# ΜΙΚΡΟΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

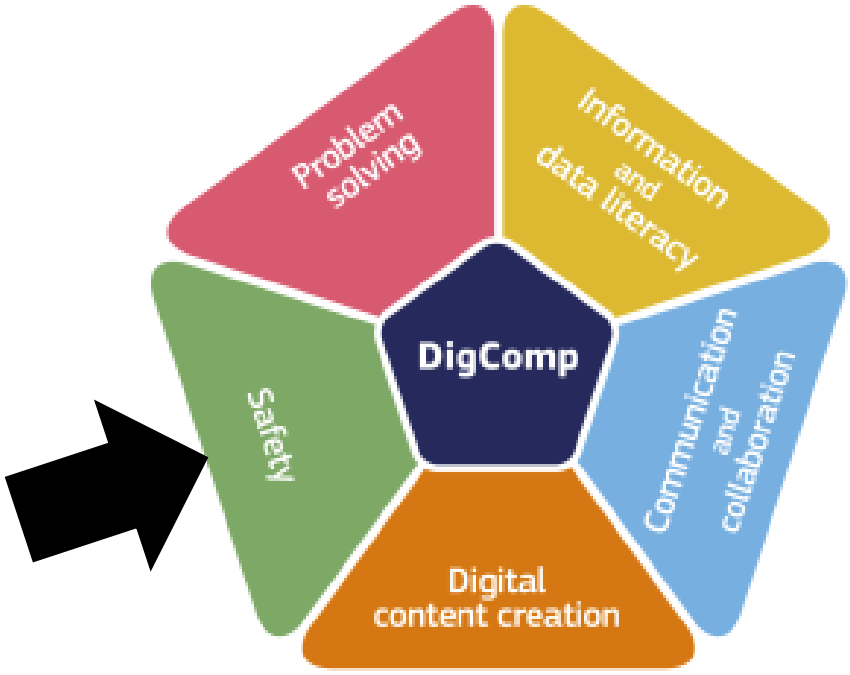
## Ικανότητα 4.1:

## ΠΡΟΣΤΑΣΙΑ ΣΥΣΚΕΥΩΝ

DSW
DIGITAL SKILLS WALLET

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

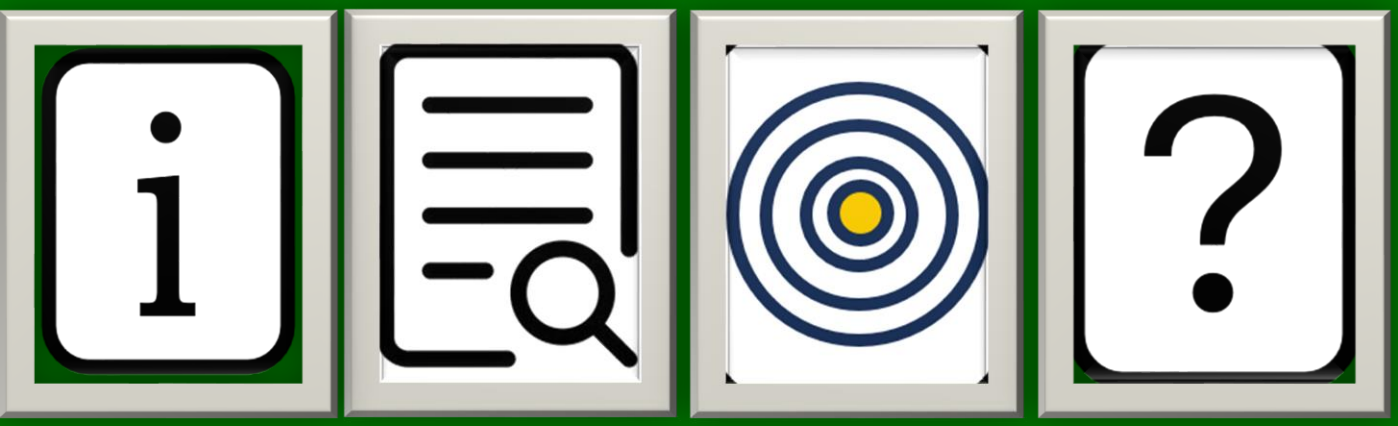
Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και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



# Βασικά στοιχεία ψηφιακής ασφάλειας (MC 4.1.A.1)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Βασικά στοιχεία ψηφιακής ασφάλειας<br>Κωδ: A.1.A.1 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16 - 20<br>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 4.1.1 και 4.1.3):

Ασφαλής ψηφιακή πρακτική

- Αναγνωρίστε τη σημασία της χρήσης μοναδικών κωδικών πρόσβασης για διαφορετικούς διαδικτυακούς λογαριασμούς για την ενίσχυση της ασφάλειας.
- Αναγνωρίστε τα κοινά σημάδια των προσπαθειών phishing και μάθετε πώς να αποφύγετε να πέσετε θύμα τέτοιων απατών.

## Περιγραφή

Το Micro Credential "**Essentials of Digital Security**" είναι ένα αρχικό πρόγραμμα που έχει σχεδιαστεί σχολαστικά για να παρέχει στους εκπαιδευόμενους μια σε βάθος κατανόηση και πρακτικές δεξιότητες στην ψηφιακή ασφάλεια. Υποστηριζόμενο από επαγγελματίες της κυβερνοασφάλειας παγκοσμίως, το μάθημα αυτό έχει δεσμευτεί να διδάξει βασικά μέτρα για τη διατήρηση της ακεραιότητας της ψηφιακής ταυτότητας και των περιουσιακών στοιχείων του ατόμου, από τη χρήση μοναδικών κωδικών πρόσβασης έως την ανίχνευση και αποφυγή του phishing.

Το πρόγραμμα ξεκινά με έμφαση στην ασφάλεια των κωδικών πρόσβασης, ένα κρίσιμο αλλά συχνά παραγνωρισμένο στοιχείο της ψηφιακής ασφάλειας. Οι εκπαιδευόμενοι θα κατανοήσουν την ουσία της δημιουργίας ισχυρών, μοναδικών κωδικών πρόσβασης για κάθε έναν από τους διαδικτυακούς λογαριασμούς τους, γεγονός που μειώνει τον κίνδυνο παραβίασης πολλαπλών λογαριασμών σε περίπτωση παραβίασης του ενός. Το μάθημα προσφέρει πρακτικές ασκήσεις για τον σχεδιασμό κωδικών πρόσβασης που εξισορροπούν την απομνημόνευση και την πολυπλοκότητα, αξιοποιώντας βέλτιστες πρακτικές όπως η χρήση διαχειριστών κωδικών πρόσβασης και ο έλεγχος ταυτότητας πολλαπλών παραγόντων για ένα επιπλέον επίπεδο ασφάλειας.

Από την ασφάλεια των κωδικών πρόσβασης, το μάθημα περνά στη σφαίρα της ανίχνευσης και της αποφυγής του phishing. Οι εκπαιδευόμενοι εισάγονται στην έννοια του phishing - παραπλανητικές προσπάθειες απόκτησης ευαίσθητων πληροφοριών προσποιούμενοι ότι είναι μια αξιόπιστη οντότητα. Μαθαίνουν να αναγνωρίζουν κοινές τακτικές phishing, όπως απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα ή ιστότοπους. Το μάθημα παρέχει ένα ασφαλές, προσομοιωμένο περιβάλλον όπου οι εκπαιδευόμενοι μπορούν να εξασκηθούν στην αναγνώριση και την αντίδραση σε απόπειρες phishing, ενισχύοντας έτσι την εμπειρία μάθησης.

Επιπλέον, το μάθημα καλύπτει πρόσθετες πτυχές της ψηφιακής ασφάλειας, συμπεριλαμβανομένης της κατανόησης των κινδύνων των μη ασφαλών δικτύων, της σημασίας της τακτικής ενημέρωσης του λογισμικού για την επιδιόρθωση των τρωτών σημείων ασφαλείας και της χρήσης της κρυπτογράφησης για την ασφαλή μετάδοση δεδομένων. Δίνει επίσης έμφαση στις συνήθειες ασφαλούς περιήγησης, όπως η επαλήθευση των πιστοποιητικών ασφαλείας των ιστότοπων και η αποφυγή λήψεων από μη επαληθευμένες πηγές.

Το πρόγραμμα κορυφώνεται με σενάρια πραγματικού κόσμου όπου οι μαθητές μπορούν να εφαρμόσουν τις έννοιες που έχουν μάθει, παρέχοντας ένα πρακτικό μέτρο της κατανόησης και της ετοιμότητάς τους. Οι αξιολογήσεις είναι σχεδιασμένες έτσι ώστε να μιμούνται τις ψηφιακές απειλές που μπορεί να αντιμετωπίσουν οι εκπαιδευόμενοι στην καθημερινή τους ζωή, βοηθώντας τους να κατανοήσουν πώς να αντιδράσουν κατάλληλα και να διαφυλάξουν την ψηφιακή τους ασφάλεια.

Με την επιτυχή ολοκλήρωση του προγράμματος, οι εκπαιδευόμενοι λαμβάνουν το Micro Credential "Essentials of Digital Security", μια αναγνώριση της ικανότητάς τους στην προστασία της ψηφιακής τους ταυτότητας και των περιουσιακών τους στοιχείων. Είτε είστε επαγγελματίας που επιθυμεί να ενισχύσει τις δεξιότητές του στην ψηφιακή ασφάλεια, είτε ένα άτομο που επιθυμεί να ενισχύσει την προσωπική του ασφάλεια στο διαδίκτυο, αυτό το πρόγραμμα παρέχει μια θεμελιώδη βάση γνώσεων και ένα σύνολο εργαλείων για την ενίσχυση της ψηφιακής ασφάλειας.
Αυτό το μικροπιστοποιητικό ευθυγραμμίζεται με τη δέσμευση της ΕΕ να ενισχύσει τις ψηφιακές δεξιότητες των πολιτών και την ευαισθητοποίηση τους σε θέματα διαδικτυακής ασφάλειας και εγκρίνεται ως ένα συμπαγές, συγκεκριμένο και ουσιαστικό

μαθησιακό επίτευγμα που αποδεικνύει τη γνώση βασικών πτυχών της ψηφιακής ασφάλειας.

## Ερωτήσεις

Μοναδικοί κωδικοί πρόσβασης για διαδικτυακούς λογαριασμούς

1. Εξηγήστε τις πιθανές συνέπειες της χρήσης του ίδιου κωδικού πρόσβασης για πολλούς διαδικτυακούς λογαριασμούς.
2. Πώς ενισχύει την ασφάλεια η χρήση μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό;
3. Ποιες είναι μερικές βέλτιστες πρακτικές για τη δημιουργία ενός ισχυρού, μοναδικού κωδικού πρόσβασης;
4. Συζητήστε το ρόλο των διαχειριστών κωδικών πρόσβασης στη διατήρηση μοναδικών κωδικών πρόσβασης. Είναι αποτελεσματικοί;

Επαγρύπνηση και επίγνωση του περιβάλλοντος

5. Περιγράψτε μια κατάσταση όπου η έλλειψη επίγνωσης του περιβάλλοντός σας θα μπορούσε να θέσει σε κίνδυνο την προσωπική σας ασφάλεια ή την ασφάλεια των ψηφιακών σας συσκευών.
6. Πώς θα μπορούσε η επαγρύπνηση να το αποτρέψει αυτό;
7. Μπορείτε να εξηγήσετε ορισμένες στρατηγικές για την αύξηση της επίγνωσης της κατάστασης, ιδίως σε δημόσιους χώρους;
8. Ποιες τεχνολογίες είναι διαθέσιμες για τη διατήρηση της επίγνωσης και της προσωπικής ασφάλειας;

Απόπειρες phishing και απάτες

9. Περιγράψτε τρεις συνήθεις ενδείξεις μιας απόπειρας phishing.
10. Εξηγήστε πώς να αντιδράσετε αν υποψιάζεστε ότι έχετε λάβει μήνυμα ή ηλεκτρονικό μήνυμα ηλεκτρονικού "ψαρέματος".
11. Ποια βήματα πρέπει να ακολουθήσετε αν πέσατε θύμα επίθεσης phishing;
12. Συζητήστε το ρόλο του ελέγχου ταυτότητας δύο παραγόντων (2FA) στην προστασία από το phishing.

Γενικά μέτρα ασφαλείας

13. Πώς μπορεί η γενική εκπαίδευση σχετικά με τις βέλτιστες πρακτικές ασφάλειας στον κυβερνοχώρο να ενισχύσει τόσο την προσωπική όσο και τη συλλογική ψηφιακή ασφάλεια;

# Βασική ευαισθητοποίηση σε θέματα ασφάλειας στον κυβερνοχώρο και προσωπικής ασφάλειας (MC 4.1.A.2)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Βασική ευαισθητοποίηση σε θέματα κυβερνοασφάλειας και προσωπικής ασφάλειας<br>Κωδ: A.2: MC 4.1.A.2 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16 - 20<br>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 4.1.2 και 4.1.4):

Ψηφιακή επαγρύπνηση

1. Αναγνωρίστε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα ή ιστότοπους που μπορεί να προσπαθήσουν να σας εξαπατήσουν ώστε να αποκαλύψετε προσωπικές πληροφορίες ή διαπιστευτήρια σύνδεσης.

Περιβαλλοντική ευαισθητοποίηση

2. Διατηρήστε μια στάση επαγρύπνησης και επίγνωσης του περιβάλλοντός σας.

## Περιγραφή

Το Micro Credential "**Basic Cybersecurity and Personal Safety Awareness**" είναι ένα καινοτόμο πρόγραμμα που ενσωματώνει την εκπαίδευση σε θέματα ψηφιακής ασφάλειας με την ευαισθητοποίηση σε θέματα προσωπικής ασφάλειας. Αυτό το ξεχωριστό μάθημα, το οποίο σχεδιάστηκε από ειδικούς σε θέματα κυβερνοασφάλειας και προσωπικής ασφάλειας, έχει ως στόχο να μεταδώσει στους εκπαιδευόμενους μια ολοκληρωμένη κατανόηση τόσο των ψηφιακών απειλών όσο και των πραγματικών ζητημάτων ασφάλειας.

Στον τομέα της κυβερνοασφάλειας, το πρόγραμμα παρέχει μια ολοκληρωμένη εισαγωγή στο τοπίο των ψηφιακών απειλών. Το μάθημα βοηθά τους εκπαιδευόμενους να διακρίνουν πιθανές απειλές στον κυβερνοχώρο, όπως ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, παραπλανητικά μηνύματα και κακόβουλους ιστότοπους. Οι συμμετέχοντες θα εξερευνήσουν διάφορους τύπους κακόβουλου λογισμικού, απάτες phishing και επιθέσεις κοινωνικής μηχανικής, μαθαίνοντας να αναγνωρίζουν τα προδηλωτικά σημάδια τέτοιων απειλών και πώς να αντιδρούν κατάλληλα. Το πρόγραμμα εμβαθύνει επίσης στις συνήθειες ασφαλούς περιήγησης, στις πρακτικές ασφαλούς επικοινωνίας και στην υπεύθυνη χρήση των κοινωνικών μέσων και των διαδικτυακών πλατφορμών, εξοπλίζοντας τους εκπαιδευόμενους με τις απαραίτητες γνώσεις για να περιηγηθούν με ασφάλεια στον ψηφιακό κόσμο.

Όσον αφορά την προσωπική ασφάλεια, το μάθημα προάγει μια έντονη αίσθηση της επίγνωσης του περιβάλλοντος. Αυτό περιλαμβάνει την εκπαίδευση σε τεχνικές επίγνωσης της κατάστασης που είναι ζωτικής σημασίας για την προσωπική ασφάλεια σε διάφορα περιβάλλοντα, είτε πρόκειται για δημόσιους χώρους, είτε για την εργασία, είτε ακόμη και για το σπίτι. Το μάθημα προσφέρει πρακτικές συμβουλές σχετικά με τον τρόπο εντοπισμού και αποφυγής δυνητικά επικίνδυνων καταστάσεων, καθώς και τεχνικές για την αποκλιμάκωση των καταστάσεων και την προστασία του εαυτού του όταν βρίσκεται αντιμέτωπος με μια απειλή. Το πρόγραμμα υπογραμμίζει τη σύνδεση μεταξύ της ψηφιακής ασφάλειας και της προσωπικής ασφάλειας, καταδεικνύοντας πώς η βελτίωση των διαδικτυακών συνηθειών μπορεί να μειώσει τις ευπάθειες στον πραγματικό κόσμο.

Το τελικό μέρος του προγράμματος περιλαμβάνει μια σειρά πρακτικών ασκήσεων και πραγματικών σεναρίων, όπου οι εκπαιδευόμενοι μπορούν να εφαρμόσουν τις νέες γνώσεις τους για την ασφάλεια στον κυβερνοχώρο και την προσωπική ασφάλεια. Αυτές οι αξιολογήσεις, προσεκτικά σχεδιασμένες ώστε να μιμούνται καταστάσεις του πραγματικού κόσμου, παρέχουν στους εκπαιδευόμενους μια πρακτική ευκαιρία να δοκιμάσουν τις δεξιότητές τους και να ενισχύσουν τη μάθησή τους.

Με την επιτυχή ολοκλήρωση του μαθήματος, οι εκπαιδευόμενοι θα αποκτήσουν το Πιστοποιητικό Micro Credential "Cybersecurity and Personal Safety Awareness". Αυτό το επίτευγμα σηματοδοτεί την ικανότητά τους στον εντοπισμό και τον μετριασμό πιθανών ψηφιακών απειλών, καθώς και την ενισχυμένη κατανόηση των αρχών και πρακτικών προσωπικής ασφάλειας.

Το πρόγραμμα Micro Credential "Basic Cybersecurity and Personal Safety Awareness" υιοθετεί μια μαθητοκεντρική προσέγγιση, προσαρμόζοντας το ρυθμό του μαθήματος στις ανάγκες του κάθε μαθητή και διασφαλίζοντας ότι όλοι, ανεξάρτητα από το επίπεδο της τεχνικής τους εμπειρίας, μπορούν να παρακολουθήσουν και να αποκομίσουν τη μέγιστη δυνατή αξία από το μάθημα.

Στο τμήμα του μαθήματος για την ασφάλεια στον κυβερνοχώρο, το πρόγραμμα παρέχει μια βαθιά εμβάθυνση σε διάφορα είδη διαδικτυακών απειλών. Για παράδειγμα, οι εκπαιδευόμενοι κατανοούν σε βάθος το κακόβουλο λογισμικό - τις μορφές του, τον τρόπο λειτουργίας του και τις πιθανές ζημιές που μπορεί να προκαλέσει. Μαθαίνουν επίσης για τις επιθέσεις phishing, οι οποίες εξαπατούν τους χρήστες ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, και πώς να εντοπίζουν και να αποφεύγουν να πέφτουν θύματα τέτοιων απατών. Το μάθημα εξοικειώνει επίσης τους εκπαιδευόμενους με την έννοια των επιθέσεων κοινωνικής μηχανικής, οι οποίες εκμεταλλεύονται την ανθρώπινη ψυχολογία για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα ή συστήματα. Το μάθημα δίνει ιδιαίτερη έμφαση στην πρακτική γνώση και υιοθετεί μια πρακτική προσέγγιση, με τους εκπαιδευόμενους να εξασκούν τις δεξιότητές τους σε προσομοιωμένα περιβάλλοντα.

Παράλληλα με την εκπαίδευση για την ασφάλεια στον κυβερνοχώρο, το πρόγραμμα παρέχει στους εκπαιδευόμενους ζωτικής σημασίας εκπαίδευση για την προσωπική ασφάλεια. Αυτό περιλαμβάνει την επίγνωση της κατάστασης - να έχει κανείς επίγνωση του περιβάλλοντός του και να εντοπίζει πιθανές απειλές. Το μάθημα παρουσιάζει διάφορα σενάρια από την πραγματική ζωή για να βοηθήσει τους εκπαιδευόμενους να κατανοήσουν τους πιθανούς κινδύνους και πώς να αποφεύγουν ή να χειρίζονται τέτοιες καταστάσεις. Δίνεται έμφαση στην καλλιέργεια μιας γενικής στάσης επαγρύπνησης και στη λήψη προληπτικών μέτρων για τη διασφάλιση της προσωπικής ασφάλειας.

Το μάθημα διανθίζεται με αξιολογήσεις για να διασφαλιστεί ότι οι εκπαιδευόμενοι κατανοούν και μπορούν να εφαρμόσουν τις έννοιες που έχουν μάθει. Αυτές οι αξιολογήσεις μιμούνται πραγματικές καταστάσεις, βοηθώντας τους εκπαιδευόμενους να προετοιμαστούν για το είδος των απειλών που μπορεί να αντιμετωπίσουν στην καθημερινή τους ζωή, τόσο online όσο και offline.

Πέρα από τον εξοπλισμό των μαθητών με κρίσιμες δεξιότητες κυβερνοασφάλειας και προσωπικής ασφάλειας, το πρόγραμμα επιδιώκει επίσης να εμφυσήσει μια κουλτούρα συνεχούς μάθησης. Το τοπίο των ψηφιακών απειλών εξελίσσεται διαρκώς και νέες προκλήσεις προσωπικής ασφάλειας εμφανίζονται τακτικά. Ως εκ τούτου, το πρόγραμμα ενθαρρύνει τους εκπαιδευόμενους να ενημερώνονται για τις τελευταίες εξελίξεις και στους δύο τομείς, διασφαλίζοντας ότι οι δεξιότητές τους παραμένουν επίκαιρες μπροστά στις νέες απειλές.
Με άλλα λόγια, το Micro Credential "Cybersecurity and Personal Safety Awareness" δεν αφορά απλώς θεωρητικές γνώσεις, αλλά την εμπέδωση μιας νοοτροπίας επαγρύπνησης, τόσο online όσο και offline. Απευθύνεται σε όλους όσους επιθυμούν να βελτιώσουν τη στάση τους στον τομέα της ψηφιακής ασφάλειας και της ευαισθητοποίησης σε θέματα προσωπικής ασφάλειας, συμπεριλαμβανομένων των επαγγελματιών, των φοιτητών και των καθημερινών χρηστών του Διαδικτύου.

Εν κατακλείδι, το πρόγραμμα Micro Credential "Basic Cybersecurity and Personal Safety Awareness" είναι ένα ολιστικό μαθησιακό ταξίδι που ενδυναμώνει τους εκπαιδευόμενους με βασικές δεξιότητες για την πλοήγηση στον σύγχρονο, διασυνδεδεμένο κόσμο. Είτε είστε επαγγελματίας στον τομέα της κυβερνοασφάλειας που επιθυμεί να ενισχύσει τις δεξιότητές του σε θέματα προσωπικής ασφάλειας, είτε ένα άτομο που επιθυμεί να ενισχύσει την κατανόηση των ψηφιακών απειλών και της προσωπικής ασφάλειας, αυτό το πρόγραμμα παρέχει τις γνώσεις και τα εργαλεία που είναι απαραίτητα για να βελτιώσετε τη στάση ασφαλείας σας τόσο online όσο και offline.

Αυτό το μικροπιστοποιητικό ευθυγραμμίζεται με τη δέσμευση της Ευρωπαϊκής Ένωσης να ενισχύσει τις ψηφιακές ικανότητες και να προωθήσει την προσωπική ασφάλεια των πολιτών της. Παρέχει μια πιστοποιημένη μαρτυρία της αρχικής κυριαρχίας του εκπαιδευόμενου σε αυτούς τους ζωτικούς τομείς της ασφάλειας και της προστασίας.

## Ερωτήσεις

Ψηφιακή επαγρύπνηση

1. Ποια είναι τρία κοινά χαρακτηριστικά ενός ύποπτου ηλεκτρονικού ταχυδρομείου ή μηνύματος που μπορεί να προσπαθεί να σας εξαπατήσει ώστε να αποκαλύψετε προσωπικές πληροφορίες ή διαπιστευτήρια σύνδεσης; Πώς θα αντιμετωπίζατε μια τέτοια κατάσταση;
2. Ποιες είναι μερικές επιπλέον κόκκινες σημαίες που πρέπει να προσέξετε σε πιθανά δόλια μηνύματα ή ιστότοπους;
3. Περιγράψτε το ρόλο των τειχών προστασίας και του λογισμικού προστασίας από ιούς στην ενίσχυση της ψηφιακής επαγρύπνησης.
4. Πόσο σημαντικό είναι να ενημερώνετε τακτικά το λογισμικό σας για τη διατήρηση της ψηφιακής ασφάλειας;
5. Εξηγήστε πώς ο έλεγχος ταυτότητας πολλαπλών παραγόντων μπορεί να χρησιμεύσει ως πρόσθετο επίπεδο

προστασίας από μη εξουσιοδοτημένη πρόσβαση στους λογαριασμούς σας.

Περιβαλλοντική ευαισθητοποίηση

6. Περιγράψτε μια κατάσταση στην οποία η επίγνωση του περιβάλλοντός σας θα μπορούσε ενδεχομένως να αποτρέψει μια παραβίαση της ασφάλειας ή έναν κίνδυνο για την προσωπική σας ασφάλεια.
7. Ποια μέτρα μπορούν να ληφθούν για τη βελτίωση της περιβαλλοντικής ευαισθητοποίησης;
8. Πώς αντιλαμβάνεστε τα θέματα ασφάλειας προκειμένου να συμβάλλετε σε ένα ασφαλέστερο περιβάλλον;
9. Ελλείψει τεχνολογίας, ποιες βασικές πρακτικές μπορείτε να ακολουθήσετε για να διασφαλίσετε ότι έχετε επίγνωση του περιβάλλοντός σας;
10. Ποιες είναι ορισμένες περιβαλλοντικές ενδείξεις που μπορεί να υποδηλώνουν πιθανό κίνδυνο για την ασφάλεια;

Συνδυασμός και των δύο

11. Φανταστείτε ότι λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου στο τηλέφωνό σας ενώ βρίσκεστε σε μια καφετέρια με πολλή κίνηση, το οποίο σας ζητά να επικυρώσετε αμέσως τα διαπιστευτήρια σύνδεσής σας για τον τραπεζικό σας λογαριασμό. Ποιες ενέργειες θα κάνατε σε αυτό το σενάριο, λαμβάνοντας υπόψη τόσο την ψηφιακή επαγρύπνηση όσο και την περιβαλλοντική ευαισθητοποίηση;
12. Πώς θα διέφερε η αντίδρασή σας αν λαμβάνατε το ίδιο ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου ενώ βρισκόσασταν σε ιδιωτικό περιβάλλον;
13. Ποιοι είναι μερικοί από τους πιθανούς κινδύνους της πρόσβασης σε προσωπικούς λογαριασμούς μέσω δημόσιου Wi-Fi; Πώς μπορούν να μετριαστούν αυτοί οι κίνδυνοι;

Γενικές ερωτήσεις

14. Πώς μπορούν οι οργανισμοί να διαδραματίσουν ρόλο στην εκπαίδευση των ατόμων σχετικά με την ψηφιακή επαγρύπνηση και την περιβαλλοντική ευαισθητοποίηση;
15. Ποια είναι τα οφέλη του συνδυασμού της ψηφιακής επαγρύπνησης και της περιβαλλοντικής ευαισθητοποίησης σε μια ολοκληρωμένη στρατηγική ασφάλειας;

# Βασικά στοιχεία ψηφιακής ασφάλειας και προστασίας προσωπικών δεδομένων (MC 4.1.A.3)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος του μικροπιστοποιητικού | Ψηφιακή ασφάλεια και ιδιωτικότητα<br>Βασικά στοιχεία<br>**Κωδ: A.3: MC 4.1.A.3** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.5, 4.1.6 και 4.1.7):
Ασφάλεια συσκευής

1. Εφαρμόστε τη δεξιότητα να ασφαλίζετε τη συσκευή σας όταν είναι αφύλακτη.

Ασφάλεια δικτύου

2. Περιγράψτε τη σημασία της διασφάλισης του οικιακού σας δικτύου με ισχυρούς κωδικούς πρόσβασης και πρωτόκολλα κρυπτογράφησης.

Δημόσια ασφάλεια Wi-Fi

3. Προσδιορίστε τους κινδύνους που συνδέονται με τη χρήση δημόσιων δικτύων Wi-Fi.

## Περιγραφή

Το Micro Credential "**Digital Security and Privacy Essential**" είναι ένα εντατικά σχεδιασμένο πρόγραμμα που έχει εγκριθεί από την Ευρωπαϊκή Επιτροπή και στοχεύει στην ενδυνάμωση των εκπαιδευομένων με μια ολιστική κατανόηση των μέτρων ψηφιακής ασφάλειας και των αρχών προστασίας της ιδιωτικής ζωής. Αυτό το ολοκληρωμένο πρόγραμμα είναι δομημένο γύρω από τρεις πρωταρχικούς πυλώνες της ψηφιακής ασφάλειας και της ιδιωτικότητας - την ασφάλεια φυσικών συσκευών, την ασφάλεια οικιακών δικτύων και την ασφαλή χρήση δημόσιων δικτύων Wi-Fi.

Το ταξίδι αυτού του μικροπιστοποιητικού ξεκινά με έμφαση στην ασφάλεια των φυσικών συσκευών. Ως μείγμα θεωρίας και πρακτικής, αυτό το τμήμα δίνει τη δυνατότητα στους εκπαιδευόμενους να αποκτήσουν τις απαραίτητες δεξιότητες για την ασφάλεια συσκευών χωρίς επιτήρηση και να εξοικειωθούν με μια σειρά μηχανισμών κλειδώματος, βιομετρικών συστημάτων και άλλων χαρακτηριστικών ασφαλείας συγκεκριμένων συσκευών. Επισημαίνει ότι τα θεμέλια της ασφάλειας των συσκευών εδράζονται σε μεγάλο βαθμό σε πρακτικές προφυλάξεις και πρακτικές, οι οποίες μπορούν να αποτρέψουν αποτελεσματικά τη μη εξουσιοδοτημένη φυσική πρόσβαση.

