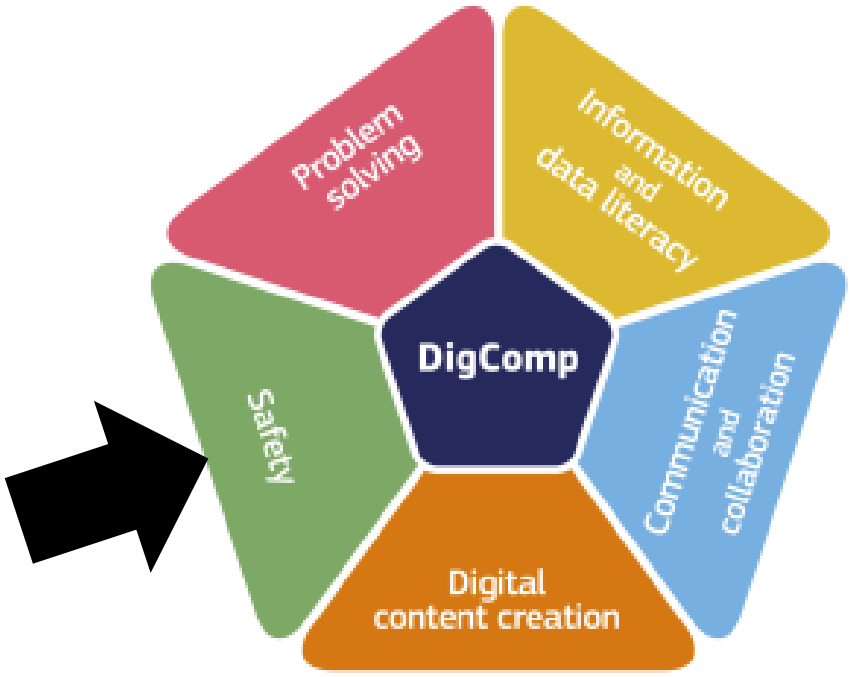
MICRO-CREDITE PENTRU SIGURANȚĂ
COMPETENȚA 4.1:
PROTECȚIA DISPOZITIVELOR

DSW
DIGITAL SKILLS WALLET

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Micro-credite pentru competența 4.2: PROTECȚIA DISPOZITIVELOR



Cuprins

NIVELUL DEBUTANT....9
(Nivelul 1 și Nivelul 2)....9
Elementele fundamentale ale securității digitale (MC 4.1.A.1)....10
Specificații....10
Rezultatele învățării....11
Descriere....11
Întrebări....12
Securitatea cinernetică și siguranța personală (MC 4.1.A.2)....13
Specificații....13
Rezultatele învățării....14
Descriere....14
Întrebări....15
Elemente esențiale de securitate digitală și confidențialitate (MC 4.1.A.3)....17
Specificații....17
Rezultatele învățării....18
Descriere....18
Întrebări....19
Managementul confidențialității digitale și al securității cibernetice (MC 4.1.A.4)....20
Specificații....20
Rezultatele învățării....21
Descriere....21
Întrebări....22
Principiile utilizării în siguranță a dispozitivelor și a colaborării digitale (MC 4.1.A.5)....23
Specificații....23
Rezultatele învățării....24
Descriere....24
Întrebări....25
Confidențialitatea online și siguranța copiilor în lumea digitală (MC 4.1.A.6)....26
Specificații....26
Rezultatele învățării....27
Descriere....27
Întrebări....28
Comportamentul digital și securitatea dispozitivului (MC 4.1.A.7)....29
Specificații....29

Rezultatele învăţării 30
Descriere 30
Întrebări 31
Managementul securității dispozitivului și a protecției datelor (MC 4.1.A.8) 32
Specificații 32
Rezultatele învăţării 33
Descriere 33
Întrebări 34
NIVELUL INTERMEDIAR 35
(Nivelul 3 și Nivelul 4) 35
Cele mai bune practici de securitate cibernetică (MC 4.1.B.1) 36
Specificații 36
Rezultatele învăţării 37
Descriere 37
Întrebări 38
Gestionarea pierderilor dispozitivelor și a protecției datelor (MC 4.1.B.2) 39
Specificații 39
Rezultatele învăţării 40
Descriere 40
Întrebări 41
Confidențialitatea online și securitatea aplicațiilor (MC 4.1.B.3) 42
Specificații 42
Rezultatele învăţării 43
Descriere 43
Întrebări 44
Comportamentul digital securizat și securitatea dispozitivului fizic (MC 4.1.B.4) 45
Specificații 45
Rezultatele învăţării 46
Descriere 46
Întrebări 47
Conștientizarea amenințărilor digitale și gestionarea/management-ul parolelor (MC 4.1.B.5) 48
Specificații 48
Rezultatele învăţării 49
Descriere 49
Întrebări 50

Securitatea dispozitivului și întreținerea software-ului (MC 4.1.B.6) 51
Specificații 51
Rezultatele învățării 52
Descriere 52
Întrebări 53
Gestionarea securității dispozitivelor și protejarea confidențialității datelor (MC 4.1.B.7) 54
Specificații 54
Rezultatele învățării 55
Descriere 55
Întrebări 56
Securitatea lucrului la distanță (remote working) și securitatea arhivării digitale (MC 4.1.B.8) 57
Specificații 57
Rezultatele învățării 58
Descriere 58
Întrebări 59
Securitatea dispozitivelor portabile și siguranța descărcărilor aplicațiilor (MC 4.1.B.9) 60
Specificații 60
Rezultatele învățării 61
Descriere 61
Întrebări 61
NIVELUL AVANSAT 63
(Nivelul 5 și Nivelul 6) 63
Securitatea dispozitivelor personale și cele mai bune practici (MC 4.1.C.1) 64
Specificații 64
Rezultatele învățării 65
Descriere 65
Întrebări 65
Securitatea parolelor și cele mai bune practici (MC 4.1.C.2) 67
Specificații 67
Rezultatele învățării 68
Descriere 68
Întrebări 69
Managementul securității dispozitivelor și eficiența datelor (MC 4.1.C.3) 70
Specificații 70
Rezultatele învățării 71

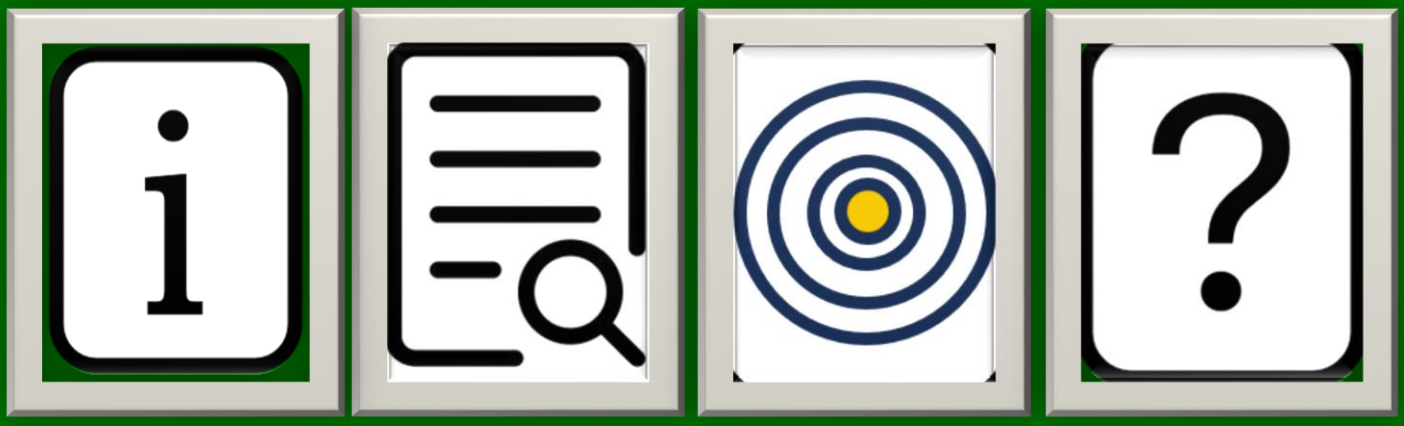
Descriere 71
Întrebări 72
Siguranța digitală și manipularea securizată a datelor (MC 4.1.C.4) 73
Specificații 73
Rezultatele învățării 74
Descriere 74
Întrebări 75
Securitatea dispozitivului și protecția datelor (MC 4.1.C.5) 76
Specificații 76
Rezultatele învățării 77
Descriere 77
Întrebări 78
Instruire și implementare cuprinzătoare în domeniul securității (MC 4.1.C.6) 79
Specificații 79
Rezultatele învățării 80
Descriere 80
Întrebări 81
Conștientizarea securității cibernetice și protecția dispozitivelor (MC 4.1.C.7) 82
Specificații 82
Rezultatele învățării 83
Descriere 83
Întrebări 84
Practici avansate de securitate pentru dispozitivele și sistemele personale (MC 4.1.C.8) 85
Informatii de baza 85
Rezultatele învățării 86
Descriere 86
Întrebări 87
NIVELUL EXPERT 88
(Nivelul 7 și Nivelul 8) 88
Managementul riscurilor de securitate cibernetică și conștientizarea personalului (MC 4.1.D.1) 89
Specificații 89
Rezultatele învățării 90
Descriere 90
Întrebări 91
Securitatea cibernetică centrată pe date și managementul datelor redundante (MC 4.1.D.2) 92

Specificații 92
Rezultatele învățării 93
Descriere 93
Întrebări 94
Conducerea securității cibernetice și dezvoltarea culturii (MC 4.1.D.3) 95
Specificații 95
Rezultatele învățării 96
Descriere 96
Întrebări 97
Managementul securității datelor și conștientizarea cibernetică (MC 4.1.D.4) 98
Specificații 98
Rezultatele învățării 99
Descriere 99
Întrebări 100
Securitate cibernetică avansată și hacking etic (MC 4.1.D.5) 101
Specificații 101
Rezultatele învățării 102
Descriere 102
Întrebări 104
Expert în securitatea cibernetică - Parole sigure și gestionarea accesului (MC 4.1.D.6) 105
Specificații 105
Rezultatele învățării 106
Descriere 106
Întrebări 107
Conștientizarea în securitate cibernetică și gestionarea conturilor (MC 4.1.D.7) 108
Specificații 108
Rezultatele învățării 109
Descriere 109
Întrebări 110
Managementul securității cibernetice - Protecția endpoint-urilor și păstrarea datelor (MC 4.1.D.8) 111
Specificații 111
Rezultatele învățării 112
Descriere 112
Întrebări 113
Optimizarea browserului și gestionarea securității (MC 4.1.D.9) 114

Specificații 114
Rezultatele învățării 115
Descriere 115
Întrebări 116
DICȚIONAR DE TERMENI 117
INTRODUCERE: 121
CERINȚE PRELIMINARE 123
ANEXĂ - COMPETENȚA 4.1. – PROECȚIA DISPOZITIVELOR 124

NIVELUL DEBUTANT

(Nivelul 1 și Nivelul 2)



Elementele fundamentale ale securității digitale (MC 4.1.A.1)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Elementele fundamentale ale securității digitale Cod: MC 4.1.A.1
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: 101087628
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	DEBUTANT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.1 și 4.1.3):

Elementele fundamentale ale securității digitale

- Recunoașteți importanța utilizării parolelor unice pentru diferite conturi online, pentru sporirea securității.
- Identificați semnele comune ale încercărilor de phishing și aflați cum să evitați să deveniți victima unor astfel de escrocherii.

Descriere

Micro-creditul (MC-ul) **„Elementele fundamentale ale securității digitale”** este un program de inițiere, conceput meticulos pentru a oferi cursanților o înțelegere aprofundată și abilități practice în domeniul securității digitale. Avizat de către profesioniștii în securitate cibernetică din întreaga lume, acest curs prezintă măsurile esențiale pentru păstrarea integrității identității digitale și a activelor utilizatorului, de la utilizarea parolei unice până la detectarea și evitarea phishing-ului.

Programul începe cu importanța securității parolei. Securitatea parolei este o componentă critică a securității digitale, trecută cu vederea de cele mai multe ori. Cursanții vor înțelege importanța creării unor parole puternice și unice pentru fiecare dintre conturile lor online, ceea ce reduce riscul ca mai multe conturi să fie compromise în cazul în care unul dintre ele este spart. Cursul oferă exerciții practice pentru a proiecta parole care echilibrează memorabilitatea și complexitatea, valorificând cele mai bune practici, cum ar fi utilizarea managerilor de parole și autentificarea prin mai mulți factori, pentru un nivel suplimentar de securitate.

De la securitatea parolei, cursul trece în domeniul detectării și răspândirii phishing-ului. Cursanții sunt introduși în conceptul de phishing - încercări înșelătoare de a obține informații sensibile pretinzând că sunt o entitate de încredere. Aceștia sunt învățați să identifice tacticile comune de phishing, cum ar fi e-mailurile, mesajele sau site-urile web frauduloase. Cursul oferă un mediu sigur, simulat, în care cursanții pot recunoaște și răspunde practic la încercările de phishing, consolidându-și astfel experiența de învățare.

În plus, cursul acoperă aspecte suplimentare ale securității digitale, inclusiv înțelegerea riscurilor rețelelor nesecurizate, importanța actualizării regulate a software-ului pentru a corecta vulnerabilitățile de securitate și utilizarea criptării pentru a securiza transmiterea datelor. De asemenea, pune accent navigarea în siguranță, cum ar fi verificarea certificatelor de securitate ale site-urilor web și evitarea descărcărilor din surse neverificate.

Programul culminează cu scenarii din lumea reală în care cursanții pot aplica conceptele pe care le-au învățat, oferind o măsură practică a înțelegerii și pregătirii lor. Evaluările sunt concepute pentru a emula amenințările digitale pe care cursanții le pot întâlni în viața lor de zi cu zi, ajutându-i să înțeleagă cum să reacționeze în mod corespunzător și să-și protejeze securitatea digitală.

La finalizarea cu succes, cursanții primesc Micro-Creditul „Elementele fundamentale ale securității digitate”, o recunoaștere a competenței lor în protejarea identității și a activelor digitale. Fie că ești un profesionist care dorește să-și consolideze abilitățile de securitate digitală, fie o persoană care dorește să-și îmbunătățească siguranța personală online, acest program oferă o bază de cunoștințe fundamentale și un set de instrumente

pentru consolidarea securității digitale.
Acest MC se aliniază cu angajamentul UE care vizează consolidarea competențelor digitale ale cetățenilor și conștientizarea siguranței online și este aprobat ca o realizare de învățare compactă, specifică și semnificativă, care demonstrează stăpânirea aspectelor esențiale ale securității digitale.

Întrebări

Parole unice pentru conturile online

1. Explicați posibilele consecințe ale utilizării aceleiași parole pentru mai multe conturi online.
2. Cum sporește securitatea folosirea parolelor unice pentru fiecare cont?
3. Care sunt cele mai bune practici pentru crearea unei parole puternice, unice?
4. Discutați rolul managerilor de parole în menținerea parolelor unice. Sunt eficiente?

Vigilență și conștientizarea împrejurărilor

5. Descrieți o situație în care lipsa de conștientizare a împrejurărilor vă poate compromite siguranța personală sau securitatea dispozitivelor digitale.
6. Cum ar fi putut un comportament vigilent să împiedice acest lucru?
7. Puteți explica câteva strategii de creștere a conștientizării situației, în special în spațiile publice?
8. Ce tehnologii sunt disponibile pentru a ajuta la menținerea conștientizării și a siguranței personale?

Tentative de phishing și escrocherii

9. Descrieți trei indicatori comuni ai unei încercări de phishing.
10. Explicați cum să răspundeți dacă bănuiți că ați primit un mesaj sau un e-mail de phishing.
11. Ce pași ar trebui urmați dacă ați căzut victima unui atac de tip phishing?
12. Discutați rolul autentificării cu doi factori (2FA) în protejarea împotriva phishing-ului.

Măsuri generale de securitate

13. Cum poate educația generală privind cele mai bune practici de securitate cibernetică să îmbunătățească atât siguranța digitală personală, cât și cea colectivă?

Securitatea cinernetică și siguranța personală (MC 4.1.A.2)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea cibernetică și siguranța personală **Cod: MC 4.1.A.2**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	DEBUTANT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.2 și 4.1.4):
Securitatea cibernetică și siguranța personală

Vigilența digitală

1. Recunoașteți e-mailurile, mesajele sau site-urile web suspecte care ar putea încerca să vă înșele pentru a dezvălui informații personale sau credențiale de conectare.

Conștientizarea mediului

2. Promovează o atitudine de vigilență și de conștientizare a mediului înconjurător.

Descriere

„**Securitatea cibernetică și siguranța personală**” este un program inovator care integrează formarea în domeniul securității digitale cu conștientizarea asupra siguranței personale. Acest curs distinctiv, conceput de experți în securitate cibernetică și susținători ai siguranței personale, își propune să ofere cursanților o înțelegere cuprinzătoare atât a amenințărilor digitale, cât și a problemelor de securitate din lumea reală.

În domeniul securității cibernetice, programul oferă o introducere cuprinzătoare în peisajul amenințărilor digitale. Cursul îi ajută pe cursanți să identifice potențialele amenințări cibernetice, cum ar fi e-mailurile suspecte, mesajele înșelătoare și site-urile web rău intenționate. Participanții vor explora diferite tipuri de programe malware, escrocherii de tip phishing și atacuri de inginerie socială, învățând să identifice semnele distinctive ale unor astfel de amenințări și cum să reacționeze în mod corespunzător. Programul analizează, de asemenea, obiceiurile de navigare în siguranță, practicile de comunicare sigură și utilizarea responsabilă a rețelelor sociale și a platformelor online, urnizând cursanților cunoștințele necesare pentru a naviga în lumea digitală în siguranță.

În ceea ce privește siguranța personală, cursul promovează un sentiment acut de conștientizare a mediului înconjurător. Aceasta implică instruirea în tehnici de conștientizare a situației, cruciale pentru securitatea personală în diverse medii (spații publice, serviciu, acasă). Cursul oferă sfaturi practice pentru identificarea și evitarea situațiilor potențial periculoase, dar și tehnici de dezescaladare a situațiilor și protecție la confruntarea cu o amenințare. Programul subliniază legătura dintre securitatea digitală și siguranța personală, demonstrând modul în care îmbunătățirea obiceiurilor online poate reduce vulnerabilitățile din lumea reală.

Partea finală a programului include o serie de exerciții practice și scenarii din lumea reală în care cursanții își pot aplica noile cunoștințe în materie de securitate cibernetică și siguranță personală. Aceste evaluări, concepute cu atenție pentru a imita situațiile din lumea reală, oferă cursanților o oportunitate practică de a-și testa abilitățile și de a-și consolida învățarea.

La finalizarea cu succes a MC-ului, cursanții vor dobândi competențe în identificarea și atenuarea potențialelor amenințări digitale, precum și în o mai bună înțelegere a principiilor și a practicilor de siguranță personală.

MC-ul „Securitatea cibernetică și siguranța personale” adoptă o abordare centrată pe cursant, ajustând ritmul cursului pentru a se potrivi nevoilor fiecărui cursant. Astfel, toți cursanții, indiferent de nivelul lor de expertiză

tehnică, poate urma și valoariza la maxim acest curs.
În segmentul de securitate cibernetică, programul prezintă în profunzime diferitele tipuri de amenințări online. De exemplu, cursanții obțin o înțelegere aprofundată a programelor malware - formele acestuia, modul în care funcționează și daunele potențiale pe care le poate provoca un malware. Ei învață, de asemenea, despre atacurile de tip phishing, care păcălesc utilizatorii să dezvăluie informații sensibile și cum să detecteze și să evite astfel de escrocherii. De asemenea, cursul îi familiarizează pe cursanți cu conceptul de atacuri de inginerie socială, care exploatează psihologia umană pentru a obține acces neautorizat la date sau sisteme. Cursul pune un accent deosebit pe cunoștințele practice și adoptă o abordare practică, cursanții exersându-și abilitățile în medii simulate.

