Wi-Fi Network Security αναγνωρίζει την ικανότητα ενός ατόμου να πλοηγείται και να κατανοεί δύο κρίσιμες πτυχές της προσωπικής ψηφιακής ασφάλειας: τη σημασία της περιοδικής τροποποίησης των κωδικών πρόσβασης και την κατανόηση των κινδύνων που σχετίζονται με μη ασφαλή δημόσια δίκτυα Wi-Fi.
Η ακεραιότητα της ψηφιακής ταυτότητας και η ασφάλεια των προσωπικών δεδομένων είναι στενά συνδεδεμένες με την ισχύ και τη διατήρηση των κωδικών πρόσβασης. Οι κωδικοί πρόσβασης λειτουργούν ως η πρώτη γραμμή άμυνας κατά της μη εξουσιοδοτημένης πρόσβασης σε προσωπικούς λογαριασμούς και πληροφορίες. Ως εκ τούτου, δεν είναι μόνο σημαντικό να δημιουργείτε ισχυρούς, δύσκολα αναγνωρίσιμους κωδικούς πρόσβασης, αλλά είναι επίσης ζωτικής σημασίας να τους τροποποιείτε ανά τακτά χρονικά διαστήματα. Οι τακτικές αλλαγές κωδικών πρόσβασης μπορούν να αποτρέψουν τη μακροπρόθεσμη μη εξουσιοδοτημένη πρόσβαση, ακόμη και αν ο κωδικός πρόσβασης είχε παραβιαστεί προηγουμένως χωρίς να το γνωρίζει το άτομο. Ως εκ τούτου, η δυνατότητα διαχείρισης και αλλαγής των κωδικών πρόσβασης σε τακτά χρονικά διαστήματα αποτελεί βασικό παράγοντα για τη μείωση του κινδύνου πιθανών παραβιάσεων δεδομένων.
Εκτός από τη διατήρηση του κωδικού πρόσβασης, το Micro Credential αναδεικνύει την κατανόηση των κινδύνων που ενέχει η χρήση μη ασφαλών δημόσιων δικτύων Wi-Fi.
Τα δημόσια δίκτυα Wi-Fi, ιδίως εκείνα που δεν διαθέτουν ασφαλή πρωτόκολλα σύνδεσης, ενέχουν σημαντικούς κινδύνους για την ασφάλεια. Τα μη ασφαλή δίκτυα αποτελούν πρωταρχικούς στόχους για τους εγκληματίες του κυβερνοχώρου, οι οποίοι μπορούν εύκολα να υποκλέψουν τα δεδομένα που μεταδίδονται μέσω του δικτύου. Αυτό γίνεται ιδιαίτερα ανησυχητικό όταν τα δίκτυα αυτά χρησιμοποιούνται για συναλλαγές που αφορούν προσωπικά δεδομένα ή ευαίσθητες πληροφορίες.
Το άτομο πρέπει να συμπεράνει τους διάφορους κινδύνους που συνδέονται με αυτά τα δίκτυα, οι οποίοι περιλαμβάνουν, μεταξύ άλλων, επιθέσεις "Man-in-the-Middle", κατασκοπεία και sniffing, διανομή κακόβουλου λογισμικού, ακόμη και την απειλή κακόβουλων hotspots που μεταμφιέζονται σε νόμιμα δίκτυα. Η κατανόηση αυτών των κινδύνων υπογραμμίζει τη σημασία της αποφυγής τέτοιων δικτύων όταν πρόκειται για προσωπικά, ευαίσθητα δεδομένα, ή της επιλογής μέτρων προστασίας, όπως τα Εικονικά Ιδιωτικά Δίκτυα (VPN) για την κρυπτογράφηση της μετάδοσης των δεδομένων τους.
Εν κατακλείδι, το Πιστοποιητικό πιστοποίησης Micro για την επάρκεια στη συντήρηση κωδικών πρόσβασης και την κατανόηση της ασφάλειας δημόσιων δικτύων Wi-Fi επικυρώνει τις δεξιότητες και την κατανόηση των ζωτικών πτυχών της ασφάλειας των προσωπικών δεδομένων. Η τακτική αλλαγή των κωδικών πρόσβασης μειώνει σημαντικά τον κίνδυνο παραβίασης δεδομένων, ενώ η αναγνώριση των κινδύνων από τη χρήση μη ασφαλών δημόσιων δικτύων Wi-Fi υπογραμμίζει την ανάγκη επαγρύπνησης και προφύλαξης για την ασφάλεια των δεδομένων. Οι γνώσεις αυτές και η ικανότητα αποτελεσματικής εφαρμογής τους εξοπλίζουν τα άτομα με

τις απαραίτητες δεξιότητες για να περιηγηθούν με ασφάλεια στο ψηφιακό τοπίο, προστατεύοντας τις προσωπικές τους πληροφορίες από ενδεχόμενες απειλές στον κυβερνοχώρο.

Ερωτήσεις

1. Πώς συμβάλλει η τακτική αλλαγή κωδικών πρόσβασης στην ασφάλεια των προσωπικών δεδομένων;
2. Ποιοι είναι οι πιθανοί κίνδυνοι εάν ένα άτομο δεν τροποποιεί περιοδικά τους κωδικούς πρόσβασης;
3. Γιατί τα μη ασφαλή δημόσια δίκτυα Wi-Fi θεωρούνται απειλή για την ασφάλεια των προσωπικών δεδομένων;
4. Μπορείτε να εξηγήσετε ορισμένους από τους ειδικούς κινδύνους που συνδέονται με τη χρήση μη ασφαλών δημόσιων δικτύων Wi-Fi για συναλλαγές που αφορούν προσωπικά δεδομένα;
5. Τι είναι η επίθεση "Man-in-the-Middle" και πώς σχετίζεται με τη χρήση μη ασφαλών δημόσιων δικτύων Wi-Fi;
6. Περιγράψτε την έννοια του "snooping και sniffing" στο πλαίσιο των μη ασφαλών δικτύων Wi-Fi.
7. Πώς γίνεται η διανομή κακόβουλου λογισμικού στο πλαίσιο δημόσιων δικτύων Wi-Fi;
8. Τι είναι ένα κακόβουλο hotspot και πώς απειλεί την ασφάλεια των δεδομένων;
9. Πώς μπορούν μέτρα προστασίας, όπως τα Εικονικά Ιδιωτικά Δίκτυα (VPN), να μετριάσουν τους κινδύνους που συνδέονται με τη χρήση δημόσιων δικτύων Wi-Fi;

Κυριαρχία στην εθιμοτυπία ψηφιακού περιεχομένου και στην ασφάλεια προσωπικών δεδομένων (MC 4.2.A.6)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Κυριαρχία στην εθιμοτυπία ψηφιακού περιεχομένου και στην ασφάλεια προσωπικών δεδομένων **Κωδ: A.6**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΙΔΡΥΜΑ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.11 και 4.2.12):

- Διαχωρίστε το κατάλληλο και το ακατάλληλο ψηφιακό περιεχόμενο για κοινοποίηση σε λογαριασμούς κοινωνικής δικτύωσης.
- Συζητήστε τη σημασία της προστασίας των προσωπικών δεδομένων κατά τη χρήση ψηφιακών πλατφορμών.

Περιγραφή

Το Mastery in Digital Content Etiquette and Personal Data Security είναι ένα Micro Credential που αναγνωρίζει την ευρεία κατανόηση ενός ατόμου για την κατάλληλη διαδικτυακή συμπεριφορά και την κρίσιμη φύση της ασφάλειας των προσωπικών δεδομένων στο ψηφιακό σύμπαν. Καθώς ο κόσμος κινείται προς την κατεύθυνση της ολοκληρωμένης ψηφιοποίησης, η κατανόηση του τρόπου ενασχόλησης με τις ψηφιακές πλατφόρμες, ιδίως τα μέσα κοινωνικής δικτύωσης, και η διατήρηση της επαγρύπνησης σχετικά με την προστασία των προσωπικών δεδομένων, έχουν καταστεί επιτακτική ανάγκη τόσο στον προσωπικό όσο και στον επαγγελματικό τομέα.

Ένα αναπόσπαστο στοιχείο αυτής της γνώσης περιλαμβάνει την ικανότητα διάκρισης μεταξύ κατάλληλου και ακατάλληλου περιεχομένου για διάδοση σε πλατφόρμες κοινωνικής δικτύωσης. Με την πανταχού παρούσα παρουσία των μέσων κοινωνικής δικτύωσης, τα άτομα μοιράζονται τακτικά προσωπικά ανέκδοτα, απόψεις και διάφορες μορφές πληροφοριών στο διαδίκτυο. Ενώ αυτό ενισχύει την αίσθηση της παγκόσμιας κοινότητας και ενθαρρύνει τον διάλογο, ταυτόχρονα εισάγει την ανάγκη για σύνεση στην απόφαση για το ποιο περιεχόμενο θα μοιραστεί.

Το τι συνιστά κατάλληλο ή ακατάλληλο περιεχόμενο μπορεί να εξαρτάται σε μεγάλο βαθμό από διάφορους παράγοντες, όπως οι κοινωνικοί και επαγγελματικοί κύκλοι του ατόμου, η εν λόγω πλατφόρμα μέσων κοινωνικής δικτύωσης, τα πολιτιστικά έθιμα και οι κοινωνικοί κανόνες. Οι παράγοντες που συχνά οριοθετούν τα όρια μεταξύ κατάλληλου και ακατάλληλου περιεχομένου περιλαμβάνουν την ευαισθησία των πληροφοριών, τη δυνατότητα πρόκλησης βλάβης ή δυσφορίας και το επίπεδο άνεσης του ατόμου ή του κοινού. Ως εκ τούτου, τα άτομα πρέπει να αξιολογούν τη φύση του περιεχομένου και να εκτιμούν την καταλληλότητά του πριν από την κοινοποίηση.

Επιπλέον, τα άτομα πρέπει να έχουν επίγνωση των πιθανών συνεπειών που μπορεί να προκύψουν από την κοινοποίηση ορισμένων τύπων περιεχομένου. Αυτές θα μπορούσαν να περιλαμβάνουν βλάβη της προσωπικής φήμης, απώλεια εργασίας, παραβίαση της ιδιωτικής ζωής, ακόμη και νομικές επιπτώσεις σε ορισμένες περιπτώσεις. Αυτό υπογραμμίζει τη σημασία της εφαρμογής κριτικής σκέψης και της προσοχής όταν αποφασίζεται ποιο ψηφιακό περιεχόμενο θα κοινοποιηθεί στις πλατφόρμες κοινωνικής δικτύωσης.

Ένα άλλο βασικό στοιχείο του Micro Credential υπογραμμίζει την κρίσιμη σημασία της διασφάλισης των προσωπικών δεδομένων κατά την αλληλεπίδραση με ψηφιακές πλατφόρμες. Η διατήρηση της ασφάλειας των προσωπικών δεδομένων αποτελεί ακρογωνιαίο λίθο για τη διαφύλαξη της προσωπικής ιδιωτικής ζωής και την αποτροπή πιθανών απειλών, όπως η απάτη ταυτότητας, οι οικονομικές απάτες και η μη εξουσιοδοτημένη εισβολή σε προσωπικούς λογαριασμούς. Διάφορες μορφές προσωπικών πληροφοριών, από οικονομικές

ιδιαιτερότητες έως δεδομένα ταυτοποίησης, μεταδίδονται και αποθηκεύονται σε μια σειρά ψηφιακών πλατφορμών, καθιστώντας τες ευάλωτες σε κυβερνοεπεμβάσεις.

Η κατανόηση των πιθανών συνεπειών των παραβιάσεων δεδομένων και η γνώση του τρόπου προφύλαξης από τέτοιου είδους συμβάντα είναι ζωτικής σημασίας δεξιότητα. Αυτό περιλαμβάνει τη χρήση ισχυρών τεχνικών κωδικών πρόσβασης, την τακτική ενημέρωση του λογισμικού ασφαλείας, την επιφυλακτικότητα απέναντι σε αμφίβολα μηνύματα ηλεκτρονικού ταχυδρομείου ή συνδέσμους και την άσκηση διακριτικότητας σχετικά με τις πληροφορίες που μοιράζονται στις πλατφόρμες κοινωνικής δικτύωσης. Η ευαισθητοποίηση και η εφαρμογή αυτών των πρακτικών ενισχύουν σημαντικά την προστασία των προσωπικών δεδομένων και προάγουν μια ασφαλέστερη ψηφιακή εμπειρία.

Συνοψίζοντας, το Mastery in Digital Content Etiquette and Personal Data Security είναι ένα Micro Credential που επικυρώνει την ικανότητα και την κατανόηση ενός ατόμου στη διάκριση του κατάλληλου ψηφιακού περιεχομένου για την ανταλλαγή και την προστασία των προσωπικών δεδομένων. Πιστοποιεί την ικανότητα του ατόμου να διαχειρίζεται υπεύθυνα την ψηφιακή του παρουσία και να δίνει προτεραιότητα στην ασφάλεια των δεδομένων. Αυτή η κατανόηση και η επάρκεια είναι απαραίτητες για τη διατήρηση ενός σεβαστού και ασφαλούς ψηφιακού περιβάλλοντος. Η ικανότητα κατάλληλης διαχείρισης του ψηφιακού περιεχομένου και προστασίας των προσωπικών δεδομένων δεν αποτελεί απλώς ένδειξη ψηφιακής επάρκειας, αλλά καταδεικνύει επίσης σεβασμό για τα ψηφιακά δικαιώματα και την ιδιωτικότητα του ίδιου και των άλλων. Παίζει καθοριστικό ρόλο στη διαμόρφωση μιας ασφαλέστερης, πιο υπεύθυνης και με σεβασμό ψηφιακής κοινότητας.

Ερωτήσεις

1. Μπορείτε να εξηγήσετε γιατί είναι κρίσιμο να διακρίνουμε μεταξύ κατάλληλου και ακατάλληλου περιεχομένου για κοινοποίηση στα μέσα κοινωνικής δικτύωσης;
2. Πώς μπορεί το πλαίσιο, όπως τα πολιτισμικά έθιμα και οι κοινωνικοί κανόνες, να επηρεάσει το περιεχόμενο που θεωρείται κατάλληλο για κοινοποίηση στις πλατφόρμες κοινωνικής δικτύωσης;
3. Ποιες είναι ορισμένες πιθανές συνέπειες της κοινοποίησης ακατάλληλων ή ευαίσθητων πληροφοριών σε πλατφόρμες κοινωνικής δικτύωσης;
4. Γιατί είναι σημαντικό να διασφαλίζονται τα προσωπικά δεδομένα κατά τη χρήση ψηφιακών πλατφορμών;
5. Μπορείτε να περιγράψετε ορισμένες πιθανές απειλές που προκύπτουν από την ανεπαρκή προστασία των προσωπικών δεδομένων στις ψηφιακές πλατφόρμες;
6. Ποια μέτρα μπορούν να λάβουν τα άτομα για να προστατεύσουν τα προσωπικά τους δεδομένα στις ψηφιακές πλατφόρμες;
7. Πώς συμβάλλει η τακτική ενημέρωση του λογισμικού ασφαλείας στην προστασία των προσωπικών δεδομένων;
8. Γιατί είναι ζωτικής σημασίας η διακριτικότητα κατά την κοινοποίηση πληροφοριών σε πλατφόρμες κοινωνικής δικτύωσης;
9. Κατά τη γνώμη σας, πώς συμβάλλει στη συνολική ψηφιακή κοινότητα η ικανότητα του ατόμου να διαχειρίζεται κατάλληλα το ψηφιακό περιεχόμενο και να προστατεύει τα προσωπικά δεδομένα;

Εμπειρογνωμοσύνη στη διαχείριση του ψηφιακού απορρήτου και στις πρακτικές ασφαλούς ηλεκτρονικού εμπορίου (MC 4.2.A.7)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Εμπειρογνωμοσύνη στη διαχείριση ψηφιακού απορρήτου και σε πρακτικές ασφαλούς ηλεκτρονικού εμπορίου **Κωδ: A.7**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΙΔΡΥΜΑ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.13 και 4.2.14):

- Επικυρώστε τα κατάλληλα μέτρα για την προστασία των προσωπικών δεδομένων πριν από την κοινοποίησή τους σε ψηφιακές πλατφόρμες.
- Επισημαίνετε τις ηλεκτρονικές συναλλαγές μετά τη λήψη των κατάλληλων μέτρων ασφαλείας και προστασίας.

Περιγραφή

Η Εμπειρογνωμοσύνη στη Διαχείριση του Ψηφιακού Απορρήτου και στις Ασφαλείς Πρακτικές Ηλεκτρονικού Εμπορίου είναι ένα Πιστοποιητικό Micro που αντιπροσωπεύει την εκτεταμένη κατανόηση και πρακτική εφαρμογή μέτρων για την προστασία των προσωπικών δεδομένων στις ψηφιακές πλατφόρμες και την εκτέλεση ασφαλών ηλεκτρονικών συναλλαγών. Στον σημερινό κόσμο, όπου οι ψηφιακές αλληλεπιδράσεις αντικαθιστούν με ταχείς ρυθμούς τους παραδοσιακούς τρόπους, η γνώση της ψηφιακής ασφάλειας έχει αναδειχθεί σε κρίσιμη απαίτηση. Η διασφάλιση των ευαίσθητων και προσωπικών δεδομένων αποτελεί βασικό παράγοντα της ψηφιακής εμπιστοσύνης, εξασφαλίζοντας ομαλές και ασφαλείς προσωπικές και επαγγελματικές αλληλεπιδράσεις στον εικονικό κόσμο.

Το Micro Credential υπογραμμίζει δύο σημαντικά μαθησιακά αποτελέσματα. Το πρώτο αφορά τις αυστηρές στρατηγικές που απαιτούνται για την προστασία των προσωπικών δεδομένων πριν από την κυκλοφορία τους σε ψηφιακές πλατφόρμες. Τα προσωπικά δεδομένα είναι ένας όρος ομπρέλα, που περιλαμβάνει όχι μόνο βασικά στοιχεία ταυτοποίησης, όπως ονόματα και στοιχεία επικοινωνίας, αλλά και ιδιαίτερα ευαίσθητα δεδομένα, όπως οικονομικά αρχεία, πληροφορίες υγειονομικής περίθαλψης και άλλα. Ελλείψει ισχυρών μέτρων ασφαλείας, οι πληροφορίες αυτές μπορεί να αποτελέσουν προσοδοφόρο στόχο για τους εγκληματίες του κυβερνοχώρου, με αποτέλεσμα μη εξουσιοδοτημένες παραβιάσεις δεδομένων, κλοπή ταυτότητας και κατάχρηση προσωπικών δεδομένων.

Για το λόγο αυτό, η υιοθέτηση αυστηρών μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων είναι απαραίτητη. Σε αυτά περιλαμβάνονται η δημιουργία και η χρήση σύνθετων και μοναδικών κωδικών πρόσβασης που είναι δύσκολο να παραβιαστούν, η ενεργοποίηση του ελέγχου ταυτότητας δύο ή πολλών παραγόντων για την παροχή ενός επιπλέον επιπέδου ασφάλειας και η διατήρηση υψηλού επιπέδου προσοχής όσον αφορά την ποσότητα και το είδος των πληροφοριών που μοιράζονται σε δημόσιους ψηφιακούς τομείς. Αυτό απαιτεί την κατανόηση των κινδύνων που συνδέονται με την υπερβολική κοινή χρήση και τη σημασία της διακριτικότητας στα δημόσια ψηφιακά φόρουμ.

Επιπλέον, είναι υψίστης σημασίας να πραγματοποιείτε τακτικούς ελέγχους και προσαρμογές των ρυθμίσεων απορρήτου στις διάφορες ψηφιακές πλατφόρμες. Οι ρυθμίσεις απορρήτου λειτουργούν ως η πρώτη γραμμή άμυνας για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση και θα πρέπει να διαχειρίζονται προσεκτικά και στρατηγικά. Για ενισχυμένη προστασία, ιδίως κατά την πρόσβαση σε δημόσια δίκτυα Wi-Fi, συνιστάται η χρήση εικονικών ιδιωτικών δικτύων (VPN). Τα VPN εξασφαλίζουν ένα ασφαλές, κρυπτογραφημένο κανάλι για τη μετάδοση δεδομένων, καθιστώντας σημαντικά πιο δύσκολη την υποκλοπή και την πρόσβαση στα δεδομένα από μη εξουσιοδοτημένες οντότητες. Αυτά τα συλλογικά μέτρα ενισχύουν

σημαντικά τον αμυντικό μηχανισμό κατά των απειλών στον κυβερνοχώρο, εξασφαλίζοντας έτσι μια ασφαλέστερη εμπειρία πλοήγησης στο διαδίκτυο και ενισχύοντας την προσωπική ιδιωτικότητα.

Το δεύτερο βασικό μαθησιακό αποτέλεσμα του Micro Credential αφορά τη διεξαγωγή ασφαλών ηλεκτρονικών συναλλαγών με τη χρήση κατάλληλων πρωτοκόλλων ασφαλείας. Με την εξάπλωση των ψηφιακών πλατφορμών, πληθώρα συναλλαγών, από το ηλεκτρονικό εμπόριο και τις πληρωμές λογαριασμών έως τις ηλεκτρονικές τραπεζικές συναλλαγές και τη διαχείριση χαρτοφυλακίου, έχουν μεταφερθεί στο διαδίκτυο. Κατά συνέπεια, η διασφάλιση της ασφάλειας αυτών των συναλλαγών έχει καταστεί κρίσιμο ζήτημα.

Για την ασφαλή διεξαγωγή ηλεκτρονικών συναλλαγών, είναι σημαντικό να χρησιμοποιείτε μόνο ιστότοπους που χαρακτηρίζονται από το πρόθεμα HTTPS, το οποίο υποδηλώνει την κρυπτογραφημένη φύση της μετάδοσης δεδομένων μεταξύ του προγράμματος περιήγησης του χρήστη και του ιστότοπου. Συνιστάται επίσης η διενέργεια τακτικών ελέγχων των τραπεζικών συναλλαγών, ώστε να διευκολύνεται ο έγκαιρος εντοπισμός και η επίλυση τυχόν μη εξουσιοδοτημένων συναλλαγών. Η εφαρμογή ελέγχου ταυτότητας δύο παραγόντων ή πολλαπλών παραγόντων για τις ηλεκτρονικές συναλλαγές παρέχει ένα πρόσθετο επίπεδο ασφάλειας, καθώς απαιτεί περισσότερες από μία μεθόδους επαλήθευσης της ταυτότητας του χρήστη.

Επιπλέον, θα πρέπει να αποφεύγεται η κοινή χρήση ευαίσθητων δεδομένων μέσω μη ασφαλών δικτύων, καθώς συχνά αποτελούν εύκολο στόχο για κυβερνοεπιθέσεις. Με την υιοθέτηση αυτών των μέτρων ασφαλείας, ο κίνδυνος απάτης ή μη εξουσιοδοτημένης πρόσβασης μπορεί να μειωθεί σημαντικά, εξασφαλίζοντας μια ασφαλή και απρόσκοπτη εμπειρία ηλεκτρονικών συναλλαγών.

Εν κατακλείδι, το Micro Credential in Expertise in Digital Privacy Management and Secure E-commerce Practices επικυρώνει την εις βάθος κατανόηση και τις πρακτικές δεξιότητες ενός ατόμου στην υιοθέτηση αυστηρών μέτρων για την προστασία των προσωπικών δεδομένων και τη διεξαγωγή ασφαλών ηλεκτρονικών συναλλαγών. Αυτές οι δεξιότητες δεν είναι μόνο ζωτικής σημασίας για την προσωπική ψηφιακή ασφάλεια, αλλά συμβάλλουν επίσης στη δημιουργία ενός ασφαλέστερου και ασφαλέστερου ψηφιακού οικοσυστήματος για όλους. Η ικανότητα ασφαλούς πλοήγησης στις ψηφιακές πλατφόρμες, προστασίας των προσωπικών δεδομένων και διεξαγωγής ασφαλών ηλεκτρονικών συναλλαγών αποδεικνύει υψηλό επίπεδο ψηφιακού αλφαβητισμού και υπευθυνότητας στη σημερινή ψηφιακή εποχή.

Ερωτήσεις

1. Ποια είναι η σημασία των μοναδικών και σύνθετων κωδικών πρόσβασης στο πλαίσιο της διαχείρισης της ψηφιακής ιδιωτικότητας;
2. Πώς ο έλεγχος ταυτότητας δύο ή πολλών παραγόντων ενισχύει την ασφάλεια των προσωπικών δεδομένων στις ψηφιακές πλατφόρμες;
3. Ποιες πρέπει να είναι οι βασικές εκτιμήσεις κατά την ανταλλαγή πληροφοριών σε δημόσιες ψηφιακές πλατφόρμες;
4. Γιατί είναι ζωτικής σημασίας ο τακτικός έλεγχος και η προσαρμογή των ρυθμίσεων απορρήτου στις διάφορες ψηφιακές πλατφόρμες;
5. Πώς ένα εικονικό ιδιωτικό δίκτυο (VPN) βελτιώνει την ασφάλεια, ειδικά κατά την πρόσβαση σε δημόσια δίκτυα Wi-Fi;
6. Γιατί είναι σημαντικό να πραγματοποιείτε ηλεκτρονικές συναλλαγές μόνο σε ιστότοπους που χαρακτηρίζονται από το πρόθεμα HTTPS;

7. Πώς συμβάλλει η τακτική παρακολούθηση των τραπεζικών λογαριασμών στην ασφάλεια των ηλεκτρονικών συναλλαγών;
8. Ποιοι είναι οι κίνδυνοι που συνδέονται με την κοινή χρήση ευαίσθητων δεδομένων μέσω μη ασφαλών δικτύων και πώς μπορούν να μετριαστούν οι κίνδυνοι αυτοί;
9. Πώς οι αρχές της διαχείρισης της ψηφιακής ιδιωτικότητας και οι ασφαλείς πρακτικές ηλεκτρονικού εμπορίου συμβάλλουν σε ένα ασφαλέστερο ψηφιακό οικοσύστημα;

Πρακτικές ασφαλούς ανταλλαγής δεδομένων και ηλεκτρονικών συναλλαγών (MC 4.2.A.8)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Πρακτικές ασφαλούς ανταλλαγής δεδομένων και ηλεκτρονικών συναλλαγών **Κωδ: A.8**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΙΔΡΥΜΑ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή

Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.15 και 4.2.16):

- Συζητήστε τη σημασία της αποφυγής μη ασφαλών ιστότοπων κατά τη διαχείριση πληροφοριών καρτών.
- Καθορισμός μέτρων για την επαλήθευση της αξιοπιστίας των ατόμων πριν από την ανταλλαγή ευαίσθητων δεδομένων μαζί τους.

Περιγραφή

Το Micro Credential Secure Data Exchange and Online Transaction Practices αναγνωρίζει την ολοκληρωμένη κατανόηση και εφαρμογή μεθόδων για την προστασία προσωπικών και οικονομικών δεδομένων κατά τη διάρκεια διαδικτυακών συναλλαγών, καθώς και στρατηγικές για την εξακρίβωση της αξιοπιστίας ατόμων πριν από την ανταλλαγή ευαίσθητων πληροφοριών μαζί τους. Το διαπιστευτήριο πιστοποιεί την ικανότητα ασφαλούς πλοήγησης στο ψηφιακό τοπίο, λαμβάνοντας τεκμηριωμένες αποφάσεις που διασφαλίζουν την προστασία των δεδομένων και βελτιώνουν τη συνολική διαδικτυακή εμπειρία του χρήστη.

Ένα από τα βασικά μαθησιακά αποτελέσματα περιστρέφεται γύρω από τη σημασία της αποφυγής μη ασφαλών ιστότοπων κατά την επεξεργασία πληροφοριών καρτών. Το στοιχείο αυτό αποτελεί βασικό συστατικό της διαδικασίας ηλεκτρονικών συναλλαγών και έχει κρίσιμη σημασία, λαμβάνοντας υπόψη τις αυξανόμενες περιπτώσεις εγκλημάτων στον κυβερνοχώρο και παραβιάσεων δεδομένων σε παγκόσμιο επίπεδο. Κάθε φορά που ένα άτομο επεξεργάζεται πληροφορίες κάρτας σε μια διαδικτυακή πλατφόρμα, τα δεδομένα καθίστανται ευάλωτα σε υποκλοπή ή παραβίαση, εάν ο ιστότοπος δεν διαθέτει τα κατάλληλα πρωτόκολλα ασφαλείας.

Οι μη ασφαλείς ιστότοποι έχουν συχνά αδύναμα ή καθόλου μέτρα ασφαλείας, καθιστώντας τους δυνητικές πύλες για τους εγκληματίες του κυβερνοχώρου ώστε να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα. Οι συναλλαγές σε τέτοιους ιστότοπους μπορούν να εκθέσουν τις πληροφορίες της κάρτας σε αυτές τις οντότητες, οδηγώντας σε επιζήμιες συνέπειες, όπως οικονομική απάτη, κλοπή ταυτότητας και σημαντικές οικονομικές απώλειες.

Το άτομο πρέπει να είναι ικανό να εντοπίζει τέτοιους μη ασφαλείς ιστότοπους, οι οποίοι συνήθως χαρακτηρίζονται από την έλλειψη του HTTPS στη διεύθυνση URL, την απουσία του συμβόλου του λουκέτου που υποδηλώνει ασφαλή σύνδεση ή προειδοποιήσεις από τα προγράμματα περιήγησης ιστού σχετικά με την ασφάλεια του ιστότοπου. Επιλέγοντας συνειδητά να παρέχουν πληροφορίες κάρτας μόνο σε ασφαλείς και αξιόπιστες πλατφόρμες, τα άτομα μπορούν να μειώσουν σημαντικά τον κίνδυνο πιθανών απειλών στον κυβερνοχώρο. Αυτές οι πλατφόρμες διαθέτουν ισχυρά πρωτόκολλα κρυπτογράφησης, διασφαλίζοντας ότι, ακόμη και αν τα δεδομένα υποκλαπούν, παραμένουν αδιάβαστα και συνεπώς άχρηστα για τους χάκερ.

Το δεύτερο βασικό μαθησιακό αποτέλεσμα αφορά τη θέσπιση μέτρων για την επαλήθευση της αξιοπιστίας των ατόμων πριν από την ανταλλαγή ευαίσθητων δεδομένων με αυτά. Με την αύξηση της ανταλλαγής δεδομένων στην ψηφιακή σφαίρα, η διασφάλιση της αξιοπιστίας των αποδεκτών ευαίσθητων δεδομένων καθίσταται ζωτικής σημασίας για την πρόληψη της μη εξουσιοδοτημένης πρόσβασης ή της κακής χρήσης των δεδομένων.

Η επαλήθευση μπορεί να είναι μια διαδικασία πολλών βημάτων. Αρχικά, μπορεί να ζητηθούν επίσημα έγγραφα ταυτοποίησης ή διαπιστευτήρια για την επιβεβαίωση της ταυτότητας του ατόμου. Η άμεση επικοινωνία με το άτομο μπορεί επίσης να είναι επωφελής για την κατανόηση των προθέσεών του και τη δημιουργία ενός ορισμένου βαθμού εμπιστοσύνης. Ωστόσο, αυτά τα βήματα από μόνα τους μπορεί να μην αρκούν, ιδίως σε σενάρια που αφορούν την ανταλλαγή δεδομένων μέσω ψηφιακών πλατφορμών.

Εδώ, η χρήση ασφαλών διαύλων επικοινωνίας για την ανταλλαγή δεδομένων μπορεί να προσθέσει ένα επίπεδο ασφάλειας. Αυτά τα κανάλια χρησιμοποιούν κρυπτογράφηση για να διασφαλίσουν ότι τα δεδομένα, εάν υποκλαπούν, δεν μπορούν να διαβαστούν χωρίς το σωστό κλειδί αποκρυπτογράφησης. Επιπλέον, κατά την ανταλλαγή δεδομένων με οργανισμούς, η επισκόπηση των πολιτικών απορρήτου και των μέτρων ασφαλείας τους μπορεί να δώσει μια εικόνα για τον τρόπο με τον οποίο θα γίνεται ο χειρισμός, η αποθήκευση και η κοινή χρήση των δεδομένων. Πριν προχωρήσετε στην κοινή χρήση δεδομένων, η λήψη της ρητής συγκατάθεσης του ατόμου είναι ένα κρίσιμο βήμα. Αυτό διασφαλίζει ότι ο παραλήπτης γνωρίζει τα δεδομένα που λαμβάνει, τον σκοπό των δεδομένων και την ευθύνη του για την προστασία τους.

Η εφαρμογή αυτών των μέτρων μπορεί να συμβάλει στη διασφάλιση της προστασίας των δεδομένων και να μειώσει σημαντικά τον κίνδυνο πιθανών παραβιάσεων δεδομένων ή μη εξουσιοδοτημένης πρόσβασης.

Εν κατακλείδι, το Micro Credential Secure Data Exchange and Online Transaction Practices επικυρώνει την προηγμένη κατανόηση και τις πρακτικές δεξιότητες ενός ατόμου στην ασφαλή πλοήγηση στον ψηφιακό κόσμο. Από την αναγνώριση μη ασφαλών ιστότοπων και πρακτικών ασφαλούς ανταλλαγής δεδομένων έως την κατανόηση της σημασίας της επαλήθευσης της αξιοπιστίας πριν από την ανταλλαγή δεδομένων, αυτό το διαπιστευτήριο αντιπροσωπεύει τη δέσμευση για ψηφιακή ασφάλεια και υπευθυνότητα, μια απαραίτητη πτυχή στην εποχή των αυξανόμενων ψηφιακών αλληλεπιδράσεων.

Η τεχνογνωσία αυτή δεν βοηθά μόνο στην ασφάλεια των προσωπικών δεδομένων, αλλά συμβάλλει επίσης σημαντικά στην ενίσχυση της συνολικής ψηφιακής εμπιστοσύνης και στη δημιουργία ενός ασφαλέστερου διαδικτυακού περιβάλλοντος για όλους τους χρήστες.

Ερωτήσεις

1. Γιατί είναι σημαντικό να αποφεύγετε μη ασφαλείς ιστότοπους κατά την επεξεργασία πληροφοριών καρτών και ποιοι είναι οι πιθανοί κίνδυνοι από τη μη τήρηση των κανόνων αυτών;
2. Ποια χαρακτηριστικά μπορεί να υποδηλώνουν ότι ένας ιστότοπος δεν είναι ασφαλής για την επεξεργασία πληροφοριών καρτών;
3. Πώς μπορούν οι ασφαλείς και αξιόπιστες πλατφόρμες να διασφαλίσουν τις πληροφορίες της κάρτας σας κατά τις ηλεκτρονικές συναλλαγές;
4. Γιατί η επαλήθευση της αξιοπιστίας των ατόμων είναι ζωτικής σημασίας πριν από την ανταλλαγή ευαίσθητων δεδομένων μαζί τους;
5. Ποια μέτρα μπορούν να ληφθούν για την επαλήθευση της αξιοπιστίας ενός ατόμου πριν από την κοινοποίηση ευαίσθητων δεδομένων;

6. Πώς μπορούν τα ασφαλή κανάλια επικοινωνίας να ενισχύσουν την ασφάλεια της ανταλλαγής δεδομένων;
7. Γιατί είναι σημαντικό να εξετάζετε τις πολιτικές απορρήτου και τα μέτρα ασφαλείας των οργανισμών πριν από την ανταλλαγή δεδομένων μαζί τους;
8. Ποιος είναι ο ρόλος της ρητής συγκατάθεσης στη διαδικασία ανταλλαγής δεδομένων και γιατί είναι σημαντικός;
9. Πώς η κατανόηση και η εφαρμογή ασφαλών πρακτικών ανταλλαγής δεδομένων και ηλεκτρονικών συναλλαγών συμβάλλει στη συνολική ψηφιακή ασφάλεια και εμπιστοσύνη;

Κατανόηση των φυλλομετρητών ιστού και της προστασίας των δεδομένων των χρηστών (MC 4.2.A.9)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Κατανόηση των φυλλομετρητών ιστού και της προστασίας δεδομένων χρήστη Κωδ: A.9
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%

Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.17 και 4.2.18):

- Αποσαφηνίστε τι είναι ένα cookie και πώς μπορεί να επηρεάσει τα ευαίσθητα δεδομένα σας.
- Αποσαφηνίστε την έννοια της "λειτουργίας ινκόγκνιτο" ή της "ιδιωτικής περιήγησης" στα προγράμματα περιήγησης στο διαδίκτυο και τον τρόπο χρήσης της.

Περιγραφή

Το Πιστοποιητικό πιστοποίησης Understanding Web Browsers and User Data Protection Micro πιστοποιεί την ολοκληρωμένη γνώση και ικανότητα πλοήγησης σε εργαλεία και στρατηγικές πλοήγησης στο διαδίκτυο που διασφαλίζουν την προστασία ευαίσθητων δεδομένων χρηστών. Η έμφαση δίνεται στην εκμάθηση βασικών εννοιών, όπως η κατανόηση των cookies ιστού και οι επιπτώσεις της χρήσης ιδιωτικής περιήγησης ή της "λειτουργίας ινκόγκνιτο".

Το πρώτο βασικό μαθησιακό αποτέλεσμα επικεντρώνεται στην έννοια του "μπισκότου". Τα cookies, ή αλλιώς HTTP cookies, είναι μικρά αρχεία που αποθηκεύονται στον υπολογιστή ενός χρήστη όταν αυτός επισκέπτεται έναν ιστότοπο. Αυτά τα αρχεία χρησιμοποιούνται από τον ιστότοπο για να θυμούνται πληροφορίες σχετικά με την επίσκεψη, όπως οι προτιμήσεις του χρήστη, οι πληροφορίες σύνδεσης ή τα στοιχεία σε ένα καλάθι αγορών. Με την αποθήκευση αυτών των πληροφοριών, οι ιστότοποι μπορούν να παρέχουν εξατομικευμένη εμπειρία χρήστη και να κάνουν τις επόμενες επισκέψεις πιο αποτελεσματικές. Ωστόσο, ενώ αυτά τα cookies συμβάλλουν σημαντικά στην ευκολία του χρήστη, μπορούν επίσης να θέσουν πιθανούς κινδύνους για το απόρρητο του χρήστη και την ασφάλεια των ευαίσθητων δεδομένων.

Τα cookies μπορούν σε γενικές γραμμές να ταξινομηθούν σε δύο τύπους: cookies συνόδου και μόνιμα cookies. Τα cookies συνόδου ή παροδικά cookies είναι προσωρινά και διαγράφονται μόλις ο χρήστης κλείσει το πρόγραμμα περιήγησής του. Χρησιμοποιούνται κυρίως για εργασίες όπως η διατήρηση ενός καλαθιού αγορών ή η απομνημόνευση των ενεργειών ενός χρήστη εντός μιας περιόδου περιήγησης. Από την άλλη πλευρά, τα μόνιμα cookies παραμένουν στον υπολογιστή του χρήστη ακόμη και αφού κλείσει το πρόγραμμα περιήγησής του. Αυτά τα cookies χρησιμοποιούνται για να θυμούνται τις προτιμήσεις και τη συμπεριφορά του χρήστη για μεγάλο χρονικό διάστημα και είναι αυτά που συνδέονται συχνότερα με ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής.

Τα cookies τρίτου μέρους, ένα υποσύνολο των μόνιμων cookies, είναι ιδιαίτερα αξιοσημείωτα στις συζητήσεις γύρω από την προστασία της ιδιωτικής ζωής των δεδομένων. Σε αντίθεση με τα cookies πρώτου μέρους, τα οποία καθορίζονται από τον ιστότοπο που επισκέπτεται ο χρήστης, τα cookies τρίτου μέρους καθορίζονται από άλλους τομείς εκτός από αυτόν που επισκέπτεται. Αυτά τα cookies χρησιμοποιούνται συχνά για διαδικτυακές διαφημίσεις και μπορούν να παρακολουθούν τις συνήθειες περιήγησης ενός χρήστη σε πολλούς ιστότοπους. Αυτή η δυνατότητα παρακολούθησης της συμπεριφοράς των χρηστών έχει εγείρει σημαντικές ανησυχίες σχετικά με την ιδιωτικότητα και την ασφάλεια των δεδομένων.

Με αυτό κατά νου, η κατανόηση του τρόπου διαχείρισης και ελέγχου των ρυθμίσεων των cookies είναι ζωτικής σημασίας. Τα περισσότερα προγράμματα περιήγησης ιστού παρέχουν επιλογές για τον αποκλεισμό των cookies τρίτων, τη διαγραφή όλων των cookies ή την ειδοποίηση του χρήστη όταν δημιουργείται ένα cookie. Διαχειριζόμενοι ενεργά αυτές τις ρυθμίσεις, οι χρήστες μπορούν να προστατεύσουν τα ευαίσθητα δεδομένα τους και να διατηρήσουν την ιδιωτική τους ζωή στο διαδίκτυο.

Το δεύτερο μαθησιακό αποτέλεσμα εξετάζει την έννοια της "λειτουργίας ινκόγκνιτο" ή της "ιδιωτικής περιήγησης". Πρόκειται για μια λειτουργία που διαθέτουν τα περισσότερα προγράμματα περιήγησης στο διαδίκτυο, η οποία επιτρέπει στον χρήστη να περιηγείται στο διαδίκτυο χωρίς το πρόγραμμα περιήγησης να αποθηκεύει πληροφορίες όπως το ιστορικό περιήγησης, το ιστορικό αναζήτησης ή τα cookies. Όταν ένας χρήστης ανοίγει ένα νέο παράθυρο ινκόγκνιτο ή συνεδρία ιδιωτικής περιήγησης, το πρόγραμμα περιήγησης δημιουργεί μια ξεχωριστή προσωρινή συνεδρία που είναι απομονωμένη από την κύρια συνεδρία περιήγησης και τα δεδομένα του χρήστη.

Ωστόσο, ενώ η ιδιωτική περιήγηση μπορεί να αποτρέψει άλλους χρήστες της ίδιας συσκευής από το να βλέπουν τη δραστηριότητά σας στην περιήγηση, δεν σας κάνει αόρατους στο διαδίκτυο.

Οι ιστότοποι που επισκέπτονται, οι πάροχοι υπηρεσιών διαδικτύου και οι διαχειριστές δικτύων μπορούν ακόμη να παρακολουθούν τις δραστηριότητες περιήγησης. Αυτό είναι σημαντικό να το θυμάστε επειδή πολλοί άνθρωποι πιστεύουν λανθασμένα ότι η ιδιωτική περιήγηση παρέχει πλήρη ανωνυμία και προστασία στο διαδίκτυο.

Συνολικά, το πρόγραμμα "Κατανόηση των προγραμμάτων περιήγησης στο Web και προστασία των δεδομένων των χρηστών" περιλαμβάνει τις περιπλοκές της διαχείρισης των δεδομένων των χρηστών κατά την πλοήγηση στο ψηφιακό τοπίο. Από την κατανόηση του ρόλου των cookies έως τη γνώση του πώς και πότε να χρησιμοποιείτε την ιδιωτική περιήγηση, το πιστοποιητικό πιστοποίησης υποδηλώνει τη δέσμευση για ψηφιακή ασφάλεια και προστασία της ιδιωτικής ζωής. Οι γνώσεις αυτές είναι αναπόσπαστο στοιχείο για την προώθηση ενός ασφαλούς και αξιόπιστου ψηφιακού περιβάλλοντος, επιτρέποντας στους χρήστες να συμμετέχουν με αυτοπεποίθηση και υπευθυνότητα στις διαδικτυακές πλατφόρμες.

Ερωτήσεις

1. Τι είναι το cookie στο πλαίσιο της περιήγησης στον ιστό και πώς λειτουργεί;
2. Ποια είναι η διαφορά μεταξύ των cookies περιόδου λειτουργίας και των μόνιμων cookies; Δώστε παραδείγματα χρήσης τους.
3. Εξηγήστε την έννοια των cookies τρίτου μέρους και γιατί συνδέονται με ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής.
4. Πώς μπορούν οι χρήστες να διαχειριστούν και να ελέγξουν τις ρυθμίσεις των cookies στα προγράμματα

περιήγησης ιστού τους για να προστατεύσουν τα ευαίσθητα δεδομένα τους;
5. Τι είναι η "λειτουργία incognito" ή η "ιδιωτική περιήγηση" και πώς διαφέρει από την κανονική περιήγηση;
6. Πώς συμβάλλει η "λειτουργία incognito" ή η "ιδιωτική περιήγηση" στην προστασία της ιδιωτικής ζωής των χρηστών;
7. Ποιοι είναι οι περιορισμοί της "incognito mode" ή της "private browsing" όσον αφορά την προστασία της ιδιωτικής ζωής των χρηστών;
8. Πώς επηρεάζει η "λειτουργία incognito" ή η "ιδιωτική περιήγηση" την αποθήκευση και τη χρήση των cookies;
9. Συζητήστε γιατί η κατανόηση των cookies και της λειτουργίας "incognito" είναι απαραίτητη για την προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων.
10. Πώς μπορεί η κατανόηση και η διαχείριση των cookies να συμβάλει σε μια εξατομικευμένη εμπειρία χρήστη;
11. Εξηγήστε πώς η χρήση της "λειτουργίας incognito" ή της "ιδιωτικής περιήγησης" επηρεάζει τη διατήρηση δεδομένων των χρηστών.

Ψηφιακή ασφάλεια και παιδεία της ιδιωτικής ζωής (MC 4.2.A.10)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ψηφιακή ασφάλεια και παιδεία απορρήτου **Κωδ: A.10**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες

Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.19 και 4.2.20):

- Να είναι σε θέση να ελέγξει τις γνώσεις σχετικά με τις πολιτικές απορρήτου των ιστότοπων που επισκέπτεται συχνά.
- Συστήστε τις βέλτιστες πρακτικές για την ασφάλεια στο διαδίκτυο σε φίλους και οικογένεια.

Περιγραφή

Στον σύγχρονο κόσμο, με την εκτεταμένη διείσδυση της ψηφιακής τεχνολογίας στην καθημερινή ζωή, η κατανόηση των περιπλοκών της ψηφιακής ιδιωτικότητας και ασφάλειας έχει αναδειχθεί σε αναγκαιότητα και όχι σε πολυτέλεια. Αυτό το μικρο-πιστοποιητικό έχει σχεδιαστεί για να ενδυναμώσει τα άτομα με τις απαραίτητες γνώσεις και δεξιότητες ώστε να περιηγηθούν στο πολύπλοκο ψηφιακό τοπίο με αυτοπεποίθηση, διασφαλίζοντας ότι οι διαδικτυακές τους αλληλεπιδράσεις διέπονται από τις αρχές της ιδιωτικότητας και της ασφάλειας.

Το πρώτο από τα δύο μαθησιακά αποτελέσματα στο πλαίσιο αυτού του μικρο-πιστοποιητικού δίνει έμφαση στην ικανότητα κατανόησης και κριτικής αξιολόγησης των πολιτικών απορρήτου των ιστότοπων που επισκέπτονται συχνά. Οι πολιτικές απορρήτου, στην ουσία, χρησιμεύουν ως νομική σύμβαση μεταξύ του φορέα εκμετάλλευσης ενός ιστότοπου και των χρηστών ή επισκεπτών του, ορίζοντας διάφορες παραμέτρους όπως οι τύποι δεδομένων που συλλέγονται, ο σκοπός της συλλογής, ο τρόπος αποθήκευσης, χρήσης και δυνητικής κοινοποίησης των δεδομένων. Οι πολιτικές αυτές, ωστόσο, συχνά παραβλέπονται ή δεν γίνονται πλήρως κατανοητές από τους χρήστες, με αποτέλεσμα την ακούσια κοινοποίηση προσωπικών πληροφοριών και την πιθανή παραβίαση της ιδιωτικής ζωής.

Για τον μετριασμό τέτοιων καταστάσεων, οι εκπαιδευόμενοι στο πλαίσιο αυτού του μικρο-πιστοποιητικού θα εμβαθύνουν στη μελέτη διαφόρων πολιτικών απορρήτου, θα αναγνωρίσουν τα κρίσιμα συστατικά τους και θα

μάθουν πώς να ερμηνεύουν τις επιπτώσεις τους σε σενάρια του πραγματικού κόσμου. Η κατανόηση αυτή αποτελεί τη βάση για τη λήψη τεκμηριωμένων αποφάσεων σχετικά με τις αλληλεπιδράσεις με ιστότοπους και την αποτελεσματική διαχείριση του ψηφιακού αποτυπώματος του ατόμου. Αυτό το αποτέλεσμα θα παρέχει στους εκπαιδευόμενους την ικανότητα να αξιολογούν κριτικά αυτές τις πολιτικές, δοκιμάζοντας τις γνώσεις τους σε μια σειρά από διαφορετικά σενάρια του πραγματικού κόσμου, διασφαλίζοντας έτσι ότι μπορούν όχι μόνο να προστατεύουν τα προσωπικά τους δεδομένα αλλά και να σέβονται τα δικαιώματα ψηφιακής ιδιωτικότητας των άλλων.

Το δεύτερο μαθησιακό αποτέλεσμα στο πλαίσιο αυτού του μικροπιστοποιητικού επικεντρώνεται στην υπεράσπιση της ψηφιακής ασφάλειας, μια κρίσιμη απαίτηση στη σημερινή ψηφιακή εποχή. Ως μέρος της ευρύτερης διαδικτυακής κοινότητας, είναι σημαντικό να επεκτείνετε την ευθύνη της ψηφιακής ασφάλειας πέρα από τον εαυτό σας, μεταδίδοντας αυτή την κρίσιμη γνώση σε άλλους. Με την κατανόηση και την εφαρμογή βέλτιστων πρακτικών για την ασφάλεια στο διαδίκτυο, τα άτομα μπορούν να καθοδηγήσουν τους φίλους και την οικογένεια στην προώθηση μιας ασφαλούς και προστατευμένης διαδικτυακής παρουσίας.

Αυτές οι βέλτιστες πρακτικές περιλαμβάνουν συμβουλές για τη δημιουργία ισχυρών κωδικών πρόσβασης, την αναγνώριση και αποφυγή απάτης phishing, την ασφάλεια των οικιακών δικτύων, τη χρήση κρυπτογραφημένων καναλιών επικοινωνίας και τον περιορισμό του όγκου των προσωπικών πληροφοριών που μοιράζονται στο διαδίκτυο. Για να μοιραστούν αποτελεσματικά αυτές τις πρακτικές, οι εκπαιδευόμενοι πρέπει να κατανοήσουν σε βάθος το σκεπτικό πίσω από κάθε σύσταση και τη συμβολή της στην ενίσχυση της συνολικής διαδικτυακής ασφάλειας. Με τον τρόπο αυτό, όχι μόνο προστατεύουν τους εαυτούς τους, αλλά διαδραματίζουν επίσης καθοριστικό ρόλο στην καλλιέργεια ενός ασφαλέστερου διαδικτυακού περιβάλλοντος για όλους.

Στο σύνολό τους, αυτά τα μαθησιακά αποτελέσματα στοχεύουν να ενισχύσουν σημαντικά την ψηφιακή ασφάλεια και τον γραμματισμό στην ιδιωτική ζωή, επιτρέποντας στα άτομα να προστατεύουν τον εαυτό τους και να συμβάλλουν θετικά στην ασφάλεια των άλλων στον ψηφιακό κόσμο. Αυτό το μικρο-πιστοποιητικό παρέχει μια ολοκληρωμένη κατανόηση των πολιτικών απορρήτου και των βέλτιστων πρακτικών για την ασφάλεια στο διαδίκτυο, εξοπλίζοντας τους εκπαιδευόμενους να εφαρμόζουν αυτές τις γνώσεις με πρακτικό, ουσιαστικό και επιδραστικό τρόπο. Το ψηφιακό τοπίο μπορεί να είναι πολύπλοκο, αλλά με τις δεξιότητες και τις γνώσεις που αποκτώνται μέσω αυτού του μικροπιστοποιητικού, η πλοήγηση σε αυτό με ασφάλεια και αυτοπεποίθηση γίνεται εφικτή.

Ερωτήσεις

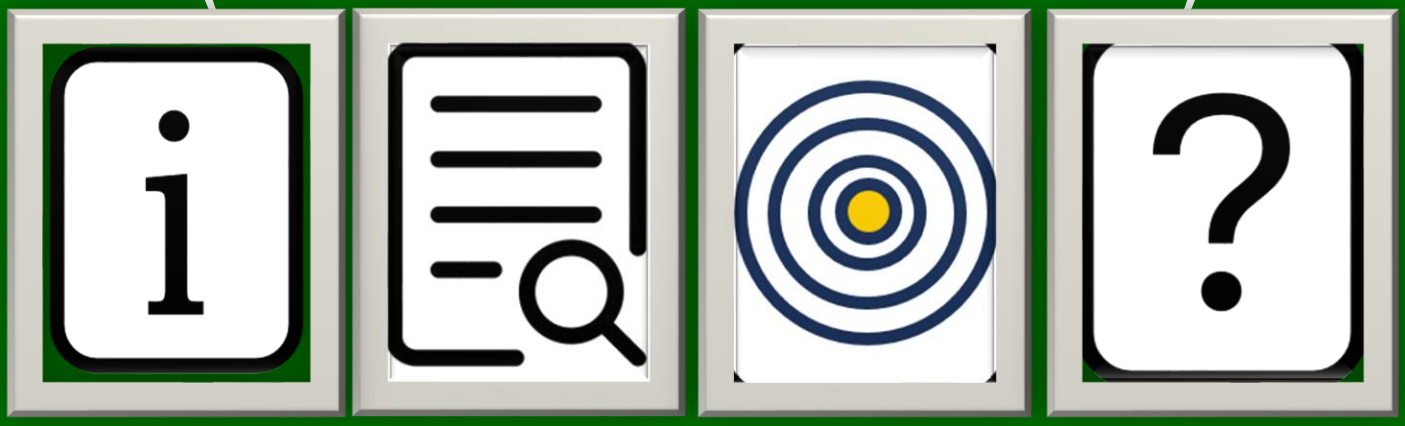
1. Ποιος είναι ο ρόλος της πολιτικής απορρήτου σε έναν ιστότοπο;
2. Πώς μπορούν οι πολιτικές απορρήτου των ιστότοπων να επηρεάσουν την αλληλεπίδρασή σας με αυτούς;
3. Ποιες είναι ορισμένες πιθανές συνέπειες της μη κατανόησης της πολιτικής απορρήτου ενός ιστότοπου;
4. Γιατί είναι σημαντικό να μοιραστείτε τις γνώσεις σας σχετικά με τις πρακτικές ασφάλειας στο διαδίκτυο με τους φίλους και την οικογένειά σας;
5. Ποια είναι τα κρίσιμα στοιχεία που πρέπει να αναζητήσετε στην πολιτική απορρήτου ενός ιστότοπου;
6. Πώς μπορεί η κατανόηση της πολιτικής απορρήτου ενός ιστότοπου να συμβάλει στη διαχείριση του ψηφιακού σας αποτυπώματος;
7. Δώστε ένα παράδειγμα βέλτιστης πρακτικής για την ασφάλεια στο διαδίκτυο που θα συνιστούσατε σε έναν φίλο ή μέλος της οικογένειας.
8. Πώς συμβάλλουν οι ισχυροί κωδικοί πρόσβασης στην ασφάλεια στο διαδίκτυο και πώς θα

συμβουλεύατε κάποιον να δημιουργήσει έναν τέτοιο κωδικό;

9. Ποια βήματα θα προτείνατε σε κάποιον για να τον βοηθήσετε να ασφαλίσει το οικιακό του δίκτυο;
10. Περιγράψτε ένα σενάριο όπου η έλλειψη κατανόησης της πολιτικής απορρήτου ενός ιστότοπου θα μπορούσε να οδηγήσει σε παραβίαση της ιδιωτικής ζωής.
11. Ποια μέτρα μπορούν να λάβουν τα άτομα για να περιορίσουν τον όγκο των προσωπικών πληροφοριών που μοιράζονται στο διαδίκτυο;
12. Τι είναι η απάτη phishing και πώς μπορούν τα άτομα να την αναγνωρίσουν και να την αποφύγουν;
13. Πώς μπορούν τα κρυπτογραφημένα κανάλια επικοινωνίας να ενισχύσουν την ασφάλεια στο διαδίκτυο και πότε πρέπει να χρησιμοποιούνται;

ΕΠΙΠΕΔΟ ΘΕΜΕΛΙΩΣΗΣ

(Επίπεδο 3 και επίπεδο 4)



Συνείδηση της ασφάλειας στον κυβερνοχώρο και προστασία της ιδιωτικής ζωής (MC 4.2.B.1)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Συνείδηση της ασφάλειας στον κυβερνοχώρο και προστασία της ιδιωτικής ζωής Κωδ: B.1: MC 4.2.B.1
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.21 και 4.2.22)

- Συστήστε τις βέλτιστες πρακτικές για την ασφάλεια στο διαδίκτυο σε φίλους και οικογένεια.
- Προσδιορισμός των κατάλληλων ενεργειών που πρέπει να λαμβάνονται όταν γίνεται κατάχρηση προσωπικών δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης.