Στη συνέχεια, το μάθημα κατευθύνει τους εκπαιδευόμενους προς την ασφάλεια του οικιακού δικτύου. Σε αυτή την ενότητα, οι εκπαιδευόμενοι περιηγούνται στις περίπλοκες πτυχές της εγκατάστασης και διαχείρισης ενός ασφαλούς οικιακού δικτύου. Οι εκπαιδευόμενοι εμβαθύνουν σε έννοιες όπως η εφαρμογή ισχυρών, μοναδικών κωδικών πρόσβασης και η χρήση πρωτοποριακών πρωτοκόλλων κρυπτογράφησης. Αυτή η ενότητα προσφέρει στους εκπαιδευόμενους μια πρακτική, πρακτική εμπειρία, εξοπλίζοντάς τους με ανεκτίμητες γνώσεις που μπορούν να εφαρμόσουν για την ασφάλεια των οικιακών τους δικτύων στην καθημερινή τους ζωή.

Ο τρίτος ακρογωνιαίος λίθος του μαθήματος επικεντρώνεται γύρω από τους πιθανούς κινδύνους ασφαλείας που εγκυμονούν τα δημόσια δίκτυα Wi-Fi. Παρά την ευρέως διαδεδομένη χρήση και την ευκολία τους, τα δημόσια δίκτυα Wi-Fi παρουσιάζουν σημαντικές προκλήσεις για την ασφάλεια. Σε αυτή την ενότητα, οι εκπαιδευόμενοι θα αποκτήσουν γνώσεις σχετικά με αυτούς τους κινδύνους και θα κατανοήσουν πώς μπορούν να υποκλαπούν ή να χειραγωγηθούν δεδομένα κατά τη χρήση τέτοιων δικτύων. Για να εξοπλίσουν τους εκπαιδευόμενους με άμυνες απέναντι σε αυτές τις πιθανές απειλές, καθοδηγούνται μέσω διαφόρων στρατηγικών για ασφαλή χρήση, συμπεριλαμβανομένης της χρήσης VPN (Virtual Private Networks), της επαλήθευσης της αυθεντικότητας του δικτύου και της αποφυγής ευαίσθητων δραστηριοτήτων κατά τη σύνδεση σε δημόσιο Wi-Fi.

Το τελικό στάδιο του προγράμματος προσφέρει στους εκπαιδευόμενους την ευκαιρία να δοκιμάσουν τις δεξιότητές τους σε πρακτικά, πραγματικά σενάρια. Αξιολογούνται με βάση την ικανότητά τους να εφαρμόζουν τις γνώσεις και τις δεξιότητες που απέκτησαν για την αποτελεσματική ασφάλεια ψηφιακών συσκευών και δικτύων, παρέχοντάς τους ένα συγκεκριμένο μέτρο της μάθησης και της προόδου τους.

Με την επιτυχή ολοκλήρωση του προγράμματος, οι εκπαιδευόμενοι αποκτούν το Micro Credential "Digital Security and Privacy Essential". Αυτή η υψηλού κύρους αναγνώριση αποτελεί απόδειξη της ολοκληρωμένης κατανόησης της ψηφιακής ασφάλειας και ιδιωτικότητας και της ικανότητάς τους να εφαρμόζουν αυτές τις γνώσεις για την ασφάλεια του ψηφιακού τους τοπίου.

Εν κατακλείδι, το Micro Credential "Digital Security and Privacy Essential" υπερβαίνει την απλή θεωρητική γνώση. Εξοπλίζει τους εκπαιδευόμενους με πρακτικές, εφαρμόσιμες δεξιότητες στον τομέα της ψηφιακής ασφάλειας και της ιδιωτικότητας. Απευθύνεται σε ένα ευρύ κοινό, από επαγγελματίες που επιθυμούν να ενισχύσουν την κατανόηση της ψηφιακής ασφάλειας μέχρι καθημερινούς χρήστες που στοχεύουν να ενισχύσουν την ασφάλεια του ψηφιακού τους περιβάλλοντος. Αυτό το Micro Credential συνάδει με τις πρωτοβουλίες της Ευρωπαϊκής Ένωσης για την ενίσχυση του ψηφιακού αλφαβητισμού και της ασφάλειας των πολιτών της, παρέχοντας ένα επικυρωμένο επίτευγμα που πιστοποιεί την επάρκεια στην ψηφιακή ασφάλεια και την ιδιωτικότητα.

## Ερωτήσεις

Ασφάλεια συσκευής:

1. Φανταστείτε ότι πρέπει να αφήσετε το φορητό σας υπολογιστή χωρίς επίβλεψη σε μια δημόσια βιβλιοθήκη για λίγα λεπτά. Ποια μέτρα θα λαμβάνατε για να ασφαλίσετε τη συσκευή σας κατά τη διάρκεια αυτής της περιόδου;

Ασφάλεια δικτύου:

2. Εξηγήστε γιατί είναι σημαντικό να ασφαλίζετε το οικιακό σας δίκτυο με ισχυρούς κωδικούς πρόσβασης και πρωτόκολλα κρυπτογράφησης. Μπορείτε να περιγράψετε τη διαδικασία εγκατάστασης τέτοιων μέτρων ασφαλείας σε έναν οικιακό δρομολογητή;

Δημόσια ασφάλεια Wi-Fi:

3. Ποιοι είναι ορισμένοι πιθανοί κίνδυνοι από τη χρήση δημόσιων δικτύων Wi-Fi και πώς μπορείτε να μετριάσετε αυτούς τους κινδύνους για να χρησιμοποιείτε με ασφάλεια αυτά τα δίκτυα;

Ένας συνδυασμός όλων:

4. Ας υποθέσουμε ότι εργάζεστε από μια καφετέρια χρησιμοποιώντας το δημόσιο δίκτυο Wi-Fi. Συζητήστε τα βήματα που θα λαμβάνατε για να διασφαλίσετε την ασφάλεια τόσο της συσκευής σας όσο και των δεδομένων σας σε αυτό το σενάριο.

# Διαχείριση ψηφιακού απορρήτου και κυβερνοασφάλειας (MC 4.1.A.4)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Διαχείριση ψηφιακού απορρήτου και κυβερνοασφάλειας<br>Κωδ: A.4: MC 4.1.A.4 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.8, 4.1.9 και 4.1.10):

Ρυθμίσεις απορρήτου

1. Περιγράψτε πώς η αναθεώρηση και η προσαρμογή των ρυθμίσεων απορρήτου μπορεί να βοηθήσει στον έλεγχο των πληροφοριών που μοιράζονται σε συσκευές και διαδικτυακούς λογαριασμούς.

Ενημέρωση για την ασφάλεια στον κυβερνοχώρο

2. Απαριθμήστε τις πιθανές απειλές που δημιουργούν οι ψηφιακοί κίνδυνοι και τη σημασία της ενημέρωσης για τις βέλτιστες πρακτικές κυβερνοασφάλειας.

Διαχείριση απώλειας συσκευής

3. Περιγράψτε τα βήματα που πρέπει να ακολουθήσετε σε περίπτωση απώλειας ή κλοπής μιας συσκευής για τη διασφάλιση των προσωπικών δεδομένων και της ιδιωτικής ζωής.

## Περιγραφή

Το Micro Credential "**Digital Privacy and Cybersecurity Management**" είναι ένα εντατικό, πολύπλευρο πρόγραμμα. Έχει σχεδιαστεί για να καλλιεργήσει προηγμένες γνώσεις στη διαφύλαξη της ψηφιακής ιδιωτικότητας και την καταπολέμηση του πλήρους φάσματος των απειλών κυβερνοασφάλειας. Αυτό το αναγνωρισμένο από την Ευρωπαϊκή Επιτροπή μάθημα χαρτογραφεί ένα ολοκληρωμένο πρόγραμμα σπουδών σε τέσσερις κρίσιμους τομείς: γνώση των ρυθμίσεων απορρήτου της συσκευής και του διαδικτυακού λογαριασμού, κατανόηση των πιθανών ψηφιακών απειλών, ενημέρωση για τις βέλτιστες πρακτικές κυβερνοασφάλειας και επινόηση στρατηγικών για τη διασφάλιση των προσωπικών δεδομένων και της ιδιωτικής ζωής σε περιπτώσεις απώλειας ή κλοπής συσκευής.

Το μάθημα ξεκινά με την εξερεύνηση των ρυθμίσεων απορρήτου, παρέχοντας στους εκπαιδευόμενους μια εξαντλητική κατανόηση του τρόπου με τον οποίο αυτές οι ρυθμίσεις μπορούν να ρυθμιστούν στις συσκευές και τους διαδικτυακούς λογαριασμούς ώστε να ανταποκρίνονται στις ανάγκες τους. Με τη διερεύνηση πραγματικών σεναρίων, οι εκπαιδευόμενοι θα αποκτήσουν πρακτική εμπειρία στη διαχείριση αυτών των ρυθμίσεων, δίνοντας έμφαση στην ανάγκη περιοδικής αναθεώρησης και τροποποίησης για την αποτελεσματική αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα και την ενίσχυση της προστασίας της ιδιωτικής ζωής.

Από εκεί και πέρα, το μάθημα κάνει μια βαθιά βουτιά στον κόσμο των ψηφιακών απειλών. Αυτή η ενότητα εκθέτει τους εκπαιδευόμενους σε μια ευρεία ποικιλία κινδύνων κυβερνοασφάλειας - από συστήματα phishing μέχρι εξελιγμένες επιθέσεις κακόβουλου λογισμικού και τις ολοένα και πιο διαδεδομένες τακτικές κοινωνικής μηχανικής. Ο στόχος δεν είναι μόνο να αναγνωρίσουν αυτές τις απειλές, αλλά να κατανοήσουν τους μηχανισμούς τους και να επινοήσουν αποτελεσματικά αντίμετρα. Μελέτες περιπτώσεων σημαντικών ιστορικών παραβιάσεων της κυβερνοασφάλειας παρέχουν κατανόηση του πλαισίου και προσφέρουν πολύτιμα μαθήματα για τον μετριασμό των απειλών.

Η τρίτη ενότητα επικεντρώνεται στη διατήρηση των εκπαιδευομένων σε επαφή με τις τελευταίες βέλτιστες πρακτικές στον τομέα της κυβερνοασφάλειας. Αναγνωρίζοντας την ταχέως εξελισσόμενη φύση του ψηφιακού τοπίου, η ενότητα αυτή εξοπλίζει τους εκπαιδευόμενους με τις πιο σύγχρονες, αποτελεσματικές στρατηγικές για την ελαχιστοποίηση της ψηφιακής ευπάθειας. Θα μάθουν όχι μόνο για αυτές τις πρακτικές αλλά και θα κατανοήσουν πώς και πότε να τις εφαρμόζουν αποτελεσματικά, διασφαλίζοντας ότι τα ψηφιακά τους περιβάλλοντα παραμένουν ασφαλή.

Το τελευταίο μέρος του μαθήματος αφορά τις στρατηγικές για τη διατήρηση της ασφάλειας και του απορρήτου των προσωπικών δεδομένων σε περιπτώσεις απώλειας ή κλοπής της συσκευής. Παρέχοντας έναν πρακτικό οδηγό για τη χρήση λειτουργιών όπως η παρακολούθηση συσκευών, το απομακρυσμένο κλείδωμα και η διαγραφή δεδομένων, οι εκπαιδευόμενοι θα είναι εξοπλισμένοι για να αντιδρούν γρήγορα και αποτελεσματικά όταν αντιμετωπίζουν τέτοιες καταστάσεις.

Μετά την ολοκλήρωση των μαθημάτων, οι εκπαιδευόμενοι υποβάλλονται σε μια ολοκληρωμένη αξιολόγηση που έχει σχεδιαστεί για να ελέγξει την κατανόηση του υλικού που καλύφθηκε και την ικανότητά τους να εφαρμόζουν τις γνώσεις αυτές σε πρακτικές, πραγματικές καταστάσεις. Η επιτυχής ολοκλήρωση αυτής της αξιολόγησης ανταμείβει τους εκπαιδευόμενους με ένα αναγνωρισμένο Πιστοποιητικό Micro, το οποίο επικυρώνει τη νεοαποκτηθείσα τεχνογνωσία τους στη διαχείριση της ψηφιακής ιδιωτικότητας και της κυβερνοασφάλειας σύμφωνα με τα πρότυπα της Ευρωπαϊκής Επιτροπής.

Στην ουσία, το Micro Credential "Digital Privacy and Cybersecurity Management" παρέχει μια ολιστική εκπαίδευση στην ψηφιακή ιδιωτικότητα και ασφάλεια. Με το μείγμα θεωρητικών γνώσεων και πρακτικών εφαρμογών, το μάθημα είναι κατάλληλο για ένα ευρύ φάσμα εκπαιδευομένων - επαγγελματίες, φοιτητές και καθημερινούς χρήστες ψηφιακών συσκευών. Απώτερος στόχος του είναι να ενδυναμώσει τους συμμετέχοντες με τα εργαλεία και τις γνώσεις που απαιτούνται για να περιηγηθούν στον ψηφιακό κόσμο με αυτοπεποίθηση και ασφάλεια. Αυτό ευθυγραμμίζεται με τη δέσμευση της Ευρωπαϊκής Ένωσης για την προώθηση του ψηφιακού αλφαβητισμού και των ψηφιακών δεξιοτήτων των πολιτών της, προσφέροντας στους εκπαιδευόμενους ένα πιστοποιημένο επίτευγμα που επικυρώνει την επάρκειά τους στη διαχείριση της ψηφιακής ιδιωτικότητας και της κυβερνοασφάλειας.

## Ερωτήσεις

Ρυθμίσεις απορρήτου:

1. Μπορείτε να συζητήσετε τη σημασία της τακτικής επανεξέτασης και προσαρμογής των ρυθμίσεων απορρήτου σε συσκευές και διαδικτυακούς λογαριασμούς; Παρακαλείστε να δώσετε παραδείγματα των τύπων πληροφοριών που μπορείτε να ελέγξετε μέσω αυτών των ρυθμίσεων.

Ενημέρωση για την κυβερνοασφάλεια:

2. Ποιες είναι μερικές κοινές ψηφιακές απειλές που μπορεί να αντιμετωπίσει κανείς; Πώς μπορεί η ενημέρωση σχετικά με τις βέλτιστες πρακτικές κυβερνοασφάλειας να βοηθήσει στον μετριασμό αυτών των απειλών;

Διαχείριση απώλειας συσκευής:

3. Σε περίπτωση απώλειας ή κλοπής μιας συσκευής, ποια μέτρα πρέπει να λάβετε για να διασφαλίσετε την προστασία των προσωπικών σας δεδομένων και της ιδιωτικής σας ζωής; Παρακαλούμε περιγράψτε τη διαδικασία τόσο για μια συσκευή Android όσο και για μια συσκευή iOS.

Ένας συνδυασμός όλων:

4. Φανταστείτε ότι έχετε χάσει το smartphone σας, το οποίο περιέχει πολλούς λογαριασμούς μέσων κοινωνικής δικτύωσης και ηλεκτρονικού ταχυδρομείου. Περιγράψτε πώς η προηγούμενη κατανόηση των ρυθμίσεων απορρήτου και των βέλτιστων πρακτικών κυβερνοασφάλειας μπορεί να σας βοηθήσει σε αυτή την κατάσταση και σε ποιες άμεσες ενέργειες θα προβείτε για την προστασία των δεδομένων και της ιδιωτικής σας ζωής.

# Αρχές ασφαλούς χρήσης συσκευών και ψηφιακής συνεργασίας (MC 4.1.A.5)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Διαχείριση ψηφιακού απορρήτου και κυβερνοασφάλειας<br>**Κωδ: A.5** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.11, 4.1.12 και 4.1.13):

Διαχείριση υπηρεσιών δικτύου

1. Αναγνωρίστε τη σημασία της απενεργοποίησης των περιττών υπηρεσιών δικτύου και των προγραμμάτων παρασκηνίου στις συσκευές σας για να μειώσετε τις πιθανές επιφάνειες επιθέσεων.

Ασφάλεια φυσικών συσκευών

2. Προσέξτε την ασφάλεια των φυσικών συσκευών, ιδίως σε δημόσιους χώρους, για να αποτρέψετε την κλοπή και τη μη εξουσιοδοτημένη πρόσβαση.

Ασφαλής ψηφιακή συνεργασία

3. Εφαρμόστε ασφαλείς πρακτικές κοινής χρήσης οθόνης κατά τη διάρκεια εικονικών συσκέψεων ή απομακρυσμένων συνεργασιών για την προστασία ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση ή έκθεση.

## Περιγραφή

Το Micro Credential "Principles of Secure Device Use and Digital Collaboration" (Αρχές ασφαλούς χρήσης συσκευών και ψηφιακής συνεργασίας) είναι ένα σε βάθος μάθημα που έχει σχεδιαστεί για να ενδυναμώσει τους εκπαιδευόμενους με βασικές δεξιότητες για τη διατήρηση της ασφαλούς χρήσης συσκευών και την προώθηση της ασφάλειας κατά τη διάρκεια της ψηφιακής συνεργασίας. Το μάθημα πραγματεύεται τα κρίσιμα θέματα της διαχείρισης των υπηρεσιών δικτύου στις συσκευές, της διασφάλισης της φυσικής ασφάλειας των συσκευών, ιδίως σε δημόσιες τοποθεσίες, και της εφαρμογής ασφαλών πρακτικών κατά την κοινή χρήση οθόνης και την εικονική συνεργασία για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες.

Το μάθημα ξεκινά με την αντιμετώπιση της κρίσιμης πτυχής της διαχείρισης υπηρεσιών δικτύου σε συσκευές. Οι εκπαιδευόμενοι θα εμβαθύνουν στη σημασία της απενεργοποίησης των περιττών υπηρεσιών δικτύου και των προγραμμάτων παρασκηνίου στις συσκευές τους. Τα μέτρα αυτά μειώνουν τις πιθανές επιφάνειες επιθέσεων και ενισχύουν τη συνολική ασφάλεια των συσκευών. Σε αυτή την ενότητα, οι εκπαιδευόμενοι θα αποκτήσουν εικόνα για το πώς λειτουργούν οι υπηρεσίες δικτύου και γιατί η ελαχιστοποίησή τους είναι αναπόσπαστο στοιχείο για τη διατήρηση μιας ασφαλούς συσκευής.

Στη συνέχεια, το μάθημα εστιάζει στην ασφάλεια φυσικών συσκευών. Αυτή η ενότητα αναγνωρίζει ότι, παρά την επικράτηση των ψηφιακών απειλών, η φυσική ασφάλεια παραμένει βασικό στοιχείο της συνολικής ασφάλειας των συσκευών. Εδώ, οι εκπαιδευόμενοι θα εξερευνήσουν στρατηγικές για να διατηρούν τις συσκευές ασφαλείς σε δημόσιους χώρους, κατανοώντας ότι η πρόληψη της κλοπής και της μη εξουσιοδοτημένης φυσικής πρόσβασης είναι εξίσου σημαντική με την προστασία από εικονικές εισβολές.

Το τελευταίο μέρος του μαθήματος επικεντρώνεται στην ασφαλή ψηφιακή συνεργασία. Καθώς η απομακρυσμένη εργασία και οι εικονικές συνεργασίες γίνονται όλο και πιο συχνές, η κατανόηση του τρόπου προστασίας των ευαίσθητων πληροφοριών κατά τη διάρκεια αυτών των αλληλεπιδράσεων είναι ζωτικής σημασίας. Οι εκπαιδευόμενοι θα αποκτήσουν δεξιότητες για την εφαρμογή ασφαλών πρακτικών κοινής χρήσης οθόνης κατά τη διάρκεια εικονικών συναντήσεων ή απομακρυσμένων συνεργασιών. Θα κατανοήσουν πώς να διασφαλίζουν ότι εμφανίζονται μόνο οι απαραίτητες πληροφορίες και πώς να αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση ή την έκθεση ευαίσθητων δεδομένων.

Διανθισμένο με πρακτικές ασκήσεις και μάθηση βάσει σεναρίων, το μάθημα αυτό διασφαλίζει ότι οι δεξιότητες που διδάσκονται είναι σχετικές και εφαρμόσιμες σε πραγματικές συνθήκες. Οι συμμετέχοντες θα έχουν την ευκαιρία να επεξεργαστούν υποθετικές καταστάσεις που ενισχύουν τα μαθήματα και εδραιώνουν την κατανόησή τους.

Το Micro Credential ολοκληρώνεται με μια αξιολόγηση που πιστοποιεί την κατανόηση του περιεχομένου του μαθήματος από τους εκπαιδευόμενους. Οι επιτυχόντες εκπαιδευόμενοι θα αποκτήσουν Πιστοποιητικό Micro που πιστοποιεί την επάρκειά τους στην ασφαλή χρήση συσκευών και την ασφαλή ψηφιακή συνεργασία, μια πιστοποίηση που αναγνωρίζεται σύμφωνα με τα πρότυπα της Ευρωπαϊκής Επιτροπής.

Συνολικά, το Micro Credential "Principles of Secure Device Use and Digital Collaboration" προσφέρει ένα ολοκληρωμένο, πρακτικό και εφαρμόσιμο σύνολο δεξιοτήτων που εξοπλίζει τους εκπαιδευόμενους να περιηγηθούν στο ψηφιακό τοπίο με αυτοπεποίθηση και ασφάλεια. Αποτελεί ανεκτίμητο πόρο για απομακρυσμένους εργαζόμενους, ψηφιακούς νομάδες, φοιτητές και οποιονδήποτε συνεργάζεται ή επικοινωνεί συχνά ψηφιακά.

Σύμφωνα με τις πρωτοβουλίες της Ευρωπαϊκής Ένωσης για την ενίσχυση του ψηφιακού αλφαβητισμού και της ασφάλειας των πολιτών της, αυτό το Μικροπιστοποιητικό παρέχει μια επικυρωμένη απόδειξη της επάρκειας των εκπαιδευομένων στην ασφαλή χρήση των συσκευών τους και στη συμμετοχή τους σε ψηφιακή συνεργασία με έμφαση στην προστασία της ιδιωτικής ζωής και την ασφάλεια.

### Ερωτήσεις

Για τη διαχείριση υπηρεσιών δικτύου:

1. Γιατί είναι σημαντικό να απενεργοποιείτε τις περιττές υπηρεσίες δικτύου και τα προγράμματα παρασκηνίου στις συσκευές σας; Πώς συμβάλλει αυτή η πρακτική στη μείωση των πιθανών επιφανειών επίθεσης;

Για την ασφάλεια φυσικών συσκευών:

2. Περιγράψτε ορισμένες βέλτιστες πρακτικές για τη διασφάλιση της φυσικής ασφάλειας των συσκευών σας, ιδίως σε δημόσιους χώρους. Ποια μέτρα θα λαμβάνατε για να αποτρέψετε τη μη εξουσιοδοτημένη πρόσβαση ή κλοπή;

Για ασφαλή ψηφιακή συνεργασία:

3. Ποιες είναι μερικές από τις βέλτιστες πρακτικές για τη διασφάλιση του απορρήτου και της ασφάλειας των δεδομένων κατά την κοινή χρήση οθόνης σε εικονικές συσκέψεις ή απομακρυσμένες συνεργασίες;

Για ένα συνδυασμό όλων:

4. Ας υποθέσουμε ότι εργάζεστε σε δημόσιο χώρο και πρέπει να συμμετάσχετε σε μια εικονική συνάντηση όπου πρέπει να μοιραστείτε την οθόνη σας. Περιγράψτε τα βήματα που θα λαμβάνατε για να ασφαλίσετε τη συσκευή σας, να διαχειριστείτε τις υπηρεσίες δικτύου και να διασφαλίσετε την ασφαλή ψηφιακή συνεργασία.

## Ηλεκτρονικό απόρρητο και ασφάλεια των παιδιών στον ψηφιακό κόσμο (MC 4.1.A.6)

### Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ηλεκτρονικό απόρρητο και ασφάλεια των παιδιών στον ψηφιακό κόσμο<br>**Κωδ: A.6** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.14 και 4.1.15):

Απόρρητο των μέσων κοινωνικής δικτύωσης

1. Γνωρίζετε τη σημασία της τακτικής επανεξέτασης και αφαίρεσης των προσωπικών σας πληροφοριών που είναι αποθηκευμένες σε βάσεις δεδομένων των μέσων κοινωνικής δικτύωσης για την προστασία του απορρήτου του ψηφιακού σας περιεχομένου.

Παιδική ασφάλεια στο διαδίκτυο

2. Εφαρμόστε λογισμικό γονικού ελέγχου και φιλτραρίσματος για την προστασία των παιδιών από ακατάλληλο περιεχόμενο και διαδικτυακούς κινδύνους.

## Περιγραφή

Το Micro Credential "Online Privacy and Child Safety in the Digital World" είναι ένα εξειδικευμένο πρόγραμμα που ασχολείται με δύο καίριες πτυχές της ψηφιακής ασφάλειας - τη διατήρηση της ιδιωτικής ζωής στο διαδίκτυο και την προστασία των παιδιών από τις ψηφιακές απειλές. Το πρόγραμμα αυτό ενθαρρύνει την υπεύθυνη ψηφιακή ιδιότητα του πολίτη, δίνοντας έμφαση στην ανάγκη αποτελεσματικής διαχείρισης των προσωπικών πληροφοριών στα μέσα κοινωνικής δικτύωσης και στη χρήση του γονικού ελέγχου και του λογισμικού φιλτραρίσματος για τη δημιουργία ενός ασφαλέστερου διαδικτυακού περιβάλλοντος για τα παιδιά.

Ξεκινώντας με μια βαθιά κατάδυση στην ιδιωτικότητα στο διαδίκτυο, η πρώτη ενότητα ασχολείται με την κρίσιμη πτυχή της διαχείρισης των προσωπικών πληροφοριών στα μέσα κοινωνικής δικτύωσης. Οι συμμετέχοντες θα αποκτήσουν μια ισχυρή κατανόηση των ρυθμίσεων απορρήτου στις διάφορες πλατφόρμες κοινωνικής δικτύωσης και του τρόπου βελτιστοποίησής τους για τη διασφάλιση των προσωπικών τους πληροφοριών. Θα μάθουν τη σημασία της τακτικής επανεξέτασης και της αφαίρεσης των προσωπικών πληροφοριών που είναι αποθηκευμένες σε βάσεις δεδομένων των μέσων κοινωνικής δικτύωσης και πώς αυτά τα μέτρα προστατεύουν την ιδιωτικότητα του ψηφιακού τους περιεχομένου.

Στη συνέχεια, το μάθημα περνάει στο θέμα της ασφάλειας των παιδιών στον ψηφιακό κόσμο. Αναγνωρίζοντας τη διάδοση της ψηφιακής τεχνολογίας στη ζωή των παιδιών, η ενότητα διερευνά τις πιθανές απειλές που μπορεί να αντιμετωπίσουν τα παιδιά στο διαδίκτυο και πώς οι ενήλικες μπορούν να μετριάσουν αυτές τις απειλές. Παρέχει ολοκληρωμένες οδηγίες σχετικά με την εφαρμογή γονικού ελέγχου και λογισμικού φιλτραρίσματος, προσφέροντας στους συμμετέχοντες πρακτικές στρατηγικές για τη θωράκιση των παιδιών από ακατάλληλο περιεχόμενο και διαδικτυακούς κινδύνους.

Το μάθημα συνδυάζει τη θεωρητική διδασκαλία με πρακτικές ασκήσεις, διασφαλίζοντας ότι οι συμμετέχοντες όχι μόνο κατανοούν τις έννοιες αλλά και μπορούν να τις εφαρμόσουν αποτελεσματικά. Οι μελέτες περιπτώσεων πραγματικού κόσμου και οι δραστηριότητες που βασίζονται σε σενάρια θα παρέχουν μια καθηλωτική μαθησιακή εμπειρία, επιτρέποντας στους εκπαιδευόμενους να πλαισιώσουν καλύτερα τη μάθησή τους.

Το πρόγραμμα ολοκληρώνεται με μια αξιολόγηση που επικυρώνει την κατανόηση της ύλης του μαθήματος από τους εκπαιδευόμενους, με αποτέλεσμα την απόκτηση Micro Credential μετά την επιτυχή ολοκλήρωση. Αυτό το επίτευγμα μπορεί

να κοινοποιηθεί σε εργοδότες ή επαγγελματικά δίκτυα, παρέχοντας απόδειξη της ικανότητας του εκπαιδευόμενου να διαχειρίζεται την ιδιωτικότητα στο διαδίκτυο και να εφαρμόζει μέτρα για την ασφάλεια των παιδιών στο διαδίκτυο.

Το μικροπιστοποιητικό "Διαδικτυακή ιδιωτικότητα και ασφάλεια των παιδιών στον ψηφιακό κόσμο" ευθυγραμμίζεται με τους πρωταρχικούς στόχους της Ευρωπαϊκής Επιτροπής για την προώθηση του ψηφιακού αλφαβητισμού και της ασφαλούς χρήσης του διαδικτύου. Χρησιμεύει ως πολύτιμη πηγή για γονείς, εκπαιδευτικούς και οποιονδήποτε ενδιαφέρεται να δημιουργήσει ένα ασφαλέστερο διαδικτυακό περιβάλλον για τους ίδιους και τα παιδιά, μια κρίσιμη ανάγκη στον ολοένα και πιο ψηφιακό κόσμο μας.