În paralel cu instruirea în domeniul securității cibernetice, programul oferă cursanților o formare vitală privind siguranța personală. Aceasta include conștientizarea situației – a fi conștient de mediul utilizatorului și a identifica potențialele amenințări. Cursul prezintă diverse scenarii din viața reală pentru a ajuta cursanții să înțeleagă potențialele pericole și cum să le evite sau cum să gestioneze astfel de situații. Se pune accent pe promovarea unei atitudini generale de vigilență și luarea de măsuri proactive pentru a asigura siguranța personală.

Cursul este punctat cu evaluări pentru a se asigura că cursanții înțeleg și pot aplica conceptele pe care le-au învățat. Aceste evaluări imită situațiile din lumea reală, ajutând să pregătească cursanții pentru tipul de amenințări cu care se pot confrunta în viața lor de zi cu zi, atât online, cât și offline.

Dincolo de a viza dobândirea de către cursanți a abilităților critice de securitate cibernetică și de siguranță personală, programul urmărește, de asemenea, să le insufle o cultură a învățării continue. Peisajul amenințărilor digitale este în continuă evoluție, iar noile provocări privind siguranța personală apar în mod regulat. Ca atare, cursul încurajează cursanții să rămână la curent cu cele mai recente evoluții din ambele domenii, asigurându-se că abilitățile lor fac față[noilor amenințări.
Cu alte cuvinte, MC-ul „Securitatea cibernetică și siguranța personală” nu oferă doar cunoștințe teoretice și practice; mai mult, insuflă o mentalitate de vigilență, atât online, cât și offline. Se adresează oricărei persoane care dorește să-și îmbunătățească poziția în materie de securitate digitală și conștientizarea siguranței personale, inclusiv profesioniști, studenți și utilizatori de internet de zi cu zi.

În concluzie, MC-ul „Securitatea cibernetică și siguranța personală” constituie o călătorie de învățare holistică, în care cursanții dobândesc abilitățile esențiale pentru a naviga în lumea modernă, interconectată. Fie că ești un profesionist în securitate cibernetică care dorește să-și îmbunătățească abilitățile de siguranță personală sau o persoană care dorește să-și consolideze înțelegerea amenințărilor digitale și a siguranței personale, acest program oferă cunoștințele și instrumentele necesare pentru a-ți îmbunătăți securitatea atât în online, cât și în offline.

Acest MC se aliniază cu angajamentul UE care vizează consolidarea competențelor digitale ale cetățenilor și conștientizarea și promovarea siguranței personale. Acest MC certifică faptul că elevul stăpânește foarte bine conceptele din aceste două domenii vitale: siguranță și securitate.

Întrebări

Vigilență digitală

1. Care sunt trei caracteristici comune ale unui e-mail sau mesaj suspect care ar putea încerca să vă înșele pentru a dezvălui informații personale sau credențiale de conectare? Cum ai face față unei asemenea situații?

2. Care sunt alte câteva semne suplimentare de avertizare care trebuie căutate în mesajele sau site-urile web potențial frauduloase?
3. Descrieți rolul firewall-urilor și al software-ului antivirus în îmbunătățirea vigilenței digitale.
4. Cât de important este să vă actualizați software-ul în mod regulat pentru menținerea securității digitale?
5. Explicați cum autentificarea cu mai mulți factori poate oferi un nivel suplimentar de protecție împotriva accesului neautorizat la conturile dvs.

Conștientizare a mediului

1. Descrieți o situație conștientizarea împrejurimilor v-ar putea ajuta să preveniți un potențial pericol (o încălcare a securității sau un risc pentru siguranța personală).
2. Ce măsuri pot fi luate pentru a îmbunătăți conștientizarea mediului?
3. Cum percepeți problemele de securitate în scopul de a contribui la un mediu mai sigur?
4. În absența tehnologiei, ce practici elementare puteți urma pentru a vă asigura că sunteți conștient de mediul înconjurător?
5. Care sunt câteva indicii de mediu care pot indica un potențial risc de siguranță?

Combinarea vigilenței digitale cu conștientizarea mediului

6. Imaginați-vă că primiți un e-mail pe telefon în timp ce vă aflați într-o cafenea aglomerată, solicitându-vi-se să vă validați imediat datele de conectare pentru contul dvs. bancar. Ce acțiuni ați lua în acest scenariu, luând în considerare atât vigilența digitală, cât și conștientizarea mediului?
7. Cum ar diferi răspunsul dvs. dacă ați primi același e-mail suspect într-un cadru privat?
8. Care sunt riscurile potențiale ale accesării conturilor personale printr-un Wi-Fi public? Cum pot fi atenuate aceste riscuri?

Întrebări generale

9. Cum pot organizațiile să joace un rol important în educarea indivizilor atât despre vigilența digitală, cât și despre conștientizarea mediului?
10. Care sunt beneficiile combinării vigilenței digitale și a conștientizării mediului într-o strategie cuprinzătoare de securitate?

Elemente esențiale de securitate digitală și confidențialitate (MC 4.1.A.3)

Specificații

Identificarea cursantului	Orice cetățean
Titlul micro-acreditării	Elemente esențiale de securitate digitală și confidențialitate **Cod: MC 4.1.A.3**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	DEBUTANT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.5, 4.1.6 și 4.1.7):
Elemente esențiale de securitate digitală și confidențialitate
Securitatea dispozitivului

1. Securizați-vă dispozitivul atunci când este nesupravegheat.

Securitatea rețelei

2. Descrieți importanța securizării rețelei dvs. de la domiciliu cu parole puternice și protocoale de criptare.

Siguranța rețelei publice Wi-Fi

3. Identificați riscurile asociate cu utilizarea rețelelor Wi-Fi publice.

Descriere

„Elementele esențiale de securitate digitală și confidențialitate" este un program intens, aprobat de Comisia Europeană, care are drept scop dobândirea de către cursanți a unei înțelegeri holistice a măsurilor de securitate digitală și a principiilor de confidențialitate. Acest program cuprinzător este structurat în jurul a trei piloni principali de securitate digitală și confidențialitate - securitatea dispozitivelor fizice, siguranța rețelei de acasă și utilizarea în siguranță a rețelelor Wi-Fi publice.

Călătoria din acest MC începe cu suiectul securității dispozitivului fizic. Printr-o îmbinare a teoriei cu practica, acest segment le va permite cursanților să stăpânească abilitățile necesare pentru a securiza dispozitivele nesupravegheate și să se familiarizeze cu o serie de mecanisme de blocare, sisteme biometrice și alte facilități de securizare specifice dispozitivului. Se evidențiază că securitatea dispozitivului este în mare parte înrădăcinată în precauții și în practici, care pot împiedica în mod eficient accesul fizic neautorizat.

Cursul îi îndreaptă ulterior pe cursanți spre domeniul securității rețelei de acasă. În această secțiune, cursanții navighează în aspectele complexe ale instalării și ale gestionării unei rețele de acasă, care să fie sigură. Cursanții vor cinoaște în profunzime concepte precum implementarea de parole robuste și unice și utilizarea protocoalelor de criptare de ultimă oră. Acest modul oferă cursanților o experiență practică, furnizânde-le cunoștințe neprețuite pe care le pot aplica pentru a-și securiza rețelele de acasă în viața de zi cu zi.

A treia piatră de temelie a cursului este centrată pe potențialele riscuri de securitate prezentate de rețelele Wi-Fi publice. În ciuda utilizării pe scară largă și a confortului lor, rețelele Wi-Fi publice prezintă provocări semnificative de securitate. În acest modul, cursanții vor dobândi informații despre aceste riscuri și vor înțelege cum datele pot fi interceptate sau manipulate atunci când folosesc rețelele Wi-Fi publice. Pentru a se proteja împotriva potențialelor amenințări din Wi-Fi-urile publice, cursanții vor cunoaște diverse strategii de utilizare în siguranță, inclusiv utilizarea VPN-urilor (rețele private virtuale), verificarea autenticității rețelei și evitarea activităților sensibile în timp ce sunt conectați la un Wi-Fi public. .

Etapa finală a programului oferă cursanților oportunitatea de dovedi abilitățile dobândite în scenarii practice, din lumea reală. Aceștia sunt evaluați pe baza capacității lor de a aplica cunoștințele și abilitățile dobândite

pentru a securiza eficient dispozitivele și rețelele digitale, oferindu-le o măsură concretă a învățării și progresului lor.

După finalizarea cu succes MC-ului „Elemente esențiale de securitate digitală și confidențialitate", cursanții primesc certificatul de absolvire - o recunoaștere prestigioasă, care constituie dovada înțelegerii lor cuprinzătoare despre securitatea digitală și confidențialitatea și capacitatea lor de a implementa aceste cunoștințe pentru a-și asigura peisajul digital.

În concluzie, MC-ul „Elemente esențiale de securitate digitală și confidențialitate" nu vizează doar dobândirea cunoștințelor teoretice. Acesta oferă cursanților abilități practice și aplicabile în securitate digitală și confidențialitate. Se adresează unui public larg, de la profesioniștii care doresc să-și îmbunătățească înțelegerea securității digitale până la utilizatorii obișnuiți care urmăresc să consolideze securitatea mediului lor digital. Acest MC se aliniază cu angajamentul UE care vizează îmbunătățirea competențelor digitale și ale securității cetățenilor, oferind un certificat validat care demonstrează competențe în securitate digitală și confidențialitate.

Întrebări

Securitatea dispozitivului:

1. Imaginați-vă că trebuie să lăsați laptopul nesupravegheat într-o bibliotecă publică pentru câteva minute. Ce pași ați urma pentru a vă securiza dispozitivul în acest timp?

Securitatea rețelei:

2. Explicați de ce este important să vă asigurați rețeaua de acasă cu parole puternice și protocoale de criptare. Puteți schița procesul de configurare a unor astfel de măsuri de securitate pe un router de acasă?

Siguranța în rețelele Wi-Fi publice:

3. Care sunt unele riscuri potențiale ale utilizării rețelelor Wi-Fi publice și cum puteți micșora/elimina aceste riscuri pentru a utiliza aceste rețele în siguranță?

Combinația securității dispozitivului, a rețelei de acasă și a rețelelor Wi-Fi prublice:

4. Să presupunem că lucrați într-o cafenea, folosind rețeaua Wi-Fi publică. Discutați pașii pe care i-ați urma pentru a vă asigura atât dispozitivul, cât și securitatea datelor, în acest scenariu.

Managementul confidențialității digitale și al securității cibernetice (MC 4.1.A.4)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul confidențialității digitale și al securității cibernetice **Cod: MC 4.1.A.4**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	FUNDAȚIE
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.8, 4.1.9 și 4.1.10):

Setările de confidențialitate

1. Descrieți modul în care revizuirea și ajustarea setărilor de confidențialitate pot ajuta la controlul informațiilor partajate pe dispozitive și a informațiilor de pe conturile online.

Conștientizarea securității cibernetice

2. Enumerați potențialele amenințări reprezentate prin riscurile digitale și importanța de a rămâne informați cu privire la cele mai bune practici de securitate cibernetică.

Gestionarea pierderii unui dispozitiv

3. Descrieți pașii pe care trebuie să îi urmați pentru a proteja datele personale și confidențialitatea, în cazul în care un dispozitiv este pierdut sau furat.

Descriere

„Managementul confidențialității digitale și al securității cibernetice” este un program intensiv, cu mai multe fațete. Este conceput pentru a cultiva competențe avansate în păstrarea confidențialității digitale și combaterea întregii game de amenințări la adresa securității cibernetice. Acest curs recunoscut de Comisia Europeană prezintă un curriculum cuprinzător în patru domenii critice: stăpânirea setărilor de confidențialitate ale dispozitivelor și ale contului online, înțelegerea potențialelor amenințări digitale, rămânerea la curent cu cele mai bune practici de securitate cibernetică și elaborarea de strategii pentru a proteja datele personale și confidențialitatea în cazul pierderii sau a furtului dispozitivului.

Cursul începe cu explorarea setărilor de confidențialitate, oferind cursanților o înțelegere exhaustivă a modului în care aceste setări pot fi reglate cu finețe pentru dispozitivele și conturile online, conform nevoilor lor. Prin explorarea unor scenarii din lumea reală, cursanții vor dobândi experiență practică în gestionarea acestor setări, subliniind necesitatea de a le revizui și modifica periodic, pentru a descuraja în mod eficient accesul neautorizat la date și pentru a îmbunătăți protecția confidențialității.

În continuare, cursul pătrunde în profunzime în lumea amenințărilor digitale. Această secțiune prezintă cursanților o mare varietate de riscuri de securitate cibernetică — de la scheme de phishing la atacuri sofisticate de malware, până la tactici din ce în ce mai răspândite de inginerie socială. Obiectivul nu este doar recunoașterea aceste amenințări, ci și înțelegerea mecanicii lor și de conceperea unor contra-măsuri eficiente. Studiile de caz ale unor breșe istorice semnificative în securitatea cibernetică oferă o înțelegere contextuală și lecții valoroase în atenuarea amenințărilor.

Al treilea modul se concentrează pe importanța de a fi, permanent, la curent cu cele mai recente bune practici de securitate cibernetică. Având în vedere evoluția rapidă a peisajului digital, acest segment prezintă cursanților cele mai actuale și eficiente strategii pentru minimizarea vulnerabilității digitale. Cursanții nu numai vor învăța despre aceste practici, ci vor înțelege și cum și când să le implementeze eficient, asigurându-se că mediile lor digitale rămân securizate.

Partea finală a cursului abordează strategiile de menținere a securității datelor personale și a confidențialității în cazul pierderii sau a furtului dispozitivului. Furnizează un ghid practic pentru utilizarea funcțiilor precum urmărirea dispozitivului, blocarea de la distanță și ștergerea datelor, astfel încât cursanții să poată răspunde rapid și eficient atunci când se confruntă cu astfel de situații.

La finalizarea cursului, cursanții sunt supuși unei evaluări cuprinzătoare, concepute pentru a le testa înțelegerea noțiunilor și a conceptelor și capacitatea de a aplica aceste cunoștințe în situații practice, din lumea reală. Finalizarea cu succes a evaluării recompensează cursanții cu o diplomă recunoscută, în conformitate cu standardele Comisiei Europene, care validează expertiza nou dobândită în managementul confidențialității digitale și al securității cibernetice.

În esență, MC-ul „Managementul confidențialității digitale și al securității cibernetice" urmărește o educație holistică în confidențialitatea și securitatea digitală. Conținând atât cunoștințe teoretice, cât și practice, cursul este recomandat unei game variate de cursanți - profesioniști, studenți și utilizatori zilnici ai dispozitiveloe digitale. Scopul său final este de a oferi participanților instrumentele și cunoștințele necesare pentru a naviga în lumea digitală cu încredere și în siguranță. Acest lucru se aliniază cu angajamentul Uniunii Europene de a promova inițiere și abilități în competențe digitale în rândul cetățenilor săi, oferind cursanților o certificare care le validează competența în gestionarea confidențialității digitale și a securității cibernetice.

Întrebări

Setările de confidențialitate:

1. Puteți discuta despre importanța revizuirii și ajustării regulate a setărilor de confidențialitate pentru dispozitivele și conturile online? Dați exemple de tipuri de informații pe care le puteți controla prin aceste setări.

Conștientizarea securității cibernetice:

2. Dați exemple de amenințări digitale pe care le-ați putea întâlni. Cum puteți fi la curent cu cele mai bune practici de securitate cibernetică, care ajută la atenuarea acestor amenințări?

Gestionarea pierderii dispozitivului:

3. În cazul unui dispozitiv pierdut sau furat, ce pași ar trebui să urmați pentru a vă asigura că datele dumneavoastră personale și confidențialitatea sunt protejate? Descrieți procesul atât pentru un dispozitiv Android, cât și pentru un dispozitiv iOS.

O combinație a tuturor:

4. Imaginează-ți că ți-ai pierdut smartphone-ul, care conține mai multe rețele sociale și conturi de e-mail. Descrieți modul în care înțelegerea prealabilă a setărilor de confidențialitate și a celor mai bune practici de securitate cibernetică vă pot ajuta în această situație. Ce acțiuni imediate ați lua pentru a vă proteja datele și confidențialitatea?

Principiile utilizării în siguranță a dispozitivelor și a colaborării digitale (MC 4.1.A.5)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Principiile utilizării în siguranță a dispozitivelor și a colaborării digitale **Cod: MC 4.1.A.5**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	DEBUTANT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.11, 4.1.12 și 4.1.13):

Managementul serviciilor de rețea

1. Recunoașteți importanța dezactivarii serviciilor de rețea inutile și a programelor care rulează în fundal (background programs) pe dispozitivele dvs. pentru a reduce potențialele zone de atac/suprafețe de atac (attack surfaces).

Securitatea dispozitivelor fizice

2. Fiți atenți la securitatea dispozitivului fizic, în special în locurile publice, pentru a preveni furtul și accesul neautorizat.

Siguranța colaborării digitale

3. Aplicați practici sigure de partajare a ecranului în timpul întâlnirilor virtuale sau a colaborărilor la distanță, pentru a proteja informațiile sensibile la accesul sau expunerea neautorizate.

Descriere

MC-ul „Principiile utilizării în siguranță a dispozitivelor și a colaborării digitale” este un curs aprofundat conceput pentru a oferi cursanților abilități-cheie pentru menținerea utilizării în siguranță a dispozitivului și promovarea siguranței în timpul colaborării digitale. Cursul abordează subiectele cruciale ale gestionării serviciilor de rețea pe dispozitive, ale asigurării securității dispozitivelor fizice (în special setările publice), și folosirea practicilor sigure în timpul partajării ecranului și al colaborării virtuale, pentru a preveni accesul neautorizat la informații sensibile.

Cursul începe prin a aborda aspectul critic al gestionării serviciilor de rețea pe dispozitive. Cursanții vor analiza importanța dezactivării serviciilor de rețea inutile și a programelor care rulează în fundal pe dispozitivele lor. Aceste măsuri reduc suprafețele potențiale de atac și sporesc securitatea generală a dispozitivelor. În acest modul, cursanții vor obține o perspectivă asupra modului în care funcționează serviciile de rețea și de ce minimizarea acestora este esențială pentru menținerea unui dispozitiv securizat.

În continuare, cursul se concentrează asupra securității dispozitivelor fizice. Acest modul recunoaște că, în ciuda predominării amenințărilor digitale, securitatea fizică rămâne o componentă esențială a siguranței globale a dispozitivului. Aici, cursanții vor explora strategii pentru a menține dispozitivele în siguranță în locuri publice, înțelegând că prevenirea furtului și a accesului fizic neautorizat este la fel de importantă ca și protejarea împotriva intruziunilor virtuale.

Partea finală a cursului se concentrează pe siguranța colaborării digitale. Pe măsură ce lucrul de la distanță și colaborările virtuale devin din ce în ce mai frecvente, înțelegerea modului de a proteja informațiile sensibile în timpul acestor interacțiuni este crucială. Cursanții vor dobândi abilități de a aplica practici sigure de partajare a ecranului în timpul întâlnirilor virtuale sau a colaborărilor la distanță. Ei vor înțelege cum să se asigure că sunt afișate doar informațiile necesare și cum să prevină accesul neautorizat sau expunerea datelor sensibile.