Περιγραφή

Στο εκτεταμένο έδαφος του σημερινού ψηφιακού σύμπαντος, η σημασία της κατοχής ολοκληρωμένων γνώσεων σχετικά με την ασφάλεια στο διαδίκτυο και την προστασία των δεδομένων δεν ήταν ποτέ μεγαλύτερη. Το Micro Credential Cybersecurity Consciousness and Privacy Protection είναι σχολαστικά σχεδιασμένο για να εξοπλίσει τα άτομα με αυτές τις απαραίτητες γνώσεις.

Το πρόγραμμα καλύπτει διεξοδικά δύο καίριους τομείς, την ασφάλεια στο διαδίκτυο και τις στρατηγικές κατάχρησης δεδομένων στις πλατφόρμες κοινωνικής δικτύωσης, με στόχο τη δημιουργία ενημερωμένων και προσεκτικών ψηφιακών πολιτών.

Ο πρώτος κρίσιμος μαθησιακός τομέας του Μικροπιστοποιητικού Συνείδησης Κυβερνοασφάλειας και Προστασίας Ιδιωτικού Απορρήτου περιλαμβάνει την καλλιέργεια μιας διαφοροποιημένης ικανότητας καθοδήγησης των φίλων και της οικογένειας σχετικά με τις βέλτιστες πρακτικές για την ασφάλεια στο διαδίκτυο. Εν μέσω του κλιμακούμενου αριθμού ψηφιακών απειλών, που περιλαμβάνουν κυβερνοεπιθέσεις, διαδικτυακές απάτες και κυβερνοενοχλήσεις, είναι ζωτικής σημασίας οι χρήστες να γίνουν γνώστες των μέτρων προστασίας. Το πιστοποιητικό micro στοχεύει στην καλλιέργεια των δεξιοτήτων που απαιτούνται για την ανάλυση των χαρακτηριστικών ασφάλειας και προστασίας των διαφόρων ψηφιακών πλατφορμών, την αναγνώριση πιθανών κινδύνων και την πρόταση μετριαστικών λύσεων για τη μείωση των τρωτών σημείων. Εφοδιασμένοι με αυτές τις δεξιότητες, οι εκπαιδευόμενοι μπορούν να θωρακιστούν από τις ψηφιακές απειλές και να ενεργήσουν ως ενεργά μέλη για την ασφάλεια στο διαδίκτυο στις κοινότητές τους. Αυτή η πτυχή του προγράμματος ενισχύει τη σημασία της συλλογικής δράσης για την προώθηση ενός ασφαλούς ψηφιακού περιβάλλοντος.

Το δεύτερο κρίσιμο μαθησιακό στοιχείο του μικροπιστοποιητικού "Συνείδηση της ασφάλειας στον κυβερνοχώρο και προστασία της ιδιωτικής ζωής" είναι η στρατηγική διαχείριση και αντιμετώπιση της κατάχρησης προσωπικών δεδομένων στις πλατφόρμες κοινωνικής δικτύωσης. Η εκθετική άνοδος των μέσων κοινωνικής δικτύωσης έχει επιφέρει πληθώρα ανησυχιών για την προστασία της ιδιωτικής ζωής και την ασφάλεια. Η κατάχρηση προσωπικών δεδομένων, που κυμαίνεται από την κλοπή ταυτότητας έως τη μη εξουσιοδοτημένη κοινοποίηση δεδομένων, ακόμη και την εμπορική εκμετάλλευση, είναι δυστυχώς συνηθισμένη. Ως εκ τούτου, είναι επιτακτική ανάγκη τα άτομα να μπορούν να διακρίνουν πότε τα προσωπικά τους δεδομένα έχουν παραβιαστεί και να μπορούν να λαμβάνουν τα κατάλληλα αντίμετρα. Αυτό το μικροπιστοποιητικό υποστηρίζει τους εκπαιδευόμενους στην εκμάθηση των απαραίτητων δεξιοτήτων για την αποτελεσματική διαχείριση της διαδικτυακής τους προσωπικότητας, τη ρύθμιση του ψηφιακού τους αποτυπώματος, την αναγνώριση των σημείων κατάχρησης προσωπικών δεδομένων και τη λήψη κατάλληλων

διορθωτικών μέτρων, όπως η αναφορά παραβιάσεων, ο αποκλεισμός μη εξουσιοδοτημένης πρόσβασης και η προστασία των προσωπικών δεδομένων.

Μια πρόσθετη μαθησιακή πτυχή που είναι συνυφασμένη με αυτό το μικροπιστοποιητικό είναι η εισαγωγή στις ηθικές και νομικές πτυχές της ψηφιακής ασφάλειας και προστασίας. Αυτή η εισαγωγή θα βοηθήσει τους εκπαιδευόμενους να κατανοήσουν το σύνθετο πλέγμα νόμων και κανονισμών που διέπουν το πεδίο της ψηφιακής ασφάλειας και προστασίας, επιτρέποντάς τους να τα αξιοποιήσουν για να προστατεύσουν τις διαδικτυακές τους ταυτότητες και τα προσωπικά τους δεδομένα. Η κατανόηση της νομιμότητας των ψηφιακών αλληλεπιδράσεων συμβάλλει στην προώθηση της υπεύθυνης και ενημερωμένης ψηφιακής ιδιότητας του πολίτη.

Ενσωματώνοντας αυτούς τους δύο βασικούς μαθησιακούς στόχους, το Μικροπιστοποιητικό Συνείδησης Κυβερνοασφάλειας και Προστασίας Προσωπικών Δεδομένων παρουσιάζει μια λεπτομερή και ολοκληρωμένη προοπτική για την ψηφιακή ασφάλεια και την προστασία των δεδομένων. Στόχος είναι να προικίσει τους εκπαιδευόμενους με τα απαραίτητα εργαλεία και τις γνώσεις για να διασφαλίσουν τη δική τους προστασία στην ψηφιακή σφαίρα και να διαδώσουν αυτή τη σοφία στην κοινότητά τους. Ως αποτέλεσμα, όσοι ολοκληρώσουν αυτό το πρόγραμμα θα είναι ικανοί να χειρίζονται τις ποικίλες προκλήσεις και ευκαιρίες του ψηφιακού κόσμου, περιηγούμενοι στο διαδικτυακό τοπίο με ασφάλεια και αυτοπεποίθηση.

Εν κατακλείδι, το Μικροπιστοποιητικό Συνείδησης Κυβερνοασφάλειας και Προστασίας Ιδιωτικού Απορρήτου χρησιμεύει ως ένα ζωτικό εργαλείο για όποιον θέλει να ελίσσεται στον ψηφιακό κόσμο με ασφάλεια και αυτοπεποίθηση. Προάγοντας τη βαθιά κατανόηση αυτών των κρίσιμων τομέων, οι εκπαιδευόμενοι όχι μόνο θα διασφαλίσουν τη δική τους ψηφιακή ασφάλεια αλλά και θα συμβάλουν σημαντικά στη διαμόρφωση ενός ασφαλέστερου ψηφιακού περιβάλλοντος για όλους. Μέσω της ολοκληρωμένης και λεπτομερούς προσέγγισής του, το πρόγραμμα αυτό ανταποκρίνεται στην επιτακτική ανάγκη για εκπαίδευση στην ψηφιακή ασφάλεια στον ολοένα και πιο συνδεδεμένο κόσμο μας.

Ερωτήσεις

1. Ποιες είναι μερικές από τις βασικές ψηφιακές απειλές που αναφέρονται στο Μικροπιστοποιητικό Συνείδησης για την Κυβερνοασφάλεια και την Προστασία της Ιδιωτικής Ζωής και ποια είναι η σημασία της αναγνώρισης αυτών των απειλών;
2. Ποιες δεξιότητες στοχεύει να αναπτύξει το Micro Credential, ώστε να βοηθήσει τα άτομα να αξιολογήσουν την ασφάλεια και την προστασία των διαφόρων ψηφιακών πλατφορμών;
3. Πώς μπορούν τα άτομα που είναι εφοδιασμένα με τις γνώσεις αυτού του μικροπιστοποιητικού να συμβάλουν στην προώθηση ενός ασφαλούς ψηφιακού περιβάλλοντος στις κοινότητές τους;
4. Ποιες είναι ορισμένες πιθανές μορφές κατάχρησης προσωπικών δεδομένων στις πλατφόρμες κοινωνικής δικτύωσης, όπως αναφέρεται στο Micro Credential, και γιατί είναι σημαντικό να τις αναγνωρίζετε;
5. Ποιες είναι οι συνιστώμενες ενέργειες στις οποίες μπορούν να προβούν τα άτομα όταν εντοπίζουν κατάχρηση των προσωπικών τους δεδομένων στα μέσα κοινωνικής δικτύωσης;
6. Με ποιους τρόπους το Micro Credential υποστηρίζει τους εκπαιδευόμενους να διαχειρίζονται αποτελεσματικά τις διαδικτυακές τους προσωπικότητες;
7. Πώς το Micro Credential καθοδηγεί τα άτομα να ρυθμίζουν το ψηφιακό τους αποτύπωμα;
8. Πώς η κατανόηση των ηθικών και νομικών πτυχών της ψηφιακής ασφάλειας και προστασίας συμβάλλει στην ενημερωμένη ψηφιακή ιδιότητα του πολίτη, σύμφωνα με το Micro Credential;

9. Πώς μπορούν τα άτομα να αξιοποιήσουν τους νόμους και τους κανονισμούς που διέπουν την ψηφιακή ασφάλεια και προστασία για την προστασία της διαδικτυακής τους ταυτότητας και των προσωπικών τους δεδομένων;
10. Με ποιους τρόπους το Micro Credential προετοιμάζει τους εκπαιδευόμενους να αντιμετωπίσουν τις ποικίλες προκλήσεις και ευκαιρίες του ψηφιακού κόσμου;
11. Πώς συμβάλλει το Μικροπιστοποιητικό Συνείδησης Κυβερνοασφάλειας και Προστασίας Ιδιωτικού Απορρήτου στη διαμόρφωση ενός ασφαλέστερου ψηφιακού περιβάλλοντος για όλους, σύμφωνα με τους στόχους του προγράμματος;

Ικανότητα ψηφιακού πολίτη και διαδικτυακής ασφάλειας (MC 4.2.B.2)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ψηφιακή Ιδιότητα του Πολίτη και επάρκεια διαδικτυακής ασφάλειας **Κωδ: B.2.B.2**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%

Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.23, 4.2.24 και 4.2.25):

- Χρήση της ηλεκτρονικής ταυτοποίησης για υπηρεσίες που παρέχονται από τις δημόσιες αρχές και τον επιχειρηματικό τομέα.
- Δώστε προτεραιότητα στην προστασία των δεδομένων κατά τη χρήση των μέσων κοινωνικής δικτύωσης για επαγγελματικούς ή εκπαιδευτικούς σκοπούς.
- Αναγνωρίστε τις διαδικτυακές απάτες και αναπτύξτε έναν υγιή σκεπτικισμό απέναντι σε μη ζητηθείσες προσφορές στο διαδίκτυο.

Περιγραφή

Στον κόσμο στον οποίο ζούμε, παρατηρούμε μια ολοένα και μεγαλύτερη εξάρτηση από τα ψηφιακά εργαλεία και τις πλατφόρμες, η ανάγκη να γνωρίζουν τα άτομα καλά τις διαδικτυακές πρακτικές ασφάλειας και προστασίας έχει γίνει υψίστης σημασίας. Το Micro Credential Digital Citizenship and Online Security Proficiency έχει ως στόχο να ενδυναμώσει τους εκπαιδευόμενους με τις απαραίτητες γνώσεις και δεξιότητες για την ασφαλή και υπεύθυνη πλοήγηση στον ψηφιακό κόσμο. Αυτό το ολοκληρωμένο μικροπιστοποιητικό καλύπτει τρεις βασικούς τομείς - τη χρήση ηλεκτρονικών ταυτοτήτων (e-ID), την προστασία δεδομένων κατά την επαγγελματική ή εκπαιδευτική χρήση των μέσων κοινωνικής δικτύωσης και την αναγνώριση και τον σκεπτικισμό απέναντι σε διαδικτυακές απάτες.

Το πρώτο μαθησιακό αποτέλεσμα αυτού του μικροπιστοποιητικού είναι η κατανόηση και η αποτελεσματική χρήση της ηλεκτρονικής ταυτοποίησης για υπηρεσίες που προσφέρονται από δημόσιες αρχές και επιχειρήσεις. Η εξάπλωση των ηλεκτρονικών υπηρεσιών σε διάφορους τομείς, από τις τράπεζες έως την εκπαίδευση, καθιστά αναγκαία την ανάγκη για ασφαλείς μεθόδους ταυτοποίησης.

Η ηλεκτρονική ταυτοποίηση παρέχει έναν ασφαλή και αποτελεσματικό τρόπο ηλεκτρονικής επαλήθευσης της ταυτότητας ενός ατόμου, εξαλείφοντας την ανάγκη για φυσικές μεθόδους ταυτοποίησης. Ωστόσο, η χρήση των ηλεκτρονικών ταυτοτήτων επιφέρει επίσης μοναδικές προκλήσεις όσον αφορά τη διασφάλιση της ιδιωτικής ζωής και της ασφάλειας των δεδομένων. Μέσω αυτού του μικροπιστοποιητικού, οι εκπαιδευόμενοι θα κατανοήσουν σε βάθος τα συστήματα ηλεκτρονικών ταυτοτήτων, συμπεριλαμβανομένων των αρχών λειτουργίας τους, των πλεονεκτημάτων τους και των πιθανών κινδύνων ασφαλείας. Το πρόγραμμα εμβαθύνει

επίσης στις βέλτιστες πρακτικές για τη χρήση των e-IDs, όπως ο τρόπος διατήρησης των δεδομένων των e-IDs και τι πρέπει να κάνετε σε περίπτωση πιθανής κλοπής ταυτότητας ή παραβίασης δεδομένων.

Τι είναι το e-ID;

Η ηλεκτρονική ταυτοποίηση, συχνά αναφερόμενη ως e-ID, είναι μια ψηφιακή λύση για την απόδειξη της ταυτότητας. Γίνεται όλο και πιο σημαντική σε έναν κόσμο όπου οι συναλλαγές και οι αλληλεπιδράσεις πραγματοποιούνται όλο και συχνότερα ηλεκτρονικά.

Οι ηλεκτρονικές ταυτότητες είναι ψηφιακά αντίγραφα των φυσικών δελτίων ταυτότητας και εγγράφων. Πιστοποιούν την ταυτότητα του χρήστη, επιτρέποντας ασφαλείς ηλεκτρονικές συναλλαγές και αλληλεπιδράσεις. Η χρήση των ηλεκτρονικών ταυτοτήτων εκτείνεται σε διάφορους τομείς, περιλαμβάνοντας υπηρεσίες που παρέχονται τόσο από δημόσιες αρχές όσο και από επιχειρηματικές οντότητες.

Στον δημόσιο τομέα, η ηλεκτρονική ταυτοποίηση μπορεί να απλοποιήσει και να διασφαλίσει διαδικασίες όπως η υποβολή φορολογικών δηλώσεων, η υποβολή αιτήσεων για παροχές, η ψηφοφορία και άλλες αστικές δραστηριότητες.

Οι κυβερνήσεις σε όλο τον κόσμο εφαρμόζουν συστήματα e-ID για να διασφαλίσουν την ψηφιακή ταυτότητα των πολιτών τους, διευκολύνοντας έτσι την αποτελεσματική παροχή δημόσιων υπηρεσιών.

Στον επιχειρηματικό τομέα, η χρήση της ηλεκτρονικής ταυτοποίησης είναι διάχυτη σε πολλούς τομείς. Για παράδειγμα, στον τραπεζικό και χρηματοπιστωτικό τομέα, η ηλεκτρονική ταυτότητα χρησιμοποιείται για την επαλήθευση της ταυτότητας για την πρόληψη της απάτης κατά τις συναλλαγές, τη δημιουργία λογαριασμού και την πρόσβαση σε χρηματοπιστωτικές υπηρεσίες. Στον τομέα του ηλεκτρονικού εμπορίου, η ηλεκτρονική ταυτότητα μπορεί να βοηθήσει στη διασφάλιση της ασφαλούς συναλλαγής αγαθών και υπηρεσιών, προστατεύοντας τόσο τους καταναλωτές όσο και τις επιχειρήσεις από την απάτη. Στον τομέα της υγειονομικής περίθαλψης, η ηλεκτρονική ταυτοποίηση μπορεί να χρησιμοποιηθεί για την ασφαλή πρόσβαση σε προσωπικά αρχεία υγείας, τον προγραμματισμό ραντεβού και τη διεξαγωγή διαβουλεύσεων τηλεϊατρικής.

Παρά την ευρεία χρήση και τα προφανή οφέλη, η ηλεκτρονική ταυτοποίηση επιφέρει και τις δικές της προκλήσεις. Οι κυριότερες από αυτές είναι οι ανησυχίες για την προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων. Οι ηλεκτρονικές ταυτότητες, εάν δεν προστατεύονται σωστά, μπορεί να είναι ευάλωτες σε μη εξουσιοδοτημένη πρόσβαση, πειρατεία ή ακόμη και κλοπή ταυτότητας. Ως εκ τούτου, οι χρήστες πρέπει να κατανοήσουν τους μηχανισμούς των συστημάτων ηλεκτρονικών ταυτοτήτων, την ασφαλή αποθήκευση και διαχείριση των διαπιστευτηρίων τους, καθώς και τις διαδικασίες που πρέπει να ακολουθήσουν σε περίπτωση υποψίας παραβίασης.

Το Micro Credential Digital Citizenship and Online Security Mastery αναγνωρίζει τη σημασία της ηλεκτρονικής ταυτότητας στον σύγχρονο ψηφιακό κόσμο. Στόχος του είναι να παρέχει στους εκπαιδευόμενους μια εις βάθος κατανόηση των αρχών λειτουργίας της ηλεκτρονικής ταυτότητας, των πλεονεκτημάτων της, των πιθανών κινδύνων ασφαλείας και των βέλτιστων πρακτικών για την ασφαλή χρήση της ηλεκτρονικής ταυτότητας. Οι εκπαιδευόμενοι ενημερώνονται για τις αποχρώσεις της διατήρησης της ασφάλειας των δεδομένων ηλεκτρονικής ταυτοποίησης και για τα βήματα που πρέπει να ακολουθήσουν εάν υποπτεύονται ότι τα δεδομένα τους έχουν παραβιαστεί.

Επενδύοντας χρόνο στην κατανόηση της ηλεκτρονικής ταυτοποίησης και των σχετικών πτυχών ασφαλείας, τα άτομα μπορούν να αξιοποιήσουν τις δυνατότητες των ψηφιακών υπηρεσιών, διασφαλίζοντας παράλληλα την

προστασία της ταυτότητάς τους. Το Micro Credential διασφαλίζει ότι οι εκπαιδευόμενοι είναι εφοδιασμένοι με τις γνώσεις και τα εργαλεία για να περιηγηθούν σε αυτόν τον πολύπλοκο αλλά ουσιαστικό τομέα του ψηφιακού κόσμου.

Το δεύτερο μαθησιακό αποτέλεσμα είναι η κατανόηση και η ιεράρχηση της προστασίας των δεδομένων κατά τη χρήση των μέσων κοινωνικής δικτύωσης για επαγγελματικούς ή εκπαιδευτικούς σκοπούς. Με την αυξανόμενη χρήση των πλατφορμών κοινωνικών μέσων για την εργασία και την εκπαίδευση, η ασφάλεια των προσωπικών και επαγγελματικών δεδομένων δεν ήταν ποτέ πιο κρίσιμη. Αυτό το μικροπιστοποιητικό εκπαιδεύει τους εκπαιδευόμενους σχετικά με τους πιθανούς κινδύνους που συνδέονται με την επαγγελματική ή εκπαιδευτική χρήση των μέσων κοινωνικής δικτύωσης, όπως η ακούσια διαρροή δεδομένων ή η κατάχρηση δεδομένων από τρίτους. Παρέχει επίσης ολοκληρωμένη κατάρτιση σχετικά με τις ρυθμίσεις απορρήτου, τις ασφαλείς πρακτικές κοινής χρήσης δεδομένων και τη διαχείριση των ψηφιακών αποτυπωμάτων. Επιπλέον, οι εκπαιδευόμενοι θα αποκτήσουν βαθιά κατανόηση των σχετικών νόμων και κανονισμών για την προστασία των δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), επιτρέποντάς τους να κατανοήσουν τα δικαιώματα και τις ευθύνες τους όσον αφορά την προστασία των δεδομένων.

Το δεύτερο μαθησιακό αποτέλεσμα του μικροπιστοποιητικού Digital Citizenship and Online Security Proficiency περιστρέφεται γύρω από την κατανόηση και την ιεράρχηση της προστασίας των δεδομένων κατά τη χρήση των μέσων κοινωνικής δικτύωσης για επαγγελματικούς ή εκπαιδευτικούς σκοπούς. Η εστίαση αυτή είναι υψίστης σημασίας σε μια εποχή όπου οι πλατφόρμες των μέσων κοινωνικής δικτύωσης αποτελούν αναπόσπαστο μέρος πολλών πτυχών της ζωής, συμπεριλαμβανομένης της εργασίας και της εκπαίδευσης.

Οι πλατφόρμες κοινωνικής δικτύωσης, ενώ παρέχουν ευκαιρίες για συνδεσιμότητα, ανταλλαγή πληροφοριών και συνεργασία, μπορούν επίσης να παρουσιάσουν σημαντικούς κινδύνους για την προστασία της ιδιωτικής ζωής. Οι κίνδυνοι αυτοί είναι ιδιαίτερα έντονοι όταν οι πλατφόρμες αυτές χρησιμοποιούνται για επαγγελματικούς ή εκπαιδευτικούς σκοπούς. Για παράδειγμα, τα άτομα μπορεί να μοιράζονται ευαίσθητες πληροφορίες που αφορούν τον χώρο εργασίας τους ή το εκπαιδευτικό τους ίδρυμα, εκθέτοντας εν αγνοία τους τους εαυτούς τους σε διαρροές δεδομένων ή παραβιάσεις.

Η κατανόηση αυτών των δυνητικών κινδύνων αποτελεί κρίσιμη πτυχή αυτού του μαθησιακού αποτελέσματος. Οι εκπαιδευόμενοι θα ενημερωθούν για τις συνήθεις απειλές ασφάλειας δεδομένων που σχετίζονται με την επαγγελματική ή εκπαιδευτική χρήση των μέσων κοινωνικής δικτύωσης, όπως η μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς, η ακούσια διαρροή δεδομένων και η κατάχρηση δεδομένων από τρίτους.

Επιπλέον, οι εκπαιδευόμενοι διδάσκονται τη σημασία της προστασίας των δεδομένων στα μέσα κοινωνικής δικτύωσης και εισάγονται σε αποτελεσματικές στρατηγικές για την προστασία των πληροφοριών τους. Αυτό περιλαμβάνει την εκμάθηση των ρυθμίσεων απορρήτου στις διάφορες πλατφόρμες, τη γνώση του ποιες πληροφορίες πρέπει να μοιράζονται και ποιες να διατηρούνται ιδιωτικές και την κατανόηση των επιπτώσεων του ψηφιακού τους αποτυπώματος. Οι μαθητές ενθαρρύνονται επίσης να αναπτύξουν τη συνήθεια να ελέγχουν και να ενημερώνουν τακτικά τις ρυθμίσεις απορρήτου τους σύμφωνα με τα επίπεδα άνεσης και τις απαιτήσεις τους.

Επιπλέον, αυτό το μαθησιακό αποτέλεσμα εισάγει τους εκπαιδευόμενους στις νομικές πτυχές της προστασίας δεδομένων. Αυτό θα μπορούσε να περιλαμβάνει τη μελέτη κανονισμών όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) και την κατανόηση του τρόπου με τον οποίο οι κανονισμοί αυτοί προστατεύουν τα δικαιώματά τους στο διαδίκτυο. Τέτοιες γνώσεις είναι ανεκτίμητες στο επαγγελματικό ή εκπαιδευτικό περιβάλλον, όπου η συμμόρφωση με τους νόμους περί προστασίας δεδομένων είναι συχνά υποχρεωτική.

Επιπλέον, το πρόγραμμα παρέχει πληροφορίες σχετικά με τις βέλτιστες πρακτικές για την ασφαλή ανταλλαγή δεδομένων και την επαγγελματική συνεργασία με άλλους σε αυτές τις πλατφόρμες. Αυτό καλύπτει πτυχές όπως η ασφαλής επικοινωνία, η ασφαλής κοινή χρήση αρχείων και εγγράφων και η αναγνώριση και αποφυγή δυνητικά επιβλαβών συνδέσμων ή συνημμένων αρχείων.

Η κατανόηση και η ιεράρχηση της προστασίας των δεδομένων κατά τη χρήση των μέσων κοινωνικής δικτύωσης για επαγγελματικούς ή εκπαιδευτικούς σκοπούς είναι μια σύνθετη, αλλά ζωτικής σημασίας δεξιότητα στη σημερινή ψηφιακή εποχή. Κατακτώντας αυτό το μαθησιακό αποτέλεσμα, τα άτομα μπορούν να χρησιμοποιούν με αυτοπεποίθηση και ασφάλεια τα μέσα κοινωνικής δικτύωσης για την επαγγελματική και εκπαιδευτική τους ανέλιξη, διασφαλίζοντας παράλληλα ότι τα προσωπικά τους δεδομένα παραμένουν ασφαλή.

Το τρίτο μαθησιακό αποτέλεσμα επικεντρώνεται στην αναγνώριση των διαδικτυακών απάτης και στην ανάπτυξη ενός υγιούς σκεπτικισμού απέναντι σε ανεπιθύμητες προσφορές στο διαδίκτυο. Στην ψηφιακή εποχή, οι απάτες έχουν γίνει όλο και πιο εξελιγμένες, καθιστώντας απαραίτητο για τα άτομα να παραμένουν σε εγρήγορση και να αντιμετωπίζουν με σκεπτικισμό τις πιθανές απειλές. Αυτό το μικροπιστοποιητικό παρέχει μια επισκόπηση των κοινών τύπων διαδικτυακών απατών, όπως το phishing, το κακόβουλο λογισμικό και η κλοπή ταυτότητας. Παρέχει επίσης πρακτικές στρατηγικές για τον εντοπισμό απάτης, συμπεριλαμβανομένης της αναγνώρισης ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου, συνδέσμων και ιστότοπων και της επαλήθευσης της αυθεντικότητας μη ζητηθέντων προσφορών. Το πρόγραμμα παρέχει επίσης καθοδήγηση σχετικά με το τι πρέπει να κάνει κανείς αν πέσει θύμα απάτης, συμπεριλαμβανομένων των μηχανισμών αναφοράς και των βημάτων για τον περιορισμό της ζημίας.

Το τρίτο μαθησιακό αποτέλεσμα του Micro Credential Digital Citizenship and Online Security Proficiency επικεντρώνεται στην αναγνώριση των διαδικτυακών απάτων και στην καλλιέργεια ενός υγιούς σκεπτικισμού απέναντι σε ανεπιθύμητες προσφορές στο διαδίκτυο. Αυτή η κατανόηση είναι ζωτικής σημασίας στο σημερινό ψηφιακό τοπίο, όπου οι απάτες και οι δόλιες δραστηριότητες είναι όλο και πιο εξελιγμένες και διαδεδομένες.

Οι διαδικτυακές απάτες έχουν πολλές μορφές και συχνά εκμεταλλεύονται την έλλειψη γνώσεων των ατόμων σχετικά με τις ασφαλείς πρακτικές του διαδικτύου. Μεταξύ των πιο συνηθισμένων απάτης είναι οι απόπειρες phishing, όπου οι απατεώνες υποδύονται νόμιμες οντότητες για να εξαπατήσουν τους χρήστες ώστε να αποκαλύψουν προσωπικές πληροφορίες, και η απάτη με προκαταβολές, όπου οι απατεώνες υπόσχονται μεγάλες αποδόσεις με αντάλλαγμα μια προκαταβολική αμοιβή. Άλλες απάτες μπορεί να αφορούν ψεύτικες λοταρίες ή βραβεία, απατηλές διαδικτυακές αγορές ή ακόμη και απάτες ρομαντικών σχέσεων που εκμεταλλεύονται τους μοναχικούς και ευάλωτους.

Μέσω αυτού του μικροπιστοποιητικού, οι εκπαιδευόμενοι εισάγονται στους διάφορους τύπους διαδικτυακών απατών και στον τρόπο λειτουργίας τους. Μαθαίνουν να αναγνωρίζουν τα σημάδια των απάτης, τα οποία μπορεί να περιλαμβάνουν μη ζητηθείσες επικοινωνίες, τακτικές πίεσης, υπερβολικά καλές προσφορές, αιτήματα για ευαίσθητες πληροφορίες και ασυνήθιστες μεθόδους πληρωμής.

Επιπλέον, οι εκπαιδευόμενοι είναι εφοδιασμένοι με τα εργαλεία και τις στρατηγικές για να επαληθεύουν τη γνησιότητα των μη ζητηθέντων προσφορών. Αυτά μπορεί να περιλαμβάνουν τεχνικές όπως ο έλεγχος της διεύθυνσης ηλεκτρονικού ταχυδρομείου ή της διεύθυνσης URL του αποστολέα για ανωμαλίες, η έρευνα της προσφοράς ή του αποστολέα στο διαδίκτυο, η απευθείας επικοινωνία με τον υποτιθέμενο αποστολέα μέσω μιας επαληθευμένης μεθόδου και η μη επιλογή ύποπτων συνδέσμων ή συνημμένων αρχείων.

Βασικό μέρος αυτού του μαθησιακού αποτελέσματος είναι η καλλιέργεια ενός υγιούς σκεπτικισμού απέναντι σε ανεπιθύμητες προσφορές στο διαδίκτυο. Οι εκπαιδευόμενοι ενθαρρύνονται να αμφισβητούν τη νομιμότητα

των απροσδόκητων προσφορών και να αφιερώνουν πάντα χρόνο για να επαληθεύουν πριν συμμετάσχουν. Τους υπενθυμίζεται ότι οι νόμιμες οντότητες σπάνια, αν ποτέ, ζητούν ευαίσθητες πληροφορίες ή πληρωμές μέσω ηλεκτρονικού ταχυδρομείου ή γραπτού μηνύματος.

Σημαντικό είναι επίσης να παρέχεται στους εκπαιδευόμενους καθοδήγηση σχετικά με το τι πρέπει να κάνουν αν πέσουν θύματα απάτης. Αυτό περιλαμβάνει άμεσα βήματα όπως η επικοινωνία με την τράπεζα ή την εταιρεία πιστωτικών καρτών τους, η αλλαγή κωδικών πρόσβασης και η αναφορά της απάτης στις τοπικές αστυνομικές αρχές και στις διαδικτυακές πλατφόρμες. Εκπαιδεύονται επίσης για πιο μακροπρόθεσμα μέτρα, όπως η παρακολούθηση των πιστωτικών τους αναφορών για ενδείξεις κλοπής ταυτότητας.

Η ικανότητα να αναγνωρίζετε τις διαδικτυακές απάτες και να διατηρείτε έναν υγιή σκεπτικισμό απέναντι στις ανεπιθύμητες προσφορές στο διαδίκτυο αποτελεί βασική δεξιότητα για την πλοήγηση στον ψηφιακό κόσμο. Μέσω αυτού του μαθησιακού αποτελέσματος, τα άτομα εφοδιάζονται με τις γνώσεις και τα εργαλεία για να προστατεύονται από τις διαδικτυακές απάτες, συμβάλλοντας σε ένα ασφαλέστερο και ασφαλέστερο διαδικτυακό περιβάλλον.

Συνοπτικά, το Micro Credential Digital Citizenship and Online Security Proficiency παρέχει στους εκπαιδευόμενους μια ολοκληρωμένη κατανόηση τριών κρίσιμων πτυχών της διαδικτυακής ασφάλειας - ηλεκτρονική ταυτοποίηση, προστασία δεδομένων στα μέσα κοινωνικής δικτύωσης και διαδικτυακές απάτες. Με την ολοκλήρωση αυτού του προγράμματος, οι εκπαιδευόμενοι θα είναι εφοδιασμένοι με τις γνώσεις και τις δεξιότητες να περιηγούνται με ασφάλεια στον ψηφιακό κόσμο, να προστατεύουν τα προσωπικά και επαγγελματικά τους δεδομένα και να υπερασπίζονται ασφαλείς και υπεύθυνες ψηφιακές πρακτικές στις κοινότητές τους.

Αυτό το εμπεριστατωμένο, λεπτομερές πρόγραμμα απαιτεί σημαντική δέσμευση από τους εκπαιδευόμενους, αλλά υπόσχεται να προσφέρει κρίσιμες γνώσεις και δεξιότητες που γίνονται όλο και πιο απαραίτητες στον σύγχρονο ψηφιακό κόσμο. Καθώς η ζωή μας γίνεται όλο και πιο συνυφασμένη με τις ψηφιακές τεχνολογίες, αυτό το μικροπιστοποιητικό αποτελεί μια κρίσιμη επένδυση στην ατομική και συλλογική ψηφιακή ασφάλεια και προστασία.

Ερωτήσεις

1. Τι είναι η ηλεκτρονική ταυτοποίηση (e-ID) και γιατί είναι σημαντική στον σημερινό ψηφιακό κόσμο;
2. Ποιοι είναι οι πιθανοί κίνδυνοι ασφαλείας που συνδέονται με τη χρήση της ηλεκτρονικής ταυτότητας και πώς μπορούν να μετριαστούν;
3. Εξηγήστε τις βέλτιστες πρακτικές για την ασφαλή χρήση του e-ID.
4. Ποια μέτρα πρέπει να ληφθούν εάν ένα άτομο υποπτεύεται ότι τα δεδομένα του e-ID έχουν παραβιαστεί;
5. Γιατί η προστασία των δεδομένων είναι ζωτικής σημασίας όταν χρησιμοποιείτε τα μέσα κοινωνικής δικτύωσης για επαγγελματικούς ή εκπαιδευτικούς σκοπούς;
6. Ποιες είναι ορισμένες κοινές απειλές για την ασφάλεια των δεδομένων που σχετίζονται με την επαγγελματική ή εκπαιδευτική χρήση των μέσων κοινωνικής δικτύωσης;
7. Πώς μπορεί ένα άτομο να διαχειριστεί αποτελεσματικά το ψηφιακό του αποτύπωμα στις πλατφόρμες κοινωνικής δικτύωσης;
8. Περιγράψτε το ρόλο των νόμων και των κανονισμών, όπως ο ΓΚΠΔ, στην προστασία των δεδομένων στα μέσα κοινωνικής δικτύωσης.

9. Ποιες είναι οι βέλτιστες πρακτικές για την ασφαλή ανταλλαγή δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης για επαγγελματικούς ή εκπαιδευτικούς σκοπούς;
10. Ορισμός των διαδικτυακών απάτης και παραδείγματα κοινών τύπων απάτης που μπορεί να συναντήσουν τα άτομα στο διαδίκτυο.
11. Ποιες είναι κάποιες κόκκινες σημαίες ή σημάδια ηλεκτρονικών απάτης που πρέπει να γνωρίζουν οι πολίτες;
12. Εξηγήστε τις τεχνικές επαλήθευσης της αυθεντικότητας των μη ζητηθέντων προσφορών στο διαδίκτυο.
13. Συζητήστε τη σημασία της ανάπτυξης ενός υγιούς σκεπτικισμού απέναντι σε ανεπιθύμητες προσφορές στο διαδίκτυο.
14. Τι άμεσες ενέργειες πρέπει να κάνει κάποιος αν πέσει θύμα ηλεκτρονικής απάτης;
15. Ποια είναι ορισμένα μακροπρόθεσμα μέτρα που μπορούν να λάβουν τα άτομα που πέφτουν θύματα μιας διαδικτυακής απάτης;

Βέλτιστες πρακτικές κυβερνοασφάλειας και αξιολόγηση διαδικτυακής συμπεριφοράς (MC 4.2.B.3)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Βέλτιστες πρακτικές κυβερνοασφάλειας και αξιολόγηση διαδικτυακής συμπεριφοράς **Κωδ: B.3**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες

Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.26 και 4.2.27):

- Προετοιμάστε τον υπολογιστή και το smartphone σας εγκαθιστώντας και ενημερώνοντας το απαραίτητο λογισμικό ασφαλείας.
- Βαθμολογήστε τις διαδικτυακές σας συνήθειες ως προς τον κίνδυνο ασφαλείας τους.

Περιγραφή

Στην επικρατούσα ψηφιακή εποχή, όπου η χρήση τεχνολογικών συσκευών όπως οι υπολογιστές και τα smartphones έχει γίνει καθημερινό φαινόμενο, η κατανόηση των πρακτικών κυβερνοασφάλειας και η διαχείριση της διαδικτυακής συμπεριφοράς είναι ζωτικής σημασίας. Το πρόγραμμα "Βέλτιστες πρακτικές κυβερνοασφάλειας και αξιολόγηση της διαδικτυακής συμπεριφοράς" Micro Credential εστιάζει σε αυτά τα δύο βασικά στοιχεία, καθοδηγώντας τους εκπαιδευόμενους τόσο να προετοιμάζουν τις ψηφιακές συσκευές τους μέσω κατάλληλων μέτρων ασφαλείας όσο και να αξιολογούν τις διαδικτυακές τους συνήθειες στο πλαίσιο του κινδύνου ασφαλείας.

Το πρώτο μαθησιακό αποτέλεσμα αφορά την παροχή στους εκπαιδευόμενους της δυνατότητας να προετοιμάζουν αποτελεσματικά τους υπολογιστές και τα smartphones τους μέσω της εγκατάστασης και τακτικής ενημέρωσης κρίσιμου λογισμικού ασφαλείας. Οι τεχνολογικές συσκευές αποτελούν αναπόσπαστο μέρος της ζωής μας, αποθηκεύοντας ευαίσθητα δεδομένα που κυμαίνονται από προσωπικές πληροφορίες έως επαγγελματικά έγγραφα.

Ως εκ τούτου, η διασφάλιση της ασφάλειας αυτών των συσκευών καθίσταται υψίστης σημασίας.

Η εγκατάσταση λογισμικού ασφαλείας είναι ένα πρώτο βήμα για την προστασία αυτών των συσκευών. Το λογισμικό ασφαλείας χρησιμεύει ως αμυντικό τείχος ενάντια σε διάφορες διαδικτυακές απειλές, όπως ιούς, κακόβουλο λογισμικό, ransomware και spyware. Η γκάμα του λογισμικού ασφαλείας περιλαμβάνει, μεταξύ άλλων, προγράμματα προστασίας από ιούς, τείχη προστασίας, προγράμματα προστασίας από προγράμματα κατασκοπείας και εργαλεία κρυπτογράφησης. Αυτό το μαθησιακό αποτέλεσμα καλύπτει την κατανόηση των διαφόρων τύπων λογισμικού ασφαλείας, των συγκεκριμένων ρόλων τους και τη σημασία της διατήρησης των πιο πρόσφατων εκδόσεων.

Η τακτική ενημέρωση του λογισμικού ασφαλείας είναι εξίσου κρίσιμη. Οι απειλές στον κυβερνοχώρο εξελίσσονται συνεχώς, με νέους τύπους ιών και κακόβουλου λογισμικού να εμφανίζονται τακτικά. Για την καταπολέμηση αυτών των εξελισσόμενων απειλών, οι πάροχοι λογισμικού ασφαλείας κυκλοφορούν τακτικά ενημερώσεις, διορθώσεις και βελτιώσεις στα προγράμματά τους. Αυτές οι ενημερώσεις περιέχουν σημαντικές βελτιώσεις και νέες άμυνες κατά των απειλών που εντοπίστηκαν πρόσφατα.

Το πρόγραμμα παρέχει κατανόηση της διαδικασίας ενημέρωσης, των κινδύνων που σχετίζονται με το ξεπερασμένο λογισμικό ασφαλείας και της σημασίας της διατήρησης όλου του λογισμικού, συμπεριλαμβανομένων των λειτουργικών συστημάτων, των προγραμμάτων περιήγησης στο διαδίκτυο και των εφαρμογών, σε ισχύ.

Επιπλέον, το μάθημα αναφέρεται σε άλλες πρακτικές ασφαλείας, όπως η δημιουργία ισχυρών κωδικών πρόσβασης, ο έλεγχος ταυτότητας δύο παραγόντων και οι συνήθειες ασφαλούς περιήγησης.

Το Micro Credential στοχεύει στη δημιουργία μιας σταθερής βάσης διασφάλισης της ασφάλειας σε υπολογιστές και smartphones μέσω της εγκατάστασης και της τακτικής ενημέρωσης του σχετικού λογισμικού.

Η ασφάλεια λογισμικού είναι ένας ευρύς όρος που περιλαμβάνει μια ποικιλία εφαρμογών που έχουν αναπτυχθεί για τη θωράκιση των υπολογιστών και των smartphones από ψηφιακές απειλές. Περιλαμβάνει προγράμματα προστασίας από ιούς που έχουν σχεδιαστεί για τον εντοπισμό, την εξάλειψη και την άμυνα κατά ιών και άλλων ειδών κακόβουλου λογισμικού, τείχη προστασίας που διαχειρίζονται και αποκλείουν τη μη εξουσιοδοτημένη πρόσβαση στη συσκευή, λογισμικό anti-spyware που προστατεύει από τη μη εξουσιοδοτημένη συλλογή δεδομένων και εργαλεία κρυπτογράφησης που διασφαλίζουν τα δεδομένα μετατρέποντάς τα σε μορφή που μπορεί να αποκρυπτογραφηθεί μόνο με το κατάλληλο κλειδί.

Αυτό το μαθησιακό αποτέλεσμα επικεντρώνεται στη μετάδοση γνώσεων σχετικά με τη σημασία κάθε τύπου λογισμικού για τη διατήρηση της ασφάλειας της συσκευής. Δίνει επίσης έμφαση στην αναγκαιότητα μιας συνεκτικής προσέγγισης της ασφάλειας, όπου οι διάφοροι τύποι λογισμικού δημιουργούν συλλογικά ένα εκτεταμένο φράγμα ασφαλείας.

Η συχνότητα ενημέρωσης όλου του εγκατεστημένου λογισμικού ασφαλείας είναι ένα άλλο καίριο στοιχείο της ασφάλειας της συσκευής. Με τη διαρκώς εξελισσόμενη φύση των απειλών στον κυβερνοχώρο και την εμφάνιση συνεχώς νέων τύπων ιών και κακόβουλου λογισμικού, οι πάροχοι λογισμικού ασφαλείας κυκλοφορούν τακτικά ενημερώσεις που περιλαμβάνουν βελτιώσεις, επίλυση υφιστάμενων προβλημάτων και νέες άμυνες κατά αυτών των εξελισσόμενων απειλών. Διατηρώντας το λογισμικό ασφαλείας τους ενημερωμένο, οι χρήστες μπορούν να εξασφαλίσουν τη βέλτιστη άμυνα των συσκευών τους έναντι των επικρατούντων απειλών.

Αυτό το μαθησιακό αποτέλεσμα περιλαμβάνει επίσης άλλα μέτρα ασφαλείας, όπως οι περιοδικές ενημερώσεις του λειτουργικού συστήματος και των εφαρμογών, οι ασφαλείς πρακτικές χρήσης κωδικών πρόσβασης, ο

έλεγχος ταυτότητας δύο παραγόντων και οι συνήθειες ασφαλούς περιήγησης, που συνολικά αποτελούν ένα ολοκληρωμένο πρωτόκολλο ασφαλείας για την προστασία των χρηστών από τις περισσότερες ψηφιακές απειλές.

Το δεύτερο μαθησιακό αποτέλεσμα αφορά την ανάπτυξη δεξιοτήτων αξιολόγησης των διαδικτυακών συνηθειών όσον αφορά τον κίνδυνο ασφαλείας τους. Το διαδίκτυο, ενώ αποτελεί έναν τεράστιο πόρο, κρύβει επίσης πιθανές απειλές για την ασφάλεια. Οι διαδικτυακές συνήθειες ενός ατόμου μπορούν να επηρεάσουν σημαντικά την έκθεσή του σε αυτές τις απειλές.

Αυτό το μαθησιακό αποτέλεσμα καθοδηγεί τους εκπαιδευόμενους σχετικά με την έννοια του κινδύνου στο πλαίσιο της διαδικτυακής συμπεριφοράς. Παρέχει μια επισκόπηση των συνήθων διαδικτυακών συμπεριφορών υψηλού κινδύνου, όπως το κλικ σε άγνωστους συνδέσμους, η χρήση μη ασφαλών δικτύων Wi-Fi και η κοινοποίηση ευαίσθητων πληροφοριών στο διαδίκτυο. Επισημαίνει επίσης συνήθειες χαμηλού κινδύνου που ενισχύουν την ασφάλεια στο διαδίκτυο, όπως η επίσκεψη μόνο σε ιστότοπους που είναι ασφαλείς με HTTPS, η αποσύνδεση από λογαριασμούς όταν δεν χρησιμοποιούνται και η τακτική ενημέρωση των ρυθμίσεων απορρήτου.

Μέσω αυτού του προγράμματος, οι εκπαιδευόμενοι αναπτύσσουν την ικανότητα να αναλύουν κριτικά τις διαδικτυακές τους συνήθειες, να διακρίνουν μεταξύ συμπεριφορών υψηλού και χαμηλού κινδύνου και να κάνουν τις απαραίτητες προσαρμογές για να ενισχύσουν την διαδικτυακή τους ασφάλεια. Αυτό το μαθησιακό αποτέλεσμα δεν καλύπτει μόνο τις προσωπικές συνήθειες, αλλά επεκτείνεται και στην επαγγελματική συμπεριφορά, αναδεικνύοντας τη σημασία των ασφαλών διαδικτυακών συνηθειών για την προστασία όχι μόνο των ατόμων, αλλά και των χώρων εργασίας και των ιδρυμάτων.

Οι ενέργειες και οι συνήθειες που επιδεικνύουν τα άτομα στο διαδίκτυο επηρεάζουν σημαντικά την ευαισθησία τους σε απειλές στον κυβερνοχώρο. Ορισμένες πρακτικές, όπως η πλοήγηση μόνο σε ασφαλείς ιστότοπους HTTPS, η χρήση ισχυρών, διακριτών κωδικών πρόσβασης και η αποσύνδεση από λογαριασμούς όταν δεν χρησιμοποιούνται, μπορούν να μειώσουν σημαντικά τον κίνδυνο να πέσουν θύματα κυβερνοαπειλών.

Από την άλλη πλευρά, ενέργειες υψηλού κινδύνου, όπως το κλικ σε συνδέσμους από άγνωστα μηνύματα ηλεκτρονικού ταχυδρομείου, η χρήση μη ασφαλών δικτύων Wi-Fi και η αποκάλυψη υπερβολικών προσωπικών πληροφοριών στο διαδίκτυο μπορούν να αυξήσουν σημαντικά τον κίνδυνο αυτό.

Σε αυτό το μαθησιακό αποτέλεσμα, τα άτομα διδάσκονται να αξιολογούν κριτικά τη διαδικτυακή τους συμπεριφορά. Εκπαιδεύονται να αναγνωρίζουν συμπεριφορές που θα μπορούσαν ενδεχομένως να τους εκθέσουν σε κινδύνους και οπλίζονται με τη γνώση να προσαρμόζουν τις συνήθειές τους για τη βελτίωση της ασφάλειας.

Το σημαντικότερο είναι ότι η ανάλυση αυτή δεν περιορίζεται στις προσωπικές συνήθειες. Το μάθημα καλύπτει επίσης τον αντίκτυπο της διαδικτυακής συμπεριφοράς σε εργασιακό πλαίσιο. Με την αυξανόμενη εξάρτηση από τις ψηφιακές πλατφόρμες στους χώρους εργασίας, οι ασφαλείς διαδικτυακές πρακτικές έχουν καταστεί απαραίτητες για την προστασία όχι μόνο των ατόμων αλλά και των επιχειρήσεων και των ιδρυμάτων.

Συνοψίζοντας, το πρόγραμμα Μικροπιστοποιητικό Αξιολόγησης Βέλτιστων Πρακτικών Κυβερνοασφάλειας και Διαδικτυακής Συμπεριφοράς δίνει στους εκπαιδευόμενους τη δυνατότητα να βελτιώσουν την ψηφιακή τους ασφάλεια μέσω της αποτελεσματικής προετοιμασίας των συσκευών τους και της προσεκτικής εξέτασης των διαδικτυακών τους συνηθειών. Με την ολοκλήρωση αυτού του προγράμματος, τα άτομα όχι μόνο θα βελτιώσουν τη δική τους ψηφιακή ασφάλεια αλλά και θα συμβάλουν σε μια ασφαλέστερη ψηφιακή κοινότητα.

Παρέχει μια ολοκληρωμένη κατανόηση και γνώση της προσωπικής κυβερνοασφάλειας, δημιουργώντας υπεύθυνους ψηφιακούς πολίτες καλά εξοπλισμένους για να περιηγούνται με ασφάλεια στο ψηφιακό τοπίο.

Ερωτήσεις

1. Ποια είναι η σημασία της εγκατάστασης λογισμικού ασφαλείας σε τεχνολογικές συσκευές όπως οι υπολογιστές και τα smartphones;
2. Ποιοι τύποι λογισμικού ασφαλείας είναι διαθέσιμοι και ποιος είναι ο συγκεκριμένος ρόλος τους στην προστασία των ψηφιακών συσκευών;
3. Γιατί είναι ζωτικής σημασίας να διατηρείτε το λογισμικό ασφαλείας ενημερωμένο; Πώς συμβάλλουν οι τακτικές ενημερώσεις στην ασφάλεια στον κυβερνοχώρο;
4. Ποιοι είναι μερικοί από τους κινδύνους που συνδέονται με τη χρήση ξεπερασμένου λογισμικού ασφαλείας;
5. Πέρα από την ενημέρωση του λογισμικού ασφαλείας, ποιες είναι άλλες σημαντικές πρακτικές για τη διασφάλιση της ασφάλειας των ψηφιακών συσκευών;
6. Πώς συμβάλλουν η ασφαλής δημιουργία κωδικού πρόσβασης και ο έλεγχος ταυτότητας δύο παραγόντων στη συνολική ασφάλεια της συσκευής;
7. Πώς επηρεάζουν οι ενέργειες και οι συνήθειες ενός ατόμου στο διαδίκτυο την ευαισθησία του σε απειλές στον κυβερνοχώρο;
8. Ποια είναι τα παραδείγματα διαδικτυακών συμπεριφορών υψηλού και χαμηλού κινδύνου στο πλαίσιο της κυβερνοασφάλειας;
9. Πώς μπορεί κανείς να αξιολογήσει κριτικά τη διαδικτυακή του συμπεριφορά για να εντοπίσει πιθανούς κινδύνους για την ασφάλεια;
10. Γιατί είναι σημαντικό να κάνετε τις απαραίτητες προσαρμογές στις διαδικτυακές συνήθειες για να ενισχύσετε την ασφάλεια;
11. Με ποιους τρόπους μπορούν οι ασφαλείς διαδικτυακές συνήθειες να προστατεύσουν όχι μόνο τα άτομα αλλά και τους χώρους εργασίας και τα ιδρύματα;
12. Πώς συμβάλλει το πρόγραμμα Μικροπιστοποιητικό Αξιολόγησης Βέλτιστων Πρακτικών Κυβερνοασφάλειας και Διαδικτυακής Συμπεριφοράς στη δημιουργία υπεύθυνων ψηφιακών πολιτών;
13. Πώς οι γνώσεις που αποκτώνται από το πρόγραμμα Micro Credential βελτιώνουν την προσωπική ψηφιακή ασφάλεια και συμβάλλουν σε μια ασφαλέστερη ψηφιακή κοινότητα;

Ολοκληρωμένη γνώση ψηφιακού απορρήτου, ασφάλειας παιδιών και ασφαλούς πλοήγησης (MC 4.2.B.4)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ολοκληρωμένος **κώδικας** επάρκειας ψηφιακού απορρήτου, ασφάλειας παιδιών και ασφαλούς περιήγησης: **B.4**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.28, 4.2.29 και 4.2.30):

- Συζητήστε ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα υπόκειται σε τοπικούς κανονισμούς όπως ο ΓΚΠΔ.
- Υποδείξτε την ύπαρξη φιλικών προς τα παιδιά προγραμμάτων περιήγησης και δείξτε ενδιαφέρον για την ασφάλεια των παιδιών στο διαδίκτυο, χρησιμοποιώντας ή συνιστώντας αυτά τα προγράμματα περιήγησης.
- Να διακρίνετε μεταξύ ασφαλών και μη ασφαλών ιστότοπων κατά την περιήγηση.

Περιγραφή

Το Comprehensive Digital Privacy, Child Safety, and Secure Browsing Proficiency Micro Credential είναι ένα πολύπλευρο πρόγραμμα που εμβαθύνει την κατανόηση και τις δεξιότητες των εκπαιδευομένων σχετικά με τρεις κρίσιμους τομείς της ψηφιακής ασφάλειας: νόμοι για την προστασία των προσωπικών δεδομένων, εργαλεία διαδικτύου για την ασφάλεια των παιδιών και αναγνώριση ασφαλών και μη ασφαλών ιστότοπων.

Το πρόγραμμα εξετάζει την κρίσιμη πτυχή της επεξεργασίας προσωπικών δεδομένων και τους σχετικούς κανονισμούς. Δεδομένου του όγκου των προσωπικών δεδομένων που κυκλοφορούν στο διαδίκτυο, η σημασία των νόμων για την προστασία της ιδιωτικής ζωής, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ), είναι σημαντική. Ο ΓΚΠΔ, ένας αυστηρός νόμος για την προστασία της ιδιωτικής ζωής και την ασφάλεια που εφαρμόζεται στην Ευρωπαϊκή Ένωση, έχει εκτεταμένες επιπτώσεις στη διαχείριση δεδομένων σε όλο τον κόσμο. Αυτό το πρόγραμμα προσφέρει ολοκληρωμένα μαθησιακά αποτελέσματα με επίκεντρο τον GDPR και παρόμοιους νόμους που έχουν σχεδιαστεί για την προστασία των προσωπικών δεδομένων. Αυτό περιλαμβάνει την κατανόηση του σκοπού και των βασικών στοιχείων αυτών των κανονισμών, την αναγνώριση των δικαιωμάτων των υποκειμένων των δεδομένων και τον προσδιορισμό των ευθυνών των υπευθύνων επεξεργασίας και των υπευθύνων επεξεργασίας δεδομένων.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα αναφέρεται σε κάθε ενέργεια που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, συμπεριλαμβανομένης της συλλογής, καταγραφής, οργάνωσης, διάρθρωσης, αποθήκευσης, προσαρμογής ή τροποποίησης, ανάκτησης, διαβούλευσης, χρήσης, κοινοποίησης με διαβίβαση, διάδοσης ή άλλης διάθεσης, ευθυγράμμισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής.

Η ρύθμιση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα έχει αποκτήσει κρίσιμη σημασία με την αύξηση της ψηφιοποίησης των υπηρεσιών και των δραστηριοτήτων. Νόμοι όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) στην Ευρωπαϊκή Ένωση δημιουργήθηκαν για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων των πολιτών.

Ο ΓΚΠΔ εγκρίθηκε το 2016 και τέθηκε σε ισχύ το 2018. Θεωρείται ένας από τους αυστηρότερους νόμους για την προστασία της ιδιωτικής ζωής και την ασφάλεια στον κόσμο, παρόλο που εκπονήθηκε και ψηφίστηκε από την Ευρωπαϊκή Ένωση, επιβάλλει υποχρεώσεις σε οργανισμούς οπουδήποτε, εφόσον στοχεύουν ή συλλέγουν δεδομένα που σχετίζονται με άτομα στην ΕΕ.