Αυτό το μικροπιστοποιητικό συνάδει με τη δέσμευση της Ευρωπαϊκής Ένωσης για την ενίσχυση των ψηφιακών ικανοτήτων και την προώθηση της διαδικτυακής ασφάλειας των πολιτών της, ιδίως όσον αφορά την προστασία της ιδιωτικής ζωής και την προστασία των παιδιών. Παρέχει στους εκπαιδευόμενους πιστοποιημένη επάρκεια για την κατανόηση και την επάρκειά τους στη διαχείριση της ιδιωτικής ζωής στο διαδίκτυο και την ασφάλεια των παιδιών στο διαδίκτυο.

## Ερωτήσεις

Για το απόρρητο των μέσων κοινωνικής δικτύωσης:

1. Εξηγήστε γιατί είναι σημαντικό να επανεξετάζετε και να αφαιρείτε τακτικά τις προσωπικές πληροφορίες που είναι αποθηκευμένες σε βάσεις δεδομένων των μέσων κοινωνικής δικτύωσης. Πώς προστατεύει αυτή η πρακτική την ιδιωτικότητα του ψηφιακού σας περιεχομένου;
2. Ποια είναι μερικά από τα μέτρα που θα λαμβάνατε για την προστασία της ιδιωτικής σας ζωής στις πλατφόρμες κοινωνικής δικτύωσης; Παρακαλείστε να δώσετε συγκεκριμένα παραδείγματα σχετικά με τις ρυθμίσεις απορρήτου και την αφαίρεση προσωπικών πληροφοριών.

Για τη διαδικτυακή ασφάλεια των παιδιών:

3. Συζητήστε το ρόλο του γονικού ελέγχου και του λογισμικού φιλτραρίσματος στην προστασία των παιδιών από ακατάλληλο περιεχόμενο και διαδικτυακούς κινδύνους. Μπορείτε να δώσετε ένα παράδειγμα μιας κατάστασης όπου τα εργαλεία αυτά θα ήταν χρήσιμα;
4. Πώς θα προσεγγίζατε τη ρύθμιση του γονικού ελέγχου σε μια συσκευή που θα χρησιμοποιείται από ένα παιδί; Ποιους παράγοντες θα λαμβάνατε υπόψη σας;

Για συνδυασμό και των δύο:

5. Φανταστείτε ότι δημιουργείτε έναν λογαριασμό στα μέσα κοινωνικής δικτύωσης για ένα παιδί υπό την επίβλεψή σας. Πώς θα διασφαλίζατε την προστασία της ιδιωτικής ζωής του παιδιού και τη θωράκισή του από ακατάλληλο περιεχόμενο και διαδικτυακούς κινδύνους;

# Ψηφιακή συμπεριφορά και ασφάλεια συσκευών (MC 4.1.A.7)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ψηφιακή συμπεριφορά και ασφάλεια συσκευών<br>**Κωδ: A.7** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.16 και 4.1.17):

Ασφαλείς πρακτικές λήψης

1. Κατανοήστε τους κινδύνους που σχετίζονται με τη λήψη προγραμμάτων ή εφαρμογών από ανεπίσημες ή τρίτες πηγές.

Ακεραιότητα συσκευής

2. Αποφύγετε τη χρήση jailbroken ή rooted συσκευών, καθώς αυτές οι μέθοδοι μπορούν να παρακάμψουν τα μέτρα ασφαλείας και να θέσουν σε κίνδυνο την ασφάλεια των δεδομένων σας.

## Περιγραφή

Το Micro Credential "Safe Digital Behavior and Device Security" είναι ένα ολοκληρωμένο πρόγραμμα που αποσκοπεί στην εκπαίδευση των εκπαιδευομένων σχετικά με τις πιθανές απειλές στον κυβερνοχώρο και τον τρόπο ασφαλούς πλοήγησης στο ψηφιακό τοπίο. Το μάθημα δίνει έμφαση στους κινδύνους που ενέχει η λήψη λογισμικού από ανεπίσημες πηγές και στις επιπτώσεις στην ασφάλεια της χρήσης jailbroken ή rooted συσκευών. Προσφέρει πρακτικές κατευθυντήριες γραμμές για την υιοθέτηση ασφαλών ψηφιακών συμπεριφορών και την ασφάλεια των συσκευών, αντιμετωπίζοντας βασικές πτυχές της κυβερνοασφάλειας στον σημερινό τεχνολογικά καθοδηγούμενο κόσμο.

Το πρόγραμμα ξεκινά με την εκπαίδευση των μαθητών σχετικά με τους κινδύνους που σχετίζονται με τη λήψη λογισμικού ή εφαρμογών από ανεπίσημες ή τρίτες πηγές. Αυτό το τμήμα παρέχει πληροφορίες για το πώς ανεπίσημες πηγές μπορούν συχνά να φιλοξενήσουν κακόβουλο λογισμικό, λογισμικό κατασκοπείας ή άλλα επιβλαβή προγράμματα μεταμφιεσμένα ως νόμιμο λογισμικό. Οι συμμετέχοντες θα μάθουν πώς να εντοπίζουν ασφαλείς πηγές για λήψεις και πόσο σημαντικό είναι να διατηρούν το λογισμικό τους ενημερωμένο μέσω επίσημων καναλιών.

Το επόμενο τμήμα του μαθήματος επικεντρώνεται στους πιθανούς κινδύνους ασφαλείας των jailbroken ή rooted συσκευών. Οι εκπαιδευόμενοι θα εμβαθύνουν στον τρόπο με τον οποίο αυτές οι μέθοδοι, ενώ παρέχουν στους χρήστες μεγαλύτερο έλεγχο στις συσκευές τους, μπορούν να παρακάμψουν τα μέτρα ασφαλείας και να τις εκθέσουν ενδεχομένως σε κακόβουλο λογισμικό. Το τμήμα τονίζει τη σημασία της κατανόησης του συμβιβασμού μεταξύ του αυξημένου ελέγχου και των αυξημένων κινδύνων ασφαλείας που συνεπάγεται το jailbreaking ή το rooting των συσκευών.

Εκτός από αυτά τα βασικά θέματα, το μάθημα προσφέρει επίσης μια επισκόπηση της γενικής ασφαλούς ψηφιακής συμπεριφοράς. Οι συμμετέχοντες θα εκπαιδευτούν σχετικά με τις συνήθειες ασφαλούς περιήγησης, την ασφάλεια των κωδικών πρόσβασης, την αναγνώριση των προσπαθειών ηλεκτρονικού "ψαρέματος" και τη διατήρηση της ασφάλειας των συσκευών. Η ενότητα αυτή θα τονίσει επίσης τη σημασία της προσοχής στη φυσική ασφάλεια των συσκευών, ιδίως σε δημόσιους χώρους, για την αποφυγή κλοπής και μη εξουσιοδοτημένης πρόσβασης.

Το μάθημα ολοκληρώνεται με πρακτικές ασκήσεις που έχουν σχεδιαστεί για να θέσουν σε εφαρμογή τη διδαχθείσα θεωρία, επιτρέποντας στους εκπαιδευόμενους να εφαρμόσουν τις νέες γνώσεις τους σε πραγματικές συνθήκες. Οι συμμετέχοντες θα έχουν την ευκαιρία να συμμετάσχουν σε διαδραστικές εργασίες που προσομοιώνουν κοινές απειλές στον κυβερνοχώρο και θα μάθουν πώς να ανταποκρίνονται αποτελεσματικά σε αυτές τις καταστάσεις.

Με την ολοκλήρωση αυτού του Micro Credential, οι εκπαιδευόμενοι θα είναι εφοδιασμένοι με μια ισχυρή κατανόηση της ασφαλούς ψηφιακής συμπεριφοράς και της ασφάλειας των συσκευών. Θα είναι σε θέση να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τη λήψη λογισμικού, τη διαχείριση των συσκευών τους και την ασφαλή πλοήγηση στον ψηφιακό κόσμο. Το μάθημα αυτό ευθυγραμμίζεται με την εστίαση της Ευρωπαϊκής Ένωσης στην προώθηση του ψηφιακού αλφαβητισμού και της ασφάλειας στο διαδίκτυο, καθιστώντας το πολύτιμο πόρο για άτομα και επαγγελματίες στην ψηφιακή εποχή.

Σύμφωνα με τη δέσμευση της Ευρωπαϊκής Ένωσης για την προώθηση του ψηφιακού αλφαβητισμού και της ασφάλειας, αυτό το Πιστοποιητικό Micro παρέχει ένα πιστοποιημένο επίτευγμα που επαληθεύει την κατανόηση και τη γνώση του εκπαιδευόμενου σε θέματα ασφαλούς ψηφιακής συμπεριφοράς και ασφάλειας συσκευών.

## Ερωτήσεις

Για πρακτικές ασφαλούς λήψης:

1. Ποιος είναι ο κύριος κίνδυνος από τη λήψη λογισμικού ή εφαρμογών από ανεπίσημες ή τρίτες πηγές;
2. Πώς μπορούν ανεπίσημες πηγές να συγκαλύπτουν επιβλαβή προγράμματα;
3. Ποιες δεξιότητες απαιτούνται για τον εντοπισμό ασφαλών πηγών λήψης;

4. Γιατί είναι σημαντικό να ενημερώνετε το λογισμικό μέσω επίσημων καναλιών;
5. Μπορείτε να αναφέρετε συγκεκριμένους τύπους επιβλαβών προγραμμάτων που μπορεί να φιλοξενούνται σε ανεπίσημες πηγές;

Για την ακεραιότητα της συσκευής:

6. Ποιοι είναι οι πιθανοί κίνδυνοι ασφαλείας που σχετίζονται με το jailbreaking ή το rooting των συσκευών;
7. Πώς το jailbreaking και το rooting παρέχουν στους χρήστες μεγαλύτερο έλεγχο των συσκευών τους;
8. Με ποιους τρόπους μπορεί το jailbreaking ή το rooting να παρακάμψει τα μέτρα ασφαλείας;
9. Σε τι είδους κακόβουλο λογισμικό θα μπορούσαν να εκτεθούν οι χρήστες με το jailbreaking ή το rooting των συσκευών τους;
10. Γιατί είναι σημαντικό για τους χρήστες να κατανοήσουν την αντιστάθμιση μεταξύ του αυξημένου ελέγχου και των αυξημένων κινδύνων ασφαλείας όταν σκέφτονται να κάνουν jailbreaking ή rooting στις συσκευές τους;

Για το συνδυασμό και των δύο

11. Ποια είναι τα βασικά στοιχεία της ασφαλούς ψηφιακής συμπεριφοράς;
12. Πώς προτείνει το πρόγραμμα τη διατήρηση της ασφάλειας του κωδικού πρόσβασης;
13. Ποιες συμβουλές παρέχει το πρόγραμμα για την αναγνώριση προσπαθειών phishing;
14. Εκτός από τις ψηφιακές προφυλάξεις, τι τονίζει το πρόγραμμα σχετικά με την ασφάλεια των φυσικών συσκευών;
15. Γιατί είναι ιδιαίτερα σημαντικό να προσέχετε την ασφάλεια των συσκευών σε δημόσιους χώρους;

# Ασφαλής διαχείριση συσκευών και προστασία δεδομένων (MC 4.1.A.8)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ασφαλής διαχείριση συσκευών και προστασία δεδομένων<br>**Κωδ: A.8** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.18, 4.1.19 και 4.1.20):

Διάθεση συσκευής

1. Γνωρίζετε τη σημασία της ασφαλούς διαγραφής και απόρριψης των παλαιών συσκευών για να αποτρέψετε την ανάκτηση των δεδομένων σας από άλλους.

Κρυπτογράφηση δεδομένων

2. Χρησιμοποιήστε κρυπτογράφηση για να προστατεύσετε τα ευαίσθητα δεδομένα στις συσκευές σας, ειδικά για τα δεδομένα που είναι αποθηκευμένα σε κινητές συσκευές και αφαιρούμενα μέσα μαζικής αποθήκευσης.

Ενημέρωση για την παραβίαση δεδομένων

3. Κατανοήστε τους κινδύνους που συνδέονται με τη διαβίβαση ή την αποθήκευση προσωπικών πληροφοριών σε συσκευές και το ενδεχόμενο παραβίασης δεδομένων.

## Περιγραφή

Το Micro Credential "Secure Device Management and Data Protection" είναι ένα πρόγραμμα που καθοδηγεί τους εκπαιδευόμενους στις βασικές έννοιες και πρακτικές εφαρμογές της ασφαλούς διαχείρισης ψηφιακών συσκευών και της προστασίας ευαίσθητων δεδομένων. Καλύπτει μια σειρά από κρίσιμα θέματα, όπως η κατανόηση της σημασίας της ασφαλούς απόρριψης παλαιών συσκευών, η εφαρμογή κρυπτογράφησης για την προστασία ευαίσθητων δεδομένων και η συνειδητοποίηση των πιθανών κινδύνων παραβίασης δεδομένων κατά τη μετάδοση ή την αποθήκευση προσωπικών πληροφοριών σε συσκευές.

Το μάθημα ξεκινά με τη διερεύνηση της έννοιας της διαχείρισης συσκευών. Παρέχει σε βάθος κάλυψη των βέλτιστων πρακτικών για την ασφαλή διαγραφή και απόρριψη παλαιών συσκευών ώστε να αποτραπεί η ανάκτηση ευαίσθητων δεδομένων από μη εξουσιοδοτημένα άτομα.

Οι εκπαιδευόμενοι θα κατανοήσουν πώς να αφαιρούν αποτελεσματικά δεδομένα από συσκευές, τόσο χειροκίνητα όσο και με τη χρήση διαφόρων εργαλείων λογισμικού. Θα μάθουν επίσης για ασφαλείς μεθόδους διάθεσης, όπως προγράμματα ανακύκλωσης και καταστροφής συσκευών, για να διασφαλίσουν ότι οι παλιές συσκευές δεν θα αποτελέσουν κίνδυνο για την ασφάλεια.

Η δεύτερη ενότητα εμβαθύνει στη σφαίρα της προστασίας δεδομένων. Συζητούνται εκτενώς οι αρχές και η εφαρμογή της κρυπτογράφησης για την προστασία ευαίσθητων δεδομένων σε συσκευές, ιδίως σε κινητές συσκευές και αφαιρούμενα μέσα μαζικής αποθήκευσης. Οι εκπαιδευόμενοι θα κατανοήσουν τις διάφορες μεθόδους κρυπτογράφησης, τον τρόπο εφαρμογής τους και τη σημασία τους σε μια προσέγγιση πολυεπίπεδης ασφάλειας.

Τέλος, το μάθημα εξετάζει τους κινδύνους παραβίασης δεδομένων κατά την αποθήκευση και τη διαβίβαση προσωπικών πληροφοριών σε συσκευές. Οι συμμετέχοντες θα εκτεθούν σε πραγματικά σενάρια παραβίασης δεδομένων, τις αιτίες και τις συνέπειές τους. Θα μάθουν για τις μεθόδους πρόληψης των παραβιάσεων δεδομένων, όπως ασφαλή πρωτόκολλα επικοινωνίας, ασφαλείς λύσεις αποθήκευσης και βέλτιστες πρακτικές για την ανταλλαγή προσωπικών πληροφοριών. Η ενότητα αυτή θα θίξει επίσης νομικά και ηθικά ζητήματα που σχετίζονται με τις παραβιάσεις δεδομένων.

Αυτό το Micro Credential χρησιμοποιεί μια διαδραστική μαθησιακή προσέγγιση, συνδυάζοντας τη θεωρία με πρακτικές ασκήσεις. Οι εκπαιδευόμενοι θα έχουν την ευκαιρία να ασχοληθούν με το υλικό μέσω πρακτικών δραστηριοτήτων, κουίζ και μελετών περιπτώσεων. Στο τέλος αυτού του μαθήματος, οι συμμετέχοντες θα έχουν τις γνώσεις και τις δεξιότητες να διαχειρίζονται με ασφάλεια τις συσκευές τους και να εφαρμόζουν ισχυρά μέτρα προστασίας δεδομένων.

Σε ευθυγράμμιση με την εστίαση της Ευρωπαϊκής Ένωσης στον ψηφιακό αλφαβητισμό και την ασφάλεια, το Micro Credential "Secure Device Management and Data Protection" προσφέρει πολύτιμες γνώσεις και δεξιότητες για όσους ανησυχούν για την ψηφιακή τους ασφάλεια στον σημερινό συνδεδεμένο κόσμο. Δίνει στους εκπαιδευόμενους τη δυνατότητα να διαχειρίζονται με αυτοπεποίθηση τις συσκευές τους και να προστατεύουν τα ευαίσθητα δεδομένα τους από πιθανές απειλές, κάτι που είναι όλο και πιο σημαντικό στην ψηφιακή εποχή μας.

## Ερωτήσεις

Για την απόρριψη συσκευών:

1. Γιατί είναι ζωτικής σημασίας η ασφαλής διαγραφή και απόρριψη παλαιών συσκευών; Εξηγήστε τι θα μπορούσε να συμβεί εάν παραμεληθεί αυτό το βήμα.
2. Περιγράψτε τα βήματα που θα ακολουθούσατε για την ασφαλή διαγραφή και απόρριψη ενός παλιού φορητού υπολογιστή. Ποιες προφυλάξεις θα λαμβάνατε για να διασφαλίσετε ότι δεν μπορούν να ανακτηθούν δεδομένα;"

Για κρυπτογράφηση δεδομένων:

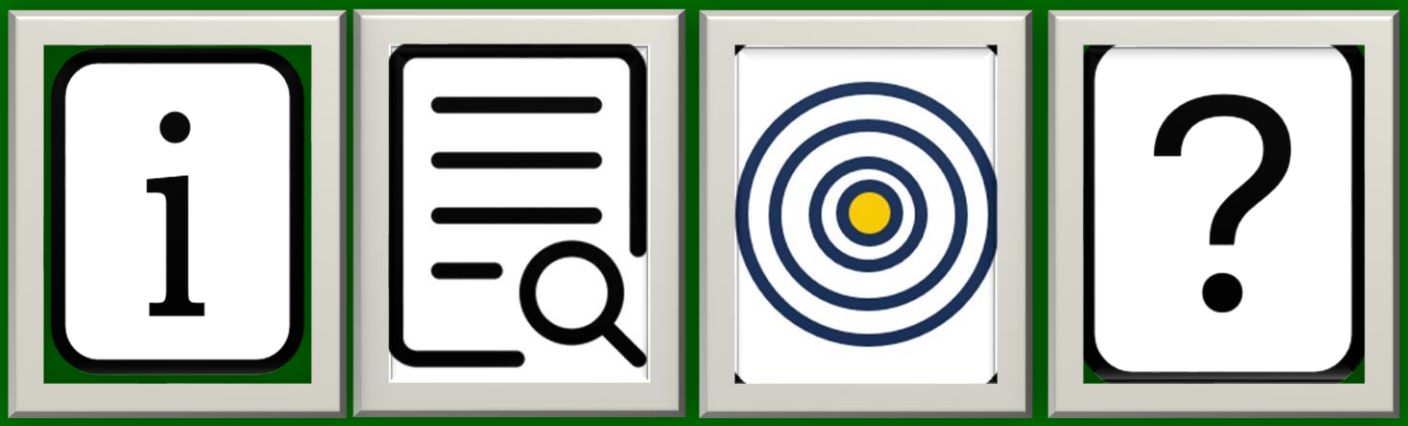
3. Εξηγήστε πώς η κρυπτογράφηση μπορεί να προστατεύσει τα ευαίσθητα δεδομένα στις συσκευές σας. Δώστε παραδείγματα καταστάσεων όπου αυτό θα μπορούσε να είναι ιδιαίτερα χρήσιμο.
4. Συζητήστε τα βήματα για την κρυπτογράφηση δεδομένων σε κινητή συσκευή ή αφαιρούμενη μονάδα μαζικής αποθήκευσης. Γιατί είναι σημαντικό να κρυπτογραφούνται τα δεδομένα που είναι αποθηκευμένα σε τέτοιες συσκευές;

Για την ευαισθητοποίηση σε θέματα παραβίασης δεδομένων:

5. Ποιοι είναι οι κίνδυνοι που συνδέονται με τη διαβίβαση ή την αποθήκευση προσωπικών πληροφοριών σε συσκευές; Πώς μπορούν τέτοιες πρακτικές να οδηγήσουν σε πιθανές παραβιάσεις δεδομένων;
6. Περιγράψτε ένα σενάριο στο οποίο θα μπορούσε να συμβεί παραβίαση δεδομένων λόγω μη ασφαλούς διαβίβασης ή αποθήκευσης δεδομένων. Ποια μέτρα θα μπορούσαν να ληφθούν για την πρόληψη ενός τέτοιου σεναρίου;

# ΕΝΔΙΑΜΕΣΟ ΕΠΙΠΕΔΟ

(Επίπεδο 3 και 4)



# Βέλτιστες πρακτικές κυβερνοασφάλειας (MC 4.1.B.1)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Βέλτιστες πρακτικές κυβερνοασφάλειας<br>**Κωδ: B.1.B.1: MC 4.1.B.1** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 LOs 4.1.21, 4.1.22):

Ασφαλής περιήγηση και πρακτικές λήψης

- Χειριστείτε με προσοχή ύποπτους συνδέσμους και αποφύγετε τη λήψη αρχείων από άγνωστες πηγές για να προστατεύσετε τις συσκευές σας από πιθανές απειλές κακόβουλου λογισμικού.

Δημιουργία αντιγράφων ασφαλείας και προστασία δεδομένων

- Υποδείξτε τη σημασία της τακτικής δημιουργίας αντιγράφων ασφαλείας δεδομένων για την προστασία από απώλεια δεδομένων και βλάβες συσκευών.

## Περιγραφή

Το Micro Credential "Cybersecurity Best Practices" είναι ένα ολοκληρωμένο πρόγραμμα ειδικά σχεδιασμένο για να ενδυναμώσει τους εκπαιδευόμενους με κρίσιμες γνώσεις και δεξιότητες που είναι απαραίτητες για την προστασία των ψηφιακών πληροφοριών και συσκευών από ένα ευρύ φάσμα απειλών. Το πρόγραμμα αυτό εμβαθύνει στην κατανόηση και την εφαρμογή πρακτικών ασφαλούς περιήγησης και λήψης δεδομένων για τον μετριασμό των απειλών από κακόβουλο λογισμικό. Επιπλέον, υπογραμμίζει τη σημασία της τακτικής δημιουργίας αντιγράφων ασφαλείας δεδομένων ως ισχυρή στρατηγική για τη θωράκιση έναντι πιθανής απώλειας δεδομένων ή βλαβών συσκευών.

Το πρώτο τμήμα αυτού του μαθήματος έχει ως στόχο να εφοδιάσει τους εκπαιδευόμενους με μια βαθιά κατανόηση των πρακτικών ασφαλούς πλοήγησης. Αναλύει την ανατομία των απειλών στον κυβερνοχώρο, όπως το phishing, το κακόβουλο λογισμικό και το ransomware, μεταδίδοντας την ικανότητα εντοπισμού και μετριασμού τους. Οι συμμετέχοντες θα ενημερωθούν για τις πρακτικές ασφαλούς περιήγησης, συμπεριλαμβανομένης της χρήσης του HTTPS, της επαλήθευσης των πιστοποιητικών ιστότοπων και των επιπτώσεων των cookies και της παρακολούθησης. Θα μάθουν επίσης πώς να χειρίζονται ύποπτους συνδέσμους και να αποφεύγουν τη λήψη αρχείων από άγνωστες πηγές για να αποτρέψουν πιθανές απειλές κακόβουλου λογισμικού.

Η δεύτερη ενότητα καταδύεται σε πρακτικές ασφαλούς λήψης. Οι εκπαιδευόμενοι θα διερευνήσουν τους κινδύνους που σχετίζονται με τη λήψη προγραμμάτων, αρχείων ή εφαρμογών από ανεπίσημες ή τρίτες πηγές. Θα μάθουν πώς να εξακριβώνουν την ασφάλεια μιας πηγής και τη σημασία της χρήσης επίσημων πλατφορμών για λήψεις. Η ενότητα καλύπτει επίσης τους πιθανούς κινδύνους από το άνοιγμα συμπιεσμένων αρχείων όπως αρχεία zip ή rar από μη αξιόπιστες ή άγνωστες πηγές.

Η τελευταία ενότητα επικεντρώνεται στη σημασία της δημιουργίας αντιγράφων ασφαλείας δεδομένων. Οι συμμετέχοντες θα γνωρίσουν διάφορες τεχνικές δημιουργίας αντιγράφων ασφαλείας δεδομένων και θα κατανοήσουν το ρόλο των τακτικών αντιγράφων ασφαλείας δεδομένων στην ασφάλεια στον κυβερνοχώρο. Αυτή η ενότητα εμβαθύνει επίσης στη δημιουργία χρονοδιαγραμμάτων δημιουργίας αντιγράφων ασφαλείας, στην επιλογή μεταξύ λύσεων δημιουργίας αντιγράφων ασφαλείας που βασίζονται στο cloud ή σε φυσικές λύσεις και στην κρυπτογράφηση αντιγράφων ασφαλείας για ένα πρόσθετο επίπεδο ασφάλειας.

Το μάθημα αυτό περιλαμβάνει επίσης πρακτικές δραστηριότητες και σενάρια από τον πραγματικό κόσμο, προωθώντας την πρακτική εφαρμογή των δεξιοτήτων που διδάχθηκαν. Τακτικά κουίζ και αξιολογήσεις θα μετρούν την πρόοδο των συμμετεχόντων, διασφαλίζοντας ότι έχουν κατακτήσει κάθε θέμα πριν προχωρήσουν.

Με την ολοκλήρωση αυτού του Micro Credential, οι εκπαιδευόμενοι θα έχουν κατανοήσει τις αρχές και τις πρακτικές της κυβερνοασφάλειας. Θα είναι εξοπλισμένοι για να περιηγούνται με αυτοπεποίθηση στο ψηφιακό τοπίο, διατηρώντας τα δεδομένα τους ασφαλή και τις συσκευές τους ασφαλείς. Αυτό ευθυγραμμίζεται καλά με την εστίαση της Ευρωπαϊκής Ένωσης στην κυβερνοασφάλεια και τον ψηφιακό γραμματισμό, καθιστώντας το μάθημα ιδιαίτερα πολύτιμο τόσο για τα άτομα όσο και για τους επαγγελματίες στον σημερινό ολοένα και πιο ψηφιακό κόσμο.

Ευθυγραμμισμένο με την εστίαση της Ευρωπαϊκής Ένωσης στην ενίσχυση του ψηφιακού αλφαβητισμού και της ασφάλειας, αυτό το Micro Credential παρέχει μια πιστοποιημένη μαρτυρία της επάρκειας του εκπαιδευόμενου σε βασικές πτυχές των βέλτιστων πρακτικών κυβερνοασφάλειας.

## Ερωτήσεις

Για πρακτικές ασφαλούς περιήγησης και λήψης:

1. Γιατί είναι σημαντικό να είστε προσεκτικοί όταν κάνετε κλικ σε συνδέσμους ή κατεβάζετε αρχεία από το διαδίκτυο; Ποιους κινδύνους θα μπορούσατε ενδεχομένως να αντιμετωπίσετε αν δεν είστε προσεκτικοί;
2. Φανταστείτε ότι λαμβάνετε ένα email με έναν σύνδεσμο από έναν άγνωστο αποστολέα. Ποια βήματα θα κάνατε πριν αποφασίσετε αν θα κάνετε κλικ στο σύνδεσμο;
3. Περιγράψτε τους κινδύνους που σχετίζονται με τη λήψη αρχείων από άγνωστες πηγές. Πώς μπορούν να μετριαστούν αυτοί οι κίνδυνοι;

Για δημιουργία αντιγράφων ασφαλείας και προστασία δεδομένων:

4. Γιατί είναι σημαντικό να δημιουργείτε τακτικά αντίγραφα ασφαλείας των δεδομένων σας; Πώς προστατεύει αυτή η πρακτική από την απώλεια δεδομένων και τις βλάβες της συσκευής;
5. Περιγράψτε τα βήματα που θα ακολουθούσατε για τη δημιουργία αντιγράφων ασφαλείας των δεδομένων στον υπολογιστή σας. Πόσο συχνά θα συνιστούσατε να γίνεται αυτή η διαδικασία;

# Διαχείριση απώλειας συσκευών και προστασία δεδομένων (MC 4.1.B.2)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Διαχείριση απώλειας συσκευών και προστασία δεδομένων<br>**Κωδ: B.2** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 LOs 4.1.23, 4.1.24):

Ευαισθητοποίηση απώλειας συσκευής

- Γνωρίζετε ότι οι χαμένες ή κλεμμένες συσκευές μπορούν να εντοπιστούν, να κλειδωθούν ή να διαγραφούν χρησιμοποιώντας δωρεάν εργαλεία που βασίζονται στο Web και είναι διαθέσιμα στις περισσότερες συσκευές.

Πρακτική διαχείριση απώλειας συσκευής

- Χρησιμοποιήστε επιδέξια τις λειτουργίες εντοπισμού, κλειδώματος και διαγραφής για την προστασία των δεδομένων και του απορρήτου σας σε περίπτωση απώλειας ή κλοπής της συσκευής σας.