Intercalate cu exerciții practice și învățare bazată pe scenarii, acest curs vizează ca abilitățile predate sunt relevante și aplicabile în mediile reale. Participanții vor avea ocazia să lucreze în situații ipotetice, care consolidează cunoștințele dobândite și înțelegerea acestora.

MC-ul se încheie cu o evaluare care certifică înțelegerea de către cursanți a conținutului cursului. Cursanții care finalizează cu succes obțin un certificat care atestă competența lor în utilizarea sigură a dispozitivelor și în colaborarea digitală sigură, o certificare recunoscută în conformitate cu standardele Comisiei Europene.

Per total, MC-ul „Principiile utilizării în siguranță a dispozitivelor și a colaborării digitale" vizează formarea unei multitudini de abilități care vor permite cursanților să navigheze în mediul digital cu încredere și în siguranță. MC-ul constituie o resursă de neprețuit pentru cei care lucrează la distanță, pentru nomazii digitali, pentru studenți și pentru oricine colaborează frecvent sau comunică digital.

În conformitate cu inițiativele Uniunii Europene de a spori inițierea în mediul digital și securitatea, în rândul cetățenilor săi, acest MC conferă o validare a competenței cursanților în utilizarea în siguranță a dispozitivelor lor și participarea la colaborarea digitală, cu accent pe confidențialitate și securitate.

Întrebări

Pentru managementul serviciilor de rețea:

1. De ce este important să dezactivați serviciile de rețea inutile și programele de fundal pe dispozitivele dvs.? Cum contribuie această practică la reducerea suprafețelor potențiale de atac?

Pentru securitatea dispozitivelor fizice:

2. Descrieți câteva dintre cele mai bune practici pentru asigurarea securității fizice a dispozitivelor dvs., în special în locuri publice. Ce măsuri ați lua pentru a preveni accesul neautorizat sau furtul?

Pentru o colaborare digitală sigură:

3. Care sunt unele dintre cele mai bune practici pentru asigurarea confidențialității și securității datelor în timpul partajării ecranului în întâlnirile virtuale sau colaborările de la distanță?

Pentru o combinație a tuturor:

4. Să presupunem că lucrați într-un loc public și trebuie să participați la o întâlnire virtuală în care trebuie să vă partajați ecranul. Descrieți pașii pe care i-ați urma pentru a vă securiza dispozitivul, pentru a gestiona serviciile de rețea și pentru a asigura o colaborare digitală sigură.

Confidențialitatea online și siguranța copiilor în lumea digitală (MC 4.1.A.6)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Confidențialitatea online și siguranța copiilor în lumea digitală **Cod: MC 4.1.A.6**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	DEBUTANT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.14 și 4.1.15):

Confidențialitatea în rețelele sociale

1. Cunoașteți importanța revizuirii și a eliminării periodice a informațiilor dvs. personale stocate în bazele de date din rețelele sociale, pentru a vă proteja confidențialitatea conținutului digital.

Siguranța online a copiilor

2. Implementați controale parentale și software-uri de filtrare pentru a proteja copiii de conținutul neadecvat și de riscurile online.

Descriere

MC-ul „Confidențialitatea online și siguranța copiilor în lumea digitală” este un program specializat care abordează două aspecte esențiale ale siguranței digitale - menținerea confidențialității online și protejarea copiilor față de amenințările digitale. Acest program încurajează un comportament responsabil al cetățenilor, subliniind necesitatea de a gestiona eficient informațiile personale de pe rețelele sociale și utilizarea controlului parental și a software-ului de filtrare pentru a crea un mediu online mai sigur pentru copii.

Debutând cu o incursiune profundă în confidențialitatea online, primul modul abordează aspectul crucial al gestionării informațiilor personale pe rețelele sociale. Participanții vor dobândi cunoștințe solide despre setările de confidențialitate de pe diferite platforme de social media și despre modul de optimizare a acestora, în vederea protejării informațiilor personale. Cursanții vor afla despre importanța revizuirii și a eliminării periodice a informațiilor personale stocate în bazele de date ale rețelelor sociale și despre modul în care aceste măsuri protejează confidențialitatea conținutului digital al utilizatorului.

Cursul face apoi tranziție la subiectul siguranței copiilor în lumea digitală. Recunoscând proliferarea tehnologiei digitale în viața copiilor, modulul explorează potențialele amenințări cu care se pot confrunta copiii în mediul online, dar și modul în care adulții pot atenua aceste amenințări. Oferă instrucțiuni cuprinzătoare despre implementarea controalelor parentale și a software-ului de filtrare, oferind participanților strategii practice pentru a proteja copiii de conținutul neadecvat și de riscurile online.

Cursul combină instruirea teoretică cu exercițiile practice, astfel încât participanții să înțeleagă conceptele, dar să le și aplice într-un mod eficient. Studiile de caz din lumea reală și activitățile bazate pe scenarii vor oferi o experiență de învățare captivantă, permițând cursanților să-și contextualizeze mai bine învățarea.

Programul se încheie cu o evaluare care validează înțelegerea cursanților cu privire la subiectele vizate, rezultând un certificat de absolvire a MC-ului. Acest certificat poate fi partajat cu angajatorii sau în rețelele profesionale, oferind dovezi ale competenței cursantului în gestionarea confidențialității online și implementând măsuri pentru a asigura siguranța copiilor online.

MC-ul „Confidențialitatea online și siguranța copiilor în lumea digitală” se aliniază cu obiectivele principale ale Comisiei Europene de promovare a inițierii în competențele digitale și a utilizării în siguranță a internetului. MC-ul constituie o resursă valoroasă pentru părinți, educatori și pentru oricine este interesat să creeze un mediu online mai sigur pentru ei înșiși și pentru copii - o necesitate esențială în lumea noastră digitală.

Acest MC este în concordanță cu angajamentul Uniunii Europene de a consolida competențele digitale și de a promova siguranța online în rândul cetățenilor săi, în special în ceea ce privește confidențialitatea și protecția copilului. Oferă cursanților o certificare a înțelegerii și a competenței lor în gestionarea confidențialității online și a siguranței online a copiilor.

Întrebări

Pentru confidențialitatea rețelelor sociale:

1. Explicați de ce este important să revizuiți și să eliminați periodic informațiile personale stocate în bazele de date din rețelele sociale. Cum protejează această practică confidențialitatea conținutului digital?
2. Care sunt câțiva dintre pașii pe care i-ați urma pentru a vă proteja confidențialitatea pe platformele sociale? Furnizați exemple specifice legate de setările de confidențialitate și eliminarea informațiilor personale.

Pentru siguranța online a copiilor:

3. Discutați rolul controlului parental și al software-ului de filtrare în protejarea copiilor împotriva conținutului neadecvat și a riscurilor online. Dați un exemplu de situație în care aceste instrumente sunt utile.
4. Cum ați aborda configurarea controalelor parentale pe un dispozitiv care va fi folosit de un copil? Ce factori ați lua în considerare?

Pentru o combinație a ambelor:

5. Imaginează-ți că vrei să creezi un cont de social media pentru un copil sub supravegherea ta. Cum v-ați asigura de protejarea confidențialității copilului și de faptul că aceștia sunt protejați de conținutul neadecvat și de riscurile online?

Comportamentul digital și securitatea dispozitivului (MC 4.1.A.7)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Comportamentul digital și securitatea dispozitivului **Cod: MC 4.1.A.7**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	DEBUTANT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.16 și 4.1.17):

Practici de descărcare sigură

1. Înțelegeți riscurile asociate cu descărcarea de programe sau aplicații din surse neoficiale sau terțe.

Integritatea dispozitivului

2. Evitați utilizarea dispozitivelor afectate de jailbreaking sau rooting. Cum pot ocoli aceste metode (jailbreak și rootate) măsurile de securitate și cum pot compromite siguranța datelor dvs.?

Descriere

MC-ul „Comportamentul digital și securitatea dispozitivului” este un program cuprinzător menit să educe cursanții despre potențialele amenințări cibernetice și despre cum să navigheze în siguranță în mediul digital. Cursul subliniază riscurile implicate în descărcarea de software din surse neoficiale și implicațiile de securitate ale utilizării dispozitivelor cu jailbreak sau rootate. Oferă orientări practice privind adoptarea de comportamente digitale sigure și securizarea dispozitivelor, abordând aspectele cheie ale securității cibernetice în lumea de astăzi - condusă de tehnologie.

Programul începe prin prezentarea pericolelor asociate cu descărcarea de software sau aplicații din surse neoficiale sau terțe. Acest segment oferă o perspectivă asupra modului în care sursele neoficiale pot conține adesea programe malware, spyware sau alte programe dăunătoare deghizate în software legitim. Participanții vor învăța cum să identifice sursele sigure pentru descărcări și importanța menținerii software-ului actualizat prin canalele oficiale.

Următorul segment al cursului se concentrează pe potențialele riscuri de securitate ale dispozitivelor jailbreak sau rootate. Cursanții vor analiza modul în care aceste metode, oferind utilizatorilor un control mai mare asupra dispozitivelor lor, pot ocoli măsurile de securitate și le pot expune la software rău intenționat. Segmentul subliniază importanța înțelegerii compromisului dintre controlul îmbunătățit și riscurile crescute de securitate, care vin cu dispozitivele de jailbreaking sau rooting.

Pe lângă aceste subiecte cheie, cursul oferă și o prezentare generală a comportamentului digital sigur în general. Participanții vor fi educați cu privire la tehnicile de navigare în siguranță, securitatea parolei, recunoașterea încercărilor de phishing și menținerea securității dispozitivului. Această secțiune va evidenția, de asemenea, importanța acordării unei atenții sporite la securitatea dispozitivelor fizice, în special în locurile publice, pentru a preveni furtul și accesul neautorizat.

Cursul culminează cu exerciții practice, menite să pună în practică elementele teoretice, permițând cursanților să aplice cunoștințele dobândite în contexte reale. Participanții vor avea ocazia să participe la activități interactive, care simulează amenințările cibernetice comune, și vor învăța cum să răspundă eficient în astfel de situații.

După finalizarea acestei MC, cursanții dobîndi o înțelegere temeinică a comportamentului digital sigur și a securității dispozitivului. Ei vor putea lua decizii informate cu privire la descărcarea software-ului, la gestionarea dispozitivelor și la navigarea în siguranță în lumea digitală. Acest curs se aliniază cu angajamentul Uniunii Europene pentru promovarea inițierii în mediile digitale și a siguranței pe internet, făcându-l o resursă valoroasă pentru indivizi și profesioniști, deopotrivă.

În conformitate cu angajamentul Uniunii Europene de a promova inițirea în mediile digitale și securitatea digitală, această MC oferă un certifict validează înțelegerea și expertiza unui cursant în comportamentul digital sigur și securitatea dispozitivului.

Întrebări

Pentru practici de descărcare sigură:

1. Care este principalul pericol de a descărca software sau aplicații din surse neoficiale sau terțe?
2. Cum pot sursele neoficiale să mascheze programele dăunătoare?
3. Ce abilități sunt necesare în ceea ce privește identificarea surselor de descărcare sigure?
4. De ce este important să păstrăm software-ul actualizat prin canale oficiale?
5. Puteți enumera anumite tipuri de programe dăunătoare care ar putea fi găzduite pe surse neoficiale?

Pentru integritatea dispozitivului:

6. Care sunt potențialele riscuri de securitate asociate pentru dispozitivele cu jailbreaking sau rooting?
7. Cum jailbreaking-ul și rooting-ul oferă utilizatorilor un control mai mare asupra dispozitivelor lor?
8. În ce moduri poate ocoli măsurile de securitate jailbreaking-ul sau rooting-ul?
9. La ce tip de software rău intenționat ar putea fi expuși utilizatorii prin jailbreaking sau rootarea dispozitivelor lor?
10. De ce este important ca utilizatorii să înțeleagă compromisul dintre controlul îmbunătățit și riscurile de securitate sporite atunci când iau în considerare jailbreak-ul sau rootarea dispozitivelor lor?

Pentru combinarea ambelor

11. Care sunt componentele cheie ale comportamentului digital sigur?
12. Cum sugerează programul menținerea securității parolei?
13. Ce sugestii oferă programul pentru recunoașterea tentativelor de phishing?
14. Pe lângă precauțiile digitale, ce evidențiază programul despre securitatea dispozitivelor fizice?
15. De ce este deosebit de important să fim atenți la securitatea dispozitivului în locuri publice?

Managementul securității dispozitivului și a protecției datelor (MC 4.1.A.8)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul securității dispozitivului și a protecției datelor **Cod: MC 4.1.A.8**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	DEBUTANT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.18, 4.1.19 și 4.1.20):

Renunțarea la un dispozitiv

1. Cunoașteți importanța ștergerii și renunțării în siguranță a dispozitivelor vechi, pentru a preveni recuperarea datelor dvs. de către alții.

Criptarea datelor

2. Utilizați criptarea pentru a proteja datele sensibile de pe dispozitivele dvs., în special a datelor stocate pe dispozitivele mobile și a celor memorate pe alte dispozitive de memorare.

Conștientizarea încălcării datelor

3. Înțelegeți riscurile asociate cu transmiterea sau memorarea informațiilor personale pe dispozitive și potențialul de încălcare a datelor.

Descriere

MC-ul „Managementul securității dispozitivului și a protecției datelor” este un program captivant care ghidează cursanții prin conceptele cheie și prin aplicațiile de gestionare în siguranță a dispozitivelor digitale și a celor de protejare a datelor sensibile. Acesta acoperă o serie de subiecte critice, cum ar fi înțelegerea importanței renunțării în siguranță aa dispozitivele vechi, aplicarea criptării pentru protejarea datelor sensibile și conștientizarea potențialelor riscuri ale încălcării datelor atunci când se transmit sau se memorează informații personale pe dispozitive.

Cursul începe explorarea conceptului de management (gestionare) al dispozitivelor. Oferă o acoperire aprofundată a celor mai bune practici pentru ștergerea și eliminarea în siguranță a dispozitivelor vechi pentru a preveni recuperarea datelor sensibile de către persoane neautorizate.

Cursanții vor înțelege cum să elimine în mod eficient datele de pe dispozitive, atât manual, cât și folosind diverse instrumente software. De asemenea, vor învăța despre metodele de eliminare în siguranță, cum ar fi programele de reciclare și distrugere a dispozitivelor, pentru a se asigura că dispozitivele vechi nu devin un risc de securitate.

Al doilea modul aprofundează domeniul protecției datelor. Principiile și aplicarea criptării pentru a proteja datele sensibile de pe dispozitive, în special dispozitivele mobile și medii de stocare externe (removable mass storage), sunt discutate pe larg. Cursanții vor înțelege diferitele metode de criptare, cum să le aplice și importanța lor într-o abordare stratificată de securitate.

În cele din urmă, cursul abordează riscurile breșelor care pot să apară la memorarea și transmiterea informațiilor personale pe dispozitive. Participanții vor folosi scenarii din lumea reală, în care apar breșe ale datelor, cauzele și consecințele acestora. Cursanții vor învăța despre metodele de prevenire a breșelor de date, cum ar fi protocoalele de comunicații securizate, soluțiile de memorare securizate și cele mai bune practici pentru partajarea informațiilor personale. Acest modul va aborda, de asemenea, considerentele legale și etice legate de breșele de date.

Acest MC adoptă o abordare interactivă de învățare, combinând teoria cu exerciții practice. Cursanții vor avea ocazia să își aplice cunoștințele în activități practice, chestionare și studii de caz. Până la sfârșitul acestui curs, participanții vor avea cunoștințele și abilitățile necesare pentru a-și gestiona dispozitivele în siguranță și pentru a implementa măsuri solide de protecție a datelor.

În concordanță cu angajamentul Uniunii Europene în privința inițierii în mdiul digital și în securitatea digitală, MC-ul „Managementul securității dispozitivului și al protecției datelor" oferă informații și abilități valoroase pentru oricine este preocupat de securitatea digitală din lumea de astăzi. Le permite cursanților să își gestioneze cu încredere dispozitivele și să își protejeze datele sensibile de potențiale amenințări, ceea ce este din ce în ce mai important în era noastră digitală.

Întrebări

Pentru renunțarea la un dispozitivi:

1. De ce este esențial să ștergeți și să aruncați în siguranță dispozitivele vechi? Explicați ce s-ar putea întâmpla dacă acest pas este neglijat.
2. Descrieți pașii pe care i-ați urma pentru a șterge și a elimina în siguranță un laptop vechi. Ce măsuri de precauție ați lua pentru a vă asigura că nicio dată nu poate fi recuperată?"

Pentru criptarea datelor:

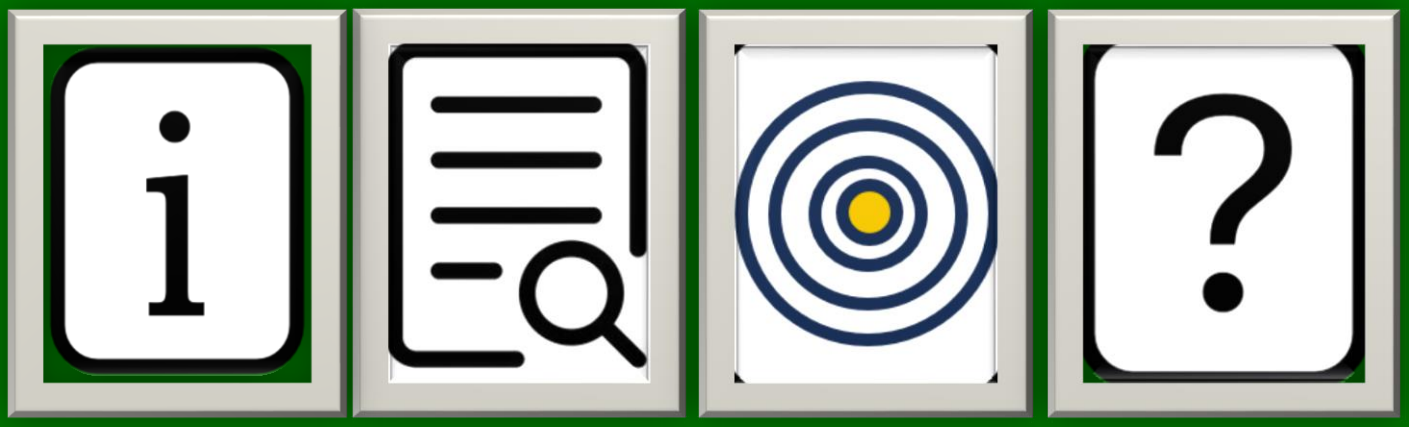
3. Explicați modul în care criptarea poate proteja datele sensibile de pe dispozitivele dvs. Dați exemple de situații în care acest lucru ar putea fi deosebit de util.
4. Discutați pașii de urmat pentru criptarea datelor de pe un dispozitiv mobil sau pentru cel de memorare pe un suport extern. De ce este important să criptăm datele stocate în astfel de dispozitive?

Pentru conștientizarea apariției breșelor de date:

5. Care sunt riscurile asociate cu transmiterea sau memorarea informațiilor personale pe dispozitive? Cum pot astfel de practici să ducă la potențiale breșe ale datelor?
6. Descrieți un scenariu în care ar putea apărea o breșă asupra datelor din cauza transmiterii sau memorării nesigure a datelor. Ce măsuri ar putea fi luate pentru a preveni un astfel de scenariu?