Ο κανονισμός βασίζεται σε διάφορες αρχές σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Αυτές περιλαμβάνουν τη νομιμότητα, τη δικαιοσύνη και τη διαφάνεια, τον περιορισμό του σκοπού, την ελαχιστοποίηση των δεδομένων, την ακρίβεια, τον περιορισμό της αποθήκευσης, την ακεραιότητα και την εμπιστευτικότητα και τη λογοδοσία.

Σύμφωνα με τον ΓΚΠΔ, τα άτομα έχουν διάφορα δικαιώματα, μεταξύ των οποίων:

1. Το δικαίωμα ενημέρωσης: Τα άτομα έχουν το δικαίωμα να ενημερώνονται για τη συλλογή και τη χρήση των προσωπικών τους δεδομένων.

2. Το δικαίωμα πρόσβασης: Τα άτομα έχουν δικαίωμα πρόσβασης στα προσωπικά τους δεδομένα και στις συμπληρωματικές πληροφορίες.

3. Το δικαίωμα διόρθωσης: Τα άτομα έχουν το δικαίωμα διόρθωσης ανακριβών προσωπικών δεδομένων ή συμπλήρωσης αν αυτά είναι ελλιπή.

4. Το δικαίωμα διαγραφής (γνωστό και ως "δικαίωμα στη λήθη"): Τα άτομα έχουν το δικαίωμα διαγραφής προσωπικών δεδομένων.

5. Το δικαίωμα περιορισμού της επεξεργασίας: Τα άτομα έχουν το δικαίωμα να ζητήσουν τον περιορισμό ή την εξάλειψη των προσωπικών τους δεδομένων.

6. Το δικαίωμα φορητότητας των δεδομένων: Αυτό επιτρέπει στα άτομα να λαμβάνουν και να επαναχρησιμοποιούν τα προσωπικά τους δεδομένα για τους δικούς τους σκοπούς σε διάφορες υπηρεσίες.

7. Δικαίωμα ένστασης: Σε ορισμένες περιπτώσεις, τα άτομα έχουν το δικαίωμα να αντιταχθούν στην επεξεργασία των προσωπικών τους δεδομένων.

8. Δικαιώματα σε σχέση με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ: Τα άτομα έχουν το δικαίωμα να μην υπόκεινται σε απόφαση που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που τα αφορούν ή τα επηρεάζει με παρόμοιο τρόπο σημαντικά.

Επιπλέον, το πρόγραμμα εστιάζει επίσης στον αντίκτυπο αυτών των κανονισμών στην καθημερινή χρήση του διαδικτύου, διερευνώντας πώς οι νόμοι αυτοί επηρεάζουν τον τρόπο συλλογής, αποθήκευσης και επεξεργασίας των προσωπικών δεδομένων. Αυτή η κατανόηση είναι υψίστης σημασίας όχι μόνο για τη διασφάλιση των δικών μας ψηφιακών πληροφοριών, αλλά συμβάλλει επίσης στη διατήρηση υψηλών προτύπων προστασίας της ιδιωτικής ζωής σε επαγγελματικά και προσωπικά διαδικτυακά περιβάλλοντα.

Ένας άλλος σημαντικός τομέας εστίασης είναι η ασφάλεια των παιδιών στο διαδίκτυο. Με έναν ολοένα αυξανόμενο αριθμό παιδιών που έχουν πρόσβαση στο διαδίκτυο, η ανάγκη για ψηφιακά εργαλεία φιλικά προς τα παιδιά δεν ήταν ποτέ πιο κρίσιμη. Οι φιλικοί προς τα παιδιά φυλλομετρητές παρέχουν ένα ασφαλέστερο, πιο ελεγχόμενο περιβάλλον για την εξερεύνηση του διαδικτύου από τα παιδιά, περιορίζοντας την πρόσβαση σε δυνητικά επιβλαβές περιεχόμενο και διασφαλίζοντας την ιδιωτικότητα του νεαρού χρήστη.

Το πρόγραμμα Micro Credential δίνει μεγάλη έμφαση στην κατανόηση αυτών των εργαλείων, αναλύοντας λεπτομερώς τον τρόπο λειτουργίας τους, τα βασικά χαρακτηριστικά τους και τα οφέλη που προσφέρουν στην εξασφάλιση μιας ασφαλέστερης εμπειρίας στο διαδίκτυο για τα παιδιά. Οι γνώσεις αυτές αποδεικνύονται καθοριστικές για τα άτομα που εμπλέκονται στις διαδικτυακές δραστηριότητες των παιδιών, όπως οι γονείς, οι εκπαιδευτικοί και οι κηδεμόνες. Τους δίνει τη δυνατότητα να προτείνουν ή να χρησιμοποιούν αυτά τα προγράμματα περιήγησης, προωθώντας και επιτρέποντας έτσι ενεργά την ασφαλέστερη χρήση του διαδικτύου από τους νεαρούς ψηφιακούς ιθαγενείς.

Τα προγράμματα περιήγησης που είναι φιλικά προς τα παιδιά, γνωστά και ως προγράμματα περιήγησης για παιδιά, είναι προγράμματα περιήγησης που έχουν σχεδιαστεί ειδικά για χρήση από παιδιά. Αυτά τα προγράμματα περιήγησης δίνουν προτεραιότητα στην ασφάλεια στο διαδίκτυο, παρέχοντας ένα περιβάλλον όπου τα παιδιά μπορούν να εξερευνούν το διαδίκτυο με ασφάλεια, χωρίς τον κίνδυνο να πέσουν πάνω σε ακατάλληλο περιεχόμενο ή να πέσουν θύματα διαδικτυακών απειλών. Η χρήση αυτών των προγραμμάτων περιήγησης αποδεικνύει τη δέσμευση για την ασφάλεια των παιδιών στο διαδίκτυο και μπορεί να προταθεί σε γονείς, εκπαιδευτικούς ή φροντιστές ως εργαλείο για την προώθηση της ασφαλούς και θετικής χρήσης του διαδικτύου.

Ένα από τα κύρια χαρακτηριστικά των φιλικών προς τα παιδιά προγραμμάτων περιήγησης είναι το φιλτράρισμα περιεχομένου. Αυτό το χαρακτηριστικό αποτρέπει την πρόσβαση σε ιστότοπους που περιέχουν ρητό, βίαιο ή ακατάλληλο υλικό, μπλοκάροντάς τους αυτόματα. Ορισμένα φιλικά προς τα παιδιά προγράμματα περιήγησης χρησιμοποιούν μια προσέγγιση λευκής λίστας, όπου είναι δυνατή η πρόσβαση μόνο σε προεγκεκριμένους ιστότοπους. Άλλοι χρησιμοποιούν ένα σύστημα μαύρης λίστας, όπου αποκλείονται συγκεκριμένοι επιβλαβείς ή ακατάλληλοι ιστότοποι. Πολλοί χρησιμοποιούν συνδυασμό και των δύο.

Ορισμένα προγράμματα περιήγησης που είναι φιλικά προς τα παιδιά περιλαμβάνουν επίσης λειτουργίες διαχείρισης χρόνου, επιτρέποντας στους ενήλικες να θέτουν όρια στον χρόνο που τα παιδιά μπορούν να περνούν στο διαδίκτυο. Αυτό προάγει τον ισορροπημένο χρόνο χρήσης της οθόνης και συμβάλλει στην πρόληψη του εθισμού στο διαδίκτυο.

Ένα άλλο κοινό χαρακτηριστικό αυτών των φυλλομετρητών είναι οι απλοποιημένες διεπαφές χρήστη με μεγαλύτερα κουμπιά και απλοποιημένα μενού, στα οποία είναι ευκολότερο να περιηγηθούν οι νεαροί χρήστες. Ορισμένοι προσφέρουν ακόμη και οπτικές και ακουστικές ενδείξεις για την καθοδήγηση της περιήγησης των παιδιών.

Το απόρρητο είναι μια άλλη κρίσιμη πτυχή των φιλικών προς τα παιδιά προγραμμάτων περιήγησης. Δεν συλλέγουν προσωπικά δεδομένα και δεν επιτρέπουν διαφημίσεις τρίτων, κάτι που είναι ζωτικής σημασίας στην εποχή των ανησυχιών για την ψηφιακή ιδιωτικότητα. Επίσης, συχνά ενσωματώνονται με εκπαιδευτικά εργαλεία και πόρους, παρέχοντας ένα παραγωγικό διαδικτυακό περιβάλλον για μάθηση.

Παραδείγματα φυλλομετρητών φιλικών προς τα παιδιά περιλαμβάνουν τα Zoodles, KidzSearch και KIDOZ. Αυτές οι πλατφόρμες παρέχουν ένα ασφαλές και ελεγχόμενο περιβάλλον για να εξερευνούν τα παιδιά τον ιστό, να μαθαίνουν νέα πράγματα και να διασκεδάζουν στο διαδίκτυο.

Η προώθηση της χρήσης προγραμμάτων περιήγησης φιλικών προς τα παιδιά είναι ένα σημαντικό βήμα για τη διασφάλιση της διαδικτυακής ασφάλειας των παιδιών. Αποτελεί μέρος της ψηφιακής ιθαγένειας και της ευαισθητοποίησης, δείχνοντας ενδιαφέρον και υπευθυνότητα για τις διαδικτυακές εμπειρίες των παιδιών.

Χρησιμοποιώντας ή συνιστώντας αυτά τα προγράμματα περιήγησης, μπορεί κανείς να συμβάλει σε ένα ασφαλέστερο διαδικτυακό περιβάλλον για τους πιο ευάλωτους χρήστες του διαδικτύου.

Είναι σημαντικό να σημειωθεί ότι, ενώ οι φιλικοί προς τα παιδιά φυλλομετρητές αποτελούν ένα εξαιρετικό εργαλείο για την ασφάλεια στο διαδίκτυο, θα πρέπει να χρησιμοποιούνται σε συνδυασμό με την ενεργή επίβλεψη και καθοδήγηση ενηλίκων σχετικά με την ασφαλή συμπεριφορά στο διαδίκτυο. Ο συνδυασμός τεχνολογίας και εκπαίδευσης είναι η καλύτερη προσέγγιση για την ασφάλεια των παιδιών στο διαδίκτυο.

Το τελευταίο κρίσιμο μαθησιακό αποτέλεσμα του προγράμματος επικεντρώνεται στη διάκριση μεταξύ ασφαλών και μη ασφαλών ιστότοπων. Με τις πολυάριθμες δυνητικές απειλές για την κυβερνοασφάλεια, είναι ζωτικής σημασίας για τους χρήστες του διαδικτύου να μπορούν να αναγνωρίζουν και να διακρίνουν μεταξύ των ιστότοπων που παρέχουν ασφαλή, κρυπτογραφημένη σύνδεση και εκείνων που δεν παρέχουν.

Αυτό περιλαμβάνει την κατανόηση των αρχών των ασφαλών συνδέσεων, την αναγνώριση των οπτικών ενδείξεων που σχετίζονται με τους ασφαλείς ιστότοπους (όπως τα πρωτόκολλα HTTPS και το σύμβολο του λουκέτου) και την κατανόηση των πιθανών κινδύνων από την πλοήγηση σε μη ασφαλείς ιστότοπους. Το αποτέλεσμα παρέχει τα εργαλεία για την αποφυγή πιθανών απειλών, όπως κακόβουλο λογισμικό, phishing και κλοπή δεδομένων, ενισχύοντας σημαντικά την ασφάλεια του ατόμου και την ασφάλεια των προσωπικών του δεδομένων κατά την περιήγησή του στο διαδίκτυο.

Οι ασφαλείς συνδέσεις αποτελούν θεμελιώδες μέρος της ασφαλούς περιήγησης στο διαδίκτυο, ιδίως όταν αλληλεπιδράτε με ιστότοπους που απαιτούν ευαίσθητες πληροφορίες, όπως οι ιστότοποι ηλεκτρονικών τραπεζικών συναλλαγών ή αγορών. Η κατανόηση των αρχών των ασφαλών συνδέσεων βοηθά τα άτομα να διακρίνουν μεταξύ ασφαλών και μη ασφαλών ιστότοπων, γεγονός που με τη σειρά του συμβάλλει στον περιορισμό του κινδύνου κλοπής δεδομένων ή άλλων κακόβουλων δραστηριοτήτων.

Μια ασφαλής σύνδεση με τον ιστότοπο δημιουργείται με τη χρήση ενός πρωτοκόλλου που είναι γνωστό ως HTTPS (Hypertext Transfer Protocol Secure). Πρόκειται για μια έκδοση του HTTP που λειτουργεί σε συνδυασμό με ένα άλλο πρωτόκολλο, το SSL (Secure Sockets Layer), ή τον διάδοχό του, το TLS (Transport Layer Security), για την ασφαλή μεταφορά δεδομένων.

Όταν ένας χρήστης επισκέπτεται έναν ιστότοπο με σύνδεση HTTPS, το πρόγραμμα περιήγησής του δημιουργεί μια ασφαλή σύνδεση με τον διακομιστή του ιστότοπου. Η σύνδεση αυτή είναι κρυπτογραφημένη, πράγμα που σημαίνει ότι οποιαδήποτε δεδομένα μεταφέρονται μεταξύ της συσκευής του χρήστη και του διακομιστή (όπως κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών ή άλλες προσωπικές πληροφορίες) δεν μπορούν να διαβαστούν ή να αλλοιωθούν εύκολα από τρίτους. Η κρυπτογράφηση πραγματοποιείται με τη χρήση ενός πιστοποιητικού SSL ή TLS, το οποίο παρέχει ο διακομιστής του ιστότοπου.

Για την αναγνώριση μιας ασφαλούς σύνδεσης σε ιστότοπο, υπάρχουν διάφορα οπτικά στοιχεία που πρέπει να αναζητούν οι χρήστες στο πρόγραμμα περιήγησης ιστού:

1. Η διεύθυνση URL της ιστοσελίδας: https:// στην αρχή της διεύθυνσης URL. Το "s" σημαίνει "secure" (ασφαλής) και είναι ο βασικός δείκτης ασφαλούς σύνδεσης.

2. Εικονίδιο λουκέτου: Οι περισσότεροι σύγχρονοι φυλλομετρητές ιστού εμφανίζουν ένα εικονίδιο λουκέτου στη γραμμή διευθύνσεων όταν ο χρήστης επισκέπτεται έναν ασφαλή ιστότοπο. Κάνοντας κλικ στο λουκέτο συχνά παρέχονται πρόσθετες πληροφορίες σχετικά με την ασφάλεια του ιστότοπου.

3. Πληροφορίες πιστοποιητικού: Οι χρήστες μπορούν να έχουν πρόσβαση σε πληροφορίες σχετικά με το πιστοποιητικό SSL ή TLS του ιστότοπου, συμπεριλαμβανομένου του ποιος το εξέδωσε και μέχρι πότε είναι έγκυρο.

4. Σφραγίδα ιστοσελίδας: Ορισμένοι ασφαλείς ιστότοποι εμφανίζουν μια σφραγίδα ασφαλείας, η οποία είναι μια οπτική ένδειξη που παρέχεται από την οντότητα που εξέδωσε το πιστοποιητικό SSL ή TLS.

5. Πράσινη γραμμή διευθύνσεων: Σε ορισμένα προγράμματα περιήγησης, η γραμμή διεύθυνσης ή το όνομα του ιδιοκτήτη του ιστότοπου θα γίνει πράσινη για ιδιαίτερα ασφαλείς ιστότοπους που διαθέτουν πιστοποιητικό SSL Extended Validation (EV).

Είναι σημαντικό να σημειωθεί ότι ενώ αυτές οι οπτικές ενδείξεις υποδεικνύουν ότι έχει δημιουργηθεί ασφαλής σύνδεση, δεν εγγυώνται ότι ο ίδιος ο ιστότοπος είναι ασφαλής ή απαλλαγμένος από κακόβουλο περιεχόμενο. Οι χρήστες θα πρέπει να εξακολουθούν να επιδεικνύουν προσοχή και καλή κρίση όταν εισάγουν προσωπικές πληροφορίες στο διαδίκτυο.

Ουσιαστικά, το ολοκληρωμένο πιστοποιητικό πιστοποίησης ψηφιακού απορρήτου, ασφάλειας των παιδιών και επάρκειας ασφαλούς περιήγησης είναι ένα ολοκληρωμένο πρόγραμμα που στοχεύει στην πλήρη προετοιμασία των εκπαιδευομένων για ασφαλή πλοήγηση στον ψηφιακό κόσμο. Τελειοποιώντας τις γνώσεις και τις δεξιότητές τους στους κρίσιμους τομείς των κανονισμών προσωπικών δεδομένων, της ασφάλειας των παιδιών στο διαδίκτυο και του εντοπισμού ασφαλών ιστότοπων, οι εκπαιδευόμενοι μπορούν να προστατεύουν καλύτερα τον εαυτό τους και τους άλλους, προωθώντας ένα ασφαλέστερο ψηφιακό τοπίο για όλους. Η ολοκλήρωση αυτού του προγράμματος σηματοδοτεί όχι μόνο προσωπική επάρκεια αλλά και την ικανότητα να συμβάλλουν ουσιαστικά σε μια πιο ασφαλή ψηφιακή κοινωνία.

Ερωτήσεις

1. Ποιος είναι ο σκοπός των νόμων για την προστασία των προσωπικών δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ);
2. Πώς εφαρμόζεται ο ΓΚΠΔ σε οργανισμούς εκτός της Ευρωπαϊκής Ένωσης;
3. Ποιες είναι ορισμένες από τις βασικές αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τον ΓΚΠΔ;
4. Μπορείτε να απαριθμήσετε και να εξηγήσετε εν συντομία τα δικαιώματα που έχουν τα άτομα βάσει του ΓΚΠΔ;
5. Πώς επηρεάζουν οι νόμοι για την προστασία της ιδιωτικής ζωής, όπως ο ΓΚΠΔ, τον τρόπο με τον οποίο συλλέγονται, αποθηκεύονται και υποβάλλονται σε επεξεργασία τα προσωπικά δεδομένα σε καθημερινή βάση;
6. Ποιος είναι ο ρόλος και η σημασία των φιλικών προς τα παιδιά φυλλομετρητών στη διασφάλιση της διαδικτυακής ασφάλειας των παιδιών;
7. Ποια είναι μερικά από τα βασικά χαρακτηριστικά των φιλικών προς τα παιδιά προγραμμάτων περιήγησης που τα καθιστούν κατάλληλα για παιδιά;
8. Αναφέρετε μερικά προγράμματα περιήγησης φιλικά προς τα παιδιά και συζητήστε πώς συμβάλλουν στη δημιουργία ενός ασφαλέστερου διαδικτυακού περιβάλλοντος για τα παιδιά.
9. Πώς αντιμετωπίζουν οι φιλικοί προς τα παιδιά φυλλομετρητές τις ανησυχίες για το απόρρητο;
10. Πώς δημιουργείται μια ασφαλής σύνδεση σε ιστότοπο και γιατί είναι σημαντική;
11. Τι σημαίνει HTTPS και τι σημαίνει στη διεύθυνση URL ενός ιστότοπου;
12. Πώς σχετίζεται το εικονίδιο του λουκέτου στη γραμμή διευθύνσεων ενός προγράμματος περιήγησης

με την ασφάλεια του ιστότοπου;
13. Τι είναι η σφραγίδα ασφαλείας σε έναν ιστότοπο και τι αντιπροσωπεύει;
14. Πώς το χρώμα της γραμμής διευθύνσεων ή το όνομα του ιδιοκτήτη του ιστότοπου υποδεικνύουν το επίπεδο ασφάλειας ενός ιστότοπου;
15. Γιατί εξακολουθεί να είναι σημαντικό να είστε προσεκτικοί όταν εισάγετε προσωπικές πληροφορίες στο διαδίκτυο, ακόμη και αν υπάρχουν οπτικές ενδείξεις ασφαλούς σύνδεσης;

Εξειδικευμένη ψηφιακή ασφάλεια και κρυπτογράφηση (MC 4.2.B.5)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Προχωρημένη ψηφιακή ασφάλεια και κρυπτογράφηση **Κωδ: B.5**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.31, 4.2.32 και 4.2.33):

- Εντοπίστε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου που μπορεί να περιέχουν απόπειρες ηλεκτρονικού "ψαρέματος" ή κακόβουλο λογισμικό.
- Καθορισμός προηγμένων μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων στους λογαριασμούς κοινωνικών μέσων.
- Εξηγήστε την έννοια της κρυπτογράφησης και τον ρόλο της στην προστασία των προσωπικών πληροφοριών.

Περιγραφή

Το πρόγραμμα Advanced Digital Security and Encryption Proficiency Micro Credential είναι μια ολοκληρωμένη μαθησιακή πορεία που δίνει έμφαση στη σημασία των προληπτικών πρακτικών κυβερνοασφάλειας σε μια άκρως ψηφιακή εποχή. Επικεντρώνεται σε τρεις κρίσιμους τομείς διαδικτυακής ασφάλειας και ασφάλειας δεδομένων: εντοπισμός ύποπτων δραστηριοτήτων ηλεκτρονικού ταχυδρομείου, διασφάλιση προσωπικών δεδομένων σε πλατφόρμες μέσων κοινωνικής δικτύωσης και κατανόηση της έννοιας της κρυπτογράφησης.

Το πρώτο μαθησιακό αποτέλεσμα επικεντρώνεται στον εντοπισμό ύποπτων δραστηριοτήτων ηλεκτρονικού ταχυδρομείου που μπορεί να υποδηλώνουν απόπειρες phishing ή διάδοση κακόβουλου λογισμικού. Η επικράτηση του ηλεκτρονικού ταχυδρομείου ως εργαλείου επικοινωνίας το έχει καταστήσει συχνό στόχο για τους εγκληματίες του κυβερνοχώρου και, ως εκ τούτου, η κατανόηση του τρόπου εντοπισμού και διαχείρισης αυτών των πιθανών απειλών είναι ζωτικής σημασίας. Το πρόγραμμα εξοπλίζει τους εκπαιδευόμενους με τις απαραίτητες δεξιότητες για να διακρίνουν τα νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου από τα κακόβουλα, επισημαίνοντας τις συνήθεις ενδείξεις των μηνυμάτων ηλεκτρονικού ταχυδρομείου phishing ή εκείνων που μεταφέρουν κακόβουλο λογισμικό. Αυτοί μπορεί να περιλαμβάνουν μη ζητηθέντα συνημμένα αρχεία, επείγοντα στον τόνο του μηνύματος, ορθογραφικά ή γραμματικά λάθη και αναντιστοιχίες στις πληροφορίες του αποστολέα του ηλεκτρονικού ταχυδρομείου.

Το ηλεκτρονικό ταχυδρομείο έχει γίνει μια πανταχού παρούσα μορφή επικοινωνίας τόσο σε προσωπικό όσο και σε επαγγελματικό επίπεδο. Ωστόσο, η ευρεία χρήση του το έχει καταστήσει επίσης συχνό στόχο για εγκληματίες του κυβερνοχώρου που χρησιμοποιούν παραπλανητικές τεχνικές όπως το phishing ή η διανομή κακόβουλου λογισμικού για να εξαπατήσουν τους παραλήπτες, συχνά με στόχο την κλοπή ευαίσθητων πληροφοριών ή την παραβίαση συστημάτων ασφαλείας.

Το "ψάρεμα" είναι ένας τύπος κυβερνοεπίθεσης όπου ο επιτιθέμενος μεταμφιέζεται ως μια αξιόπιστη οντότητα ή πρόσωπο σε ένα ηλεκτρονικό ταχυδρομείο ή άλλη επικοινωνία για να διανείμει κακόβουλους συνδέσμους ή συνημμένα αρχεία που μπορούν να εκτελέσουν μια ποικιλία λειτουργιών,

συμπεριλαμβανομένης της κλοπής διαπιστευτηρίων σύνδεσης ή τραπεζικών πληροφοριών, της εγκατάστασης κακόβουλου λογισμικού ή του αποκλεισμού του χρήστη από τα δεδομένα του μέχρι να πληρώσει λύτρα.

Στο παρόν πρόγραμμα Micro Credential, οι εκπαιδευόμενοι διδάσκονται πώς να αναγνωρίζουν τα σημάδια του phishing και άλλων κακόβουλων δραστηριοτήτων ηλεκτρονικού ταχυδρομείου. Για παράδειγμα, τα ηλεκτρονικά μηνύματα phishing

συχνά προσπαθούν να δημιουργήσουν μια αίσθηση επείγοντος ή φόβου, ενθαρρύνοντας τον παραλήπτη να κάνει κλικ σε έναν σύνδεσμο ή να ανοίξει ένα συνημμένο αρχείο χωρίς να το σκεφτεί. Μπορεί να περιέχουν γενικούς χαιρετισμούς, ορθογραφικά και γραμματικά λάθη, ενώ συχνά η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα δεν ταιριάζει απόλυτα με τον οργανισμό που υποτίθεται ότι εκπροσωπεί.

Το κακόβουλο λογισμικό, ή κακόβουλο λογισμικό, αναφέρεται σε οποιοδήποτε πρόγραμμα ή αρχείο που είναι επιβλαβές για έναν χρήστη υπολογιστή. Το κακόβουλο λογισμικό περιλαμβάνει ιούς υπολογιστών, σκουλήκια, δούρειους ίππους και λογισμικό κατασκοπείας. Αυτά τα κακόβουλα προγράμματα μπορούν να επιτελέσουν μια ποικιλία λειτουργιών, συμπεριλαμβανομένης της κλοπής, της κρυπτογράφησης ή της διαγραφής ευαίσθητων δεδομένων, της τροποποίησης ή της κατάληψης βασικών υπολογιστικών λειτουργιών και της παρακολούθησης της δραστηριότητας των χρηστών στον υπολογιστή χωρίς την άδειά τους.

Τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να χρησιμοποιηθούν για τη διανομή κακόβουλου λογισμικού με διάφορους τρόπους, μεταξύ άλλων μέσω συνημμένων ή ενσωματωμένων συνδέσμων. Το μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να φαίνεται ότι προέρχεται από μια αξιόπιστη πηγή, όπως ένας φίλος ή μια γνωστή εταιρεία, και να παροτρύνει τον παραλήπτη να ανοίξει ένα συνημμένο ή να κάνει κλικ σε έναν σύνδεσμο. Μόλις ο χρήστης προβεί σε αυτή την ενέργεια, το κακόβουλο λογισμικό μπορεί να εγκατασταθεί στο σύστημά του.

Στο πρόγραμμα Micro Credential, οι εκπαιδευόμενοι διδάσκονται πώς να εντοπίζουν πιθανές απειλές κακόβουλου λογισμικού σε μηνύματα ηλεκτρονικού ταχυδρομείου. Αυτό περιλαμβάνει την κατανόηση των τύπων αρχείων που χρησιμοποιούνται συχνά για τη μετάδοση κακόβουλου λογισμικού (όπως τα αρχεία .exe ή .zip), τους κινδύνους από το κλικ σε άγνωστους συνδέσμους και τη σημασία της διατήρησης ενημερωμένου λογισμικού προστασίας από ιούς.

Το πρόγραμμα υπογραμμίζει τη σημασία του να αντιμετωπίζετε πάντα με προσοχή τα μη ζητηθέντα μηνύματα ηλεκτρονικού ταχυδρομείου, ιδίως εκείνα που ζητούν ευαίσθητες πληροφορίες, προτρέπουν σε γρήγορη δράση, έχουν αντιεπαγγελματικό σχεδιασμό ή κακή γραμματική ή περιέχουν μη ζητηθέντα συνημμένα αρχεία. Αναγνωρίζοντας αυτές τις κόκκινες σημαίες, οι χρήστες μπορούν να μειώσουν σημαντικά τον κίνδυνο να πέσουν θύματα επιθέσεων phishing ή κακόβουλου λογισμικού.

Συνολικά, η ικανότητα εντοπισμού ύποπτων δραστηριοτήτων ηλεκτρονικού ταχυδρομείου είναι μια κρίσιμη δεξιότητα στη σύγχρονη ψηφιακή εποχή. Μπορεί να προστατεύσει τα άτομα και τους οργανισμούς από παραβιάσεις δεδομένων, οικονομικές απώλειες και άλλες σοβαρές συνέπειες που σχετίζονται με επιθέσεις στον κυβερνοχώρο. Το πρόγραμμα Micro Credential παρέχει τις απαραίτητες γνώσεις και δεξιότητες για την ασφαλή και αποτελεσματική πλοήγηση στον ψηφιακό κόσμο, προωθώντας μια πιο ασφαλή και συνειδητοποιημένη ως προς την προστασία της ιδιωτικής ζωής ψηφιακή κοινωνία.

Η γνώση αυτή μπορεί να μειώσει σημαντικά τον κίνδυνο παραβίασης δεδομένων και άλλων απειλών στον κυβερνοχώρο που ενδέχεται να θέσουν σε κίνδυνο την ψηφιακή ασφάλεια του χρήστη.

Στην εποχή των μέσων κοινωνικής δικτύωσης, το πρόγραμμα ασχολείται επίσης με την προστασία των προσωπικών δεδομένων σε αυτές τις πλατφόρμες ως δεύτερο μαθησιακό αποτέλεσμα. Ακόμα και αν αυτές οι πλατφόρμες προσφέρουν πολυάριθμα οφέλη, δημιουργούν επίσης σημαντικές ανησυχίες για την προστασία της ιδιωτικής ζωής. Το πρόγραμμα παρέχει μια εμπεριστατωμένη κατανόηση των προηγμένων μέτρων ασφαλείας που μπορούν να ληφθούν για την προστασία των προσωπικών δεδομένων στις πλατφόρμες των μέσων κοινωνικής δικτύωσης. Αυτό περιλαμβάνει οδηγίες σχετικά με τις βέλτιστες πρακτικές, όπως ο καθορισμός ισχυρών, μοναδικών κωδικών πρόσβασης, η ενεργοποίηση του ελέγχου ταυτότητας πολλαπλών παραγόντων, ο περιορισμός της κοινής χρήσης ευαίσθητων πληροφοριών, η κατανόηση και η αποτελεσματική διαχείριση των ρυθμίσεων απορρήτου και η αναγνώριση και αποφυγή πιθανών απάτης ή δόλιων δραστηριοτήτων.

Τα μέσα κοινωνικής δικτύωσης έχουν αλλάξει ριζικά τον τρόπο με τον οποίο οι άνθρωποι επικοινωνούν, μοιράζονται πληροφορίες και αλληλεπιδρούν. Ωστόσο, η διείσδυσή τους στην καθημερινή ζωή έχει δημιουργήσει σημαντικές ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων. Δεδομένου του τεράστιου όγκου προσωπικών δεδομένων που μοιράζονται σε αυτές τις πλατφόρμες, οι χρήστες συχνά γίνονται στόχοι για εγκληματίες του κυβερνοχώρου, με αποτέλεσμα πιθανές παραβιάσεις δεδομένων, κλοπή ταυτότητας και άλλες μορφές εγκλήματος στον κυβερνοχώρο.

Σε αυτό το πρόγραμμα Micro Credential, το δεύτερο μαθησιακό αποτέλεσμα περιστρέφεται γύρω από την κατανόηση και την εφαρμογή προηγμένων μέτρων ασφαλείας για την προστασία των προσωπικών πληροφοριών στις πλατφόρμες κοινωνικής δικτύωσης. Οι πλατφόρμες αυτές περιλαμβάνουν μεταξύ άλλων το Facebook, το Instagram, το Twitter, το LinkedIn και το Snapchat.

Μία από τις κύριες πτυχές που καλύπτονται από αυτό το μαθησιακό αποτέλεσμα είναι η δημιουργία και η διαχείριση ισχυρών, μοναδικών κωδικών πρόσβασης. Ένας ισχυρός κωδικός πρόσβασης είναι η πρώτη γραμμή άμυνας ενός χρήστη έναντι μη εξουσιοδοτημένης πρόσβασης. Το πρόγραμμα περιγράφει λεπτομερώς τα στοιχεία των ισχυρών κωδικών πρόσβασης, οι οποίοι συνήθως περιλαμβάνουν έναν συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών και συμβόλων και δεν είναι εύκολα μαντεύσιμοι (όπως το "password123" ή το "qwerty"). Επιπλέον, το πρόγραμμα ενθαρρύνει τη χρήση διαφορετικών κωδικών πρόσβασης για διαφορετικές πλατφόρμες, ώστε να αποφευχθεί η παραβίαση της ασφάλειας σε μια πλατφόρμα να επηρεάσει άλλους λογαριασμούς.

Εκτός από τις αξιόπιστες πρακτικές χρήσης κωδικών πρόσβασης, το πρόγραμμα καλύπτει τη σημασία της ενεργοποίησης του ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) στους λογαριασμούς των μέσων κοινωνικής δικτύωσης. Ο MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας από τους χρήστες να παρέχουν τουλάχιστον δύο ή περισσότερους παράγοντες επαλήθευσης για να αποκτήσουν πρόσβαση σε έναν λογαριασμό, καθιστώντας δυσκολότερη την πρόσβαση σε πιθανούς εισβολείς.

Το πρόγραμμα τονίζει επίσης τη σημασία της κατανόησης και της αποτελεσματικής διαχείρισης των ρυθμίσεων απορρήτου στις πλατφόρμες κοινωνικής δικτύωσης. Οι χρήστες συχνά μοιράζονται ευαίσθητες πληροφορίες σε αυτές τις πλατφόρμες χωρίς να συνειδητοποιούν ότι οι αναρτήσεις, τα σχόλια, οι συμπάθειες, οι κοινοποιήσεις, ακόμη και τα προσωπικά τους στοιχεία μπορεί να είναι ορατά σε ένα ευρύτερο κοινό από ό,τι σκόπευαν. Το πρόγραμμα παρέχει μια εμπεριστατωμένη κατανόηση των ρυθμίσεων απορρήτου, καθοδηγώντας τους εκπαιδευόμενους σχετικά με το πώς να ελέγχουν ποιος μπορεί να δει τις πληροφορίες τους και πώς μπορούν να κοινοποιηθούν.

Επιπλέον, το πρόγραμμα καλύπτει τον εντοπισμό και την αποφυγή απάτης και δόλιων δραστηριοτήτων που συναντώνται συνήθως στα μέσα κοινωνικής δικτύωσης. Αυτές θα μπορούσαν να περιλαμβάνουν απόπειρες phishing, μηνύματα απάτης, απατηλά αιτήματα φιλίας ή διαφημίσεις απάτης.

Στο τέλος αυτής της ενότητας, οι εκπαιδευόμενοι θα έχουν κατανοήσει πλήρως πώς να προστατεύουν τα προσωπικά τους δεδομένα στις πλατφόρμες κοινωνικής δικτύωσης. Αυτές οι γνώσεις και το σύνολο των δεξιοτήτων δεν συμβάλλουν μόνο στην προσωπική ψηφιακή ασφάλεια, αλλά επηρεάζουν επίσης μια ευρύτερη κουλτούρα διαδικτυακής ασφάλειας και προστασίας των δεδομένων. Αυτό το μαθησιακό αποτέλεσμα αποτελεί ουσιαστική πτυχή της διασφάλισης της ψηφιακής ευημερίας των ατόμων και των κοινοτήτων, προωθώντας ένα ασφαλέστερο και πιο ευαισθητοποιημένο στην προστασία της ιδιωτικής ζωής τοπίο στα μέσα κοινωνικής δικτύωσης.

Η γνώση αυτή συμβάλλει στην ασφαλή χρήση των πλατφορμών κοινωνικής δικτύωσης, προστατεύοντας τους χρήστες από παραβιάσεις δεδομένων και πιθανή κλοπή ταυτότητας.

Τέλος, το πρόγραμμα εξετάζει την έννοια της κρυπτογράφησης και τον πρωταρχικό της ρόλο στην προστασία των προσωπικών πληροφοριών. Προσφέρει μια σε βάθος διερεύνηση του τρόπου με τον οποίο η κρυπτογράφηση λειτουργεί ως μέτρο ασφαλείας, κωδικοποιώντας τα δεδομένα σε μη αναγνώσιμη μορφή που μπορεί να αποκρυπτογραφηθεί μόνο με το σωστό κλειδί αποκρυπτογράφησης. Διερευνά περαιτέρω τις διάφορες μορφές κρυπτογράφησης, όπως η συμμετρική και η ασύμμετρη κρυπτογράφηση, και τα πλαίσια στα οποία εφαρμόζονται. Η κατανόηση αυτή επιτρέπει στα άτομα να εκτιμήσουν το ρόλο της κρυπτογράφησης στη διατήρηση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων, είτε πρόκειται για προσωπικές επικοινωνίες, είτε για επιχειρηματικές συναλλαγές, είτε για το ευρύτερο ψηφιακό τοπίο. Η κρυπτογράφηση αποτελεί κρίσιμη πτυχή της ασφάλειας στον κυβερνοχώρο και της ιδιωτικότητας των δεδομένων. Πρόκειται για μια διαδικασία που μετατρέπει αναγνώσιμο κείμενο ή δεδομένα, γνωστό ως απλό κείμενο, σε μια κωδικοποιημένη έκδοση που ονομάζεται κρυπτογράφημα, το οποίο μπορεί να αποκωδικοποιηθεί ή να αποκρυπτογραφηθεί μόνο από εκείνους που διαθέτουν το κατάλληλο κλειδί αποκρυπτογράφησης. Ο πρωταρχικός σκοπός της κρυπτογράφησης είναι η προστασία της εμπιστευτικότητας των ψηφιακών δεδομένων που αποθηκεύονται σε συστήματα υπολογιστών ή μεταδίδονται μέσω του διαδικτύου ή άλλων δικτύων υπολογιστών.

Η κρυπτογράφηση λειτουργεί με τη χρήση πολύπλοκων αλγορίθμων για την κρυπτογράφηση των δεδομένων. Υπάρχουν δύο κύριοι τύποι κρυπτογράφησης: συμμετρική και ασύμμετρη.

1. Συμμετρική κρυπτογράφηση: Στην συμμετρική κρυπτογράφηση, το ίδιο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Αυτό σημαίνει ότι ο αποστολέας και ο παραλήπτης πρέπει να έχουν και οι δύο το ίδιο κλειδί. Ο πιο συνηθισμένος τύπος συμμετρικής κρυπτογράφησης είναι το Advanced Encryption Standard (AES), το οποίο έχει εγκριθεί από την κυβέρνηση των ΗΠΑ και από τους ευρωπαϊκούς κανονισμούς για την κρυπτογράφηση διαβαθμισμένων πληροφοριών, τόσο σε πολιτικά όσο και σε στρατιωτικά πρότυπα κρυπτογράφησης. Τα τρέχοντα πρότυπα προβλέπουν τουλάχιστον AES 256 (μήκος κλειδιού σε bit) για να χαρακτηριστεί ως "ασφαλές".

2. Ασύμμετρη κρυπτογράφηση: Η ασύμμετρη κρυπτογράφηση, γνωστή και ως κρυπτογράφηση δημόσιου κλειδιού, χρησιμοποιεί δύο κλειδιά αντί για ένα. Το δημόσιο κλειδί, το οποίο είναι γνωστό σε όλους, χρησιμοποιείται για την κρυπτογράφηση, ενώ το ιδιωτικό κλειδί, το οποίο παραμένει μυστικό από τον παραλήπτη, χρησιμοποιείται για την αποκρυπτογράφηση. Ο πιο συνηθισμένος τύπος ασύμμετρης κρυπτογράφησης είναι ο αλγόριθμος RSA. Η ασύμμετρη κρυπτογράφηση χρησιμοποιείται συχνά σε ασφαλείς

επικοινωνίες, όπως τα πρωτόκολλα SSL και TLS (https://), τα οποία εξασφαλίζουν τη μετάδοση δεδομένων στο διαδίκτυο. Τα διεθνή πρότυπα υποδεικνύουν ένα ελάχιστο μήκος κλειδιού 2048 bit για να θεωρηθεί η κρυπτογράφηση "ασφαλής".

Η τεράστια διαφορά στο μήκος του κλειδιού (256 V/s 2024 bits) μεταξύ συμμετρικών και ασύμμετρων κλειδιών, βασίζεται στον εγγενή σχεδιασμό του ασύμμετρου αλγορίθμου RSA, ο οποίος χρειάζεται το γινόμενο δύο πρώτων αριθμών (σημειώνεται ως d "p" και "q") για τη δημιουργία του πυρήνα των ασύμμετρων κλειδιών (σημειώνεται ως "n"). Καθώς οι πρώτοι αριθμοί μπορούν εύκολα να διευθυνσιοδοτηθούν με αριθμούς 5, 6 ή περισσότερων ψηφίων, το στατιστικό σύμπαν θα είναι εξαιρετικά μεγαλύτερο από τους φυσικούς αριθμούς.

Μία από τις κύριες χρήσεις της κρυπτογράφησης είναι η προστασία της ακεραιότητας των δεδομένων κατά τη μετάδοση. Όταν τα δεδομένα κρυπτογραφούνται, καθίστανται μη αναγνώσιμα από οποιονδήποτε χωρίς το κλειδί αποκρυπτογράφησης, διασφαλίζοντας έτσι ότι τα δεδομένα δεν μπορούν να υποκλαπούν και να διαβαστούν κατά τη μετάδοση. Αυτό είναι ιδιαίτερα σημαντικό όταν μεταδίδονται ευαίσθητα δεδομένα, όπως αριθμοί πιστωτικών καρτών ή προσωπικές πληροφορίες, μέσω του διαδικτύου.

Μια άλλη κρίσιμη χρήση της κρυπτογράφησης είναι η προστασία των αποθηκευμένων δεδομένων. Με την κρυπτογράφηση αρχείων ή ολόκληρων συσκευών αποθήκευσης, οι χρήστες μπορούν να διασφαλίσουν ότι ακόμη και αν τα δεδομένα κλαπούν ή αποκτήσουν πρόσβαση χωρίς εξουσιοδότηση, θα παραμείνουν μη αναγνώσιμα και, επομένως, άχρηστα για τον μη εξουσιοδοτημένο.

Η κρυπτογράφηση διαδραματίζει ζωτικό ρόλο σε πολλούς τομείς, όπως η ασφάλεια του διαδικτύου, τα συστήματα επικοινωνίας, οι τραπεζικές και χρηματοοικονομικές υπηρεσίες, η υγειονομική περίθαλψη κ.ά. Αποτελεί θεμελιώδη πυλώνα της ασφαλούς ψηφιακής επικοινωνίας και αποθήκευσης δεδομένων, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση και διατηρώντας την ακεραιότητα και την εμπιστευτικότητα των δεδομένων.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι ενώ η κρυπτογράφηση μπορεί να ενισχύσει σημαντικά την ασφάλεια των δεδομένων, δεν είναι αλάνθαστη και θα πρέπει να χρησιμοποιείται ως μέρος μιας ευρύτερης προσέγγισης για την ασφάλεια στον κυβερνοχώρο που περιλαμβάνει καλές συνήθειες ψηφιακής υγιεινής, χρήση ασφαλών δικτύων και τακτικές ενημερώσεις λογισμικού.

Στην ουσία, το πρόγραμμα Advanced Digital Security and Encryption Proficiency Micro Credential έχει σχεδιαστεί για να ενισχύσει την κατανόηση και τις ικανότητες του εκπαιδευόμενου όσον αφορά κρίσιμες πτυχές της ψηφιακής ασφάλειας και της ασφάλειας δεδομένων. Με την ολοκλήρωση του προγράμματος, το άτομο θα είναι καλά καταρτισμένο στον εντοπισμό και τον μετριασμό πιθανών διαδικτυακών απειλών, στην προστασία των προσωπικών του δεδομένων σε περιβάλλοντα μέσων κοινωνικής δικτύωσης και στην κατανόηση του ζωτικού ρόλου της κρυπτογράφησης στην εξασφάλιση ψηφιακών πληροφοριών. Αυτή η επάρκεια δεν είναι μόνο προσωπικά επωφελής, αλλά μπορεί επίσης να συμβάλει σημαντικά σε μια ασφαλέστερη, ασφαλέστερη ψηφιακή κοινωνία.

Ερωτήσεις

1. Ποιες είναι μερικές κοινές ενδείξεις ενός ηλεκτρονικού μηνύματος ηλεκτρονικού "ψαρέματος";
2. Μπορείτε να εξηγήσετε τον όρο "κακόβουλο λογισμικό" και να απαριθμήσετε ορισμένα από τα είδη του;
3. Πώς μπορείτε να εντοπίσετε μια πιθανή απειλή κακόβουλου λογισμικού σε ένα email;

4. Ποια είναι η σημασία της προσεκτικής αντιμετώπισης των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου;
5. Ποια είναι τα στοιχεία ενός ισχυρού, μοναδικού κωδικού πρόσβασης;
6. Μπορείτε να εξηγήσετε την έννοια του ελέγχου ταυτότητας πολλαπλών παραγόντων και τη σημασία του στις πλατφόρμες κοινωνικής δικτύωσης;
7. Πώς μπορεί να γίνει αποτελεσματική διαχείριση των ρυθμίσεων απορρήτου στις πλατφόρμες κοινωνικής δικτύωσης;
8. Τι είδους απάτες ή δόλιες δραστηριότητες συναντώνται συνήθως στα μέσα κοινωνικής δικτύωσης;
9. Γιατί η κρυπτογράφηση είναι σημαντική για την προστασία των προσωπικών πληροφοριών;
10. Μπορείτε να εξηγήσετε τη διαφορά μεταξύ συμμετρικής και ασύμμετρης κρυπτογράφησης;
11. Ποιος είναι ο ρόλος της κρυπτογράφησης στη μετάδοση δεδομένων;
12. Πώς συμβάλλει η κρυπτογράφηση στην προστασία των αποθηκευμένων δεδομένων;
13. Γιατί η κρυπτογράφηση πρέπει να εξεταστεί ως μέρος μιας ευρύτερης προσέγγισης της ασφάλειας στον κυβερνοχώρο;
14. Ποιος είναι ο ρόλος της κρυπτογράφησης στην ασφάλεια του διαδικτύου και στα συστήματα επικοινωνίας;
15. Πώς η καλή κατανόηση της ασφάλειας των ηλεκτρονικών μηνυμάτων συμβάλλει σε μια ασφαλέστερη, ασφαλέστερη ψηφιακή κοινωνία;
16. Με ποιους τρόπους η αποτελεσματική διαχείριση των κωδικών πρόσβασης στις πλατφόρμες κοινωνικής δικτύωσης ενισχύει την ασφάλεια των προσωπικών δεδομένων;
17. Πώς η κατανόηση της κρυπτογράφησης ενισχύει τις ικανότητές μας όσον αφορά την ψηφιακή ασφάλεια και την προστασία των δεδομένων;
18. Μπορείτε να δώσετε παραδείγματα καταστάσεων στις οποίες η συμμετρική κρυπτογράφηση είναι πιο συμφέρουσα από την ασύμμετρη κρυπτογράφηση και το αντίστροφο;
19. Πώς διαφέρει η διαχείριση των κλειδιών στη συμμετρική και την ασύμμετρη κρυπτογράφηση και ποιες είναι οι συνέπειες αυτών των διαφορών όσον αφορά την ασφάλεια και την ευκολία;
20. Μπορείτε να εξηγήσετε τη λειτουργία του αλγορίθμου Advanced Encryption Standard (AES) που χρησιμοποιείται στη συμμετρική κρυπτογράφηση και του αλγορίθμου RSA που χρησιμοποιείται στην ασύμμετρη κρυπτογράφηση;
21. Πώς επηρεάζουν οι διαφορές στους αλγορίθμους της συμμετρικής (όπως ο AES) και της ασύμμετρης κρυπτογράφησης (όπως ο RSA) την αντίστοιχη ασφάλεια και τις επιδόσεις τους;

Προηγμένη ανάλυση προστασίας προσωπικών δεδομένων και προστασίας της ιδιωτικής ζωής (MC 4.2.B.6)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Προηγμένη προστασία προσωπικών δεδομένων και ανάλυση απορρήτου **Κωδ: B.6**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%

Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.34, 4.2.35):

- Αναγνωρίστε τους πιθανούς κινδύνους από την κοινοποίηση προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης και λάβετε τις απαραίτητες προφυλάξεις.
- Συγκρίνετε τις πολιτικές απορρήτου διαφόρων εφαρμογών ή υπηρεσιών για να προσδιορίσετε τις πρακτικές συλλογής δεδομένων που εφαρμόζουν.

Περιγραφή

Το πρόγραμμα Advanced Personal Data Protection and Privacy Analysis Micro Credential είναι μια εξαντλητική εκπαιδευτική διαδρομή που έχει σχεδιαστεί για να ενισχύσει την κατανόηση της ιδιωτικότητας των δεδομένων, των πρακτικών προσωπικής κυβερνοασφάλειας και των δικαιωμάτων τους ως ψηφιακών πολιτών. Αυτό το πρόγραμμα υπογραμμίζει τη σημασία των προληπτικών και ενημερωμένων πρακτικών μπροστά σε ένα ολοένα και πιο ψηφιακό τοπίο, με έντονη εστίαση στους πιθανούς κινδύνους από την κοινοποίηση προσωπικών δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης, καθώς και την ικανότητα αξιολόγησης και αντιπαραβολής των πρακτικών συλλογής δεδομένων σε διάφορες ψηφιακές εφαρμογές και υπηρεσίες.

Το πρώτο μαθησιακό αποτέλεσμα εμπλέκει τους εκπαιδευόμενους στη διερεύνηση των πιθανών κινδύνων που συνδέονται με την κοινοποίηση προσωπικών δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης. Παρά τα πολυάριθμα πλεονεκτήματα επικοινωνίας και σύνδεσης που παρέχουν οι πλατφόρμες των μέσων κοινωνικής δικτύωσης, παρουσιάζουν επίσης σημαντικές απειλές που σχετίζονται με το απόρρητο και την ασφάλεια των δεδομένων. Η διάχυτη φύση αυτών των πλατφορμών και η συνακόλουθη εκτεταμένη κοινοποίηση προσωπικών πληροφοριών καθιστούν τους χρήστες ευάλωτους σε δραστηριότητες κυβερνοεγκληματιών, οι οποίες μπορούν να οδηγήσουν σε παραβιάσεις δεδομένων, κλοπή ταυτότητας και άλλα εγκλήματα στον κυβερνοχώρο.

Μαθησιακό αποτέλεσμα 1: Αναγνώριση των πιθανών κινδύνων από την κοινοποίηση προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης και λήψη των απαραίτητων προφυλάξεων.

Οι πλατφόρμες κοινωνικής δικτύωσης έχουν γίνει αναπόσπαστο μέρος της καθημερινής ζωής. Ωστόσο, καθώς τα άτομα μοιράζονται σημαντικό αριθμό προσωπικών πληροφοριών σε αυτές τις πλατφόρμες, υπάρχουν σημαντικοί δυνητικοί κίνδυνοι που σχετίζονται με την ιδιωτικότητα και την ασφάλεια των δεδομένων. Το πρόγραμμα παρέχει μια εις βάθος κατανόηση του τρόπου με τον οποίο οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται αυτές τις πλατφόρμες και τους χρήστες τους. Για παράδειγμα, οι κυβερνοεγκληματίες χρησιμοποιούν συχνά τεχνικές ‘’ψαρέματος’’ για να παρασύρουν τους χρήστες να αποκαλύψουν ευαίσθητες

πληροφορίες ή μπορούν να εκμεταλλευτούν τις κακές ρυθμίσεις απορρήτου για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα.

Το πρόγραμμα διευκρινίζει περαιτέρω τις στρατηγικές και τα προληπτικά μέτρα που μπορούν να λάβουν οι χρήστες για να προστατεύσουν τα προσωπικά τους δεδομένα σε αυτές τις πλατφόρμες. Αυτό περιλαμβάνει την εκμάθηση του τρόπου αποτελεσματικής χρήσης των ρυθμίσεων απορρήτου, τον περιορισμό του ποιος μπορεί να δει τις προσωπικές πληροφορίες, την επιφυλακτικότητα σε αιτήματα φιλίας από άγνωστα άτομα και την κατανόηση των συνεπειών των γεωγραφικών ετικετών και των δημόσιων check-ins.

Επιπλέον, το πρόγραμμα καλύπτει τη σημασία της κριτικής αξιολόγησης των εφαρμογών που συνδέονται με πλατφόρμες κοινωνικής δικτύωσης, καθώς αυτές συχνά έχουν πρόσβαση σε προσωπικές πληροφορίες και ενδέχεται να μην τηρούν τα ίδια πρότυπα προστασίας της ιδιωτικής ζωής με την ίδια την πλατφόρμα.

Ως απάντηση σε αυτό, οι εκπαιδευόμενοι καθοδηγούνται μέσω των βέλτιστων πρακτικών για την προστασία των προσωπικών τους πληροφοριών σε αυτές τις πλατφόρμες. Το πρόγραμμα σπουδών περιλαμβάνει συζητήσεις σχετικά με την κατανόηση του τρόπου με τον οποίο τα κοινά δεδομένα μπορούν να χρησιμοποιηθούν ή να χρησιμοποιηθούν καταχρηστικά, τη σημασία της αποτελεσματικής διαχείρισης των ρυθμίσεων απορρήτου για τον περιορισμό του ποιος μπορεί να δει το κοινόχρηστο περιεχόμενό τους, καθώς και την έννοια του ψηφιακού αποτυπώματος και τις μακροχρόνιες επιπτώσεις του. Οι συζητήσεις αυτές αποσκοπούν στο να εμπεδώσουν στους μαθητές την επίγνωση των πιθανών συνεπειών της αδιάκριτης κοινής χρήσης δεδομένων σε τέτοιες πλατφόρμες.

Το δεύτερο μαθησιακό αποτέλεσμα επικεντρώνεται στην ανάπτυξη των ικανοτήτων των εκπαιδευομένων να αξιολογούν κριτικά και να συγκρίνουν τις πολιτικές απορρήτου διαφόρων ψηφιακών εφαρμογών και υπηρεσιών. Με δεδομένο το σημερινό ψηφιακό τοπίο, όπου τα δεδομένα θεωρούνται ένα ιδιαίτερα πολύτιμο αγαθό, ένα ευρύ φάσμα εφαρμογών και υπηρεσιών συγκεντρώνει συχνά σημαντικά δεδομένα χρηστών, συχνά με τη δικαιολογία της βελτίωσης της εμπειρίας των χρηστών. Ωστόσο, οι πρακτικές αυτές εγείρουν αξιοσημείωτες ανησυχίες για την προστασία της ιδιωτικής ζωής.

Μαθησιακό Αποτέλεσμα 2: Σύγκριση των πολιτικών απορρήτου διαφόρων εφαρμογών ή υπηρεσιών για τον προσδιορισμό των πρακτικών συλλογής δεδομένων τους

Αυτό το μαθησιακό αποτέλεσμα επικεντρώνεται στο να εφοδιάσει τους εκπαιδευόμενους με την ικανότητα να αξιολογούν κριτικά και να συγκρίνουν τις πολιτικές απορρήτου και τις πρακτικές συλλογής δεδομένων διαφόρων εφαρμογών και ψηφιακών υπηρεσιών. Με την έλευση της ψηφιακής εποχής, τα δεδομένα έχουν γίνει πολύτιμο περιουσιακό στοιχείο και πολλές εταιρείες χρησιμοποιούν στρατηγικές που βασίζονται στα δεδομένα για να βελτιώσουν την εμπειρία των χρηστών, συχνά εις βάρος της ιδιωτικής ζωής των χρηστών.

Η διδακτέα ύλη περιλαμβάνει την κατανόηση της ορολογίας και των νομικών πλαισίων που χρησιμοποιούνται συχνά στις πολιτικές απορρήτου, την αναγνώριση του τρόπου συλλογής, αποθήκευσης και κοινής χρήσης των δεδομένων και τον προσδιορισμό του ελέγχου που έχουν οι χρήστες επί των δεδομένων τους. Το πρόγραμμα συζητά πρακτικά παραδείγματα πολιτικών απορρήτου, ρίχνοντας φως στις διαφορετικές πολιτικές και στον τρόπο με τον οποίο οι εταιρείες μπορούν να χρησιμοποιούν τα δεδομένα που συλλέγονται.