## Περιγραφή

Το Micro Credential "Διαχείριση απώλειας συσκευών και προστασία δεδομένων" είναι ένα εντατικό, πρακτικό μάθημα που αποσκοπεί στο να εξοπλίσει τους εκπαιδευόμενους με τις απαραίτητες γνώσεις και δεξιότητες για την αποτελεσματική διαχείριση και προστασία των συσκευών και των δεδομένων τους σε περιπτώσεις απώλειας ή κλοπής συσκευών. Αυτό περιλαμβάνει την εμπεριστατωμένη κατανόηση του τρόπου εντοπισμού, κλειδώματος και διαγραφής χαμένων ή κλεμμένων συσκευών με τη χρήση διαδικτυακών εργαλείων και την αποτελεσματική εφαρμογή αυτών των χαρακτηριστικών για την προστασία των προσωπικών δεδομένων και τη διασφάλιση της ιδιωτικής ζωής.

Η πρώτη ενότητα του μαθήματος είναι αφιερωμένη στην εκπαίδευση των συμμετεχόντων σχετικά με τα μέτρα που πρέπει να λαμβάνονται όταν μια συσκευή χάνεται ή κλέβεται. Οι συμμετέχοντες θα μάθουν πώς να εντοπίζουν τις χαμένες συσκευές χρησιμοποιώντας ενσωματωμένα εργαλεία εντοπισμού ή εργαλεία εντοπισμού τρίτων. Θα διερευνήσουν επίσης πώς να κλειδώνουν τις συσκευές τους εξ αποστάσεως, καθιστώντας τις μη προσβάσιμες σε μη εξουσιοδοτημένους χρήστες. Θα καλυφθεί επίσης η δυνατότητα απομακρυσμένης διαγραφής όλων των δεδομένων της συσκευής, αποτρέποντας έτσι να πέσουν ευαίσθητα προσωπικά δεδομένα σε λάθος χέρια.

Πρακτικές επιδείξεις θα δώσουν στους συμμετέχοντες μια πρακτική κατανόηση αυτών των διαδικασιών.

Η δεύτερη ενότητα επικεντρώνεται στα προληπτικά βήματα για την προστασία των δεδομένων. Οι συμμετέχοντες θα διδαχθούν πώς να δημιουργούν τακτικά αντίγραφα ασφαλείας των δεδομένων, ελαχιστοποιώντας την απώλεια δεδομένων σε περίπτωση κλοπής ή βλάβης της συσκευής. Θα εξερευνήσουν διάφορες μεθόδους και λύσεις δημιουργίας αντιγράφων ασφαλείας, συμπεριλαμβανομένων των αντιγράφων ασφαλείας που βασίζονται στο cloud και των επιλογών φυσικής αποθήκευσης. Θα δοθεί επίσης έμφαση στη σημασία της κρυπτογράφησης για την προστασία ευαίσθητων δεδομένων και οι συμμετέχοντες θα μάθουν πώς να εφαρμόζουν κρυπτογράφηση στις συσκευές τους και για τα αντίγραφα ασφαλείας τους.

Πρόσθετα θέματα που καλύπτονται στο μάθημα περιλαμβάνουν τη δημιουργία και διαχείριση της ασφάλισης συσκευών, την κατανόηση των νομικών πτυχών της κλοπής συσκευών και τον τρόπο αναφοράς μιας χαμένης ή κλεμμένης συσκευής στις αρχές και στους παρόχους υπηρεσιών. Το μάθημα θα καλύψει επίσης τη σημασία της εξασφάλισης των συσκευών με ισχυρούς κωδικούς πρόσβασης, βιομετρικά δεδομένα ή άλλα μέτρα ασφαλείας για την καθυστέρηση ή την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε περίπτωση απώλειας ή κλοπής μιας συσκευής.

Στο τέλος αυτού του Micro Credential, οι εκπαιδευόμενοι θα έχουν κατανοήσει πλήρως πώς να διαχειρίζονται την απώλεια ή την κλοπή μιας συσκευής και να προστατεύουν αποτελεσματικά τα δεδομένα τους, διασφαλίζοντας ότι η ψηφιακή τους ασφάλεια και η ιδιωτική τους ζωή παραμένουν ανέπαφες ακόμη και σε αντίξοες καταστάσεις. Οι γνώσεις αυτές ευθυγραμμίζονται με τη δέσμευση της Ευρωπαϊκής Ένωσης για ψηφιακό αλφαβητισμό και ασφάλεια, παρέχοντας στους συμμετέχοντες ένα βασικό σύνολο δεξιοτήτων για την ψηφιακή εποχή.

Σύμφωνα με τη δέσμευση της Ευρωπαϊκής Ένωσης για την προώθηση του ψηφιακού αλφαβητισμού και της ασφάλειας, αυτό το Micro Credential παρέχει στους εκπαιδευόμενους μια πιστοποιημένη απόδειξη της επάρκειάς τους στη διαχείριση της απώλειας συσκευών και την προστασία των δεδομένων.

### Ερωτήσεις

Για την ευαισθητοποίηση απώλειας συσκευής:

1. "Περιγράψτε τη σημασία της γνώσης ότι οι χαμένες ή κλεμμένες συσκευές μπορούν να εντοπιστούν, να κλειδωθούν ή να διαγραφούν με τη χρήση δωρεάν εργαλείων που βασίζονται στον Παγκόσμιο Ιστό. Πώς αυτή η γνώση ενδυναμώνει τους χρήστες ώστε να προστατεύουν τα δεδομένα και την ιδιωτική τους ζωή;"
2. "Πώς θα εξηγούσατε την έννοια του εντοπισμού, του κλειδώματος ή της διαγραφής μιας χαμένης ή κλεμμένης συσκευής σε κάποιον που δεν είναι εξοικειωμένος με αυτές τις λειτουργίες;"

Για πρακτική διαχείριση απώλειας συσκευής:

3. "Αν το smartphone σας είχε χαθεί, ποια μέτρα θα λαμβάνατε για να το εντοπίσετε, να το κλειδώσετε ή να το διαγράψετε χρησιμοποιώντας τα διαθέσιμα διαδικτυακά εργαλεία; Πώς θα ιεραρχούσατε αυτές τις ενέργειες;"
4. "Φανταστείτε ότι έχετε κλειδώσει εξ αποστάσεως την χαμένη σας συσκευή. Ποια άλλα μέτρα θα λαμβάνατε για την προστασία των δεδομένων και της ιδιωτικής σας ζωής σε μια τέτοια περίπτωση;"

Για συνδυασμό και των δύο:

5. "Ας υποθέσουμε ότι ο φορητός σας υπολογιστής εκλάπη. Πώς θα εφαρμόζατε τις γνώσεις σας σχετικά με την ευαισθητοποίηση σε θέματα απώλειας συσκευών και την πρακτική διαχείριση απώλειας συσκευών για την προστασία των δεδομένων και της ιδιωτικής σας ζωής σε αυτό το σενάριο;"

## Ηλεκτρονικό απόρρητο και ασφάλεια εφαρμογών (MC 4.1.B.3)

### Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Διαδικτυακό απόρρητο και ασφάλεια εφαρμογών<br>**Κωδ: B.3** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.25, 4.1.26):

Διαχείριση συνόδου

- Κατανοήστε τη σημασία της αποσύνδεσης στο τέλος των περιόδων σας στο διαδίκτυο ή στις εφαρμογές, ώστε να προστατεύετε τις προσωπικές σας πληροφορίες από μη εξουσιοδοτημένη πρόσβαση.

Διαχείριση δικαιωμάτων εφαρμογών

- Κατανοήστε πώς να διαχειρίζεστε τα δικαιώματα των εφαρμογών για να προστατεύετε το απόρρητό σας και να γνωρίζετε τα δεδομένα που συλλέγονται από τις εφαρμογές στις συσκευές σας.

## Περιγραφή

Το Micro Credential "Online Privacy and Application Security" είναι ένα ολοκληρωμένο πρόγραμμα, προσεκτικά σχεδιασμένο για να μεταδώσει μια ισχυρή κατανόηση των πρακτικών διαδικτυακής ιδιωτικότητας και ασφάλειας εφαρμογών. Το πρόγραμμα αυτό δίνει έμφαση στη σημασία της αποτελεσματικής διαχείρισης συνεδριών και του κατάλληλου χειρισμού των δικαιωμάτων εφαρμογών για τη διατήρηση της εμπιστευτικότητας των προσωπικών δεδομένων και της ιδιωτικότητας των χρηστών.

Η πρώτη ενότητα αυτού του μαθήματος επικεντρώνεται στην κρίσιμη έννοια της διαδικτυακής ιδιωτικότητας. Οι συμμετέχοντες θα εμβαθύνουν στις διάφορες πτυχές που συνιστούν την ιδιωτικότητα στο διαδίκτυο, συμπεριλαμβανομένης της κατανόησης των cookies, των τεχνολογιών παρακολούθησης, του διαδικτυακού αποτυπώματος και των πρακτικών ανταλλαγής δεδομένων. Θα μάθουν πώς χρησιμοποιούνται, αποθηκεύονται και μοιράζονται οι πληροφορίες τους στο διαδίκτυο, καθώς και τους σχετικούς κινδύνους προστασίας της ιδιωτικής ζωής. Αυτή η ενότητα εστιάζει επίσης στη σημασία της σωστής διαχείρισης συνεδριών, δίνοντας έμφαση στη σημασία της αποσύνδεσης στο τέλος των συνεδριών στο διαδίκτυο

ή σε εφαρμογές για την προστασία των προσωπικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. Οι συμμετέχοντες θα αποκτήσουν πρακτική εμπειρία στη διαχείριση των διαδικτυακών συνόδων τους και στη χρήση εργαλείων ενίσχυσης της ιδιωτικότητας, όπως τα VPN, η ιδιωτική περιήγηση και οι διαχειριστές cookies.

Η δεύτερη ενότητα ασχολείται με την ασφάλεια των εφαρμογών, εστιάζοντας στο ρόλο των δικαιωμάτων των εφαρμογών στη διατήρηση του απορρήτου των χρηστών. Οι συμμετέχοντες θα διερευνήσουν τον τρόπο με τον οποίο οι εφαρμογές αποκτούν πρόσβαση και χρησιμοποιούν προσωπικά δεδομένα μέσω των δικαιωμάτων και τις πιθανές επιπτώσεις στην ιδιωτικότητα. Θα κατανοήσουν πώς να διαχειρίζονται αποτελεσματικά τα δικαιώματα των εφαρμογών, παρέχοντας μόνο την απαραίτητη πρόσβαση για τη διατήρηση της λειτουργικότητας χωρίς να διακυβεύεται η ιδιωτικότητα. Η ενότητα περιλαμβάνει πρακτικές ασκήσεις για τη διαχείριση των δικαιωμάτων σε διάφορες εφαρμογές και πλατφόρμες, παρέχοντας στους συμμετέχοντες πρακτικές δεξιότητες που μπορούν να εφαρμόσουν στην ψηφιακή τους ζωή.

Επιπλέον, το μάθημα περιλαμβάνει συνεδρίες σχετικά με τις αναδυόμενες τάσεις για την προστασία της ιδιωτικής ζωής και την ασφάλεια στο διαδίκτυο και τις πιθανές μελλοντικές εξελίξεις σε αυτόν τον δυναμικό τομέα. Οι συμμετέχοντες θα συμμετάσχουν σε συζητήσεις για θέματα όπως η προστασία της ιδιωτικής ζωής στα μέσα κοινωνικής δικτύωσης, ο ρόλος της τεχνητής νοημοσύνης στην προστασία της ιδιωτικής ζωής και ο αντίκτυπος των κανονισμών για την προστασία της ιδιωτικής ζωής.

Με την ολοκλήρωση αυτού του Micro Credential, οι εκπαιδευόμενοι θα έχουν μια ισχυρή κατανόηση των πρακτικών προστασίας της ιδιωτικής ζωής στο διαδίκτυο και της ασφάλειας των εφαρμογών, καθώς και την ικανότητα να εφαρμόζουν αυτές τις αρχές στις καθημερινές ψηφιακές τους δραστηριότητες. Αυτό ευθυγραμμίζεται με τη δέσμευση της Ευρωπαϊκής Ένωσης για την προώθηση του ψηφιακού αλφαβητισμού και της ιδιωτικής ζωής, καθιστώντας το μάθημα πολύτιμο για κάθε άτομο που επιδιώκει να ενισχύσει την ασφάλεια και την ιδιωτική του ζωή στο διαδίκτυο.

Αυτό το μικροπιστοποιητικό ευθυγραμμίζεται με τη δέσμευση της Ευρωπαϊκής Ένωσης να ενισχύσει τις ψηφιακές ικανότητες και να προωθήσει την ασφάλεια στο διαδίκτυο μεταξύ των πολιτών της. Παρέχει μια πιστοποιημένη απόδειξη της δεξιοτεχνίας του εκπαιδευόμενου στη διαχείριση της διαδικτυακής ιδιωτικότητας και της ασφάλειας των εφαρμογών.

## Ερωτήσεις

Για τη διαχείριση συνόδου:

1. Γιατί είναι σημαντικό να αποσυνδέεστε στο τέλος των περιόδων σύνδεσης στο διαδίκτυο ή στις εφαρμογές; Ποιοι κίνδυνοι μπορεί να προκύψουν αν δεν το κάνετε;
2. Συζητήστε τις πιθανές συνέπειες του να αφήνετε τις προσωπικές σας πληροφορίες προσβάσιμες με το να μην αποσυνδέεστε από μια περίοδο λειτουργίας στο διαδίκτυο ή σε μια εφαρμογή. Πώς θα μπορούσε να γίνει κατάχρηση αυτών των πληροφοριών;

Για τη διαχείριση δικαιωμάτων εφαρμογών:

3. Εξηγήστε την έννοια των αδειών χρήσης εφαρμογών και τη σημασία τους για τη διασφάλιση του απορρήτου σας. Πώς επηρεάζουν τα δικαιώματα εφαρμογών την ασφάλεια των προσωπικών σας δεδομένων;
4. Φανταστείτε ότι έχετε εγκαταστήσει μια νέα εφαρμογή στο smartphone σας. Πώς θα διαχειριστείτε τα δικαιώματά της για να διασφαλίσετε την προστασία της ιδιωτικής σας ζωής κατά τη χρήση της εφαρμογής;

Για συνδυασμό και των δύο:

5. Ας υποθέσουμε ότι χρησιμοποιείτε έναν δημόσιο υπολογιστή σε μια βιβλιοθήκη. Πώς θα διαχειρίζεστε τις συνεδρίες σας στο διαδίκτυο και τις εφαρμογές για να διασφαλίσετε τις προσωπικές σας πληροφορίες και το απόρρητό σας;

# Ασφαλής ψηφιακή συμπεριφορά και ασφάλεια φυσικών συσκευών (MC 4.1.B.4)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ασφαλής ψηφιακή συμπεριφορά και ασφάλεια φυσικών συσκευών<br>Κωδ: B.4: MC 4.1.B.4 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.27, 4.1.28):

Πρακτικές ασφαλούς περιήγησης

- Εφαρμόστε ασφαλείς συνήθειες περιήγησης, όπως η αποφυγή ύποπτων ιστότοπων και η χρήση συνδέσεων HTTPS, για να μειώσετε τον κίνδυνο κακόβουλου λογισμικού και κλοπής δεδομένων.

Ασφάλεια φυσικών συσκευών

- Αναγνωρίστε τη σημασία της φύλαξης των συσκευών με φυσική ασφάλεια, ιδίως σε δημόσιους χώρους, για την αποφυγή κλοπής και μη εξουσιοδοτημένης πρόσβασης.

## Περιγραφή

Το Micro Credential "Secure Digital Behavior and Physical Device Security" προσφέρει ένα εκτεταμένο και διαδραστικό μάθημα που αποσκοπεί στην εμπέδωση ασφαλών ψηφιακών συνηθειών και στη σαφή κατανόηση της ασφάλειας των φυσικών συσκευών. Καθοδηγεί τους εκπαιδευόμενους να υιοθετήσουν και να διατηρήσουν ασφαλείς πρακτικές περιήγησης, να εκτιμήσουν τη σημασία της ασφάλειας των φυσικών συσκευών και να εφαρμόσουν αυτές τις γνώσεις για την προστασία των συσκευών τους από κακόβουλο λογισμικό, κλοπή δεδομένων και μη εξουσιοδοτημένη πρόσβαση.

Στο πρώτο μέρος του μαθήματος, η έμφαση δίνεται στην προώθηση της ασφαλούς ψηφιακής συμπεριφοράς. Οι συμμετέχοντες θα μάθουν για ασφαλείς συνήθειες περιήγησης, όπως η χρήση ασφαλών συνδέσεων (HTTPS), η αποφυγή ύποπτων ιστότοπων και λήψεων και η αναγνώριση και αντιμετώπιση προσπαθειών phishing. Θα μάθουν επίσης για τις πιθανές συνέπειες των μολύνσεων από κακόβουλο λογισμικό και της κλοπής δεδομένων, ενισχύοντας την κατανόησή τους για τη σημασία των ασφαλών συνηθειών περιήγησης. Η ενότητα αυτή περιλαμβάνει πρακτικές ασκήσεις και παραδείγματα, επιτρέποντας στους συμμετέχοντες να εφαρμόσουν όσα έμαθαν σε πραγματικά σενάρια.

Το δεύτερο μέρος του μαθήματος είναι αφιερωμένο στην ασφάλεια φυσικών συσκευών. Τονίζεται η σημασία της φύλαξης των συσκευών με φυσική ασφάλεια, ιδίως σε δημόσιους χώρους, για την αποφυγή κλοπής και μη εξουσιοδοτημένης πρόσβασης. Οι συμμετέχοντες θα μάθουν για διάφορους τρόπους φυσικής ασφάλειας των συσκευών τους, όπως κλειδαριές συσκευών, βιομετρικός έλεγχος ταυτότητας και χρήση λύσεων ασφαλούς αποθήκευσης. Θα κατανοήσουν επίσης τους πιθανούς κινδύνους από την αφή των συσκευών χωρίς επίβλεψη ή την αποθήκευσή τους σε εύκολα προσβάσιμες τοποθεσίες.

Επιπλέον, το μάθημα υπογραμμίζει επίσης την αλληλεπίδραση μεταξύ της ψηφιακής συμπεριφοράς και της φυσικής ασφάλειας, καθώς και τον τρόπο με τον οποίο οι δύο αυτοί τομείς μπορούν να αλληλοσυμπληρώνονται για τη δημιουργία μιας ολοκληρωμένης προσέγγισης ασφάλειας. Οι συμμετέχοντες θα μάθουν πώς να εξισορροπούν την ευκολία της χρήσης των συσκευών με την ανάγκη για ασφάλεια και πώς μικρές αλλαγές στις συνήθειές τους μπορούν να βελτιώσουν σημαντικά τη συνολική τους στάση ασφαλείας.

Με την ολοκλήρωση αυτού του Micro Credential, οι συμμετέχοντες θα έχουν αναπτύξει μια βαθιά κατανόηση της ασφαλούς ψηφιακής συμπεριφοράς και της ασφάλειας των φυσικών συσκευών και θα είναι σε θέση να εφαρμόζουν αυτές τις έννοιες για την αποτελεσματική προστασία των ψηφιακών δεδομένων και των συσκευών τους. Το πρόγραμμα ευθυγραμμίζεται με τις προσπάθειες της Ευρωπαϊκής Ένωσης για την αύξηση του ψηφιακού αλφαβητισμού και της ασφάλειας, καθιστώντας το απαραίτητο σύνολο δεξιοτήτων για κάθε πολίτη που ασχολείται με την ψηφιακή τεχνολογία.

Σύμφωνα με τις προσπάθειες της Ευρωπαϊκής Ένωσης να ενισχύσει τον ψηφιακό αλφαβητισμό και την ασφάλεια των πολιτών της, αυτό το Micro Credential προσφέρει μια επικυρωμένη μαρτυρία της εμπειρίας του εκπαιδευόμενου στην άσκηση ασφαλούς ψηφιακής συμπεριφοράς και στη διατήρηση της ασφάλειας των φυσικών συσκευών.

## Ερωτήσεις

Για πρακτικές ασφαλούς περιήγησης:

1. Εξηγήστε τη σημασία της χρήσης συνδέσεων HTTPS κατά την περιήγηση στο διαδίκτυο. Πώς συμβάλλει αυτή η πρακτική στη μείωση του κινδύνου κακόβουλου λογισμικού και κλοπής δεδομένων;
2. Ποιες είναι ορισμένες κόκκινες σημαίες που μπορεί να υποδεικνύουν ότι ένας ιστότοπος είναι ύποπτος ή δυνητικά μη ασφαλής; Πώς θα αντιμετωπίζατε τη συνάντηση με έναν τέτοιο ιστότοπο;

Για την ασφάλεια φυσικών συσκευών:

3. Γιατί είναι ζωτικής σημασίας η φυσική ασφάλεια των συσκευών σας, ιδίως σε δημόσιους χώρους; Ποιοι πιθανοί κίνδυνοι μπορεί να προκύψουν αν αφήσετε τη συσκευή σας χωρίς επίβλεψη;

4. Περιγράψτε ορισμένα πρακτικά μέτρα που θα μπορούσατε να λάβετε για να διασφαλίσετε τη φυσική ασφάλεια των συσκευών σας όταν βρίσκεστε σε δημόσιο χώρο.

# Ενημέρωση για τις ψηφιακές απειλές και διαχείριση κωδικών πρόσβασης (MC 4.1.B.5)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ενημέρωση για τις ψηφιακές απειλές και διαχείριση κωδικών πρόσβασης<br>**Κωδ: B.5** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.29, 4.1.30):

Κίνδυνοι δημόσιων σταθμών φόρτισης

- Προσδιορίστε τους κινδύνους που σχετίζονται με τη χρήση δημόσιων σταθμών φόρτισης και το ενδεχόμενο κλοπής δεδομένων ή εγκατάστασης κακόβουλου λογισμικού.

Ασφαλής διαχείριση κωδικού πρόσβασης

- Η δυνατότητα εφαρμογής ενός διαχειριστή κωδικών πρόσβασης για την ασφαλή αποθήκευση και δημιουργία σύνθετων κωδικών πρόσβασης για διάφορους διαδικτυακούς λογαριασμούς, μειώνοντας τον κίνδυνο παραβιάσεων ασφαλείας που σχετίζονται με τους κωδικούς πρόσβασης.

## Περιγραφή

Το Micro Credential "Digital Threats Awareness and Password Management" παρέχει ένα ολοκληρωμένο πρόγραμμα που έχει ως στόχο να ενισχύσει την κατανόηση των συμμετεχόντων για τις διάφορες ψηφιακές απειλές και τις επιπτώσεις τους και να τους εξοπλίσει με αποτελεσματικές πρακτικές διαχείρισης κωδικών πρόσβασης. Αυτό το Micro Credential περιλαμβάνει τους κινδύνους που σχετίζονται με τους δημόσιους σταθμούς φόρτισης και υπογραμμίζει την αξία των διαχειριστών κωδικών πρόσβασης για την εξασφάλιση ψηφιακών ταυτοτήτων και περιουσιακών στοιχείων.

Στο πρώτο τμήμα του μαθήματος, οι εκπαιδευόμενοι θα εντρυφήσουν στο σύνθετο τοπίο των ψηφιακών απειλών. Θα εξερευνήσουν διάφορες μορφές απειλών στον κυβερνοχώρο, όπως κακόβουλο λογισμικό, phishing, ransomware και παραβιάσεις δεδομένων, και θα μάθουν πώς να εντοπίζουν και να αντιδρούν σε αυτές τις απειλές. Ιδιαίτερη έμφαση θα δοθεί στους κινδύνους που σχετίζονται με τη χρήση δημόσιων σταθμών φόρτισης, οι οποίοι μπορούν δυνητικά να εκθέσουν τους χρήστες σε "juice jacking" - μια κυβερνοεπίθεση που περιλαμβάνει τη μη εξουσιοδοτημένη πρόσβαση και χειραγώγηση συσκευών μέσω θυρών φόρτισης USB. Οι συμμετέχοντες θα αποκτήσουν επίγνωση της σημασίας της χρήσης ασφαλών λύσεων φόρτισης, όπως προσωπικοί φορτιστές ή power banks, και της κατανόησης των κινδύνων των δημόσιων σταθμών φόρτισης.

Η δεύτερη συνιστώσα αυτού του Micro Credential επικεντρώνεται στο κρίσιμο θέμα της διαχείρισης κωδικών πρόσβασης. Οι εκπαιδευόμενοι θα κατανοήσουν τη σημασία της δημιουργίας ισχυρών, μοναδικών κωδικών πρόσβασης για διαφορετικούς διαδικτυακούς λογαριασμούς και πώς η επαναχρησιμοποίηση κωδικών πρόσβασης μπορεί να οδηγήσει σε παραβιάσεις της ασφάλειας. Το μάθημα τονίζει τη χρήση των διαχειριστών κωδικών πρόσβασης, οι οποίοι βοηθούν τους χρήστες να αποθηκεύουν και να δημιουργούν σύνθετους κωδικούς πρόσβασης με ασφάλεια, μειώνοντας έτσι σημαντικά τον κίνδυνο περιστατικών ασφαλείας που σχετίζονται με τους κωδικούς πρόσβασης. Οι εκπαιδευόμενοι θα γνωρίσουν διάφορους διαχειριστές κωδικών πρόσβασης, μαθαίνοντας πώς να τους χρησιμοποιούν αποτελεσματικά για τη διαχείριση της ψηφιακής τους ταυτότητας.

Εκτός από αυτά τα βασικά θέματα, το μάθημα θα προσφέρει πρακτικές οδηγίες και συμβουλές για τη διατήρηση της προσωπικής διαδικτυακής ασφάλειας, όπως τακτικές ενημερώσεις λογισμικού, έλεγχο ταυτότητας πολλαπλών παραγόντων, ασφαλείς συνήθειες περιήγησης και ασφαλή χειρισμό ύποπτων συνδέσμων ή λήψεων.

Στο τέλος αυτού του Micro Credential, οι συμμετέχοντες θα έχουν αποκτήσει μια ισχυρή κατανόηση των ψηφιακών απειλών και ένα σύνολο ισχυρών δεξιοτήτων διαχείρισης κωδικών πρόσβασης, που θα τους επιτρέψει να περιηγηθούν στον ψηφιακό κόσμο με αυξημένη ασφάλεια και αυτοπεποίθηση. Ευθυγραμμισμένο με τη δέσμευση της Ευρωπαϊκής Ένωσης για ψηφιακό αλφαβητισμό και ασφάλεια, το μάθημα αυτό παρέχει ανεκτίμητες δεξιότητες για κάθε άτομο στη σύγχρονη ψηφιακή εποχή. Σύμφωνα με τη δέσμευση της Ευρωπαϊκής Ένωσης για την προώθηση του ψηφιακού αλφαβητισμού και της ασφάλειας, αυτό το Micro Credential παρέχει μια πιστοποιημένη μαρτυρία της επάρκειας του εκπαιδευόμενου στην αναγνώριση ψηφιακών απειλών και στην ασφαλή διαχείριση κωδικών πρόσβασης.

## Ερωτήσεις

Για τους κινδύνους των δημόσιων σταθμών φόρτισης:

1. Ποιοι είναι οι πιθανοί κίνδυνοι που σχετίζονται με τη χρήση δημόσιων σταθμών φόρτισης για τις συσκευές σας, όπως smartphones ή φορητούς υπολογιστές; Πώς θα μπορούσε η χρήση δημόσιου σταθμού φόρτισης να οδηγήσει σε κλοπή

δεδομένων ή εγκατάσταση κακόβουλου λογισμικού;

2. Περιγράψτε ορισμένες προφυλάξεις που μπορείτε να λάβετε για να προστατεύσετε τη συσκευή σας από κινδύνους όταν χρησιμοποιείτε δημόσιους σταθμούς φόρτισης.

Για ασφαλή διαχείριση κωδικών πρόσβασης:

3. Εξηγήστε τη σημασία της χρήσης ενός διαχειριστή κωδικών πρόσβασης για την ασφαλή αποθήκευση και δημιουργία σύνθετων κωδικών πρόσβασης για διάφορους διαδικτυακούς λογαριασμούς. Πώς μειώνει αυτή η πρακτική τον κίνδυνο παραβίασης της ασφάλειας που σχετίζεται με τον κωδικό πρόσβασης;
4. Ποια είναι μερικά βασικά χαρακτηριστικά που θα αναζητούσατε σε έναν διαχειριστή κωδικών πρόσβασης για να διασφαλίσετε ότι ανταποκρίνεται στις ανάγκες ασφαλείας σας;

# Ασφάλεια συσκευής και συντήρηση λογισμικού (MC 4.1.B.6)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ασφάλεια συσκευών και συντήρηση λογισμικού<br>**Κωδ: B.6** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.31, 4.1.32):

Βελτίωση ασφάλειας συσκευής

- Εφαρμόστε χαρακτηριστικά ασφαλείας για συγκεκριμένες συσκευές, όπως βιομετρική πιστοποίηση ταυτότητας ή κρυπτογράφηση συσκευής, για να ενισχύσετε την προστασία των ευαίσθητων δεδομένων.

Ενημέρωση για τη συντήρηση λογισμικού

- Κατανοήστε τους κινδύνους από τη χρήση ξεπερασμένου ή μη υποστηριζόμενου λογισμικού στις συσκευές σας και τη σημασία της ενημέρωσης ή αντικατάστασης του λογισμικού αυτού για τη διατήρηση της ασφάλειας.

## Περιγραφή

Το Micro Credential "Device Security and Software Maintenance" προσφέρει ένα ολοκληρωμένο πρόγραμμα σπουδών που στοχεύει στην παροχή στους εκπαιδευόμενους μιας σε βάθος κατανόησης της ασφάλειας των συσκευών και του καθοριστικού ρόλου της συντήρησης λογισμικού στη διασφάλιση ισχυρής ψηφιακής προστασίας.