NIVELUL INTERMEDIAR

(Nivelul 3 și Nivelul 4)



Cele mai bune practici de securitate cibernetică (MC 4.1.B.1)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Cele mai bune practici de securitate cibernetică **Cod: MC 4.1.B.1**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	INTERMEDIAR
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LOs LO 4.1.21, 4.1.22):

Navigarea în siguranță și practici de descărcare

- Gestionați cu prudență link-urile suspecte și evitați descărcarea fișierelor care provin din surse necunoscute, pentru a vă proteja dispozitivele de potențialele amenințări malware.

Copii de rezervă (Data backup) și protecție

- Realizați cât este de important să realizați periodic de copii de rezervă ale datelor (data backup) pentru a vă proteja împotriva pierderii datelor și/sau a defectării dispozitivului.

Descriere

MC-ul „**Cele mai bune practici de securitate cibernetică**” este un program amplu, special conceput pentru a furniza cursanților cunoștințe și abilități cruciale, necesare pentru protejarea informațiilor și a dispozitivelor digitale împotriva unei game largi de amenințări. Acest program vizează aprofundarea înțelegerii și implementării practicilor sigure de navigare și descărcare, pentru a atenua amenințările malware. Mai mult, subliniază importanța copiilor de rezervă (backup-urilor) regulate ale datelor - o strategie puternică de protejare împotriva potențialelor pierderi de date sau defecțiuni ale dispozitivului.

Primul segment al acestui curs își urmărește o înțelegere profundă – de către cursanți - a practicilor de navigare în siguranță. Acesta analizează diverse tipuri de amenințări cibernetice, cum ar fi phishingul, programele malware și ransomware. Cursanții vor dobândi capacitatea de a le identifica și de a le atenua. Participanții vor deprinde practici de navigare sigură, inclusiv utilizarea HTTPS-lor, verificarea certificatelor site-urilor, implicațiile cookie-urilor și ale urmăririi (tracking-ului). Ei vor învăța, de asemenea, cum să gestioneze link-urile suspecte și cum să evite descărcarea fișierelor din surse necunoscute, pentru a preveni potențialele amenințări malware.

Al doilea modul vizează aprofundarea practicilor de descărcare sigură. Cursanții vor învăța despre riscurile asociate cu descărcarea programelor, fișierelor sau ale aplicațiilor care provin din surse neoficiale sau terțe. Ei vor învăța cum să analizeze siguranța unei surse și cât de important este să utilizeze pentru descărcări platformele oficiale. Modulul prezintă, de asemenea, riscurile potențiale ale deschiderii fișierelor comprimate, cum ar fi arhivele .zip sau .rar, provenite din surse nesigure sau necunoscute.

Modulul final se concentrează pe importanța realizării copiilor de rezervă a datelor (data backups). Participanții vor fi familiarizați cu diverse tehnici de back-up a datelor și vor înțelege rolul backup-urilor efectuate cu regularitate în securitatea cibernetică. Acest modul aprofundează crearea de back-upuri programate (backup schedules), alegând între soluțiile de backup în cloud sau fizice și criptarea backup-urilor pentru un nivel suplimentar de securitate.

Acest curs include, de asemenea, activități practice și scenarii din lumea reală, încurajând aplicarea practică a abilităților învățate. Testele și evaluările regulate vor urmări progresul participanților, asigurându-se că aceștia stăpânesc fiecare subiect, înainte de a trece la următorul.

La finalizarea acestui MC, cursanții vor dobândi o înțelegere solidă a principiilor și a practicilor securității cibernetice. Ei vor fi pregătiți pentru a naviga cu încredere în peisajul digital, păstrându-și datele și dispozitivele în siguranță. Acest MC se aliniază cu atenția cordată de Uniunea Europeană securității cibernetică și inițierii în lumea digitală, făcându-l un curs extrem de valoros pentru indivizi și profesioniști deopotrivă, în contextul actual.

Aliniindu-se cu obiectivul Uniunii Europeane de a îmbunătăți securitatea digitală, acest MC oferă o certificare a competenței unui cursant în aspectele cheie ale celor mai bune practici de securitate cibernetică.

Întrebări

Pentru practici sigure de navigare și descărcare:

1. De ce este important să fii precaut atunci când dați click pe linkuri sau când descărcați fișiere de pe internet? Ce riscuri ați putea întâmpina dacă nu sunteți precaut?
2. Imaginează-ți că primești un e-mail care conține un link, de la un expeditor necunoscut. Ce pași ați urma înainte de a decide dacă să faceți click pe link?
3. Descrieți riscurile asociate cu descărcarea fișierelor care provin din surse necunoscute. Cum pot fi atenuate aceste riscuri?

Pentru backup și protecția datelor:

4. De ce este important să faceți în mod regulat copii de siguranță ale datelor (data backups) dvs.? Cum protejează această practică împotriva pierderii de date și/sau a defecțiunilor dispozitivului?
5. Descrieți pașii pe care i-ați urma pentru a face copii de rezervă ale datelor de pe calculatorul Dvs. Cât de des ați recomanda efectuarea acestui proces?

Gestionarea pierderilor dispozitivelor și a protecției datelor (MC 4.1.B.2)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Gestionarea pierderilor dispozitivelor și a protecției datelor **Cod: MC 4.1.B.2**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	INTERMEDIAR
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LOs LO 4.1.23, 4.1.24):

Conștientizarea pierderii dispozitivelor

- Învățați că dispozitivele pierdute sau furate pot fi urmărite, blocate sau șterse folosind instrumente gratuite bazate pe web, disponibile pe majoritatea dispozitivelor.

Managementul practic al pierderilor dispozitivelor

- Utilizați cu pricepere funcțiile de urmărire, de blocare și de ștergere, pentru a vă proteja datele și confidențialitatea, în cazul în care dispozitivul este pierdut sau furat.

Descriere

MC-ul „**Gestionarea pierderilor dispozitivelor și a protecției datelor**” este un curs intensiv, practic, destinat să furnizeze cursanților cunoștințele și abilitățile necesare pentru a-și gestiona și pentru a-și proteja în mod eficient dispozitivele și datele, în cazuri de pierdere sau furt a dispozitivelor. Cusrul vizează o înțelegere aprofundată a modului de urmărire, blocare și ștergere a dispozitivelor pierdute sau furate - folosind instrumente bazate pe web - și aplicarea eficientă a acestor facilități pentru a proteja datele personale și pentru a asigura confidențialitatea.

Primul modul al cursului urmărește educarea participanților cu privire la măsurile care trebuie luate atunci când un dispozitiv este pierdut sau furat. Participanții vor învăța cum să urmărească aceste dispozitive utilizând instrumente de urmărire încorporate sau instrumente terță parte. Ei vor învăța, de asemenea, cum să-și blocheze dispozitivele de la distanță, făcându-le inaccesibile utilizatorilor neautorizați. Cursanții vor învăța cum să își șteargă de la distanță toate datele de pe dispozitivul pierdut sau furat, prevenind ca datele personale sensibile să cadă în mâinile altora.

Demonstrațiile practice vor oferi participanților o înțelegere aplicată a acestor proceduri.

Al doilea modul se concentrează pe pașii proactivi pentru protecția datelor. Participanții vor învăța cum să realizeze, în mod regulat, copii de siguranță ale datelor, minimizând pierderea de date în cazul furtului/pierderii sau defecțiunii dispozitivului. Ei vor explora diverse metode și soluții de backup, inclusiv backup-uri bazate pe cloud și opțiuni de memorare fizică. De asemenea, este subliniată importanța criptării pentru protejarea datelor sensibile, iar participanții vor învăța cum să implementeze criptarea pentru dispozitivele lor și pentru copiile de rezervă.

Subiectele suplimentare abordate în curs includ configurarea și gestionarea asigurării dispozitivului, înțelegerea aspectelor legale ale furtului dispozitivului și modul de raportare a unui dispozitiv pierdut sau furat către autorități și furnizori de servicii. Cursul va acoperi, de asemenea, importanța securizării dispozitivelor cu parole puternice, date biometrice sau alte măsuri de securitate, pentru a întârzia sau a preveni accesul neautorizat în cazul în care un dispozitiv este pierdut sau furat.

La sfârșitul acestui MC, cursanții vor înțelege în profunzime modul în care să gestioneze pierderea sau furtul unui dispozitiv și să își protejeze datele în mod eficient, asigurându-se că securitatea digitală și

confidențialitatea lor rămân intacte, chiar și în situații adverse. Acest MC se înscrie în angajamentul Uniunii Europene privind inițierea în securitatea digitală, oferind participanților un set de abilități esențiale pentru era digitală.

În concordanță cu angajamentul Uniunii Europene de a promova inițierea în digital și securitatea digitală, acest MC-ul oferă cursanților un certificat al competenței lor în gestionarea pierderii dispozitivelor și protejarea datelor.

Întrebări

Pentru conștientizarea pierderii dispozitivului:

1. „Descrieți importanța de a fi informat că dispozitivele pierdute sau furate pot fi urmărite, blocate sau șterse, folosind instrumente gratuite bazate pe web. Cum pot aceste cunoștințe să determine utilizatorii să își protejeze datele și confidențialitatea?”
2. „Cum ați explica cuiva care nu este familiarizat cu aceste facilități conceptul de urmărire, blocare sau ștergere a unui dispozitiv pierdut sau furat?”

Pentru managementul practic al pierderilor dispozitivelor:

3. „Dacă smartphone-ul tău s-ar pierde, ce pași ai realiza pentru a-l urmări, bloca sau șterge, folosind instrumentele disponibile pe web? Cum ai prioritiza aceste acțiuni?”
4. "Imaginați-vă că v-ați blocat de la distanță dispozitivul pierdut. Ce alți pași ați urma pentru a vă proteja datele și confidențialitatea într-o astfel de situație?"

Pentru o combinație a ambelor:

5. „Să presupunem că v-a fost furat laptopul. Cum ai aplica cunoștințele despre pierderea dispozitivului și gestionarea practică a pierderii dispozitivului, pentru a-ți proteja datele și confidențialitatea, în acest scenariu?”

Confidențialitatea online și securitatea aplicațiilor (MC 4.1.B.3)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Confidențialitatea online și securitatea aplicațiilor **Cod: MC 4.1.B.3**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	INTERMEDIAR
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.25, 4.1.26):

Managementul (gestionarea) sesiunii

- Înțelegeți importanța deconectarii la sfârșitul sesiunilor dvs. din internet sau din aplicații, pentru a vă proteja informațiile personale împotriva accesului neautorizat.

Gestionarea permisiunilor aplicației

- Înțelegeți cum să gestionați permisiunile aplicațiilor pentru a vă proteja confidențialitatea și fiți conștienți de datele colectate de către aplicațiile de pe dispozitivele dvs.

Descriere

MC-ul „**Confidențialitatea online și securitatea aplicațiilor**” este un program cuprinzător, meticulos conceput pentru a oferi o înțelegere solidă a confidențialității online și a practicilor de securitate a aplicațiilor. Acest program subliniază importanța gestionării eficiente a sesiunilor și a gestionării adecvate a permisiunilor aplicației, pentru a menține confidențialitatea datelor personale și confidențialitatea utilizatorilor.

Primul modul al acestui curs este centrat în jurul conceptului critic de confidențialitate online. Participanții vor aprofunda diferitele aspecte despre confidențialitatea online, inclusiv înțelegerea cookie-urilor, a tehnologiilor de urmărire, a amprentelor online și a practicilor de partajare a datelor. Ei vor învăța cum sunt utilizate, memorate și partajate online informațiile lor, și despre riscurile legate de confidențialitate. Acest modul se concentrează, de asemenea, pe importanța gestionării adecvate a sesiunilor, subliniind importanța deconectarii la sfârșitul sesiunilor de internet sau deconectării din aplicații, pentru a proteja informațiile personale împotriva accesului neautorizat. Participanții vor câștiga experiență practică în gestionarea sesiunilor online și în utilizarea instrumentelor de îmbunătățire a confidențialității, cum ar fi VPN-uri, navigarea privată și managerii de cookie-uri.

Al doilea modul abordează securitatea aplicațiilor, concentrându-se pe rolul permisiunilor aplicației în menținerea confidențialității utilizatorilor. Participanții vor explora modul în care aplicațiile accesează și utilizează datele personale prin permisiuni și potențialele implicații privind confidențialitatea. Ei vor înțelege cum să gestioneze în mod eficient permisiunile aplicației, oferind doar accesul necesar pentru a menține funcționalitatea, fără a compromite confidențialitatea. Modulul include exerciții practice de gestionare a permisiunilor pe o varietate de aplicații și platforme, oferind participanților abilități practice pe care le pot aplica în mediul digital.

În plus, cursul include sesiuni despre tendințele emergente privind confidențialitatea și securitatea online și potențialele dezvoltări viitoare în acest domeniu dinamic. Participanții se vor angaja în discuții pe subiecte precum confidențialitatea în rețelele sociale, rolul inteligenței artificiale în confidențialitate și a impactului reglementărilor privind confidențialitatea.

La finalizarea acestui MC, cursanții vor dobândi o înțelegere în profunzime a practicilor de confidențialitate online și a securității a aplicațiilor, împreună cu capacitatea de a implementa aceste principii în activitățile lor digitale zilnice. Acest MC se înscrie în angajamentul Uniunii Europene de a promova inițierea în mediul digital

și confidențialitatea, făcându-l un curs valoros pentru orice persoană care încearcă să îmbunătățească securitatea și confidențialitatea online.

Această MC se aliniază cu angajamentul Uniunii Europene de a consolida competențele digitale și de a promova siguranța online în rândul cetățenilor săi. Acesta oferă o certificare a măiestriei cursantului în gestionarea confidențialității online și a securității aplicațiilor.

Întrebări

Pentru managementul sesiunii:

1. De ce este important să vă deconectați la sfârșitul sesiunilor dvs. de internet sau din aplicații? Ce riscuri ar putea apărea dacă nu reușiți să faceți acest lucru?
2. Discutați potențialele consecințe ale lăsarii informațiilor dvs. personale accesibile, în cazul în care nu vă deconectați de la o sesiune de internet sau dintr-o aplicație. Cum ar putea fi folosită în mod greșit această informație?

Pentru gestionarea permisiunilor aplicației:

3. Explicați conceptul de permisiuni ale aplicației și relevanța acestora pentru protejarea confidențialității Dvs. Cum afectează permisiunile aplicației securitatea datelor dvs. personale?
4. Imaginați-vă că ați instalat o nouă aplicație pe smartphone. Cum i-ați gestiona permisiunile pentru a vă asigura că confidențialitatea este protejată în timp ce utilizați aplicația?

Pentru o combinație a ambelor:

5. Să presupunem că utilizați un computer public într-o bibliotecă. Cum ați gestiona sesiunile de internet și sesiunile pentru aplicații, cu scopul de a vă proteja informațiile personale și confidențialitatea?

Comportamentul digital securizat și securitatea dispozitivului fizic (MC 4.1.B.4)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Comportamentul digital securizat și securitatea dispozitivelor fizice **Cod: MC 4.1.B.4**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	INTERMEDIAR
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.27, 4.1.28):

Practici de navigare sigură

- Aplicați deprinderile de navigare în siguranță, cum ar fi evitarea site-urilor web suspecte și utilizarea conexiunilor HTTPS, pentru a reduce riscul de malware și furtul de date.

Securitatea dispozitivelor fizice

- Recunoașteți importanța menținerii dispozitivelor în siguranță din punct de vedere fizic, în special în locuri publice, pentru a preveni furtul și accesul neautorizat.

Descriere

MC-ul „Comportamentul digital securizat și securitatea dispozitivelor fizice" este un curs extins și interactiv, menit să formeze obiceiuri digitale sigure și o înțelegere clară a securității dispozitivelor fizice. MC-ul îi îndrumă pe cursanți să adopte și să mențină practici de navigare în siguranță, să aprecieze importanța securității dispozitivelor fizice și să aplice aceste cunoștințe pentru a-și proteja dispozitivele față de de malware, furtul de date și accesul neautorizat.

În prima parte a cursului, accentul este pus pe promovarea comportamentului digital securizat. Participanții vor învăța despre obiceiurile de navigare sigură, cum ar fi utilizarea conexiunilor securizate (HTTPS), evitarea site-urilor web suspicioase și a descărcărilor suspecte, recunoașterea și gestionarea încercărilor de phishing. Ei vor afla, de asemenea, despre potențialele consecințe ale infecțiilor cu programe malware și ale furtului de date, îmbunătățindu-și înțelegerea importanței obiceiurilor de a naviga în siguranță. Această secțiune include exerciții practice și exemple, permițând participanților să aplice ceea ce au învățat în scenarii din lumea reală.

A doua parte a cursului vizează securitatea dispozitivelor fizice. Subliniază importanța menținerii dispozitivelor în siguranță fizică, în special în locuri publice, pentru a preveni furtul și accesul neautorizat. Participanții vor învăța despre diferite modalități de a-și securiza fizic dispozitivele, inclusiv blocarea dispozitivelor, autentificarea biometrică și utilizarea soluțiilor de memorare securizate. Ei vor înțelege, de asemenea, potențialele riscuri de a-și lăsa dispozitivele nesupravegheate sau de a le depozita în locații ușor accesibile.

În plus, cursul evidențiază, de asemenea, interacțiunea dintre comportamentul digital și securitatea fizică și modul în care acestea se pot completa reciproc pentru a crea o abordare extinsă de securitate. Participanții vor învăța cum să balanseze confortul utilizării dispozitivului cu nevoia de securitate și cum micile schimbări în obiceiurile lor le pot îmbunătăți semnificativ poziția generală de securitate.

Concluzionând, la încheierea acestui MC, participanții vor deține o înțelegere aprofundată a comportamentului digital securizat și a securității dispozitivelor fizice, și vor fi capabili să aplice aceste concepte pentru a-și proteja datele și dispozitivele digitale în mod eficient. Programul se aliniază eforturilor Uniunii Europene de a crește inițierea în mediul digitaș și în securitatea digitală, furnizându-I o mulțime de abilități indispensabile oricăriu cetățean implicat digital.

În conformitate cu eforturile Uniunii Europene de a promova inițializarea în mediul digital și securitatea în rândul cetățenilor săi, acest MC oferă un certificat care validează experiența cursantului în practicarea unui comportament digital sigur și în menținerea securității dispozitivelor fizice.

Întrebări

Pentru practici de navigare sigură:

1. Explicați semnificația utilizării conexiunilor HTTPS atunci când navigați pe internet. Cum ajută această practică la reducerea riscului de malware și a furtului de date?
2. Care sunt unele semne de avertizare care v-ar putea indica un site web suspect sau potențial nesigur? Cum v-ați descurca dacă întâlniți un astfel de site?

Pentru securitatea dispozitivelor fizice:

3. De ce este esențial să vă păstrați dispozitivele în siguranță din punct de vedere fizic, în special în locuri publice? Ce riscuri potențiale ar putea apărea dacă lăsați dispozitivul nesupravegheat?
4. Descrieți câțiva pași practici pe care îi puteți urmapentru a asigura securitatea fizică a dispozitivelor dvs., atunci când vă aflați într-un cadru public.

Conștientizarea amenințărilor digitale și gestionarea/management-ul parolelor (MC 4.1.B.5)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Conștientizarea amenințărilor digitale și gestionarea/management-ul parolelor **Cod: MC 4.1.B.5**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	INTERMEDIAR
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.29, 4.1.30):

Riscurile încărcării la stațiile publice

- Identificați riscurile asociate cu utilizarea stațiilor publice de încărcare și potențialul de furt de date sau instalarea de malware.

Gestionarea în siguranță a parolelor

- Implementați un manager de parole pentru a stoca și a genera în siguranță parole complexe pentru diferite conturi online, reducând riscul de încălcare a securității legate de parole.