Το πρόγραμμα καλύπτει επίσης σημαντικούς κανονισμούς προστασίας δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ), παρέχοντας στους εκπαιδευόμενους σαφή κατανόηση των δικαιωμάτων τους όσον αφορά τα προσωπικά τους δεδομένα.

Ως αποτέλεσμα του προγράμματος Advanced Personal Data Protection and Privacy Analysis Micro Credential, οι εκπαιδευόμενοι όχι μόνο θα έχουν κατανοήσει πλήρως τους πιθανούς κινδύνους που σχετίζονται με την ανταλλαγή προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης, αλλά θα έχουν επίσης αναπτύξει τις δεξιότητες που απαιτούνται για την κριτική αξιολόγηση και σύγκριση των πρακτικών συλλογής δεδομένων και των πολιτικών απορρήτου διαφόρων ψηφιακών υπηρεσιών.

Σε αυτό το πλαίσιο, οι εκπαιδευόμενοι διδάσκονται πώς να διακρίνουν τι είδους δεδομένα συλλέγουν αυτές οι υπηρεσίες και εφαρμογές, πώς χρησιμοποιούνται, αποθηκεύονται και ενδεχομένως κοινοποιούνται αυτές οι πληροφορίες και ποιος είναι ο έλεγχος που διατηρούν οι χρήστες επί των προσωπικών τους δεδομένων. Αυτό προϋποθέτει την κατανόηση των συχνά πολύπλοκων και μακροσκελών πολιτικών απορρήτου και των συμφωνιών παροχής υπηρεσιών, τις οποίες πολλοί χρήστες αποδέχονται χωρίς ενδελεχή εξέταση. Η διδασκαλία καλύπτει επίσης κανονιστικά πλαίσια όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ), ο οποίος παρέχει αυστηρά δικαιώματα και προστασία στους καταναλωτές όσον αφορά τα προσωπικά τους δεδομένα.

Με την ολοκλήρωση του προγράμματος Advanced Personal Data Protection and Privacy Analysis Micro Credential, οι εκπαιδευόμενοι θα έχουν κατανοήσει σε βάθος τους πιθανούς κινδύνους και τα απαιτούμενα προληπτικά μέτρα που σχετίζονται με την κοινή χρήση προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης. Θα έχουν επίσης εκπαιδευτεί στην ικανότητά τους να αξιολογούν κριτικά και να συγκρίνουν τις πρακτικές συλλογής δεδομένων και προστασίας της ιδιωτικής ζωής διαφόρων ψηφιακών υπηρεσιών. Αυτές οι ικανότητες επεκτείνονται πέρα από το προσωπικό όφελος, προωθώντας μια πιο ενημερωμένη, υπεύθυνη και συνειδητοποιημένη ψηφιακή κοινωνία με γνώμονα την προστασία της ιδιωτικής ζωής.

Ερωτήσεις

1. Ποιοι είναι ορισμένοι συνήθεις κίνδυνοι που συνδέονται με την κοινοποίηση προσωπικών δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης;
2. Πώς μπορούν οι ρυθμίσεις απορρήτου στις πλατφόρμες κοινωνικής δικτύωσης να βοηθήσουν στην προστασία των προσωπικών δεδομένων;
3. Ποιες προφυλάξεις πρέπει να λαμβάνονται όταν δέχεστε αιτήματα φιλίας ή ακολούθους στα μέσα κοινωνικής δικτύωσης;
4. Ποιες είναι οι πιθανές επιπτώσεις της γεωγραφικής σήμανσης και του δημόσιου ελέγχου στα μέσα κοινωνικής δικτύωσης;
5. Πώς μπορούν εφαρμογές τρίτων που συνδέονται με πλατφόρμες μέσων κοινωνικής δικτύωσης να θέσουν σε κίνδυνο τα προσωπικά δεδομένα;
6. Γιατί είναι σημαντικό να διαβάζετε και να κατανοείτε τις πολιτικές απορρήτου των ψηφιακών υπηρεσιών;
7. Ποιους βασικούς όρους και ποια νομικά πλαίσια πρέπει να γνωρίζει κανείς κατά την αξιολόγηση των πολιτικών απορρήτου;
8. Πώς μπορεί ένας χρήστης να προσδιορίσει τους τύπους δεδομένων που συλλέγονται από μια υπηρεσία, όπως περιγράφονται λεπτομερώς στην πολιτική απορρήτου της;
9. Ποιες πτυχές της αποθήκευσης και της κοινής χρήσης δεδομένων πρέπει να αναζητήσει κανείς σε μια πολιτική απορρήτου;
10. Πώς επηρεάζουν κανονισμοί όπως ο ΓΚΠΔ τα δικαιώματα ενός χρήστη όσον αφορά τα προσωπικά του δεδομένα;
11. Πώς μπορεί η σύγκριση των πολιτικών απορρήτου μεταξύ διαφορετικών υπηρεσιών να βοηθήσει έναν χρήστη να κάνει τεκμηριωμένες επιλογές σχετικά με το ποιες υπηρεσίες θα χρησιμοποιήσει;

Προηγμένη ασφάλεια και προστασία προσωπικών δεδομένων (MC 4.2.B.7)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Προηγμένη ασφάλεια και προστασία προσωπικών δεδομένων **Κωδ: B.7**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%

Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.36, 4.2.37 και 4.2.38):

- Περιγράψτε την έννοια της κρυπτογραφημένης επικοινωνίας και εκτιμήστε το απόρρητό σας επιλέγοντας εφαρμογές επικοινωνίας που παρέχουν κρυπτογράφηση από άκρο σε άκρο.
- Υιοθετήστε τις βέλτιστες πρακτικές για την προστασία των προσωπικών δεδομένων σε διάφορα επιγραμμικά πλαίσια.
- Διερευνήστε τυχόν ανωμαλίες στις συσκευές σας που μπορεί να υποδηλώνουν παραβίαση του απορρήτου.

Περιγραφή

Καθώς ο κόσμος μεταβαίνει ταχύτατα σε ψηφιακές πλατφόρμες, το πρόγραμμα Advanced Personal Data Security and Privacy Micro Credential δίνει στους εκπαιδευόμενους τη δυνατότητα να κατανοήσουν ολιστικά την ασφάλεια των προσωπικών δεδομένων στη διαδικτυακή σφαίρα. Μέσα από μια εις βάθος διερεύνηση της κρυπτογραφημένης επικοινωνίας, των πρακτικών προστασίας προσωπικών δεδομένων και της ανίχνευσης παραβιάσεων της ιδιωτικής ζωής, το πρόγραμμα μεταδίδει τις απαραίτητες δεξιότητες και γνώσεις για να διασφαλίσει ασφαλείς ψηφιακές αλληλεπιδράσεις.

Αρχικά, η κρυπτογραφημένη επικοινωνία αποτελεί τον ακρογωνιαίο λίθο της ασφαλούς διαδικτυακής επικοινωνίας, αποτελώντας το πρώτο μαθησιακό αποτέλεσμα. Η κρυπτογράφηση είναι ένα ισχυρό εργαλείο ασφαλείας που συγκαλύπτει τις πληροφορίες για να αποτρέψει τη μη εξουσιοδοτημένη πρόσβαση. Η κρυπτογραφημένη επικοινωνία αξιοποιεί αυτή την τεχνολογία για την προστασία των πληροφοριών καθώς ταξιδεύουν από τον αποστολέα στον παραλήπτη, διασφαλίζοντας ότι το περιεχόμενο παραμένει εμπιστευτικό και διατηρεί την ακεραιότητά του.

Το πρόγραμμα ρίχνει φως στην έννοια της κρυπτογράφησης από άκρο σε άκρο, μια συγκεκριμένη μορφή κρυπτογράφησης όπου μόνο οι χρήστες που επικοινωνούν μπορούν να διαβάσουν τα μηνύματα. Κατ' αρχήν, εμποδίζει τους πιθανούς υποκλοπέους - συμπεριλαμβανομένων των παρόχων τηλεπικοινωνιών, των παρόχων διαδικτύου, ακόμη και του ίδιου του παρόχου υπηρεσιών - να έχουν πρόσβαση στα κρυπτογραφικά κλειδιά που απαιτούνται για την αποκρυπτογράφηση της συνομιλίας. Αυτό το προηγμένο μέτρο ασφαλείας χρησιμοποιείται από πολλές σύγχρονες εφαρμογές επικοινωνίας για την προστασία της ιδιωτικής ζωής των χρηστών.

Παρέχεται μια σε βάθος ανάλυση για διάφορες εφαρμογές κρυπτογραφημένης επικοινωνίας, όπως το Signal, το WhatsApp και το Telegram, οι οποίες διαφέρουν ως προς το επίπεδο ασφάλειας, τις πολιτικές προστασίας της ιδιωτικής ζωής και τα πρωτόκολλα κρυπτογράφησης. Το πρόγραμμα, ωστόσο, δεν προωθεί τη μία εφαρμογή έναντι της άλλης. Αντίθετα, τονίζει τη σημασία της τεκμηριωμένης λήψης αποφάσεων με βάση την αξιολόγηση των αναγκών προστασίας της ιδιωτικής ζωής, την κατανόηση των πολιτικών προστασίας της ιδιωτικής ζωής και την κατανόηση των προτύπων κρυπτογράφησης κάθε εφαρμογής.

Πέρα από την απλή επικοινωνία, το δεύτερο μαθησιακό αποτέλεσμα παρέχει στους εκπαιδευόμενους μια ολοκληρωμένη κατανόηση των βέλτιστων πρακτικών για την προστασία των προσωπικών δεδομένων σε διάφορα διαδικτυακά πλαίσια. Το πρόγραμμα υπογραμμίζει ότι κάθε διαδικτυακή πλατφόρμα ή υπηρεσία απαιτεί μια μοναδική προσέγγιση για την προστασία των δεδομένων λόγω της ιδιαίτερης λειτουργικότητας, των πολιτικών απορρήτου και των μέτρων ασφαλείας.

Με την πανταχού παρούσα παρουσία των ηλεκτρονικών συναλλαγών, οι πλατφόρμες ηλεκτρονικού εμπορίου έχουν γίνει εστία εγκληματιών του κυβερνοχώρου. Ως εκ τούτου, το πρόγραμμα υπογραμμίζει τη σημασία των ασφαλών επιλογών πληρωμής, της χρήσης εξουσιοδοτημένων πλατφορμών και της προσοχής απέναντι στην κοινοποίηση ευαίσθητων οικονομικών πληροφοριών.

Οι πλατφόρμες κοινωνικής δικτύωσης, λόγω της μεγάλης εμβέλειάς τους και της ικανότητάς τους να διαδίδουν γρήγορα πληροφορίες, συχνά διευκολύνουν ακούσια τη διάδοση προσωπικών δεδομένων. Ως εκ τούτου, η κατανόηση των ρυθμίσεων απορρήτου, η διάκριση ως προς την αποδοχή αιτημάτων σύνδεσης και η προσοχή ως προς το είδος των πληροφοριών που μοιράζονται αποτελούν μέρος αυτής της ενότητας.

Το ηλεκτρονικό ταχυδρομείο και άλλα εργαλεία επαγγελματικής επικοινωνίας, που χρησιμοποιούνται συχνά για την ανταλλαγή ευαίσθητων επαγγελματικών δεδομένων, απαιτούν επίσης αυστηρές πρακτικές ασφαλείας. Το πρόγραμμα καθοδηγεί τους εκπαιδευόμενους μέσα από τις διαδικασίες καθορισμού ισχυρών κωδικών πρόσβασης, αναγνώρισης ηλεκτρονικών μηνυμάτων ηλεκτρονικού "ψαρέματος" και υπεύθυνης ανταλλαγής δεδομένων σε αυτά τα πλαίσια.

Το τρίτο μαθησιακό αποτέλεσμα του προγράμματος αφορά την ανίχνευση πιθανών παραβιάσεων της ιδιωτικής ζωής. Ανωμαλίες στις συσκευές, όπως απροσδόκητες καταρρεύσεις του συστήματος, αργές επιδόσεις, υπερβολικές αναδυόμενες διαφημίσεις, μη αναγνωρισμένες εφαρμογές ή ασυνήθιστη αποστράγγιση της μπαταρίας, θα μπορούσαν να υποδηλώνουν παραβίαση της ιδιωτικής ζωής.

Στο πλαίσιο αυτό, το πρόγραμμα παρέχει κατανόηση των διαφόρων εργαλείων και μεθόδων κυβερνοασφάλειας, όπως το λογισμικό προστασίας από ιούς, τα τείχη προστασίας και τα συστήματα ανίχνευσης εισβολών, που μπορούν να εντοπίσουν και να διαχειριστούν αυτές τις απειλές. Το πρόγραμμα εκπαιδεύει περαιτέρω τους εκπαιδευόμενους στο πώς να ελέγχουν τακτικά τις συσκευές και τους διαδικτυακούς λογαριασμούς τους για απροσδόκητες αλλαγές και πώς να λαμβάνουν διορθωτικά μέτρα σε περίπτωση παραβίασης, όπως αλλαγή κωδικών πρόσβασης, αποσύνδεση από το διαδίκτυο ή επικοινωνία με επαγγελματίες κυβερνοασφάλειας.

Ουσιαστικά, το πρόγραμμα Advanced Personal Data Security and Privacy Micro Credential καλλιεργεί μια ολοκληρωμένη κατανόηση της διαδικτυακής ασφάλειας και του απορρήτου των δεδομένων. Στο τέλος του προγράμματος, οι εκπαιδευόμενοι θα διαθέτουν τις δεξιότητες να επικοινωνούν με ασφάλεια στο διαδίκτυο, να διασφαλίζουν τα προσωπικά δεδομένα σε διάφορες πλατφόρμες και να εντοπίζουν και να ανταποκρίνονται αποτελεσματικά σε πιθανές παραβιάσεις της ιδιωτικής ζωής.

Το πρόγραμμα αυτό αποτελεί απόδειξη της ανάγκης για μια ευρύτερη κουλτούρα ψηφιακής ασφάλειας και ευαισθητοποίησης της ιδιωτικής ζωής στην ολοένα και πιο διασυνδεδεμένη κοινωνία μας. Οι δεξιότητες και οι γνώσεις που αποκτώνται εδώ δεν περιορίζονται μόνο σε προσωπικό όφελος. Συμβάλλουν επίσης στη δημιουργία ασφαλέστερων ψηφιακών χώρων για όλους, βοηθώντας τις κοινότητες να ευδοκιμήσουν στην ψηφιακή εποχή. Σε έναν κόσμο όπου τα όρια μεταξύ ψηφιακού και φυσικού συνεχώς θολώνουν, η διασφάλιση της ψηφιακής ασφάλειας δεν αποτελεί πλέον πολυτέλεια αλλά αναγκαιότητα. Αυτό το πρόγραμμα Micro Credential σηματοδοτεί ένα σημαντικό βήμα προς αυτή την κατεύθυνση, προωθώντας την ικανότητα να περιηγείται κανείς με αυτοπεποίθηση στον ψηφιακό κόσμο, προστατεύοντας τόσο τον εαυτό του όσο και τους άλλους από πιθανές απειλές στον κυβερνοχώρο.

Ερωτήσεις

1. Ποιος είναι ο σκοπός της κρυπτογραφημένης επικοινωνίας στο πλαίσιο της διαδικτυακής ασφάλειας;
2. Εξηγήστε την έννοια της κρυπτογράφησης από άκρο σε άκρο και τη σημασία της για τη διατήρηση της ιδιωτικής ζωής.
3. Συγκρίνετε και αντιπαραβάλλετε τα πρωτόκολλα κρυπτογράφησης των Signal, WhatsApp και Telegram.
4. Γιατί είναι ζωτικής σημασίας η κατανόηση και η αξιολόγηση των πολιτικών απορρήτου των διαφόρων εφαρμογών επικοινωνίας;
5. Ποιες είναι οι βέλτιστες πρακτικές για την προστασία των προσωπικών δεδομένων σε πλατφόρμες ηλεκτρονικού εμπορίου;
6. Συζητήστε τις βασικές εκτιμήσεις για την προστασία των προσωπικών δεδομένων στις πλατφόρμες κοινωνικής δικτύωσης.
7. Ποια είναι ορισμένα μέτρα που μπορούν να ληφθούν για την ενίσχυση της ασφάλειας των εργαλείων επαγγελματικής επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο;
8. Προσδιορίστε και εξηγήστε τρεις ανωμαλίες σε συσκευές που μπορεί να υποδηλώνουν παραβίαση του απορρήτου.
9. Πώς μπορούν τα εργαλεία κυβερνοασφάλειας, όπως το λογισμικό προστασίας από ιούς και τα τείχη προστασίας, να βοηθήσουν στον εντοπισμό πιθανών παραβιάσεων της ιδιωτικής ζωής;
10. Συζητήστε τα βήματα που απαιτούνται για τη διενέργεια ελέγχου των συσκευών και των διαδικτυακών λογαριασμών για παραβιάσεις του απορρήτου.
11. Ποιες ενέργειες πρέπει να γίνουν σε περίπτωση εντοπισμού παραβίασης της ιδιωτικής ζωής;
12. Πώς συμβάλλουν οι γνώσεις και οι πρακτικές για την ασφάλεια των προσωπικών δεδομένων στη συνολική κουλτούρα ψηφιακής ασφάλειας;
13. Πώς η διασφάλιση της προσωπικής ψηφιακής ασφάλειας συμβάλλει στην ευρύτερη ψηφιακή κοινότητα και την ευημερία της;

Διαχείριση ψηφιακού απορρήτου και ασφαλής διαδικτυακή αλληλεπίδραση (MC 4.2.B.8)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης

Τίτλος και κωδικός του μικροπιστοποιητικού	Διαχείριση ψηφιακού απορρήτου & ασφαλής διαδικτυακή αλληλεπίδραση **Κωδ: B.8**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ΕΝΔΙΑΜΕΣΟ
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.39, 4.2.40):

- Διακρίνετε όλους τους τύπους "cookies" και πώς μπορούν να χρησιμοποιηθούν από τους ιστότοπους για την αποθήκευση δεδομένων των χρηστών.
- Δώστε προτεραιότητα στους διαδικτυακούς σας λογαριασμούς με βάση την ευαισθησία των πληροφοριών που περιέχουν.

Περιγραφή

Το πρόγραμμα "Διαχείριση ψηφιακού απορρήτου και ασφαλής διαδικτυακή αλληλεπίδραση" προσφέρει μια ολοκληρωμένη κατανόηση δύο πρωταρχικών τομέων της ψηφιακής ασφάλειας και της ασφάλειας δεδομένων: τη διάκριση διαφορετικών τύπων "cookies" και τη χρήση τους στην αποθήκευση δεδομένων σε ιστότοπους και την κατηγοριοποίηση των διαδικτυακών λογαριασμών με βάση την ευαισθησία των πληροφοριών που περιέχουν.

Το πρόγραμμα ξεκινά μια εξερεύνηση του διαφοροποιημένου κόσμου των "cookies" - μικρά αρχεία που οι ιστότοποι στέλνουν και αποθηκεύουν στις συσκευές των χρηστών για να θυμούνται συγκεκριμένες λεπτομέρειες σχετικά με την επίσκεψη. Τα cookies έχουν γίνει αναπόσπαστα στοιχεία της εμπειρίας περιήγησης στον ιστό, επηρεάζοντας τον τρόπο με τον οποίο οι χρήστες αλληλεπιδρούν με τους ιστότοπους, τις πληροφορίες που θυμούνται οι ιστότοποι και τους τύπους διαφημίσεων που βλέπουν οι χρήστες. Ωστόσο, δεν είναι όλα τα cookies ίδια και η κατανόηση των διαφορετικών ποικιλιών είναι ζωτικής σημασίας για τη διαχείριση της διαδικτυακής ιδιωτικότητας και της ασφάλειας των δεδομένων.

Τα cookies είναι μικρά κομμάτια δεδομένων που αποθηκεύονται στον υπολογιστή του χρήστη από το πρόγραμμα περιήγησης ιστού κατά την περιήγηση σε έναν ιστότοπο. Παίζουν ουσιαστικό ρόλο στη βελτίωση της εμπειρίας του χρήστη, καθώς θυμούνται πληροφορίες σχετικά με την επίσκεψή του, όπως πληροφορίες σύνδεσης, γλωσσικές προτιμήσεις και άλλες ρυθμίσεις. Όμως, ενώ τα cookies προσφέρουν ευκολία, μπορούν επίσης να παρουσιάσουν ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής, επειδή μπορούν να παρακολουθούν τη δραστηριότητα περιήγησης και να συλλέγουν δεδομένα σχετικά με τη διαδικτυακή συμπεριφορά των χρηστών.

Οι διαφορετικοί τύποι cookies έχουν διαφορετικούς σκοπούς και η κατανόηση αυτών των σκοπών μπορεί να βοηθήσει τα άτομα να διαχειριστούν καλύτερα το διαδικτυακό τους απόρρητο:

1. Cookies συνόδου: Τα cookies αυτά είναι προσωρινά και διαγράφονται όταν ο χρήστης κλείσει το πρόγραμμα περιήγησής του. Χρησιμοποιούνται για να θυμούνται τις ενέργειες του χρήστη μέσα σε μια περίοδο περιήγησης, όπως τα στοιχεία που προστίθενται σε ένα καλάθι αγορών σε έναν ιστότοπο ηλεκτρονικού εμπορίου. Αυτά τα cookies συνήθως δεν εγείρουν σημαντικές ανησυχίες για την προστασία της ιδιωτικής ζωής, επειδή δεν παρακολουθούν τη δραστηριότητα του χρήστη σε πολλαπλές περιόδους ή ιστότοπους.
2. Επίμονα cookies: Τα μόνιμα cookies παραμένουν στον υπολογιστή του χρήστη ακόμη και όταν αυτός κλείσει το πρόγραμμα περιήγησής του. Χρησιμοποιούνται για να θυμούνται τις προτιμήσεις και τις ενέργειες ενός χρήστη σε πολλαπλές περιόδους περιήγησης, όπως οι προτιμήσεις διάταξης του ιστότοπου ή οι πληροφορίες σύνδεσης. Επειδή παρακολουθούν τη δραστηριότητα με την πάροδο του χρόνου, μπορεί να εγείρουν ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής, ιδίως εάν συλλέγουν ευαίσθητες πληροφορίες.
3. Ασφαλή cookies: Αυτά μεταδίδονται μέσω κρυπτογραφημένων συνδέσεων (HTTPS), καθιστώντας τα ασφαλέστερα από τα κανονικά cookies. Αποτρέπουν την υποκλοπή των δεδομένων που μεταδίδουν από μη εξουσιοδοτημένα μέρη.
4. HTTP-only cookies: Αυτά τα cookies δεν είναι προσβάσιμα από σενάρια από την πλευρά του πελάτη, όπως η JavaScript. Αυτό τα καθιστά πιο ασφαλή έναντι ορισμένων τύπων επιθέσεων, όπως οι επιθέσεις cross-site scripting (XSS), οι οποίες χρησιμοποιούν κακόβουλα σενάρια για να κλέψουν τα cookies και τις πληροφορίες που περιέχουν.

5. Cookies τρίτων: Τα cookies αυτά δημιουργούνται από άλλους τομείς εκτός από αυτόν που επισκέπτεται ο χρήστης αυτή τη στιγμή. Χρησιμοποιούνται συχνά για διαδικτυακές διαφημίσεις και μπορούν να παρακολουθούν τη δραστηριότητα ενός χρήστη σε πολλούς ιστότοπους, εγείροντας σημαντικές ανησυχίες για την προστασία της ιδιωτικής ζωής.

Με την κατανόηση αυτών των διαφορετικών τύπων cookies, τα άτομα μπορούν να λαμβάνουν πιο τεκμηριωμένες αποφάσεις σχετικά με το διαδικτυακό τους απόρρητο. Για παράδειγμα, μπορεί να επιλέξουν να μπλοκάρουν τα cookies τρίτων μερών για να αποτρέψουν τη διασταυρούμενη παρακολούθηση ή να διαγράφουν τακτικά τα cookies τους για να αφαιρέσουν τα μόνιμα cookies και να περιορίσουν τον όγκο των δεδομένων που μπορούν να συλλεχθούν σχετικά με το ιστορικό περιήγησής τους.

Επιπλέον, η κατανόηση των cookies μπορεί να βοηθήσει τα άτομα να ερμηνεύσουν τις πολιτικές απορρήτου των ιστότοπων, οι οποίες συχνά αποκαλύπτουν τους τύπους των cookies που χρησιμοποιεί ένας ιστότοπος και για ποιο λόγο χρησιμοποιούνται. Αυτή η γνώση επιτρέπει στους χρήστες να κάνουν πιο τεκμηριωμένες επιλογές σχετικά με το αν θα χρησιμοποιήσουν έναν ιστότοπο και πώς θα ορίσουν τις ρυθμίσεις απορρήτου τους.

Τέλος, η κατανόηση των επιπτώσεων των cookies μπορεί να ενθαρρύνει πιο υγιεινές διαδικτυακές συνήθειες. Για παράδειγμα, η αναγνώριση ότι τα cookies μπορούν να παρακολουθούν τη διαδικτυακή δραστηριότητα μπορεί να παρακινήσει τα άτομα να χρησιμοποιούν εργαλεία που ενισχύουν την ιδιωτικότητα, όπως αποκλειστές διαφημίσεων ή εικονικά ιδιωτικά δίκτυα (VPN), ή να χρησιμοποιούν προγράμματα περιήγησης ή μηχανές αναζήτησης που δεν παρακολουθούν τη δραστηριότητα του χρήστη.

Τα cookies διαδραματίζουν κρίσιμο ρόλο στο σύγχρονο διαδίκτυο, αλλά εγείρουν επίσης ανησυχίες για την προστασία της ιδιωτικής ζωής. Με την κατανόηση των διαφόρων τύπων cookies και του τρόπου με τον οποίο τα χρησιμοποιούν οι ιστότοποι, τα άτομα μπορούν να λάβουν προληπτικά μέτρα για τη διαχείριση του διαδικτυακού απορρήτου τους, όπως η προσαρμογή των ρυθμίσεων του προγράμματος περιήγησής τους, η τακτική εκκαθάριση των cookies, η χρήση εργαλείων βελτίωσης του απορρήτου και η λήψη πιο τεκμηριωμένων αποφάσεων σχετικά με τους ιστότοπους που θα χρησιμοποιήσουν. Αυτό μπορεί να οδηγήσει σε μια ασφαλέστερη, πιο συνειδητή εμπειρία ιδιωτικότητας στο διαδίκτυο.

Το δεύτερο μείζον μαθησιακό αποτέλεσμα σε αυτό το πρόγραμμα σχετίζεται με την ιεράρχηση των ηλεκτρονικών λογαριασμών με βάση την ευαισθησία των πληροφοριών που περιέχουν. Στη σημερινή ψηφιακή εποχή, τα περισσότερα άτομα έχουν πολλούς διαδικτυακούς λογαριασμούς, από πλατφόρμες μέσων κοινωνικής δικτύωσης έως διαδικτυακές τραπεζικές συναλλαγές και αγορές, καθένας από τους οποίους αποθηκεύει ποικίλες ποσότητες προσωπικών πληροφοριών.

Η ιεράρχηση των διαδικτυακών λογαριασμών με βάση την ευαισθησία των πληροφοριών που περιέχουν είναι ένα κρίσιμο βήμα προς τη διατήρηση της ιδιωτικότητας και της ασφάλειας στην ψηφιακή σφαίρα. Τα περισσότερα άτομα σήμερα διαχειρίζονται πολυάριθμους διαδικτυακούς λογαριασμούς σε ένα ευρύ φάσμα υπηρεσιών.

Αυτά μπορεί να περιλαμβάνουν προφίλ στα μέσα κοινωνικής δικτύωσης, λογαριασμούς ηλεκτρονικού ταχυδρομείου, ηλεκτρονικές τραπεζικές συναλλαγές, πλατφόρμες ηλεκτρονικού εμπορίου, συνδρομητικές υπηρεσίες, αρχεία υγείας και πολλά άλλα. Κάθε ένας από αυτούς τους λογαριασμούς διατηρεί διαφορετικές ποσότητες προσωπικών πληροφοριών και, ως εκ τούτου, παρουσιάζει διαφορετικά επίπεδα κινδύνου σε περίπτωση παραβίασης.

Η διαδικασία ιεράρχησης περιλαμβάνει την αξιολόγηση του δυνητικού αντίκτυπου ή της ζημίας που θα μπορούσε να προκληθεί εάν ένα μη εξουσιοδοτημένο άτομο αποκτούσε πρόσβαση σε κάθε συγκεκριμένο λογαριασμό.

Ακολουθούν ορισμένα στοιχεία που πρέπει να λάβετε υπόψη σας κατά την ιεράρχηση των λογαριασμών:

1. Οικονομικές πληροφορίες: θα πρέπει να είναι στην κορυφή της λίστας προτεραιότητας. Μια παραβίαση αυτών των λογαριασμών μπορεί να οδηγήσει σε οικονομική απώλεια και κλοπή ταυτότητας.
2. Λογαριασμοί ηλεκτρονικού ταχυδρομείου: Ο κύριος λογαριασμός ηλεκτρονικού ταχυδρομείου σας, ειδικά αν χρησιμοποιείται ως email ανάκτησης για άλλες υπηρεσίες, είναι επίσης ένας λογαριασμός υψηλής προτεραιότητας. Η μη εξουσιοδοτημένη πρόσβαση στο email σας μπορεί να οδηγήσει σε ντόμινο παραβιάσεων, καθώς μπορεί να χρησιμοποιηθεί για την επαναφορά κωδικών πρόσβασης και την απόκτηση πρόσβασης σε άλλους λογαριασμούς.
3. Αρχεία υγείας: Μια παραβίαση εδώ θα μπορούσε να οδηγήσει σε σοβαρές παραβιάσεις της ιδιωτικής ζωής και πιθανή κατάχρηση προσωπικών πληροφοριών υγείας.
4. Επαγγελματικοί λογαριασμοί: ή οποιαδήποτε πλατφόρμα που περιέχει τα επαγγελματικά σας δεδομένα. Η υπονόμευση αυτών των λογαριασμών μπορεί να οδηγήσει σε απώλεια πνευματικής ιδιοκτησίας και βλάβη της επαγγελματικής φήμης.
5. Λογαριασμοί στα μέσα κοινωνικής δικτύωσης: Παρόλο που μπορεί να μην φαίνονται τόσο κρίσιμοι όσο οι οικονομικοί ή επαγγελματικοί λογαριασμοί, οι λογαριασμοί κοινωνικής δικτύωσης περιέχουν πολλές προσωπικές πληροφορίες που μπορούν να αξιοποιηθούν για κλοπή ταυτότητας ή να χρησιμοποιηθούν για να στοχεύσουν εσάς και τις επαφές σας σε επιθέσεις phishing.

Μετά τον εντοπισμό και την ιεράρχηση των λογαριασμών, θα πρέπει να χρησιμοποιηθούν διάφορες στρατηγικές για την ενίσχυση της ασφάλειας αυτών των λογαριασμών:

- Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης για κάθε λογαριασμό. Εξετάστε το ενδεχόμενο χρήσης ενός διαχειριστή κωδικών πρόσβασης για την παρακολούθησή τους.
- Ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων (2FA) ή τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) όποτε είναι δυνατόν.
- Παρακολουθείτε και ενημερώνετε τακτικά τις ρυθμίσεις ασφαλείας.
- Να είστε προσεκτικοί όσον αφορά την ανταλλαγή πληροφοριών, ιδίως ευαίσθητων δεδομένων, στο διαδίκτυο.

Η κατανόηση της ευαισθησίας των πληροφοριών που κατέχουν οι διάφοροι λογαριασμοί και η λήψη των κατάλληλων μέτρων με βάση το επίπεδο του σχετικού κινδύνου αποτελεί βασική πρακτική για τη διατήρηση των προσωπικών πληροφοριών με ασφάλεια στην ψηφιακή εποχή. Με την ιεράρχηση των διαδικτυακών λογαριασμών με βάση την ευαισθησία των δεδομένων που κατέχουν, τα άτομα μπορούν να κατανέμουν αποτελεσματικά τις προσπάθειές τους για την ασφάλεια, εστιάζοντας στην προστασία των λογαριασμών που θα μπορούσαν να προκαλέσουν τη μεγαλύτερη ζημιά σε περίπτωση παραβίασης.

Συνολικά, αυτό το πρόγραμμα Micro Credential εξοπλίζει τα άτομα με κρίσιμες γνώσεις σχετικά με τις λειτουργίες των cookies και την ανάγκη ιεράρχησης των διαδικτυακών λογαριασμών με βάση την ευαισθησία των δεδομένων, επιτρέποντάς τους να περιηγηθούν στον ψηφιακό κόσμο με αυξημένη ευαισθητοποίηση και επάρκεια. Με αυτές τις δεξιότητες, τα άτομα μπορούν να προστατεύουν καλύτερα τις προσωπικές τους

πληροφορίες, να συμβάλλουν σε μια ευρύτερη κουλτούρα απορρήτου δεδομένων και να προωθήσουν μια πιο ασφαλή ψηφιακή κοινωνία.

Ερωτήσεις

1. Ορισμός των cookies στο πλαίσιο της περιήγησης στο διαδίκτυο και εξήγηση της κύριας λειτουργίας τους.
2. Διακρίνετε μεταξύ των cookies περιόδου λειτουργίας και των μόνιμων cookies. Πώς διαφέρουν οι λειτουργίες τους;
3. Ποια είναι η σημασία των ασφαλών cookies; Γιατί θεωρούνται ασφαλέστερα από τα κανονικά cookies;
4. Περιγράψτε τα cookies HTTP-only και συζητήστε πώς παρέχουν πρόσθετη ασφάλεια.
5. Τι είναι τα cookies τρίτου μέρους και γιατί μπορεί να θεωρηθούν ανησυχητικά για την προστασία της ιδιωτικής ζωής;
6. Πώς η κατανόηση των διαφορετικών τύπων cookies βοηθά στη διαχείριση του διαδικτυακού απορρήτου;
7. Πώς μπορεί η γνώση για τα cookies να βοηθήσει ένα άτομο στην ερμηνεία της πολιτικής απορρήτου ενός ιστότοπου;
8. Περιγράψτε ορισμένες στρατηγικές διαχείρισης των cookies για την ενίσχυση της διαδικτυακής ιδιωτικότητας.
9. Εξηγήστε τη σημασία της ιεράρχησης των διαδικτυακών λογαριασμών με βάση την ευαισθησία των πληροφοριών που περιέχουν.
10. Ποιοι παράγοντες πρέπει να λαμβάνονται υπόψη κατά την ιεράρχηση των ηλεκτρονικών λογαριασμών για αυξημένη ιδιωτικότητα και ασφάλεια;
11. Συζητήστε τους κινδύνους που συνδέονται με την παραβίαση διαδικτυακών λογαριασμών υψηλής προτεραιότητας, όπως αυτοί που περιέχουν οικονομικές πληροφορίες ή αρχεία υγείας.
12. Ποιες μπορεί να είναι οι πιθανές συνέπειες μιας παραβίασης των επαγγελματικών λογαριασμών;
13. Γιατί είναι σημαντικό να λαμβάνονται υπόψη οι λογαριασμοί κοινωνικής δικτύωσης κατά την ιεράρχηση των ηλεκτρονικών λογαριασμών, ακόμη και αν δεν περιέχουν προφανώς ευαίσθητα δεδομένα;
14. Περιγράψτε τα μέτρα που μπορεί να λάβει κανείς για να ενισχύσει την ασφάλεια των διαδικτυακών λογαριασμών υψηλής προτεραιότητας.
15. Πώς συμβάλλει η πρακτική της ιεράρχησης των διαδικτυακών λογαριασμών με βάση την ευαισθησία των δεδομένων στη συνολική ασφάλεια των προσωπικών πληροφοριών και στην προστασία της ιδιωτικής ζωής των δεδομένων;

Ασφάλεια προσωπικών συσκευών και βέλτιστες πρακτικές (MC 4.2.C.1)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ασφάλεια προσωπικών συσκευών και βέλτιστες πρακτικές Κωδ: C.1: MC 4.2.C.1
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ADVANCED
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.41, 4.2.42):

- Αξιολογήστε και συγκρίνετε διάφορες λύσεις λογισμικού ασφαλείας, όπως προγράμματα προστασίας από ιούς και τείχη προστασίας, για να επιλέξετε τις πιο αποτελεσματικές για τη συγκεκριμένη συσκευή και τις ανάγκες σας.
- Υποστηρίξτε την αποφυγή της χρήσης ευαίσθητων ή εύκολα ανιχνεύσιμων πληροφοριών στους κωδικούς πρόσβασης για να ενισχύσετε την ισχύ και την ασφάλειά τους.

Περιγραφή

Το Micro Credential "Personal Device Security and Best Practices" είναι ένα ολοκληρωμένο και πρακτικό πρόγραμμα που έχει σχεδιαστεί για να ενδυναμώσει τους εκπαιδευόμενους με βασικές γνώσεις και δεξιότητες ώστε να προστατεύουν τις προσωπικές τους συσκευές και τα δεδομένα τους σε έναν ολοένα και πιο διασυνδεδεμένο κόσμο. Με την έγκριση της Ευρωπαϊκής Επιτροπής, το πρόγραμμα αυτό εξοπλίζει τους συμμετέχοντες με πρακτικά εργαλεία και τεχνικές για την αξιολόγηση και την επιλογή των πιο αποτελεσματικών λύσεων λογισμικού ασφαλείας, όπως προγράμματα antivirus και firewalls, προσαρμοσμένων στις συγκεκριμένες συσκευές και ανάγκες ασφαλείας τους.

Στην πρώτη ενότητα, οι εκπαιδευόμενοι εμβαθύνουν στον κόσμο του λογισμικού ασφαλείας, εξερευνώντας τις διάφορες επιλογές που διατίθενται στην αγορά. Μαθαίνουν να αξιολογούν τα χαρακτηριστικά, τις δυνατότητες και τις επιδόσεις των διαφόρων λύσεων antivirus και firewall για να εντοπίσουν την καλύτερη δυνατή λύση για τις συσκευές τους. Μέσω προσομοιώσεων και ασκήσεων πραγματικού κόσμου, οι συμμετέχοντες αποκτούν πρακτική εμπειρία στην αποτελεσματική εγκατάσταση και διαμόρφωση λογισμικού ασφαλείας.

Η δεύτερη ενότητα επικεντρώνεται στη διαχείριση κωδικών πρόσβασης, μια κρίσιμη πτυχή της ασφάλειας προσωπικών συσκευών. Οι εκπαιδευόμενοι ενημερώνονται για τα τρωτά σημεία που σχετίζονται με τη χρήση ευαίσθητων ή εύκολα ανιχνεύσιμων πληροφοριών σε κωδικούς πρόσβασης. Κατανοώντας τις αρχές της δημιουργίας ισχυρών κωδικών πρόσβασης, είναι σε θέση να υποστηρίξουν τις βέλτιστες πρακτικές και να συνηγορήσουν υπέρ της χρήσης διαχειριστών κωδικών πρόσβασης για την ασφαλή αποθήκευση και διαχείριση σύνθετων κωδικών πρόσβασης σε διάφορους διαδικτυακούς λογαριασμούς.

Καθ' όλη τη διάρκεια του Micro Credential, οι εκπαιδευόμενοι εκτίθενται σε πραγματικές μελέτες περιπτώσεων και σενάρια ασφάλειας στον κυβερνοχώρο, επιτρέποντάς τους να εφαρμόσουν τις νεοαποκτηθείσες γνώσεις τους σε πρακτικές καταστάσεις. Ενθαρρύνονται να αναλύουν κριτικά πιθανούς κινδύνους ασφάλειας και να σχεδιάζουν προληπτικές στρατηγικές για τον αποτελεσματικό μετριασμό των απειλών.

Με την επιτυχή ολοκλήρωση του Micro Credential "Personal Device Security and Best Practices", οι συμμετέχοντες θα κερδίσουν μια υψηλού κύρους έγκριση από την Ευρωπαϊκή Επιτροπή, επιβεβαιώνοντας την κυριαρχία τους στην ασφάλεια των συσκευών και τη διαχείριση κωδικών πρόσβασης. Οπλισμένοι με αυτές τις ικανότητες, οι εκπαιδευόμενοι θα είναι εξοπλισμένοι για να προστατεύουν με αυτοπεποίθηση τις προσωπικές τους συσκευές και τα δεδομένα τους από απειλές στον κυβερνοχώρο, συμβάλλοντας σε ένα ασφαλέστερο και ασφαλέστερο ψηφιακό περιβάλλον για τους ίδιους και τους γύρω τους.

Ερωτήσεις

1. Ερώτηση σχετικά με την αξιολόγηση λύσεων λογισμικού ασφαλείας: "Βρίσκεστε στη διαδικασία επιλογής λογισμικού ασφαλείας για το φορητό σας υπολογιστή, τον οποίο χρησιμοποιείτε κυρίως για ηλεκτρονικές τραπεζικές συναλλαγές και εργασίες που σχετίζονται με την εργασία σας. Περιγράψτε τα κριτήρια που θα λαμβάνατε υπόψη σας κατά την αξιολόγηση διαφόρων προγραμμάτων προστασίας από ιούς και τείχη προστασίας. Ποιοι παράγοντες θα ήταν απαραίτητοι για να εξασφαλίσετε την πιο αποτελεσματική προστασία για τη συγκεκριμένη συσκευή και τις ανάγκες σας;"
2. Ερώτηση σχετικά με την προάσπιση της ασφάλειας του κωδικού πρόσβασης: "και ένας από αυτούς προτείνει τη χρήση εύκολα ανιχνεύσιμων πληροφοριών, όπως ημερομηνίες γέννησης ή κοινές λέξεις, στους κωδικούς πρόσβασης. Πώς θα συνηγορούσατε υπέρ της αποφυγής της χρήσης τέτοιων πληροφοριών και της προώθησης ισχυρότερων πρακτικών χρήσης κωδικών πρόσβασης; Δώστε λόγους και παραδείγματα για να υποστηρίξετε το επιχείρημά σας".
3. Ερώτηση με βάση σενάρια για την εφαρμογή των συστάσεων για τον κωδικό πρόσβασης: "Φανταστείτε ότι έχετε πολλούς διαδικτυακούς λογαριασμούς σε διαφορετικούς ιστότοπους και χρησιμοποιείτε αδύναμους και επαναλαμβανόμενους κωδικούς πρόσβασης. Αφού μάθατε για τη σημασία των ισχυρών κωδικών πρόσβασης, αποφασίζετε να ενισχύσετε την ασφάλεια των κωδικών πρόσβασης. Περιγράψτε τα βήματα που θα κάνατε για να βελτιώσετε την ισχύ και την ασφάλεια των κωδικών πρόσβασης. Πώς θα διασφαλίζατε ότι θα θυμάστε αυτούς τους σύνθετους κωδικούς πρόσβασης διατηρώντας παράλληλα υψηλό επίπεδο ασφάλειας;"

Ασφάλεια κωδικού πρόσβασης και βέλτιστες πρακτικές (MC 4.2.C.2)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ασφάλεια κωδικού πρόσβασης και βέλτιστες πρακτικές **Κωδ: C.2.C.2**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ADVANCED
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.43, 4.2.44 και 4.2.45):

- Κατανοήστε τη σημασία της αποφυγής λέξεων λεξικού ή κοινών μοτίβων στους κωδικούς πρόσβασης για την αποτροπή επιθέσεων με ωμή βία.
- Αναγνωρίστε τον κίνδυνο από τη χρήση του ίδιου κωδικού πρόσβασης σε πολλούς λογαριασμούς και τη σημασία της χρήσης μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό.
- Αναγνωρίστε τη σημασία της περιοδικής ενημέρωσης των κωδικών πρόσβασης και της αποφυγής της επαναχρησιμοποίησης παλαιών κωδικών πρόσβασης.

Περιγραφή

Το Micro Credential "Ασφάλεια κωδικών πρόσβασης και βέλτιστες πρακτικές" είναι ένα ολοκληρωμένο και εξειδικευμένο πρόγραμμα που έχει σχεδιαστεί με ακρίβεια για να ενδυναμώσει τους εκπαιδευόμενους με προηγμένες γνώσεις και δεξιότητες για τη διαφύλαξη της ψηφιακής τους ταυτότητας μέσω ισχυρών πρακτικών κωδικών πρόσβασης. Αυτό το πρόγραμμα, το οποίο έχει εγκριθεί από την αξιόλογη Ευρωπαϊκή Επιτροπή, εμβαθύνει στις περιπλοκές της ασφάλειας των κωδικών πρόσβασης, εξοπλίζοντας τους συμμετέχοντες με την τεχνογνωσία που απαιτείται για τη δημιουργία, διαχείριση και διατήρηση ισχυρών, μοναδικών κωδικών πρόσβασης που οχυρώνουν την ηλεκτρονική τους παρουσία έναντι πιθανών απειλών.

Στην πρώτη ενότητα, οι εκπαιδευόμενοι ξεκινούν ένα ταξίδι για να εξερευνήσουν τα τρωτά σημεία που σχετίζονται με τη χρήση λέξεων λεξικού ή κοινών μοτίβων σε κωδικούς πρόσβασης. Μέσα από διαφωτιστικές μελέτες περιπτώσεων και παραδείγματα από τον πραγματικό κόσμο, αποκτούν βαθιά κατανόηση του τρόπου με τον οποίο τέτοιες πρακτικές καθιστούν τους λογαριασμούς τους ευάλωτους σε επιθέσεις brute-force. Οπλισμένοι με αυτές τις γνώσεις, οι συμμετέχοντες θα καθοδηγηθούν σε εναλλακτικές στρατηγικές και βέλτιστες πρακτικές για την ανάπτυξη ιδιαίτερα ασφαλών κωδικών πρόσβασης που αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση και ματαιώνουν κακόβουλες προσπάθειες.

Η δεύτερη ενότητα εξετάζει τους κρίσιμους κινδύνους και τις συνέπειες της χρήσης του ίδιου κωδικού πρόσβασης σε πολλούς λογαριασμούς. Οι εκπαιδευόμενοι εκτίθενται σε εντυπωσιακά σενάρια που αναδεικνύουν το φαινόμενο ντόμινο της επαναχρησιμοποίησης κωδικών πρόσβασης, όπου ένας μόνο παραβιασμένος λογαριασμός μπορεί να οδηγήσει σε μια αλυσιδωτή σειρά παραβιάσεων ασφαλείας. Μέσω διαδραστικών ασκήσεων, αντιλαμβάνονται την ύψιστη σημασία της υιοθέτησης μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό, της διαφύλαξης των ψηφιακών τους περιουσιακών στοιχείων και της διατήρησης μιας ενισχυμένης άμυνας έναντι των αντιπάλων στον κυβερνοχώρο.

Στην τελευταία ενότητα, οι εκπαιδευόμενοι εισάγονται στην απαραίτητη σημασία της τακτικής ενημέρωσης των κωδικών πρόσβασης και της αποφυγής της επαναχρησιμοποίησης παλαιών κωδικών πρόσβασης. Αντιλαμβάνονται πώς αυτές οι πρακτικές συμβάλλουν σε μια διαρκώς εξελισσόμενη στάση ασφαλείας, οχυρώνοντας τα ψηφιακά τους φρούρια έναντι των αναδυόμενων απειλών στον κυβερνοχώρο. Με την εμπλοκή σε πρακτικές δραστηριότητες και προσομοιώσεις, οι συμμετέχοντες εσωτερικεύουν τις αρχές της αποτελεσματικής διαχείρισης κωδικών πρόσβασης, ενισχύοντας έτσι την ετοιμότητά τους να προσαρμοστούν στις εξελισσόμενες προκλήσεις ασφαλείας.

Κατά τη διάρκεια του Micro Credential, οι εκπαιδευόμενοι επωφελούνται από ένα δυναμικό και διαδραστικό περιβάλλον μάθησης, το οποίο διευκολύνεται από ειδικούς του κλάδου και έμπειρους επαγγελματίες της κυβερνοασφάλειας.

Συμμετέχουν σε πρακτικές ασκήσεις και προσομοιώσεις πραγματικής ζωής, που τους επιτρέπουν να εφαρμόζουν με αυτοπεποίθηση τις νεοαποκτηθείσες γνώσεις τους στις καθημερινές τους ψηφιακές αλληλεπιδράσεις.

Με την επιτυχή ολοκλήρωση του Micro Credential "Password Security and Best Practices", οι συμμετέχοντες όχι μόνο θα κερδίσουν μια υψηλού κύρους έγκριση από την Ευρωπαϊκή Επιτροπή, αλλά και θα γίνουν βασικοί παράγοντες αλλαγής στην προώθηση των βέλτιστων πρακτικών για την ασφάλεια των κωδικών πρόσβασης. Οπλισμένοι με προηγμένη τεχνογνωσία, θα λειτουργήσουν ως πυρπολητές, διαδίδοντας τις γνώσεις τους και προωθώντας μια κουλτούρα αυξημένης ψηφιακής ασφάλειας στις κοινότητες και τους οργανισμούς τους.

Συνοψίζοντας, το Micro Credential "Password Security and Best Practices" είναι ένα μετασχηματιστικό πρόγραμμα που υπερβαίνει τη θεωρία, ενδυναμώνοντας τους εκπαιδευόμενους με πρακτικές, εφαρμόσιμες γνώσεις και δεξιότητες για να ενισχύσουν την ψηφιακή τους ταυτότητα και να προστατεύσουν τα προσωπικά τους δεδομένα από το συνεχώς εξελισσόμενο πεδίο των απειλών στον κυβερνοχώρο. Είναι κατάλληλο για επαγγελματίες που επιδιώκουν να ενισχύσουν την ευστροφία τους στον τομέα της κυβερνοασφάλειας και για καθημερινούς χρήστες που φιλοδοξούν να διασφαλίσουν τα ψηφιακά τους πεδία με απόλυτη επάρκεια.

Ερωτήσεις

1. Ερώτηση σχετικά με την πολυπλοκότητα των κωδικών πρόσβασης: "Γιατί είναι ζωτικής σημασίας να αποφεύγεται η χρήση λέξεων λεξικού ή κοινών μοτίβων στους κωδικούς πρόσβασης; Πώς η εφαρμογή τέτοιων πρακτικών ενισχύει την ασφάλεια των λογαριασμών σας και αποτρέπει τις επιθέσεις brute-force; Δώστε παραδείγματα για να υποστηρίξετε την απάντησή σας".
2. Ερώτηση βάσει σεναρίου σχετικά με την επαναχρησιμοποίηση κωδικού πρόσβασης: "Χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης τόσο για το ηλεκτρονικό σας ταχυδρομείο όσο και για τους λογαριασμούς σας στις ηλεκτρονικές τράπεζες. Ποιοι είναι οι πιθανοί κίνδυνοι που συνδέονται με αυτή την πρακτική; Πώς μπορεί η χρήση μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό να μετριάσει αυτούς τους κινδύνους και να ενισχύσει τη συνολική σας ασφάλεια;"
3. Ερώτηση σχετικά με τη συχνότητα ενημέρωσης του κωδικού πρόσβασης: "Εξηγήστε τη σημασία της περιοδικής ενημέρωσης των κωδικών πρόσβασης. Πώς συμβάλλει αυτή η πρακτική στη διατήρηση ισχυρής ασφάλειας λογαριασμών με την πάροδο του χρόνου; Ποιους παράγοντες θα πρέπει να λάβετε υπόψη σας όταν αποφασίζετε πόσο συχνά θα ενημερώνετε τους κωδικούς πρόσβασης;"
4. Ερώτηση βάσει σεναρίου για την αλλαγή κωδικού πρόσβασης: "Ας υποθέσουμε ότι δεν έχετε αλλάξει τους κωδικούς πρόσβασης για τους λογαριασμούς σας στα μέσα κοινωνικής δικτύωσης εδώ και πάνω από ένα χρόνο. Ποιοι κίνδυνοι θα μπορούσαν να προκύψουν από αυτή την έλλειψη ενημέρωσης των κωδικών πρόσβασης; Περιγράψτε τα βήματα που θα λαμβάνατε για να ενημερώσετε αυτούς τους κωδικούς πρόσβασης και να διασφαλίσετε ότι είναι ισχυροί και μοναδικοί."
5. Ερώτηση σχετικά με τον μετριασμό της παραβίασης λογαριασμού: "Υποψιάζεστε ότι ο κωδικός πρόσβασής σας για έναν λογαριασμό ηλεκτρονικών αγορών μπορεί να έχει παραβιαστεί. Πώς η χρήση μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό θα βοηθούσε στον μετριασμό των πιθανών συνεπειών αυτής της παραβίασης της ασφάλειας; Ποια πρόσθετα μέτρα θα λαμβάνατε για την προστασία των άλλων λογαριασμών σας;"
6. Ερώτηση σχετικά με τις στρατηγικές διαχείρισης κωδικών πρόσβασης: "Πώς μπορούν οι διαχειριστές

κωδικών πρόσβασης να βοηθήσουν στην εφαρμογή μοναδικών και ασφαλών κωδικών πρόσβασης για κάθε λογαριασμό; Ποια είναι τα πλεονεκτήματα και τα πιθανά μειονεκτήματα της χρήσης διαχειριστών κωδικών πρόσβασης για τη διαχείριση κωδικών πρόσβασης;"

7. Ερώτηση βάσει σεναρίου σχετικά με την επαναχρησιμοποίηση παλαιών κωδικών πρόσβασης: "Φανταστείτε ότι χρησιμοποιήσατε κατά λάθος έναν παλιό κωδικό πρόσβασης από έναν προηγούμενο λογαριασμό για μια νέα διαδικτυακή υπηρεσία συνδρομής. Ποιους κινδύνους μπορεί να αντιμετωπίσετε εξαιτίας αυτής της αβλεψίας; Πώς θα διορθώνατε την κατάσταση και θα αποτρέπατε παρόμοια περιστατικά στο μέλλον;"

Ασφαλής διαχείριση συσκευών και αποδοτικότητα δεδομένων (MC 4.2.C.3)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ασφαλής διαχείριση συσκευών και αποδοτικότητα δεδομένων Κωδ: C.3: MC 4.2.C.3
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ADVANCED
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%

Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.46, 4.2.47):

- Χρησιμοποιήστε επιδέξια ένα πρόγραμμα συμπίεσης στη συσκευή σας για να μειώσετε τον όγκο των δεδομένων, εξασφαλίζοντας αποτελεσματική αποθήκευση και μετάδοση.
- Δυνατότητα διαμόρφωσης των ρυθμίσεων της συσκευής ώστε να κλειδώνει αυτόματα ή να αποσυνδέεται μετά από μια περίοδο αδράνειας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Περιγραφή

Το Micro Credential "Secure Device Management and Data Efficiency" είναι ένα πρωτοποριακό και ολοκληρωμένο πρόγραμμα που έχει σχεδιαστεί σχολαστικά για να ενδυναμώσει τους εκπαιδευόμενους με βασικές δεξιότητες για την ασφαλή διαχείριση των συσκευών τους και τη βελτιστοποίηση της αποδοτικότητας των δεδομένων. Το πρόγραμμα αυτό, το οποίο έχει εγκριθεί από την περίφημη Ευρωπαϊκή Επιτροπή, εξοπλίζει τους συμμετέχοντες με την τεχνογνωσία για να περιηγηθούν στο ψηφιακό τοπίο με αυτοπεποίθηση, διασφαλίζοντας ότι οι συσκευές τους είναι ανθεκτικές απέναντι σε πιθανές απειλές ασφαλείας και αποτελεσματικές στη διαχείριση δεδομένων.

Στην πρώτη ενότητα, οι εκπαιδευόμενοι ξεκινούν μια ενδιαφέρουσα εξερεύνηση της συμπίεσης δεδομένων. Με την καθοδήγηση έμπειρων εκπαιδευτών, οι συμμετέχοντες αποκτούν πρακτική εμπειρία στη χρήση προγραμμάτων συμπίεσης στις συσκευές τους για την αποτελεσματική μείωση του όγκου των δεδομένων χωρίς συμβιβασμούς στην ποιότητα. Μέσω πρακτικών ασκήσεων, μαθαίνουν να βελτιστοποιούν τον αποθηκευτικό χώρο και να βελτιώνουν τη μετάδοση δεδομένων, εξορθολογίζοντας έτσι τις ψηφιακές ροές εργασίας τους και καθιστώντας τις συσκευές τους πιο ευέλικτες και ανταποκρινόμενες. Είτε πρόκειται για τη διαχείριση μεγάλων αρχείων, είτε για την ενίσχυση της ανταλλαγής δεδομένων είτε για τη βελτιστοποίηση της χωρητικότητας αποθήκευσης, οι εκπαιδευόμενοι θα αποκτήσουν την ικανότητα να αξιοποιούν στο έπακρο τις δυνατότητες διαχείρισης δεδομένων των συσκευών τους.