Στο πρώτο τμήμα του μαθήματος, το οποίο επικεντρώνεται στην ασφάλεια των συσκευών, οι συμμετέχοντες θα εμβαθύνουν σε διάφορους τρόπους ενίσχυσης της ασφάλειας των συσκευών τους. Θα μάθουν για το πλήθος των χαρακτηριστικών ασφαλείας συγκεκριμένων συσκευών που είναι διαθέσιμα στο σημερινό τεχνολογικό τοπίο, όπως βιομετρικός έλεγχος ταυτότητας, κρυπτογράφηση συσκευών, μηχανισμοί ασφαλούς εκκίνησης, τείχη προστασίας και πολλά άλλα. Μέσα από πρακτικά παραδείγματα και σενάρια, οι εκπαιδευόμενοι θα ανακαλύψουν πώς να αξιοποιούν αυτά τα χαρακτηριστικά για να ενισχύσουν την προστασία των ευαίσθητων δεδομένων τους και να αποκρούσουν πιθανές απειλές στον κυβερνοχώρο. Θα αποκτήσουν τη γνώση να διαμορφώνουν αυτές τις ρυθμίσεις σύμφωνα με τις συγκεκριμένες ανάγκες και περιπτώσεις χρήσης τους, δίνοντάς τους περαιτέρω τη δυνατότητα να αναλάβουν τον έλεγχο της ψηφιακής τους ασφάλειας.

Η δεύτερη συνιστώσα του μαθήματος εστιάζει στη συντήρηση του λογισμικού, μια πτυχή της ασφάλειας των συσκευών που συχνά παραβλέπεται από πολλούς χρήστες. Οι συμμετέχοντες θα κατανοήσουν τους κινδύνους που συνδέονται με τη χρήση ξεπερασμένου ή μη υποστηριζόμενου λογισμικού, όπως η αυξημένη ευπάθεια σε επιθέσεις κακόβουλου λογισμικού, παραβιάσεις δεδομένων και άλλες απειλές κυβερνοασφάλειας. Το μάθημα θα αναδείξει τη σημασία των τακτικών ενημερώσεων λογισμικού, των επιδιορθώσεων και της έγκαιρης αντικατάστασης μη υποστηριζόμενου λογισμικού. Θα διδάξει στους εκπαιδευόμενους να ερμηνεύουν τα αρχεία καταγραφής ενημερώσεων και να κατανοούν τις βελτιώσεις ασφαλείας που συνοδεύουν κάθε ενημέρωση λογισμικού.

Επιπλέον, το μάθημα θα θίξει τις πρακτικές ασφαλούς εγκατάστασης και αφαίρεσης λογισμικού, διασφαλίζοντας ότι οι εκπαιδευόμενοι κατανοούν πώς να προσθέτουν και να αφαιρούν με ασφάλεια λογισμικό από τις συσκευές τους χωρίς να θέτουν σε κίνδυνο την ασφάλεια.

Με την ολοκλήρωση αυτού του Micro Credential, οι συμμετέχοντες θα έχουν μια σταθερή κατανόηση των τεχνικών βελτίωσης της ασφάλειας των συσκευών και του κρίσιμου ρόλου της συντήρησης λογισμικού στη διατήρηση ενός ασφαλούς ψηφιακού περιβάλλοντος. Το πρόγραμμα ευθυγραμμίζεται με τη δέσμευση της Ευρωπαϊκής Ένωσης για την προώθηση του ψηφιακού αλφαβητισμού και της ασφάλειας, καθιστώντας το μια πολύτιμη προσθήκη στις ψηφιακές δεξιότητες οποιουδήποτε. Το μάθημα αυτό θα αποτελέσει πλεονέκτημα για κάθε άτομο ή επαγγελματία που θέλει να διασφαλίσει ότι οι συσκευές του είναι όσο το δυνατόν πιο ασφαλείς, συμβάλλοντας σε έναν ασφαλέστερο και ασφαλέστερο ψηφιακό κόσμο.

Σύμφωνα με τη δέσμευση της Ευρωπαϊκής Ένωσης για την ενίσχυση του ψηφιακού αλφαβητισμού και της ασφάλειας, αυτό το Πιστοποιητικό Micro παρέχει μια πιστοποιημένη απόδειξη για τη γνώση του εκπαιδευόμενου στη διατήρηση της ασφάλειας των συσκευών και την κατανόηση του ρόλου της συντήρησης λογισμικού στην κυβερνοασφάλεια.

## Ερωτήσεις

Για την ενίσχυση της ασφάλειας συσκευής:

1. Εξηγήστε τη σημασία της εφαρμογής χαρακτηριστικών ασφαλείας για συγκεκριμένες συσκευές, όπως βιομετρικός έλεγχος ταυτότητας ή κρυπτογράφηση συσκευής. Πώς αυτά τα χαρακτηριστικά ενισχύουν την προστασία των ευαίσθητων δεδομένων;
2. Περιγράψτε τα βήματα που θα κάνατε για να ενεργοποιήσετε τον βιομετρικό έλεγχο ταυτότητας (π.χ. αναγνώριση

δακτυλικών αποτυπωμάτων ή προσώπου) στο smartphone ή το φορητό σας υπολογιστή. Πώς σας ωφελεί αυτό το πρόσθετο επίπεδο ασφάλειας;

Για ευαισθητοποίηση στη συντήρηση λογισμικού:

3. Συζητήστε τους κινδύνους που σχετίζονται με τη χρήση ξεπερασμένου ή μη υποστηριζόμενου λογισμικού στις συσκευές σας. Πώς μπορεί το ξεπερασμένο λογισμικό να θέσει σε κίνδυνο την ασφάλεια των δεδομένων και της συσκευής σας;
4. Φανταστείτε ότι λαμβάνετε μια ειδοποίηση για μια ενημέρωση λογισμικού στον υπολογιστή σας. Πώς θα χειριζόσασταν αυτή την ενημέρωση για να διασφαλίσετε ότι η ασφάλεια και η λειτουργικότητα της συσκευής σας διατηρούνται;

## Διαχείριση ασφάλειας συσκευών και διατήρηση της ιδιωτικής ζωής (MC 4.1.B.7)

### Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Διαχείριση ασφάλειας συσκευών και διαφύλαξη απορρήτου<br>**Κωδ: B.7** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.33, 4.1.34 και 4.1.35):

Αναγνώριση ύποπτων δραστηριοτήτων

- Εντοπίστε ύποπτες δραστηριότητες στις συσκευές σας, όπως απροσδόκητα αναδυόμενα παράθυρα ή ασυνήθιστη αποστράγγιση της μπαταρίας, οι οποίες μπορεί να υποδεικνύουν πιθανό κακόβουλο λογισμικό ή παραβιάσεις της ασφάλειας.

Αξιολόγηση ασφάλειας συσκευής

- Αξιολογήστε τα χαρακτηριστικά ασφαλείας των διαφόρων συσκευών και επιλέξτε τις πιο ασφαλείς επιλογές με βάση τις συγκεκριμένες ανάγκες και περιπτώσεις χρήσης σας.

Διαχείριση δικαιωμάτων εφαρμογών

- Αναγνωρίστε τη σημασία της τακτικής επανεξέτασης και διαχείρισης των δικαιωμάτων των εφαρμογών για τον περιορισμό της πρόσβασης σε προσωπικά δεδομένα και τη διασφάλιση της ιδιωτικής ζωής.

## Περιγραφή

Το Micro Credential "Device Security Management and Privacy Preservation" παρέχει ένα ολοκληρωμένο μάθημα προσαρμοσμένο στην ενδυνάμωση των ατόμων με τις γνώσεις και τις δεξιότητες για ασφαλή πλοήγηση στον ψηφιακό κόσμο. Επικεντρώνεται σε τρεις θεμελιώδεις τομείς: εντοπισμός πιθανών απειλών ασφαλείας, αξιολόγηση των χαρακτηριστικών ασφαλείας της συσκευής και αποτελεσματική διαχείριση των δικαιωμάτων χρήσης εφαρμογών.

Το πρώτο μέρος του μαθήματος είναι αφιερωμένο στον εντοπισμό πιθανών απειλών για την ασφάλεια. Οι συμμετέχοντες θα εκτεθούν στο φάσμα των απειλών κυβερνοασφάλειας που υπάρχουν στον ψηφιακό κόσμο, από κακόβουλο λογισμικό και ιούς έως απόπειρες ηλεκτρονικού "ψαρέματος" και επιθέσεις ransomware. Θα αποκτήσουν κατανόηση του τρόπου λειτουργίας αυτών των απειλών και της δυνητικής ζημίας που μπορούν να προκαλέσουν. Οπλισμένοι με αυτές τις γνώσεις, οι εκπαιδευόμενοι θα είναι καλύτερα προετοιμασμένοι να αναγνωρίζουν αυτές τις απειλές όταν τις συναντούν και να αντιδρούν κατάλληλα για να μετριάσουν τις πιθανές ζημιές.

Η δεύτερη συνιστώσα του μαθήματος εξετάζει την αξιολόγηση των χαρακτηριστικών ασφαλείας των συσκευών. Καθώς βασιζόμαστε όλο και περισσότερο σε ψηφιακές συσκευές για διάφορες προσωπικές και επαγγελματικές εργασίες, η κατανόηση του τρόπου διατήρησης της ασφάλειας αυτών των συσκευών καθίσταται υψίστης σημασίας. Οι συμμετέχοντες θα μάθουν για τα διάφορα χαρακτηριστικά ασφαλείας των συσκευών και πώς να αξιολογούν την αποτελεσματικότητά τους. Θα μάθουν για την κρυπτογράφηση, τον βιομετρικό έλεγχο ταυτότητας, τις διαδικασίες ασφαλούς εκκίνησης και πολλά άλλα. Με τον τρόπο αυτό, θα είναι σε θέση να λαμβάνουν τεκμηριωμένες αποφάσεις κατά την επιλογή συσκευών και τη ρύθμιση των ρυθμίσεων ασφαλείας τους.

Το τελευταίο τμήμα του μαθήματος επικεντρώνεται στην αποτελεσματική διαχείριση των δικαιωμάτων των εφαρμογών. Στην εποχή των εφαρμογών για κινητά τηλέφωνα, είναι σημαντικό να κατανοήσετε την πρόσβαση που έχουν αυτές οι εφαρμογές σε προσωπικά δεδομένα. Το μάθημα θα καθοδηγήσει τους εκπαιδευόμενους κατά τη διαδικασία εξέτασης και διαχείρισης των αδειών χρήσης εφαρμογών, τον περιορισμό της περιττής πρόσβασης σε προσωπικά δεδομένα και την κατανόηση των πιθανών κινδύνων των εφαρμογών με υπερβολικές άδειες χρήσης.

Στο τέλος αυτού του Micro Credential, οι συμμετέχοντες θα διαθέτουν ένα ισχυρό σύνολο δεξιοτήτων που όχι μόνο θα ενισχύουν τη δική τους ψηφιακή ασφάλεια, αλλά θα μπορούν επίσης να το μοιραστούν στις κοινότητές τους για να προωθήσουν ένα ασφαλέστερο ψηφιακό περιβάλλον για όλους. Το μάθημα ευθυγραμμίζεται με τη δέσμευση της Ευρωπαϊκής Ένωσης για την ενίσχυση του ψηφιακού αλφαβητισμού και της ψηφιακής ασφάλειας, καθιστώντας το μια ουσιαστική προσθήκη στο σύνολο των δεξιοτήτων του σύγχρονου, υπεύθυνου ψηφιακού πολίτη.

Ευθυγραμμισμένο με την αποστολή της Ευρωπαϊκής Ένωσης να ενισχύσει τον ψηφιακό αλφαβητισμό και την ασφάλεια, αυτό το Micro Credential παρέχει μια πιστοποιημένη μαρτυρία για την επάρκεια του εκπαιδευόμενου στη διαχείριση της ασφάλειας των συσκευών και τη διαφύλαξη της ιδιωτικής ζωής.

## Ερωτήσεις

Για την ταυτοποίηση ύποπτων δραστηριοτήτων:

1. Ποια είναι μερικά σημάδια ύποπτων δραστηριοτήτων στη συσκευή σας που μπορεί να υποδεικνύουν πιθανό κακόβουλο λογισμικό ή παραβιάσεις της ασφάλειας;
2. Περιγράψτε μια κατάσταση στην οποία αντιμετωπίσατε ένα απροσδόκητο αναδυόμενο παράθυρο στη συσκευή σας. Πώς χειριστήκατε την κατάσταση για να διασφαλίσετε την ασφάλεια της συσκευής σας;

Για την αξιολόγηση της ασφάλειας της συσκευής:

3. Κατά την αξιολόγηση των χαρακτηριστικών ασφαλείας των διαφόρων συσκευών, ποιοι είναι ορισμένοι παράγοντες που θα λαμβάνατε υπόψη για να καθορίσετε ποια συσκευή είναι η πιο ασφαλής για τις συγκεκριμένες ανάγκες και περιπτώσεις χρήσης σας;
4. Συγκρίνετε τα χαρακτηριστικά ασφαλείας ενός smartphone και ενός tablet. Με βάση την αξιολόγησή σας, ποια συσκευή θα επιλέγατε για ασφαλή χρήση και γιατί;

Για τη διαχείριση δικαιωμάτων εφαρμογών:

5. Γιατί είναι απαραίτητο να επανεξετάζετε και να διαχειρίζεστε τακτικά τα δικαιώματα εφαρμογών στις συσκευές σας; Πώς μπορεί αυτή η πρακτική να περιορίσει την πρόσβαση σε προσωπικά δεδομένα και να διασφαλίσει την ιδιωτικότητά σας;
6. Φανταστείτε ότι έχετε εγκαταστήσει μια νέα εφαρμογή στο smartphone σας. Πώς θα ελέγξετε και θα διαχειριστείτε τα δικαιώματά της για να προστατεύσετε το απόρρητό σας;

# Ασφάλεια απομακρυσμένης εργασίας και ασφάλεια ψηφιακής αρχειοθέτησης (MC 4.1.B.8)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ασφάλεια απομακρυσμένης εργασίας και ασφάλεια ψηφιακής αρχειοθέτησης<br>**Κωδ: B.8** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.36, 4.1.37 και 4.1.38):

Ασφάλεια απομακρυσμένης εργασίας

- Επεκτείνετε τα μέτρα ασφαλείας των συσκευών σας για να συμπεριλάβετε απομακρυσμένα περιβάλλοντα εργασίας, εξασφαλίζοντας προστασία δεδομένων και ασφαλή κανάλια επικοινωνίας.

Διευκόλυνση της ευαισθητοποίησης σε θέματα ασφάλειας

- Διευκολύνετε την ευαισθητοποίηση των συναδέλφων ή των μελών της οικογένειάς σας σε θέματα ασφάλειας, εκπαιδεύοντάς τους στις βέλτιστες πρακτικές για την ασφάλεια των συσκευών και την ασφαλή συμπεριφορά στο διαδίκτυο.

Ενημέρωση για την ασφάλεια του αρχείου

- Αναγνωρίστε τους πιθανούς κινδύνους που σχετίζονται με το άνοιγμα αρχείων zip ή rar από μη αξιόπιστες ή άγνωστες πηγές.

## Περιγραφή

Το μικροπιστοποιητικό "Ασφάλεια απομακρυσμένης εργασίας και προώθηση ψηφιακού γραμματισμού" παρέχει ένα εκτεταμένο και σε βάθος μάθημα που επικεντρώνεται στην ασφάλεια απομακρυσμένων περιβαλλόντων εργασίας και στην προώθηση του ψηφιακού γραμματισμού σε προσωπικό και επαγγελματικό επίπεδο. Το πρόγραμμα διευκρινίζει επίσης τους πιθανούς κινδύνους που σχετίζονται με το χειρισμό αρχείων από αβέβαιες ή άγνωστες πηγές.

Καθώς εισερχόμαστε σε μια εποχή που εξαρτάται όλο και περισσότερο από την εξ αποστάσεως εργασία και την ψηφιακή επικοινωνία, το μάθημα αυτό έχει ως στόχο να βοηθήσει τους εκπαιδευόμενους να προσαρμοστούν σε αυτές τις αλλαγές με ασφάλεια και υπευθυνότητα. Οι συμμετέχοντες θα αποκτήσουν εικόνα για τις διάφορες προκλήσεις ασφαλείας που θέτουν τα περιβάλλοντα απομακρυσμένης εργασίας, όπως το απόρρητο των δεδομένων, τα μη ασφαλή δίκτυα, οι επιθέσεις phishing και άλλες πιθανές απειλές κυβερνοασφάλειας. Θα μάθουν επίσης αποτελεσματικές στρατηγικές για την ασφάλεια των εικονικών χώρων εργασίας τους, όπως η χρήση ασφαλών καναλιών επικοινωνίας, η ισχυρή κρυπτογράφηση, ο έλεγχος ταυτότητας πολλαπλών παραγόντων και οι ασφαλείς ψηφιακές συνήθειες.

Μια βασική πτυχή αυτού του μαθήματος είναι η διευκόλυνση και η προώθηση του ψηφιακού αλφαβητισμού. Οι συμμετέχοντες θα μάθουν πώς να καθοδηγούν τους συναδέλφους ή τα μέλη της οικογένειάς τους προς την κατανόηση και την υιοθέτηση βέλτιστων πρακτικών για την ασφάλεια των συσκευών και την ασφαλή διαδικτυακή συμπεριφορά. Αυτό περιλαμβάνει εκπαίδευση σχετικά με την υγιεινή των κωδικών πρόσβασης, τις ασφαλείς συνήθειες περιήγησης, τα δικαιώματα χρήσης εφαρμογών και την αναγνώριση πιθανών προσπαθειών phishing ή απάτης. Με την προώθηση του ψηφιακού αλφαβητισμού, οι συμμετέχοντες μπορούν να συμβάλουν στη δημιουργία ασφαλέστερων ψηφιακών κοινοτήτων στη δουλειά, στο σπίτι και όχι μόνο.

Το μάθημα διερευνά επίσης τους κινδύνους που σχετίζονται με το άνοιγμα αρχείων όπως αρχεία zip ή rar από μη αξιόπιστες ή άγνωστες πηγές. Οι συμμετέχοντες θα μάθουν για τις πιθανές απειλές που μπορεί να ενέχουν αυτά τα αρχεία, όπως κακόβουλο λογισμικό, ransomware ή άλλες μορφές επιβλαβούς λογισμικού. Το μάθημα θα καθοδηγήσει τους εκπαιδευόμενους σχετικά με τις ασφαλέστερες πρακτικές χειρισμού αυτών των αρχείων, όπως η επαλήθευση της πηγής, η χρήση προστατευτικού λογισμικού και η κατανόηση της σημασίας της τακτικής δημιουργίας αντιγράφων ασφαλείας του συστήματος.

Με την ολοκλήρωση αυτού του Micro Credential, οι εκπαιδευόμενοι θα είναι καλύτερα εξοπλισμένοι για να διασφαλίσουν τα απομακρυσμένα περιβάλλοντα εργασίας τους, να εκπαιδεύσουν τους άλλους σε ασφαλείς ψηφιακές πρακτικές και να περιηγηθούν αποτελεσματικότερα στις πιθανές ψηφιακές απειλές. Αυτό ευθυγραμμίζεται με τη δέσμευση της Ευρωπαϊκής Ένωσης για την ενίσχυση του ψηφιακού αλφαβητισμού και της ασφάλειας, καθιστώντας αυτό μια πολύτιμη επένδυση στην εκπαίδευση κάθε ψηφιακού πολίτη.

Σύμφωνα με τη δέσμευση της Ευρωπαϊκής Ένωσης να ενισχύσει τον ψηφιακό αλφαβητισμό και την ασφάλεια των πολιτών της, αυτό το μικροπιστοποιητικό παρέχει πιστοποιημένη επάρκεια των ικανοτήτων του εκπαιδευόμενου στη διαχείριση της ασφάλειας της απομακρυσμένης εργασίας και στην προώθηση του ψηφιακού αλφαβητισμού.

## Ερωτήσεις

Για ασφάλεια απομακρυσμένης εργασίας:

1. Εξηγήστε πώς μπορείτε να επεκτείνετε τα μέτρα ασφαλείας των συσκευών σας για να διασφαλίσετε την προστασία των δεδομένων και τα ασφαλή κανάλια επικοινωνίας κατά την απομακρυσμένη εργασία. Ποιες πρόσθετες προφυλάξεις θα λαμβάνατε σε σύγκριση με την εργασία από ένα ασφαλές περιβάλλον γραφείου;
2. Περιγράψτε μια κατάσταση στην οποία τα μέτρα ασφαλείας για την απομακρυσμένη εργασία ήταν ζωτικής σημασίας για την προστασία ευαίσθητων δεδομένων ή την αποτροπή παραβίασης της ασφάλειας.

Για τη διευκόλυνση της ευαισθητοποίησης σε θέματα ασφάλειας:

3. Ως άτομο με επίγνωση της ασφάλειας, πώς θα διευκολύνατε την επίγνωση της ασφάλειας μεταξύ των συναδέλφων ή των μελών της οικογένειάς σας; Σε ποια θέματα και ποιες βέλτιστες πρακτικές θα εστιάζατε κατά τη διάρκεια των συνεδριών ευαισθητοποίησής σας;
4. Ποιες είναι κάποιες στρατηγικές που μπορείτε να εφαρμόσετε για να ενθαρρύνετε μια κουλτούρα ευαισθητοποιημένης ασφάλειας μεταξύ των συναδέλφων ή των μελών της οικογένειάς σας;

Για την ευαισθητοποίηση σε θέματα ασφάλειας αρχείων:

5. Συζητήστε τους πιθανούς κινδύνους που σχετίζονται με το άνοιγμα αρχείων zip ή rar από μη αξιόπιστες ή άγνωστες πηγές. Πώς μπορούν τέτοια αρχεία να χρησιμοποιηθούν για τη διάδοση κακόβουλου λογισμικού ή για απόπειρες phishing;
6. Φανταστείτε ότι λαμβάνετε ένα αρχείο zip από μια άγνωστη διεύθυνση ηλεκτρονικού ταχυδρομείου. Ποιες προφυλάξεις θα λαμβάνατε πριν ανοίξετε το αρχείο;

# Ασφάλεια φορητών συσκευών και ασφαλές κατέβασμα εφαρμογών (MC 4.1.B.9)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ασφάλεια φορητών συσκευών και ασφαλές κατέβασμα εφαρμογών<br>**Κωδ: B.9** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.39, 4.1.40):

Ασφάλεια φορητών συσκευών και μέσων

- Αναπτύξτε τη συνήθεια να διασφαλίζετε την ασφάλεια των φορητών μέσων υλικού και των συσκευών αφαίρεσης, αποφεύγοντας την εμπιστοσύνη σε μη ασφαλείς συσκευές ή περιεχόμενα μέσων.

Πρακτικές ασφαλούς λήψης εφαρμογών

- Εξηγήστε τους κινδύνους της λήψης εφαρμογών από άγνωστες πηγές και τη σημασία της χρήσης επίσημων καταστημάτων εφαρμογών.

## Περιγραφή

Το μικροπιστοποιητικό "Ασφάλεια φορητών συσκευών και ασφαλές κατέβασμα εφαρμογών" στοχεύει στην καλλιέργεια σωστών συνηθειών ασφάλειας όσον αφορά τις φορητές συσκευές και τα μέσα ενημέρωσης και στην κατανόηση των πρακτικών ασφαλούς λήψης εφαρμογών.

Μέσω αυτού του μαθήματος, οι εκπαιδευόμενοι θα αποκτήσουν τη γνώση να διακρίνουν το ασφαλές από το μη ασφαλές φορητό υλικό, και θα γίνουν πιο έμπειροι στο χειρισμό τέτοιων συσκευών με την απαραίτητη προσοχή. Θα αναπτύξουν κατανόηση των κινδύνων που σχετίζονται με μη ασφαλείς συσκευές ή μη επαληθευμένο περιεχόμενο πολυμέσων, μαθαίνοντας τη σημασία της ασφάλειας των συσκευών και τις πιθανές απειλές για την ψηφιακή τους ασφάλεια.

Επιπλέον, αυτό το Micro Credential δίνει έμφαση στα πρωτόκολλα ασφαλείας κατά τη λήψη εφαρμογών. Οι εκπαιδευόμενοι θα είναι εφοδιασμένοι με την κατανόηση των κινδύνων που σχετίζονται με τη λήψη εφαρμογών από άγνωστες πηγές, συμπεριλαμβανομένων πιθανών απειλών κακόβουλου λογισμικού, κλοπής δεδομένων και άλλων τρωτών σημείων της κυβερνοασφάλειας. Το μάθημα υπογραμμίζει τη σημασία της χρήσης επίσημων καταστημάτων εφαρμογών, τα οποία τηρούν αυστηρά πρότυπα ασφαλείας και διαδικασίες επαλήθευσης εφαρμογών.

Σύμφωνα με τη δέσμευση της Ευρωπαϊκής Ένωσης να ενισχύσει τον ψηφιακό αλφαβητισμό και την ασφάλεια, αυτό το Πιστοποιητικό Micro παρέχει μια πιστοποιημένη απόδειξη της επάρκειας του εκπαιδευόμενου στη διαχείριση της ασφάλειας φορητών συσκευών και των πρακτικών ασφαλούς λήψης εφαρμογών. Οι εκπαιδευόμενοι που ολοκληρώνουν αυτό το μάθημα θα είναι καλύτερα εξοπλισμένοι για να προστατεύουν τα ψηφιακά τους περιουσιακά στοιχεία και να περιηγούνται στον ψηφιακό κόσμο με μεγαλύτερη ασφάλεια.

Αυτό το Micro Credential ευθυγραμμίζεται με τη δέσμευση της Ευρωπαϊκής Ένωσης για την ενίσχυση του ψηφιακού αλφαβητισμού και της ασφάλειας, παρέχοντας πιστοποιημένη επάρκεια της επάρκειας του εκπαιδευόμενου στη διαχείριση της ασφάλειας φορητών συσκευών και στην εξάσκηση της ασφαλούς λήψης εφαρμογών.

## Ερωτήσεις

Για την ασφάλεια φορητών συσκευών και μέσων:

1. Γιατί είναι σημαντικό να διασφαλίζεται η ασφάλεια των φορητών μέσων υλικού και των συσκευών αφαίρεσης; Ποιοι κίνδυνοι μπορεί να προκύψουν αν εμπιστευτείτε μη ασφαλείς συσκευές ή περιεχόμενα μέσων;
2. Περιγράψτε ορισμένες προφυλάξεις που μπορείτε να λάβετε για να διασφαλίσετε την ασφάλεια των φορητών μέσων υλικού, όπως οι μονάδες USB ή οι εξωτερικοί σκληροί δίσκοι, από πιθανούς κινδύνους και απώλεια δεδομένων.

Για πρακτικές ασφαλούς λήψης εφαρμογών:

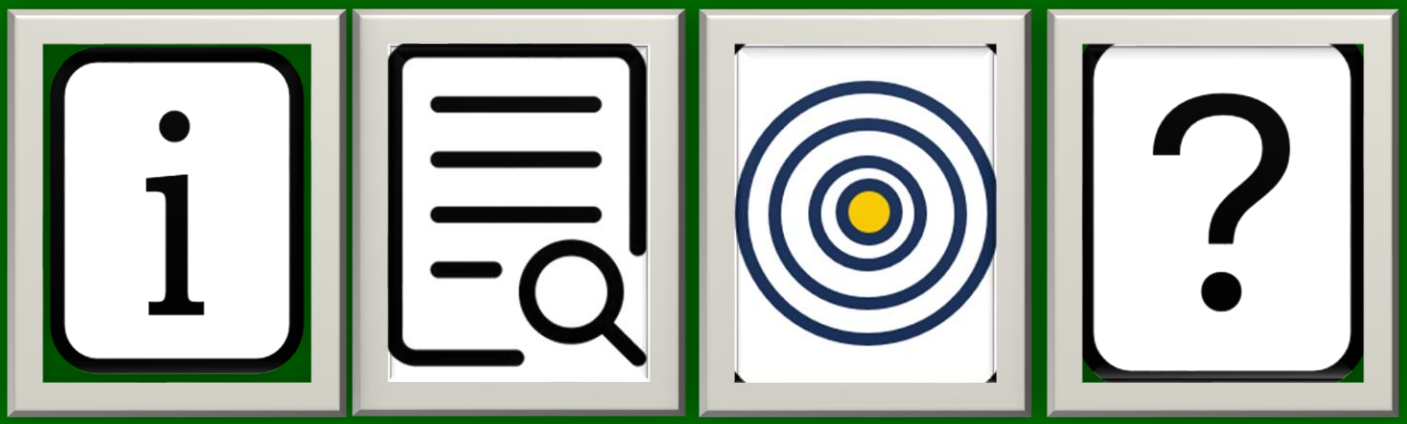
3. Συζητήστε τους πιθανούς κινδύνους που σχετίζονται με τη λήψη εφαρμογών από άγνωστες πηγές. Πώς μπορούν τέτοιες πρακτικές να θέσουν σε κίνδυνο την ασφάλεια της συσκευής και των δεδομένων σας;
4. Εξηγήστε τη σημασία της χρήσης των επίσημων καταστημάτων εφαρμογών για τη λήψη εφαρμογών. Πώς συμβάλλει αυτή η πρακτική στη διασφάλιση της ασφάλειας και της προστασίας των εφαρμογών που εγκαθιστάτε στη συσκευή σας;

Για συνδυασμό και των δύο:

5. Φανταστείτε ότι θέλετε να μεταφέρετε κάποια αρχεία στον φίλο σας χρησιμοποιώντας μια φορητή μονάδα USB. Πώς θα διασφαλίζατε την ασφάλεια της μονάδας USB και των περιεχομένων της πριν την μοιραστείτε με τον φίλο σας; Επιπλέον, πώς θα διασφαλίζατε την ασφάλεια της συσκευής σας κατά τη σύνδεση της μονάδας USB;

# ΕΠΙΠΕΔΟ ΠΡΟΗΓΜΕΝΩΝ

(Επίπεδο 5 και 6)



# Ασφάλεια προσωπικών συσκευών και βέλτιστες πρακτικές (MC 4.1.C.1)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ασφάλεια προσωπικών συσκευών και βέλτιστες πρακτικές<br>**Κωδ: C.1.C.1** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.41, 4.1.42):

- 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 εξετάζατε 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 4.1.C.2)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ασφάλεια κωδικού πρόσβασης και βέλτιστες πρακτικές<br>Κωδ: C.2: MC 4.1.C.2 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.43, 4.1.44 και 4.1.45):

- 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. Οι συμμετέχοντες, συμμετέχοντας σε πρακτικές δραστηριότητες και προσομοιώσεις, 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 4.1.C.3)

### Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ασφαλής διαχείριση συσκευών και αποδοτικότητα δεδομένων<br>Κωδ: C.3: MC 4.1.C.3 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |

| | |
|---|---|
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.46, 4.1.47):

- 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 4.1.C.4)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ψηφιακή ασφάλεια και ασφαλής χειρισμός δεδομένων Κωδικός: C.4: MC 4.1.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 4.1.48, 4.1.49 και 4.1.50):

- 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 δίνει στους εκπαιδευόμενους 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 όπου θα ήταν σκόπιμο να απενεργοποιήσετε την αυτόματη σύνδεση".
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 4.1.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<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.51, 4.1.52):

- 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 σενάρια πραγματικής ζωής, 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 σχετικά με 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 4.1.C.6)

### Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ολοκληρωμένη εκπαίδευση και εφαρμογή ασφάλειας<br>Κωδ: C.6: MC 4.1.C.6 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.53, 4.1.54 και 4.1.55):

- 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 προωθεί 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 4.1.C.7)

### Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |

| | |
|---|---|
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ενημέρωση για την ασφάλεια στον κυβερνοχώρο και προστασία συσκευών<br>Κωδ: C.7: MC 4.1.C.7 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.56, 4.1.57 και 4.1.58):

- 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 4.1.C.8)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Προηγμένες πρακτικές ασφάλειας για προσωπικές συσκευές και συστήματα<br>Κωδ: C.8: MC 4.1.C.8 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.59, 4.1.60):

- 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.