Descriere

MC-ul „**Conștientizarea amenințărilor digitale și gestionarea/management-ul parolelor**” este un program cuprinzător menit să stimuleze înțelegerea de către participanți a diferitelor amenințări digitale și implicațiile acestora și să îi învețe practicile eficiente de gestionare a parolelor. Acest MC expune pericolele asociate cu stațiile publice de încărcare și subliniază valoarea managerilor de parole pentru securizarea identităților și activelor digitale.

În primul segment al cursului, cursanții vor pătrunde în profunzime în peisajul complex al amenințărilor digitale. Ei vor explora diferite forme de amenințări cibernetice, cum ar fi malware, phishing, ransomware și breșe ale datelor și vor învăța cum să identifice și să răspundă acestor amenințări. Un accent deosebit va fi acordat riscurilor asociate cu utilizarea stațiilor publice de încărcare, care pot expune utilizatorii la „juice jacking” – un atac cibernetic care implică accesul neautorizat și manipularea dispozitivelor prin porturile de încărcare USB. Participanții vor conștientiza importanța utilizării soluțiilor de încărcare sigure, cum ar fi încărcătoare personale sau bănci de alimentare, și vor înțelege riscurile utilizării stațiilor publice de încărcare.

A doua componentă a acestui MC se concentrează pe subiectul crucial al gestionării parolelor. Cursanții vor înțelege importanța creării de parole puternice și unice pentru diferite conturi online și modul în care reutilizarea parolelor poate conduce la breșe de securitate. Cursul evidențiază utilizarea managerilor de parole, care ajută utilizatorii să stocheze și să genereze parole complexe, în siguranță, reducând astfel semnificativ riscul incidentelor de securitate legate de parole. Cursanților li se vor prezenta diverși manageri de parole, învățând cum să le folosească eficient pentru a-și gestiona identitățile digitale.

Pe lângă aceste teme de bază, cursul va furniza îndrumări practice și sfaturi pentru menținerea securității personale online, cum ar fi actualizările regulate de software, autentificarea cu mai mulți factori, obiceiurile de navigare în siguranță și gestionarea în siguranță a link-urilor sau a descărcărilor suspecte.

Până la finalul acestui MC, participanții vor dobândi o înțelegere solidă a amenințărilor digitale și vor avea o mulțime de abilități puternice de gestionare a parolelor; acestea le vor permite să navigheze în lumea digitală cu siguranță și cu încredere sporite. Aliniindu-se cu angajamentul Uniunii Europene de inițializare în lumea digitală și securitate digitală, acest curs urmărește formarea unor abilități absolut necesare oricărei persoane, în era digitală contemporană. În conformitate cu angajamentul Uniunii Europene de a promova inițializarea în

lumea digitală și securitatea digitală, acest MC oferă un certificat al competențlor unui cursant în domeniul recunoașterii amenințărilor digitale și în gestionarea în siguranță a parolelor.

Întrebări

Pentru riscurile încărcării la stațiile publice:

1. Care sunt riscurile potențiale asociate cu utilizarea stațiilor publice de încărcare pentru dispozitivele dvs., cum ar fi smartphone-urile sau laptopurile? Cum ar putea folosirea unei stații publice de încărcare să ducă la furtul de date sau la instalarea de malware?
2. Descrieți câteva măsuri de precauție pe care le puteți lua pentru a vă proteja dispozitivul de riscuri, atunci când utilizați stații publice de încărcare.

Pentru gestionarea sigură a parolelor:

3. Explicați importanța utilizării unui manager de parole pentru a memora și a genera în siguranță parole complexe pentru diferite conturi online. Cum reduce această practică riscul de încălcare a securității legate de parole?
4. Care sunt câteva caracteristici cheie pe care ar trebui să le aibă un manager de parole, pentru a răspunde nevoilor Dvs. de securitate?

Securitatea dispozitivului și întreținerea software-ului (MC 4.1.B.6)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea dispozitivului și întreținerea software-ului **Cod: MC 4.1.B.6**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	INTERMEDIAR
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.31, 4.1.32):

Îmbunătățirea securității dispozitivului

- Implementați caracteristicile de securitate specifice dispozitivului, cum ar fi autentificarea biometrică sau criptarea dispozitivului, pentru a îmbunătăți protecția datelor sensibile.

Conștientizarea întreținerii software-ului

- Înțelegeți riscurile utilizării de software învechit sau neacceptat pe dispozitivele dvs. și importanța actualizării sau înlocuirii unui astfel de software, pentru a menține securitatea.

Descriere

MC-ul „Securitatea dispozitivului și întreținerea software-ului” oferă un curriculum cuprinzător, menit să ofere cursanților o înțelegere aprofundată a securității dispozitivelor și a rolului esențial al întreținerii software-ului pentru a asigura o protecție digitală robustă.

În primul segment al cursului, care se concentrează pe securitatea dispozitivelor, participanții vor aprofunda diferite moduri de a consolida securitatea dispozitivelor. Ei vor afla despre multitudinea de caracteristici de securitate specifice dispozitivelor disponibile în peisajul tehnologic de astăzi, inclusiv autentificarea biometrică, criptarea dispozitivului, mecanismele de pornire securizată, firewall-uri și multe altele. Prin exemple practice, în scenarii reale, cursanții vor descoperi cum să utilizeze aceste caracteristici pentru a îmbunătăți protecția datelor lor sensibile și pentru a evita potențialele amenințări cibernetice. Ei vor dobândi cunoștințele necesare pentru a configura aceste setări în funcție de nevoile lor specifice și de cazurile de utilizare, sporindu-și puterea de a controla securitea digitală.

A doua componentă a cursului se concentrează pe întreținerea software-ului, o fațetă a securității dispozitivelor adesea trecută cu vederea de mulți utilizatori. Participanții vor înțelege riscurile asociate cu utilizarea software-ului învechit sau neacceptat, cum ar fi vulnerabilitatea crescută la atacuri malware, breșe ale datelor și alte amenințări la securitatea cibernetică. Cursul va evidenția importanța actualizărilor regulate a software-ului, a patch-urilor și a înlocuirii la timp a software-ului neacceptat. Cursanți vor învăța să interpreteze jurnalele de actualizare (update logs) și să înțeleagă îmbunătățirile de securitate aduse de fiecare actualizare de software.

În plus, cursul va aborda practicile securizate de instalare și eliminare a software-ului, astfel încât cursanții să înțeleagă cum să adauge și să elimine în siguranță software-ul de pe dispozitivele lor, fără a compromite securitatea.

La finalizarea acestui MC, participanții vor dobândi o înțelegere solidă a tehnicilor de îmbunătățire a securității dispozitivelor și a rolului critic al întreținerii software-ului în menținerea unui mediu digital securizat. Programul se înscrie în angajamentul Uniunii Europene de a promova inițierea în mediul digital și securitatea digitală, făcându-l un plus valoros la setul de abilități digitale ale oricui. Acest curs constituie un avantaj pentru orice persoană sau profesionist care dorește să se asigure că dispozitivele sale sunt cât mai sigure, contribuind la o lume digitală mai sigură și mai sigură.

În concordanță cu angajamentul Uniunii Europene de a consolida inițierea în mediul digital și în securitatea digitală, acest MC oferă o certificare care atestă măiestria unui cursant în menținerea securității dispozitivelor și înțelegerea rolului întreținerii software-ului în securitatea cibernetică.

Întrebări

Pentru îmbunătățirea securității dispozitivului:

1. Explicați importanța implementării caracteristicilor de securitate specifice dispozitivului, cum ar fi autentificarea biometrică sau criptarea dispozitivului. Cum îmbunătățesc aceste caracteristici protecția datelor sensibile?
2. Descrieți pașii pe care i-ați urma pentru a activa autentificarea biometrică (de exemplu, amprenta digitală sau recunoașterea facială) pe smartphone sau pe laptop. Cum vă avantajează acest nivel suplimentar de securitate?

Pentru conștientizarea necesității întreținerii software-ului:

3. Discutați riscurile asociate cu utilizarea unui software învechit sau neacceptat pe dispozitivele Dvs. Cum poate un software învechit să compromită securitatea datelor și a dispozitivului Dvs.?
4. Imaginați-vă că primiți o notificare pentru o actualizare de software pe computer. Cum gestionați această actualizare pentru a vă asigura că securitatea și funcționalitatea dispozitivului Dvs. sunt menținute?

Gestionarea securității dispozitivelor și protejarea confidențialității datelor (MC 4.1.B.7)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Gestionarea securității dispozitivelor și protejarea confidențialității datelor **Cod: MC 4.1.B.7**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	INTERMEDIAR
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.33, 4.1.34 și 4.1.35):

Identificarea activităților suspecte

- Identificați activitățile suspecte de pe dispozitivele dvs., cum ar fi ferestre pop-up neașteptate sau descărcarea neobișnuită a bateriei, care pot indica potențiale programe malware sau breșe de securitate.

Evaluarea securității dispozitivului

- Evaluați caracteristicile de securitate ale diferitelor dispozitive și alegeți cele mai sigure opțiuni în funcție de nevoile dvs. specifice și de cazurile de utilizare.

Gestionarea permisiunilor aplicației

- Recunoașteți importanța revizuirii și a gestionării periodice a permisiunilor aplicațiilor, pentru a limita accesul la datele personale și pentru a proteja confidențialitatea.

Descriere

MC-ul „Gestionarea securității dispozitivelor și protejarea confidențialității" este un curs cuprinzător, adaptat pentru a oferi indivizilor cunoștințele și abilitățile necesare pentru a naviga în siguranță în lumea digitală. Se concentrează pe trei domenii fundamentale: identificarea potențialelor amenințări de securitate, evaluarea caracteristicilor de securitate a dispozitivului și gestionarea eficientă a permisiunilor aplicației.

Prima parte a cursului vizează identificarea potențialelor amenințări de securitate. Participanții vor învăța despre toată gama de amenințări de securitate cibernetică care există în lumea digitală, de la malware și viruși până la încercări de phishing și atacuri ransomware. Ei vor înțelege cum funcționează aceste amenințări și potenţialele daune pe care le pot provoca. Stăpânind aceste cunoștințe, cursanții vor fi mai bine pregătiți să recunoască aceste amenințări atunci când le întâlnesc și să reacționeze în mod corespunzător pentru a atenua potențialele daune.

A doua componentă a cursului vizează o cunoaștere în profunzime a caracteristicilor de securitate a dispozitivelor. Pe măsură ce ne bazăm din ce în ce mai mult pe dispozitivele digitale pentru diverse sarcini personale și profesionale, înțelegerea modului de a menține aceste dispozitive în siguranță devine primordială. Participanții vor afla despre diferitele caracteristici de securitate ale dispozitivului și despre cum să le evalueze eficacitatea. Ei vor învăța despre criptare, autentificare biometrică, procese securizate de pornire și multe altele. Pe aza acestor cunoștințe, cursanții vor putea lua decizii în cunoștință de cauză atunci când aleg dispozitivele și își pot stabili configurațiile de securitate.

Segmentul final al cursului se concentrează pe gestionarea eficientă a permisiunilor aplicației. În era aplicațiilor mobile, este important să înțelegem accesul pe care aceste aplicații îl au la datele personale. Cursul va ghida cursanții prin procesul de revizuire și gestionare a permisiunilor aplicațiilor, limitând accesul inutil la datele personale, și înțelegerea riscurilor potențiale ale aplicațiilor prea permisive.

La finalizarea acestui MC, participanții vor deține o numeroase abilități care nu numai că le îmbunătățesc propria siguranță digitală, dar pot fi, de asemenea, împărtășite în comunitățile lor, pentru a promova un mediu digital mai sigur pentru toți. Cursul se înscrie în angajamentul Uniunii Europene de a consolida inițierea în mediul digital și securitatea digitală, constituind un plus esențial la setul de competențe al cetățeanului digital modern și responsabil.

Aliniat cu misiunea Uniunii Europene de a îmbunătăți cunoștințele și securitatea digitală, acest MC oferă o certificare a competenței unui cursant în gestionarea securității dispozitivelor și păstrarea confidențialității.

Întrebări

Pentru identificarea activităților suspecte:

1. Care sunt câteva dintre semnele activităților suspecte pe dispozitivul dvs. care pot indica potențiale malware sau încălcări de securitate?
2. Descrieți o situație în care ați întâlnit o fereastră pop-up neașteptată pe dispozitiv. Cum ați gestionat situația pentru a asigura securitatea dispozitivului dvs.?

Pentru evaluarea securității dispozitivului:

3. Când evaluați caracteristicile de securitate ale diferitelor dispozitive, care sunt câțiva factori pe care i-ați lua în considerare pentru a determina care dispozitiv este cel mai sigur pentru nevoile dvs. specifice și cazurile de utilizare?
4. Comparați caracteristicile de securitate ale unui smartphone și ale unei tablete. Pe baza evaluării dvs., ce dispozitiv ați alege pentru utilizarea în siguranță și de ce?

Pentru gestionarea permisiunilor aplicației:

5. De ce este esențial să revizuiți și să gestionați în mod regulat permisiunile aplicațiilor pe dispozitivele dvs.? Cum poate această practică să limiteze accesul la datele personale și să vă protejeze confidențialitatea?
6. Imaginați-vă că ați instalat o nouă aplicație pe smartphone. Cum ați analiza și gestiona permisiunile acesteia pentru a vă proteja confidențialitatea?

Securitatea lucrului la distanță (remote working) și securitatea arhivării digitale (MC 4.1.B.8)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea lucrului la distanță și securitatea arhivării digitale **Cod: MC 4.1.B.8**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	INTERMEDIAR
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.36, 4.1.37 și 4.1.38):

Securitatea lucrului la distanță (remote working)

- Extindeți măsurile de securitate a dispozitivului dvs. pentru a include medii de lucru la distanță, asigurând protecția datelor și securizați canalele de comunicație.

Facilitarea conștientizării securității

- Facilitați conștientizarea securității în rândul colegilor sau a membrilor familiei dvs., educându-i despre cele mai bune practici pentru securitatea dispozitivelor și despre comportamentul online, în siguranță.

Conștientizarea securității arhivării

- Recunoașteți riscurile potențiale asociate cu deschiderea arhivelor de tip zip sau rar provenite din surse necunoscute sau lipsite de încredere.

Descriere

MC-ul „Securitatea lucrului la distanţă şi securitatea arhivării digitale” constituie un curs abordează în profunzime securizarea mediilor de lucru la distanță și promovează inițierea digitală în sfera personală și profesională. Programul prezintă, de asemenea, riscurile potențiale asociate cu manipularea arhivelor care provin din surse incerte sau necunoscute.

Pe măsură ce trecem într-o eră care depinde din ce în ce mai mult de lucrul la distanță și de comunicarea digitală, acest curs își propune să ajute cursanții să se adapteze la aceste schimbări în mod sigur și responsabil. Participanții vor obține o perspectivă asupra diferitelor provocări de securitate reprezentate de mediile de lucru la distanță, inclusiv confidențialitatea datelor, rețelele nesecurizate, atacurile de phishing și alte potențiale amenințări la adresa securității cibernetice. Ei vor deprinde, de asemenea, strategii eficiente pentru a-și securiza spațiile de lucru virtuale, cum ar fi utilizarea canalelor securiate de comunicație, criptarea puternică, autentificarea cu mai mulți factori și obiceiurile digitale sigure.

Un aspect cheie al acestui curs este facilitarea și promovarea inițierii în mediile digitale. Participanții vor învăța cum să-și ghideze colegii sau membrii familiei spre înțelegerea și adoptarea celor mai bune practici pentru securitatea dispozitivelor și pentru a dobândi un comportament online sigur. MC-ul include educația privind igiena parolelor, obiceiurile de navigare în siguranță, permisiunile aplicațiilor și recunoașterea potențialelor tentative de phishing sau de escrocherie. Prin promovarea inițierii în mediile digitale, participanții pot contribui la crearea de comunități digitale mai sigure la locul de muncă, acasă și nu numai.

Cursul explorează, de asemenea, riscurile asociate cu deschiderea arhivelor, cum ar fi fișierele zip sau rar, care provin din surse nesigure sau necunoscute. Participanții vor afla despre potențialele amenințări pe care le pot prezenta aceste fișiere, inclusiv malware, ransomware sau alte forme de software dăunător. Cursul va ghida cursanții cu privire la cele mai sigure practici de manipulare a acestor fișiere, cum ar fi verificarea sursei, utilizarea software-ului de protecție și înțelegerea importanței backup-urilor regulate ale sistemului.

După finalizarea acestui MC, cursanții vor fi mai bine pregătiți să-și securizeze mediile de lucru la distanță, dar și să îi educe pe alții în privința practicilor digitale sigure și în tratarea cât mai eficientă a potențialelor amenințări digitale. Acest MC se aliniază cu angajamentul Uniunii Europene de a îmbunătăți inițierea în mediile digitale și în securitatea digitală, constituind o investiție valoroasă în educația oricărui cetățean digital.

În conformitate cu angajamentul Uniunii Europene de a îmbunătăți inițierea în mediile digitale și în securitatea digitală în rândul cetățenilor săi, acest MC certifică competențele cursantului în gestionarea securității lucrului la și inițierea în mediile digitale.

Întrebări

Pentru securitatea lucrului la distanță:

1. Explicați cum puteți extinde măsurile de securitate a dispozitivului, pentru a asigura protecția datelor, și securizați-vă canalele de comunicație în timp ce lucrați la distanță. Ce măsuri de precauție suplimentare ați lua în comparație cu situația în care lucrați la birou, într-un mediu securizat?
2. Descrieți o situație în care măsurile de securitate pentru lucrul la distanță au fost cruciale pentru protejarea datelor sensibile sau pentru prevenirea unei breșe de securitate.

Pentru facilitarea conștientizării securității:

3. Ca persoană conștientă de securitate, cum ați facilita conștientizarea securității în rândul colegilor sau ai membrilor familiei dvs.? Pe ce subiecte și pe care practici v-ați concentra în timpul sesiunilor de conștientizare?
4. Care sunt câteva strategii pe care le puteți folosi pentru a încuraja o cultură conștientă de securitate în rândul colegilor sau ai membrilor familiei dvs.?

Pentru conștientizarea securității arhivelor:

5. Discutați riscurile potențiale asociate cu deschiderea arhivelor zip sau rar care provin din surse necunoscute sau care nu sunt de încredere. Cum pot fi folosite astfel de arhive pentru a răspândi programe malware sau tentative de phishing?
6. Imaginați-vă că primiți un fișier arhivă .zip, de la o adresă de e-mail necunoscută. Ce măsuri de precauție ați lua înainte de a deschide arhiva?

Securitatea dispozitivelor portabile și siguranța descărcărilor aplicațiilor (MC 4.1.B.9)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea dispozitivelor portabile și siguranța descărcărilor aplicațiilor **Cod: MC 4.1.B.9**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	INTERMEDIAR
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.39, 4.1.40):

Siguranța dispozitivelor portabile și siguranța mediului digital

- Dezvoltați obiceiul de a vă asigura de siguranța suporturilor hardware portabile și a dispozitivelor șterse, evitând să aveți încredere în dispozitivele sau conținuturile media nesigure.

Practici de descărcare sigură a aplicațiilor

- Explicați riscurile descărcării de aplicații care provin din surse necunoscute și importanța utilizării site-urilor sau a magazinelor oficiale de aplicații.

Descriere

MC-ul „**Securitatea dispozitivelor portabile și siguranța descărcărilor aplicațiilor**” își propune să cultive obiceiuri adecvate siguranței în ceea ce privește dispozitivele portabile și mediile digitale și să ofere o înțelegere a practicilor sigure de descărcare a aplicațiilor.