Η δεύτερη ενότητα εξετάζει την ύψιστη πτυχή της ασφάλειας των συσκευών μέσω αυτοματοποιημένων μηχανισμών κλειδώματος και αποσύνδεσης. Οι εκπαιδευόμενοι γίνονται έμπειροι στη διαμόρφωση των ρυθμίσεων της συσκευής για την εφαρμογή λειτουργιών αυτόματου κλειδώματος ή αποσύνδεσης μετά από περιόδους αδράνειας.

Οπλισμένοι με αυτή τη γνώση, θωρακίζουν αποτελεσματικά τις συσκευές τους έναντι μη εξουσιοδοτημένης πρόσβασης, προστατεύοντας ευαίσθητες πληροφορίες και προσωπικά δεδομένα από πιθανές παραβιάσεις της

ασφάλειας. Η επιδέξια εφαρμογή αυτών των μέτρων διασφαλίζει ότι οι εκπαιδευόμενοι διατηρούν τον έλεγχο των σημείων πρόσβασης των συσκευών τους, καλλιεργώντας ένα ανθεκτικό και ασφαλές ψηφιακό περιβάλλον.

Καθ' όλη τη διάρκεια του Micro Credential, οι εκπαιδευόμενοι συμμετέχουν σε διαδραστικές προσομοιώσεις και σενάρια πραγματικής ζωής που τους επιτρέπουν να εφαρμόσουν τις νεοαποκτηθείσες γνώσεις τους σε πρακτικές καταστάσεις. Αντιμετωπίζοντας και επιλύοντας προκλήσεις σχετικές με τις καθημερινές ψηφιακές εμπειρίες τους, οι συμμετέχοντες αποκτούν ανεκτίμητες δεξιότητες για την αντιμετώπιση πραγματικών προβλημάτων διαχείρισης συσκευών και αποδοτικότητας δεδομένων.

Με την επιτυχή ολοκλήρωση του Micro Credential "Secure Device Management and Data Efficiency", οι συμμετέχοντες κερδίζουν μια υψηλού κύρους έγκριση από την Ευρωπαϊκή Επιτροπή, αναγνωρίζοντας την ικανότητά τους στην ασφάλεια των συσκευών τους και τη βελτιστοποίηση του χειρισμού των δεδομένων. Οπλισμένοι με αυτές τις προηγμένες δεξιότητες, οι εκπαιδευόμενοι είναι σε θέση να αγκαλιάσουν το εξελισσόμενο ψηφιακό τοπίο με αυτοπεποίθηση, συμβάλλοντας σε ένα ασφαλέστερο, πιο παραγωγικό και πολυδάπανο ψηφιακό οικοσύστημα.

Συνοψίζοντας, το Micro Credential "Secure Device Management and Data Efficiency" είναι ένα μετασχηματιστικό πρόγραμμα που συνδυάζει βασικές πρακτικές ασφάλειας και τεχνικές βελτιστοποίησης δεδομένων. Προσαρμοσμένο για άτομα που επιδιώκουν να αναβαθμίσουν τις ψηφιακές τους ικανότητες, το πρόγραμμα αυτό εξοπλίζει τους εκπαιδευόμενους ώστε να είναι έμπειροι πλοηγοί στο ψηφιακό πεδίο, διασφαλίζοντας ότι οι συσκευές τους παραμένουν ασφαλείς και ότι η χρήση των δεδομένων μεγιστοποιείται στο μέγιστο δυνατό βαθμό.

Ερωτήσεις

1. Πρακτική αξιολόγηση δεξιοτήτων στη συμπίεση δεδομένων: "Χρησιμοποιώντας ένα πρόγραμμα συμπίεσης της επιλογής σας, δείξτε πώς θα συμπιέζατε ένα μεγάλο αρχείο βίντεο χωρίς να υποβαθμίσετε την ποιότητά του. Εξηγήστε τα βήματα που ακολουθήσατε και τα αναμενόμενα οφέλη από τη συμπίεση του αρχείου όσον αφορά τη μείωση του όγκου δεδομένων και την αποτελεσματική αποθήκευση."
2. Ερώτηση βάσει σεναρίου σχετικά με τις ρυθμίσεις κλειδώματος συσκευών: "Φανταστείτε ότι χρησιμοποιείτε συχνά τη συσκευή σας σε δημόσιους χώρους και ανησυχείτε για μη εξουσιοδοτημένη πρόσβαση όταν αυτή μένει χωρίς επιτήρηση. Πώς θα διαμορφώνατε επιδέξια τις ρυθμίσεις της συσκευής σας ώστε να κλειδώνει αυτόματα μετά από μια περίοδο αδράνειας; Περιγράψτε τα βήματα που θα κάνατε και τα πιθανά οφέλη ασφαλείας από την εφαρμογή αυτής της λειτουργίας".
3. Ερώτηση κριτικής σκέψης σχετικά με την αποδοτικότητα των δεδομένων: "Ας υποθέσουμε ότι έχετε περιορισμένο αποθηκευτικό χώρο στη συσκευή σας και πρέπει να διαχειριστείτε διάφορα αρχεία, όπως έγγραφα, φωτογραφίες και μουσική. Πώς η επιδέξια συμπίεση δεδομένων και οι ρυθμίσεις της συσκευής για αυτόματο κλείδωμα/αποσύνδεση θα βοηθούσαν στη βελτιστοποίηση της αποδοτικότητας των δεδομένων και θα βελτίωναν τη συνολική ψηφιακή σας εμπειρία; Εξηγήστε τα πλεονεκτήματα αυτών των πρακτικών για τη διασφάλιση τόσο της ασφάλειας των δεδομένων όσο και της ομαλής διαχείρισης των δεδομένων."

Ψηφιακή ασφάλεια και ασφαλής χειρισμός δεδομένων (MC 4.2.C.4)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ψηφιακή ασφάλεια και ασφαλής χειρισμός δεδομένων Κωδικός: C.4: MC 4.2.C.4
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ADVANCED
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.48, 4.2.49 και 4.2.50):

- Γνωρίστε τους κινδύνους από τη χρήση των λειτουργιών αυτόματης σύνδεσης για ιστότοπους ή εφαρμογές που αποθηκεύουν προσωπικές πληροφορίες.
- Υποστηρίξτε τη χρήση ασφαλών μεθόδων μεταφοράς αρχείων, όπως το SFTP ή η ασφαλής αποθήκευση στο cloud, για την ανταλλαγή ευαίσθητων αρχείων μεταξύ συσκευών.
- Αναγνωρίστε τους πιθανούς κινδύνους από τη χρήση άγνωστου λογισμικού ή εφαρμογών στις συσκευές σας.

Περιγραφή

Το Micro Credential "Ψηφιακή ασφάλεια και ασφαλής χειρισμός δεδομένων" είναι ένα ολοκληρωμένο και προοδευτικό πρόγραμμα που έχει σχεδιαστεί για να ενδυναμώσει τους εκπαιδευόμενους με βασικές γνώσεις και δεξιότητες ώστε να περιηγούνται με ασφάλεια στο ψηφιακό τοπίο και να προστατεύουν ευαίσθητα δεδομένα. Το πρόγραμμα αυτό, το οποίο έχει εγκριθεί από την έγκριτη Ευρωπαϊκή Επιτροπή, εφοδιάζει τους συμμετέχοντες με την τεχνογνωσία ώστε να λαμβάνουν τεκμηριωμένες αποφάσεις, να υπερασπίζονται ασφαλείς πρακτικές και να προστατεύουν αποτελεσματικά τις ψηφιακές τους πληροφορίες.

Στην πρώτη ενότητα, οι εκπαιδευόμενοι κατανοούν σε βάθος τους κινδύνους που σχετίζονται με τις λειτουργίες αυτόματης σύνδεσης. Μέσω πραγματικών παραδειγμάτων και μελετών περίπτωσης, οι συμμετέχοντες αποκτούν οξεία επίγνωση των πιθανών συνεπειών του να επιτρέπει κανείς σε ιστότοπους ή εφαρμογές να αποθηκεύουν αυτόματα προσωπικές πληροφορίες. Οπλισμένοι με αυτές τις γνώσεις, οι εκπαιδευόμενοι είναι εξοπλισμένοι για να λαμβάνουν συνειδητές αποφάσεις σχετικά με την ενεργοποίηση ή την απενεργοποίηση τέτοιων χαρακτηριστικών για την προστασία των ευαίσθητων δεδομένων τους και τη διατήρηση της ψηφιακής τους ιδιωτικότητας.

Η δεύτερη ενότητα επικεντρώνεται σε ασφαλείς μεθόδους μεταφοράς αρχείων. Οι συμμετέχοντες εξοικειώνονται με τις τυποποιημένες πρακτικές της βιομηχανίας, όπως το SFTP (Secure File Transfer Protocol) και η ασφαλής αποθήκευση στο νέφος. Μέσω πρακτικών επιδείξεων και διαδραστικών ασκήσεων, οι εκπαιδευόμενοι κατανοούν τη σημασία της χρήσης αυτών των μεθόδων για την ασφαλή ανταλλαγή ευαίσθητων αρχείων μεταξύ συσκευών. Υποστηρίζοντας την ασφαλή μεταφορά αρχείων, οι συμμετέχοντες ενισχύουν την ικανότητά τους να προστατεύουν τις εμπιστευτικές πληροφορίες κατά την ψηφιακή επικοινωνία, μειώνοντας τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης ή παραβίασης δεδομένων.

Η τελευταία ενότητα ρίχνει φως στους πιθανούς κινδύνους από τη χρήση άγνωστου λογισμικού ή εφαρμογών σε προσωπικές συσκευές. Οι συμμετέχοντες διερευνούν τους κινδύνους που σχετίζονται με τη λήψη και την εκτέλεση λογισμικού από μη επαληθευμένες πηγές. Αναγνωρίζοντας αυτούς τους κινδύνους, οι εκπαιδευόμενοι ενισχύουν την ψηφιακή τους επαγρύπνηση και επιδεικνύουν προσοχή κατά την αξιολόγηση και τη χρήση νέων εφαρμογών, προστατεύοντας τις συσκευές τους από πιθανό κακόβουλο λογισμικό και τρωτά σημεία ασφαλείας.

Καθ' όλη τη διάρκεια του Micro Credential, οι εκπαιδευόμενοι συμμετέχουν σε πρακτικές δραστηριότητες, προσομοιώσεις και διαδραστικές συζητήσεις, επιτρέποντάς τους να εμπεδώσουν τις βέλτιστες πρακτικές για

την ψηφιακή ασφάλεια και τον ασφαλή χειρισμό δεδομένων. Με την επιτυχή ολοκλήρωση του προγράμματος οι εκπαιδευόμενοι όχι μόνο κερδίζουν μια υψηλού κύρους πιστοποίηση από την Ευρωπαϊκή Επιτροπή, αλλά και αποκτούν τη δυνατότητα να κάνουν υπεύθυνες και τεκμηριωμένες επιλογές στις ψηφιακές τους αλληλεπιδράσεις, συμβάλλοντας σε ένα ασφαλέστερο και ασφαλέστερο ψηφιακό περιβάλλον για τους ίδιους και τους άλλους.

Συνοψίζοντας, το Micro Credential "Ψηφιακή ασφάλεια και ασφαλής χειρισμός δεδομένων" είναι ένα μετασχηματιστικό πρόγραμμα που ενδυναμώνει τους εκπαιδευόμενους με τις γνώσεις και τις δεξιότητες για να περιηγηθούν στο ψηφιακό τοπίο με αυτοπεποίθηση. Οι συμμετέχοντες αναδεικνύονται σε υποστηρικτές ασφαλών πρακτικών, εξοπλισμένοι για την προστασία ευαίσθητων δεδομένων και την προώθηση της ψηφιακής ασφάλειας σε διάφορα πλαίσια, επιφέροντας θετικό αντίκτυπο στον προσωπικό και επαγγελματικό τους χώρο.

Ερωτήσεις

1. Ερώτηση ευαισθητοποίησης κινδύνου σχετικά με τις λειτουργίες αυτόματης σύνδεσης: "Εξηγήστε τους πιθανούς κινδύνους από τη χρήση χαρακτηριστικών αυτόματης σύνδεσης για ιστότοπους ή εφαρμογές που αποθηκεύουν προσωπικές πληροφορίες. Πώς μπορούν αυτά τα χαρακτηριστικά να θέσουν σε κίνδυνο το ψηφιακό σας απόρρητο και την ασφάλειά σας; Δώστε παραδείγματα σεναρίων στα οποία θα ήταν σκόπιμο να απενεργοποιήσετε την αυτόματη είσοδο".
2. Ερώτηση συνηγορίας και αιτιολόγησης σχετικά με τις μεθόδους ασφαλούς μεταφοράς αρχείων: "Σας έχει ανατεθεί να υποστηρίξετε τη χρήση ασφαλών μεθόδων μεταφοράς αρχείων στον χώρο εργασίας ή στην κοινότητά σας. Γράψτε μια πειστική δήλωση που να περιγράφει τη σημασία της χρήσης μεθόδων όπως το SFTP ή η ασφαλής αποθήκευση στο cloud για την ανταλλαγή ευαίσθητων αρχείων μεταξύ συσκευών. Περιλάβετε συγκεκριμένα οφέλη και πλεονεκτήματα αυτών των ασφαλών μεθόδων μεταφοράς έναντι των παραδοσιακών επιλογών μεταφοράς αρχείων."
3. Ερώτηση κριτικής σκέψης σχετικά με τους κινδύνους λογισμικού: "Συναντάτε μια νέα εφαρμογή λογισμικού από μια άγνωστη πηγή που ισχυρίζεται ότι παρέχει μοναδικά χαρακτηριστικά και λειτουργίες. Πώς θα προσεγγίζατε την απόφαση για το αν θα εγκαταστήσετε και θα χρησιμοποιήσετε αυτό το λογισμικό στη συσκευή σας; Συζητήστε τους πιθανούς κινδύνους που ενέχει η χρήση άγνωστου λογισμικού και περιγράψτε τα βήματα που θα κάνατε για να αξιολογήσετε τη νομιμότητα και την ασφάλειά του πριν προχωρήσετε".

Ασφάλεια συσκευών και προστασία δεδομένων (MC 4.2.C.5)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	**Κώδικας** ασφάλειας συσκευών και προστασίας δεδομένων: **C.6**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ADVANCED
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.51, 4.2.52):

- Αναγνωρίστε τη σημασία της απενεργοποίησης του Bluetooth στις συσκευές σας όταν δεν το χρησιμοποιείτε.
- Δυνατότητα εκτέλεσης σαρώσεων από ιούς σε εξωτερικές συσκευές αποθήκευσης.

Περιγραφή

Το Micro Credential "Device Security and Data Protection" είναι ένα εστιασμένο και πρακτικό πρόγραμμα που στοχεύει να εξοπλίσει τους εκπαιδευόμενους με βασικές δεξιότητες για να προστατεύουν τις συσκευές και τα δεδομένα τους από πιθανές απειλές ασφαλείας. Το πρόγραμμα αυτό, το οποίο έχει εγκριθεί από την αξιόλογη Ευρωπαϊκή Επιτροπή, ενδυναμώνει τους συμμετέχοντες με τις γνώσεις και τις ικανότητες να οχυρώνουν τις συσκευές τους έναντι ευπαθειών που σχετίζονται με το Bluetooth και να εκτελούν κρίσιμες σαρώσεις ιών σε εξωτερικές συσκευές αποθήκευσης.

Στην πρώτη ενότητα, οι εκπαιδευόμενοι διερευνούν τους κινδύνους που σχετίζονται με τη συνδεσιμότητα Bluetooth όταν αυτή παραμένει ενεργοποιημένη στις συσκευές τους, ειδικά όταν δεν χρησιμοποιούνται. Μέσω πραγματικών παραδειγμάτων και μελετών περίπτωσης, οι συμμετέχοντες αποκτούν έντονη επίγνωση των πιθανών τρωτών σημείων ασφαλείας που μπορεί να προκύψουν λόγω των συνδέσεων Bluetooth. Κατανοούν τη σημασία της απενεργοποίησης του Bluetooth όταν δεν χρησιμοποιείται ενεργά, μειώνοντας έτσι τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης ή παραβίασης δεδομένων.

Η δεύτερη ενότητα επικεντρώνεται στην κρίσιμη πρακτική της εκτέλεσης σαρώσεων από ιούς σε εξωτερικές συσκευές αποθήκευσης. Οι συμμετέχοντες αποκτούν γνώσεις σχετικά με τους πιθανούς κινδύνους που συνδέονται με τη χρήση εξωτερικών μέσων αποθήκευσης, όπως μονάδες USB ή εξωτερικοί σκληροί δίσκοι, και μαθαίνουν πώς οι ιοί και το κακόβουλο λογισμικό μπορούν να μεταφερθούν ακούσια στις συσκευές τους μέσω μολυσμένων συσκευών αποθήκευσης. Με την απόκτηση πρακτικών δεξιοτήτων για τη διενέργεια σαρώσεων ιών σε εξωτερικά μέσα αποθήκευσης, οι εκπαιδευόμενοι μπορούν να ανιχνεύουν και να μετριάζουν προληπτικά τις απειλές, διασφαλίζοντας ότι οι συσκευές και τα δεδομένα τους παραμένουν ασφαλή.

Καθ' όλη τη διάρκεια του Micro Credential, οι εκπαιδευόμενοι συμμετέχουν σε πρακτικές δραστηριότητες, προσομοιώσεις και πρακτικές ασκήσεις για να ενισχύσουν την κατανόηση της ασφάλειας συσκευών και της προστασίας δεδομένων. Αποκτούν αυτοπεποίθηση στην εφαρμογή των νεοαποκτηθέντων γνώσεών τους σε πραγματικά σενάρια, λαμβάνοντας τεκμηριωμένες αποφάσεις για την αποτελεσματική προστασία των συσκευών και των δεδομένων τους.

Με την επιτυχή ολοκλήρωση του Micro Credential "Device Security and Data Protection", οι συμμετέχοντες αποκτούν ισχυρές γνώσεις, επικυρώνοντας την επάρκειά τους στην ασφάλεια των συσκευών τους και την προστασία των δεδομένων τους. Οπλισμένοι με αυτές τις βασικές δεξιότητες, οι εκπαιδευόμενοι είναι καλά προετοιμασμένοι να περιηγηθούν στο ψηφιακό τοπίο με αυτοπεποίθηση, διασφαλίζοντας ότι οι συσκευές τους παραμένουν ασφαλείς και τα δεδομένα τους προστατεύονται από πιθανές απειλές.

Συνοπτικά, το Micro Credential "Device Security and Data Protection" είναι ένα μετασχηματιστικό πρόγραμμα που δίνει στους εκπαιδευόμενους πρακτικές γνώσεις και δεξιότητες στην ασφάλεια συσκευών και την προστασία δεδομένων. Οι συμμετέχοντες αναδεικνύονται σε προληπτικούς φύλακες των ψηφιακών συσκευών και δεδομένων τους, εξοπλισμένοι για να μετριάζουν τους κινδύνους ασφαλείας και να προωθούν ένα ασφαλέστερο ψηφιακό περιβάλλον για τους ίδιους και τους άλλους.

Ερωτήσεις

1. Ερώτηση με βάση σενάρια για την ασφάλεια Bluetooth: "Φανταστείτε ότι μόλις ολοκληρώσατε τη χρήση του Bluetooth για να συνδέσετε τη συσκευή σας με ένα ασύρματο ηχείο. Ποια μέτρα θα λαμβάνατε για να διασφαλίσετε την ασφάλεια της συσκευής σας μετά την αποσύνδεση από το ηχείο; Εξηγήστε τους πιθανούς κινδύνους που εγκυμονεί η παραμονή του Bluetooth ενεργοποιημένου όταν δεν χρησιμοποιείται και αναφέρετε τους λόγους για τους οποίους είναι απαραίτητο να απενεργοποιείτε το Bluetooth σε τέτοιες περιπτώσεις."
2. Πρακτική αξιολόγηση δεξιοτήτων για τη σάρωση ιών: "Λαμβάνετε μια μονάδα USB από έναν συνάδελφο που περιέχει σημαντικά έγγραφα για ένα επερχόμενο έργο. Πριν αποκτήσετε πρόσβαση στα αρχεία, εξηγήστε τα βήματα που θα ακολουθούσατε για να εκτελέσετε μια ενδελεχή σάρωση από ιούς στην εξωτερική συσκευή αποθήκευσης. Περιγράψτε τα εργαλεία και το λογισμικό που θα χρησιμοποιούσατε και τη σημασία της διενέργειας σάρωσης από ιούς για την προστασία της συσκευής και των δεδομένων σας."
3. Ερώτηση κριτικής σκέψης για την προστασία δεδομένων: "Σχεδιάζετε να μεταφέρετε ορισμένα αρχεία από τον υπολογιστή σας σε έναν εξωτερικό σκληρό δίσκο για σκοπούς δημιουργίας αντιγράφων ασφαλείας. Πώς θα διασφαλίζατε ότι η εξωτερική συσκευή αποθήκευσης είναι απαλλαγμένη από κακόβουλο λογισμικό ή ιούς που ενδέχεται να μολύνουν τον υπολογιστή σας κατά τη διαδικασία μεταφοράς; Συζητήστε τη σημασία της σάρωσης των εξωτερικών συσκευών αποθήκευσης από ιούς και πώς αυτή η πρακτική συμβάλλει στη συνολική προστασία των δεδομένων και την ασφάλεια της συσκευής."

Ολοκληρωμένη εκπαίδευση και εφαρμογή της ασφάλειας (MC 4.2.C.6)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	**Ολοκληρωμένη εκπαίδευση και εφαρμογή ασφάλειας** **Κωδ: C.6**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ADVANCED
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.53, 4.2.54 και 4.2.55):

- Κατανοήστε τη σημασία της εκπαίδευσης των εργαζομένων σε τεχνικές ασφάλειας ΤΠ.
- Ανάπτυξη ολοκληρωμένων μέτρων φυσικής ασφάλειας για την προστασία των περιουσιακών στοιχείων του οργανισμού.
- Να γνωρίζουν τη σημασία της έννοιας του ελέγχου ταυτότητας δύο παραγόντων (2FA) και το ρόλο του στην παροχή ενός επιπλέον επιπέδου προστασίας για τους διαδικτυακούς λογαριασμούς.

Περιγραφή

Το Micro Credential "Comprehensive Security Training and Implementation" είναι ένα ολοκληρωμένο και εξειδικευμένο πρόγραμμα που έχει σχεδιαστεί για να εξοπλίσει τους εκπαιδευόμενους με τις γνώσεις και τις δεξιότητες που απαιτούνται για να εξασφαλίσουν ισχυρές πρακτικές ασφάλειας στους οργανισμούς.

Το πρόγραμμα αυτό, το οποίο έχει εγκριθεί από την αξιόλογη Ευρωπαϊκή Επιτροπή, επικεντρώνεται σε τρεις βασικές πτυχές της ασφάλειας: την εκπαίδευση σε θέματα ασφάλειας ΤΠ, τα μέτρα φυσικής ασφάλειας και τον έλεγχο ταυτότητας δύο παραγόντων (2FA).

Στην πρώτη ενότητα, οι συμμετέχοντες εμβαθύνουν στον κρίσιμο τομέα της κατάρτισης για την ασφάλεια της πληροφορικής. Μαθαίνουν πώς να εκπαιδεύουν αποτελεσματικά τους υπαλλήλους σχετικά με τις βέλτιστες πρακτικές, τα πρωτόκολλα κυβερνοασφάλειας και την ευαισθητοποίηση σε θέματα απειλών. Με τη χρήση διαδραστικών μεθόδων μάθησης, μελετών περιπτώσεων και πραγματικών σεναρίων, οι εκπαιδευόμενοι αναπτύσσουν την τεχνογνωσία για να εκπαιδεύουν και να καθοδηγούν τους υπαλλήλους σχετικά με τη διαφύλαξη των δεδομένων, τον εντοπισμό πιθανών απειλών και την αντιμετώπιση περιστατικών ασφαλείας.

Η δεύτερη ενότητα δίνει έμφαση στη σημασία των ολοκληρωμένων μέτρων φυσικής ασφάλειας. Οι συμμετέχοντες αποκτούν γνώσεις σχετικά με την αξιολόγηση και την ανάπτυξη ισχυρών μέτρων ασφαλείας για την προστασία των οργανωτικών περιουσιακών στοιχείων, της υποδομής και των ευαίσθητων πληροφοριών. Μέσω πρακτικών ασκήσεων και αξιολογήσεων χώρων, οι εκπαιδευόμενοι διαμορφώνουν προσαρμοσμένα σχέδια ασφαλείας, που περιλαμβάνουν έλεγχο πρόσβασης, επιτήρηση και μέτρα έκτακτης ανάγκης για τον μετριασμό των κινδύνων φυσικής ασφάλειας.

Στην τρίτη ενότητα, οι συμμετέχοντες εμβαθύνουν στην έννοια του ελέγχου ταυτότητας δύο παραγόντων (2FA). Κατανοούν τα οφέλη του 2FA για την ενίσχυση της ασφάλειας των διαδικτυακών λογαριασμών με την προσθήκη ενός πρόσθετου επιπέδου προστασίας πέραν των παραδοσιακών κωδικών πρόσβασης. Μέσω διαδραστικών συζητήσεων και πρακτικών επιδείξεων, οι εκπαιδευόμενοι κατανοούν τις διάφορες μεθόδους 2FA, όπως οι κωδικοί μιας χρήσης (OTP) και ο βιομετρικός έλεγχος ταυτότητας, και μαθαίνουν πώς να εφαρμόζουν και να υποστηρίζουν αυτή τη βασική πρακτική ασφάλειας.

Καθ' όλη τη διάρκεια του Micro Credential, οι εκπαιδευόμενοι συμμετέχουν σε πρακτικά σενάρια, ασκήσεις ρόλων και έργα υλοποίησης για να εφαρμόσουν αποτελεσματικά τις γνώσεις τους. Το πρόγραμμα προάγει μια

προληπτική και συνειδητή νοοτροπία ασφάλειας, επιτρέποντας στους εκπαιδευόμενους να λαμβάνουν τεκμηριωμένες αποφάσεις και να προωθούν μια κουλτούρα ασφάλειας στους οργανισμούς τους.

Με την επιτυχή ολοκλήρωση του Micro Credential "Comprehensive Security Training and Implementation", οι συμμετέχοντες κερδίζουν μια υψηλού κύρους γνώση, επικυρώνοντας την τεχνογνωσία τους στην ενίσχυση της οργανωτικής ασφάλειας. Οπλισμένοι με αυτό το ολοκληρωμένο σύνολο δεξιοτήτων, οι εκπαιδευόμενοι είναι καλά εξοπλισμένοι για να αναλάβουν βασικούς ρόλους στην προώθηση πρωτοβουλιών ασφάλειας, τη διαφύλαξη ευαίσθητων δεδομένων και την προώθηση ενός ασφαλούς και ανθεκτικού οργανωτικού περιβάλλοντος.

Συνοψίζοντας, το Micro Credential "Comprehensive Security Training and Implementation" είναι ένα πρόγραμμα που δίνει στους εκπαιδευόμενους τη δυνατότητα να αντιμετωπίσουν προληπτικά τις προκλήσεις της ασφάλειας στους οργανισμούς. Οι συμμετέχοντες αναδεικνύονται σε ηγέτες στην εφαρμογή αποτελεσματικών μέτρων ασφαλείας, στην εκπαίδευση των εργαζομένων και στην υπεράσπιση των βέλτιστων πρακτικών ασφαλείας, συμβάλλοντας σε ένα ασφαλέστερο ψηφιακό τοπίο και ενισχύοντας την ανθεκτικότητα των οργανισμών έναντι των απειλών στον κυβερνοχώρο.

Ερωτήσεις

1. Εκπαιδευτική προσέγγιση Ερώτηση: "Ως εκπαιδευτής ασφάλειας πληροφορικής, περιγράψτε τα βήματα που θα ακολουθούσατε για να σχεδιάσετε ένα αποτελεσματικό πρόγραμμα εκπαίδευσης των εργαζομένων σε τεχνικές ασφάλειας πληροφορικής. Πώς θα προσαρμόζατε την εκπαίδευση στους διάφορους ρόλους και στα επίπεδα τεχνικής εξειδίκευσης εντός του οργανισμού;"
2. Ερώτηση σχεδιασμού φυσικής ασφάλειας: "Είστε επιφορτισμένοι με την ανάπτυξη ολοκληρωμένων μέτρων φυσικής ασφάλειας για τα νέα κεντρικά γραφεία της εταιρείας. Περιγράψτε τα βασικά βήματα που θα κάνατε για να αξιολογήσετε τους πιθανούς κινδύνους ασφαλείας, να εντοπίσετε τα περιουσιακά στοιχεία που απαιτούν προστασία και να σχεδιάσετε ένα σχέδιο ασφαλείας που περιλαμβάνει έλεγχο πρόσβασης, επιτήρηση και μέτρα έκτακτης ανάγκης."
3. 2FA Επεξήγηση και πλεονεκτήματα: "Εξηγήστε την έννοια του ελέγχου ταυτότητας δύο παραγόντων (2FA) σε κάποιον που δεν είναι εξοικειωμένος με τον όρο. Περιγράψτε τον τρόπο λειτουργίας του 2FA και τα συγκεκριμένα πλεονεκτήματα που παρέχει σε σύγκριση με τις μεθόδους ελέγχου ταυτότητας ενός παράγοντα, όπως οι παραδοσιακοί κωδικοί πρόσβασης."
4. Πραγματικό σενάριο για την εκπαίδευση σε θέματα ασφάλειας πληροφορικής: "Πραγματοποιείτε μια εκπαιδευτική συνεδρία για την ασφάλεια της πληροφορικής για τους υπαλλήλους ενός μεγάλου οργανισμού. Επιλέξτε ένα από τα ακόλουθα σενάρια: επιθέσεις phishing, ασφάλεια κωδικών πρόσβασης ή προστασία δεδομένων. Περιγράψτε πώς θα προσομοιώνατε μια πραγματική κατάσταση που σχετίζεται με το επιλεγμένο σενάριο για την αποτελεσματική εκπαίδευση και κατάρτιση των εργαζομένων."
5. Υλοποίηση της φυσικής ασφάλειας: "Μετά την αξιολόγηση των αναγκών φυσικής ασφάλειας μιας εταιρείας, σας έχει ανατεθεί η εφαρμογή των συνιστώμενων μέτρων ασφαλείας. Περιγράψτε τα βασικά βήματα που θα κάνατε για την εφαρμογή συστημάτων ελέγχου πρόσβασης, επιτήρησης και διαχείρισης επισκεπτών, εξασφαλίζοντας τη μέγιστη δυνατή προστασία των περιουσιακών στοιχείων του οργανισμού."
6. Εφαρμογή και συνηγορία 2FA: "(2FA) για τους διαδικτυακούς λογαριασμούς ενός οργανισμού. Περιγράψτε τα βήματα που θα ακολουθήσετε για την εφαρμογή του 2FA σε όλους τους υπαλλήλους και εξηγήστε πώς θα υποστηρίξετε την υιοθέτησή του για να διασφαλίσετε την ευρεία χρήση του."
7. Δέσμευση και συμμετοχή των εργαζομένων: "Ως εκπαιδευτής ασφάλειας, πώς θα διασφαλίζατε την ενεργό συμμετοχή και εμπλοκή των εργαζομένων κατά τη διάρκεια των εκπαιδευτικών συνεδριών για

την ασφάλεια της πληροφορικής;". Περιγράψτε τις στρατηγικές που θα χρησιμοποιούσατε για να ενθαρρύνετε τους εργαζόμενους να υιοθετήσουν τις βέλτιστες πρακτικές ασφάλειας στην καθημερινή τους εργασία".

8. Σύγκριση μεθόδων 2FA: "Συγκρίνετε και αντιπαραβάλλετε δύο διαφορετικές μεθόδους ελέγχου ταυτότητας δύο παραγόντων (π.χ. κωδικούς πρόσβασης μιας χρήσης και βιομετρικό έλεγχο ταυτότητας). Εξηγήστε τα πλεονεκτήματα και τις αδυναμίες κάθε μεθόδου και προσδιορίστε συγκεκριμένα σενάρια όπου η μία μέθοδος μπορεί να είναι πιο κατάλληλη από την άλλη."

Ενημέρωση για την ασφάλεια στον κυβερνοχώρο και προστασία συσκευών (MC 4.2.C.7)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ενημέρωση για την ασφάλεια στον κυβερνοχώρο και προστασία συσκευών Κωδ: C.7: MC 4.2.C.7
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ADVANCED
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%

Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.56, 4.2.57 και 4.2.58):

- Γνωρίζετε πώς να διαγνώσετε και να αντιμετωπίσετε προβλήματα ασφαλείας στις συσκευές σας, εντοπίζοντας πιθανό κακόβουλο λογισμικό ή απόπειρες μη εξουσιοδοτημένης πρόσβασης.
- Κατανοήστε τους πιθανούς κινδύνους της αποθήκευσης κωδικών πρόσβασης σε προγράμματα περιήγησης στο διαδίκτυο και τη σημασία της χρήσης ειδικών εργαλείων διαχείρισης κωδικών πρόσβασης.
- Αναπτύξτε ένα προσωπικό σχέδιο ευαισθητοποίησης σε θέματα κυβερνοασφάλειας, ώστε να ενημερώνεστε για τις τρέχουσες απειλές και να υιοθετείτε βέλτιστες πρακτικές για την προστασία των προσωπικών συσκευών και δεδομένων.

Περιγραφή

Το Micro Credential "Cybersecurity Awareness and Device Protection" είναι ένα ολοκληρωμένο και πρακτικό πρόγραμμα που έχει σχεδιαστεί για να ενδυναμώσει τους εκπαιδευόμενους με βασικές γνώσεις και δεξιότητες στον τομέα της κυβερνοασφάλειας.

Αυτό το πρόγραμμα επικεντρώνεται σε τρεις ζωτικές πτυχές της κυβερνοασφάλειας, ώστε να διασφαλιστεί η προστασία των προσωπικών συσκευών και δεδομένων.

Στην πρώτη ενότητα, οι συμμετέχοντες εισέρχονται στον πρακτικό κόσμο της διάγνωσης και της αντιμετώπισης προβλημάτων ασφαλείας στις συσκευές τους. Μέσω διαδραστικών προσομοιώσεων και πραγματικών σεναρίων, οι εκπαιδευόμενοι αποκτούν τεχνογνωσία στον εντοπισμό πιθανών μολύνσεων από κακόβουλο λογισμικό, στην ανίχνευση προσπαθειών μη εξουσιοδοτημένης πρόσβασης και στην εφαρμογή αποτελεσματικών στρατηγικών αποκατάστασης. Κατακτώντας αυτές τις δεξιότητες, οι συμμετέχοντες μπορούν να προστατεύουν προληπτικά τις συσκευές τους από απειλές ασφαλείας και να διατηρούν την ακεραιότητα των ψηφιακών περιουσιακών τους στοιχείων.

Η δεύτερη ενότητα εξετάζει τους πιθανούς κινδύνους που εγκυμονεί η αποθήκευση κωδικών πρόσβασης σε προγράμματα περιήγησης ιστού και τον καθοριστικό ρόλο των ειδικών εργαλείων διαχείρισης κωδικών πρόσβασης. Οι εκπαιδευόμενοι διερευνούν τα τρωτά σημεία που σχετίζονται με την αποθήκευση κωδικών πρόσβασης σε προγράμματα περιήγησης και τους αυξημένους κινδύνους μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητους λογαριασμούς. Οπλισμένοι με αυτές τις γνώσεις, οι συμμετέχοντες ανακαλύπτουν τη σημασία της χρήσης αξιόπιστων εργαλείων διαχείρισης κωδικών πρόσβασης για τη δημιουργία και την ασφαλή αποθήκευση σύνθετων, μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό. Οι πρακτικές δραστηριότητες

επιτρέπουν στους εκπαιδευόμενους να εφαρμόσουν ισχυρές πρακτικές διαχείρισης κωδικών πρόσβασης για την ενίσχυση της διαδικτυακής τους ασφάλειας.

Στην τελευταία ενότητα, οι συμμετέχοντες αναπτύσσουν ένα εξατομικευμένο σχέδιο ευαισθητοποίησης για την κυβερνοασφάλεια, ώστε να ενημερώνονται για τις τρέχουσες απειλές και να υιοθετούν βέλτιστες πρακτικές για την προστασία των συσκευών και των δεδομένων. Μαθαίνουν πώς να έχουν πρόσβαση σε αξιόπιστους πόρους κυβερνοασφάλειας, να παρακολουθούν τις ενημερώσεις του κλάδου και να παραμένουν σε εγρήγορση απέναντι στις αναδυόμενες απειλές στον κυβερνοχώρο. Καλλιεργώντας μια προληπτική νοοτροπία και εφαρμόζοντας βέλτιστες πρακτικές ασφάλειας, οι συμμετέχοντες δημιουργούν μια ισχυρή άμυνα απέναντι σε πιθανές επιθέσεις στον κυβερνοχώρο και παραβιάσεις δεδομένων.

Καθ' όλη τη διάρκεια του Micro Credential, οι εκπαιδευόμενοι συμμετέχουν σε διαδραστικές αξιολογήσεις, πρακτικές ασκήσεις και εξατομικευμένα σχέδια δράσης για να εφαρμόσουν τις νεοαποκτηθείσες γνώσεις τους. Το πρόγραμμα δίνει έμφαση στην κριτική σκέψη, την επίλυση προβλημάτων και την υιοθέτηση προληπτικών μέτρων ασφαλείας για την προστασία των προσωπικών συσκευών και δεδομένων στο σημερινό δυναμικό ψηφιακό τοπίο.

Με την επιτυχή ολοκλήρωση του Micro Credential "Cybersecurity Awareness and Device Protection", οι συμμετέχοντες λαμβάνουν την πιστοποίηση του MC. Η αναγνώριση αυτή επικυρώνει την ικανότητά τους στη διάγνωση προβλημάτων ασφαλείας, τη χρήση τεχνικών ασφαλούς διαχείρισης κωδικών πρόσβασης και την ανάπτυξη ενός προληπτικού σχεδίου ευαισθητοποίησης στον κυβερνοχώρο.

Εν κατακλείδι, το Micro Credential "Cybersecurity Awareness and Device Protection" παρέχει στους εκπαιδευόμενους βασικές δεξιότητες και γνώσεις κυβερνοασφάλειας για την προστασία της ψηφιακής τους ζωής. Οι συμμετέχοντες αναδεικνύονται σε προληπτικούς υπερασπιστές των απειλών στον κυβερνοχώρο, εξοπλισμένοι για την προστασία των προσωπικών συσκευών και δεδομένων και συμβάλλουν στην οικοδόμηση ενός ασφαλέστερου ψηφιακού οικοσυστήματος για τους ίδιους και τις κοινότητές τους.

Ερωτήσεις

1. Παρατηρείτε ότι ο υπολογιστής σας λειτουργεί πιο αργά από το συνηθισμένο και ότι λαμβάνετε συχνά αναδυόμενες διαφημίσεις κατά την περιήγησή σας στο διαδίκτυο. Ποιο πρόβλημα ασφαλείας θα μπορούσατε να υποψιαστείτε και ποια βήματα θα ακολουθούσατε για την αντιμετώπιση και επίλυση αυτού του προβλήματος;
2. Εξηγήστε τους πιθανούς κινδύνους που εγκυμονεί η αποθήκευση κωδικών πρόσβασης σε προγράμματα περιήγησης στο διαδίκτυο και πώς μπορεί να θέσει σε κίνδυνο την ηλεκτρονική σας ασφάλεια. Ποια είναι τα πλεονεκτήματα της χρήσης ειδικών εργαλείων διαχείρισης κωδικών πρόσβασης και πώς ενισχύουν την ασφάλεια των κωδικών πρόσβασης;
3. Φανταστείτε ότι λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχεται από την τράπεζά σας και σας ζητά να κάνετε κλικ σε έναν σύνδεσμο για να ενημερώσετε επειγόντως τα στοιχεία του λογαριασμού σας. Τι πρέπει να κάνετε για να επαληθεύσετε τη νομιμότητα του email και να προστατευτείτε από το να πέσετε θύμα απάτης phishing;
4. Αναπτύξτε ένα σχέδιο ευαισθητοποίησης στον κυβερνοχώρο, στο οποίο περιγράφονται τα βήματα που θα ακολουθήσετε για να ενημερώνεστε σχετικά με τις τρέχουσες απειλές και τις βέλτιστες πρακτικές για την προστασία των προσωπικών σας συσκευών και δεδομένων. Περιλάβετε συγκεκριμένες

ενέργειες στις οποίες θα προβείτε, όπως η εγγραφή σε πηγές ειδήσεων για την κυβερνοασφάλεια, η ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων και η τακτική ενημέρωση του λογισμικού της συσκευής σας.

Προηγμένες πρακτικές ασφάλειας για προσωπικές συσκευές και συστήματα (MC 4.2.C.8)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Προηγμένες πρακτικές ασφάλειας για προσωπικές συσκευές και συστήματα Κωδ: C.8: MC 4.2.C.8
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	ADVANCED
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%

Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.59, 4.2.60):

- Υιοθετήστε αξιόπιστο λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό στις προσωπικές συσκευές για τον εντοπισμό και την απομάκρυνση πιθανών απειλών.
- Εφαρμόστε ελέγχους πρόσβασης για τη ρύθμιση και τον περιορισμό της εισόδου σε συστήματα, λογαριασμούς ή προσωπικά προφίλ, εξασφαλίζοντας καλύτερη ασφάλεια και προστασία της ιδιωτικής ζωής.

Περιγραφή

Το Micro Credential "Advanced Security Practices for Personal Devices and Systems" είναι ένα εξειδικευμένο πρόγραμμα που έχει επιμεληθεί για να παρέχει σε άτομα προηγμένες τεχνικές ασφαλείας για την προστασία των προσωπικών τους συσκευών και των ψηφιακών τους προφίλ. Αυτό το ολοκληρωμένο μάθημα επικεντρώνεται σε δύο βασικές ικανότητες που είναι κρίσιμες για την ενίσχυση της ψηφιακής ασφάλειας και της ιδιωτικής ζωής.

Η πρώτη ενότητα είναι αφιερωμένη στην ενδυνάμωση των συμμετεχόντων με τις γνώσεις και τις δεξιότητες για την υιοθέτηση αξιόπιστου λογισμικού προστασίας από ιούς και κακόβουλο λογισμικό στις προσωπικές τους συσκευές. Εξερευνώντας τις βέλτιστες πρακτικές για την επιλογή και εγκατάσταση αποτελεσματικών λύσεων ασφαλείας, οι εκπαιδευόμενοι αποκτούν γνώσεις σχετικά με τον εντοπισμό και την απομάκρυνση πιθανών απειλών που μπορούν να θέσουν σε κίνδυνο την ακεραιότητα των συσκευών τους. Τα σενάρια πραγματικού κόσμου και οι πρακτικές προσομοιώσεις επιτρέπουν στους συμμετέχοντες να εφαρμόσουν την τεχνογνωσία τους στον εντοπισμό και τον μετριασμό διαφόρων τύπων κακόβουλου λογισμικού, συμπεριλαμβανομένων ιών, trojans και spyware. Κατακτώντας τη χρήση αυτών των βασικών εργαλείων, οι εκπαιδευόμενοι δημιουργούν μια ισχυρή άμυνα απέναντι στις ψηφιακές απειλές και ενισχύουν τη συνολική τους θέση στην κυβερνοασφάλεια.

Στη δεύτερη ενότητα, οι συμμετέχοντες εμβαθύνουν στη σφαίρα των ελέγχων πρόσβασης και τη σημασία τους στη ρύθμιση της εισόδου σε συστήματα, λογαριασμούς και προσωπικά προφίλ.
Οι εκπαιδευόμενοι θα εξερευνήσουν διάφορες μεθόδους ελέγχου πρόσβασης, όπως κωδικούς πρόσβασης, έλεγχο ταυτότητας πολλαπλών παραγόντων και έλεγχο πρόσβασης βάσει ρόλων (RBAC). Πρακτικές ασκήσεις καθοδηγούν τους συμμετέχοντες στη διαμόρφωση ελέγχων πρόσβασης για διάφορα σενάρια, επιτρέποντάς τους να διασφαλίσουν αποτελεσματικά τα δεδομένα, τις εφαρμογές και τις διαδικτυακές ταυτότητές τους.

Επιπλέον, η ενότητα τονίζει τη σημασία της διατήρησης ισχυρών και μοναδικών κωδικών πρόσβασης για την ενίσχυση των μηχανισμών ελέγχου πρόσβασης, μειώνοντας τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης και πιθανών παραβιάσεων δεδομένων.

Καθ' όλη τη διάρκεια του Micro Credential, οι εκπαιδευόμενοι θα αξιολογούνται μέσω διαδραστικών μαθημάτων, πρακτικών εργασιών και προσομοιώσεων που αντικατοπτρίζουν πραγματικές προκλήσεις ασφαλείας. Οι συμμετέχοντες θα αναπτύξουν βαθιά κατανόηση των προηγμένων πρακτικών ασφάλειας, επιτρέποντάς τους να προστατεύουν προληπτικά τις προσωπικές τους συσκευές και τα ψηφιακά τους περιουσιακά στοιχεία από τις αναδυόμενες απειλές.

Με την επιτυχή ολοκλήρωση του Micro Credential "Advanced Security Practices for Personal Devices and Systems", οι συμμετέχοντες θα λάβουν την αναγνώριση που επικυρώνει την επάρκειά τους στην υιοθέτηση και εφαρμογή προηγμένων μέτρων ασφαλείας, ενισχύοντας την αξιοπιστία τους στο τοπίο της ψηφιακής ασφάλειας.

Συμπερασματικά, το Micro Credential "Advanced Security Practices for Personal Devices and Systems" εφοδιάζει τους εκπαιδευόμενους με την τεχνογνωσία που απαιτείται για την αποτελεσματική προστασία της ψηφιακής τους ζωής. Οπλισμένοι με μια βαθύτερη κατανόηση του αξιόπιστου λογισμικού ασφαλείας, των προηγμένων ελέγχων πρόσβασης και των πρακτικών ασφαλούς κωδικού πρόσβασης, οι συμμετέχοντες αναδεικνύονται σε έμπειρους φύλακες των προσωπικών τους συσκευών και συστημάτων, προωθώντας ένα ασφαλέστερο ψηφιακό οικοσύστημα για τους ίδιους και την κοινωνία στο σύνολό της.

Ερωτήσεις

1. Γιατί είναι σημαντικό να υιοθετήσετε αξιόπιστο λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό σε προσωπικές συσκευές; Δώστε παραδείγματα πιθανών απειλών που αυτές οι λύσεις λογισμικού μπορούν να βοηθήσουν στον εντοπισμό και την απομάκρυνση.
2. Εξηγήστε την έννοια των ελέγχων πρόσβασης και τον ρόλο τους στην εξασφάλιση καλύτερης ασφάλειας και προστασίας της ιδιωτικής ζωής για συστήματα, λογαριασμούς ή προσωπικά προφίλ. Να δώσετε συγκεκριμένα παραδείγματα μεθόδων ελέγχου πρόσβασης και σεναρίων όπου μπορούν να εφαρμοστούν αποτελεσματικά.
3. Φανταστείτε ότι μόλις αγοράσατε μια νέα προσωπική συσκευή. Περιγράψτε τα βήματα που θα ακολουθούσατε για να ερευνήσετε, να επιλέξετε και να εγκαταστήσετε αξιόπιστο λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό στη συσκευή σας.
4. Είστε υπεύθυνοι για την ασφάλεια μιας διαδικτυακής εφαρμογής που χρησιμοποιείται από τους υπαλλήλους του οργανισμού σας. Περιγράψτε πώς θα εφαρμόζατε ελέγχους πρόσβασης για τη ρύθμιση και τον περιορισμό της εισόδου στα διάφορα χαρακτηριστικά και τις λειτουργίες της εφαρμογής. Συμπεριλάβετε τις συγκεκριμένες μεθόδους ελέγχου πρόσβασης που θα χρησιμοποιούσατε και το σκεπτικό των επιλογών σας.

DSW
DIGITAL SKILLS WALLET

Co-funded by
the European Union

Διαχείριση κινδύνων κυβερνοασφάλειας και ευαισθητοποίηση του προσωπικού (MC 4.2.D.1)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Διαχείριση κινδύνων κυβερνοασφάλειας και **ευαισθητοποίηση του** προσωπικού **Κωδ: D.1: MC 4.2.D.1**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	EXPERT
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.61, 4.2.62 και 4.2.63):

- Κατανοήστε τη σημασία της διεξαγωγής ετήσιας εκπαίδευσης ευαισθητοποίησης του προσωπικού σε θέματα κυβερνοασφάλειας.
- Αναλύστε και κατηγοριοποιήστε τους πιθανούς κινδύνους κυβερνοασφάλειας με βάση τον αντίκτυπο και την πιθανότητα εμφάνισής τους.
- Να επανεξετάζετε και να επικαιροποιείτε τακτικά τις πολιτικές και τις διαδικασίες που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.

Περιγραφή

Το Micro Credential "Cybersecurity Risk Management and Staff Awareness" είναι ένα ολοκληρωμένο πρόγραμμα που έχει σχεδιαστεί για να εξοπλίσει τα άτομα με την τεχνογνωσία για την αποτελεσματική διαχείριση των κινδύνων κυβερνοασφάλειας στους οργανισμούς τους. Αυτό το εξειδικευμένο μάθημα επικεντρώνεται σε τρεις βασικές ικανότητες που είναι θεμελιώδεις για τη διασφάλιση ισχυρών πρακτικών κυβερνοασφάλειας και την προώθηση μιας κουλτούρας ευαισθητοποίησης του προσωπικού σε θέματα ασφάλειας.

Η πρώτη ενότητα υπογραμμίζει τη σημασία της διεξαγωγής ετήσιας εκπαίδευσης ευαισθητοποίησης του προσωπικού σε θέματα ασφάλειας στον κυβερνοχώρο. Οι συμμετέχοντες θα μάθουν πώς οι εκπαιδευμένοι και σε εγρήγορση εργαζόμενοι διαδραματίζουν καθοριστικό ρόλο στη διαφύλαξη των περιουσιακών στοιχείων και των δεδομένων του οργανισμού από απειλές στον κυβερνοχώρο. Με την κατανόηση των κοινών κινδύνων κυβερνοασφάλειας και των βέλτιστων πρακτικών, οι εκπαιδευόμενοι μπορούν να προσαρμόσουν αποτελεσματικά εκπαιδευτικά προγράμματα για την αντιμετώπιση των συγκεκριμένων αναγκών του οργανισμού τους. Πρακτικά παραδείγματα και μελέτες περίπτωσης θα αναδείξουν τον αντίκτυπο του καλά ενημερωμένου προσωπικού στον μετριασμό των κινδύνων και στην προώθηση μιας ανθεκτικής στάσης κυβερνοασφάλειας.

Στη δεύτερη ενότητα, οι συμμετέχοντες θα εντρυφήσουν στον κόσμο της ανάλυσης και κατηγοριοποίησης των κινδύνων κυβερνοασφάλειας. Οι εκπαιδευόμενοι θα αποκτήσουν πολύτιμες γνώσεις για την αξιολόγηση πιθανών απειλών με βάση τον αντίκτυπο και την πιθανότητα εμφάνισής τους. Μέσω μεθοδολογιών και πλαισίων αξιολόγησης κινδύνων, οι συμμετέχοντες θα μάθουν να ιεραρχούν και να κατανέμουν αποτελεσματικά τους πόρους για την αντιμετώπιση των πιο κρίσιμων κινδύνων κυβερνοασφάλειας. Οι πρακτικές ασκήσεις θα δώσουν στους εκπαιδευόμενους την ικανότητα να εκτελούν αξιολογήσεις κινδύνου, επιτρέποντάς τους να εντοπίζουν τρωτά σημεία, να εφαρμόζουν αντίμετρα και να βελτιστοποιούν τις στρατηγικές κυβερνοασφάλειας.

Η τρίτη ενότητα επικεντρώνεται στη σημασία της τακτικής αναθεώρησης και επικαιροποίησης των πολιτικών και διαδικασιών κυβερνοασφάλειας. Οι συμμετέχοντες θα διερευνήσουν τις βέλτιστες πρακτικές για τη δημιουργία και τη διατήρηση ολοκληρωμένων πολιτικών κυβερνοασφάλειας που ευθυγραμμίζονται με τους στόχους του οργανισμού και τις απαιτήσεις συμμόρφωσης. Θα μάθουν πώς να προσαρμόζουν τις πολιτικές και τις διαδικασίες ώστε να αντιμετωπίζουν τις αναδυόμενες απειλές στον κυβερνοχώρο και τις αλλαγές στο

τεχνολογικό τοπίο. Πρακτικές μελέτες περιπτώσεων και ομαδικές συζητήσεις θα επιτρέψουν στους εκπαιδευόμενους να εντοπίσουν τομείς προς βελτίωση και να εφαρμόσουν τις απαραίτητες ενημερώσεις για την ενίσχυση της άμυνας του οργανισμού τους στον κυβερνοχώρο.

Καθ' όλη τη διάρκεια του Micro Credential, οι εκπαιδευόμενοι θα αξιολογούνται μέσω ενός συνδυασμού κουίζ, μελετών περιπτώσεων και πρακτικών εργασιών που αξιολογούν την ικανότητά τους να εφαρμόζουν τις γνώσεις που απέκτησαν σε πραγματικά σενάρια. Οι συμμετέχοντες θα αναδειχθούν με βαθύτερη κατανόηση της διαχείρισης των κινδύνων κυβερνοασφάλειας και του ρόλου της εκπαίδευσης ευαισθητοποίησης του προσωπικού στην προώθηση ενός ασφαλούς οργανωτικού περιβάλλοντος.

Με την επιτυχή ολοκλήρωση του Micro Credential "Cybersecurity Risk Management and Staff Awareness", οι συμμετέχοντες θα αποκτήσουν μια ισχυρή κατανόηση στη διαχείριση των κινδύνων κυβερνοασφάλειας και την προώθηση μιας κουλτούρας ευαισθητοποίησης του προσωπικού σε θέματα ασφάλειας, συμβάλλοντας στην ενίσχυση των πρακτικών κυβερνοασφάλειας σε διάφορους οργανισμούς.

Συνοπτικά, το Micro Credential "Διαχείριση κινδύνων στον κυβερνοχώρο και ευαισθητοποίηση του προσωπικού" παρέχει στους εκπαιδευόμενους τις γνώσεις και τις δεξιότητες για την αποτελεσματική ανάλυση των κινδύνων στον κυβερνοχώρο, τον σχεδιασμό στοχευμένων εκπαιδευτικών προγραμμάτων ευαισθητοποίησης του προσωπικού και τη διατήρηση επικαιροποιημένων πολιτικών και διαδικασιών κυβερνοασφάλειας. Ενισχύοντας τα άτομα να λαμβάνουν προληπτικά μέτρα κατά των απειλών στον κυβερνοχώρο, αυτό το Micro Credential διαδραματίζει κρίσιμο ρόλο στην ενίσχυση της ψηφιακής ανθεκτικότητας των οργανισμών σε διάφορους κλάδους.