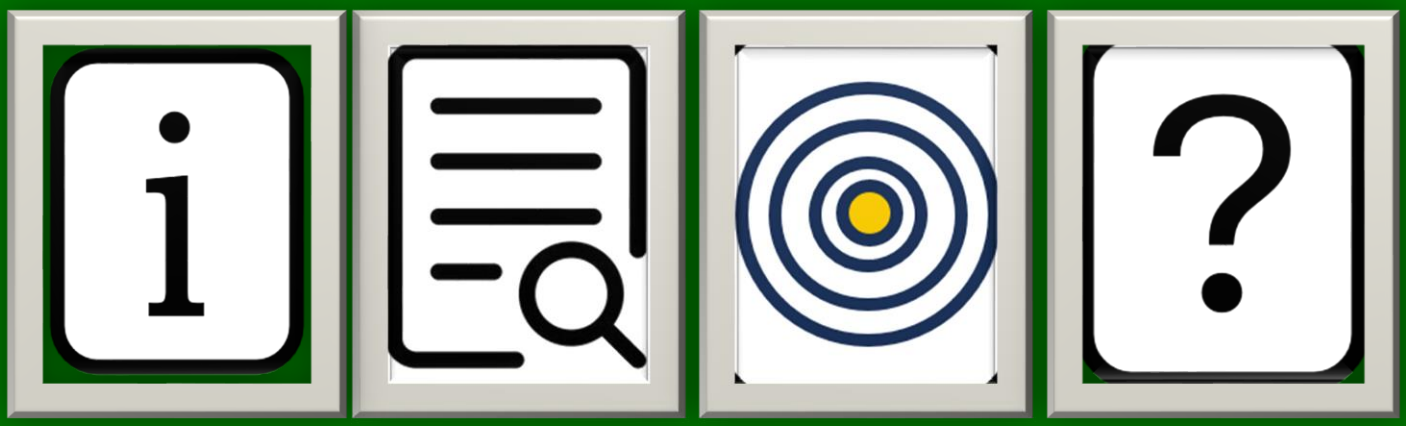
## Ερωτήσεις

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.

# ΕΠΙΠΕΔΟ ΕΜΠΕΙΡΟΓΝΩΜΟΝΟΥ

(Επίπεδο 7 και επίπεδο 8)



# Διαχείριση κινδύνων κυβερνοασφάλειας και ευαισθητοποίηση του προσωπικού (MC 4.1.D.1)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Διαχείριση κινδύνων κυβερνοασφάλειας και **ευαισθητοποίηση του** προσωπικού **Κωδ: Δ.1.Δ.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 4.1.61, 4.1.62 και 4.1.63):

- 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 εμβαθύνουν 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 4.1.D.2)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Κυβερνοασφάλεια με επίκεντρο τα δεδομένα και διαχείριση πλεοναζόντων δεδομένων<br>Κωδ: D.2: MC 4.1.D.2 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.64, 4.1.65):

- 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 ΤΠ 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 4.1.D.3)

### Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ανάπτυξη ηγεσίας και κουλτούρας στον τομέα της κυβερνοασφάλειας<br>**Κωδ: D.3** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.66, 4.1.67):

- 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. Μέσω μελετών περιπτώσεων και συζητήσεων υπό την καθοδήγηση εμπειρογνωμόνων, οι εκπαιδευόμενοι θα διερευνήσουν τις βέλτιστες πρακτικές για τη διενέργεια 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 4.1.D.4)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ασφαλής διαχείριση δεδομένων και ευαισθητοποίηση στον κυβερνοχώρο<br>**Κωδ: D.4: MC 4.1.D.4** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.68, 4.1.69 και 4.1.70):

- 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 θέση 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 στην

προστασία 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 4.1.D.5)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Προηγμένη κυβερνοασφάλεια και ηθικό χάκινγκ<br>**Κωδ: D.5** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.71, 4.1.72):

- 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 επικεντρώνεται 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. Footprinting 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 τις ευαίσθητες πληροφορίες ή τα τρωτά σημεία που ανακαλύφθηκαν κατά τη διάρκεια της αξιολόγησης για να διατηρήσετε τις δεοντολογικές 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 4.1.D.6)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Κυβερνοασφάλεια - Ασφαλείς κωδικοί πρόσβασης και διαχείριση πρόσβασης<br>**Κωδ: D.6** |

| | |
|---|---|
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.73, 4.1.74):

- 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: Εφαρμογή στρατηγικών 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 4.1.D.7)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Ενημέρωση για την ασφάλεια στον κυβερνοχώρο και διαχείριση λογαριασμών<br>Κωδ: D.7 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.75, 4.1.76):

- 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 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 4.1.D.8)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Διαχείριση κυβερνοασφάλειας - Προστασία τελικών σημείων και διατήρηση δεδομένων<br>Κωδ: D.8 |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.77, 4.1.78):

- 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 έναντι 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 περιήγησης και διαχείριση ασφάλειας (MC 4.1.D.9)

## Βασικές πληροφορίες

| | |
|---|---|
| Προσδιορισμός του μαθητή | Οποιοσδήποτε πολίτης |
| Τίτλος και κωδικός του μικροπιστοποιητικού | Βελτιστοποίηση προγράμματος περιήγησης και διαχείριση ασφάλειας<br>**Κωδ: D.9** |
| Χώρα(ες)/Περιοχή(ες) του εκδότη | ΙΡΛΑΝΔΙΑ, ΙΤΑΛΙΑ, ΚΥΠΡΟΣ, ΕΛΛΑΔΑ, ΡΟΥΜΑΝΙΑ<br>http://dsw.projectsgallery.eu |
| Φορέας(-ες) απονομής | Κοινοπραξία DSW<br>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<br>Αριθμός ερωτήσεων: 16- 20<br>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 4.1.79, 4.1.80):

- Βελτιστοποιήστε τις ρυθμίσεις και τις επιδόσεις του προγράμματος περιήγησής σας 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 τ
ης 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 επιδιορθώσεις 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.

Μέσω θεωρητικών γνώσεων και πρακτικών ασκήσεων, 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 αποτελεσματικότητα 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 της απόδοσης.
6. Πώς μπορεί η χρήση επεκτάσεων να επηρεάσει τις επιδόσεις 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: ΣΥΣΚΕΥΕΣ ΠΡΟΣΤΑΣΙΑΣ

| ΤΟΜΈΑΣ ΙΚΑΝΟΤΉΤΩΝ: ΑΣΦΆΛΕΙΑ (4) | | |
|---|---|---|
| ΙΚΑΝΟΤΗΤΑ: (4.1) | | |
| **1** | Σε βασικό επίπεδο και με καθοδήγηση, μπορώ: | • **να εντοπίζω** απλούς τρόπους προστασίας των συσκευών μου και του ψηφιακού μου περιεχομένου,<br>• **να διακρίνετε** απλούς κινδύνους και απειλές σε ψηφιακά περιβάλλοντα.<br>• **επιλέξτε** απλά μέτρα ασφαλείας και προστασίας<br>• **να εντοπίζετε** απλούς τρόπους για να λαμβάνετε δεόντως υπόψη την αξιοπιστία και την προστασία της ιδιωτικής ζωής. |
| **2** | Σε βασικό επίπεδο και με αυτονομία και κατάλληλη καθοδήγηση όπου χρειάζεται, μπορώ: | • **να εντοπίζω** απλούς τρόπους προστασίας των συσκευών μου και του ψηφιακού μου περιεχομένου.<br>• **να διακρίνετε** απλούς κινδύνους και απειλές σε ψηφιακά περιβάλλοντα.<br>• **ακολουθήστε** απλά μέτρα ασφαλείας και προστασίας.<br>• **να εντοπίζετε** απλούς τρόπους για να λαμβάνετε δεόντως υπόψη την αξιοπιστία και την προστασία της ιδιωτικής ζωής. |
| **3** | Μόνος μου και επιλύοντας απλά προβλήματα, μπορώ: | • **υποδεικνύουν** σαφώς καθορισμένους και συνήθεις τρόπους για την προστασία των συσκευών μου και του ψηφιακού μου περιεχομένου<br>• **να διακρίνουν** σαφώς καθορισμένους και συνήθεις κινδύνους και απειλές σε ψηφιακά περιβάλλοντα<br>• **επιλέξτε** σαφώς καθορισμένα και συνήθη μέτρα ασφαλείας και προστασίας.<br>• **υποδεικνύουν** σαφώς καθορισμένους και συνήθεις τρόπους για να λαμβάνεται δεόντως υπόψη η αξιοπιστία και η ιδιωτική ζωή. |
| **4** | Ανεξάρτητα, σύμφωνα με τις δικές μου ανάγκες, και επιλύοντας καλά καθορισμένα και μη συνήθη προβλήματα, μπορώ: | • να **οργανώνω** τρόπους προστασίας των συσκευών και του ψηφιακού μου περιεχομένου.<br>• **να διακρίνουν** τους κινδύνους και τις απειλές σε ψηφιακά περιβάλλοντα.<br>• **επιλέξτε** μέτρα ασφαλείας και προστασίας.<br>• **να εξηγήσετε** τρόπους για να λαμβάνετε δεόντως υπόψη την αξιοπιστία και την ιδιωτικότητα. |
| **5** | Μπορώ να καθοδηγώ και άλλους: | • **εφαρμόζουν** διαφορετικούς τρόπους για την προστασία των συσκευών και του ψηφιακού περιεχομένου.<br>• να **διακρίνετε** ποικίλους κινδύνους και απειλές σε ψηφιακά περιβάλλοντα.<br>• **να εφαρμόζετε** μέτρα ασφαλείας και προστασίας.<br>• **χρησιμοποιούν** διαφορετικούς τρόπους για να έχουν τη δέουσα προσοχή στην αξιοπιστία και την ιδιωτικότητα. |
| **6** | Σε προχωρημένο επίπεδο, ανάλογα με τις δικές μου ανάγκες και τις ανάγκες των άλλων και σε σύνθετα πλαίσια, μπορώ: | • **να επιλέξετε** την καταλληλότερη προστασία για τις συσκευές και το ψηφιακό περιεχόμενο.<br>• **να διακρίνουν** τους κινδύνους και τις απειλές σε ψηφιακά περιβάλλοντα.<br>• **να επιλέξετε** τα καταλληλότερα μέτρα ασφαλείας και προστασίας.<br>• **να αξιολογούν** τους καταλληλότερους τρόπους για να λαμβάνουν δεόντως υπόψη την αξιοπιστία και την ιδιωτικότητα. |
| **7** | Σε πολύ εξειδικευμένο επίπεδο, μπορώ: | • **να δημιουργούν λύσεις σε σύνθετα προβλήματα** με περιορισμένο ορισμό που σχετίζονται με την προστασία συσκευών και ψηφιακού περιεχομένου, τη διαχείριση κινδύνων και απειλών, την εφαρμογή μέτρων ασφάλειας και προστασίας, καθώς και την αξιοπιστία και την προστασία της ιδιωτικής ζωής σε ψηφιακά περιβάλλοντα.<br>• **να ενσωματώνω** τις γνώσεις μου για να συμβάλλω στην επαγγελματική πρακτική και γνώση και να καθοδηγώ τους άλλους στην προστασία των συσκευών.., |

| | | |
|---|---|---|
| **8** | Στο πιο προηγμένο και εξειδικευμένο επίπεδο, μπορώ: | • **δημιουργούν λύσεις για την επίλυση σύνθετων προβλημάτων** με πολλούς αλληλεπιδρώντες παράγοντες που σχετίζονται με την προστασία συσκευών και ψηφιακού περιεχομένου, τη διαχείριση κινδύνων και απειλών, την εφαρμογή μέτρων ασφάλειας και προστασίας, καθώς και την αξιοπιστία και την προστασία της ιδιωτικής ζωής σε ψηφιακά περιβάλλοντα.<br>• να **προτείνει νέες** ιδέες και διαδικασίες στον τομέα. |

# ΕΙΣΑΓΩΓΗ:

Η ψηφιακή ασφάλεια και ο ψηφιακός αλφαβητισμός περιλαμβάνουν τις δεξιότητες και τις γνώσεις που απαιτούνται για την προστασία των συσκευών, του ψηφιακού περιεχομένου και των προσωπικών δεδομένων, ενώ παράλληλα κατανοούν τους κινδύνους και τις απειλές που υπάρχουν στα ψηφιακά περιβάλλοντα. Στον σημερινό διασυνδεδεμένο κόσμο, όπου η τεχνολογία είναι πανταχού παρούσα, η καλλιέργεια πρακτικών ψηφιακής ασφάλειας είναι απαραίτητη για την προστασία του ατόμου από πιθανές βλάβες.

Σε βασικό επίπεδο, με καθοδήγηση, τα άτομα μπορούν να εντοπίσουν απλούς τρόπους προστασίας των συσκευών και του ψηφιακού τους περιεχομένου. Αυτό περιλαμβάνει την υιοθέτηση ασφαλών πρακτικών χρήσης κωδικών πρόσβασης και την αναγνώριση της σημασίας της χρήσης διαφορετικών ισχυρών κωδικών πρόσβασης για διάφορες διαδικτυακές υπηρεσίες. Μπορούν επίσης να διακρίνουν βασικούς κινδύνους και απειλές σε ψηφιακά περιβάλλοντα, όπως η κλοπή ταυτότητας, οι απάτες και οι επιθέσεις κακόβουλου λογισμικού. Επιπλέον, μαθαίνουν να επιλέγουν απλά μέτρα ασφάλειας και προστασίας και συνειδητοποιούν τη σημασία της ιδιωτικότητας και της αξιοπιστίας.

Καθώς οι μαθητές προχωρούν στο ενδιάμεσο επίπεδο, αποκτούν αυτονομία και μπορούν να ακολουθούν ανεξάρτητα απλά μέτρα ασφαλείας και προστασίας. Κατανοούν τη σημασία της ενημέρωσης των συσκευών και των εφαρμογών τους για τον μετριασμό των τρωτών σημείων ασφαλείας. Επιπλέον, μαθαίνουν για τον έλεγχο ταυτότητας δύο παραγόντων και πώς αυτός ενισχύει την ψηφιακή τους προστασία.

Προχωρώντας στο ενδιάμεσο επίπεδο, τα άτομα μπορούν να υποδείξουν σαφώς καθορισμένους και συνήθεις τρόπους για την προστασία των συσκευών και του ψηφιακού τους περιεχομένου. Μπορούν να διακρίνουν καλά καθορισμένους και συνήθεις κινδύνους και απειλές σε ψηφιακά περιβάλλοντα. Επιλέγουν και εφαρμόζουν καλά καθορισμένα και συνήθη μέτρα ασφάλειας και προστασίας. Κατανοούν τη σημασία της κρυπτογράφησης ευαίσθητων δεδομένων και μπορούν να αντιδρούν κατάλληλα σε παραβιάσεις της ασφάλειας.

Στο προχωρημένο επίπεδο, οι εκπαιδευόμενοι επιδεικνύουν μια ολοκληρωμένη κατανόηση των μέτρων ψηφιακής ασφάλειας και προστασίας. Μπορούν να εφαρμόζουν διάφορες μεθόδους για την αποτελεσματική προστασία των συσκευών τους και του ψηφιακού τους περιεχομένου. Διαφοροποιούν ένα ευρύ φάσμα κινδύνων και απειλών σε ψηφιακά περιβάλλοντα και εφαρμόζουν ανάλογα τα κατάλληλα μέτρα ασφάλειας και προστασίας. Επιπλέον, διαθέτουν τις γνώσεις για να καθοδηγήσουν άλλους στην υιοθέτηση προστατευτικών πρακτικών.

Σε επίπεδο υψηλής εξειδίκευσης, τα άτομα μπορούν να δημιουργήσουν καινοτόμες λύσεις σε σύνθετα προβλήματα που σχετίζονται με την προστασία συσκευών, τη διαχείριση κινδύνων και απειλών και την εφαρμογή μέτρων ασφάλειας και προστασίας σε ψηφιακά περιβάλλοντα. Η εξειδίκευσή τους τους επιτρέπει να συμβάλλουν στην επαγγελματική πρακτική και γνώση, αποτελώντας πολύτιμους πόρους για την καθοδήγηση άλλων στην προστασία των συσκευών και του ψηφιακού τους περιεχομένου.

Τέλος, στο πιο προχωρημένο και εξειδικευμένο επίπεδο, οι εκπαιδευόμενοι μπορούν να επινοήσουν εξελιγμένες λύσεις σε πολύπλευρα προβλήματα ψηφιακής ασφάλειας και προστασίας. Μπορούν να προτείνουν νέες ιδέες και διαδικασίες για την ενίσχυση του τομέα, προωθώντας πρακτικές προστασίας αιχμής.

Σε διάφορες περιπτώσεις χρήσης, τα άτομα εφαρμόζουν τις γνώσεις τους σε θέματα ψηφιακής ασφάλειας και προστασίας σε πραγματικά σενάρια. Για παράδειγμα, σε ένα εργασιακό περιβάλλον, μπορούν να διασφαλίσουν εταιρικούς λογαριασμούς κοινωνικών μέσων, να εντοπίσουν και να αντιμετωπίσουν κινδύνους και να εκπαιδεύσουν τους συναδέλφους τους σχετικά με τις βέλτιστες πρακτικές. Σε εκπαιδευτικά περιβάλλοντα, μπορούν να διασφαλίσουν ψηφιακές πλατφόρμες μάθησης, να εντοπίσουν πιθανές απειλές και να βοηθήσουν τους συνομηλίκους τους να πλοηγηθούν με ασφάλεια σε αυτές τις πλατφόρμες.

# ΠΡΟΫΠΟΘΕΣΕΙΣ

| |
|---|
| 1. Βασικές γνώσεις σχετικά με το διαδίκτυο, συμπεριλαμβανομένων των λειτουργιών του και του τρόπου με τον οποίο διευκολύνει την ανταλλαγή δεδομένων μεταξύ υπολογιστών. |
| 2. Κατανόηση της σημασίας των ισχυρών κωδικών πρόσβασης, καθώς και γνώση του τρόπου ασφαλούς διαχείρισης και προστασίας τους. |
| 3. Γνώση ασφαλών διαδικτυακών πρακτικών, όπως η αποφυγή δημόσιου Wi-Fi για ευαίσθητες δραστηριότητες και η προσοχή κατά την ανταλλαγή προσωπικών πληροφοριών στο διαδίκτυο. |
| 4. Ενημέρωση για τον έλεγχο ταυτότητας δύο παραγόντων και τον τρόπο ενεργοποίησής του για πρόσθετη ασφάλεια στους διαδικτυακούς λογαριασμούς. |
| 5. Βασικές γνώσεις οργάνωσης και ασφαλούς διαχείρισης ψηφιακού περιεχομένου και αρχείων. |

# 4.1

| ΤΟΜΈΑΣ ΙΚΑΝΟΤΉΤΩΝ: ΑΣΦΆΛΕΙΑ (4)<br>ΙΚΑΝΟΤΗΤΑ: (4.1) | | | |
|---|---|---|---|
| Μαθησιακά αποτελέσματα | Επίπεδο | K - S - A | Επεξήγηση |
| 1. Αναγνωρίστε τη σημασία της χρήσης μοναδικών κωδικών πρόσβασης για διαφορετικούς διαδικτυακούς λογαριασμούς για την ενίσχυση της ασφάλειας. | L1 | K | Κατανοήστε ότι η χρήση διαφορετικών ισχυρών κωδικών πρόσβασης για κάθε λογαριασμό μπορεί να μειώσει τον κίνδυνο παραβίασης πολλαπλών λογαριασμών σε περίπτωση έκθεσης ενός κωδικού πρόσβασης. Κατανοήστε ότι η χρήση μοναδικών, ισχυρών κωδικών πρόσβασης για κάθε λογαριασμό συμβάλλει στη μείωση της πιθανότητας να εκτεθούν πολλοί λογαριασμοί, εάν ένας κωδικός πρόσβασης δημοσιοποιηθεί. |
| 2. Προωθήστε μια στάση επαγρύπνησης και συνειδητοποίησης του περιβάλλοντός σας. | L1 | A | Ενθαρρύνοντας τα άτομα να έχουν επίγνωση του περιβάλλοντός τους, θα αναπτύξουν μια στάση επαγρύπνησης και προσοχής σε πιθανούς κινδύνους ή απειλές στο περιβάλλον τους. Αυτή η αυξημένη ευαισθητοποίηση μπορεί να συμβάλει στην προσωπική ασφάλεια και προστασία, επιτρέποντας στα άτομα να ανταποκρίνονται κατάλληλα σε τυχόν απροσδόκητες καταστάσεις ή κινδύνους που μπορεί να συναντήσουν. |
| 3. Προσδιορίστε τα κοινά σημάδια των προσπαθειών ηλεκτρονικού "ψαρέματος" και μάθετε πώς να αποφεύγετε να πέσετε θύμα τέτοιων απατών. | L1 | K - S | Αναγνωρίστε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα ή ιστότοπους που μπορεί να προσπαθήσουν να σας εξαπατήσουν ώστε να αποκαλύψετε προσωπικές πληροφορίες ή διαπιστευτήρια σύνδεσης. |
| 4. Αναγνωρίστε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα ή ιστότοπους που μπορεί να προσπαθήσουν να σας εξαπατήσουν ώστε να αποκαλύψετε προσωπικές πληροφορίες ή διαπιστευτήρια σύνδεσης. | L1 | K | Αναφέρετε τα πλεονεκτήματα της εγκατάστασης αξιόπιστου λογισμικού προστασίας από ιούς για τον εντοπισμό και την αφαίρεση επιβλαβών προγραμμάτων από τις συσκευές σας. |

| | | | |
|---|---|---|---|
| 5. Εφαρμόστε τη δεξιότητα να ασφαλίζετε τη συσκευή σας όταν δεν την προσέχετε. | L1 | S | Μαθαίνοντας να εφαρμόζουν τη δεξιότητα να ασφαλίζουν τις συσκευές τους όταν δεν τις επιτηρούν, τα άτομα μπορούν να λαμβάνουν προληπτικά μέτρα για την αποτροπή μη εξουσιοδοτημένης πρόσβασης ή κακής χρήσης. Αυτό μπορεί να περιλαμβάνει το κλείδωμα της συσκευής με κωδικό πρόσβασης, PIN ή βιομετρικό έλεγχο ταυτότητας, την ενεργοποίηση του αυτόματου κλειδώματος της οθόνης όταν βρίσκεται σε αδράνεια και την προσοχή στην αφή των συσκευών σε δημόσιους χώρους. Η εφαρμογή αυτών των μέτρων συμβάλλει στην προστασία των ευαίσθητων δεδομένων και διασφαλίζει ότι η συσκευή παραμένει ασφαλής από πιθανές απειλές ασφαλείας όταν βρίσκεται χωρίς επιτήρηση. |
| 6. Περιγράψτε τη σημασία της διασφάλισης του οικιακού σας δικτύου με ισχυρούς κωδικούς πρόσβασης και πρωτόκολλα κρυπτογράφησης. | L1 | K | Εξηγήστε πώς ο καθορισμός ενός ισχυρού κωδικού πρόσβασης Wi-Fi και η ενεργοποίηση πρωτοκόλλων κρυπτογράφησης συμβάλλουν στην αποτροπή μη εξουσιοδοτημένης πρόσβασης στο δίκτυό σας. |

| | | | |
|---|---|---|---|
| 7. Προσδιορίστε τους κινδύνους που συνδέονται με τη χρήση δημόσιων δικτύων Wi-Fi | L1 | K - S | Αναγνωρίστε ότι τα δημόσια δίκτυα Wi-Fi μπορεί να είναι ανασφαλή, ενώ η εισαγωγή κωδικών πρόσβασης σε δημόσια Wi-Fi αποθαρρύνεται έντονα. |
| 8. Περιγράψτε πώς η αναθεώρηση και η προσαρμογή των ρυθμίσεων απορρήτου μπορεί να βοηθήσει στον έλεγχο των πληροφοριών που μοιράζονται σε συσκευές και διαδικτυακούς λογαριασμούς. | L1 | K | Εξηγήστε τη σημασία του τακτικού ελέγχου και της ενημέρωσης των ρυθμίσεων απορρήτου για τη διαχείριση των προσωπικών πληροφοριών που μοιράζονται με εφαρμογές και υπηρεσίες. |
| 9. Απαριθμήστε τις πιθανές απειλές που δημιουργούν οι ψηφιακοί κίνδυνοι και τη σημασία της ενημέρωσης σχετικά με τις βέλτιστες λύσεις για την ασφάλεια στον κυβερνοχώρο. | L1 | K | Καταγράψτε τους διάφορους τύπους ψηφιακών κινδύνων, όπως το phishing, το κακόβουλο λογισμικό και η κοινωνική μηχανική, και την ανάγκη ενημέρωσης για την προστασία από αυτούς. |
| 10. Περιγράψτε τα βήματα που πρέπει να ακολουθήσετε σε περίπτωση απώλειας ή κλοπής μιας συσκευής για τη διασφάλιση των προσωπικών δεδομένων και της ιδιωτικής ζωής. | L1 | K - S - A | Όταν μια συσκευή χαθεί ή κλαπεί, η άμεση δράση προστατεύει τις ευαίσθητες πληροφορίες. Το άτομο πρέπει πρώτα να δηλώσει την κλοπή στην αστυνομία και στη συνέχεια να χρησιμοποιήσει τις λειτουργίες απομακρυσμένου κλειδώματος για να ασφαλίσει τη συσκευή. Πρέπει να αλλάξει γρήγορα τους κωδικούς πρόσβασης για τους λογαριασμούς που είναι προσβάσιμοι στη συσκευή, ενώ παράλληλα να χρησιμοποιήσει εργαλεία εντοπισμού για να επιχειρήσει να εντοπίσει τη θέση του. Η ενημέρωση των προσωπικών και επαγγελματικών επαφών συμβάλλει στην προστασία από μη εξουσιοδοτημένη επικοινωνία, ενώ η επικοινωνία με την ασφαλιστική εταιρεία μπορεί να οδηγήσει σε απαίτηση. Η ταχύτητα είναι απαραίτητη για την ελαχιστοποίηση των πιθανών ζημιών. |
| 11. Αναγνωρίστε τη σημασία της απενεργοποίησης περιττών υπηρεσιών δικτύου και προγραμμάτων παρασκηνίου στις συσκευές σας για να μειώσετε τις πιθανές επιφάνειες επιθέσεων. | L2 | K | Κατανοήστε ότι η απενεργοποίηση περιττών υπηρεσιών δικτύου και προγραμμάτων παρασκηνίου μπορεί να συμβάλει στην ελαχιστοποίηση του κινδύνου ευπαθειών ασφαλείας. |

| | | | |
|---|---|---|---|
| 12. Να προσέχετε την ασφάλεια των φυσικών συσκευών, ιδίως σε δημόσιους χώρους, για την αποφυγή κλοπής και μη εξουσιοδοτημένης πρόσβασης. | L2 | S | Αναπτύξτε τη συνήθεια να προσέχετε την ασφάλεια των κινητών σας συσκευών και να τις έχετε υπό την επίβλεψή σας σε δημόσιους χώρους για να αποτρέψετε την κλοπή. |