Prin acest curs, cursanții vor dobândi cunoștințele necesare pentru a diferenția hardware-ul portabil sigur de cel nesigur, devenind mai precauți în manipularea unor astfel de dispozitive. Ei vor dezvolta o înțelegere a riscurilor asociate cu dispozitivele nesigure sau conținutul media neverificat, conștientizând importanța siguranței dispozitivelor și potențialele amenințări la adresa securității lor digitale.

În plus, acest MC pune accent pe protocoalele de siguranță aplicate la descărcarea aplicațiilor. Cursanții vor înțelege riscurile asociate descărcării aplicațiilor care provin din surse necunoscute, inclusiv potențiale amenințări malware, furtul de date și alte vulnerabilități de securitate cibernetică. Cursul subliniază importanța utilizării magazinelor și a site-urilor oficiale de aplicații, care respectă standardele stricte de securitate și procesele de verificare a aplicațiilor.

În conformitate cu angajamentul Uniunii Europene de a îmbunătăți cunoștințele în inițierea în mediile digitale și securitatea digitală, acest MC oferă o dovadă certificată a competenței unui cursant în gestionarea securității dispozitivelor portabile și a practicilor de descărcare în siguranță a aplicațiilor. Cursanții care urmează acest curs vor fi mai bine pregătiți pentru a-și proteja dispozitivele digitale și pentru a naviga în siguranță în lumea digitală.

Acest MC se înscrie în angajamentul Uniunii Europene de a îmbunătăți inițierea în mediile digitale și în securitatea digitală și certifică competența cursantului în gestionarea securității dispozitivelor portabile și practicarea descărcării în siguranță a aplicațiilor.

Întrebări

Siguranța dispozitivelor portabile și a suporturilor media:

1. De ce este important să se asigure siguranța suporturilor hardware portabile și a dispozitivelor șterse? Ce riscuri pot apărea dacă aveți încredere în dispozitive sau conținut media nesigure?
2. Descrieți câteva măsuri de precauție pe care le puteți lua pentru a asigura siguranța suporturilor

hardware portabile, cum ar fi unitățile USB sau hard disk-urile externe, împotriva riscurilor potențiale și a pierderii de date.

Practici de descărcare a aplicațiilor în siguranță:

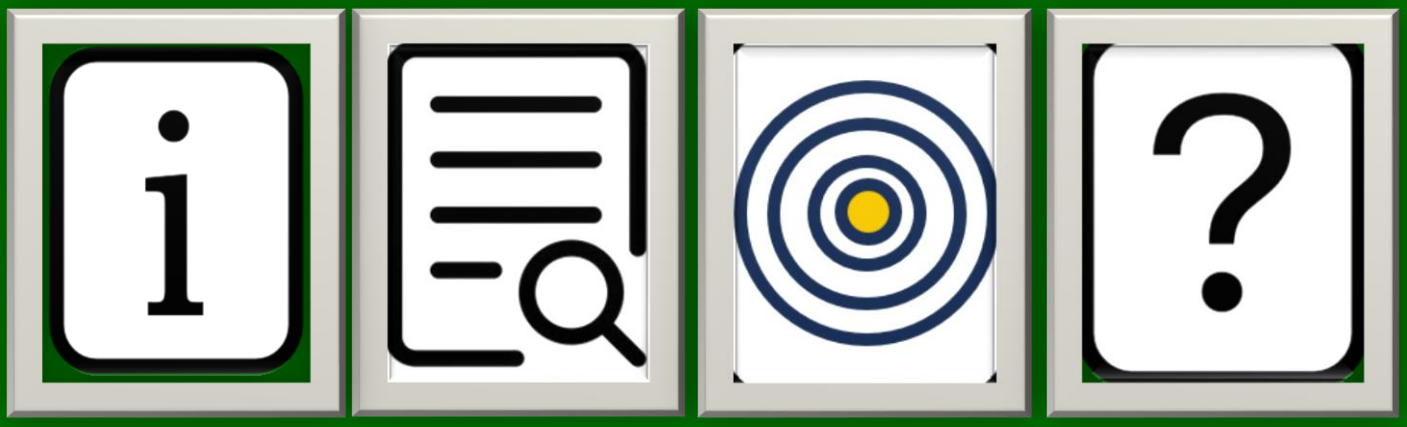
3. Discutați potențialele riscuri asociate cu descărcarea de aplicații din surse necunoscute. Cum pot astfel de practici să compromită securitatea dispozitivului și a datelor dvs.?
4. Explicați importanța utilizării magazinelor și a site-urilor oficiale de aplicații pentru a descărca aplicații. Cum contribuie această practică la asigurarea siguranței și a securității aplicațiilor pe care le instalați pe dispozitiv?

Siguranța dispozitivelor portabile și a suporturilor media și practici de descărcare a aplicațiilor în siguranță:

5. Imaginați-vă că doriți să transferați câteva fișiere, prietenului dvs., folosind o unitate USB portabilă. Cum ați asigura siguranța unității USB și a conținutului acesteia înainte de a o partaja cu prietenul dvs.? În plus, cum ați asigura siguranța dispozitivului dvs. atunci când conectați unitatea USB?

NIVELUL AVANSAT

(Nivelul 5 și Nivelul 6)



Securitatea dispozitivelor personale și cele mai bune practici (MC 4.1.C.1)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea dispozitivelor personale și cele mai bune practici **Cod: MC 4.1.C.1**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	AVANSAT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.41, 4.1.42):

- Evaluați și comparați diferite soluții software de securitate, cum ar fi programele antivirus și firewall-urile, pentru a le selecta pe cele mai eficiente pentru dispozitivul și nevoile Dvs. specifice.
- Evitați utilizarea de informații sensibile sau ușor de urmărit în parole, pentru a le spori puterea și securitatea.

Descriere

MC-ul „**Securitatea dispozitivelor personale și cele mai bune practici**" este un program complet, teoretic și practic, conceput pentru a oferi cursanților cunoștințele și abilitățile pentru a-și proteja dispozitivele și datele personale într-o lume din ce în ce mai interconectată. Avizat de către Comisia Europeană, acest program oferă participanților instrumente și tehnici practice pentru a evalua și selecta cele mai eficiente soluții software de securitate, cum ar fi programe antivirus și firewall-uri, adaptate la dispozitivul și nevoile lor specifice de securitate.

În primul modul, cursanții studiază în profunzime lumea software-ului de securitate, explorând diverse opțiuni disponibile pe piață. Ei învață să evalueze caracteristicile, capacitățile și performanța diferitelor soluții antivirus și firewall pentru a o identifica pe cea mai potrivită pentru dispozitivele lor. Prin simulări și exerciții din lumea reală, participanții dobândesc experiență practică în implementarea și configurarea eficientă a software-ului de securitate.

Al doilea modul se concentrează pe gestionarea parolelor, un aspect critic al securității dispozitivelor personale. Cursanții sunt informați cu privire la vulnerabilitățile asociate cu utilizarea informațiilor sensibile sau ușor de urmărit în parole. Înțelegând principiile creării de parole puternice, aceștia sunt capabili să aplice cele mai bune practici și să utilizeze managerii de parole pentru a stoca și gestiona în siguranță parole complexe pentru diferite conturi online.

Pe parcursul MC-ului, cursanților li se vor prezenta studii de caz din lumea reală și scenarii de securitate cibernetică. Astfel, participanții își vor aplica cunoștințele nou dobândite în situații practice. Ei vor analiza critic potențialele riscuri de securitate și vor elabora strategii proactive pentru a atenua amenințările în mod eficient.

După finalizarea cu succes a Micro Credentialului „Securitatea dispozitivelor personale și cele mai bune practici", participanții vor câștiga un certificat recunoscut de Comisia Europeană; certificatul confirmă că au competențe în securitatea dispozitivului și gestionarea parolelor. Deținând aceste competențe, cursanții vor fi bine pregătiți pentru a-și proteja și datele personale de amenințările cibernetice, contribuind astfel la un mediu digital mai sigur pentru ei și cei din jurul lor.

Întrebări

1. Întrebare despre evaluarea soluțiilor software de securitate: „Doriți să selectați un software de securitate pentru laptopul pe care îl utilizați în principal pentru activități bancare online și pentru activități legate de muncă. Subliniați criteriile pe care le-ați lua în considerare atunci când evaluați

diferite programe antivirus și firewall-uri. Ce factori ar fi esențiali pentru a asigura cea mai eficientă protecție pentru dispozitivul Dvs. În acest caz?"

2. Întrebare despre promovarea securității parolelor: „Discutați despre cele mai bune practici de securitate a parolei cu colegii dvs. și unul dintre ei sugerează utilizarea unor informații ușor de urmărit, cum ar fi datele de naștere sau cuvinte comune, în parole. Cum ați argumenta evitarea utilizării acestor informații și ce practici referitoare la parole ați folosi? Oferiți motive și exemple pentru a vă susține răspunsurile."
3. Întrebare bazată pe scenarii privind implementarea recomandărilor privind parolele: „Imaginați-vă că aveți mai multe conturi online pe site-uri web diferite și că utilizați parole slabe și repetitive. După ce ați aflat despre importanța parolelor puternice, decideți să vă îmbunătățiți securitatea parolei. Descrieți pașii pe care îi urmați pentru a spori puterea și securitatea parolelor dvs. Cum v-ați asigura că vă amintiți aceste parole complexe, menținând în același timp un nivel ridicat de securitate?

Securitatea parolelor și cele mai bune practici (MC 4.1.C.2)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea parolelor și cele mai bune practici **Cod: MC 4.1.C.2**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	AVANSAT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.43, 4.1.44 și 4.1.45):

- Înțelegeți importanța evitării cuvintelor din dicționar sau a modelelor comune în parole, pentru a preveni atacurile de tip “brute-force”.
- Recunoașteți riscul utilizării aceleiași parole pentru mai multe conturi și importanța utilizării unei parole unice pentru fiecare cont.
- Recunoașteți importanța actualizării periodice a parolelor și a evitați reutilizarea parolelor vechi.

Descriere

MC-ul „**Securitatea parolelor și cele mai bune practici**” este un program cuprinzător, specializat, creat cu meticulozitate, pentru a oferi cursanților cunoștințe și abilități avansate în protejarea identității digitale prin practicile de a crea parole robuste. Acest program, avizat de prestigioasa Comisie Europeană, explorează în profunzime subiectul securității cu ajutorul parolelor, furnizând participanților expertiza necesară pentru a crea, pentru a gestiona și a menține parole puternice și unice, care să le întărească prezența online împotriva potențialelor amenințări.

În primul modul, cursanții pornesc într-o călătorie care explorează vulnerabilitățile asociate cu utilizarea cuvintelor din dicționar sau a modelelor comune în parole. Prin studii de caz ilustrative și exemple din lumea reală, participanții vor înțelege în profunzime modul în care astfel de practici fac conturile lor susceptibile la atacuri de tip “brute force”. Având aceste cunoștințe, participanții vor fi îndrumați să folosească la strategii alternative și cele mai bune practici pentru a dezvolta parole foarte sigure, care descurajează accesul neautorizat și împiedică încercările rău intenționate.

Al doilea modul analizează riscurile și consecințele critice ale utilizării aceleiași parole pentru mai multe conturi. Cursanții sunt expuși la scenarii revelatoare care evidențiază efectul de domino al reutilizării parolelor, în care un singur cont compromis poate conduce la o serie de încălcări de securitate în cascadă. Prin exerciții interactive, cursanții înțeleg importanța primordială a adoptării parolelor unice pentru fiecare cont, pentru a-și proteja activele digitale și pentru a menține o apărare fortificată împotriva adversarilor cibernetici.

În modulul final, cursanții sunt introduși în procesul extrem de important al actualizării regulate a parolelor și a evitării reutilizării parolelor vechi. Ei înțeleg modul în care aceste practici contribuie la o securitate în continuă evoluție, întărindu-și fortărețele digitale împotriva amenințărilor cibernetice emergente. Angajându-se în activități practice și în simulări, participanții internalizează principiile managementului eficient al parolelor, sporindu-și astfel pregătirea de a se adapta la provocările de securitate, aflate într-o continuă evoluție.

Pe parcursul MC-ului, cursanții lucrează într-un mediu de învățare dinamic și interactiv, facilitat de experți din industrie și de profesioniști experimentați în securitatea cibernetică.

Cursanții vor fi implicați în exerciții practice și simulări din viața reală, permițându-le să-și aplice cu încredere noile cunoștințe, în interacțiunile digitale de zi cu zi.

După finalizarea cu succes a MC-ului „**Securitatea parolelor și cele mai bune practici**”, participanții nu numai că vor dobândi o certificare prestigioasă din partea Comisiei Europene, ci și vor deveni agenți cheie ai schimbării în promovarea celor mai bune practici de securitate a parolelor. Înarmați cu expertiză avansată,

aceștia vor servi ca purtători de torțe, diseminându-și cunoștințele și promovând o cultură a securității digitale sporite, în comunitățile și organizațiile lor.

În concluzie, MC-ul „**Securitatea parolelor și cele mai bune practici**” este un program transformator care, dincolo de teorie, înzestrează cursanții cu abilitățile practice necesare pentru a-și consolida identitățile digitale și pentru a-și proteja datele personale, împotriva amenințărilor cibernetice, aflate în continuă dezvoltare. MC-ul este recomandat atât profesioniștilor care doresc să-și îmbunătățească abilitățile în domeniul securității cibernetice, cât și utilizatorilor obișnuiți, care doresc să se protejeze într-un mod cât mai competent.

Întrebări

1. Întrebare despre complexitatea parolelor: „De ce este esențial să evitați utilizarea cuvintelor din dicționar sau a modelelor/tiparelor comune în alegerea parolelor? Cum îmbunătățește utilizarea unor astfel de practici securitatea conturilor dumneavoastră și cum previne atacurile de tip “brute force”? Furnizați exemple pentru a vă susține răspunsul.”
2. Întrebare bazată pe scenariul privind reutilizarea parolei: „Ați folosit aceeași parolă atât pentru conturile dvs. de e-mail, cât și pentru conturile bancare online. Care sunt riscurile potențiale asociate cu această practică? Cum puteți folosi parole unice pentru fiecare cont, astfel încât riscurile să fie atenuate și să vă sporiți toată securitatea?"
3. Întrebare despre frecvența actualizării parolelor: „Explicați importanța actualizării periodice a parolelor. Cum contribuie această practică la menținerea unei securități puternice a contului, de-a lungul timpului? Ce factori ar trebui să luați în considerare atunci când decideți cât de des să vă actualizați parolele?"
4. Întrebare bazată pe scenariu privind schimbarea parolei: „Să presupunem că nu ți-ai schimbat parolele pentru conturile pe care le deții pe rețele sociale de peste un an. Ce riscuri ar putea apărea din lipsa de actualizare a parolelor? Descrieți pașii pe care i-ați urma pentru a actualiza aceste parole și asigurați-vă că acestea sunt puternice și unice.”
5. Întrebare despre atenuarea compromiterii contului: „Bănuiți că parola dvs. pentru un cont de cumpărături online a fost compromisă. Cum ar ajuta utilizarea parolelor unice pentru fiecare cont la atenuarea potențialor consecințe ale acestei breșe de securitate? Ce pași suplimentari ați lua pentru a vă proteja celelalte conturi?"
6. Întrebare despre strategiile de gestionare a parolelor: „Cum pot managerii de parole să ajute la implementarea parolelor unice și sigure pentru fiecare cont? Care sunt potențialele avantaje și dezavantaje ale utilizării managerilor de parole pentru gestionarea parolelor?”
7. Întrebare bazată pe scenariul privind reutilizarea parolei vechi: „Imaginați-vă că ați folosit accidental o parolă veche dintr-un cont anterior, pentru un nou serviciu de abonament online. Cu ce riscuri vă puteți confrunta din cauza acestei neglijențe? Cum ați remedia situația și cum preveniți apariția similară în viitor?"

Managementul securității dispozitivelor și eficiența datelor (MC 4.1.C.3)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul securizății dispozitivelor și eficiența datelor **Cod: MC 4.1.C.3**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	AVANSAT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.46, 4.1.47):

- Utilizați cu măiestrie un program de compresie pe dispozitivul Dvs., pentru a reduce volumul de date, asigurând atfel memorarea și transmisia eficiente.
- Fiți capabil să configurați setările dispozitivului pentru a se bloca automat sau a se deconecta după o perioadă de inactivitate, pentru a preveni accesul neautorizat.

Descriere

MC-ul „**Managementul securizării dispozitivelor și eficiența datelor**” este un program de ultimă oră, cuprinzător, conceput cu mare atenție, pentru a oferi cursanților abilitățile esențiale în gestionarea în siguranță a dispozitivelor și în optimizarea eficienței datelor. Avizat de prestigioasa Comisie Europeană, acest program oferă participanților cunoștințele necesare pentru a naviga cu încredere în peisajul digital, asigurându-se că dispozitivele lor sunt rezistente împotriva potențialelor amenințări de securitate și eficiente în gestionarea datelor.

În primul modul, cursanții se lansează într-o explorare captivantă a compresiei datelor. Ghidați de către instructori experți, participanții dobândesc experiență practică folosind programe de compresie pe dispozitivele lor, pentru a reduce eficient volumul de date, fără a compromite calitatea acestora. Prin exerciții practice, participanții învață să optimizeze spațiul de memorare și să îmbunătățească transmisia de date, simplificându-și astfel fluxurile digitale de lucru și făcând dispozitivele lor mai agile și mai receptive. Fie că este vorba de gestionarea fișierelor mari, de îmbunătățirea partajării datelor sau de optimizarea capacității de memorare, cursanții vor dobândi priceperea de a profita la maximum de capabilitățile de manipulare a datelor de pe dispozitivele lor.

Al doilea modul analizează aspectul primordial al securității dispozitivului prin mecanisme automate de blocare și deconectare. Cursanții capătă abilități în configurarea setărilor dispozitivului, pentru a implementa funcții de blocare sau deconectare automată, după perioade de inactivitate.

Înarmați cu aceste cunoștințe, cursanții își protejează în mod eficient dispozitivele împotriva accesului neautorizat. Implementarea cu pricepere a acestor măsuri va permite cursanților să păstreze controlul asupra punctelor de acces ale dispozitivelor lor, și să promoveze un mediu digital rezistent și sigur.

Pe parcursul acestui MC, cursanții vor fi angajați în simulări interactive și scenarii din viața reală, care le vor permite să aplice cunoștințele nou dobândite în situații practice. Întâmpinând și rezolvând provocări relevante pentru experiențele lor digitale de zi cu zi, participanții dobândesc abilități neprețuite pentru a aborda problemele de gestionare a dispozitivelor din lumea reală și problemele despre eficiența datelor.

După finalizarea cu succes a MC-ului „Managementul securizării dispozitivelor și eficiența datelor”, participanții obțin o certificare prestigioasă din partea Comisiei Europene, recunoscându-li-se competența în securizarea dispozitivelelor și optimizarea gestionării datelor. Înarmați cu aceste abilități avansate, cursanții sunt pregătiți să pășească cu încredere în peisajul digital aflat în continuă evoluție, contribuind la un ecosistem digital mai sigur, mai productiv și mai plin de resurse.

Pe scurt, MC-ul „Managementul securizării dispozitivelor și eficiența datelor” este un program transformator, care îmbină practicile esențiale de securitate cu tehnicile de optimizare a datelor. Conceput pentru persoanele care doresc să-și îmbunătățească competențele digitale, acest program formează cursanții să devină navigatori pricepuți în peisajul digital, asigurându-se că dispozitivele lor rămân în siguranță și utilizarea datelor este maximizată la întregul său potențial.