Ερωτήσεις

1. Γιατί η διεξαγωγή ετήσιας εκπαίδευσης ευαισθητοποίησης του προσωπικού σε θέματα κυβερνοασφάλειας είναι απαραίτητη για τους οργανισμούς; Δώστε συγκεκριμένα παραδείγματα για το πώς οι καλά ενημερωμένοι εργαζόμενοι μπορούν να συμβάλουν σε καλύτερες πρακτικές κυβερνοασφάλειας.
2. Περιγράψτε τη διαδικασία ανάλυσης και κατηγοριοποίησης των πιθανών κινδύνων κυβερνοασφάλειας με βάση τον αντίκτυπο και την πιθανότητα εμφάνισής τους. Πώς αυτή η αξιολόγηση κινδύνων βοηθά στην ιεράρχηση των μέτρων ασφαλείας και στην κατανομή των πόρων;
3. Γιατί είναι ζωτικής σημασίας για τους οργανισμούς να αναθεωρούν και να επικαιροποιούν τακτικά τις πολιτικές και τις διαδικασίες που σχετίζονται με την ασφάλεια στον κυβερνοχώρο; Πώς μπορούν οι ξεπερασμένες πολιτικές να θέσουν σε κίνδυνο τη θέση ασφαλείας του οργανισμού;
4. Είστε επαγγελματίας ασφάλειας πληροφορικής και σας έχει ανατεθεί η διεξαγωγή εκπαίδευσης ευαισθητοποίησης του προσωπικού σε θέματα κυβερνοασφάλειας για μια εταιρεία. Περιγράψτε τα βασικά θέματα και τις βέλτιστες πρακτικές που θα συμπεριλάβατε στο εκπαιδευτικό πρόγραμμα, λαμβάνοντας υπόψη τον κλάδο της εταιρείας και τις συγκεκριμένες προκλήσεις ασφαλείας.
5. Φανταστείτε ότι είστε αναλυτής κινδύνων κυβερνοασφάλειας για ένα χρηματοπιστωτικό ίδρυμα. Αναλύστε ένα υποθετικό σενάριο κινδύνου κυβερνοασφάλειας, κατηγοριοποιώντας τους κινδύνους με βάση τον αντίκτυπο και την πιθανότητα εμφάνισής τους. Παρέχετε συστάσεις για τον μετριασμό των εντοπισμένων κινδύνων και εξηγήστε γιατί τα μέτρα αυτά είναι απαραίτητα για τη στρατηγική ασφάλειας του οργανισμού.

Κυβερνοασφάλεια με επίκεντρο τα δεδομένα και διαχείριση πλεοναζόντων δεδομένων (MC 4.2.D.2)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Κυβερνοασφάλεια με επίκεντρο τα δεδομένα και διαχείριση πλεοναζόντων δεδομένων **Κωδ: Δ.2.Δ.2**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	EXPERT
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.64, 4.2.65):

- Δώστε έμφαση σε μέτρα ασφάλειας επικεντρωμένα στα δεδομένα αντί να βασίζεστε αποκλειστικά σε περιμετρικές άμυνες.
- Επίδειξη γνώσεων και δεξιοτήτων για τον εντοπισμό και την αφαίρεση περιττών δεδομένων για την ενίσχυση της ασφάλειας στον κυβερνοχώρο.

Περιγραφή

Το Micro Credential "Data-Centric Cybersecurity and Redundant Data Management" είναι ένα πρόγραμμα αιχμής που έχει σχεδιαστεί για να εξοπλίσει τους συμμετέχοντες με προηγμένες τεχνικές κυβερνοασφάλειας που επικεντρώνονται στην προστασία των δεδομένων, το πιο κρίσιμο περιουσιακό στοιχείο για κάθε οργανισμό. Αυτό το ολοκληρωμένο μάθημα επικεντρώνεται σε δύο βασικές ικανότητες που αντιμετωπίζουν τις σύγχρονες προκλήσεις της κυβερνοασφάλειας.

Στο σημερινό δυναμικό τοπίο των απειλών, οι παραδοσιακές περιμετρικές άμυνες από μόνες τους δεν αρκούν πλέον για να προστατεύσουν τα ευαίσθητα δεδομένα από εξελιγμένες απειλές στον κυβερνοχώρο. Η πρώτη ενότητα αυτού του Micro Credential δίνει έμφαση στη μετατόπιση του παραδείγματος προς τα μέτρα ασφαλείας που επικεντρώνονται στα δεδομένα. Οι συμμετέχοντες θα αποκτήσουν βαθιά κατανόηση των αρχών της ασφάλειας με επίκεντρο τα δεδομένα, εξερευνώντας την κρυπτογράφηση, την κωδικοποίηση, τους ελέγχους πρόσβασης και τις τεχνικές απόκρυψης δεδομένων. Μελέτες περιπτώσεων από τον πραγματικό κόσμο και βέλτιστες πρακτικές θα καταδείξουν πώς η ασφάλεια με επίκεντρο τα δεδομένα ενισχύει την προστασία των ευαίσθητων πληροφοριών και θωρακίζει τους οργανισμούς έναντι παραβιάσεων δεδομένων και κυβερνοεπιθέσεων.

Η δεύτερη ενότητα είναι αφιερωμένη στη διαχείριση πλεοναζόντων δεδομένων, μια κρίσιμη πτυχή της ασφάλειας στον κυβερνοχώρο που συχνά παραβλέπεται. Οι συμμετέχοντες θα μάθουν τη σημασία του εντοπισμού και της αφαίρεσης των περιττών δεδομένων για την ελαχιστοποίηση της επιφάνειας επίθεσης και τη βελτίωση της ακεραιότητας των δεδομένων. Μέσω πρακτικών ασκήσεων, οι εκπαιδευόμενοι θα αναπτύξουν τις δεξιότητες για τη διενέργεια ελέγχων δεδομένων, τον εντοπισμό και την εξάλειψη περιττών δεδομένων και τον εξορθολογισμό των συστημάτων αποθήκευσης δεδομένων. Αυτή η προληπτική προσέγγιση όχι μόνο ενισχύει την ασφάλεια στον κυβερνοχώρο, αλλά προωθεί επίσης την αποδοτικότητα των δεδομένων, μειώνοντας το κόστος αποθήκευσης και βελτιώνοντας τις πρακτικές διαχείρισης δεδομένων.

Καθ' όλη τη διάρκεια του Micro Credential, οι συμμετέχοντες θα αξιολογούνται με συνδυασμό πρακτικών εργασιών, ασκήσεων ελέγχου δεδομένων και αξιολογήσεων βάσει σεναρίων. Θα έχουν την ευκαιρία να εφαρμόσουν τις γνώσεις τους σε προσομοιωμένα περιστατικά κυβερνοασφάλειας, αποδεικνύοντας την ικανότητά τους στην εφαρμογή μέτρων ασφάλειας με επίκεντρο τα δεδομένα και τη διαχείριση πλεοναζόντων δεδομένων.

Με την επιτυχή ολοκλήρωση του Micro Credential "Data-Centric Cybersecurity and Redundant Data Management", οι συμμετέχοντες θα λάβουν επίσημη έγκριση από την Ευρωπαϊκή Επιτροπή. Αυτή η υψηλού κύρους αναγνώριση επικυρώνει την εξειδίκευσή τους στη διαφύλαξη των δεδομένων μέσω μέτρων ασφάλειας

με επίκεντρο τα δεδομένα και την εφαρμογή αποτελεσματικών στρατηγικών διαχείρισης πλεοναζόντων δεδομένων.

Συνοπτικά, το Micro Credential "Data-Centric Cybersecurity and Redundant Data Management" παρέχει στους συμμετέχοντες τις πιο πρόσφατες γνώσεις και δεξιότητες στον τομέα της ασφάλειας στον κυβερνοχώρο και της διαχείρισης πλεοναζόντων δεδομένων. Θέτοντας ως προτεραιότητα την προστασία των δεδομένων και τον εξορθολογισμό των πρακτικών αποθήκευσης δεδομένων, το πρόγραμμα αυτό διαδραματίζει καθοριστικό ρόλο στην ενίσχυση της ανθεκτικότητας της κυβερνοασφάλειας και στην προώθηση της αποδοτικότητας των δεδομένων σε οργανισμούς διαφόρων τομέων. Οι συμμετέχοντες θα είναι καλά εξοπλισμένοι για να περιηγηθούν στο εξελισσόμενο τοπίο της κυβερνοασφάλειας και θα γίνουν πολύτιμα περιουσιακά στοιχεία για τη διαφύλαξη ευαίσθητων δεδομένων από τις συνεχώς εξελισσόμενες απειλές στον κυβερνοχώρο.

Ερωτήσεις

1. Εξηγήστε την έννοια της ασφάλειας με επίκεντρο τα δεδομένα και πώς διαφέρει από τη στήριξη αποκλειστικά σε περιμετρικές άμυνες. Δώστε συγκεκριμένα παραδείγματα μέτρων ασφάλειας επικεντρωμένων στα δεδομένα που μπορούν να προστατεύσουν αποτελεσματικά τις ευαίσθητες πληροφορίες ακόμη και όταν δεν υπάρχουν ισχυρές περιμετρικές άμυνες.
2. Είστε επαγγελματίας ασφάλειας πληροφορικής, υπεύθυνος για την ενίσχυση της ασφάλειας στον κυβερνοχώρο στον οργανισμό σας. Περιγράψτε τα βήματα που θα λαμβάνατε για τον εντοπισμό και την αφαίρεση των περιττών δεδομένων από τα συστήματα αποθήκευσης δεδομένων του οργανισμού. Πώς συμβάλλει αυτή η πρακτική στη βελτίωση της ανθεκτικότητας της κυβερνοασφάλειας και της ακεραιότητας των δεδομένων;
3. Σε ένα υποθετικό σενάριο, μια εταιρεία υπέστη παραβίαση δεδομένων παρά την ύπαρξη ισχυρής περιμετρικής άμυνας. Πώς θα μπορούσαν τα μέτρα ασφάλειας με επίκεντρο τα δεδομένα να έχουν ενδεχομένως μετριάσει ή ελαχιστοποιήσει τον αντίκτυπο της παραβίασης; Δώστε πληροφορίες σχετικά με τις βασικές στρατηγικές ασφάλειας με επίκεντρο τα δεδομένα που θα μπορούσαν να είχαν κάνει τη διαφορά στην πρόληψη ή την αντιμετώπιση του περιστατικού.

Ανάπτυξη ηγεσίας και κουλτούρας στον τομέα της κυβερνοασφάλειας (MC 4.2.D.3)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ανάπτυξη ηγεσίας και κουλτούρας στον τομέα της κυβερνοασφάλειας **Κωδ: D.3**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	EXPERT
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.66, 4.2.67):

- Υποστήριξη για αυξημένες επενδύσεις στην κυβερνοασφάλεια και αποτελεσματική κατανομή των πόρων
- Να γνωρίζουν τη σημασία της προώθησης μιας νοοτροπίας ασφάλειας σε ολόκληρη την εταιρεία και της προώθησης μιας κουλτούρας ευαισθητοποίησης σε θέματα κυβερνοασφάλειας.

Περιγραφή

Το Micro Credential "Cybersecurity Leadership and Culture Development" είναι ένα ολοκληρωμένο πρόγραμμα που ενδυναμώνει τους συμμετέχοντες να υπερασπίζονται την κυβερνοασφάλεια εντός των οργανισμών, να προωθούν μια κουλτούρα με συνείδηση της ασφάλειας και να προωθούν την αποτελεσματική κατανομή των πόρων για αυξημένη ανθεκτικότητα στον κυβερνοχώρο. Αυτό το μετασχηματιστικό πρόγραμμα που αναπτύχθηκε σε συνεργασία με την Ευρωπαϊκή Επιτροπή, εξοπλίζει τους συμμετέχοντες με τις βασικές γνώσεις και δεξιότητες για να γίνουν προληπτικοί ηγέτες στον τομέα της κυβερνοασφάλειας.

Στο ραγδαία εξελισσόμενο ψηφιακό τοπίο, η κυβερνοασφάλεια έχει καταστεί στρατηγική επιταγή για τους οργανισμούς όλων των μεγεθών και τομέων. Η πρώτη ενότητα αυτού του Micro Credential εμβαθύνει στη σημασία των αυξημένων επενδύσεων στην κυβερνοασφάλεια.
Οι συμμετέχοντες θα αποκτήσουν γνώσεις σχετικά με τις αναδυόμενες απειλές στον κυβερνοχώρο, τις πιθανές συνέπειες των επιθέσεων στον κυβερνοχώρο και την αυξανόμενη σημασία της διάθεσης επαρκών πόρων για την ενίσχυση της άμυνας στον κυβερνοχώρο. Μέσα από μελέτες περιπτώσεων και συζητήσεις υπό την καθοδήγηση ειδικών, οι εκπαιδευόμενοι θα διερευνήσουν τις βέλτιστες πρακτικές για τη διεξαγωγή αναλύσεων κόστους-οφέλους για την αιτιολόγηση των επενδύσεων στην κυβερνοασφάλεια και την ευθυγράμμιση των στρατηγικών ασφάλειας με τους οργανωτικούς στόχους.

Η δεύτερη ενότητα επικεντρώνεται στην καλλιέργεια μιας νοοτροπίας ασφάλειας σε ολόκληρη την εταιρεία και στην καλλιέργεια μιας κουλτούρας ευαισθητοποίησης σε θέματα κυβερνοασφάλειας. Οι συμμετέχοντες θα εμβαθύνουν στην ψυχολογία της ανθρώπινης συμπεριφοράς και στον αντίκτυπό της στην ασφάλεια στον κυβερνοχώρο. Οπλισμένοι με αυτή την κατανόηση, οι εκπαιδευόμενοι θα αναπτύξουν στρατηγικές για να εμπλέξουν και να εκπαιδεύσουν τους εργαζόμενους σε όλα τα επίπεδα, ώστε να γίνουν ενεργοί συμμετέχοντες στην προστασία των ψηφιακών περιουσιακών στοιχείων. Η ενότητα θα ασχοληθεί με αποτελεσματικές τεχνικές επικοινωνίας, ελκυστικές μεθόδους κατάρτισης και την καθιέρωση ισχυρών πολιτικών και κατευθυντήριων γραμμών για την κυβερνοασφάλεια.
Οι συμμετέχοντες θα αποκτήσουν τα απαραίτητα εφόδια για την εφαρμογή προγραμμάτων ευαισθητοποίησης σε θέματα ασφάλειας που θα ενσταλάξουν μια προληπτική κουλτούρα ασφάλειας και θα δώσουν στους υπαλλήλους τη δυνατότητα να αναγνωρίζουν και να ανταποκρίνονται αποτελεσματικά στις απειλές στον κυβερνοχώρο.

Κατά τη διάρκεια του Micro Credential, οι συμμετέχοντες θα συμμετάσχουν σε διαδραστικά εργαστήρια,

ασκήσεις ρόλων και προσομοιώσεις με βάση σενάρια. Θα μάθουν από ειδικούς του κλάδου και ηγέτες της κυβερνοασφάλειας, οι οποίοι θα μοιραστούν τις εμπειρίες και τις γνώσεις τους σχετικά με τη διαχείριση πρωτοβουλιών κυβερνοασφάλειας. Το μάθημα δίνει έμφαση στις πρακτικές εφαρμογές και στις προκλήσεις του πραγματικού κόσμου, επιτρέποντας στους συμμετέχοντες να αναπτύξουν ηγετικές δεξιότητες στο πλαίσιο της κυβερνοασφάλειας.

Στο πλαίσιο της διαδικασίας αξιολόγησης, οι συμμετέχοντες θα πρέπει να αναπτύξουν ένα σχέδιο ηγεσίας στον κυβερνοχώρο προσαρμοσμένο στον οργανισμό τους. Το σχέδιο αυτό θα καταδεικνύει την ικανότητά τους να υποστηρίζουν επενδύσεις στην κυβερνοασφάλεια, να προωθούν μια κουλτούρα με συνείδηση της ασφάλειας και να κατανέμουν αποτελεσματικά τους πόρους για την αντιμετώπιση των αναγκών του οργανισμού σε θέματα κυβερνοασφάλειας.

Με την επιτυχή ολοκλήρωση του Micro Credential "Cybersecurity Leadership and Culture Development", οι συμμετέχοντες θα λάβουν επίσημη αναγνώριση από το Πανεπιστήμιο UniNettuno. Αυτό το αξιόλογο πιστοποιητικό πιστοποίησης πιστοποιεί τις ικανότητές τους στην ηγεσία πρωτοβουλιών κυβερνοασφάλειας, στην καλλιέργεια μιας κουλτούρας με επίγνωση της ασφάλειας και στην καθοδήγηση του οργανισμού τους προς την κατεύθυνση της ανθεκτικότητας στον κυβερνοχώρο και του μετριασμού των κινδύνων.

Συνοπτικά, το Micro Credential "Cybersecurity Leadership and Culture Development" εξοπλίζει τους συμμετέχοντες με την τεχνογνωσία και τις στρατηγικές για να ηγηθούν των προσπαθειών κυβερνοασφάλειας εντός των οργανισμών. Από την υποστήριξη στρατηγικών επενδύσεων έως την προώθηση μιας κουλτούρας με συνείδηση της ασφάλειας, οι συμμετέχοντες θα αναδειχθούν ως αποτελεσματικοί ηγέτες και παράγοντες αλλαγής στον τομέα της κυβερνοασφάλειας. Ενσωματώνοντας τις τεχνικές γνώσεις με τις ηγετικές δεξιότητες, το πρόγραμμα αυτό διαδραματίζει καθοριστικό ρόλο στη διασφάλιση ότι οι οργανισμοί θα παραμείνουν μπροστά από τις απειλές στον κυβερνοχώρο και θα υιοθετήσουν την κυβερνοασφάλεια ως στρατηγικό παράγοντα για τη μακροπρόθεσμη επιτυχία τους.

Ερωτήσεις

1. Ως υπέρμαχος της ασφάλειας στον κυβερνοχώρο, πώς θα προσεγγίζατε τα ανώτερα στελέχη ή τη διοίκηση για να τονίσετε τη σημασία των αυξημένων επενδύσεων στην ασφάλεια στον κυβερνοχώρο; Παρέχετε συγκεκριμένα επιχειρήματα και δεδομένα για να υποστηρίξετε την υπόθεσή σας.
2. Περιγράψτε τα βήματα που θα ακολουθούσατε για να διενεργήσετε μια ενδελεχή αξιολόγηση κινδύνων κυβερνοασφάλειας στον οργανισμό σας. Πώς θα χρησιμοποιούσατε τα ευρήματα της αξιολόγησης για να κατανείμετε αποτελεσματικά τους πόρους για την αντιμετώπιση των ευπαθειών και των απειλών που εντοπίστηκαν;
3. Πώς θα επικοινωνούσατε τη σημασία της κυβερνοασφάλειας στους υπαλλήλους σε όλα τα επίπεδα του οργανισμού; Δώστε παραδείγματα στρατηγικών και μεθόδων επικοινωνίας που θα χρησιμοποιούσατε για να προωθήσετε τη νοοτροπία ασφάλειας σε ολόκληρη την εταιρεία και να προωθήσετε την ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας.
4. Στο πλαίσιο της προώθησης μιας κουλτούρας ευαισθητοποίησης στον τομέα της κυβερνοασφάλειας, πώς θα σχεδιάζατε και θα εφαρμόζατε ένα πρόγραμμα κατάρτισης των εργαζομένων στον τομέα της κυβερνοασφάλειας; Ποια θέματα θα περιλαμβάνατε στο πρόγραμμα και πώς θα διασφαλίζατε τη δέσμευση και τη συμμετοχή των εργαζομένων;
5. Ως ηγέτης της ασφάλειας στον κυβερνοχώρο, πώς θα μετρήσετε την επιτυχία των προσπαθειών σας για την προώθηση μιας κουλτούρας με συνείδηση της ασφάλειας εντός του οργανισμού; Ποιες

μετρήσεις και βασικούς δείκτες απόδοσης (KPIs) θα χρησιμοποιούσατε για να αξιολογήσετε την αποτελεσματικότητα των πρωτοβουλιών ευαισθητοποίησης στον τομέα της κυβερνοασφάλειας;

6. Περιγράψτε ένα σενάριο όπου ο οργανισμός σας αντιμετωπίζει περιορισμούς στον προϋπολογισμό, αλλά υπάρχει επιτακτική ανάγκη για βελτιώσεις στην κυβερνοασφάλεια. Πώς θα ιεραρχούσατε τις πρωτοβουλίες κυβερνοασφάλειας και θα λαμβάνατε αποφάσεις κατανομής πόρων για την αντιμετώπιση κρίσιμων τρωτών σημείων με παράλληλη βελτιστοποίηση των διαθέσιμων πόρων;
7. Ως υπέρμαχος της αύξησης των επενδύσεων στην κυβερνοασφάλεια, πώς θα αντιμετωπίζατε τις οργανωτικές προκλήσεις και την αντίσταση των ενδιαφερομένων μερών που μπορεί να μην αντιλαμβάνονται πλήρως τη σημασία της κυβερνοασφάλειας; Πώς θα οικοδομούσατε συναίνεση και υποστήριξη για τις προτάσεις σας;
8. Μοιραστείτε ένα παράδειγμα μιας επιτυχημένης εκστρατείας ή πρωτοβουλίας ευαισθητοποίησης για την κυβερνοασφάλεια που έχετε υλοποιήσει στο παρελθόν. Εξηγήστε τα βασικά στοιχεία που συνέβαλαν στην επιτυχία της και τον αντίκτυπο που είχε στη συνολική κατάσταση ασφάλειας του οργανισμού.

Ασφαλής διαχείριση δεδομένων και ευαισθητοποίηση στον κυβερνοχώρο (MC 4.2.D.4)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ασφαλής διαχείριση δεδομένων και ευαισθητοποίηση στον κυβερνοχώρο Κωδ: D.4: MC 4.2.D.4
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες

Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	EXPERT
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.68, 4.2.69 και 4.2.70):

- Επίδειξη της ικανότητας ταξινόμησης δεδομένων ανάλογα με την προτεραιότητα και τη σημασία τους
- Αναγνωρίστε τη σημασία του ελέγχου ταυτότητας δύο ή πολλαπλών παραγόντων
- Εφαρμόστε προσοχή και επαγρύπνηση κατά τη χρήση των πλατφορμών κοινωνικής δικτύωσης

Περιγραφή

Το Micro Credential "Secure Data Management and Cyber Awareness" είναι ένα ολοκληρωμένο πρόγραμμα που έχει σχεδιαστεί για να εξοπλίσει τους εκπαιδευόμενους με τις απαραίτητες γνώσεις και δεξιότητες για να διασφαλίσουν την ασφάλεια των δεδομένων τους και να προωθήσουν την ευαισθητοποίηση στον κυβερνοχώρο σε διάφορα πλαίσια. Το πρόγραμμα αυτό επικεντρώνεται σε τρεις κρίσιμες πτυχές της ασφάλειας: ταξινόμηση δεδομένων, έλεγχος ταυτότητας δύο ή πολλών παραγόντων (MFA) και ασφαλείς πρακτικές στα μέσα κοινωνικής δικτύωσης.

Τα δεδομένα αποτελούν την αιμοδοσία των σύγχρονων οργανισμών και η ασφάλειά τους είναι υψίστης σημασίας. Η πρώτη ενότητα αυτού του Micro Credential επικεντρώνεται στην ταξινόμηση δεδομένων, μια θεμελιώδη πρακτική για τη διασφάλιση ευαίσθητων πληροφοριών. Οι εκπαιδευόμενοι θα εμβαθύνουν στην έννοια της ταξινόμησης δεδομένων, κατανοώντας τη σημασία της στην ιεράρχηση και τη διασφάλιση των πληροφοριών με βάση την ευαισθησία και την κρισιμότητά τους. Μέσα από πραγματικά παραδείγματα και πρακτικές ασκήσεις, οι συμμετέχοντες θα αποδείξουν την ικανότητά τους να ταξινομούν δεδομένα ανάλογα με την προτεραιότητα και τη σημασία τους.

Η δεύτερη ενότητα του Micro Credential εισάγει τους εκπαιδευόμενους στον έλεγχο ταυτότητας δύο παραγόντων ή πολλαπλών παραγόντων (MFA), μια ισχυρή πρακτική ασφάλειας που υπερβαίνει τους παραδοσιακούς κωδικούς πρόσβασης. Οι εκπαιδευόμενοι θα εξερευνήσουν τις διάφορες μορφές MFA,

συμπεριλαμβανομένων των κωδικών που βασίζονται σε SMS, των εφαρμογών ελέγχου ταυτότητας, της βιομετρικής επαλήθευσης και των μαρκών υλικού. Θα μάθουν πώς η MFA προσθέτει ένα επιπλέον επίπεδο προστασίας, απαιτώντας από τους χρήστες να παρέχουν πολλαπλές μορφές ταυτοποίησης πριν από την πρόσβαση σε ευαίσθητους λογαριασμούς ή συστήματα. Οι συμμετέχοντες θα αποκτήσουν πρακτική εμπειρία στην εφαρμογή MFA σε διάφορες πλατφόρμες και συσκευές, διασφαλίζοντας ότι μπορούν να διασφαλίσουν αποτελεσματικά τις διαδικτυακές ταυτότητες και τα ψηφιακά περιουσιακά τους στοιχεία.

Η τελευταία ενότητα τονίζει τη σημασία της άσκησης προσοχής και επαγρύπνησης κατά τη χρήση των πλατφορμών κοινωνικής δικτύωσης. Τα μέσα κοινωνικής δικτύωσης έχουν γίνει αναπόσπαστο μέρος της σύγχρονης ζωής, αλλά ενέχουν επίσης σημαντικούς κινδύνους για την ασφάλεια εάν δεν χρησιμοποιούνται με υπευθυνότητα.
Οι εκπαιδευόμενοι θα καθοδηγηθούν σχετικά με τις βέλτιστες πρακτικές για την ασφάλεια των λογαριασμών τους στα μέσα κοινωνικής δικτύωσης, την προστασία της ιδιωτικής τους ζωής και την αποφυγή κοινών παγίδων, όπως η υπερβολική κοινοποίηση προσωπικών πληροφοριών. Θα διερευνήσουν επίσης τις πιθανές συνέπειες της κακής χρήσης των μέσων κοινωνικής δικτύωσης και θα μάθουν πώς να αναγνωρίζουν και να ανταποκρίνονται σε ύποπτες δραστηριότητες ή απόπειρες ηλεκτρονικού "ψαρέματος" σε αυτές τις πλατφόρμες.

Καθ' όλη τη διάρκεια του προγράμματος, οι εκπαιδευόμενοι θα συμμετέχουν σε διαδραστικές δραστηριότητες, μελέτες περιπτώσεων και κουίζ για να ενισχύσουν την κατανόηση των εννοιών και των πρακτικών δεξιοτήτων που παρουσιάζονται. Θα έχουν επίσης πρόσβαση σε πόρους και εργαλεία για να ενισχύσουν περαιτέρω τις γνώσεις τους σχετικά με την ασφάλεια δεδομένων και την ευαισθητοποίηση στον κυβερνοχώρο. Το Micro Credential προσφέρει μια ευέλικτη εμπειρία μάθησης, επιτρέποντας στους συμμετέχοντες να προχωρούν με το δικό τους ρυθμό, ενώ παράλληλα λαμβάνουν εξειδικευμένη καθοδήγηση από έμπειρους εκπαιδευτές.

Με την επιτυχή ολοκλήρωση του Micro Credential "Secure Data Management and Cyber Awareness", οι εκπαιδευόμενοι θα κερδίσουν μια πιστοποιημένη αναγνώριση που έχει εγκριθεί από την UniNettuno. Αυτή η πιστοποίηση θα πιστοποιεί την επάρκειά τους στην ταξινόμηση δεδομένων, την εφαρμογή MFA και τις ασφαλείς πρακτικές των μέσων κοινωνικής δικτύωσης, καθιστώντας τους πολύτιμα περιουσιακά στοιχεία για κάθε οργανισμό που επιδιώκει να ενισχύσει τη στάση του στον κυβερνοχώρο.

Συμπερασματικά, το Micro Credential "Secure Data Management and Cyber Awareness" είναι ένα ολοκληρωμένο πρόγραμμα που έχει σχεδιαστεί για να εφοδιάσει τους εκπαιδευόμενους με τις βασικές γνώσεις και δεξιότητες που απαιτούνται για την προστασία των δεδομένων τους και την προώθηση μιας κουλτούρας ευαισθητοποίησης στον κυβερνοχώρο. Αντιμετωπίζει την αυξανόμενη ανάγκη των ατόμων και των οργανισμών να υιοθετήσουν προληπτικά μέτρα ασφαλείας σε ένα διαρκώς εξελισσόμενο ψηφιακό τοπίο. Με την ολοκλήρωση αυτού του Micro Credential, οι εκπαιδευόμενοι θα γίνουν έμπειροι στη διαφύλαξη των δεδομένων, στην ασφάλεια των λογαριασμών και στην άσκηση επαγρύπνησης στις διαδικτυακές τους αλληλεπιδράσεις, συμβάλλοντας σε ένα ασφαλέστερο και ασφαλέστερο ψηφιακό περιβάλλον για όλους.

Ερωτήσεις

1. Πώς θα καθορίζατε την προτεραιότητα και τη σημασία των διαφόρων τύπων δεδομένων σε έναν οργανισμό; Δώστε συγκεκριμένα παραδείγματα κατηγοριών δεδομένων και εξηγήστε πώς θα τα κατατάσσατε.
2. Περιγράψτε τη διαδικασία εφαρμογής του ελέγχου ταυτότητας δύο παραγόντων (2FA) ή του ελέγχου

ταυτότητας πολλαπλών παραγόντων (MFA) για έναν ηλεκτρονικό λογαριασμό ή σύστημα. Περιλάβετε τα βήματα που απαιτούνται και τυχόν πιθανές προκλήσεις ή προβληματισμούς.

3. Εξηγήστε τα πλεονεκτήματα της χρήσης του ελέγχου ταυτότητας δύο ή πολλαπλών παραγόντων σε σύγκριση με τις παραδοσιακές μεθόδους ελέγχου ταυτότητας ενός παράγοντα. Πώς ενισχύει την ασφάλεια;
4. Δώστε παραδείγματα καταστάσεων στις οποίες η χρήση ελέγχου ταυτότητας δύο ή πολλών παραγόντων θα ήταν ιδιαίτερα σημαντική και εξηγήστε γιατί τα σενάρια αυτά απαιτούν ένα πρόσθετο επίπεδο ασφάλειας.
5. Πώς παραμένετε προσεκτικοί και άγρυπνοι κατά τη χρήση των πλατφορμών κοινωνικής δικτύωσης; Περιγράψτε συγκεκριμένες πρακτικές ή συνήθειες που ακολουθείτε για την προστασία της ιδιωτικής ζωής και των προσωπικών σας πληροφοριών.
6. Προσδιορίστε τους συνήθεις κινδύνους ασφάλειας των μέσων κοινωνικής δικτύωσης, όπως επιθέσεις phishing ή μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς. Εξηγήστε στρατηγικές για τον μετριασμό αυτών των κινδύνων και την προστασία της παρουσίας σας στα μέσα κοινωνικής δικτύωσης.
7. Περιγράψτε τις πιθανές συνέπειες της κοινοποίησης ευαίσθητων ή προσωπικών πληροφοριών σε πλατφόρμες κοινωνικής δικτύωσης χωρίς τις κατάλληλες ρυθμίσεις απορρήτου. Πώς μπορούν τα άτομα να διασφαλίσουν τα δεδομένα τους σε τέτοια περιβάλλοντα;
8. Πώς μπορούν οι οργανισμοί να προωθήσουν την ευαισθητοποίηση των υπαλλήλων τους σε θέματα κυβερνοασφάλειας όσον αφορά τη χρήση των πλατφορμών κοινωνικής δικτύωσης τόσο στο χώρο εργασίας όσο και σε προσωπικό επίπεδο;
9. Φανταστείτε ότι συναντάτε ένα ύποπτο μήνυμα ή σύνδεσμο σε μια πλατφόρμα κοινωνικής δικτύωσης. Ποια μέτρα θα λαμβάνατε για να επαληθεύσετε τη γνησιότητά του και να διασφαλίσετε την ασφάλειά σας προτού ασχοληθείτε με αυτό;

Προηγμένη κυβερνοασφάλεια και ηθική πειρατεία (MC 4.2.D.5)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Προηγμένη κυβερνοασφάλεια και ηθικό χάκινγκ Κωδ: D.5
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628

Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	EXPERT
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.71, 4.2.72):

- Να ξέρετε πώς να προσλάβετε έναν χάκερ "λευκού καπέλου" για αξιολογήσεις κυβερνοασφάλειας
- Αναγνώριση και άμυνα κατά των τακτικών κοινωνικής μηχανικής

Περιγραφή

Το Micro Credential "Advanced Cybersecurity and Ethical Hacking" είναι ένα εκτεταμένο και καθηλωτικό πρόγραμμα που έχει σχεδιαστεί για να εξοπλίσει τους εκπαιδευόμενους με προηγμένες γνώσεις και δεξιότητες στην αναγνώριση και την άμυνα απέναντι σε τακτικές κοινωνικής μηχανικής. Επιπλέον, οι συμμετέχοντες θα μάθουν πώς να χρησιμοποιούν τεχνικές ηθικού hacking χρησιμοποιώντας hackers "λευκού καπέλου" για αξιολογήσεις κυβερνοασφάλειας.

Επισκόπηση διαπιστευτηρίων μικροϋπολογιστών:
Το πρόγραμμα χωρίζεται σε δύο ολοκληρωμένες ενότητες, καθεμία από τις οποίες εστιάζει σε βασικές πτυχές της ασφάλειας στον κυβερνοχώρο και της ηθικής πειρατείας. Οι εκπαιδευόμενοι θα εντρυφήσουν σε πραγματικά σενάρια και πρακτικές ασκήσεις, αποκτώντας πρακτική εμπειρία στην αντιμετώπιση εξελιγμένων

απειλών στον κυβερνοχώρο.

Ενότητα 1: Αναγνώριση και άμυνα απέναντι σε τακτικές κοινωνικής μηχανικής
Αυτή η ενότητα παρέχει στους εκπαιδευόμενους μια εις βάθος κατανόηση των τακτικών κοινωνικής μηχανικής που χρησιμοποιούνται συνήθως από κακόβουλους φορείς για την εκμετάλλευση ανθρώπινων τρωτών σημείων.
Οι συμμετέχοντες θα μάθουν να αναγνωρίζουν αυτές τις τεχνικές χειραγώγησης και να αναπτύσσουν αποτελεσματικούς μηχανισμούς άμυνας για την προστασία από επιθέσεις κοινωνικής μηχανικής.

1. Εισαγωγή στην κοινωνική μηχανική
   - Ορισμός της κοινωνικής μηχανικής και των διαφόρων μορφών της, όπως το phishing, το pretexting, το baiting, το tailgating και άλλα.
   - Κατανοήστε τις ψυχολογικές πτυχές που καθιστούν τα άτομα ευάλωτα σε επιθέσεις κοινωνικής μηχανικής.

2. Επιθέσεις phishing και πλαστογράφηση ηλεκτρονικού ταχυδρομείου
   - Εντοπίστε κοινούς δείκτες phishing σε μηνύματα ηλεκτρονικού ταχυδρομείου και μηνύματα.
   - Αναλύστε τις επικεφαλίδες email για να εντοπίσετε προσπάθειες παραποίησης email.
   - Εξασκηθείτε στον ασφαλή χειρισμό ηλεκτρονικών μηνυμάτων και αναφέρετε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου στις αρμόδιες αρχές.

3. Pretexting και χειραγώγηση
   - Αναγνωρίστε τις συνήθεις τακτικές προσποίησης που χρησιμοποιούνται για να κερδίσουν την εμπιστοσύνη και να εξαπατήσουν τα θύματα.
   - Ανάπτυξη στρατηγικών για την επαλήθευση της γνησιότητας των αιτημάτων και των επικοινωνιών.

4. Baiting και Tailgating
   - Κατανόηση της έννοιας του baiting και του τρόπου με τον οποίο οι κακόβουλοι φορείς χρησιμοποιούν δελεαστικές προσφορές για να θέσουν σε κίνδυνο την ασφάλεια.
   - Εφαρμογή διαδικασιών για την αποτροπή της μη εξουσιοδοτημένης φυσικής πρόσβασης σε ασφαλείς χώρους μέσω του tailgating.

5. Social Engineering Ευαισθητοποίηση και κατάρτιση
   - Υποστηρίξτε τη σημασία της τακτικής εκπαίδευσης ευαισθητοποίησης των εργαζομένων και των ατόμων σε θέματα κυβερνοασφάλειας.
   - Ανάπτυξη και εφαρμογή εκστρατειών ευαισθητοποίησης κοινωνικής μηχανικής σε οργανισμούς.

6. Μηχανισμοί άμυνας και αντιμετώπιση περιστατικών
   - Δημιουργία σχεδίων αντιμετώπισης περιστατικών για τη διαχείριση περιστατικών κοινωνικής μηχανικής.
   - Αξιολόγηση και βελτίωση των μηχανισμών άμυνας έναντι επιθέσεων κοινωνικής μηχανικής.

Ενότητα 2: Ethical Hacking και αξιολογήσεις "White Hat"
Σε αυτή την ενότητα, οι εκπαιδευόμενοι θα καταδυθούν στον κόσμο του ethical hacking, κατανοώντας τις μεθοδολογίες και τα εργαλεία που χρησιμοποιούνται από τους "white hat" hackers για την εκτέλεση αξιολογήσεων κυβερνοασφάλειας. Η έμφαση δίνεται στη χρήση τεχνικών ηθικού hacking για τον εντοπισμό ευπαθειών και την προληπτική ενίσχυση της κατάστασης κυβερνοασφάλειας ενός οργανισμού.

1. Εισαγωγή στο Ethical Hacking
   - Ορισμός του ethical hacking και διαφοροποίησή του από τις κακόβουλες δραστηριότητες hacking.
   - Κατανοήστε τις δεοντολογικές και νομικές εκτιμήσεις που σχετίζονται με τις εκτιμήσεις ηθικού hacking.

2. Οριοθέτηση και κανόνες εμπλοκής
   - Καθορίστε το πεδίο εφαρμογής και τους κανόνες εμπλοκής για τις αξιολογήσεις ηθικού hacking.
   - Ανάπτυξη σαφών κατευθυντήριων γραμμών για τη διενέργεια αξιολογήσεων με ελεγχόμενο και ασφαλή τρόπο.

3. Αποτύπωση και αναγνώριση
   - Διεξαγωγή αποτύπωσης και αναγνώρισης για τη συλλογή πληροφοριών σχετικά με τα συστήματα και τα δίκτυα-στόχους.
   - Χρήση εργαλείων και τεχνικών πληροφοριών ανοικτού κώδικα (OSINT) για τη συλλογή δεδομένων.

4. Αξιολόγηση τρωτότητας και δοκιμή διείσδυσης
   - Εκτελείτε αξιολογήσεις ευπάθειας και δοκιμές διείσδυσης για τον εντοπισμό και την εκμετάλλευση αδυναμιών ασφαλείας.
   - Αναφορά ευρημάτων και σύσταση μέτρων αποκατάστασης για την αντιμετώπιση τρωτών σημείων.

5. Δοκιμές ασφάλειας εφαρμογών ιστού
   - Κατανόηση των κοινών ευπαθειών εφαρμογών ιστού και των επιπτώσεών τους στην ασφάλεια.
   - Εφαρμογή εργαλείων και μεθοδολογιών για την αξιολόγηση και την ασφάλεια διαδικτυακών εφαρμογών.

6. Αξιολόγηση ασφάλειας ασύρματου δικτύου
   - Αξιολόγηση της ασφάλειας ασύρματου δικτύου και εντοπισμός πιθανών ευπαθειών.
   - Εφαρμογή ασφαλών ρυθμίσεων για ασύρματα δίκτυα.

7. Social Engineering στο Ethical Hacking
   - Χρησιμοποιήστε τεχνικές κοινωνικής μηχανικής σε αξιολογήσεις ηθικού hacking για να ελέγξετε την οργανωτική ανθεκτικότητα.
   - Συζητήστε τις ηθικές επιπτώσεις και τις ευθύνες που σχετίζονται με τη χρήση κοινωνικής μηχανικής στις αξιολογήσεις.

Αξιολόγηση και πιστοποίηση:
Η αξιολόγηση Micro Credential θα περιλαμβάνει πρακτικά σενάρια και πρακτικές ασκήσεις που αξιολογούν την ικανότητα των εκπαιδευομένων να αναγνωρίζουν και να αμύνονται έναντι τακτικών κοινωνικής μηχανικής. Επιπλέον, οι εκπαιδευόμενοι θα επιδείξουν την ικανότητά τους στην εφαρμογή τεχνικών ηθικού hacking κατά τη διάρκεια μιας προσομοιωμένης αξιολόγησης "λευκού καπέλου". Με την επιτυχή ολοκλήρωση του προγράμματος οι συμμετέχοντες θα αποκτήσουν το Micro Credential "Advanced Cybersecurity and Ethical Hacking", επικυρώνοντας την εμπειρία τους στον μετριασμό των απειλών κοινωνικής μηχανικής και στη διεξαγωγή αξιολογήσεων ηθικού hacking.

Συμπέρασμα:
Το Micro Credential "Advanced Cybersecurity and Ethical Hacking" παρέχει μια σε βάθος και πρακτική εμπειρία

μάθησης, ενδυναμώνοντας τους συμμετέχοντες με τις απαραίτητες γνώσεις και δεξιότητες για την αντιμετώπιση εξελιγμένων απειλών στον κυβερνοχώρο. Από την αναγνώριση τακτικών κοινωνικής μηχανικής έως τη διεξαγωγή αξιολογήσεων ηθικού hacking, οι εκπαιδευόμενοι θα είναι εξοπλισμένοι για να προστατεύουν τους οργανισμούς από απειλές στον κυβερνοχώρο και να συμβάλλουν σε ένα ασφαλέστερο ψηφιακό περιβάλλον.

Ερωτήσεις

1. Ποιες είναι ορισμένες κοινές τακτικές κοινωνικής μηχανικής που χρησιμοποιούνται από κακόβουλους φορείς για την εκμετάλλευση ανθρώπινων τρωτών σημείων και πώς μπορούν τα άτομα να αμυνθούν απέναντι σε αυτές τις τακτικές;
2. Πώς θα χρησιμοποιούσατε τεχνικές ηθικού hacking ως χάκερ "λευκού καπέλου" για να αξιολογήσετε την κατάσταση της κυβερνοασφάλειας ενός οργανισμού; Δώστε ένα παράδειγμα ενός σεναρίου όπου το ethical hacking μπορεί να χρησιμοποιηθεί αποτελεσματικά.
3. Εξηγήστε τη σημασία της εκπαίδευσης ευαισθητοποίησης σε θέματα κοινωνικής μηχανικής για τους υπαλλήλους ενός οργανισμού. Πώς μπορεί μια τέτοια εκπαίδευση να συμβάλει σε μια ισχυρότερη κουλτούρα ασφάλειας;
4. Κατά τη διάρκεια μιας αξιολόγησης της κυβερνοασφάλειας ως χάκερ "λευκού καπέλου", πώς θα χειριζόσασταν ευαίσθητες πληροφορίες ή ευπάθειες που ανακαλύφθηκαν κατά τη διάρκεια της αξιολόγησης, ώστε να διατηρήσετε ηθικές πρακτικές και να προστατεύσετε τον οργανισμό;
5. Περιγράψτε το ρόλο του footprinting και της αναγνώρισης σε μια αξιολόγηση δεοντολογικής πειρατείας. Πώς μπορούν αυτές οι δραστηριότητες να βοηθήσουν στον εντοπισμό πιθανών τρωτών σημείων στην υποδομή ασφαλείας ενός οργανισμού;

Κυβερνοασφάλεια - Ασφαλείς κωδικοί πρόσβασης και διαχείριση πρόσβασης (MC 4.2.D.6)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Κυβερνοασφάλεια - Ασφαλείς κωδικοί πρόσβασης και διαχείριση πρόσβασης **Κωδ: D.6**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**

Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	EXPERT
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.73, 4.2.74):

- Να μπορείτε να δημιουργείτε ισχυρούς και ασφαλείς κωδικούς πρόσβασης για ενισχυμένη ασφάλεια στον κυβερνοχώρο.
- Σχεδιάστε αποτελεσματικές στρατηγικές διαχείρισης πρόσβασης για την ενίσχυση της ασφάλειας των συσκευών που ανήκουν στην επιχείρηση και των ευαίσθητων δεδομένων.

Περιγραφή

Σε μια ταχέως εξελισσόμενη ψηφιακή εποχή, όπου σχεδόν κάθε πτυχή της ανθρώπινης αλληλεπίδρασης διαμεσολαβείται μέσω ψηφιακών πλατφορμών και συσκευών, η κυβερνοασφάλεια έχει καταστεί επιτακτική προτεραιότητα. Η εμφάνιση τεχνολογιών όπως η τεχνητή νοημοσύνη, η υπολογιστική νέφους, το Διαδίκτυο των πραγμάτων και η μηχανική μάθηση έχει ενισχύσει σημαντικά την αξία και την ευπάθεια των δεδομένων. Η κατάσταση αυτή προσκαλεί αναπόφευκτα κακόβουλους φορείς που είναι πρόθυμοι να εκμεταλλευτούν αυτά τα τρωτά σημεία. Ως αποτέλεσμα, υπάρχει μια κλιμακούμενη ανάγκη για αποτελεσματικές πρακτικές κυβερνοασφάλειας που ενσωματώνουν ισχυρή προστασία κωδικών πρόσβασης και ολοκληρωμένες στρατηγικές διαχείρισης πρόσβασης.

Αυτό το μικρο-πιστοποιητικό έχει σχεδιαστεί για να μεταδώσει μια εμπεριστατωμένη κατανόηση της

κυβερνοασφάλειας με έμφαση στη δημιουργία ισχυρών, ασφαλών κωδικών πρόσβασης και στην εφαρμογή αποτελεσματικών στρατηγικών διαχείρισης πρόσβασης. Με την ολοκλήρωση αυτού του προγράμματος, οι συμμετέχοντες θα έχουν αποκτήσει μια ουσιαστική βάση για την ενίσχυση της ασφάλειας των συσκευών που ανήκουν στην επιχείρηση και τη διαφύλαξη των ευαίσθητων δεδομένων.

Ενότητα: Δημιουργία ασφαλούς κωδικού πρόσβασης
Η σημασία της προστασίας με κωδικό πρόσβασης, παρά τη θεμελιώδη φύση της, συχνά υποτιμάται, οδηγώντας σε σημαντικούς κινδύνους για την ασφάλεια. Οι αδύναμοι ή ανακυκλωμένοι κωδικοί πρόσβασης γίνονται εύκολος στόχος για τους εγκληματίες του κυβερνοχώρου, οι οποίοι χρησιμοποιούν επιθέσεις brute-force ή εξελιγμένους αλγορίθμους για να τους σπάσουν. Στο πρώτο μέρος αυτού του μαθήματος, οι συμμετέχοντες θα ενημερωθούν για τις βασικές αρχές δημιουργίας ισχυρών, ασφαλών κωδικών πρόσβασης, οι οποίες περιλαμβάνουν τη χρήση συνδυασμού ειδικών χαρακτήρων, γραμμάτων και αριθμών. Θα καλυφθούν επίσης στρατηγικές όπως η αποφυγή χρήσης λέξεων λεξικού, η χρήση ελέγχου ταυτότητας δύο παραγόντων και η συχνή αλλαγή κωδικών πρόσβασης για την ενίσχυση της ασφάλειας στον κυβερνοχώρο.

Αυτό το τμήμα του μικροπιστοποιητικού προσφέρει στους συμμετέχοντες τόσο θεωρητικές γνώσεις όσο και πρακτική εμπειρία στη δημιουργία ανθεκτικών κωδικών πρόσβασης που μπορούν να αντέξουν σε διάφορους τύπους επιθέσεων στον κυβερνοχώρο. Χρησιμοποιώντας σενάρια και μελέτες περιπτώσεων από τον πραγματικό κόσμο, θα τονιστεί η σημασία των ασφαλών κωδικών πρόσβασης και οι επιπτώσεις της παραβίασής τους. Οι συμμετέχοντες θα μάθουν να χρησιμοποιούν εργαλεία διαχείρισης κωδικών πρόσβασης, να εφαρμόζουν μια πολιτική ασφαλών κωδικών πρόσβασης και να διαδίδουν τη σημασία των ισχυρών κωδικών πρόσβασης στα μέλη της ομάδας τους.

Ενότητα: Στρατηγικές Διαχείρισης Πρόσβασης
Εκτός από τους κωδικούς πρόσβασης, μια άλλη κρίσιμη πτυχή της ενίσχυσης της ασφάλειας είναι η εφαρμογή αποτελεσματικών στρατηγικών διαχείρισης πρόσβασης. Αυτό περιλαμβάνει τη ρύθμιση του ποιος έχει πρόσβαση στα συστήματα, τον καθορισμό του επιπέδου πρόσβασης και τον έλεγχο του τι μπορεί να κάνει με αυτή την πρόσβαση. Η ανεπαρκής διαχείριση της πρόσβασης μπορεί να οδηγήσει στην περιέλευση ευαίσθητων δεδομένων και πόρων σε μη εξουσιοδοτημένα χέρια, με αποτέλεσμα να προκληθεί σημαντική οικονομική ζημία και ζημία στη φήμη.

Σε αυτό το τμήμα του μαθήματος, οι συμμετέχοντες θα εμβαθύνουν στις στρατηγικές διαχείρισης πρόσβασης. Θα κατανοήσουν πώς να εκχωρούν και να διαχειρίζονται τα προνόμια πρόσβασης με βάση την αρχή των λιγότερων προνομίων (PoLP), διασφαλίζοντας ότι οι χρήστες έχουν μόνο την απαραίτητη πρόσβαση για την εκτέλεση των εργασιών τους. Θα καλυφθούν θέματα όπως ο έλεγχος πρόσβασης βάσει ρόλων (RBAC), η επαλήθευση της ταυτότητας του χρήστη, η διαχείριση συνεδριών, καθώς και ο έλεγχος και η παρακολούθηση των δραστηριοτήτων των χρηστών. Στην ενότητα αυτή θα εξεταστούν επίσης μέθοδοι διαχείρισης της πρόσβασης σε συσκευές που ανήκουν στην επιχείρηση και χειρισμού της προνομιακής πρόσβασης για την αποτροπή εσωτερικών απειλών.

Με την ολοκλήρωση αυτού του μικροπιστοποιητικού, οι συμμετέχοντες θα αποκτήσουν μια ολοκληρωμένη κατανόηση των αποτελεσματικών πρακτικών κυβερνοασφάλειας. Θα αποκτήσουν τις γνώσεις και τις δεξιότητες για τη δημιουργία ασφαλών κωδικών πρόσβασης και την εφαρμογή ισχυρών στρατηγικών διαχείρισης πρόσβασης, ενισχύοντας κατά συνέπεια την ασφάλεια των συσκευών και των ευαίσθητων δεδομένων του οργανισμού τους. Επιπλέον, θα είναι σε θέση να διαδώσουν τη σημασία αυτών των πρακτικών στον οργανισμό τους, προωθώντας μια κουλτούρα ευαισθητοποίησης και υπευθυνότητας στον τομέα της κυβερνοασφάλειας.

Μέσα από ένα μείγμα θεωρίας, πρακτικών ασκήσεων και μελετών περίπτωσης, το μάθημα αυτό θα εφοδιάσει τους συμμετέχοντες με τις δεξιότητες για να περιηγηθούν με αυτοπεποίθηση στο ολοένα και πιο σύνθετο τοπίο της κυβερνοασφάλειας. Θα είναι καλά εξοπλισμένοι ώστε να εντοπίζουν προληπτικά πιθανά τρωτά σημεία ασφαλείας και να εφαρμόζουν στρατηγικές για την αποτελεσματική αντιμετώπισή τους, διασφαλίζοντας την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των πληροφοριακών περιουσιακών στοιχείων του οργανισμού τους.

Η απόκτηση αυτού του μικροπιστοποιητικού δεν θα υποδηλώνει μόνο την επάρκεια των συμμετεχόντων στην ασφάλεια κωδικών πρόσβασης και τη διαχείριση πρόσβασης, αλλά θα υπογραμμίζει επίσης τη δέσμευσή τους να παραμένουν ενήμεροι με το εξελισσόμενο τοπίο της κυβερνοασφάλειας, καθιστώντας τους έτσι ανεκτίμητη πηγή για τις πρωτοβουλίες προστασίας των δεδομένων του οργανισμού τους.

Ερωτήσεις

1. Ποια είναι τα βασικά χαρακτηριστικά ενός ισχυρού και ασφαλούς κωδικού πρόσβασης και πώς αυτά τα στοιχεία συμβάλλουν στην ενίσχυση της ασφάλειας στον κυβερνοχώρο;
2. Πώς η χρήση ενός συνδυασμού ειδικών χαρακτήρων, γραμμάτων και αριθμών σε έναν κωδικό πρόσβασης συμβάλλει στην αποτροπή επιθέσεων στον κυβερνοχώρο; Δώστε ένα παράδειγμα ενός ισχυρού κωδικού πρόσβασης που ακολουθεί αυτές τις αρχές.
3. Ποιος είναι ο ρόλος του ελέγχου ταυτότητας δύο παραγόντων στην ενίσχυση της ασφάλειας των κωδικών πρόσβασης; Εξηγήστε πώς μπορεί να προστατεύσει ένα σύστημα ακόμη και αν παραβιαστεί ένας κωδικός πρόσβασης.
4. Γιατί είναι σημαντικό να αποφεύγεται η χρήση λέξεων λεξικού στους κωδικούς πρόσβασης; Εξηγήστε το με τη βοήθεια ενός πραγματικού παραδείγματος.
5. Εξηγήστε την αρχή των ελαχίστων προνομίων (PoLP) και το ρόλο της στην αποτελεσματική διαχείριση της πρόσβασης. Πώς η εφαρμογή της PoLP ενισχύει την ασφάλεια των συσκευών που ανήκουν στην επιχείρηση και των ευαίσθητων δεδομένων;
6. Τι είναι ο έλεγχος πρόσβασης βάσει ρόλων (RBAC) και πώς μπορεί η εφαρμογή του να βοηθήσει στη διαχείριση της πρόσβασης σε ευαίσθητα δεδομένα και συσκευές που ανήκουν στην επιχείρηση;
7. Πώς συμβάλλει η επαλήθευση της ταυτότητας του χρήστη στη συνολική στρατηγική διαχείρισης πρόσβασης; Δώστε ένα παράδειγμα όπου η επαλήθευση της ταυτότητας μπορεί να αποτρέψει μια πιθανή παραβίαση της ασφάλειας.
8. Γιατί είναι σημαντικός ο συνεχής έλεγχος και η παρακολούθηση των δραστηριοτήτων των χρηστών σε μια αποτελεσματική στρατηγική διαχείρισης πρόσβασης; Πώς συμβάλλει στην έγκαιρη ανίχνευση πιθανών απειλών ασφαλείας;
9. Συζητήστε ένα σενάριο όπου η ακατάλληλη διαχείριση πρόσβασης οδήγησε σε παραβίαση δεδομένων. Πώς θα μπορούσε να είχε αποτραπεί με την εφαρμογή αποτελεσματικών στρατηγικών διαχείρισης πρόσβασης;

Ενημέρωση για την κυβερνοασφάλεια και διαχείριση λογαριασμών (MC 4.2.D.7)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Ενημέρωση για την ασφάλεια στον κυβερνοχώρο και διαχείριση λογαριασμών Κωδ: D.7
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	EXPERT
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή

Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.75, 4.2.76):

- Εκπαιδεύστε τους υπαλλήλους σχετικά με τους κινδύνους που συνδέονται με τη χρήση προσωπικών λογαριασμών για εργασίες που σχετίζονται με την εργασία και προωθήστε τη σημασία του διαχωρισμού των προσωπικών και των επαγγελματικών λογαριασμών.
- Εφαρμόστε ένα σύστημα προσωπικών λογαριασμών για κάθε υπάλληλο, ώστε να καθιερώνεται σαφής ευθύνη για την πρόσβαση σε ευαίσθητα δεδομένα και να παρακολουθούνται αποτελεσματικά οι δραστηριότητες των χρηστών.