| | | | |
|---|---|---|---|
| 13. Εφαρμόζουν ασφαλείς πρακτικές κοινής χρήσης οθόνης κατά τη διάρκεια εικονικών συναντήσεων ή απομακρυσμένων συνεργασιών για την προστασία ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση ή έκθεση | L2 | S | Για να αποτρέψετε την πρόσβαση σε ευαίσθητες πληροφορίες ή την έκθεσή τους από μη εξουσιοδοτημένα μέρη κατά τη διάρκεια εικονικών συναντήσεων ή απομακρυσμένων συνεργασιών, είναι ζωτικής σημασίας να ακολουθείτε ασφαλείς διαδικασίες κοινής χρήσης οθόνης. Μπορείτε να διασφαλίσετε ότι μόνο το προοριζόμενο κοινό μπορεί να δει το περιεχόμενο που μοιράζεται και να αποφύγετε τυχόν παραβιάσεις της ιδιωτικής ζωής ή των δεδομένων, εφαρμόζοντας ασφαλείς διαδικασίες κοινής χρήσης οθόνης. Αυτό μπορεί να συνεπάγεται τη χρήση ασφαλών πλατφορμών συσκέψεων με ενσωματωμένους περιορισμούς κοινής χρήσης οθόνης, την επιλογή του περιεχομένου που θα παρουσιάσετε με προσοχή και την παρακολούθηση του ποιος έχει πρόσβαση στην κοινή χρήση της οθόνης. Μπορείτε να διατηρήσετε τα ευαίσθητα δεδομένα σας εμπιστευτικά, να διατηρήσετε την ακεραιότητά τους και να αποτρέψετε το ενδεχόμενο να περιέλθουν σε λάθος χέρια, ακολουθώντας αυτές τις διασφαλίσεις. |
| 14. Γνωρίζετε τη σημασία της τακτικής αναθεώρησης και αφαίρεσης των προσωπικών σας πληροφοριών που είναι αποθηκευμένες στις βάσεις δεδομένων των μέσων κοινωνικής δικτύωσης για την προστασία της ιδιωτικής ζωής του ψηφιακού σας περιεχομένου | L2 | K | Να γνωρίζετε την ανάγκη να ελέγχετε και να διαχειρίζεστε τακτικά τις προσωπικές πληροφορίες που είναι αποθηκευμένες σε λογαριασμούς μέσων κοινωνικής δικτύωσης για τη διατήρηση της ιδιωτικής ζωής. |
| 15. Εφαρμογή γονικού ελέγχου και λογισμικού φιλτραρίσματος για την προστασία των παιδιών από ακατάλληλο περιεχόμενο και διαδικτυακούς κινδύνους | L2 | S | Ρυθμίστε λογισμικό γονικού ελέγχου και φιλτραρίσματος όταν χρειάζεται για να δημιουργήσετε ένα ασφαλέστερο διαδικτυακό περιβάλλον για τα παιδιά. |
| 16. Κατανοήστε τους κινδύνους που σχετίζονται με τη λήψη προγραμμάτων ή εφαρμογών από ανεπίσημες ή τρίτες πηγές | L2 | K | Να γνωρίζετε ότι η λήψη από ανεπίσημες πηγές μπορεί να εκθέσει τη συσκευή σας σε κακόβουλο λογισμικό και κινδύνους για την ασφάλεια. |

| | | | |
|---|---|---|---|
| 17. Αποφύγετε τη χρήση jailbroken ή rooted συσκευών, καθώς αυτές οι μέθοδοι μπορούν να παρακάμψουν τα μέτρα ασφαλείας και να θέσουν σε κίνδυνο την ασφάλεια των δεδομένων σας. | L2 | S | Επιλέξτε να μην χρησιμοποιείτε συσκευές με root ή jailbroken για να διατηρήσετε την ακεραιότητα των λειτουργιών ασφαλείας της συσκευής. |

| | | | |
|---|---|---|---|
| 18. Γνωρίζετε τη σημασία της ασφαλούς διαγραφής και απόρριψης παλαιών συσκευών για να αποτρέψετε την ανάκτηση των δεδομένων σας από άλλους | L2 | K | Κατανοήστε την ανάγκη ορθής διαγραφής δεδομένων από παλιές συσκευές για να διασφαλίσετε το απόρρητο των δεδομένων. |
| 19. Χρησιμοποιήστε κρυπτογράφηση για την προστασία των ευαίσθητων δεδομένων στις συσκευές σας, ειδικά για τα δεδομένα που είναι αποθηκευμένα σε κινητές συσκευές και αφαιρούμενη μονάδα μαζικής αποθήκευσης. | L2 | S | Εφαρμόστε προγράμματα κρυπτογράφησης για τη διασφάλιση ευαίσθητων δεδομένων, δίνοντας ιδιαίτερη προσοχή στις φορητές συσκευές και την εξωτερική αποθήκευση. |
| 20. Κατανοήστε τους κινδύνους που συνδέονται με τη διαβίβαση ή την αποθήκευση προσωπικών πληροφοριών σε συσκευές και το ενδεχόμενο παραβίασης δεδομένων | L2 | K | Λάβετε υπόψη σας ότι η αποθήκευση ευαίσθητων πληροφοριών, όπως στοιχεία πιστωτικών καρτών ή αριθμοί EU Heatlth Insurance, σε συσκευές μπορεί να σας εκθέσει σε κλοπή ταυτότητας, εάν η συσκευή παραβιαστεί. |
| 21. Χειριστείτε με προσοχή ύποπτους συνδέσμους και αποφύγετε τη λήψη αρχείων από άγνωστες πηγές για να προστατεύσετε τις συσκευές σας από πιθανές απειλές κακόβουλου λογισμικού. | L3 | S - A | Κατανοήστε τους κινδύνους που σχετίζονται με το κλικ σε ύποπτους συνδέσμους και τη λήψη αρχείων από μη αξιόπιστες πηγές |

| | | | |
|---|---|---|---|
| 22. Αναφέρετε τη σημασία της τακτικής δημιουργίας αντιγράφων ασφαλείας δεδομένων για την προστασία από απώλεια δεδομένων και βλάβες συσκευών. | L3 | K | Κατανοήστε ότι η τακτική δημιουργία αντιγράφων ασφαλείας των αρχείων διασφαλίζει ότι τα σημαντικά δεδομένα είναι ασφαλή και ανακτήσιμα σε περίπτωση απροσδόκητων γεγονότων. |

| | | | |
|---|---|---|---|
| 23. Γνωρίζετε ότι οι χαμένες ή κλεμμένες συσκευές μπορούν να εντοπιστούν, να κλειδωθούν ή να διαγραφούν χρησιμοποιώντας δωρεάν εργαλεία που βασίζονται στο διαδίκτυο και είναι διαθέσιμα στις περισσότερες συσκευές. | L3 | K | Να γνωρίζετε ότι οι συσκευές διαθέτουν ενσωματωμένα εργαλεία που μπορούν να σας βοηθήσουν να εντοπίσετε και να ασφαλίσετε ή να διαγράψετε δεδομένα εξ αποστάσεως σε περίπτωση απώλειας ή κλοπής. |
| 24. Χρησιμοποιήστε επιδέξια τις λειτουργίες εντοπισμού, κλειδώματος και διαγραφής για την προστασία των δεδομένων και της ιδιωτικής σας ζωής σε περίπτωση απώλειας ή κλοπής της συσκευής σας. | L3 | S | Αξιοποιήστε αποτελεσματικά τις λειτουργίες εντοπισμού, κλειδώματος και διαγραφής συσκευών για να διασφαλίσετε ευαίσθητες πληροφορίες σε περίπτωση απώλειας της συσκευής. |
| 25. Κατανοήστε τη σημασία της αποσύνδεσης στο τέλος των συνεδριών σας στο διαδίκτυο ή στις εφαρμογές για την προστασία των προσωπικών σας πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. | L3 | K | Να ξέρετε ότι η αποσύνδεση μετά τη χρήση ηλεκτρονικών υπηρεσιών διασφαλίζει ότι οι λογαριασμοί σας παραμένουν ασφαλείς και τα δεδομένα σας προστατεύονται. |
| 26. Κατανοήστε πώς να διαχειρίζεστε τα δικαιώματα των εφαρμογών για να προστατεύετε το απόρρητό σας και να γνωρίζετε τα δεδομένα που συλλέγονται από τις εφαρμογές στις συσκευές σας. | L3 | S | Χρησιμοποιήστε τα δικαιώματα της εφαρμογής με σύνεση και διαβάστε προσεκτικά τους όρους και τις προϋποθέσεις πριν τα αποδεχτείτε. |

| | | | |
|---|---|---|---|
| 27. Εφαρμόστε ασφαλείς συνήθειες περιήγησης, όπως η αποφυγή ύποπτων ιστότοπων και η χρήση συνδέσεων HTTPS, για να μειώσετε τον κίνδυνο κακόβουλου λογισμικού και κλοπής δεδομένων. | L3 | S | Εφαρμόστε πρακτικές ασφαλούς περιήγησης για την προστασία των συσκευών και των δεδομένων από πιθανές απειλές στον κυβερνοχώρο κατά την πρόσβαση στο διαδίκτυο. |

| | | | |
|---|---|---|---|
| 28. Αναγνωρίστε τη σημασία της φύλαξης των συσκευών με φυσική ασφάλεια, ιδίως σε δημόσιους χώρους, για την αποφυγή κλοπής και μη εξουσιοδοτημένης πρόσβασης. | L3 | K | Αναγνωρίστε την ανάγκη να είστε σε εγρήγορση σχετικά με την ασφάλεια των συσκευών και να διατηρείτε τις συσκευές σε οπτική επαφή για να αποφύγετε πιθανή κλοπή ή αλλοίωση. |
| 29. Προσδιορίστε τους κινδύνους που συνδέονται με τη χρήση δημόσιων σταθμών φόρτισης και το ενδεχόμενο κλοπής δεδομένων ή εγκατάστασης κακόβουλου λογισμικού. | L3 | K - S | Να γνωρίζετε τους πιθανούς κινδύνους ασφαλείας όταν χρησιμοποιείτε δημόσιους σταθμούς φόρτισης και να λαμβάνετε προφυλάξεις για την προστασία των συσκευών από τους κινδύνους αυτούς. |
| 30. Να είναι σε θέση να εφαρμόσει έναν διαχειριστή κωδικών πρόσβασης για την ασφαλή αποθήκευση και δημιουργία σύνθετων κωδικών πρόσβασης για διάφορους διαδικτυακούς λογαριασμούς, μειώνοντας τον κίνδυνο παραβίασης της ασφάλειας που σχετίζεται με τον κωδικό πρόσβασης. | L3 | S | Χρησιμοποιήστε ένα εργαλείο διαχείρισης κωδικών πρόσβασης για να δημιουργείτε και να διαχειρίζεστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης για κάθε διαδικτυακό λογαριασμό, ενισχύοντας τη συνολική ασφάλεια. |
| 31. Εφαρμόστε χαρακτηριστικά ασφαλείας για συγκεκριμένες συσκευές, όπως βιομετρική πιστοποίηση ταυτότητας ή κρυπτογράφηση συσκευής, για να ενισχύσετε την προστασία των ευαίσθητων δεδομένων. | L4 | S | Ρυθμίστε βιομετρικό έλεγχο ταυτότητας ή κρυπτογράφηση συσκευής για να ενισχύσετε την ασφάλεια της συσκευής και να διασφαλίσετε τις προσωπικές πληροφορίες. |

| | | | |
|---|---|---|---|
| 32. Κατανοήστε τους κινδύνους από τη χρήση ξεπερασμένου ή μη υποστηριζόμενου λογισμικού στις συσκευές σας και τη σημασία της ενημέρωσης ή αντικατάστασης του λογισμικού αυτού για τη διατήρηση της ασφάλειας. | L4 | K | Να γνωρίζετε τους κινδύνους ασφαλείας που εγκυμονεί η χρήση ξεπερασμένου λογισμικού και την ανάγκη ενημέρωσης ή αντικατάστασής του με υποστηριζόμενες εκδόσεις. |

| | | | |
|---|---|---|---|
| 33. Εντοπίστε ύποπτες δραστηριότητες στις συσκευές σας, όπως απροσδόκητα αναδυόμενα παράθυρα ή ασυνήθιστη αποστράγγιση της μπαταρίας, οι οποίες μπορεί να υποδεικνύουν πιθανό κακόβουλο λογισμικό ή παραβιάσεις της ασφάλειας. | L4 | K - S | Αναγνωρίστε τα σημάδια παραβίασης της συσκευής και λάβετε τις απαραίτητες ενέργειες για την αντιμετώπιση πιθανών απειλών ασφαλείας. |
| 34. Αξιολογήστε τα χαρακτηριστικά ασφαλείας των διαφόρων συσκευών και επιλέξτε τις πιο ασφαλείς επιλογές με βάση τις συγκεκριμένες ανάγκες και περιπτώσεις χρήσης σας. | L4 | A | Όταν εξετάζετε το ενδεχόμενο αγοράς, ερευνήστε διεξοδικά τα εγγενή χαρακτηριστικά ασφαλείας της συσκευής. Αξιολογήστε τα πρότυπα κρυπτογράφησης, τους μηχανισμούς ελέγχου ταυτότητας και τη συχνότητα των ενημερώσεων ασφαλείας. Αναφερθείτε στις μοναδικές απαιτήσεις σας: χρειάζεστε προηγμένη βιομετρική επαλήθευση ή έλεγχο ταυτότητας πολλαπλών παραγόντων;<br>Επίσης, λάβετε υπόψη σας τα σχόλια από ειδικούς της τεχνολογίας και καθημερινούς χρήστες. Η εξισορρόπηση της ασφάλειας με τις συγκεκριμένες ανάγκες σας εξασφαλίζει τη βέλτιστη προστασία και λειτουργικότητα. Η ασφάλεια των δεδομένων σας εξαρτάται από τεκμηριωμένες επιλογές. |
| 35. Αναγνωρίστε τη σημασία της τακτικής επανεξέτασης και διαχείρισης των δικαιωμάτων των εφαρμογών για τον περιορισμό της πρόσβασης σε προσωπικά δεδομένα και τη διασφάλιση της ιδιωτικής ζωής. | L4 | K | Η τακτική επανεξέταση και διαχείριση αυτών των δικαιωμάτων εφαρμογών είναι ζωτικής σημασίας. Με προληπτική δράση, μπορείτε να αποτρέψετε τη μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, διαφυλάσσοντας το απόρρητό σας. Οι περιοδικοί έλεγχοι διασφαλίζουν ότι χορηγούνται μόνο τα απαραίτητα δικαιώματα, ελαχιστοποιώντας τους κινδύνους. Για παράδειγμα, χρειάζεται μια εφαρμογή σημειώσεων την τοποθεσία σας; Κατά πάσα πιθανότητα όχι. Περιορίζοντας την περιττή πρόσβαση, όχι μόνο προστατεύετε τις ευαίσθητες πληροφορίες, αλλά ενισχύετε και την άμυνα της συσκευής σας έναντι πιθανών παραβιάσεων. Διασφαλίστε το απόρρητό σας με εγρήγορση. |
| 36. Επεκτείνετε τα μέτρα ασφαλείας των συσκευών σας ώστε να συμπεριλάβετε απομακρυσμένα περιβάλλοντα εργασίας, εξασφαλίζοντας προστασία δεδομένων και ασφαλή κανάλια επικοινωνίας. | L4 | K-S | Η εργασία εκτός του παραδοσιακού περιβάλλοντος γραφείου μπορεί να εκθέσει τα ευαίσθητα δεδομένα σε νέες απειλές. Για να προσαρμοστείτε, εξασφαλίστε κρυπτογραφημένες συνδέσεις, ειδικά σε δημόσια Wi-Fi. Να ενημερώνετε τακτικά και να δημιουργείτε αντίγραφα ασφαλείας των δεδομένων. Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης και ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων, όταν είναι δυνατόν. Περιορίστε την πρόσβαση στις συσκευές στο απαραίτητο προσωπικό και εγκαταστήστε αξιόπιστο λογισμικό ασφαλείας. Σε απομακρυσμένες ρυθμίσεις, η προληπτική ασφάλεια των συσκευών είναι ζωτικής σημασίας για τη διαφύλαξη ζωτικών πληροφοριών. |

| | | | |
|---|---|---|---|
| 37. Διευκολύνετε την ευαισθητοποίηση των συναδέλφων ή των μελών της οικογένειάς σας σε θέματα ασφάλειας, εκπαιδεύοντάς τους στις βέλτιστες πρακτικές για την ασφάλεια των συσκευών και την ασφαλή διαδικτυακή συμπεριφορά. | L4 | A | Προωθήστε την ευαισθητοποίηση σε θέματα ασφάλειας συσκευών και ενθαρρύνετε την υπεύθυνη διαδικτυακή συμπεριφορά μεταξύ συνομηλίκων ή μελών της οικογένειας. |

| | | | |
|---|---|---|---|
| 38. Αναγνωρίστε τους πιθανούς κινδύνους που σχετίζονται με το άνοιγμα αρχείων zip ή rar από μη αξιόπιστες ή άγνωστες πηγές. | L4 | K | Αποφεύγετε να ανοίγετε συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου ή να κατεβάζετε αρχεία από ιστότοπους εάν δεν εμπιστεύεστε τον αποστολέα ή την πηγή. Έτσι αποφεύγεται ο κίνδυνος λήψης κακόβουλων αρχείων zip ή rar που μπορεί να περιέχουν επιβλαβές λογισμικό ή ιούς. |
| 39. Αναπτύξτε τη συνήθεια να διασφαλίζετε την ασφάλεια των φορητών μέσων υλικού και των συσκευών αφαίρεσης, αποφεύγοντας την εμπιστοσύνη σε μη ασφαλείς συσκευές ή περιεχόμενα μέσων. | L4 | A | Πριν χρησιμοποιήσετε μια μονάδα USB flash ή έναν εξωτερικό σκληρό δίσκο, επιθεωρήστε την οπτικά για τυχόν φυσικές ζημιές ή ύποπτα σημάδια. Επίσης, εξετάστε το ενδεχόμενο σάρωσης του περιεχομένου του μέσου με αξιόπιστο λογισμικό προστασίας από ιούς για να αποτρέψετε την εξάπλωση πιθανών απειλών ασφαλείας στις συσκευές σας. |
| 40. Εξηγήστε τους κινδύνους της λήψης εφαρμογών από άγνωστες πηγές και τη σημασία της χρήσης επίσημων καταστημάτων εφαρμογών. | L4 | K | Η λήψη εφαρμογών από άγνωστες πηγές μπορεί να εκθέσει τη συσκευή σας σε επιβλαβές κακόβουλο λογισμικό. |
| 41. 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. | L5 | S | Ερευνήστε και συγκρίνετε διάφορα προγράμματα προστασίας από ιούς με βάση τα χαρακτηριστικά τους, τις κριτικές και την αποτελεσματικότητά τους για να επιλέξετε το καταλληλότερο για τον υπολογιστή σας. |

| | | | |
|---|---|---|---|
| 42. Υποστηρίξτε την αποφυγή της χρήσης ευαίσθητων ή εύκολα ανιχνεύσιμων πληροφοριών στους κωδικούς πρόσβασης για να ενισχύσετε την ισχύ και την ασφάλειά τους. | L5 | A | Ενθαρρύνετε τους φίλους και τους συναδέλφους να δημιουργούν ισχυρούς κωδικούς πρόσβασης που δεν περιλαμβάνουν εύκολα μαντεύσιμες πληροφορίες όπως γενέθλια, ονόματα ή κοινές φράσεις. |

| | | | |
|---|---|---|---|
| 43. Κατανοήστε τη σημασία της αποφυγής λέξεων λεξικού ή κοινών μοτίβων στους κωδικούς πρόσβασης για την αποτροπή επιθέσεων brute-force. | L5 | K | Να γνωρίζετε ότι η χρήση απλών λέξεων λεξικού ή προβλέψιμων μοτίβων στους κωδικούς πρόσβασης μπορεί να τους καταστήσει ευάλωτους σε αυτοματοποιημένα εργαλεία παραβίασης κωδικών πρόσβασης. |
| 44. Αναγνωρίστε τον κίνδυνο από τη χρήση του ίδιου κωδικού πρόσβασης σε πολλούς λογαριασμούς και τη σημασία της χρήσης μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό. | L5 | K | Δημιουργήστε ισχυρούς κωδικούς πρόσβασης με συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών και ειδικών χαρακτήρων για κάθε λογαριασμό σας. |
| 45. Αναγνωρίστε τη σημασία της περιοδικής ενημέρωσης των κωδικών πρόσβασης και της αποφυγής της επαναχρησιμοποίησης παλαιών κωδικών πρόσβασης. | L5 | K | Να γνωρίζετε ότι η τακτική αλλαγή των κωδικών πρόσβασης συμβάλλει στον περιορισμό των κινδύνων που σχετίζονται με πιθανές παραβιάσεις δεδομένων ή παραβιασμένους λογαριασμούς. |
| 46. Χρησιμοποιήστε επιδέξια ένα πρόγραμμα συμπίεσης στη συσκευή σας για να μειώσετε τον όγκο των δεδομένων, εξασφαλίζοντας αποτελεσματική αποθήκευση και μετάδοση. | L5 | S | Εφαρμόστε έναν αλγόριθμο συμπίεσης για να μειώσετε το μέγεθος των δεδομένων, διευκολύνοντας την αποθήκευση και την κοινή χρήση πληροφοριών. |

| | | | |
|---|---|---|---|
| 47. Η δυνατότητα διαμόρφωσης των ρυθμίσεων της συσκευής για αυτόματο κλείδωμα ή αποσύνδεση μετά από μια περίοδο αδράνειας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης. | L5 | S | Ρυθμίστε το smartphone ή το φορητό σας υπολογιστή να κλειδώνει αυτόματα μετά από σύντομο χρονικό διάστημα αδράνειας, για να προστατεύσετε τα δεδομένα σας από τα αδιάκριτα βλέμματα. |

| | | | |
|---|---|---|---|
| 48. Γνωρίστε τους κινδύνους από τη χρήση των λειτουργιών αυτόματης σύνδεσης σε ιστότοπους ή εφαρμογές που αποθηκεύουν προσωπικές πληροφορίες. | L5 | K | Κατανοήστε ότι η ενεργοποίηση των λειτουργιών αυτόματης σύνδεσης μπορεί να εξοικονομήσει χρόνο, αλλά μπορεί να αποτελέσει κίνδυνο για την ασφάλεια εάν κάποιος αποκτήσει φυσική πρόσβαση στη συσκευή. |
| 49. Υποστηρίξτε τη χρήση ασφαλών μεθόδων μεταφοράς αρχείων, όπως το SFTP ή η ασφαλής αποθήκευση στο cloud, για την ανταλλαγή ευαίσθητων αρχείων μεταξύ συσκευών. | L5 | A | Ενθαρρύνετε τους συναδέλφους ή τους φίλους σας να χρησιμοποιούν ασφαλείς μεθόδους μεταφοράς αρχείων για να μοιράζονται εμπιστευτικά έγγραφα χωρίς να διακυβεύεται η ασφάλειά τους. |
| 50. Αναγνωρίστε τους πιθανούς κινδύνους από τη χρήση άγνωστου λογισμικού ή εφαρμογών στις συσκευές σας. | L5 | S | Όταν συναντάτε ένα νέο λογισμικό ή μια νέα εφαρμογή με την οποία δεν είστε εξοικειωμένοι, είναι σημαντικό να είστε προσεκτικοί και να εξετάζετε τις πιθανές συνέπειες πριν την εγκαταστήσετε στη συσκευή σας.<br><br>Η χρήση άγνωστου λογισμικού μπορεί να εγκυμονεί διάφορους κινδύνους για την ασφάλεια και τη λειτουργικότητα της συσκευής σας. Ορισμένοι από αυτούς τους κινδύνους περιλαμβάνουν κακόβουλα προγράμματα, ανεπιθύμητες τροποποιήσεις, προβλήματα προστασίας της ιδιωτικής ζωής κ.λπ. |
| 51. Αναγνωρίστε τη σημασία της απενεργοποίησης του Bluetooth στις συσκευές σας όταν δεν το χρησιμοποιείτε. | L6 | K | Κατανοήστε ότι η απενεργοποίηση του Bluetooth όταν δεν είναι απαραίτητο συμβάλλει στη μείωση των πιθανών κινδύνων ασφαλείας και στην εξοικονόμηση μπαταρίας στη συσκευή σας. |
| 52. Δυνατότητα εκτέλεσης σαρώσεων από ιούς σε εξωτερικές συσκευές αποθήκευσης | L6 | K-S | Αποκτήστε τις γνώσεις και τις δεξιότητες για τη διενέργεια σαρώσεων από ιούς σε εξωτερικές συσκευές αποθήκευσης, όπως μονάδες USB ή εξωτερικοί σκληροί δίσκοι. Με τον τρόπο αυτό, μπορείτε να εντοπίσετε και να εξαλείψετε πιθανούς ιούς ή κακόβουλο λογισμικό που μπορεί να υπάρχουν στα μέσα αποθήκευσης, προστατεύοντας τις συσκευές σας από πιθανές μολύνσεις και καταστροφή δεδομένων. |

| | | | |
|---|---|---|---|
| 53. Κατανόηση της σημασίας της εκπαίδευσης των εργαζομένων σε τεχνικές ασφάλειας ΤΠ | L6 | K-A | Διαθέτει τη γνώση και την ικανότητα να διεξάγει εκπαίδευση σε θέματα ασφάλειας ΤΠ για τους υπαλλήλους. Με τον τρόπο αυτό, μπορείτε να τους εξοπλίσετε με βασικές γνώσεις και δεξιότητες για να εντοπίζουν και να ανταποκρίνονται στις απειλές κυβερνοασφάλειας effectively. Αυτή η εκπαίδευση δίνει τη δυνατότητα στους υπαλλήλους να υιοθετήσουν βέλτιστες πρακτικές, να διασφαλίσουν ευαίσθητες πληροφορίες και να συμβάλουν σε ένα πιο ασφαλές εργασιακό περιβάλλον. |
| 54. Ανάπτυξη ολοκληρωμένων μέτρων φυσικής ασφάλειας για την προστασία των περιουσιακών στοιχείων του οργανισμού | L6 | A | Με τις γνώσεις σας σχετικά με τις αρχές της φυσικής ασφάλειας, θα σχεδιάζετε και θα εφαρμόζετε ισχυρά μέτρα ασφαλείας για την προστασία των φυσικών περιουσιακών στοιχείων του οργανισμού, συμπεριλαμβανομένων των κτιρίων, του εξοπλισμού και των ευαίσθητων πληροφοριών. Εφαρμόζοντας τις δεξιότητές σας, μπορείτε να διεξάγετε αξιολογήσεις κινδύνου, να εγκαθιστάτε συστήματα ελέγχου πρόσβασης, κάμερες παρακολούθησης και συστήματα συναγερμού, καθώς και να θεσπίζετε ασφαλείς διαδικασίες εισόδου και εξόδου. Αυτή η προληπτική προσέγγιση διασφαλίζει ότι η φυσική υποδομή του οργανισμού προστατεύεται από μη εξουσιοδοτημένη πρόσβαση, κλοπή, βανδαλισμό και άλλες φυσικές απειλές. Προάγοντας μια στάση ευαισθητοποίησης σε θέματα ασφάλειας μεταξύ των εργαζομένων και των ενδιαφερομένων, δημιουργείτε ένα ασφαλέστερο εργασιακό περιβάλλον, μετριάζοντας τους πιθανούς κινδύνους και ενισχύοντας τη συνολική στάση ασφαλείας του οργανισμού. |
| 55. 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. | L6 | A | Περιγράψτε πώς η 2FA προσθέτει ένα επιπλέον βήμα επαλήθευσης πέραν του κωδικού πρόσβασης, καθιστώντας δυσκολότερη την πρόσβαση σε λογαριασμούς από μη εξουσιοδοτημένα άτομα. |
| 56. Γνωρίζετε πώς να διαγιγνώσκετε και να επιλύετε προβλήματα ασφαλείας στις συσκευές σας, εντοπίζοντας πιθανό κακόβουλο λογισμικό ή προσπάθειες μη εξουσιοδοτημένης πρόσβασης. | L6 | S | Διερεύνηση και επίλυση περιστατικών ασφαλείας με επιδεξιότητα για την προστασία των συσκευών σας από πιθανές απειλές. |
| 57. Κατανοήστε τους πιθανούς κινδύνους της αποθήκευσης κωδικών πρόσβασης σε προγράμματα περιήγησης στο διαδίκτυο και τη σημασία της χρήσης ειδικών εργαλείων διαχείρισης κωδικών πρόσβασης. | L6 | K | Λάβετε υπόψη ότι η αποθήκευση κωδικών πρόσβασης σε προγράμματα περιήγησης ιστού μπορεί να μην είναι τόσο ασφαλής όσο η χρήση ειδικών διαχειριστών κωδικών πρόσβασης. |