Întrebări

1. Evaluarea aptitudinilor practice privind comprimarea datelor: „Folosind un program de compresie la alegere, demonstrați cum ați comprima un fișier video mare, fără a-i compromite calitatea. Explicați pașii pe care i-ați urma și beneficiile așteptate ale comprimării fișierului în ceea ce privește reducerea volumului de date și memorarea eficientă.”
2. Întrebare bazată pe scenariul despre setările de blocare a dispozitivului: „Imaginați-vă că folosiți frecvent dispozitivul Dvs. în locuri publice și că sunteți îngrijorat de accesul neautorizat atunci când dispozitivul este lăsat nesupravegheat. Cum ați configura cât mai bine setările dispozitivului pentru a se bloca automat după o perioadă de inactivitate? Descrieți pașii pe care le-ați urma și potențialele beneficii de securitate ale implementării acestei facilități.”
3. Întrebare de gândire critică privind eficiența datelor: „Să presupunem că aveți spațiu de memorare limitat pe dispozitivul Dvs. și trebuie să gestionați diverse fișiere, inclusiv documente, fotografii și muzică. Cum ar ajuta compresia de date și setările dispozitivului pentru blocarea/deconectarea automată, pentru a optimiza eficiența datelor și a vă îmbunătăți experiența digitală globală?

Siguranța digitală și manipularea securizată a datelor (MC 4.1.C.4)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Siguranța digitală și manipularea securizată a datelor: MC 4.1.C.4
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: 101087628
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	AVANSAT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.48, 4.1.49 și 4.1.50):

- Cunoașteți riscurile utilizării funcțiilor de conectare automată pe site-urile web sau în aplicațiile care memorează informații personale?
- Utilizați metode securizate de transfer ale fișierelor, cum ar fi SFTP sau memorarea securizată în cloud, pentru a transfera fișiere sensibile între dispozitive.
- Recunoașteți riscurile potențiale ale utilizării de software sau de aplicații necunoscute pe dispozitivele dvs.

Descriere

MC-ul „**Siguranța digitală și manipularea securizată a datelor**” este un program cuprinzător, de perspectivă, conceput pentru a oferi cursanților cunoștințe și abilități esențiale pentru a naviga în peisajul digital în siguranță și pentru a proteja datele sensibile. Avizat de către prestigioasa Comisie Europeană, acest program oferă participanților cunoștințele necesare pentru ca aceștia să poată lua decizii în cunoștință de cauză, să poată susține practici sigure și să-ți protejează informațiile digitale în mod eficient.

În primul modul, cursanții vor înțelege în profunzime riscurile asociate funcțiilor de conectare automată. Prin exemple din lumea reală și studii de caz, participanții vor devini conștienți de potențialele implicații ale permisiunilor site-urilor web sau ale aplicațiilor să memoreze automat informații personale. Având aceste cunoștințe, cursanții sunt pregătiți pentru a lua decizii conștiente cu privire la activarea sau dezactivarea unor astfel de funcții, pentru a-și proteja datele sensibile și pentru a-și păstra confidențialitatea digitală.

Al doilea modul se concentrează pe metodele securizate ale transferelor de fișiere. Participanții sunt familiarizați cu practicile standard din industrie, cum ar fi SFTP (Secure File Transfer Protocol) și memorarea securizată în cloud. Prin demonstrații practice și exerciții interactive, cursanții înțeleg importanța utilizării acestor metode pentru a schimba de fișiere sensibile, în siguranță, între dispozitive. Susținând transferul securizat de fișiere, participanții își întăresc capacitatea de a proteja informațiile confidențiale în timpul comunicării digitale, reducând riscul accesului neautorizat sau al breșelor datelor.

Modulul final pune în lumină potențialele riscuri ale utilizării de software sau de aplicații necunoscute pe dispozitivele personale. Participanții explorează pericolele asociate cu descărcarea și rularea software-ului din surse neverificate. Recunoscând aceste riscuri, cursanții își sporesc vigilența digitală și sunt precauți în timp ce evaluează și utilizează noi aplicații, protejându-și dispozitivele de potențialele malware și vulnerabilități de securitate.

Pe parcursul MC-ului, cursanții vor fi angajați în activități practice, simulări și discuții interactive, internalizându-și, astfel, cele mai bune practici în domeniul siguranței digitale și în domeniul gestionării securizate a datelor. Finalizarea cu succes a programului nu numai că le aduce cursanților o certificare prestigioasă din partea Comisiei Europene, dar le conferă și puterea de a face alegeri responsabile și informate în interacțiunile lor digitale, contribuind la un mediu digital mai sigur pentru ei și pentru ceilalți.

Pe scurt, MC-ul „Siguranța digitală și manipularea securizată a datelor” este un program transformator, care oferă cursanților cunoștințele și abilitățile necesare pentru a naviga în peisajul digital cu încredere. Participanții

vor aplica practici sigure, vor proteja datele sensibile și vor promova siguranța digitală în diverse contexte, având un impact pozitiv în sferele lor personale și profesionale.

Întrebări

1. Întrebare despre conștientizarea riscurilor privind funcțiile de conectare automată: „Explicați potențialele riscuri ale utilizării funcțiilor de conectare automată la site-uri web sau la aplicații care stochează informații personale. Cum vă pot compromite aceste facilități confidențialitatea și securitatea digitală? Furnizați exemple de scenarii în care dezactivarea conectării automate ar fi recomandabilă. "
2. Întrebare de susținere și de justificare privind metodele securizate de transfer de fișiere: „Ați fost însărcinat să susțineți utilizarea metodelor securizate de transfer de fișiere la locul de muncă sau în comunitate. Scrieți o declarație persuasivă care să sublinieze importanța utilizării unor metode precum SFTP sau memorarea securizată în cloud, pentru a face schimb de informații sensibile/fișiere între dispozitive. Enumerați beneficiile și avantajele specifice ale acestor metode de transfer sigur față de opțiunile tradiționale de transfer de fișiere.”
3. Întrebare de gândire critică privind riscurile software: „Găsiți în mediul digital o nouă aplicație software, dintr-o sursă necunoscută, care pretinde că oferă caracteristici și funcționalități unice. Cum ați aborda decizia de a instala și utiliza acest software pe dispozitivul dvs.? Discutați riscurile potențiale implicate în utilizarea software-ului necunoscut și descrieți pașii pe care i-ați urma pentru a evalua legitimitatea aplicației și securitatea, înainte de a continua.”

Securitatea dispozitivului și protecția datelor (MC 4.1.C.5)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea dipozitivului și protecția datelor: MC 4.1.C.6
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: 101087628
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	AVANSAT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.51, 4.1.52):

- Recunoașteți importanța dezactivării Bluetooth-ului pe dispozitivele Dvs., atunci când nu sunt utilizate.
- Fiți capabiși să efectuați scanări de viruși pe dispozitivele de memorare externe.

Descriere

MC-ul „**Securitatea dipozitivului și protecția datelor**” este un program concentrat și practic, menit să doteze cursanții cu abilități esențiale pentru a-și proteja dispozitivele și datele față de potențiale amenințări de securitate. Avizat de prestigioasa Comisie Europeană, acest program oferă participanților cunoștințele și capacitățile de a-și consolida dispozitivele împotriva vulnerabilităților legate de Bluetooth și de a efectua scanări de viruși esențiale pe dispozitivele de memorare externe.

În primul modul, cursanții explorează riscurile asociate conectivității prin Bluetooth atunci când sunt active pe dispozitivele lor, mai ales atunci când nu sunt utilizate. Prin exemple din lumea reală și studii de caz, participanții devin conștienți de potențialele vulnerabilități de securitate care pot apărea din cauza conexiunilor Bluetooth. Ei înțeleg importanța dezactivării Bluetooth atunci când aceasta nu este utilizat în mod activ, reducând astfel riscul accesului neautorizat sau încălcării datelor.

Al doilea modul se concentrează pe practica critică de a efectua scanări de viruși pe dispozitivele de memorare externe. Participanții obțin informații despre riscurile potențiale asociate cu utilizarea mediilor de memorare externe, cum ar fi unități USB sau hard disk-uri externe și învață cum virușii și programele malware pot fi transferate din greșeală pe dispozitivele lor prin intermediul dispozitivelor de memorare infectate. Prin dobândirea de abilități practice în efectuarea de scanări de viruși pe medii externe, cursanții pot detecta și atenua în mod proactiv amenințările, asigurându-se că dispozitivele și datele lor rămân în siguranță.

Pe parcursul MC-ului, cursanții se angajează în activități practice, simulări și exerciții practice pentru a-și consolida înțelegerea despre securitatea dispozitivului și protecția datelor. Aceștia câștigă încredere în aplicarea cunoștințelor lor noi în scenarii din viața reală, luând decizii informate pentru a-și proteja dispozitivele și datele în mod eficient.

După finalizarea cu succes a MC-ului „Securitatea dispozitivului și protecția datelor”, participanții dobândesc cunoștințe solide, validându-și competențele în a-și securiza dispozitivele și pentru a-și proteja datele. Înarmați cu aceste abilități esențiale, cursanții sunt bine pregătiți să navigheze în peisajul digital cu încredere, asigurându-se că dispozitivele lor rămân în siguranță, iar datele lor sunt protejate împotriva potențialelor amenințări.

În conluzie, MC-ul „Securitatea dispozitivului și protecția datelor” este un program transformator, care oferă cursanților cunoștințe și abilități practice în securitatea dispozitivelor și protecția datelor. Participanții vor deveni gardieni proactivi ai dispozitivelor și a datelor lor digitale, echipați pentru a atenua riscurile de securitate și pentru a promova un mediu digital mai sigur pentru ei și ceilalți.

Întrebări

1. Întrebare bazată pe scenariu despre securitatea Bluetooth: „Imaginați-vă că tocmai ați terminat de utilizat Bluetooth pentru a vă conecta dispozitivul la un difuzor fără fir. Ce pași ați urma pentru a asigura securitatea dispozitivului Dvs. după deconectarea de la difuzor? Explicați riscurile potențiale de a părăsi Bluetooth activat atunci când nu este utilizat și furnizați motivele pentru care este esențial să dezactivați Bluetooth în astfel de situații."
2. Evaluarea aptitudinilor practice privind scanarea virușilor: „Primiți o unitate USB, de la un coleg, care conține documente importante pentru un proiect viitor. Înainte de a accesa fișierele, explicați pașii pe care i-ați urma pentru a efectua o scanare amănunțită a virușilor de pe dispozitivul de memorare extern. Descrieți instrumentele și software-ul pe care le-ați folosi și importanța efectuării unei scanări antivirus pentru a vă proteja dispozitivul și datele."
3. Întrebare de gândire critică privind protecția datelor: „Doriți să transferați anumite fișiere de pe computerul Dvs. pe un hard disk extern, în scopuri de obținere a unor copii d rezervă (backup). Cum v-ați asigura că dispozitivul de memorare externă nu conține programe malware sau viruși care v-ar putea infecta computerul în timpul procesului de transfer? Discutați despre importanța scanării virușilor posibili din dispozitivee de memorare externe și despre modul în care această practică contribuie la protecția generală a datelor și la securitatea dispozitivului."

Instruire și implementare cuprinzătoare în domeniul securității (MC 4.1.C.6)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Instruire și implementare cuprinzătoare în domeniul securității Cod: MC 4.1.C.6
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: 101087628
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	AVANSAT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.53, 4.1.54 și 4.1.55):

- Înțelegeți importanța instruirii angajaților cu privire la tehnicile de securitate IT.
- Dezvoltați măsuri cuprinzătoare de securitate fizică pentru a proteja activele organizaționale.
- Fiind conștienți de importanța conceptului de autentificare în doi factori (2FA) și de rolul acestui tip de autentificare în furnizarea unui strat suplimentar de protecție pentru conturile online.

Descriere

MC-ul „**Instruire și implementare cuprinzătoare în domeniul securității**" este un program cuprinzător, specializat, conceput pentru a dota cursanții cu cunoștințele și abilitățile necesare pentru a asigura practicile de securitate solide în cadrul organizațiilor.

Avizat de restigioasa Comisie Europeană, acest program se concentrează pe trei aspecte esențiale ale securității: instruire în domeniul securității IT, măsuri de securitate fizică și autentificare cu doi factori (2FA).

În primul modul, participanții se adâncesc în domeniul critic al formării în domeniul securității IT. Ei învață cum să educe în mod eficient angajații cu privire la cele mai bune practici, la protocoalele de securitate cibernetică și la conștientizarea amenințărilor. Prin utilizarea metodelor de învățare interactive, a studiilor de caz și a scenariilor din viața reală, cursanții dezvoltă experiența de a instrui și de a ghida angajații cu privința protejării datelor, a identificării potențialelor amenințări și a răspunsului la incidente de securitate.

Al doilea modul subliniază importanța măsurilor cuprinzătoare de securitate fizică. Participanții obțin informații despre evaluarea și dezvoltarea unor măsuri de securitate robuste pentru a proteja activele organizaționale, infrastructura și informațiile sensibile. Prin exerciții practice și evaluări ale site-ului, cursanții formulează planuri de securitate personalizate, care cuprind controlul accesului, supravegherea și măsurile de urgență pentru a atenua riscurile de securitate fizică.

În al treilea modul, participanții aprofundează conceptul de autentificare cu doi factori (2FA). Ei înțeleg beneficiile 2FA în consolidarea securității conturilor online, prin adăugarea unui nivel suplimentar de protecție dincolo de parolele tradiționale. Prin discuții interactive și demonstrații practice, cursanții înțeleg diferitele metode ale 2FA, cum ar fi parolele unice (OTP) și autentificarea biometrică, și învață cum să implementeze și să susțină aceste practici esențiale de securitate.

Pe parcursul MC-ului, cursanții se angajează în scenarii practice, jocuri de rol și proiecte de implementare, pentru a-și aplica cunoștințele în mod eficient. Programul promovează o mentalitate proactivă și conștientă de securitate, permițând cursanților să ia decizii informate și să promoveze o cultură a securității în cadrul organizațiilor lor.

După finalizarea cu succes a MC-ului „Instruire și implementare cuprinzătoare în domeniul securității", participanții dobândesc cunoștințe valoroase, validându-și expertiza în îmbunătățirea securității organizaționale. Înarmați cu o mulțime de abilități, cursanții sunt bine pregătiți pentru a-și asuma roluri cheie în conducerea inițiativelor de securitate, în protejarea datelor sensibile și în promovarea unui mediu organizațional sigur și rezistent.

În concluzie, MC-ul „Instruire și implementare cuprinzătoare în domeniul securității” este un program care pregătește cursanții să abordeze în mod proactiv provocările de securitate din organizații. Participanții vor deveni lideri în implementarea măsurilor de securitate eficiente, în instruirea angajaților și în susținerea celor mai bune practici de securitate, contribuind la un peisaj digital mai sigur și întărind rezistența organizațională împotriva amenințărilor cibernetice.

Întrebări

1. Întrebarea privind abordarea formării: „Ca trainer în securitate IT, descrieți pașii pe care i-ați urma pentru a proiecta un program eficient de instruire pentru angajați cu privire la tehnicile de securitate IT. Cum ați adapta instruirea în diferite roluri și niveluri de expertiză tehnică din cadrul organizației?"
2. Întrebare de planificare a securității fizice: „Aveți sarcina de a dezvolta măsuri extinse de securitate fizică pentru un nou sediu al companiei. Descrieți pașii cheie pe care i-ați urma pentru a evalua potențiale riscuri de securitate, identificați activele care necesită protecție și proiectați un plan de securitate care să cuprindă controlul accesului, supraveghere și măsuri de urgență”.
3. Explicați conceptele și avantajele 2FA: „Explicați unei persoane nefamiliare cu termenul conceptul de autentificare cu doi factori (2FA). Descrieți cum funcționează 2FA și avantajele specifice pe care le oferă în comparație cu metodele de autentificare cu un singur factor, cum ar fi parolele tradiționale.”
4. Scenariu real de instruire privind securitatea IT: „Conduceți o sesiune de instruire în domeniul securității IT pentru angajații unei organizații mari. Alegeți unul dintre următoarele scenarii: atacuri de tip phishing, securitate prin parolă sau protecția datelor. Descrieți cum ați simula o situație reală - situație de viață legată de scenariul ales pentru a instrui și pentru a educa efectiv angajații.”
5. Implementarea securității fizice: „După evaluarea nevoilor de securitate fizică ale unei companii, ați fost însărcinat cu implementarea măsurilor de securitate recomandate. Descrieți pașii cheie pe care i-ați urma pentru implementarea sistemelor de control al accesului, supraveghere și management al vizitatorilor, asigurând protecție maximă pentru activele organizației”.
6. Implementarea 2FA: „Veți să implementați autentificarea în doi factori (2FA) pentru conturile online ale unei organizații. Subliniați pașii pe care i-ați urma pentru a implementa 2FA pentru toți angajații și explicați cum ați susține adoptarea acestuia pentru a asigura o utilizare pe scară largă. "
7. Angajamentul și implicarea angajaților: „Ca trainer în domeniul securității, cum ați asigura participarea și implicarea activă a angajaților în timpul sesiunilor de instruire în domeniul securității IT? Descrieți strategiile pe care le-ați folosi pentru a încuraja angajații să adopte cele mai bune practici de securitate în rutina lor zilnică de lucru.”
8. Comparația metodelor 2FA: „Comparați două metode diferite de autentificare cu doi factori (de exemplu, parole unice și autentificare biometrică). Explicați punctele forte și punctele slabe ale fiecărei metode și identificați scenarii specifice în care o metodă ar putea fi mai potrivită decât cealaltă.”

Conștientizarea securității cibernetice și protecția dispozitivelor (MC 4.1.C.7)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Conștientizarea securității cibernetice și protecţia dispozitivelor Cod: MC 4.1.C.7
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: 101087628
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	AVANSAT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.56, 4.1.57 și 4.1.58):

- Învățați cum să diagnosticați și să depanați problemele de securitate pe dispozitivele dvs., identificând eventualele programe malware sau încercări de acces neautorizat.
- Înțelegeți potențialele pericole ale stocării parolelor în browserele web și importanța utilizării instrumentelor dedicate de gestionare a parolelor.
- Elaborați un plan personal de conștientizare a securității cibernetice pentru a rămâne informat cu privire la amenințările actuale și pentru a adopta cele mai bune practici pentru a proteja dispozitivele și datele personale.

Descriere

MC-ul „Conștientizarea securității cibernetice și protecţia dispozitivelor” este un program cuprinzător și practic, conceput pentru a oferi cursanților cunoștințe și abilități esențiale în materie de securitate cibernetică.

Acest program se concentrează pe trei aspecte vitale ale securității cibernetice pentru a asigura protecția dispozitivelor și datelor personale.

În primul modul, participanții pătrund în adâncime în lumea practică a diagnosticării și remedierii problemelor de securitate pe dispozitivele lor. Prin simulări interactive și scenarii din viața reală, cursanții dobândesc experiență în identificarea potențialelor infecții malware, detectarea încercărilor de acces neautorizat și aplicarea strategiilor eficiente de remediere. Prin stăpânirea acestor abilități, participanții își pot proteja în mod proactiv dispozitivele în fața amenințărilor de securitate și își pot menține integritatea activelor digitale.