Περιγραφή

Στην ψηφιακή εποχή, η ενσωμάτωση της τεχνολογίας στις καθημερινές λειτουργίες μιας επιχείρησης είναι πανταχού παρούσα, γεγονός που συνεπάγεται αύξηση του όγκου των ευαίσθητων δεδομένων που χρειάζονται προστασία. Αυτή η αλλαγή παραδείγματος απαιτεί αυστηρά μέτρα ασφαλείας και ένα εκπαιδευμένο εργατικό δυναμικό για την ελαχιστοποίηση των πιθανών απειλών στον κυβερνοχώρο. Οι κίνδυνοι που σχετίζονται με τις απειλές στον κυβερνοχώρο δεν περιορίζονται στους εξωτερικούς επιτιθέμενους, αλλά συχνά μπορεί να προέρχονται από το εσωτερικό του οργανισμού, σκόπιμα ή ακούσια, μέσω της κατάχρησης προσωπικών λογαριασμών για εργασίες που σχετίζονται με την εργασία. Ως εκ τούτου, είναι ζωτικής σημασίας η εκπαίδευση των εργαζομένων σχετικά με αυτούς τους κινδύνους και η εφαρμογή ενός συστήματος που διαχωρίζει τους προσωπικούς και τους επαγγελματικούς λογαριασμούς.

Αυτό το μικρο-πιστοποιητικό έχει σχεδιαστεί για να παρέχει στους συμμετέχοντες μια ολοκληρωμένη κατανόηση των κινδύνων που συνδέονται με τη χρήση προσωπικών λογαριασμών για εργασίες που σχετίζονται με την εργασία και τη σημασία του διαχωρισμού των προσωπικών και επαγγελματικών λογαριασμών. Οι συμμετέχοντες θα μάθουν επίσης να εφαρμόζουν ένα σύστημα προσωπικών λογαριασμών για κάθε εργαζόμενο, ώστε να καθιερώνουν σαφή ευθύνη για την πρόσβαση σε ευαίσθητα δεδομένα και να παρακολουθούν αποτελεσματικά τις δραστηριότητες των χρηστών.

Ενότητα: Εκπαίδευση των εργαζομένων σχετικά με τους κινδύνους

Η σημασία της ασφάλειας στον κυβερνοχώρο δεν μπορεί να υποτιμηθεί. Ωστόσο, ένα σύστημα ασφαλείας είναι τόσο ισχυρό όσο ο πιο αδύναμος κρίκος του. Συχνά, αυτός ο αδύναμος κρίκος τείνει να είναι το ανθρώπινο λάθος ή η αμέλεια, κυρίως όταν οι εργαζόμενοι χρησιμοποιούν τους προσωπικούς τους λογαριασμούς για εργασίες που σχετίζονται με την εργασία. Αυτό το μέρος του μαθήματος εξετάζει τους κινδύνους που συνδέονται με τη χρήση προσωπικών λογαριασμών για επαγγελματικούς σκοπούς, συμπεριλαμβανομένης της διαρροής δεδομένων, της πιθανής πειρατείας και της δυσκολίας παρακολούθησης των δραστηριοτήτων που σχετίζονται με την εργασία. Οι συμμετέχοντες θα μάθουν για παραδείγματα από τον πραγματικό κόσμο όπου

η κακή χρήση προσωπικών λογαριασμών οδήγησε σε σημαντικές παραβιάσεις της ασφάλειας. Θα κατανοήσουν τις εκτεταμένες επιπτώσεις τέτοιων παραβιάσεων, συμπεριλαμβανομένων των πιθανών οικονομικών ζημιών, της ζημίας της φήμης και της απώλειας εμπιστοσύνης μεταξύ των ενδιαφερομένων μερών. Μέσω αυτών των μαθημάτων, οι συμμετέχοντες θα εκτιμήσουν την κρίσιμη σημασία της διατήρησης ξεχωριστών προσωπικών και επαγγελματικών λογαριασμών για τη διασφάλιση της ασφάλειας και της ακεραιότητας των ευαίσθητων δεδομένων.

Ενότητα: Διαχωρισμός προσωπικών και επαγγελματικών λογαριασμών

Στο δεύτερο τμήμα του μαθήματος, οι συμμετέχοντες θα μάθουν για τη σημασία της ύπαρξης ξεχωριστών προσωπικών και επαγγελματικών λογαριασμών. Αυτός ο διαχωρισμός αποτελεί θεμελιώδες στοιχείο μιας ισχυρής στρατηγικής κυβερνοασφάλειας, καθώς επιτρέπει τον καλύτερο έλεγχο της πρόσβασης σε ευαίσθητα δεδομένα, την ευκολότερη παρακολούθηση των δραστηριοτήτων που σχετίζονται με την εργασία και τη βελτίωση της λογοδοσίας. Οι συμμετέχοντες θα διερευνήσουν τα διάφορα οφέλη του διαχωρισμού προσωπικών και επαγγελματικών λογαριασμών, όπως η αυξημένη ασφάλεια, οι σαφέστερες διαδρομές ελέγχου και ο μεγαλύτερος έλεγχος της πρόσβασης στα δεδομένα. Μελέτες περιπτώσεων που παρουσιάζουν τα πλεονεκτήματα ενός τέτοιου διαχωρισμού, καθώς και τις παγίδες της μη εφαρμογής του, θα ενισχύσουν περαιτέρω την κατανόηση αυτή.

Ενότητα: Εφαρμογή συστημάτων προσωπικών λογαριασμών

Το τελευταίο τμήμα του μαθήματος θα επικεντρωθεί στην εφαρμογή συστημάτων προσωπικών λογαριασμών για κάθε εργαζόμενο. Οι συμμετέχοντες θα μάθουν πώς να δημιουργούν ατομικούς λογαριασμούς εργασίας για τους υπαλλήλους τους, να θεσπίζουν σαφείς κανόνες και κατευθυντήριες γραμμές για τη χρήση τους και να εφαρμόζουν συστήματα παρακολούθησης για την αποτελεσματική παρακολούθηση των δραστηριοτήτων των χρηστών. Οι συμμετέχοντες θα μάθουν τις βέλτιστες πρακτικές για τη δημιουργία και τη διαχείριση συστημάτων προσωπικών λογαριασμών, συμπεριλαμβανομένου του τρόπου χειρισμού της εισόδου και της εξόδου, της διαχείρισης των δικαιωμάτων πρόσβασης και του ελέγχου των δραστηριοτήτων των χρηστών. Θα κατανοήσουν επίσης το ρόλο αυτών των συστημάτων στη διατήρηση της λογοδοσίας και στη βελτίωση της συνολικής ασφάλειας.

Με την ολοκλήρωση αυτού του μικροπιστοποιητικού, οι συμμετέχοντες θα έχουν κατανοήσει σε βάθος τη σημασία του διαχωρισμού των προσωπικών και επαγγελματικών λογαριασμών και τους κινδύνους που συνδέονται με τη χρήση προσωπικών λογαριασμών για εργασίες που σχετίζονται με την εργασία. Θα είναι εφοδιασμένοι με τις δεξιότητες για την εφαρμογή αποτελεσματικών συστημάτων προσωπικών λογαριασμών, εξασφαλίζοντας καλύτερη ασφάλεια δεδομένων και υπευθυνότητα στον οργανισμό τους.

Αυτό το μικρο-πιστοποιητικό θα τους δώσει την ευκαιρία να κατανοήσουν πώς ένα ενημερωμένο και εκπαιδευμένο εργατικό δυναμικό μπορεί να λειτουργήσει ως η πρώτη γραμμή άμυνας έναντι πιθανών απειλών κυβερνοασφάλειας. Θα είναι σε θέση να διαδώσουν την ευαισθητοποίηση των ομάδων τους σχετικά με τη σημασία του διαχωρισμού των προσωπικών και των επαγγελματικών λογαριασμών, συμβάλλοντας έτσι στη δημιουργία μιας κουλτούρας ευαισθητοποιημένης σε θέματα ασφάλειας στους οργανισμούς τους. Μέσω ενός συνδυασμού θεωρητικής μάθησης, παραδειγμάτων από τον πραγματικό κόσμο και πρακτικών ασκήσεων, οι συμμετέχοντες θα είναι καλύτερα εξοπλισμένοι για να προβλέπουν πιθανούς κινδύνους ασφαλείας και να εφαρμόζουν στρατηγικές για τον μετριασμό τους. Η ολοκλήρωση αυτού του μικροπιστοποιητικού δεν θα σηματοδοτεί μόνο την κατανόηση της σημασίας του διαχωρισμού και της διαχείρισης λογαριασμών, αλλά θα αντανακλά επίσης τη δέσμευσή τους να διατηρούν ισχυρές πρακτικές κυβερνοασφάλειας εντός του οργανισμού τους, καθιστώντας τους ανεκτίμητα περιουσιακά στοιχεία στις πρωτοβουλίες του οργανισμού τους

για την προστασία των δεδομένων.

Ερωτήσεις

1. Ποιοι είναι οι πιθανοί κίνδυνοι που συνδέονται με τη χρήση προσωπικών λογαριασμών από τους εργαζόμενους για εργασίες που σχετίζονται με την εργασία; Παρακαλείστε να δώσετε ένα πραγματικό παράδειγμα που να καταδεικνύει αυτούς τους κινδύνους.
2. Εξηγήστε τα οφέλη του διαχωρισμού των προσωπικών και επαγγελματικών λογαριασμών για τους εργαζόμενους. Πώς μπορεί αυτός ο διαχωρισμός να ενισχύσει τη στάση κυβερνοασφάλειας ενός οργανισμού;
3. Ποια μέτρα μπορεί να λάβει ένας οργανισμός για να εκπαιδεύσει τους υπαλλήλους σχετικά με τους κινδύνους της χρήσης προσωπικών λογαριασμών για εργασίες που σχετίζονται με την εργασία;
4. Πώς ο διαχωρισμός προσωπικών και επαγγελματικών λογαριασμών βοηθά στην αποτελεσματικότερη παρακολούθηση των δραστηριοτήτων που σχετίζονται με την εργασία;
5. Ποιος είναι ο ρόλος της εκπαίδευσης των εργαζομένων στην προώθηση της σημασίας του διαχωρισμού των προσωπικών και των επαγγελματικών λογαριασμών;
6. Περιγράψτε μια κατάσταση στην οποία η αποτυχία διαχωρισμού των προσωπικών και των επαγγελματικών λογαριασμών οδήγησε σε παραβίαση της ασφάλειας. Πώς θα μπορούσε να είχε αποτραπεί;
7. Ποια στοιχεία είναι ζωτικής σημασίας για την εφαρμογή ενός συστήματος προσωπικού λογαριασμού για κάθε εργαζόμενο;
8. Πώς μπορεί η εφαρμογή συστημάτων προσωπικών λογαριασμών να καθιερώσει σαφή ευθύνη για την πρόσβαση σε ευαίσθητα δεδομένα;
9. Ποιες στρατηγικές μπορεί να χρησιμοποιήσει ένας οργανισμός για την αποτελεσματική παρακολούθηση των δραστηριοτήτων των χρηστών όταν χρησιμοποιεί ένα σύστημα προσωπικών λογαριασμών για τους υπαλλήλους;

Διαχείριση κυβερνοασφάλειας - Προστασία τελικών σημείων και διατήρηση δεδομένων (MC 4.2.D.8)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Διαχείριση κυβερνοασφάλειας - Προστασία τελικών σημείων και διατήρηση δεδομένων Κωδ: D.8

Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: 101087628
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	EXPERT
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή
Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.77, 4.2.78):

- Γνωρίζετε πώς να εφαρμόζετε, να χειρίζεστε και να συντηρείτε λύσεις προστασίας τελικών σημείων για την προστασία μεμονωμένων συσκευών και δικτύων από απειλές ασφαλείας.
- Εφαρμόστε πολιτικές διατήρησης δεδομένων για να διασφαλίσετε ότι τα δεδομένα διατηρούνται μόνο για την απαραίτητη διάρκεια, ελαχιστοποιώντας τον κίνδυνο έκθεσης των δεδομένων και τις πιθανές επιπτώσεις από περιστατικά κυβερνοασφάλειας.

Περιγραφή

Στη δυναμική σφαίρα της κυβερνοασφάλειας, η προστασία των τελικών σημείων, όπως φορητοί υπολογιστές,

smartphones και άλλες ασύρματες συσκευές, αποτελεί κρίσιμο στοιχείο για την προστασία των ψηφιακών περιουσιακών στοιχείων ενός οργανισμού από απειλές ασφαλείας. Ταυτόχρονα, οι ισχυρές πολιτικές διατήρησης δεδομένων μπορούν να διαδραματίσουν καθοριστικό ρόλο στην ελαχιστοποίηση του κινδύνου έκθεσης δεδομένων και των πιθανών επιπτώσεων περιστατικών κυβερνοασφάλειας. Για την πλοήγηση στις πολυπλοκότητες αυτών των τομέων της κυβερνοασφάλειας, υπάρχει κρίσιμη ανάγκη για επαγγελματίες που είναι έμπειροι στην εφαρμογή και τη συντήρηση λύσεων προστασίας τελικών σημείων και στην άσκηση αποτελεσματικών πολιτικών διατήρησης δεδομένων.

Αυτό το μικρο-πιστοποιητικό έχει σχεδιαστεί για να προσφέρει στους συμμετέχοντες μια ολοκληρωμένη κατανόηση των στρατηγικών και πρακτικών που σχετίζονται με την προστασία μεμονωμένων συσκευών και δικτύων από απειλές ασφαλείας. Στόχος του είναι επίσης να τους εφοδιάσει με τις απαραίτητες δεξιότητες για την αποτελεσματική εφαρμογή πολιτικών διατήρησης δεδομένων, διασφαλίζοντας ότι τα δεδομένα διατηρούνται μόνο για την απαιτούμενη διάρκεια, μειώνοντας έτσι τον κίνδυνο έκθεσης των δεδομένων.

Ενότητα: Προστασία τελικών σημείων

Τα τελικά σημεία, ως πύλες εισόδου στο δίκτυο ενός οργανισμού, αποτελούν πρωταρχικούς στόχους για κυβερνοεπιθέσεις. Η διασφάλιση της ασφάλειας αυτών των συσκευών είναι ένα πολύπλοκο έργο που απαιτεί εξειδικευμένες γνώσεις και δεξιότητες. Το πρώτο μέρος αυτού του μαθήματος είναι αφιερωμένο στην κατανόηση της σημασίας της προστασίας των τερματικών σημείων και στην εκμάθηση του τρόπου αποτελεσματικής υλοποίησης και συντήρησης λύσεων προστασίας τερματικών σημείων. Οι συμμετέχοντες θα εμβαθύνουν στους διάφορους τύπους λύσεων προστασίας τελικών σημείων, που κυμαίνονται από λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό έως τείχη προστασίας και συστήματα ανίχνευσης εισβολών. Θα κατανοήσουν το ρόλο που διαδραματίζει κάθε τύπος λύσης στην άμυνα κατά των διαφόρων τύπων απειλών στον κυβερνοχώρο και πώς να επιλέγουν τις κατάλληλες λύσεις για τις συγκεκριμένες οργανωτικές τους ανάγκες. Επιπλέον, θα μάθουν για τις βέλτιστες πρακτικές για τη συντήρηση αυτών των λύσεων, συμπεριλαμβανομένων των τακτικών ενημερώσεων και διορθώσεων λογισμικού, της συνεχούς παρακολούθησης και της άμεσης αντίδρασης σε πιθανές απειλές. Μέσω πραγματικών σεναρίων και μελετών περίπτωσης, οι συμμετέχοντες θα κατανοήσουν τις συνέπειες της ανεπαρκούς προστασίας των τελικών σημείων και τον κρίσιμο ρόλο των έγκαιρων ενημερώσεων και της συνεχούς παρακολούθησης στη διατήρηση μιας ισχυρής άμυνας κατά των απειλών στον κυβερνοχώρο.

Ενότητα: Διατήρηση Δεδομένων

Μια άλλη ζωτικής σημασίας πτυχή της ασφάλειας στον κυβερνοχώρο είναι η διαχείριση του κύκλου ζωής των δεδομένων, ιδίως του χρόνου διατήρησης των δεδομένων. Το δεύτερο μέρος του μαθήματος επικεντρώνεται στις πολιτικές διατήρησης δεδομένων και στον ρόλο τους στην ελαχιστοποίηση του κινδύνου έκθεσης δεδομένων. Οι συμμετέχοντες θα μάθουν για τη σημασία της διατήρησης των δεδομένων μόνο για την απαραίτητη διάρκεια και για τους πιθανούς κινδύνους που συνδέονται με τη διατήρηση των δεδομένων για μεγαλύτερο χρονικό διάστημα από το απαιτούμενο. Θα εμβαθύνουν στις νομικές και κανονιστικές απαιτήσεις που σχετίζονται με τη διατήρηση δεδομένων και πώς να τις ενσωματώσουν στις πολιτικές διατήρησης δεδομένων του οργανισμού τους. Επιπλέον, οι συμμετέχοντες θα αποκτήσουν γνώσεις σχετικά με τις βέλτιστες πρακτικές για την εφαρμογή και τη διατήρηση πολιτικών διατήρησης δεδομένων, συμπεριλαμβανομένων των τακτικών ελέγχων, των αυτοματοποιημένων πρωτοκόλλων διαγραφής δεδομένων και της εκπαίδευσης του προσωπικού. Θα κατανοήσουν το ρόλο αυτών των πολιτικών στη μείωση της επιφάνειας για πιθανές επιθέσεις στον κυβερνοχώρο και στην ελαχιστοποίηση των επιπτώσεων τυχόν πιθανών περιστατικών κυβερνοασφάλειας.

Με την ολοκλήρωση αυτού του μικροπιστοποιητικού, οι συμμετέχοντες θα έχουν αναπτύξει μια στέρεη βάση σε δύο κρίσιμες πτυχές της κυβερνοασφάλειας: προστασία τελικών σημείων και διατήρηση δεδομένων. Θα αποκτήσουν τις γνώσεις και τις δεξιότητες για την εφαρμογή και τη διατήρηση αποτελεσματικών λύσεων προστασίας τελικών σημείων και πολιτικών διατήρησης δεδομένων, ενισχύοντας έτσι την ασφάλεια των συσκευών, των δικτύων και των δεδομένων του οργανισμού τους. Επιπλέον, θα είναι σε θέση να υποστηρίξουν τη σημασία αυτών των πρακτικών στον οργανισμό τους, προωθώντας μια κουλτούρα ευαισθητοποίησης και υπευθυνότητας στον τομέα της κυβερνοασφάλειας.

Μέσα από ένα μείγμα θεωρίας, πρακτικών ασκήσεων και μελετών περίπτωσης, το μάθημα αυτό θα εφοδιάσει τους συμμετέχοντες με τις δεξιότητες για να περιηγηθούν με αυτοπεποίθηση στο ολοένα και πιο σύνθετο τοπίο της κυβερνοασφάλειας. Θα είναι καλά εξοπλισμένοι ώστε να εντοπίζουν προληπτικά πιθανά τρωτά σημεία ασφαλείας και να εφαρμόζουν στρατηγικές για την αποτελεσματική αντιμετώπισή τους, διασφαλίζοντας την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των πληροφοριακών περιουσιακών στοιχείων του οργανισμού τους.

Η απόκτηση αυτού του μικροπιστοποιητικού δεν θα υποδηλώνει μόνο την επάρκεια των συμμετεχόντων στην προστασία τελικών σημείων και τη διατήρηση δεδομένων, αλλά θα υπογραμμίζει επίσης τη δέσμευσή τους να παραμένουν ενημερωμένοι με το εξελισσόμενο τοπίο της κυβερνοασφάλειας, καθιστώντας τους έτσι ανεκτίμητη πηγή για τις πρωτοβουλίες προστασίας δεδομένων του οργανισμού τους.

Ερωτήσεις

1. Ποια είναι τα βασικά στοιχεία μιας αποτελεσματικής λύσης προστασίας τελικών σημείων; Πώς συνεργάζονται αυτά τα στοιχεία για να προστατεύσουν μεμονωμένες συσκευές και δίκτυα από απειλές ασφαλείας;
2. Περιγράψτε τη διαδικασία υλοποίησης μιας λύσης προστασίας τελικών σημείων σε έναν οργανισμό. Ποια είναι τα βήματα που απαιτούνται και ποιοι είναι οι βασικοί παράγοντες που πρέπει να ληφθούν υπόψη;
3. Πώς μπορούν οι τακτικές ενημερώσεις και διορθώσεις να συμβάλουν στην αποτελεσματικότητα των λύσεων προστασίας τελικών σημείων; Δώστε ένα πραγματικό παράδειγμα όπου η έλλειψη τακτικών ενημερώσεων οδήγησε σε παραβίαση της ασφάλειας.
4. Εξηγήστε την έννοια των πολιτικών διατήρησης δεδομένων. Πώς οι πολιτικές αυτές συμβάλλουν στην ελαχιστοποίηση του κινδύνου έκθεσης δεδομένων;
5. Ποια είναι η σημασία του καθορισμού μιας αναγκαίας διάρκειας για τη διατήρηση των δεδομένων και ποιοι είναι οι πιθανοί κίνδυνοι από τη διατήρηση των δεδομένων για μεγαλύτερο χρονικό διάστημα από το απαιτούμενο;
6. Πώς επηρεάζουν οι νομικές και κανονιστικές απαιτήσεις τις πολιτικές διατήρησης δεδομένων; Δώστε ένα παράδειγμα κανονισμού που επηρεάζει τη διατήρηση δεδομένων και εξηγήστε πώς.
7. Περιγράψτε τη διαδικασία εφαρμογής μιας πολιτικής διατήρησης δεδομένων σε έναν οργανισμό. Ποια είναι τα κρίσιμα βήματα και ποιες προκλήσεις μπορεί να προκύψουν κατά την εφαρμογή;
8. Πώς η άσκηση αποτελεσματικών πολιτικών διατήρησης δεδομένων ελαχιστοποιεί τις πιθανές επιπτώσεις από περιστατικά κυβερνοασφάλειας; Δώστε ένα παράδειγμα για να υποστηρίξετε την εξήγησή σας.

Βελτιστοποίηση προγράμματος περιήγησης και διαχείριση ασφάλειας (MC 4.2.D.9)

Βασικές πληροφορίες

Προσδιορισμός του μαθητή	Οποιοσδήποτε πολίτης
Τίτλος και κωδικός του μικροπιστοποιητικού	Βελτιστοποίηση προγράμματος περιήγησης και διαχείριση ασφάλειας **Κωδ: D.9**
Χώρα(ες)/Περιοχή(ες) του εκδότη	ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ http://dsw.projectsgallery.eu
Φορέας(-ες) απονομής	Κοινοπραξία DSW Αριθμός έργου: **101087628**
Ημερομηνία έκδοσης	Νοέμβριος 2023
Υποθετικός φόρτος εργασίας που απαιτείται για την επίτευξη των μαθησιακών ~~αποτελεσμάτων~~	Ελάχιστο 3 - Μέγιστο 8 ώρες
Επίπεδο της μαθησιακής εμπειρίας που οδηγεί στο μικροπιστοποιητικό	EXPERT
Τύπος αξιολόγησης	Ερωτήσεις με αυτόματη σήμανση Αριθμός ερωτήσεων: 16- 20 Επιτυχία: 75%
Μορφή συμμετοχής στη μαθησιακή δραστηριότητα	Ασύγχρονη Διαδικτυακή

Τύπος διασφάλισης ποιότητας που χρησιμοποιείται για τη στήριξη του μικροπιστοποιητικού	Αξιολόγηση από ομότιμους

Μαθησιακά αποτελέσματα

Μαθησιακά αποτελέσματα (βλ. LOs 4.2.79, 4.2.80):

- Βελτιστοποιήστε τις ρυθμίσεις και τις επιδόσεις του προγράμματος περιήγησης για να βελτιώσετε την ταχύτητα και την αποτελεσματικότητα της περιήγησης.
- Εξατομικεύστε τις ρυθμίσεις ασφαλείας του προγράμματος περιήγησής σας για να ενισχύσετε την ασφάλεια και το απόρρητο στο διαδίκτυο.

Περιγραφή

Το πρόγραμμα περιήγησης χρησιμεύει ως κύρια διεπαφή μεταξύ των χρηστών και του Διαδικτύου, προσφέροντας μια πύλη πρόσβασης σε τεράστιο όγκο πληροφοριών και υπηρεσιών. Ως εκ τούτου, η απόδοση και η ασφάλεια του προγράμματος περιήγησης μπορεί να επηρεάσει σημαντικά την ποιότητα της διαδικτυακής εμπειρίας ενός χρήστη. Ως εκ τούτου, είναι ζωτικής σημασίας για τους χρήστες να βελτιστοποιούν τις ρυθμίσεις του προγράμματος περιήγησης για αυξημένη ταχύτητα και αποδοτικότητα, ενώ παράλληλα εξατομικεύουν τις ρυθμίσεις ασφαλείας για την προώθηση της ασφάλειας και της ιδιωτικότητας στο διαδίκτυο.

Αυτό το μικρο-πιστοποιητικό έχει ως στόχο να εφοδιάσει τους συμμετέχοντες με τις απαραίτητες γνώσεις και δεξιότητες για τη βελτιστοποίηση των ρυθμίσεων του προγράμματος περιήγησης για βελτιωμένη ταχύτητα και αποδοτικότητα και την εξατομίκευση των ρυθμίσεων ασφαλείας για αυξημένη ασφάλεια και ιδιωτικότητα στο διαδίκτυο. Το μάθημα θα καλύψει όλες τις πτυχές της διαχείρισης του προγράμματος περιήγησης, από την κατανόηση των διαφόρων ρυθμίσεων έως τον χειρισμό τους για τη βελτιστοποίηση της απόδοσης και την ενίσχυση της ασφάλειας.

Ενότητα: Βελτιστοποίηση του προγράμματος περιήγησης για αυξημένη ταχύτητα και αποτελεσματικότητα

Στο πρώτο μέρος του μαθήματος, οι συμμετέχοντες θα μάθουν για τις πολυάριθμες ρυθμίσεις και λειτουργίες που μπορούν να επηρεάσουν την ταχύτητα και την αποτελεσματικότητα ενός προγράμματος περιήγησης. Οι συμμετέχοντες θα εμβαθύνουν στα διάφορα στοιχεία που επηρεάζουν την ταχύτητα περιήγησης, όπως η διαχείριση της προσωρινής μνήμης cache, ο έλεγχος των cookies και η απενεργοποίηση περιττών επεκτάσεων. Μέσω πρακτικών ασκήσεων, θα μάθουν πώς να προσαρμόζουν αυτές τις ρυθμίσεις για τη βελτιστοποίηση της απόδοσης του προγράμματος περιήγησης και τη βελτίωση της συνολικής διαδικτυακής εμπειρίας. Θα καλυφθεί επίσης η σημασία των τακτικών ενημερώσεων του προγράμματος περιήγησης, με τους συμμετέχοντες να μαθαίνουν πώς οι ενημερώσεις όχι μόνο παρέχουν τις πιο πρόσφατες λειτουργίες και διορθώσεις ασφαλείας αλλά συχνά βελτιώνουν και την απόδοση του προγράμματος περιήγησης. Παραδείγματα από τον πραγματικό κόσμο θα υπογραμμίσουν περαιτέρω τη σημασία των τακτικών ενημερώσεων του προγράμματος περιήγησης και της σωστής διαχείρισης του προγράμματος περιήγησης για

τη βελτίωση της ταχύτητας περιήγησης.

Ενότητα: Προσωπικές ρυθμίσεις ασφαλείας του προγράμματος περιήγησης για αυξημένη ασφάλεια και προστασία της ιδιωτικής ζωής

Το δεύτερο μέρος του μαθήματος θα επικεντρωθεί στις ρυθμίσεις ασφαλείας του προγράμματος περιήγησης. Οι συμμετέχοντες θα μάθουν πώς να εξατομικεύουν αυτές τις ρυθμίσεις για να ενισχύσουν την ασφάλεια και το απόρρητο στο διαδίκτυο. Από την κατανόηση του ρόλου των cookies στην ηλεκτρονική παρακολούθηση έως την εκμάθηση του τρόπου εφαρμογής διαφόρων χαρακτηριστικών ασφαλείας, όπως οι αποκλεισμοί αναδυόμενων παραθύρων και η ιδιωτική περιήγηση, οι συμμετέχοντες θα αποκτήσουν μια ολοκληρωμένη κατανόηση των ρυθμίσεων ασφαλείας του προγράμματος περιήγησης. Τα θέματα θα περιλαμβάνουν επίσης τη διαχείριση αποθηκευμένων κωδικών πρόσβασης, την ενεργοποίηση αυτόματων ενημερώσεων για διορθώσεις ασφαλείας και την κατανόηση των ασφαλών συνδέσεων (HTTPS). Οι συμμετέχοντες θα μάθουν πώς να διαχειρίζονται τις ρυθμίσεις απορρήτου για να ελέγχουν πόσες προσωπικές πληροφορίες μοιράζονται με τους ιστότοπους και πώς να χρησιμοποιούν την incognito ή την ιδιωτική λειτουργία για επιπλέον προστασία της ιδιωτικής ζωής.

Στο τέλος αυτού του μικρο-πιστοποιητικού, οι συμμετέχοντες θα έχουν αποκτήσει μια ολοκληρωμένη κατανόηση του τρόπου βελτιστοποίησης και διαχείρισης των ρυθμίσεων του προγράμματος περιήγησης για βελτιωμένη ταχύτητα, αποδοτικότητα, ασφάλεια και προστασία της ιδιωτικής ζωής. Θα είναι σε θέση να περιηγούνται στο διαδικτυακό τους περιβάλλον με μεγαλύτερη αυτοπεποίθηση και έλεγχο, εξασφαλίζοντας μια ασφαλή και αποτελεσματική εμπειρία περιήγησης.

Μέσα από θεωρητικές γνώσεις και πρακτικές ασκήσεις, το μάθημα αυτό θα δώσει στους συμμετέχοντες τη δυνατότητα να κατανοήσουν τις αποχρώσεις των ρυθμίσεων του προγράμματος περιήγησης και τον αντίκτυπό τους στην ταχύτητα, την αποδοτικότητα και την ασφάλεια. Θα αποκτήσουν επίσης πολύτιμες γνώσεις σχετικά με τη σημασία της διαχείρισης του προγράμματος περιήγησης στο ευρύτερο πλαίσιο της διαδικτυακής ασφάλειας και ιδιωτικότητας.

Η ολοκλήρωση αυτού του μικροπιστοποιητικού θα αποδείξει την επάρκειά τους στη βελτιστοποίηση του προγράμματος περιήγησης και στη διαχείριση της ασφάλειας. Αυτό το επίτευγμα όχι μόνο θα βελτιώσει την διαδικτυακή τους εμπειρία, αλλά θα τους εξοπλίσει και με κρίσιμες δεξιότητες που είναι απαραίτητες στον ολοένα και πιο ψηφιακό κόσμο. Θα γίνουν πιο ικανοί και υπεύθυνοι ψηφιακοί πολίτες, έμπειροι στη διαχείριση της διαδικτυακής τους διεπαφής αποτελεσματικά και με ασφάλεια.

Ερωτήσεις

1. Ποιες είναι ορισμένες βασικές ρυθμίσεις που μπορούν να βελτιστοποιηθούν για να βελτιωθεί η ταχύτητα και η αποδοτικότητα ενός προγράμματος περιήγησης; Δώστε παραδείγματα.
2. Πώς επηρεάζει η διαχείριση της κρυφής μνήμης cache την απόδοση ενός προγράμματος περιήγησης; Συζητήστε τις επιπτώσεις της εκκαθάρισης της προσωρινής μνήμης του προγράμματος περιήγησης στην ταχύτητα και την αποδοτικότητα της περιήγησης.
3. Ποιοι είναι οι πιθανοί κίνδυνοι που σχετίζονται με τη χρήση των προεπιλεγμένων ρυθμίσεων ασφαλείας του προγράμματος περιήγησης; Πώς μπορεί η εξατομίκευση αυτών των ρυθμίσεων να βελτιώσει την ασφάλεια και την ιδιωτικότητα στο διαδίκτυο;
4. Περιγράψτε το ρόλο των cookies στην ηλεκτρονική παρακολούθηση και την προστασία της ιδιωτικής

ζωής. Πώς μπορούν να προσαρμοστούν οι ρυθμίσεις του προγράμματος περιήγησης για την αποτελεσματική διαχείριση των cookies;

5. Συζητήστε τη σημασία των ενημερώσεων του προγράμματος περιήγησης στο πλαίσιο τόσο της βελτιστοποίησης των επιδόσεων όσο και της ασφάλειας. Δώστε ένα πραγματικό παράδειγμα όπου η έλλειψη ενημερώσεων του προγράμματος περιήγησης οδήγησε σε παραβίαση της ασφάλειας ή σε μείωση των επιδόσεων.
6. Πώς μπορεί η χρήση επεκτάσεων να επηρεάσει την απόδοση και την ασφάλεια ενός προγράμματος περιήγησης; Συζητήστε ορισμένες στρατηγικές για την αποτελεσματική διαχείριση των επεκτάσεων.
7. Πώς η ιδιωτική περιήγηση ή η λειτουργία incognito ενισχύει την ιδιωτικότητα στο διαδίκτυο; Σε ποια σενάρια μπορεί να είναι ιδιαίτερα επωφελής η χρήση αυτής της λειτουργίας;

ΠΑΡΑΡΤΗΜΑ Ι: ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ

ΤΟΜΈΑΣ ΔΡΑΣΤΗΡΙΌΤΗΤΑΣ: ΑΣΦΆΛΕΙΑ (4) ΙΚΑΝΟΤΗΤΑ: (4.2)			
Μαθησιακά αποτελέσματα	Επίπεδο	K - S - A	Επεξήγηση
1. Να είναι σε θέση να αναγνωρίζουν τη σημασία της ασφαλούς ηλεκτρονικής ταυτοποίησης για την ασφαλέστερη ανταλλαγή προσωπικών δεδομένων στις συναλλαγές.	L1	K	Η ασφαλής ηλεκτρονική ταυτοποίηση είναι απαραίτητη για την ασφαλή ανταλλαγή προσωπικών δεδομένων στις συναλλαγές. Για παράδειγμα, η χρήση ελέγχου ταυτότητας δύο παραγόντων (2FA) προσθέτει ένα επιπλέον επίπεδο ασφάλειας, μειώνοντας τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες.

2. Να γνωρίζετε πώς να εντοπίζετε τα στοιχεία που συνήθως εξηγούνται στην "πολιτική απορρήτου" των εφαρμογών ή υπηρεσιών.	L1	K - S	Οι πολιτικές απορρήτου περιέχουν συνήθως διάφορα βασικά στοιχεία για τη διασφάλιση της διαφάνειας και της συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων. Τα στοιχεία αυτά περιλαμβάνουν: Τύποι δεδομένων που συλλέγονται: Αυτή η ενότητα εξηγεί τις κατηγορίες δεδομένων χρήστη που συλλέγει η εφαρμογή ή η υπηρεσία, όπως προσωπικές πληροφορίες, πληροφορίες συσκευής και δεδομένα χρήσης. Σκοπός της συλλογής δεδομένων: Εδώ, η πολιτική απορρήτου περιγράφει τους λόγους συλλογής δεδομένων χρήστη, οι οποίοι μπορεί να περιλαμβάνουν την παροχή υπηρεσιών, τη βελτίωση της εμπειρίας του χρήστη και την παροχή εξατομικευμένου περιεχομένου. Πρακτικές επεξεργασίας και κοινοποίησης δεδομένων: Η πολιτική περιγράφει λεπτομερώς τον τρόπο με τον οποίο τα δεδομένα που συλλέγονται υποβάλλονται σε επεξεργασία, αποθηκεύονται και μοιράζονται με τρίτους. Μπορεί επίσης να περιλαμβάνει πληροφορίες σχετικά με τη διαβίβαση δεδομένων και τη διασυνοριακή επεξεργασία. Συναίνεση χρήστη: Αυτό το στοιχείο εξηγεί πώς λαμβάνεται η συγκατάθεση του χρήστη για τη συλλογή και επεξεργασία δεδομένων. Μπορεί να περιλαμβάνει ρητή συγκατάθεση μέσω κουτιών ελέγχου συγκατάθεσης ή σιωπηρή συγκατάθεση μέσω της χρήσης της εφαρμογής. Δικαιώματα χρήστη: Επισημαίνονται τα δικαιώματα των χρηστών όσον αφορά τα δεδομένα τους, συμπεριλαμβανομένου του δικαιώματος πρόσβασης, διόρθωσης, διαγραφής ή περιορισμού της επεξεργασίας των προσωπικών τους πληροφοριών. Μέτρα ασφαλείας: Η πολιτική απορρήτου περιγράφει τα μέτρα ασφαλείας που εφαρμόζονται για την προστασία των δεδομένων των χρηστών από μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις ή κακή χρήση. Περίοδος διατήρησης δεδομένων: Αυτή η ενότητα καθορίζει πόσο καιρό η εφαρμογή ή η υπηρεσία διατηρεί τα δεδομένα του χρήστη και πότε διαγράφονται ή ανωνυμοποιούνται. Χρήση υπηρεσιών τρίτων: Εάν η εφαρμογή ή η υπηρεσία ενσωματώνεται με υπηρεσίες τρίτων ή μοιράζεται δεδομένα με αυτές, το στοιχείο αυτό εξηγεί τη φύση των συνεργασιών αυτών. Απόρρητο των παιδιών (κατά περίπτωση): Εάν η εφαρμογή ή η υπηρεσία απευθύνεται σε παιδιά ή συλλέγει δεδομένα από αυτά, ενδέχεται να υπάρχουν πρόσθετες πληροφορίες σχετικά με τη συμμόρφωση με τους νόμους περί απορρήτου των παιδιών. Ειδοποιήσεις ενημέρωσης πολιτικής: Η πολιτική μπορεί να αναφέρει τον τρόπο με τον οποίο οι χρήστες θα ενημερώνονται για τυχόν αλλαγές ή ενημερώσεις της πολιτικής απορρήτου. Στοιχεία επικοινωνίας: Η πολιτική απορρήτου παρέχει στοιχεία επικοινωνίας για τους χρήστες, ώστε να μπορούν να απευθύνονται για ερωτήσεις ή ανησυχίες σχετικά με το απόρρητο των δεδομένων.

3. Προσδιορίστε τους διάφορους τύπους προσωπικών δεδομένων που ενδέχεται να διατρέχουν κίνδυνο (π.χ. όνομα, ηλεκτρονικό ταχυδρομείο, διεύθυνση, αριθμός τηλεφώνου, αριθμός ασφάλισης υγείας της ΕΕ).	L1	K - S	Διάφοροι τύποι προσωπικών δεδομένων που θα μπορούσαν να διακινδυνεύσουν σε πλατφόρμες κοινωνικής δικτύωσης περιλαμβάνουν ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, διευθύνσεις κατοικίας, αριθμούς τηλεφώνου, αριθμούς EU Heatlth Insurance, ημερομηνίες γέννησης, οικονομικές πληροφορίες, στοιχεία απασχόλησης και προσωπικά ενδιαφέροντα ή δραστηριότητες. Οι χρήστες θα πρέπει να είναι προσεκτικοί στην κοινοποίηση τέτοιων ευαίσθητων πληροφοριών στο κοινό για να αποφύγουν πιθανούς κινδύνους για την ιδιωτικότητα και την ασφάλεια.

4. Να υπολογίσετε τα οφέλη και τους κινδύνους πριν επιτρέψετε σε τρίτους να επεξεργάζονται προσωπικά δεδομένα.	L1	S	Η στάθμιση των οφελών και των κινδύνων πριν επιτραπεί σε τρίτους να επεξεργάζονται προσωπικά δεδομένα είναι απαραίτητη για τη διασφάλιση της ιδιωτικότητας και της ασφάλειας των δεδομένων. Ενώ η συνεργασία με τρίτους μπορεί να προσφέρει πλεονεκτήματα, όπως βελτιωμένες υπηρεσίες και διευρυμένες δυνατότητες, ενέχει επίσης κινδύνους, όπως πιθανές παραβιάσεις δεδομένων και απώλεια του ελέγχου των ευαίσθητων πληροφοριών.
5. Συζητήστε το ρόλο του λογισμικού προστασίας από ιούς στην προστασία από κακόβουλο λογισμικό και εξασκηθείτε στην εκτέλεση τακτικών σαρώσεων από ιούς στις συσκευές σας.	L1	K - S	Το λογισμικό προστασίας από ιούς παίζει καθοριστικό ρόλο στην προστασία από κακόβουλο λογισμικό, καθώς εντοπίζει, αποκλείει και αφαιρεί κακόβουλο λογισμικό από τις συσκευές σας. Η εκτέλεση τακτικών σαρώσεων antivirus βοηθά στον προληπτικό εντοπισμό και την εξάλειψη πιθανών απειλών, διασφαλίζοντας την ασφάλεια και την ακεραιότητα των δεδομένων σας και την ομαλή λειτουργία των συσκευών σας. Με την εφαρμογή αυτής της προληπτικής προσέγγισης, οι χρήστες μπορούν να μειώσουν σημαντικά τον κίνδυνο μολύνσεων από κακόβουλο λογισμικό και να διασφαλίσουν τα ψηφιακά τους περιουσιακά στοιχεία.
6. Εξατομικεύστε τις ρυθμίσεις απορρήτου στους λογαριασμούς σας στα μέσα κοινωνικής δικτύωσης για να περιορίσετε τις πληροφορίες που είναι δημόσια ορατές.	L1	S	Η εξατομίκευση των ρυθμίσεων απορρήτου στους λογαριασμούς των μέσων κοινωνικής δικτύωσης είναι απαραίτητη για τον περιορισμό των δημόσια ορατών πληροφοριών, διασφαλίζοντας ότι μόνο το επιθυμητό περιεχόμενο κοινοποιείται στο προοριζόμενο κοινό και μειώνοντας τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης σε προσωπικά δεδομένα. Προσαρμόζοντας τις ρυθμίσεις απορρήτου, οι χρήστες μπορούν να έχουν καλύτερο έλεγχο της διαδικτυακής τους παρουσίας και να προστατεύουν την ιδιωτική τους ζωή effποτελεσματικά.
7. Ελέγξτε την ισχύ των κωδικών σας χρησιμοποιώντας εργαλεία διαχείρισης κωδικών πρόσβασης	L1	A	Ελέγξτε την ισχύ των κωδικών σας χρησιμοποιώντας εργαλεία διαχείρισης κωδικών πρόσβασης offline για να βεβαιωθείτε ότι είναι ισχυροί και ασφαλείς. Αυτά τα εργαλεία βοηθούν στον εντοπισμό των αδύναμων κωδικών πρόσβασης και παρέχουν συστάσεις για τη δημιουργία ισχυρότερων κωδικών πρόσβασης, ενισχύοντας έτσι τη συνολική διαδικτυακή σας ασφάλεια.
8. Δείξτε πώς να χρησιμοποιείτε τα ενσωματωμένα χαρακτηριστικά ασφαλείας του smartphone σας, όπως το κλείδωμα οθόνης, για να προστατεύετε τα προσωπικά σας δεδομένα.	L1	S	Για να χρησιμοποιήσετε τις ενσωματωμένες λειτουργίες ασφαλείας του smartphone σας, μεταβείτε στις ρυθμίσεις της συσκευής σας, βρείτε την επιλογή "Ασφάλεια" ή "Κλείδωμα οθόνης" και ρυθμίστε μια ισχυρή μέθοδο κλειδώματος οθόνης, όπως PIN, κωδικό πρόσβασης, μοτίβο ή βιομετρική μέθοδο (αναγνώριση δακτυλικών αποτυπωμάτων ή προσώπου). Έτσι θα προστατεύσετε τα προσωπικά σας δεδομένα από μη εξουσιοδοτημένη πρόσβαση και θα διασφαλίσετε ότι μόνο εσείς μπορείτε να ξεκλειδώσετε το smartphone σας και να αποκτήσετε πρόσβαση σε ευαίσθητες πληροφορίες.
9. Τροποποιείτε περιοδικά τον κωδικό πρόσβασής σας για να αποφύγετε πιθανές παραβιάσεις δεδομένων.	L1	S - A	Η περιοδική τροποποίηση των κωδικών πρόσβασής σας είναι σημαντική για την ελαχιστοποίηση του κινδύνου παραβίασης δεδομένων. Η τακτική αλλαγή των κωδικών πρόσβασης συμβάλλει στην αποτροπή μη εξουσιοδοτημένης πρόσβασης στους λογαριασμούς σας και ενισχύει τη συνολική διαδικτυακή σας ασφάλεια.
10. Συμπεραίνετε τους κινδύνους της χρήσης μη ασφαλών δημόσιων δικτύων Wi-Fi για συναλλαγές που αφορούν προσωπικά δεδομένα.	L1	K - S	Η χρήση μη ασφαλών δημόσιων δικτύων Wi-Fi για συναλλαγές που αφορούν προσωπικά δεδομένα ενέχει σημαντικούς κινδύνους. Μπορεί να εκθέσει ευαίσθητες πληροφορίες σε πιθανούς υποκλοπείς, οδηγώντας σε υποκλοπή δεδομένων, κλοπή ταυτότητας και μη εξουσιοδοτημένη πρόσβαση σε οικονομικούς ή προσωπικούς λογαριασμούς. Είναι σημαντικό να αποφεύγετε τη χρήση δημόσιου Wi-Fi για ευαίσθητες συναλλαγές και, αντ' αυτού, να χρησιμοποιείτε ασφαλή δίκτυα ή ένα εικονικό ιδιωτικό δίκτυο (VPN) για να διασφαλίσετε το απόρρητο και την ασφάλεια των δεδομένων.

11. Να διακρίνετε το κατάλληλο και ακατάλληλο ψηφιακό περιεχόμενο για κοινοποίηση σε λογαριασμούς κοινωνικής δικτύωσης.	L2	K - S	Το κατάλληλο ψηφιακό περιεχόμενο για κοινοποίηση σε λογαριασμούς κοινωνικής δικτύωσης περιλαμβάνει δημοσιεύσεις με σεβασμό και θετική διάθεση που συμμορφώνονται με τις κατευθυντήριες γραμμές της πλατφόρμας. Οι προσωπικές ενημερώσεις και το ενημερωτικό, εμπνευσμένο περιεχόμενο είναι επίσης κατάλληλα. Το ακατάλληλο περιεχόμενο περιλαμβάνει προσβλητικό υλικό, ρητορική μίσους, κοινοποίηση προσωπικών πληροφοριών χωρίς συγκατάθεση και παραβιάσεις πνευματικών δικαιωμάτων.

12. Συζητήστε τη σημασία της προστασίας των προσωπικών δεδομένων κατά τη χρήση ψηφιακών πλατφορμών.	L2	K	Η κατανόηση της σημασίας της προστασίας των προσωπικών δεδομένων κατά τη χρήση ψηφιακών πλατφορμών είναι ζωτικής σημασίας για τη διασφάλιση της ιδιωτικής ζωής, την πρόληψη της κλοπής ταυτότητας και την αποφυγή πιθανών ζημιών. Τα προσωπικά δεδομένα, όπως ονόματα, διευθύνσεις, οικονομικά στοιχεία και πληροφορίες επικοινωνίας, είναι πολύτιμα και μπορούν να αξιοποιηθούν από κακόβουλους φορείς για διάφορες δόλιες δραστηριότητες. Θέτοντας ως προτεραιότητα την προστασία των δεδομένων, τα άτομα μπορούν να διατηρήσουν τον έλεγχο των πληροφοριών τους και να μειώσουν τον κίνδυνο παραβίασης δεδομένων ή μη εξουσιοδοτημένης πρόσβασης, εξασφαλίζοντας μια ασφαλέστερη και ασφαλέστερη διαδικτυακή εμπειρία.
13. Επικύρωση κατάλληλων μέτρων για την προστασία των προσωπικών δεδομένων πριν από την κοινοποίησή τους σε ψηφιακές πλατφόρμες.	L2	A	Για να προστατεύσετε τα προσωπικά δεδομένα πριν τα μοιραστείτε σε ψηφιακές πλατφόρμες, χρησιμοποιήστε ισχυρούς και μοναδικούς κωδικούς πρόσβασης, ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων και να είστε προσεκτικοί σχετικά με τις πληροφορίες που μοιράζεστε δημοσίως. Ελέγχετε τακτικά και προσαρμόζετε τις ρυθμίσεις απορρήτου για τον έλεγχο της πρόσβασης στα δεδομένα και εξετάστε το ενδεχόμενο χρήσης εικονικών ιδιωτικών δικτύων (VPN) για πρόσθετη ασφάλεια κατά τη χρήση δημόσιων δικτύων Wi-Fi. Αυτά τα μέτρα συμβάλλουν στη διασφάλιση της ιδιωτικής ζωής, στην αποτροπή μη εξουσιοδοτημένης πρόσβασης και στην εξασφάλιση μιας ασφαλέστερης διαδικτυακής εμπειρίας.
14. Επισημαίνετε τις ηλεκτρονικές συναλλαγές μετά τη λήψη των κατάλληλων μέτρων ασφαλείας και προστασίας.	L2	S	Με τη λήψη των κατάλληλων μέτρων ασφαλείας και προστασίας, τα άτομα μπορούν να πραγματοποιούν με αυτοπεποίθηση ηλεκτρονικές συναλλαγές. Τα μέτρα αυτά περιλαμβάνουν τη χρήση ασφαλών ιστότοπων με HTTPS, την ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων, την τακτική παρακολούθηση των τραπεζικών λογαριασμών και την αποφυγή ανταλλαγής ευαίσθητων πληροφοριών μέσω μη ασφαλών δικτύων. Με την εφαρμογή αυτών των προφυλάξεων, ο κίνδυνος απάτης ή μη εξουσιοδοτημένης πρόσβασης ελαχιστοποιείται, επιτρέποντας μια πιο ασφαλή και ξέγνοιαστη εμπειρία ηλεκτρονικών συναλλαγών.
15. Συζητήστε τη σημασία της αποφυγής μη ασφαλών ιστότοπων κατά τη διαχείριση πληροφοριών καρτών.	L2	K	Η κατανόηση της σημασίας της αποφυγής μη ασφαλών ιστότοπων κατά τον χειρισμό πληροφοριών καρτών είναι ζωτικής σημασίας για τη διασφάλιση των προσωπικών και οικονομικών δεδομένων. Οι μη ασφαλείς ιστότοποι ενδέχεται να μην διαθέτουν τα κατάλληλα μέτρα ασφαλείας, καθιστώντας τους ευάλωτους σε παραβιάσεις δεδομένων και μη εξουσιοδοτημένη πρόσβαση. Αποφεύγοντας τέτοιους ιστότοπους και παρέχοντας πληροφορίες κάρτας μόνο σε ασφαλείς και αξιόπιστες πλατφόρμες, τα άτομα μπορούν να προστατευτούν από πιθανή απάτη, κλοπή ταυτότητας και οικονομικές απώλειες, εξασφαλίζοντας μια ασφαλέστερη διαδικτυακή εμπειρία.
16. Καθορισμός μέτρων για την επαλήθευση της αξιοπιστίας των ατόμων πριν από την ανταλλαγή ευαίσθητων δεδομένων μαζί τους	L2	S - A	Για να επαληθεύσετε την αξιοπιστία των ατόμων πριν μοιραστείτε μαζί τους ευαίσθητα δεδομένα, ζητήστε επίσημα έγγραφα ταυτοποίησης ή διαπιστευτήρια για να επιβεβαιώσετε την ταυτότητά τους, επικοινωνήστε άμεσα για να εδραιώσετε την εμπιστοσύνη και χρησιμοποιήστε ασφαλή κανάλια επικοινωνίας για την ανταλλαγή δεδομένων. Επιπλέον, ελέγξτε τις πολιτικές απορρήτου και τα μέτρα ασφαλείας σε περίπτωση κοινής χρήσης δεδομένων με εταιρείες ή διαδικτυακές πλατφόρμες και λάβετε τη ρητή συγκατάθεση των ατόμων πριν προχωρήσετε στην κοινή χρήση δεδομένων. Τα μέτρα αυτά συμβάλλουν στη διασφάλιση της προστασίας των δεδομένων και μειώνουν τον κίνδυνο πιθανών παραβιάσεων δεδομένων ή μη εξουσιοδοτημένης πρόσβασης.
17. Αποσαφηνίστε τι είναι ένα cookie και πώς μπορεί να επηρεάσει τα ευαίσθητα δεδομένα σας	L2	K	Το cookie είναι ένα μικρό αρχείο κειμένου που αποθηκεύεται στη συσκευή ενός χρήστη από έναν ιστότοπο που επισκέπτεται. Αν και τα cookies είναι γενικά αβλαβή και χρησιμοποιούνται για διάφορους σκοπούς, μπορούν ενδεχομένως να affποκάλυπταν ευαίσθητα δεδομένα αν γινόταν κατάχρηση, παρακολουθώντας τη συμπεριφορά, τις προτιμήσεις και τα διαπιστευτήρια σύνδεσης του χρήστη, θέτοντας έτσι σε κίνδυνο το απόρρητο των δεδομένων αν αποκτήσουν πρόσβαση μη εξουσιοδοτημένα μέρη ή αν χρησιμοποιηθούν για κακόβουλους σκοπούς.

18. Αποσαφηνίστε την έννοια του "incognito mode" ή της "ιδιωτικής περιήγησης" στα προγράμματα περιήγησης στο διαδίκτυο και πώς να το χρησιμοποιείτε.	L2	K	Η "λειτουργία Incognito" ή "ιδιωτική περιήγηση" είναι μια λειτουργία στα προγράμματα περιήγησης στο διαδίκτυο που επιτρέπει στους χρήστες να περιηγούνται στο διαδίκτυο χωρίς να αποθηκεύουν ιστορικό περιήγησης, cookies ή δεδομένα ιστότοπου στη συσκευή τους. Για να τη χρησιμοποιήσετε, ανοίξτε το πρόγραμμα περιήγησής σας και ενεργοποιήστε τη λειτουργία ιδιωτικής περιήγησης, που συνήθως βρίσκεται στις ρυθμίσεις ή στο μενού, και ξεκινήστε την περιήγηση. Μόλις κλείσετε το παράθυρο ιδιωτικής περιήγησης, όλα τα δεδομένα από τη συγκεκριμένη περίοδο θα διαγραφούν, offποφέροντας μια πιο ιδιωτική και ασφαλή εμπειρία περιήγησης.
19. Να είναι σε θέση να ελέγξει τις γνώσεις σχετικά με τις πολιτικές απορρήτου των ιστότοπων που επισκέπτεται συχνά.	L2	A	Ο μαθησιακός στόχος "Να είναι σε θέση να ελέγχει τις γνώσεις σχετικά με τις πολιτικές απορρήτου των ιστότοπων που επισκέπτεται συχνά" είναι ζωτικής σημασίας για τον ψηφιακό γραμματισμό και την κυβερνοασφάλεια. Υπογραμμίζει τη σημασία της κατανόησης και της κριτικής αξιολόγησης των πολιτικών απορρήτου για τη διασφάλιση των προσωπικών δεδομένων. Ο στόχος αυτός βοηθά τα άτομα να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τις διαδικτυακές τους δραστηριότητες και ενθαρρύνει ασφαλέστερες διαδικτυακές πρακτικές.
20. Συστήστε τις βέλτιστες πρακτικές για την ασφάλεια στο διαδίκτυο σε φίλους και οικογένεια.	L2	A	Για να διασφαλίσετε την ασφάλεια στο διαδίκτυο, συνιστούμε να χρησιμοποιείτε ισχυρούς και μοναδικούς κωδικούς πρόσβασης, να ενεργοποιείτε τον έλεγχο ταυτότητας δύο παραγόντων, να αποφεύγετε να κάνετε κλικ σε ύποπτους συνδέσμους ή να κατεβάζετε συνημμένα αρχεία από άγνωστες πηγές, να ενημερώνετε τακτικά το λογισμικό και τις συσκευές σας και να είστε προσεκτικοί στην κοινοποίηση προσωπικών πληροφοριών στο διαδίκτυο. Ενθαρρύνετέ τους να ενημερώνονται για τις τελευταίες διαδικτυακές απειλές και να εφαρμόζουν υπεύθυνη προστασία δεδομένων, ώστε να διασφαλίζουν την ιδιωτικότητα και την ασφάλειά τους κατά τη χρήση ψηφιακών πλατφορμών.
21. Προσδιορισμός των κατάλληλων ενεργειών που πρέπει να λαμβάνονται όταν γίνεται κατάχρηση προσωπικών δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης.	L3	K - S	Όταν γίνεται κατάχρηση προσωπικών δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης, αναφέρετε αμέσως την κατάχρηση στην ομάδα υποστήριξης ή συντονισμού της πλατφόρμας. Ελέγξτε και προσαρμόστε τις ρυθμίσεις απορρήτου σας για να περιορίσετε την πρόσβαση στα προσωπικά σας δεδομένα. Εάν είναι απαραίτητο, εξετάστε το ενδεχόμενο να αλλάξετε τους κωδικούς πρόσβασής σας για να αποτρέψετε περαιτέρω μη εξουσιοδοτημένη πρόσβαση.
22. Αναπτύξτε μια στάση προσοχής όταν κάνετε κλικ σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα και μάθετε πώς να περνάτε με το ποντίκι πάνω από τους συνδέσμους για να δείτε τον πραγματικό προορισμό τους.	L3	A	Η ανάπτυξη μιας στάσης προσοχής όταν κάνετε κλικ σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα είναι ζωτικής σημασίας για να αποφύγετε να πέσετε θύμα απάτης phishing ή κακόβουλου λογισμικού. Πάντα να περνάτε τον δείκτη του ποντικιού πάνω από τους συνδέσμους για να δείτε τον πραγματικό προορισμό τους πριν κάνετε κλικ για να βεβαιωθείτε ότι οδηγούν σε νόμιμους και ασφαλείς ιστότοπους.