| | | | |
|---|---|---|---|
| 58. 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. | L6 | A | Δημιουργήστε ένα εξατομικευμένο σχέδιο κυβερνοασφάλειας για να ενημερώνεστε για τις απειλές και να προστατεύετε τις προσωπικές συσκευές και τα δεδομένα. |
| 59. Υιοθετήστε αξιόπιστο λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό στις προσωπικές συσκευές για τον εντοπισμό και την απομάκρυνση πιθανών απειλών. | L6 | S | Διασφαλίστε την ασφάλεια των προσωπικών σας συσκευών εγκαθιστώντας και ενημερώνοντας τακτικά αξιόπιστο λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό. Αυτό το λογισμικό θα σαρώνει ενεργά τις συσκευές σας για πιθανές απειλές, όπως ιούς, κακόβουλο λογισμικό και άλλα κακόβουλα προγράμματα. Εάν εντοπιστούν απειλές, το λογισμικό θα τις απομακρύνει αμέσως, προστατεύοντας τις συσκευές και τα δεδομένα σας από βλάβες. Οι τακτικές ενημερώσεις διασφαλίζουν ότι το λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό μπορεί να ανιχνεύει και να καταπολεμά αποτελεσματικά τις πιο πρόσφατες και αναδυόμενες απειλές, παρέχοντάς σας μια ισχυρή άμυνα απέναντι σε πιθανούς κινδύνους κυβερνοασφάλειας. |
| 60. Εφαρμογή ελέγχων πρόσβασης για τη ρύθμιση και τον περιορισμό της εισόδου σε συστήματα, λογαριασμούς ή προσωπικά προφίλ, εξασφαλίζοντας καλύτερη ασφάλεια και προστασία της ιδιωτικής ζωής. | L6 | S | Χρησιμοποιώντας ελέγχους πρόσβασης, μπορείτε να διαχειριστείτε και να περιορίσετε ποιος έχει δικαίωμα πρόσβασης στα συστήματα, τους λογαριασμούς ή τα προσωπικά σας προφίλ. Αυτό συμβάλλει στην προστασία των ευαίσθητων πληροφοριών και αποτρέπει την είσοδο μη εξουσιοδοτημένων ατόμων. Χρησιμοποιώντας τεχνικές όπως κωδικούς πρόσβασης, έλεγχο ταυτότητας δύο παραγόντων και έλεγχο πρόσβασης βάσει ρόλων, μπορείτε να ενισχύσετε τη συνολική ασφάλεια των ψηφιακών σας περιουσιακών στοιχείων. Ο έλεγχος της πρόσβασης ελαχιστοποιεί επίσης τον κίνδυνο παραβίασης δεδομένων, κλοπής ταυτότητας και μη εξουσιοδοτημένης χρήσης προσωπικών πληροφοριών. Ως αποτέλεσμα, διατηρείτε υψηλότερο επίπεδο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πόρων σας, ενισχύοντας τις άμυνες κυβερνοασφάλειας. |
| 61. Κατανόηση της σημασίας της διεξαγωγής ετήσιας εκπαίδευσης ευαισθητοποίησης των μελών για την ασφάλεια στον κυβερνοχώρο. | L7 | K - S - A | Επίδειξη των γνώσεων, των δεξιοτήτων και της συμπεριφοράς για την οργάνωση και την υλοποίηση ετήσιων εκπαιδευτικών συνεδριών ευαισθητοποίησης των στελεχών με επίκεντρο την κυβερνοασφάλεια. Πραγματοποιώντας αυτές τις εκπαιδευτικές συνεδρίες, διασφαλίζετε ότι όλοι οι εργαζόμενοι είναι ενημερωμένοι σχετικά με τις τελευταίες απειλές στον κυβερνοχώρο, τις βέλτιστες πρακτικές και τις πολιτικές της εταιρείας. Αυτό συμβάλλει στην ευαισθητοποίηση των μελών του staff, ενδυναμώνοντάς τους να αναγνωρίζουν πιθανούς κινδύνους, να αποφεύγουν τις συνήθεις παγίδες και να συμβάλλουν ενεργά σε ένα ασφαλές και άγρυπνο εργασιακό περιβάλλον. Η τακτική εκπαίδευση ευαισθητοποίησης staff ενισχύει τη σημασία της ασφάλειας στον κυβερνοχώρο εντός του οργανισμού και προάγει μια κουλτούρα ευαισθητοποίησης σε θέματα ασφάλειας μεταξύ των εργαζομένων. |

| | | | |
|---|---|---|---|
| 62. Ανάλυση και κατηγοριοποίηση πιθανών κινδύνων κυβερνοασφάλειας με βάση τον αντίκτυπο και την πιθανότητα εμφάνισής τους | L7 | S | Στο πλαίσιο μιας άσκησης εκτίμησης κινδύνου, θα αποδείξετε τις γνώσεις σας (Κ) σχετικά με τις απειλές και τα τρωτά σημεία της κυβερνοασφάλειας που αντιμετωπίζουν συνήθως οι οργανισμοί. Θα είστε σε θέση να εντοπίζετε και να αναγνωρίζετε συγκεκριμένους κινδύνους, όπως επιθέσεις phishing, μολύνσεις από κακόβουλο λογισμικό και απόπειρες μη εξουσιοδοτημένης πρόσβασης. Εφαρμόζοντας τις δεξιότητές σας (Σ), θα αξιολογήσετε τις πιθανές επιπτώσεις και την πιθανότητα κάθε κινδύνου στα πληροφοριακά συστήματα και τα δεδομένα του οργανισμού. Κατηγοριοποιώντας τους κινδύνους σε υψηλά, μεσαία ή χαμηλά επίπεδα σοβαρότητας, θα ιεραρχήσετε τις προσπάθειες μετριασμού, κατανέμοντας αποτελεσματικά τους πόρους για να αντιμετωπίσετε πρώτα τους πιο κρίσιμους κινδύνους. Αυτή η προσέγγιση επιδεικνύει μια προληπτική στάση (Α) απέναντι στην ασφάλεια στον κυβερνοχώρο, διασφαλίζοντας ότι ο οργανισμός είναι καλά προετοιμασμένος για την προστασία από πιθανές απειλές και την ελαχιστοποίηση των επιπτώσεων των περιστατικών ασφαλείας. |

| | | | |
|---|---|---|---|
| 63. Τακτική επανεξέταση και επικαιροποίηση των πολιτικών και διαδικασιών που σχετίζονται με την ασφάλεια στον κυβερνοχώρο | L7 | K-S-A | Ως επαγγελματίας στον τομέα της ασφάλειας στον κυβερνοχώρο, θα επανεξετάζετε και θα επικαιροποιείτε τις πολιτικές και τις διαδικασίες ασφάλειας στον κυβερνοχώρο, ώστε να ευθυγραμμίζονται με τις τρέχουσες βέλτιστες πρακτικές και κανονισμούς. Αυτή η προληπτική προσέγγιση διασφαλίζει ότι ο οργανισμός διατηρεί μια ισχυρή θέση ασφαλείας και μπορεί να ανταποκρίνεται αποτελεσματικά στις αναδυόμενες απειλές. |
| 64. Δώστε έμφαση σε μέτρα ασφάλειας επικεντρωμένα στα δεδομένα αντί να στηρίζεστε αποκλειστικά σε περιμετρικές άμυνες. | L7 | A | Ως υπέρμαχος της κυβερνοασφάλειας, θα δώσετε προτεραιότητα στην προστασία των ίδιων των δεδομένων αντί να εστιάζετε αποκλειστικά στην εξασφάλιση της περιμέτρου του δικτύου του οργανισμού. Αυτή η προσέγγιση περιλαμβάνει την εφαρμογή κρυπτογράφησης, ελέγχων πρόσβασης και ταξινόμησης δεδομένων για τη διασφάλιση των ευαίσθητων πληροφοριών, ακόμη και αν παραβιαστεί η περίμετρος του δικτύου. Δίνοντας έμφαση στην ασφάλεια με επίκεντρο τα δεδομένα, ο οργανισμός μπορεί να διασφαλίσει ότι τα δεδομένα παραμένουν ασφαλή ανά πάσα στιγμή, είτε αποθηκεύονται, είτε μεταδίδονται, είτε αποκτούν πρόσβαση από εξουσιοδοτημένο προσωπικό. Αυτή η προληπτική στάση απέναντι στην προστασία των δεδομένων ενισχύει τη συνολική ανθεκτικότητα του οργανισμού στον κυβερνοχώρο και μειώνει τον κίνδυνο παραβίασης δεδομένων και μη εξουσιοδοτημένης πρόσβασης σε κρίσιμες πληροφορίες. |
| 65. Επίδειξη γνώσεων και δεξιοτήτων για τον εντοπισμό και την αφαίρεση περιττών δεδομένων για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. | L7 | K - S | Ως επαγγελματίας της κυβερνοασφάλειας, θα είστε ικανοί να αναγνωρίζετε τα πλεονάζοντα δεδομένα που είναι αποθηκευμένα στα συστήματα και τις βάσεις δεδομένων του οργανισμού. Εφαρμόζοντας τις γνώσεις σας, μπορείτε να αξιολογήσετε τον αντίκτυπο και τους πιθανούς κινδύνους που σχετίζονται με τα πλεονάζοντα δεδομένα, όπως το αυξημένο κόστος αποθήκευσης και η έκθεση σε παραβιάσεις δεδομένων. Αξιοποιώντας τις δεξιότητές σας, θα αναγνωρίζετε και θα εξαλείφετε αποτελεσματικά τις περιττές διπλές εγγραφές, αρχεία ή ευαίσθητες πληροφορίες. Αυτή η προληπτική προσέγγιση βελτιστοποιεί τη διαχείριση δεδομένων, μειώνει την επιφάνεια επίθεσης και ενισχύει τη συνολική ασφάλεια στον κυβερνοχώρο, ελαχιστοποιώντας τα πιθανά σημεία ευπάθειας. |
| 66. Υποστήριξη αυξημένων επενδύσεων στην κυβερνοασφάλεια και αποτελεσματική κατανομή των πόρων | L7 | S - A | Ως επαγγελματίας στον τομέα της ασφάλειας στον κυβερνοχώρο, θα υποστηρίξετε ενεργά τη διάθεση περισσότερων οικονομικών πόρων και χρόνου για την ενίσχυση των μηχανισμών ασφάλειας στον κυβερνοχώρο του οργανισμού. Αξιοποιώντας τις δεξιότητές σας, μπορείτε να αξιολογήσετε την τρέχουσα κατάσταση της κυβερνοασφάλειας και να εντοπίσετε τομείς που απαιτούν πρόσθετες επενδύσεις, όπως προηγμένα εργαλεία ασφαλείας, εκπαίδευση των εργαζομένων και ελέγχους ασφαλείας. Μέσω της effποτελεσματικής κατανομής των πόρων, μπορείτε να ενισχύσετε την ικανότητα του οργανισμού να εντοπίζει, να προλαμβάνει και να ανταποκρίνεται στις απειλές στον κυβερνοχώρο, μειώνοντας έτσι τον κίνδυνο παραβίασης της ασφάλειας και παραβίασης των δεδομένων. Αυτή η προληπτική στάση προς την κατεύθυνση της αύξησης των δαπανών για την ασφάλεια στον κυβερνοχώρο αντανακλά τη δέσμευση για τη διασφάλιση των ψηφιακών περιουσιακών στοιχείων του οργανισμού και τη διατήρηση μιας ισχυρής άμυνας έναντι πιθανών επιθέσεων στον κυβερνοχώρο. |

| | | | |
|---|---|---|---|
| 67. Να γνωρίζουν τη σημασία της προώθησης μιας νοοτροπίας ασφάλειας σε ολόκληρη την εταιρεία και της προώθησης μιας κουλτούρας ευαισθητοποίησης σε θέματα κυβερνοασφάλειας | L7 | A | Δίνοντας το παράδειγμα, θα εμπνεύσετε τους υπαλλήλους σε όλα τα επίπεδα να δίνουν προτεραιότητα στην ασφάλεια στον κυβερνοχώρο στις καθημερινές τους δραστηριότητες. Επικοινωνώντας τακτικά τη σημασία της ασφάλειας και παρέχοντας πραγματικά παραδείγματα κυβερνοαπειλών και των πιθανών επιπτώσεών τους, θα καλλιεργήσετε μια νοοτροπία ασφάλειας σε ολόκληρη την εταιρεία.<br>Ενθαρρύνοντας τους υπαλλήλους να αναφέρουν οποιεσδήποτε ανησυχίες ή περιστατικά ασφαλείας, θα δημιουργήσετε ένα περιβάλλον όπου όλοι θα διαδραματίζουν ενεργό ρόλο στη διαφύλαξη των ψηφιακών περιουσιακών στοιχείων και των ευαίσθητων δεδομένων της εταιρείας. Αυτή η προληπτική προσέγγιση θα συμβάλει σε μια ισχυρή κουλτούρα ασφάλειας, όπου οι πρακτικές ασφάλειας θα ενσωματωθούν στο DNA του οργανισμού, ενισχύοντας τη συνολική ανθεκτικότητα στην κυβερνοασφάλεια. |

| | | | |
|---|---|---|---|
| 68. Επίδειξη της ικανότητας ταξινόμησης δεδομένων ανάλογα με την προτεραιότητα και τη σημασία τους | L7 | K-S | Θα αποκτήσετε τις δεξιότητες να αξιολογείτε και να κατηγοριοποιείτε δεδομένα σε διάφορα επίπεδα προτεραιότητας, όπως κρίσιμα, ευαίσθητα και δημόσια. Αυτή η ταξινόμηση επιτρέπει στον οργανισμό να κατανέμει τους πόρους ασφαλείας με αποτελεσματικό τρόπο, διασφαλίζοντας ότι τα πιο πολύτιμα και ευαίσθητα δεδομένα λαμβάνουν ενισχυμένη προστασία. Κατανοώντας τη σημασία της ταξινόμησης δεδομένων, μπορείτε να εφαρμόσετε τα κατάλληλα μέτρα ασφαλείας για τη διαφύλαξη των κρίσιμων πληροφοριών από πιθανές απειλές στον κυβερνοχώρο. |
| 69. Αναγνωρίστε τη σημασία του ελέγχου ταυτότητας δύο ή πολλαπλών παραγόντων | L7 | K-S | Με τη γνώση των διαφόρων μεθόδων ελέγχου ταυτότητας, θα ρυθμίσετε τον έλεγχο ταυτότητας δύο παραγόντων ή πολλαπλών παραγόντων (MFA) για διάφορους λογαριασμούς και συστήματα. Εφαρμόζοντας τις δεξιότητές σας, θα ρυθμίσετε το MFA ώστε να απαιτεί ένα πρόσθετο βήμα επαλήθευσης, όπως έναν κωδικό πρόσβασης μιας χρήσης ή σάρωση δακτυλικών αποτυπωμάτων, εκτός από τον συνηθισμένο κωδικό πρόσβασης. Αυτή η προληπτική προσέγγιση ενισχύει την ασφάλεια των ευαίσθητων λογαριασμών, καθώς προσθέτει ένα επιπλέον επίπεδο προστασίας από μη εξουσιοδοτημένη πρόσβαση, μειώνοντας τον κίνδυνο επιτυχημένων επιθέσεων στον κυβερνοχώρο, όπως το phishing ή η παραβίαση κωδικών πρόσβασης. |
| 70. Εφαρμόστε προσοχή και επαγρύπνηση κατά τη χρήση των πλατφορμών κοινωνικής δικτύωσης | L7 | A | Υιοθετώντας μια προσεκτική στάση απέναντι στη χρήση των μέσων κοινωνικής δικτύωσης, θα προσέχετε τις πληροφορίες που μοιράζεστε, τις ρυθμίσεις απορρήτου που εφαρμόζετε και τις συνδέσεις που αποδέχεστε. Αυτή η προληπτική προσέγγιση συμβάλλει στην προστασία των προσωπικών σας δεδομένων και των ευαίσθητων πληροφοριών σας από πιθανές απειλές όπως η κλοπή ταυτότητας, η κοινωνική μηχανική και οι απάτες στον κυβερνοχώρο. Έχοντας επίγνωση των κινδύνων που σχετίζονται με την υπερβολική κοινοποίηση ή την αποδοχή αιτημάτων φιλίας από άγνωστα άτομα, μπορείτε να διατηρήσετε μια ασφαλέστερη διαδικτυακή παρουσία και να μειώσετε την πιθανότητα να πέσετε θύμα παραβιάσεων ασφαλείας που σχετίζονται με τα μέσα κοινωνικής δικτύωσης. |
| 71. Να γνωρίζουν πώς να χρησιμοποιούν έναν χάκερ "λευκού καπέλου" για αξιολογήσεις της κυβερνοασφάλειας | L8 | K-A | Κατανοήστε τα οφέλη της πρόσληψης ενός χάκερ "λευκού καπέλου", γνωστού και ως ηθικού χάκερ, για τη διενέργεια αξιολογήσεων κυβερνοασφάλειας και τον εντοπισμό πιθανών τρωτών σημείων στα συστήματα του οργανισμού σας. Με την πρόσληψη ενός τέτοιου επαγγελματία, μπορείτε να ελέγξετε και να ενισχύσετε προληπτικά τις άμυνές σας, διασφαλίζοντας ότι οι πιθανές αδυναμίες ασφαλείας θα αντιμετωπιστούν προτού οι κακόβουλοι χάκερς μπορέσουν να τις εκμεταλλευτούν. Η προσέγγιση αυτή συμβάλλει στην ενίσχυση της κατάστασης κυβερνοασφάλειας του οργανισμού σας και ελαχιστοποιεί τον κίνδυνο παραβίασης δεδομένων και κυβερνοεπιθέσεων. |

| | | | |
|---|---|---|---|
| 72. Αναγνώριση και άμυνα απέναντι σε τακτικές κοινωνικής μηχανικής | L8 | K-S | Απόκτηση γνώσεων σχετικά με τις τακτικές κοινωνικής μηχανικής που χρησιμοποιούν οι κακόβουλοι φορείς και ανάπτυξη δεξιοτήτων για τον εντοπισμό και την κατάλληλη αντίδραση σε τέτοιες προσπάθειες, ενισχύοντας τη συνολική ανθεκτικότητα της κυβερνοασφάλειας. |

| | | | |
|---|---|---|---|
| 73. Η ικανότητα δημιουργίας ισχυρών και ασφαλών κωδικών πρόσβασης για ενισχυμένη ασφάλεια στον κυβερνοχώρο | L8 | A | Αποκτήστε γνώσεις σχετικά με τις αρχές δημιουργίας ισχυρών κωδικών πρόσβασης για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Ανάπτυξη δεξιοτήτων για τη δημιουργία κωδικών πρόσβασης με τουλάχιστον 12 χαρακτήρες, με συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών και ειδικών συμβόλων. Η εφαρμογή αυτών των πρακτικών αυξάνει την πολυπλοκότητα των κωδικών πρόσβασης, καθιστώντας τους λιγότερο ευάλωτους σε επιθέσεις brute-force και βελτιώνοντας σημαντικά τη συνολική ασφάλεια των λογαριασμών. |
| 74. Σχεδιάστε στρατηγικές αποτελεσματικής διαχείρισης πρόσβασης για την ενίσχυση της ασφάλειας των συσκευών που ανήκουν στην επιχείρηση και των ευαίσθητων δεδομένων. | L8 | S | Ως ιδιοκτήτης επιχείρησης, η διασφάλιση της κατάλληλης διαχείρισης πρόσβασης είναι ζωτικής σημασίας για τη διατήρηση της ασφάλειας των συσκευών και των ευαίσθητων δεδομένων του οργανισμού σας. Διαθέτοντας διαχειριζόμενα δικαιώματα διαχειριστή και περιορίζοντας τους υπαλλήλους από την εγκατάσταση μη εξουσιοδοτημένου λογισμικού ή την πρόσβαση σε ορισμένα δεδομένα στο δίκτυο, μπορείτε να ελαχιστοποιήσετε τον κίνδυνο πιθανών παραβιάσεων και συμβιβασμών στην ασφάλεια. Αυτή η προληπτική προσέγγιση συμβάλλει στην προστασία της επιχείρησής σας από μη εξουσιοδοτημένη πρόσβαση, διαρροές δεδομένων και πιθανές απειλές στον κυβερνοχώρο. Ελέγχοντας προσεκτικά την πρόσβαση σε κρίσιμους πόρους και δεδομένα, μπορείτε να διατηρήσετε ένα ασφαλές και εύρωστο περιβάλλον ΤΠ, προστατεύοντας την επιχείρησή σας και τα πολύτιμα περιουσιακά της στοιχεία από πιθανές βλάβες. |
| 75. Εκπαιδεύστε τους εργαζόμενους 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. | L8 | A | Είναι σημαντικό να ενημερωθούν οι εργαζόμενοι για τους κινδύνους που ενέχει η χρήση των προσωπικών τους λογαριασμών για εργασίες που σχετίζονται με την εργασία. Η χρήση προσωπικών λογαριασμών για επαγγελματικούς σκοπούς μπορεί να εκθέσει ευαίσθητες πληροφορίες της εταιρείας σε πιθανές απειλές ασφαλείας και παραβιάσεις δεδομένων. Με την εκπαίδευση των εργαζομένων σχετικά με αυτούς τους κινδύνους και την προώθηση της πρακτικής του διαχωρισμού προσωπικών και επαγγελματικών λογαριασμών, μπορείτε να συμβάλλετε στη διαφύλαξη των δεδομένων του οργανισμού σας και στην προστασία τους από μη εξουσιοδοτημένη πρόσβαση ή έκθεση. Η ενθάρρυνση των υπαλλήλων να χρησιμοποιούν αποκλειστικούς λογαριασμούς εργασίας και η υιοθέτηση ασφαλών πρακτικών σύνδεσης μπορούν να μειώσουν σημαντικά τις πιθανότητες παραβίασης εμπιστευτικών πληροφοριών, διασφαλίζοντας τη συνολική ασφάλεια και ακεραιότητα των επιχειρηματικών σας δραστηριοτήτων. |
| 76. Εφαρμόστε ένα σύστημα προσωπικών λογαριασμών για κάθε εργαζόμενο, ώστε να καθιερωθεί σαφής ευθύνη για την πρόσβαση σε ευαίσθητα δεδομένα και να παρακολουθούνται αποτελεσματικά οι δραστηριότητες των χρηστών. | L8 | A | Με τη δημιουργία ατομικών προσωπικών λογαριασμών για κάθε υπάλληλο, δημιουργείτε ένα σαφές και ανιχνεύσιμο σύστημα παρακολούθησης του ποιος έχει πρόσβαση σε ποιες πληροφορίες και σε ποια χρονική στιγμή. Αυτή η εξατομικευμένη προσέγγιση ενισχύει την ασφάλεια, καθώς αποδίδει συγκεκριμένες ενέργειες και ευθύνες σε μεμονωμένους υπαλλήλους, επιτρέποντάς σας να εντοπίζετε ευκολότερα τυχόν πιθανές παραβιάσεις της ασφάλειας ή μη εξουσιοδοτημένες δραστηριότητες. Με τη διαχείριση προσωπικών λογαριασμών, μπορείτε να παρακολουθείτε τις δραστηριότητες των χρηστών, να παρακολουθείτε τις προσπάθειες σύνδεσης και να εξετάζετε τα αρχεία καταγραφής πρόσβασης σε δεδομένα, ώστε να διασφαλίζετε ότι μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση σε ευαίσθητα δεδομένα. Αυτό το αυξημένο επίπεδο υπευθυνότητας ενισχύει τα συνολικά μέτρα κυβερνοασφάλειας και συμβάλλει στην προστασία της επιχείρησής σας από πιθανές εσωτερικές απειλές ή μη εξουσιοδοτημένη πρόσβαση σε κρίσιμες πληροφορίες. |

| | | | |
|---|---|---|---|
| 77. Γνωρίζετε πώς να εφαρμόζετε, να χειρίζεστε και να συντηρείτε λύσεις προστασίας τελικών σημείων για την προστασία μεμονωμένων συσκευών και δικτύων από απειλές ασφαλείας. | L8 | S | Η προστασία τελικού σημείου αναφέρεται σε ένα σύνολο μέτρων ασφαλείας που έχουν σχεδιαστεί για την προστασία μεμονωμένων συσκευών, όπως υπολογιστές, φορητοί υπολογιστές και φορητές συσκευές, από απειλές κυβερνοασφάλειας. Εξασφαλίζοντας την προστασία του τελικού σημείου, αναπτύσσετε σε κάθε συσκευή antivirus, anti-malware, τείχος προστασίας και άλλα εργαλεία ασφαλείας για την προστασία από κακόβουλο λογισμικό, μη εξουσιοδοτημένη πρόσβαση και παραβιάσεις δεδομένων. Αυτές οι λύσεις βοηθούν στον εντοπισμό και τον αποκλεισμό πιθανών απειλών, διασφαλίζοντας ότι οι συσκευές είναι λιγότερο ευάλωτες σε μολύνσεις από κακόβουλο λογισμικό, κλοπή δεδομένων και επιθέσεις στον κυβερνοχώρο. Η εφαρμογή και η τακτική ενημέρωση των μέτρων προστασίας των τελικών σημείων ενισχύει τη συνολική στάση ασφαλείας σας και δημιουργεί ένα ασφαλέστερο υπολογιστικό περιβάλλον για τους υπαλλήλους και τα δεδομένα του οργανισμού. |

| | | | |
|---|---|---|---|
| 78. 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. | L8 | A | Η υιοθέτηση πολιτικών διατήρησης δεδομένων συμβάλλει στην αποτελεσματική διαχείριση των δεδομένων και στη μείωση του κινδύνου παραβίασης δεδομένων. Με το να μην διατηρείτε δεδομένα για περισσότερο χρόνο από όσο χρειάζεται, ελαχιστοποιείτε τον όγκο των προσωπικών πληροφοριών που κινδυνεύουν σε περίπτωση κυβερνοεπίθεσης ή παραβίασης δεδομένων. Η πρακτική αυτή οδηγεί επίσης στην απελευθέρωση αποθηκευτικού χώρου, στη βελτιστοποίηση της αποθήκευσης δεδομένων και στον εξορθολογισμό των διαδικασιών διαχείρισης δεδομένων. Η τακτική επανεξέταση και εκκαθάριση των περιττών δεδομένων διασφαλίζει ότι οι ευαίσθητες πληροφορίες προστατεύονται επαρκώς και μειώνει την πιθανότητα μη εξουσιοδοτημένης πρόσβασης ή διαρροής δεδομένων. Ως αποτέλεσμα, ενισχύεται η θέση του οργανισμού στον κυβερνοχώρο και διατηρείται η συμμόρφωση με τους κανονισμούς προστασίας δεδομένων. |
| 79. Βελτιστοποιήστε τις ρυθμίσεις και τις επιδόσεις του προγράμματος περιήγησης για να βελτιώσετε την ταχύτητα και την αποτελεσματικότητα της περιήγησης. | L8 | S | Προσαρμόζοντας τις ρυθμίσεις και τις διαμορφώσεις του προγράμματος περιήγησης, μπορείτε να βελτιώσετε την απόδοσή του, με αποτέλεσμα την ταχύτερη και ομαλότερη εμπειρία περιήγησης. Αυτό μπορεί να περιλαμβάνει την εκκαθάριση της cache και των cookies, την απενεργοποίηση περιττών επεκτάσεων και την ενημέρωση του προγράμματος περιήγησης στην τελευταία έκδοση. Η λήψη αυτών των μέτρων θα ενισχύσει την ταχύτητα του προγράμματος περιήγησης, καθιστώντας το πιο ευέλικτο και αποτελεσματικό στο χειρισμό του περιεχομένου του ιστού και μειώνοντας τους χρόνους φόρτωσης των ιστοσελίδων. Επιπλέον, η βελτιστοποίηση του προγράμματος περιήγησής σας μπορεί επίσης να οδηγήσει σε βελτιωμένη ασφάλεια και προστασία της ιδιωτικής ζωής, εξαλείφοντας πιθανά τρωτά σημεία και μειώνοντας τον κίνδυνο παρακολούθησης ή συλλογής δεδομένων μέσω cookies. |

| | | | |
|---|---|---|---|
| 80. Εξατομικεύστε τις ρυθμίσεις ασφαλείας του προγράμματος περιήγησης για να ενισχύσετε την ασφάλεια και το απόρρητο στο διαδίκτυο. | L8 | S | Η προσαρμογή των ρυθμίσεων ασφαλείας του προγράμματος περιήγησης σάς επιτρέπει να προσαρμόζετε την εμπειρία περιήγησής σας σύμφωνα με τις συγκεκριμένες προτιμήσεις σας όσον αφορά την ασφάλεια και το απόρρητο. Με την προσαρμογή ρυθμίσεων όπως το απόρρητο, οι αποκλεισμοί αναδυόμενων παραθύρων, η διαχείριση των cookies και τα επίπεδα ασφαλείας, μπορείτε να ενισχύσετε την ικανότητα του προγράμματος περιήγησής σας να προστατεύει από διάφορες διαδικτυακές απειλές και την παρακολούθηση δεδομένων. Για παράδειγμα, η ενεργοποίηση αυστηρών ρυθμίσεων απορρήτου μπορεί να περιορίσει τον όγκο των πληροφοριών που συλλέγουν οι ιστότοποι για εσάς, ενώ η ενεργοποίηση των μηχανισμών αποκλεισμού αναδυόμενων παραθύρων συμβάλλει στην αποτροπή ανεπιθύμητων διαφημίσεων ή δυνητικά κακόβουλου περιεχομένου. Κάνοντας αυτές τις ρυθμίσεις, μπορείτε να ενισχύσετε την ασφάλεια του προγράμματος περιήγησής σας, καθιστώντας το πιο ανθεκτικό απέναντι σε πιθανούς κινδύνους στον κυβερνοχώρο και διασφαλίζοντας τα προσωπικά σας δεδομένα κατά τη διάρκεια των διαδικτυακών αλληλεπιδράσεων. |

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.