23. Χρήση της ηλεκτρονικής ταυτοποίησης για τις υπηρεσίες που παρέχονται από τις δημόσιες αρχές και τον επιχειρηματικό τομέα.	L3	S	Η χρήση της ηλεκτρονικής ταυτοποίησης (eID) για τις υπηρεσίες που παρέχουν οι δημόσιες αρχές και ο επιχειρηματικός τομέας προσφέρει πολυάριθμα οφέλη όσον αφορά την αποτελεσματικότητα, την ασφάλεια και την ευκολία των χρηστών. Με την υιοθέτηση λύσεων ηλεκτρονικής ταυτότητας, τα άτομα μπορούν να έχουν πρόσβαση σε διάφορες κυβερνητικές και ιδιωτικές υπηρεσίες μέσω διαδικτύου, χωρίς την ανάγκη φυσικών επισκέψεων ή γραφειοκρατίας. Η πιστοποίηση ταυτότητας με ηλεκτρονική ταυτότητα εξασφαλίζει ασφαλή επαλήθευση της ταυτότητας, μειώνοντας τον κίνδυνο απάτης και μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες. Επιπλέον, εξορθολογίζει τις διαδικασίες, επιταχύνει την παροχή υπηρεσιών και προάγει μια πιο απρόσκοπτη και φιλική προς τον χρήστη εμπειρία για τους πολίτες και τους πελάτες που αλληλεπιδρούν τόσο με δημόσιους όσο και με ιδιωτικούς φορείς.

24. Δώστε προτεραιότητα στην προστασία των δεδομένων κατά τη χρήση των μέσων κοινωνικής δικτύωσης για επαγγελματικούς ή εκπαιδευτικούς σκοπούς.	L3	S	Δώστε προτεραιότητα στην προστασία των δεδομένων κατά τη χρήση των μέσων κοινωνικής δικτύωσης για επαγγελματικούς ή εκπαιδευτικούς σκοπούς, διαμορφώνοντας τις ρυθμίσεις απορρήτου, όντας επιλεκτικοί όσον αφορά το κοινόχρηστο περιεχόμενο και ενεργοποιώντας τον έλεγχο ταυτότητας δύο παραγόντων (2FA) για πρόσθετη ασφάλεια. Μείνετε σε εγρήγορση απέναντι σε απόπειρες ηλεκτρονικού "ψαρέματος", περιορίστε τις προσωπικές πληροφορίες στα προφίλ και επιδείξτε προσοχή με τις άδειες εφαρμογών τρίτων για να διασφαλίσετε ευαίσθητα δεδομένα και να εξασφαλίσετε μια ασφαλέστερη διαδικτυακή εμπειρία.
25. Αναγνωρίστε τις διαδικτυακές απάτες και αναπτύξτε έναν υγιή σκεπτικισμό απέναντι σε ανεπιθύμητες διαδικτυακές προσφορές.	L3	K - A	Η εκμάθηση σχετικά με τις ηλεκτρονικές απάτες και η ανάπτυξη ενός υγιούς σκεπτικισμού απέναντι σε ανεπιθύμητες επιστολές είναι απαραίτητη για την προστασία από απάτες και κλοπή ταυτότητας. Η επιφυλακτικότητα και η επαλήθευση της νομιμότητας των offers πριν από την παροχή προσωπικών πληροφοριών ή τη διενέργεια οικονομικών συναλλαγών μπορεί να βοηθήσει στην αποφυγή του να πέσει κανείς θύμα απάτης και να διασφαλίσει την ασφάλεια στο διαδίκτυο.
26. Προετοιμάστε τον υπολογιστή και το smartphone σας εγκαθιστώντας και ενημερώνοντας το απαραίτητο λογισμικό ασφαλείας.	L3	S - A	Προετοιμάστε τον υπολογιστή και το smartphone σας για αυξημένη ασφάλεια εγκαθιστώντας και ενημερώνοντας τακτικά το απαραίτητο λογισμικό ασφαλείας, όπως προγράμματα προστασίας από ιούς και τείχη προστασίας. Αυτά τα μέτρα συμβάλλουν στην προστασία των συσκευών σας από κακόβουλο λογισμικό, ιούς και άλλες διαδικτυακές απειλές, εξασφαλίζοντας μια ασφαλέστερη διαδικτυακή εμπειρία.
27. Βαθμολογήστε τις διαδικτυακές σας συνήθειες ως προς τον κίνδυνο ασφάλειας.	L3	A	Ως γλωσσικό μοντέλο τεχνητής νοημοσύνης, δεν έχω διαδικτυακές συνήθειες ή πρόσβαση στο διαδίκτυο. Ωστόσο, είναι ζωτικής σημασίας για τα άτομα να αξιολογούν τακτικά τις δικές τους διαδικτυακές συνήθειες και να λαμβάνουν τα απαραίτητα μέτρα για την ελαχιστοποίηση των κινδύνων ασφαλείας, όπως η χρήση ισχυρών κωδικών πρόσβασης, η ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων και η αποφυγή ανταλλαγής ευαίσθητων πληροφοριών με άγνωστες ή αναξιόπιστες πηγές.
28. Συζητήστε ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα υπόκειται σε τοπικούς κανονισμούς όπως ο ΓΚΠΔ.	L3	K	Η επεξεργασία δεδομένων προσωπικού χαρακτήρα υπόκειται σε τοπικούς κανονισμούς όπως ο ΓΚΠΔ, διασφαλίζοντας την προστασία της ιδιωτικής ζωής. Οι οργανισμοί πρέπει να συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ όταν χειρίζονται προσωπικά δεδομένα ατόμων εντός της ΕΕ.
29. Αναφέρετε την ύπαρξη φιλικών προς τα παιδιά προγραμμάτων περιήγησης και δείξτε ενδιαφέρον για την ασφάλεια των παιδιών στο διαδίκτυο, χρησιμοποιώντας ή συνιστώντας αυτά τα προγράμματα περιήγησης.	L4	K - S	Οι γονείς και οι φροντιστές θα πρέπει να γνωρίζουν τα φιλικά προς τα παιδιά προγράμματα περιήγησης που έχουν σχεδιαστεί για να παρέχουν ένα ασφαλέστερο διαδικτυακό περιβάλλον για τα παιδιά. Χρησιμοποιώντας ή συνιστώντας αυτά τα προγράμματα περιήγησης, μπορούν να βοηθήσουν στην προστασία των παιδιών από την πρόσβαση σε ακατάλληλο περιεχόμενο και να διασφαλίσουν την ηλεκτρονική τους ασφάλεια κατά την εξερεύνηση του ψηφιακού κόσμου.

30. Να διακρίνετε μεταξύ ασφαλών και μη ασφαλών ιστότοπων κατά την περιήγηση.	L3	K - S	Οι ασφαλείς ιστότοποι χρησιμοποιούν HTTPS στις διευθύνσεις URL τους και εμφανίζουν ένα εικονίδιο λουκέτου στη γραμμή διευθύνσεων του προγράμματος περιήγησης, υποδεικνύοντας ότι η σύνδεση μεταξύ του χρήστη και του ιστότοπου είναι κρυπτογραφημένη, εξασφαλίζοντας την προστασία των δεδομένων. Οι μη ασφαλείς ιστότοποι δεν διαθέτουν HTTPS στις διευθύνσεις URL τους και ενδέχεται να εμφανίζουν την προειδοποίηση "Not Secure", υποδεικνύοντας ότι τα δεδομένα που μεταδίδονται μεταξύ του χρήστη και του ιστότοπου δεν είναι κρυπτογραφημένα, ενέχοντας δυνητικούς κινδύνους για την ασφάλεια των δεδομένων.

31. Εντοπίστε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου που μπορεί να περιέχουν απόπειρες ηλεκτρονικού "ψαρέματος" ή κακόβουλο λογισμικό.	L4	K - S	Εντοπίστε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν απόπειρες ηλεκτρονικού "ψαρέματος" ή κακόβουλο λογισμικό αναζητώντας άγνωστους αποστολείς, επείγουσα ή απειλητική γλώσσα, ύποπτους συνδέσμους, αιτήματα για ευαίσθητες πληροφορίες, απροσδόκητα συνημμένα αρχεία και γενικούς χαιρετισμούς και αποφύγετε να κάνετε κλικ σε οποιοδήποτε αμφισβητούμενο περιεχόμενο. Αντ' αυτού, επαληθεύστε τη νομιμότητα του αποστολέα μέσω άλλου καναλιού ή επικοινωνήστε απευθείας με τον οργανισμό.
32. Καθορισμός προηγμένων μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων στους λογαριασμούς κοινωνικής δικτύωσης.	L4	S - A	Η εφαρμογή προηγμένων μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων στους λογαριασμούς κοινωνικής δικτύωσης περιλαμβάνει την ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων (2FA), την τακτική επανεξέταση και προσαρμογή των ρυθμίσεων απορρήτου, τη χρήση ισχυρών και μοναδικών κωδικών πρόσβασης, την προσοχή στις άδειες χρήσης εφαρμογών τρίτων και την επαγρύπνηση απέναντι σε απόπειρες ηλεκτρονικού "ψαρέματος". Επιπλέον, αποφύγετε να μοιράζεστε ευαίσθητες πληροφορίες δημοσίως, περιορίστε τα προσωπικά δεδομένα στα προφίλ και εκπαιδευτείτε σχετικά με τα πιο πρόσφατα χαρακτηριστικά απορρήτου και τους πιθανούς κινδύνους στις πλατφόρμες κοινωνικής δικτύωσης. Συνδυάζοντας αυτά τα μέτρα, μπορείτε να ενισχύσετε σημαντικά την ασφάλεια των προσωπικών σας δεδομένων και να διατηρήσετε μεγαλύτερο έλεγχο της ιδιωτικής σας ζωής στο διαδίκτυο.
33. Εξηγήστε την έννοια της κρυπτογράφησης και το ρόλο της στην προστασία των προσωπικών πληροφοριών.	L4	K - S - A	Η κρυπτογράφηση είναι η διαδικασία μετατροπής δεδομένων σε κωδικοποιημένη μορφή για την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Ο ρόλος της στην προστασία των προσωπικών πληροφοριών είναι να διασφαλίζει ότι τα δεδομένα παραμένουν ασφαλή και εμπιστευτικά, ακόμη και αν υποκλαπούν από μη εξουσιοδοτημένα μέρη, διασφαλίζοντας έτσι την προστασία της ιδιωτικής ζωής και τη διατήρηση της ακεραιότητας των δεδομένων.
34. Αναγνωρίστε τους πιθανούς κινδύνους από την κοινοποίηση προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης και λάβετε τις απαραίτητες προφυλάξεις.	L4	K	Η αναγνώριση των δυνητικών κινδύνων από την κοινοποίηση προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης είναι απαραίτητη για τη διασφάλιση της ιδιωτικής ζωής και την αποτροπή της κατάχρησης δεδομένων. Ορισμένοι κίνδυνοι περιλαμβάνουν κλοπή ταυτότητας, διαδικτυακό εκφοβισμό, επιθέσεις phishing και μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες. Οι απαραίτητες προφυλάξεις περιλαμβάνουν τη διαμόρφωση των ρυθμίσεων απορρήτου, την επιλεκτικότητα όσον αφορά το κοινόχρηστο περιεχόμενο, τη χρήση ισχυρών κωδικών πρόσβασης, την ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων και την αποφυγή της δημόσιας κοινοποίησης ευαίσθητων δεδομένων. Μένοντας ενήμεροι για τους πιθανούς κινδύνους και εφαρμόζοντας αυτές τις προφυλάξεις, τα άτομα μπορούν να απολαμβάνουν μια ασφαλέστερη και ασφαλέστερη διαδικτυακή εμπειρία στις πλατφόρμες κοινωνικής δικτύωσης.
35. Συγκρίνετε τις πολιτικές απορρήτου διαφόρων εφαρμογών ή υπηρεσιών για να προσδιορίσετε τις πρακτικές συλλογής δεδομένων τους.	L4	K - S - A	Για να αναλύσετε τις πολιτικές απορρήτου των διαφόρων εφαρμογών ή υπηρεσιών για τις πρακτικές συλλογής δεδομένων, ελέγξτε τους τύπους δεδομένων που συλλέγονται, τον σκοπό της συλλογής δεδομένων, τις πρακτικές επεξεργασίας και κοινής χρήσης δεδομένων, τη συγκατάθεση του χρήστη, τα μέτρα ασφαλείας και την περίοδο διατήρησης δεδομένων. Ελέγξτε εάν οι πολιτικές συμμορφώνονται με τα δικαιώματα των χρηστών, προσδιορίζουν τη χρήση υπηρεσιών τρίτων, αντιμετωπίζουν την προστασία της ιδιωτικής ζωής των παιδιών (εάν ισχύει) και παρέχουν ενημερώσεις σχετικά με τις αλλαγές πολιτικής.

36. Περιγράψτε την έννοια της κρυπτογραφημένης επικοινωνίας και εκτιμήστε το απόρρητό σας επιλέγοντας εφαρμογές επικοινωνίας που παρέχουν κρυπτογράφηση από άκρο σε άκρο.	L4	K - A	Η κρυπτογραφημένη επικοινωνία περιλαμβάνει την κωδικοποίηση των μηνυμάτων έτσι ώστε μόνο οι προοριζόμενοι παραλήπτες να μπορούν να τα αποκρυπτογραφήσουν, εξασφαλίζοντας την ιδιωτικότητα και την ασφάλεια των δεδομένων. Για να προστατεύσετε το απόρρητό σας, επιλέξτε εφαρμογές επικοινωνίας που διαθέτουν κρυπτογράφηση από άκρο σε άκρο, η οποία διασφαλίζει ότι τα μηνύματα είναι προσβάσιμα μόνο στον αποστολέα και τον παραλήπτη, ελαχιστοποιώντας τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης στις ευαίσθητες συνομιλίες σας.

37. Υιοθέτηση των βέλτιστων πρακτικών για την προστασία των προσωπικών δεδομένων σε διάφορα επιγραμμικά πλαίσια.	L4	K - A	Οι βέλτιστες πρακτικές για την προστασία των προσωπικών δεδομένων στο διαδίκτυο περιλαμβάνουν τη χρήση ισχυρών κωδικών πρόσβασης, την ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων, την τακτική ενημέρωση του λογισμικού, την προσοχή σε συνδέσμους και συνημμένα αρχεία, την επανεξέταση των ρυθμίσεων απορρήτου, τον περιορισμό της κοινής χρήσης προσωπικών πληροφοριών, τη χρήση ασφαλών δικτύων, την παρακολούθηση λογαριασμών και την ασφαλή δημιουργία αντιγράφων ασφαλείας των δεδομένων.
38. Διερευνήστε τυχόν ανωμαλίες στις συσκευές σας που μπορεί να υποδηλώνουν παραβίαση του απορρήτου.	L4	S	Για να προστατεύσετε το απόρρητό σας, να είστε σε εγρήγορση και να διερευνάτε τυχόν ανωμαλίες στις συσκευές σας, όπως απροσδόκητη χρήση δεδομένων, ασυνήθιστα αναδυόμενα παράθυρα, άγνωστες εφαρμογές ή μη εξουσιοδοτημένες προσπάθειες πρόσβασης. Εάν παρατηρήσετε οποιαδήποτε ύποπτη δραστηριότητα, αναλάβετε άμεσα δράση, όπως η εκτέλεση σαρώσεων antivirus, η ενημέρωση του λογισμικού ασφαλείας και η αλλαγή κωδικών πρόσβασης, για να διασφαλίσετε τα προσωπικά σας δεδομένα και να αποτρέψετε πιθανές παραβιάσεις του απορρήτου.
39. Διακρίνετε όλους τους τύπους των "cookies" και πώς μπορούν να χρησιμοποιηθούν από τους ιστότοπους για την αποθήκευση δεδομένων των χρηστών.	L4	K - S	Οι ιστότοποι χρησιμοποιούν cookies περιόδου λειτουργίας για προσωρινή αποθήκευση δεδομένων κατά τη διάρκεια μιας περιόδου περιήγησης, μόνιμα cookies για πιο μακροπρόθεσμη αποθήκευση δεδομένων και cookies τρίτων για την παρακολούθηση της συμπεριφοράς των χρηστών και τη στοχευμένη διαφήμιση. Οι χρήστες θα πρέπει να είναι προσεκτικοί όσον αφορά τη συλλογή δεδομένων και μπορούν να διαχειριστούν τις ρυθμίσεις των cookies στα προγράμματα περιήγησής τους για να ελέγχουν το απόρρητο και να περιορίζουν την παρακολούθηση.
40. Δώστε προτεραιότητα στους διαδικτυακούς σας λογαριασμούς με βάση την ευαισθησία των πληροφοριών που περιέχουν.	L4	S	Δώστε προτεραιότητα στους διαδικτυακούς σας λογαριασμούς με βάση την ευαισθησία των πληροφοριών που περιέχουν. Ενισχύστε τα μέτρα ασφαλείας, όπως η χρήση ισχυρών κωδικών πρόσβασης και η ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων, για λογαριασμούς με πιο ευαίσθητα δεδομένα, ώστε να εξασφαλίσετε καλύτερη προστασία από μη εξουσιοδοτημένη πρόσβαση.
41. Αξιολογήστε την αποτελεσματικότητα των μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων στις ψηφιακές πλατφόρμες.	L5	A	Η αποτελεσματικότητα των μέτρων ασφαλείας όσον αφορά τη διασφάλιση των προσωπικών δεδομένων στις ψηφιακές πλατφόρμες εξαρτάται από την ισχύ των μέτρων που εφαρμόζονται και την ανταπόκριση της πλατφόρμας στις αναδυόμενες απειλές. Τα ισχυρά μέτρα ασφαλείας, όπως η κρυπτογράφηση, ο έλεγχος ταυτότητας πολλαπλών παραγόντων και οι τακτικές ενημερώσεις, συμβάλλουν στην καλύτερη προστασία των δεδομένων, αλλά η συνεχής παρακολούθηση και η ευαισθητοποίηση των χρηστών είναι απαραίτητες για τη διασφάλιση της συνεχούς εφαρμοστικότητας.
42. Εφαρμόστε τα βήματα για την εκκαθάριση της προσωρινής μνήμης cache και του ιστορικού περιήγησης από προγράμματα περιήγησης στο διαδίκτυο και εφαρμογές.	L5	S	Η εκκαθάριση της προσωρινής μνήμης cache και του ιστορικού περιήγησης ενισχύει το διαδικτυακό απόρρητο και την ασφάλεια, καθώς αφαιρεί τα προσωρινά αρχεία και τα δεδομένα που αποθηκεύονται από το πρόγραμμα περιήγησης, μειώνει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες και ελαχιστοποιεί την παρακολούθηση της δραστηριότητας του χρήστη σε διάφορους ιστότοπους.

43. Απαριθμήστε τους πιθανούς κινδύνους που συνδέονται με την κοινοποίηση ευαίσθητων πληροφοριών σε δημόσιους λογαριασμούς κοινωνικής δικτύωσης.	L5	K	Οι δυνητικοί κίνδυνοι που συνδέονται με την κοινοποίηση ευαίσθητων πληροφοριών σε δημόσιους λογαριασμούς μέσων κοινωνικής δικτύωσης περιλαμβάνουν κλοπή ταυτότητας, παραβιάσεις της ιδιωτικής ζωής, στοχευμένες απάτες και διαδικτυακή παρακολούθηση, καθώς και έκθεση προσωπικών πληροφοριών σε ευρύτερο κοινό, γεγονός που μπορεί να οδηγήσει σε ανεπιθύμητη προσοχή ή κακή χρήση των δεδομένων. Είναι σημαντικό να είστε προσεκτικοί σχετικά με το είδος του περιεχομένου που μοιράζεστε σε δημόσιες πλατφόρμες για την προστασία της προσωπικής σας ιδιωτικότητας και ασφάλειας.

44. Περιγράψτε τις νομικές συνέπειες της κακής διαχείρισης προσωπικών δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης.	L5	K	Ο λανθασμένος χειρισμός προσωπικών δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης μπορεί να οδηγήσει σε νομικές συνέπειες, όπως πρόστιμα, ποινές και αστικές αγωγές για παραβίαση της νομοθεσίας περί προστασίας δεδομένων, καθώς και σε βλάβη της φήμης και απώλεια επιχειρηματικών ευκαιριών λόγω απώλειας της εμπιστοσύνης των χρηστών. Η συμμόρφωση με τους κανονισμούς προστασίας δεδομένων και οι υπεύθυνες πρακτικές χειρισμού δεδομένων είναι ζωτικής σημασίας για την αποφυγή αυτών των νομικών συνεπειών.
45. Δημιουργία και επιβολή πολιτικών προστασίας δεδομένων εντός ενός οργανισμού ή μιας κοινότητας.	L5	A	Για να δημιουργήσετε και να εφαρμόσετε πολιτικές προστασίας δεδομένων, να διενεργήσετε αξιολόγηση, να αναπτύξετε σαφείς πολιτικές, να τις κοινοποιήσετε στα ενδιαφερόμενα μέρη, να εφαρμόσετε διαδικασίες και να επανεξετάζετε και να επικαιροποιείτε τακτικά τις πολιτικές. Ορίστε έναν υπεύθυνο προστασίας δεδομένων, ενσωματώστε την προστασία της ιδιωτικής ζωής μέσω σχεδιασμού και διασφαλίστε τη συμμόρφωση τρίτων μερών για την οικοδόμηση εμπιστοσύνης και την προστασία των δεδομένων εντός του οργανισμού ή της κοινότητας.
46. Διαμόρφωση στρατηγικών για την αντιμετώπιση παραβιάσεων δεδομένων και τον μετριασμό των επιπτώσεών τους.	L5	A	Για την αντιμετώπιση παραβιάσεων δεδομένων, εφαρμόστε ένα σχέδιο ταχείας αντιμετώπισης περιστατικών, συμπεριλαμβανομένων των διαδικασιών περιορισμού, διερεύνησης και κοινοποίησης. Μετριάζετε τον αντίκτυπο με την άμεση ενημέρωση των ατόμων που έχουν επηρεαστεί, τη συνεργασία με τις ρυθμιστικές αρχές, τη διενέργεια διεξοδικών αξιολογήσεων και την ενίσχυση των μέτρων ασφαλείας για την πρόληψη μελλοντικών παραβιάσεων.
47. Εξετάστε τη σημασία της εξασφάλισης του οικιακού σας δικτύου Wi-Fi και της αλλαγής του ονόματος (SSID) και μάθετε πώς να ορίσετε έναν ισχυρό κωδικό πρόσβασης για το Wi-Fi σας και να απενεργοποιήσετε το WPS.	L5	S	Ασφαλίστε το οικιακό σας δίκτυο Wi-Fi αλλάζοντας το όνομα (SSID) και ορίζοντας έναν ισχυρό κωδικό πρόσβασης για να αποτρέψετε τη μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, απενεργοποιήστε το Wi-Fi Protected Setup (WPS) για να ελαχιστοποιήσετε τα πιθανά τρωτά σημεία ασφαλείας και να εξασφαλίσετε ένα ασφαλέστερο και πιο ιδιωτικό περιβάλλον Wi-Fi.
48. Διαγνώστε πιθανά αδύναμα σημεία στη ρύθμιση του απορρήτου των δεδομένων σας.	L5	S	Για να εντοπίσετε πιθανά αδύναμα σημεία στη ρύθμιση του απορρήτου των δεδομένων σας, επανεξετάστε τα μέτρα και τις πρακτικές ασφαλείας σας, όπως η χρήση ισχυρών και μοναδικών κωδικών πρόσβασης, η ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων, η τακτική ενημέρωση του λογισμικού και η επανεξέταση των αδειών χρήσης εφαρμογών. Επιπλέον, αξιολογήστε τον τρόπο με τον οποίο χειρίζεστε προσωπικά δεδομένα, όπως η κοινοποίησή τους στα μέσα κοινωνικής δικτύωσης ή σε τρίτους, και εντοπίστε τους τομείς στους οποίους μπορείτε να βελτιωθείτε για να ενισχύσετε το συνολικό απόρρητο των δεδομένων σας.
49. Μάθετε πώς να δικτυώνεστε σωστά με άλλους ικανούς χρήστες για να ενημερώνεστε για τις τελευταίες ανησυχίες και λύσεις σχετικά με την προστασία της ιδιωτικής ζωής.	L5	A	Για να παραμείνετε ενημερωμένοι σχετικά με τις τελευταίες ανησυχίες και λύσεις για την προστασία της ιδιωτικής ζωής, δικτυωθείτε με άλλους έμπειρους χρήστες που μοιράζονται τα ίδια ενδιαφέροντα με εσάς. Η συμμετοχή σε συζητήσεις, η παρακολούθηση εργαστηρίων ή η συμμετοχή σε διαδικτυακά φόρουμ με ομοϊδεάτες σας μπορεί να σας βοηθήσει να αποκτήσετε πολύτιμες γνώσεις και βέλτιστες πρακτικές για την ενίσχυση του απορρήτου και της ασφάλειας των δεδομένων σας.

50. Επικύρωση της γνησιότητας και της ασφάλειας των ψηφιακών λήψεων.	L5	A	Για να επικυρώσετε τη γνησιότητα και την ασφάλεια των ψηφιακών λήψεων, βεβαιωθείτε ότι κατεβάζετε αρχεία από αξιόπιστες και επίσημες πηγές. Επαληθεύστε τη διεύθυνση URL του ιστότοπου, ελέγξτε για ψηφιακές υπογραφές ή αθροίσματα ελέγχου που παρέχονται από τον προγραμματιστή και χρησιμοποιήστε αξιόπιστο λογισμικό προστασίας από ιούς για να σαρώσετε τα αρχεία που κατεβάζετε για κακόβουλο λογισμικό πριν τα ανοίξετε ή τα εγκαταστήσετε.

51. Αναγνώριση των νομικών ευθυνών και υποχρεώσεων των οργανισμών και των ατόμων κατά το χειρισμό προσωπικών δεδομένων.	L6	K	Οι οργανισμοί έχουν νομικές ευθύνες για τον ηθικό, διαφανή και ασφαλή χειρισμό των προσωπικών δεδομένων, σύμφωνα με τους νόμους και τους κανονισμούς περί προστασίας δεδομένων. Μπορούν να θεωρηθούν υπεύθυνοι για παραβιάσεις δεδομένων, μη συμμόρφωση με τους νόμους περί προστασίας δεδομένων και ενδέχεται να αντιμετωπίσουν πρόστιμα, ποινές ή νομικές ενέργειες εάν χειρίζονται κακώς τα προσωπικά δεδομένα.
52. Επισημάνετε το ρόλο των ρυθμίσεων απορρήτου στις έξυπνες οικιακές συσκευές και αναπτύξτε μια στάση προσοχής κατά τη χρήση έξυπνων οικιακών συσκευών, λαμβάνοντας υπόψη τις επιπτώσεις τους στην ιδιωτική ζωή.	L6	S - A	Κατανόηση του ρόλου των ρυθμίσεων απορρήτου στις έξυπνες οικιακές συσκευές για τον έλεγχο των δεδομένων που συλλέγουν και μοιράζονται. Αναπτύξτε μια στάση προσοχής κατά τη χρήση των έξυπνων οικιακών συσκευών, λαμβάνοντας υπόψη τις πιθανές επιπτώσεις τους στην ιδιωτική ζωή, και διαμορφώστε τις ρυθμίσεις απορρήτου για την προστασία των προσωπικών σας δεδομένων και τη διατήρηση του ελέγχου της ιδιωτικής σας ζωής.
53. Οργανώστε ολοκληρωμένες αξιολογήσεις κινδύνων για τον εντοπισμό πιθανών κινδύνων για την προστασία της ιδιωτικής ζωής των δεδομένων.	L6	A	Η διενέργεια ολοκληρωμένων αξιολογήσεων κινδύνου είναι ζωτικής σημασίας για τον αποτελεσματικό εντοπισμό πιθανών κινδύνων για την προστασία της ιδιωτικής ζωής των δεδομένων. Βοηθά τους οργανισμούς να εντοπίζουν προληπτικά τα τρωτά σημεία, να αξιολογούν τις πιθανές επιπτώσεις και να εφαρμόζουν τις κατάλληλες διασφαλίσεις για την προστασία των προσωπικών δεδομένων.
54. Παρατηρήστε το ρόλο του ανθρώπινου παράγοντα στην ασφάλεια στον κυβερνοχώρο και εφαρμόστε ευαισθητοποίηση και αντίμετρα κοινωνικής μηχανικής στις ψηφιακές σας αλληλεπιδράσεις.	L6	K	Η εκτίμηση του ρόλου των ανθρώπινων παραγόντων στην ασφάλεια στον κυβερνοχώρο προϋποθέτει την κατανόηση του γεγονότος ότι η ανθρώπινη συμπεριφορά και οι ανθρώπινες ενέργειες μπορούν να επηρεάσουν σημαντικά την ασφάλεια των δεδομένων. Με την ανάπτυξη της ευαισθητοποίησης σε θέματα κοινωνικής μηχανικής και την εφαρμογή αντιμέτρων, όπως το να είναι κανείς προσεκτικός στην ανταλλαγή προσωπικών πληροφοριών στο διαδίκτυο, να επαληθεύει τη νομιμότητα των μηνυμάτων και των αιτημάτων και να ενημερώνεται για τις τελευταίες τακτικές phishing, τα άτομα μπορούν να προστατευτούν από τις απειλές στον κυβερνοχώρο και να συμβάλουν σε ένα ασφαλέστερο ψηφιακό περιβάλλον.
55. Προτεραιότητα στην προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων ως βασική αξία.	L6	S	Η προτεραιότητα στην προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων ως βασική αξία είναι απαραίτητη για τη διαφύλαξη ευαίσθητων πληροφοριών, την προστασία της εμπιστοσύνης των χρηστών και τη συμμόρφωση με τους νόμους περί προστασίας δεδομένων. Θέτοντας το απόρρητο και την ασφάλεια των δεδομένων ως προτεραιότητα, τα άτομα και οι οργανισμοί μπορούν να δημιουργήσουν ένα ασφαλέστερο ψηφιακό περιβάλλον και να διατηρήσουν την εμπιστευτικότητα και την ακεραιότητα των προσωπικών δεδομένων.

56. Επανεξετάστε την ύπαρξη ψευδών ειδήσεων και αναπτύξτε κριτική στάση απέναντι στις πληροφορίες που συναντάτε στο διαδίκτυο.	L6	K - A	Κατανοήστε ότι υπάρχουν ψεύτικες ειδήσεις και να είστε κριτικοί όταν συναντάτε πληροφορίες στο διαδίκτυο, επαληθεύοντας τις πηγές, ελέγχοντας για πολλαπλές αξιόπιστες αναφορές, και να είστε προσεκτικοί όταν μοιράζεστε ανεπιβεβαίωτες πληροφορίες. Η ανάπτυξη μιας κριτικής στάσης βοηθά στην πρόληψη της διάδοσης της παραπληροφόρησης και συμβάλλει σε μια πιο ενημερωμένη και υπεύθυνη διαδικτυακή κοινότητα.

57. Απογραφή και διαχείριση του ψηφιακού σας αποτυπώματος σε πολλαπλές πλατφόρμες και υπηρεσίες.	L6	S	Καταγράψτε και διαχειριστείτε το ψηφιακό σας αποτύπωμα, επανεξετάζοντας και αξιολογώντας τις πληροφορίες που έχετε κοινοποιήσει σε διάφορες πλατφόρμες και υπηρεσίες. Ενημερώστε τακτικά τις ρυθμίσεις απορρήτου, περιορίστε τα προσωπικά δεδομένα που μοιράζεστε και εξετάστε το ενδεχόμενο να διαγράψετε ή να απενεργοποιήσετε λογαριασμούς που δεν είναι πλέον απαραίτητοι για να μειώσετε την παρουσία σας στο διαδίκτυο και να ενισχύσετε το απόρρητό σας.
58. Διερευνήστε προληπτικά μέτρα για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στο διαδίκτυο. Πρόληψη πιθανών απειλών.	L6	S	Για την προληπτική προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στο διαδίκτυο, χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης, ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων (2FA), ενημερώστε τακτικά το λογισμικό και τις συσκευές, να είστε προσεκτικοί με συνδέσμους και συνημμένα αρχεία, ελέγξτε τις ρυθμίσεις απορρήτου, περιορίστε την κοινή χρήση προσωπικών πληροφοριών, χρησιμοποιήστε ασφαλή δίκτυα, ενημερωθείτε για τις διαδικτυακές απειλές και παρακολουθείτε τακτικά τους λογαριασμούς για μη εξουσιοδοτημένες δραστηριότητες. Η υιοθέτηση αυτών των μέτρων ενισχύει το διαδικτυακό απόρρητο και την ασφάλεια, μειώνοντας τον κίνδυνο παραβίασης δεδομένων και κλοπής ταυτότητας.
59. Συμπεραίνετε τους πιθανούς κινδύνους και τις συνέπειες των παραβιάσεων δεδομένων στις πλατφόρμες κοινωνικής δικτύωσης.	L6	K - S	Οι παραβιάσεις δεδομένων στις πλατφόρμες κοινωνικής δικτύωσης μπορεί να έχουν σημαντικές επιπτώσεις στους χρήστες, όπως κλοπή ταυτότητας, οικονομική απώλεια και ζημία στη φήμη. Το 2018, μια παραβίαση δεδομένων στο Facebook εξέθεσε τα προσωπικά δεδομένα περισσότερων από 50 εκατομμυρίων χρηστών. Τα δεδομένα αυτά θα μπορούσαν να χρησιμοποιηθούν από εγκληματίες για τη διάπραξη κλοπής ταυτότητας, απάτης και άλλων εγκλημάτων.
60. Διερεύνηση τρωτών σημείων ασφαλείας σε ψηφιακές πλατφόρμες και σύσταση βελτιώσεων.	L6	S	Για να διερευνήσετε τα τρωτά σημεία ασφαλείας σε ψηφιακές πλατφόρμες, διεξάγετε διεξοδικές αξιολογήσεις ασφαλείας, όπως δοκιμές διείσδυσης και αναθεωρήσεις κώδικα. Εντοπίστε αδυναμίες, όπως ξεπερασμένο λογισμικό, μη ασφαλείς μεθόδους ελέγχου ταυτότητας ή ανεπαρκή κρυπτογράφηση δεδομένων, και προτείνετε βελτιώσεις, όπως τακτικές ενημερώσεις ασφαλείας, ισχυρούς μηχανισμούς ελέγχου ταυτότητας και εφαρμογή πρωτοκόλλων κρυπτογράφησης για να ενίσχυση της ασφάλειας της πλατφόρμας και προστασία των δεδομένων των χρηστών.
61. Ανίχνευση προηγμένων απειλών κυβερνοασφάλειας και των πιθανών επιπτώσεών τους στα προσωπικά δεδομένα.	L7	S	Οι προηγμένες απειλές κυβερνοασφάλειας, όπως το εξελιγμένο κακόβουλο λογισμικό, το ransomware και οι στοχευμένες επιθέσεις phishing, μπορούν να έχουν σοβαρές συνέπειες στα προσωπικά δεδομένα. Αυτές οι απειλές μπορεί να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση, παραβίαση δεδομένων, κλοπή ταυτότητας και οικονομική απάτη, θέτοντας σε κίνδυνο ευαίσθητες πληροφορίες και προκαλώντας οικονομικές απώλειες, ζημία στη φήμη και συναισθηματική οδύνη στα άτομα των οποίων τα δεδομένα εκτίθενται. Για την προστασία από τέτοιες απειλές, τα άτομα πρέπει να επαγρυπνούν, να χρησιμοποιούν ισχυρά μέτρα ασφαλείας και να δίνουν προτεραιότητα στην προστασία της ιδιωτικής ζωής των δεδομένων στις διαδικτυακές τους δραστηριότητες. Οι οργανισμοί θα πρέπει επίσης να επενδύσουν σε προηγμένα εργαλεία κυβερνοασφάλειας και στην εκπαίδευση των εργαζομένων για να προστατεύσουν τα προσωπικά δεδομένα από εξελιγμένες απειλές στον κυβερνοχώρο.

62. Εξηγήστε τις διευθύνσεις IP (Internet Protocol) και το ρόλο τους στην ηλεκτρονική σας δραστηριότητα.	L7	K - S - A	Η διεύθυνση IP (Internet Protocol) είναι μια μοναδική αριθμητική ετικέτα που αποδίδεται σε κάθε συσκευή στο διαδίκτυο και χρησιμοποιείται για την επικοινωνία και την ανταλλαγή δεδομένων. Διαδραματίζει κρίσιμο ρόλο στη δρομολόγηση δεδομένων και στην παρακολούθηση των δραστηριοτήτων των χρηστών στο διαδίκτυο, γι' αυτό και η προστασία της διεύθυνσης IP είναι σημαντική για τη διατήρηση της ιδιωτικής ζωής και της ασφάλειας στο διαδίκτυο.

63. Θυμηθείτε τι είναι το DNS, πώς μπορεί να επηρεάσει το απόρρητό σας και μάθετε πώς να το αλλάξετε στον υπολογιστή σας, καθώς και στο δρομολογητή ή το μόντεμ σας.	L7	K - S	Το σύστημα ονομάτων τομέα (DNS) μεταφράζει τα ονόματα τομέα σε διευθύνσεις IP στο διαδίκτυο. Μπορεί να επηρεάσει το απόρρητό σας, καθώς ο πάροχος υπηρεσιών διαδικτύου μπορεί να καταγράφει τα αιτήματά σας DNS, αλλά μπορείτε να ενισχύσετε το απόρρητο αλλάζοντας τις ρυθμίσεις DNS στον υπολογιστή ή το δρομολογητή σας ώστε να χρησιμοποιείτε πιο ασφαλείς και επικεντρωμένους στο απόρρητο διακομιστές DNS.
64. Μελετήστε την έννοια των μεταδεδομένων στα ψηφιακά αρχεία και εκτιμήστε το απόρρητό σας αφαιρώντας τα μεταδεδομένα από τα αρχεία πριν τα μοιραστείτε στο διαδίκτυο.	L7	K - A	Κατανοήστε ότι τα μεταδεδομένα είναι πρόσθετες πληροφορίες που είναι αποθηκευμένες σε ψηφιακά αρχεία, όπως φωτογραφίες ή έγγραφα, οι οποίες μπορούν να αποκαλύψουν λεπτομέρειες όπως η τοποθεσία, η ημερομηνία και η συσκευή που χρησιμοποιήθηκε. Για να προστατεύσετε το απόρρητό σας, αφαιρέστε τα μεταδεδομένα από τα αρχεία πριν τα μοιραστείτε στο διαδίκτυο για να αποφύγετε την ακούσια αποκάλυψη ευαίσθητων πληροφοριών.
65. Αναπτύξτε ενδιαφέρον για την ασφάλεια των επικοινωνιών σας μέσω ηλεκτρονικού ταχυδρομείου και μάθετε πώς να κρυπτογραφείτε τα μηνύματά σας.	L7	A	Αναπτύξτε ενδιαφέρον για την ασφάλεια των επικοινωνιών σας μέσω ηλεκτρονικού ταχυδρομείου, αναγνωρίζοντας τους πιθανούς κινδύνους μη εξουσιοδοτημένης πρόσβασης ή υποκλοπής. Για να ενισχύσετε την ασφάλεια του ηλεκτρονικού ταχυδρομείου, μάθετε πώς να κρυπτογραφείτε τα μηνύματά σας χρησιμοποιώντας ασφαλείς υπηρεσίες ηλεκτρονικού ταχυδρομείου ή εργαλεία κρυπτογράφησης, διασφαλίζοντας ότι μόνο οι προοριζόμενοι παραλήπτες μπορούν να διαβάσουν το περιεχόμενο και προστατεύοντας τις ευαίσθητες πληροφορίες από τα αδιάκριτα μάτια.
66. Κατανοήστε τους κινδύνους που ενέχουν τα δικαιώματα των εφαρμογών κινητής τηλεφωνίας και ελέγχετε και περιορίζετε τακτικά αυτά τα δικαιώματα στο smartphone σας.	L7	K - S	Κατανοήστε τους κινδύνους των δικαιωμάτων των εφαρμογών κινητής τηλεφωνίας, καθώς ορισμένες εφαρμογές μπορεί να ζητούν πρόσβαση σε ευαίσθητα δεδομένα ή λειτουργίες της συσκευής που δεν είναι απαραίτητες για τη λειτουργία τους. Ελέγχετε τακτικά και περιορίστε τα δικαιώματα εφαρμογών στο smartphone σας για να μειώσετε τους πιθανούς κινδύνους για το απόρρητο και να διασφαλίσετε ότι οι εφαρμογές έχουν πρόσβαση μόνο στα δεδομένα και τις λειτουργίες που πραγματικά χρειάζονται.
67. Περιγράψτε τα οφέλη και τους κινδύνους του βιομετρικού ελέγχου ταυτότητας και αναπτύξτε μια προσεκτική προσέγγιση όσον αφορά τη χρήση βιομετρικών χαρακτηριστικών ως μέτρων ασφαλείας.	L7	K - S - A	Ο βιομετρικός έλεγχος ταυτότητας προσφέρει εύκολη και ασφαλή πρόσβαση με τη χρήση μοναδικών βιολογικών χαρακτηριστικών, όπως τα δακτυλικά αποτυπώματα ή η αναγνώριση προσώπου. Ωστόσο, να είστε προσεκτικοί όταν χρησιμοποιείτε βιομετρικά χαρακτηριστικά, καθώς ενδέχεται να δημιουργούν προβλήματα προστασίας της ιδιωτικής ζωής σε περίπτωση παραβίασης ή κακού χειρισμού, και να εξετάζετε τη χρήση τους σε συνδυασμό με άλλα μέτρα ασφαλείας για καλύτερη προστασία.

68. Κατανοήστε παραδείγματα νομικών υποθέσεων που σχετίζονται με το απόρρητο των δεδομένων και τις επιπτώσεις τους.	L7	K	Μια αξιοσημείωτη νομική υπόθεση που σχετίζεται με το απόρρητο των δεδομένων είναι η υπόθεση "Facebook, Inc. v. Federal Trade Commission (FTC)", όπου το Facebook αντιμετώπισε πρόστιμο ύψους 5 δισεκατομμυρίων δολαρίων για κακό χειρισμό των δεδομένων των χρηστών. Η υπόθεση ανέδειξε τη σημασία των κανονισμών για την προστασία των δεδομένων και τις πιθανές συνέπειες για τις εταιρείες που δεν τηρούν τις δεσμεύσεις για την προστασία της ιδιωτικής ζωής και δεν διασφαλίζουν τα δεδομένα των χρηστών.
69. Προβλέψτε το μέλλον της ιδιωτικότητας των δεδομένων με βάση τις τεχνολογικές εξελίξεις και το εξελισσόμενο νομικό τοπίο.	L7	K	Το μέλλον της προστασίας των προσωπικών δεδομένων είναι πιθανό να συνεχίσει να επικεντρώνεται στις τεχνολογικές εξελίξεις στην κρυπτογράφηση, την ασφαλή αποθήκευση δεδομένων και τον έλεγχο ταυτότητας των χρηστών για την προστασία των προσωπικών δεδομένων. Επιπλέον, το εξελισσόμενο νομικό τοπίο μπορεί να οδηγήσει σε αυστηρότερους κανονισμούς προστασίας δεδομένων, αυξημένη επιβολή και μεγαλύτερη ευαισθητοποίηση των ατόμων και των οργανισμών σχετικά με τη σημασία της προστασίας των προσωπικών πληροφοριών στην ψηφιακή εποχή.

70. Χειραγωγήστε τις διαμορφώσεις συσκευών και δικτύων για βέλτιστο απόρρητο των δεδομένων.	L7	S	Χειραγωγήστε τις διαμορφώσεις συσκευών και δικτύων ενεργοποιώντας χαρακτηριστικά ασφαλείας, όπως τείχη προστασίας, VPN και έλεγχο ταυτότητας δύο παραγόντων, και ενημερώνοντας τακτικά το λογισμικό για να εξασφαλίσετε το βέλτιστο απόρρητο των δεδομένων και την προστασία από πιθανές απειλές στον κυβερνοχώρο. Η εφαρμογή αυτών των μέτρων μπορεί να ενισχύσει σημαντικά την ασφάλεια των συσκευών και του δικτύου σας, διασφαλίζοντας τα προσωπικά σας δεδομένα και τις διαδικτυακές σας δραστηριότητες.
71. Συζητήστε την έννοια των DoH, DoT και DNSSEC, πώς μπορούν να βελτιώσουν το απόρρητό σας και την ασφάλειά σας από κακόβουλο λογισμικό.	L8	K	Τα DoH (DNS-over-HTTPS), DoT (DNS-over-TLS) και DNSSEC (Domain Name System Security Extensions) είναι πρωτόκολλα που έχουν σχεδιαστεί για την ενίσχυση της ιδιωτικότητας και της ασφάλειας στην επικοινωνία DNS. Τα DoH και DoT κρυπτογραφούν τα ερωτήματα DNS, αποτρέποντας την υποκλοπή και την πιθανή υποκλοπή δεδομένων DNS, ενώ το DNSSEC προσθέτει ένα επίπεδο επικύρωσης και πιστοποίησης στις απαντήσεις DNS, μειώνοντας τον κίνδυνο παραποίησης DNS και βελτιώνοντας τη συνολική ακεραιότητα των δεδομένων και την προστασία από κακόβουλο λογισμικό και επιθέσεις phishing.
72. Ερμηνεύστε την έρευνα αιχμής για την προστασία των δεδομένων και εφαρμόστε την σε πραγματικές καταστάσεις.	L8	K - S - A	Η ερμηνεία της έρευνας αιχμής για την προστασία των δεδομένων προϋποθέτει την ενημέρωση για τις τελευταίες εξελίξεις στην κρυπτογράφηση, την ανωνυμοποίηση δεδομένων, την ασφαλή κοινή χρήση δεδομένων και τις τεχνικές διατήρησης της ιδιωτικής ζωής. Η εφαρμογή αυτών των γνώσεων σε σενάρια του πραγματικού κόσμου περιλαμβάνει την εφαρμογή των πλέον σύγχρονων μέτρων προστασίας δεδομένων σε οργανισμούς, τη διασφάλιση της συμμόρφωσης με τους νόμους περί απορρήτου των δεδομένων και την υιοθέτηση βέλτιστων πρακτικών για την προστασία των ευαίσθητων πληροφοριών από πιθανές παραβιάσεις και μη εξουσιοδοτημένη πρόσβαση. Με τον τρόπο αυτό, οι επιχειρήσεις μπορούν να οικοδομήσουν εμπιστοσύνη με τους πελάτες τους, να προστατεύσουν τη φήμη τους και να ενισχύσουν τη συνολική ασφάλεια δεδομένων στο σημερινό ψηφιακό τοπίο.
73. Μάθετε να χρησιμοποιείτε ένα VPN είτε για τοπικά δίκτυα πρόσβασης (εγχώρια) είτε για δημόσια δίκτυα.	L8	S	Για να ρυθμίσετε ένα VPN για τοπικά δίκτυα πρόσβασης (εγχώρια) και δημόσια δίκτυα, επιλέξτε έναν αξιόπιστο πάροχο υπηρεσιών VPN, εγκαταστήστε το πρόγραμμα-πελάτη VPN στις συσκευές σας και συνδεθείτε στην επιθυμητή τοποθεσία διακομιστή για ασφαλή και κρυπτογραφημένη επικοινωνία. Η χρήση ενός VPN διασφαλίζει το απόρρητο των δεδομένων και την προστασία από πιθανές απειλές κατά την απομακρυσμένη πρόσβαση σε τοπικούς πόρους ή τη χρήση δημόσιων δικτύων Wi-Fi.
74. Ανίχνευση και αντιμετώπιση εξελιγμένων κυβερνοεπιθέσεων με στόχο προσωπικά δεδομένα.	L8	S	Για τον εντοπισμό και την αντιμετώπιση εξελιγμένων κυβερνοεπιθέσεων με στόχο προσωπικά δεδομένα, χρησιμοποιήστε προηγμένα μέτρα ασφαλείας, όπως συστήματα ανίχνευσης εισβολών, εργαλεία πληροφοριών για απειλές και συνεχή παρακολούθηση για τον άμεσο εντοπισμό πιθανών απειλών. Εφαρμόστε σχέδια αντιμετώπισης περιστατικών για τον μετριασμό των επιπτώσεων των επιθέσεων και την εξασφάλιση των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση, εξασφαλίζοντας μια προληπτική προσέγγιση στην κυβερνοασφάλεια.
75. Αναλύστε προηγμένες παραβιάσεις δεδομένων για να κατανοήσετε τις μεθόδους και τα τρωτά σημεία τους.	L8	S	Η ανάλυση προηγμένων παραβιάσεων δεδομένων περιλαμβάνει την ανάλυση των τεχνικών που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες και τον εντοπισμό των ευπαθειών των συστημάτων που επέτρεψαν την παραβίαση. Με την κατανόηση των μεθόδων και των αδυναμιών, οι οργανισμοί μπορούν να ενισχύσουν τα μέτρα ασφαλείας τους και να προστατεύσουν καλύτερα τα προσωπικά δεδομένα από μελλοντικές απειλές στον κυβερνοχώρο.

76. Εξερευνήστε τα οφέλη της αποκέντρωσης στην προστασία της ιδιωτικής ζωής και μάθετε να χρησιμοποιείτε αποκεντρωμένες πλατφόρμες και υπηρεσίες.	L8	S	Η εκτίμηση των πλεονεκτημάτων της αποκέντρωσης όσον αφορά την προστασία της ιδιωτικής ζωής προϋποθέτει την κατανόηση του γεγονότος ότι οι αποκεντρωμένες πλατφόρμες και υπηρεσίες διανέμουν τα δεδομένα σε πολλαπλούς κόμβους, μειώνοντας τον κίνδυνο ενός μοναδικού σημείου αποτυχίας και ενισχύοντας την προστασία της ιδιωτικής ζωής των δεδομένων. Η εκμάθηση της χρήσης αποκεντρωμένων πλατφορμών δίνει στα άτομα τη δυνατότητα μεγαλύτερου ελέγχου των δεδομένων τους, καθώς ελαχιστοποιεί την εξάρτηση από κεντρικές οντότητες, μετριάζει τους κινδύνους για την προστασία της ιδιωτικής ζωής και προάγει ένα πιο ασφαλές και ιδιωτικό ψηφιακό περιβάλλον.

77. Ενσωμάτωση καινοτόμων προσεγγίσεων για τη διασφάλιση των προσωπικών δεδομένων στις αναδυόμενες τεχνολογίες.	L8	A	Η πρωτοπορία σε καινοτόμες προσεγγίσεις για τη διασφάλιση των προσωπικών δεδομένων στις αναδυόμενες τεχνολογίες απαιτεί προληπτικές προσπάθειες για την ενσωμάτωση των αρχών της προστασίας της ιδιωτικής ζωής μέσω του σχεδιασμού, την εφαρμογή ισχυρών τεχνικών κρυπτογράφησης και τη διασφάλιση ότι η προστασία των δεδομένων αποτελεί προτεραιότητα κατά την ανάπτυξη νέων τεχνολογιών. Με την υιοθέτηση στρατηγικών με προνοητική σκέψη, μπορούμε να αντιμετωπίσουμε τις μοναδικές προκλήσεις που θέτουν οι αναδυόμενες τεχνολογίες και να υποστηρίξουμε την προστασία της ιδιωτικής ζωής των δεδομένων ως θεμελιώδη πτυχή των ψηφιακών εξελίξεων.
78. Ανάπτυξη ολοκληρωμένου σχεδίου ευαισθητοποίησης στον κυβερνοχώρο για την προστασία των προσωπικών δεδομένων.	L8	A	Αναπτύξτε ένα ολοκληρωμένο σχέδιο ευαισθητοποίησης στον κυβερνοχώρο για την προστασία των προσωπικών δεδομένων, εκπαιδεύοντας τα άτομα σχετικά με τις συνήθεις απειλές στον κυβερνοχώρο, προωθώντας ισχυρές πρακτικές χρήσης κωδικών πρόσβασης, ευαισθητοποιώντας τα άτομα σχετικά με το phishing και την κοινωνική μηχανική, ενθαρρύνοντας την τακτική ενημέρωση του λογισμικού και τονίζοντας τη σημασία του απορρήτου των δεδομένων σε όλες τις διαδικτυακές δραστηριότητες. Η εφαρμογή αυτού του σχεδίου θα δώσει τη δυνατότητα στα άτομα να προστατεύουν προληπτικά τα προσωπικά τους δεδομένα και θα συμβάλει σε ένα ασφαλέστερο διαδικτυακό περιβάλλον.
79. Μάθετε την έννοια της "άμυνας σε βάθος" στην κυβερνοασφάλεια και εκτιμήστε τη σημασία της εφαρμογής πολλαπλών επιπέδων ασφάλειας.	L8	K - S - A	Η "άμυνα σε βάθος" στην κυβερνοασφάλεια αναφέρεται στη στρατηγική της εφαρμογής πολλαπλών επιπέδων μέτρων ασφαλείας για την προστασία από διάφορους τύπους απειλών στον κυβερνοχώρο. Εκτιμώντας τη σημασία αυτών των στρωμάτων, όπως τα τείχη προστασίας, το λογισμικό προστασίας από ιούς, η κρυπτογράφηση και οι έλεγχοι πρόσβασης, τα άτομα και οι οργανισμοί μπορούν να ενισχύσουν σημαντικά τη συνολική τους θέση στον κυβερνοχώρο και να προστατεύσουν καλύτερα τα ευαίσθητα δεδομένα από πιθανές παραβιάσεις.
80. Υποστηρίξτε τον τρόπο με τον οποίο υποστηρίζεται η ενίσχυση της προστασίας της ιδιωτικής ζωής των δεδομένων και των ηθικών ψηφιακών πρακτικών.	L8	A	Η πρωτοπορία στην υπεράσπιση ισχυρότερης προστασίας της ιδιωτικής ζωής των δεδομένων και ηθικών ψηφιακών πρακτικών περιλαμβάνει την ενεργή προώθηση της ευαισθητοποίησης σχετικά με τη σημασία της ιδιωτικής ζωής των δεδομένων, την υποστήριξη της εφαρμογής ισχυρών κανονισμών για την προστασία της ιδιωτικής ζωής και τη δημιουργία θετικού παραδείγματος με την τήρηση ηθικών προτύπων στις διαδικτυακές δραστηριότητες. Με την υπεράσπιση αυτών των πρωτοβουλιών, μπορούμε να δημιουργήσουμε ένα ασφαλέστερο και πιο σεβαστό ψηφιακό περιβάλλον τόσο για τα άτομα όσο και για τους οργανισμούς.

Συντονιστής έργου:

EdiTC EDUCATION & INFORMATION TECHNOLOGY CENTRE

Συνεργάτες:

DIMITRA educational organization

UNIVERSITAS GALATIENSIS

CYPRUS COMPUTER SOCIETY

MMC Mediterranean Management Centre

UNIVERSITÀ TELEMATICA INTERNAZIONALE UNINETTUNO

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University

DSW DIGITAL SKILLS WALLET

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.