Al doilea modul analizează potențialele pericole ale stocării parolelor în browserele web și rolul esențial al instrumentelor dedicate de gestionare a parolelor. Cursanții explorează vulnerabilitățile asociate stocării parolelor bazate pe browser și riscurile sporite ale accesului neautorizat la conturile sensibile. Înarmați cu aceste cunoștințe, participanții descoperă importanța utilizării instrumentelor fiabile de gestionare a parolelor pentru a genera și memora în siguranță parole complexe și unice pentru fiecare cont. Activitățile practice permit cursanților să implementeze practici solide de gestionare a parolelor, pentru a le spori securitatea online.

În modulul final, participanții dezvoltă un plan personalizat de conștientizare a securității cibernetice pentru a rămâne informați cu privire la amenințările actuale și pentru a adopta cele mai bune practici pentru protecția dispozitivelor și a datelor. Ei învață cum să acceseze resurse credibile de securitate cibernetică, să urmărească actualizările din industrie și să rămână vigilenți împotriva amenințărilor cibernetice emergente. Cultivând o mentalitate proactivă și implementând cele mai bune practici de securitate, participanții creează o apărare solidă împotriva potențialelor atacuri cibernetice și a încălcării datelor.

Pe parcursul MC-ului, cursanții se angajează în evaluări interactive, exerciții practice și planuri de acțiune personalizate, pentru a-și aplica noile cunoștințe dobândite. Programul pune accent pe gândirea critică, rezolvarea problemelor și adoptarea de măsuri de securitate proactive pentru a proteja dispozitivele și datele personale în peisajul digital dinamic de astăzi.

După finalizarea cu succes a MC-ului „Conștientizarea securității cibernetice și protecţia dispozitivelor”, participanții primesc certificarea MC. Această recunoaștere le validează competența în diagnosticarea problemelor de securitate, utilizarea tehnicilor de gestionare a parolelor sigure și dezvoltarea unui plan proactiv de conștientizare a securității cibernetice.

În concluzie, MC-ul „Conștientizarea securității cibernetice și protecţia dispozitivelor” furnizează cursanților abilitățile și cunoștințele esențiale de securitate cibernetică pentru a-și proteja viața digitală. Participanții vor deveni apărători proactivi împotriva amenințărilor cibernetice, pregătiți pentru a-și proteja dispozitivele și datele personale, contribuind la construirea unui ecosistem digital mai sigur pentru ei și pentru comunitățile lor.

Întrebări

1. Calculatorul dumneavoastră funcționează mai lent decât de obicei și primiți frecvent anunțuri pop-up în timp ce navigați pe internet. Ce problemă de securitate ar putea fi și ce pași ați urma pentru a depana și a rezolva această problemă?
2. Explicați potențialele pericole ale memorării parolelor în browserele web și cum vă poate compromite acest lucru securitatea online. Care sunt beneficiile utilizării instrumentelor dedicate de gestionare a parolelor și cum sporesc acestea securitatea parolelor?
3. Imaginați-vă că primiți un e-mail care pare a fi de la banca dvs., prin care vi se cere să accesați un link pentru a vă actualiza urgent informațiile contului. Ce ar trebui să faceți pentru a verifica legitimitatea e-mailului și pentru a vă proteja să cădeți victima unei escrocherii de tip phishing?
4. Elaborați un plan de conștientizare a securității cibernetice care să sublinieze pașii pe care îi veți urma pentru a rămâne informat cu privire la amenințările actuale și la cele mai bune practici pentru protejarea dispozitivelor și a datelor dumneavoastră personale. Includeți acțiuni specifice pe care le veți întreprinde, cum ar fi abonarea la surse de știri privind securitatea cibernetică, activarea autentificării cu doi factori și actualizarea regulată a software-ului dispozitivului dvs.

Practici avansate de securitate pentru dispozitivele și sistemele personale (MC 4.1.C.8)

Informatii de baza

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Practici avansate de securitate pentru dispozitivele și sistemele personale Cod: MC 4.1.C.8
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: 101087628
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	AVANSAT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.59, 4.1.60):

- Adoptați software antivirus și anti-malware de renume pe dispozitivele personale pentru a detecta și elimina potențialele amenințări.
- Implementați controale de acces pentru a reglementa și restricționa intrarea în sisteme, conturi sau profiluri personale, asigurând o mai bună securitate și confidențialitate.

Descriere

MC-ul „Practici avansate de securitate pentru dispozitivele și sistemele personale" este un program specializat, conceput pentru ca persoanele să deprindă tehnici avansate de securitate, pentru a-și proteja dispozitivele personale și profilurile digitale. Acest curs cuprinzător se concentrează pe două competențe cheie, esențiale pentru consolidarea securității digitale și a confidențialității.

Primul modul este dedicat înzestrării participanților cu cunoștințele și abilitățile necesare pentru a instala și utiliza software-uri antivirus și anti-malware recunoscute, pe dispozitivele lor personale. Explorând cele mai bune practici pentru selectarea și instalarea soluțiilor de securitate eficiente, cursanții capătă informații despre detectarea și eliminarea potențialelor amenințări care pot compromite integritatea dispozitivelor lor. Scenariile din lumea reală și simulările practice le vor permite participanților să își aplice experiența în identificarea și atenuarea diferitelor tipuri de malware, inclusiv viruși, troieni și spyware. Prin stăpânirea utilizării acestor instrumente esențiale, cursanții își pot construi o apărare solidă împotriva amenințărilor digitale și își pot îmbunătăți comportamentul general în securitatea cibernetică.

În cel de-al doilea modul, participanții pătrund în adâncime în domeniul controalelor de acces și în semnificația acestora în reglementarea intrării în sisteme, conturi și profiluri personale.
Cursanții vor explora diverse metode de control al accesului, cum ar fi parolele, autentificarea cu mai mulți factori și controlul accesului bazat pe roluri (RBAC). Exercițiile practice ghidează participanții în configurarea controalelor de acces pentru diferite scenarii, permițându-le să-și securizeze în mod eficient datele, aplicațiile și identitățile online. În plus, modulul subliniază importanța menținerii parolelor puternice și unice pentru a consolida mecanismele de control al accesului, atenuând riscul accesului neautorizat și potențialele încălcări ale datelor.

Pe parcursul MC-ului, cursanții vor fi evaluați prin cursuri interactive, sarcini practice și simulări ale provocărilor de securitate din lumea reală. Participanții vor dezvolta o înțelegere profundă a practicilor avansate de securitateș aceste practicle vor permite să își protejeze în mod proactiv dispozitivele personale și activele digitale împotriva amenințărilor emergente.

După finalizarea cu succes a MC-ului „Practici avansate de securitate pentru dispozitivele și sistemele personale", participanții vor primi recunoașterea care le validează competența în adoptarea și implementarea măsurilor avansate de securitate, întărindu-le credibilitatea în peisajul securității digitale.

În concluzie, MC-ul „Practici avansate de securitate pentru dispozitivele și sistemele personale" înzestrează cursanții cu expertiza necesară pentru a-și proteja în mod eficient viața digitală. Înarmați cu o înțelegere mai profundă a software-ului de securitate de renume, a controalelor avansate de acces și a practicilor de parole sigure, participanții vor deveni gardieni ai dispozitivelor și sistemelor lor personale, promovând un ecosistem

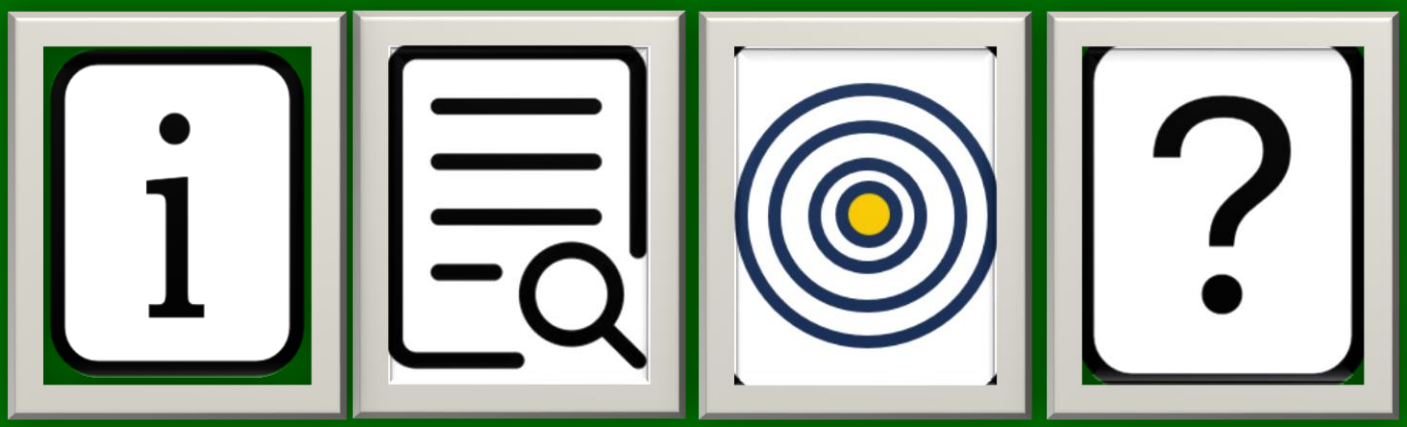
digital mai sigur pentru ei înșiși și pentru societate în ansamblu.

Întrebări

1. De ce este important să instalați și să utilizați software antivirus și anti-malware recunoscute pe dispozitivele personale? Furnizați exemple de potențiale amenințări pe care aceste soluții software le pot detecta și elimina.
2. Explicați conceptul de control al accesului și rolul acestuia în asigurarea unei securități și a unei confidențialități mai bune pentru sisteme, conturi sau profiluri personale. Furnizați exemple specifice de metode de control al accesului și scenarii în care acestea pot fi implementate eficient.
3. Imagina-ți-vă că tocmai ați achiziționat un nou dispozitiv personal. Descrieți pașii pe care i-ați urma pentru a căuta, selecta și instala software antivirus și anti-malware, recunoscute, pe dispozitiv.
4. Sunteți responsabil pentru securizarea unei aplicații bazate pe web utilizată de angajații organizației dvs. Descrieți cum ați implementa controalele de acces pentru a reglementa și a restricționa accesul la diferitele caracteristici și funcționalități ale aplicației. Includeți metodele specifice de control al accesului pe care le-ați utiliza și argumentați alegerile dvs.

NIVELUL EXPERT

(Nivelul 7 și Nivelul 8)



Managementul riscurilor de securitate cibernetică și conștientizarea personalului (MC 4.1.D.1)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul riscurilor de securitate cibernetică și conștientizarea personalului **Cod: MC 4.1.D.1**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	EXPERT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.61, 4.1.62 și 4.1.63):

- Înțelegeți importanța organizării anuale de formare anuală de conștientizare a personalului cu privire la securitatea cibernetică.
- Analizați și clasificați potențialele riscuri de securitate cibernetică pe baza impactului și probabilității lor de apariție.
- Examinați și actualizați în mod regulat politicile și procedurile legate de securitatea cibernetică.

Descriere

MC-ul „**Managementul riscurilor de securitate cibernetică și conștientizarea personalului**” este un program cuprinzător, conceput pentru oferi cursanților expertiza necesară pentru a gestiona eficient riscurile de securitate cibernetică în cadrul organizațiilor lor. Acest curs de specialitate se concentrează pe trei competențe cheie, fundamentale pentru asigurarea unor practici solide de securitate cibernetică și pentru promovarea unei culturi a conștientizării securității în rândul personalului.

Primul modul subliniază importanța desfășurării anuale a unor cursuri de formare în conștientizarea personalului cu privire la securitatea cibernetică. Participanții vor afla cum angajații educați și vigilenți joacă un rol esențial în protejarea activelor și a datelor organizaționale împotriva amenințărilor cibernetice. Înțelegând riscurile de securitate cibernetică și cele mai bune practici, cursanții pot participa la programe de formare eficiente pentru a răspunde nevoilor specifice ale organizației lor. Exemplele practice și studiile de caz vor evidenția impactul personalului bine informat în atenuarea riscurilor și în promovarea unei poziții rezistente de securitate cibernetică.

În cel de-al doilea modul, participanții vor pătrunde în profunzime în lumea analizei și a categorizării riscurilor de securitate cibernetică. Cursanții vor obține informații valoroase în evaluarea potențialelor amenințări pe baza impactului și a probabilității lor de apariție. Prin metodologii și cadre de evaluare a riscurilor, participanții vor învăța să prioritizeze și să aloce resursele în mod eficient, pentru a aborda cele mai critice riscuri de securitate cibernetică. Exercițiile practice vor oferi cursanților capacitatea de a efectua evaluări ale riscurilor, permițându-le să identifice vulnerabilitățile, să implementeze contramăsuri și să optimizeze strategiile de securitate cibernetică.

Al treilea modul se concentrează pe importanța revizuirii și a actualizării periodice a politicilor și a procedurilor de securitate cibernetică. Participanții vor explora cele mai bune practici pentru crearea și menținerea politicilor cuprinzătoare de securitate cibernetică, care se aliniază cu obiectivele și cerințele de conformitate ale organizației. Ei vor învăța cum să adapteze politicile și procedurile pentru a aborda amenințările cibernetice emergente și schimbările din peisajul tehnologic. Studiile de caz practice și discuțiile de grup le vor permite cursanților să identifice domeniile de îmbunătățire și să implementeze actualizările necesare pentru a consolida securitatea cibernetică a organizației lor.

Pe parcursul MC-ului, cursanții vor fi evaluați prin chestionare, studii de caz și sarcini practice. Toate acesteavor evalua capacitatea cursanților de a-și aplica cunoștințele dobândite în scenarii din lumea reală. Participanții vor dobândi o înțelegere mai profundă a managementului riscului de securitate cibernetică și a rolului cursurilor de formare în conștientizarea personalului, în promovarea unui mediu organizațional sigur.

După finalizarea cu succes a MC-ului „Managementul riscurilor de securitate cibernetică și conștientizarea personalului”, participanții vor dobândi o înțelegere puternică în gestionarea riscurilor de securitate cibernetică și încurajarea unei culturi de conștientizare a securității în rândul personalului, contribuind la îmbunătățirea practicilor de securitate cibernetică în diverse organizații.

Pe scurt, MC-ul „Managementul riscului de securitate cibernetică și conștientizarea personalului” furnizează cursanților cunoștințele și abilitățile necesare pentru a analiza în mod eficient riscurile de securitate cibernetică, pentru a concepe programe de instruire și conștientizare a personalului și pentru a actualiza menține politicile și procedurile de securitate cibernetică la zi. Prin împuternicirea persoanelor să ia măsuri proactive împotriva amenințărilor cibernetice, acest MC joacă un rol esențial în consolidarea rezistenței digitale a organizațiilor din diverse industrii.

Întrebări

1. De ce este esențial să se organizeze anual cursuri de formare în conștientizare a personalului cu privire la securitatea cibernetică? Furnizați exemple specifice despre modul în care angajații bine informați pot contribui la practici mai bune de securitate cibernetică.
2. Descrieți procesul de analiză și clasificare a riscurilor potențiale de securitate cibernetică în funcție de impactul și probabilitatea de apariție a acestora. Cum ajută această evaluare a riscurilor la prioritizarea măsurilor de securitate și a alocării resurselor?
3. De ce este crucial pentru organizații să revizuiască și să actualizeze în mod regulat politicile și procedurile legate de securitatea cibernetică? Cum pot politicile învechite să prezinte riscuri pentru securitatea organizației?
4. Sunteți un profesionist IT în securitate, însărcinat cu desfășurarea cursurilor de formare în conștientizarea personalului, privind securitatea cibernetică pentru o companie. Descrieți subiectele cheie și cele mai bune practici pe care le-ați include în programul de formare, ținând cont de companie și de provocările specifice de securitate.
5. Imaginați-vă că sunteți un analist al riscurilor de securitate cibernetică pentru o instituție financiară. Analizați un scenariu ipotetic de risc de securitate cibernetică, clasificând riscurile în funcție de impactul și de probabilitatea de apariție a acestora. Oferiți recomandări pentru atenuarea riscurilor identificate și explicați de ce aceste măsuri sunt esențiale pentru strategia de securitate a organizației.

Securitatea cibernetică centrată pe date și managementul datelor redundante (MC 4.1.D.2)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea cibernetică centrată pe date și managementul datelor redundante **Cod: MC 4.1.D.2**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	EXPERT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.64, 4.1.65):

- Puneți accent pe măsurile de securitate centrate pe date, mai degrabă decât să vă bazați doar pe apărarea perimetrului.
- Demonstrați-vă cunoștințele și abilitățile pentru a identifica și a elimina datele redundante, pentru a îmbunătăți securitatea cibernetică.

Descriere

MC-ul „Securitatea cibernetică centrată pe date și managementul datelor redundante" este un program de ultimă oră, conceput pentru instrui participanții în tehnicile avansate de securitate cibernetică centrate pe protejarea datelor, aspect important pentru orice organizație. Acest curs cuprinzător se concentrează pe două competențe cheie care abordează provocările moderne legate de securitatea cibernetică.

În peisajul dinamic al amenințărilor de astăzi, apărarea perimetrului tradițional nu mai este suficientă pentru a proteja datele sensibile față de amenințările cibernetice sofisticate. Primul modul al acestei MC subliniază schimbarea paradigmei către măsurile de securitate centrate pe date. Participanții vor dobândi o înțelegere profundă a principiilor securității centrate pe date, explorând criptarea, token-izarea, controalele accesului și tehnicile de mascare a datelor. Studiile de caz din lumea reală și cele mai bune practici vor demonstra modul în care securitatea centrată pe date întărește protecția informațiilor sensibile și întărește organizațiile împotriva breșelor datelor și a atacurilor cibernetice.

Al doilea modul este dedicat managementului datelor redundante, un aspect crucial al securității cibernetice, adesea trecut cu vederea. Participanții vor învăța importanța identificării și a eliminării datelor redundante, cu scopul de a minimiza suprafața de atac și de a îmbunătăți integritatea datelor. Prin exerciții practice, cursanții vor dezvolta abilitățile de a efectua audituri de date, de a detecta și a elimina datele redundante și de a eficientiza sistemele de memorare a datelor. Această abordare proactivă nu numai că îmbunătățește securitatea cibernetică, ci și promovează eficiența datelor, reducând costurile de memorare și îmbunătățind practicile de gestionare a datelor.

Pe parcursul MC-ului, participanții vor fi evaluați prin sarcini practice, exerciții de audit al datelor și scenarii. Ei vor avea ocazia să-și aplice cunoștințele în incidente simulate de securitate cibernetică, demonstrându-și competența în implementarea măsurilor de securitate centrate pe date și gestionarea datelor redundante.

După finalizarea cu succes a MC-ului „Securitatea cibernetică centrată pe date și managementul datelor redundante", participanții vor primi un certificat de absolvire din partea Comisiei Europene. Această recunoaștere prestigioasă le validează expertiza în protejarea datelor prin măsuri de securitate centrate pe date și prin implementarea unor strategii eficiente de gestionare a datelor redundante.

Pe scurt, MC-ul „Securitatea cibernetică centrată pe date și managementul datelor redundante" înzestrează participanții cu cele mai recente cunoștințe și abilități în domeniul securității cibernetice centrate pe date și al managementului datelor redundante. Prin prioritizarea protecției datelor și eficientizarea practicilor de memorare a datelor, acest program joacă un rol crucial în consolidarea securității cibernetice și în promovarea eficienței datelor, în cadrul organizațiilor din diferite sectoare. Participanții vor fi bine pregătiți să navigheze în peisajul securității cibernetice în evoluție și să devină active valoroase în protejarea datelor sensibile de

amenințările cibernetice în continuă evoluție.

Întrebări

1. Explicați conceptul de securitate centrată pe date și modul în care diferă de a vă baza doar pe apărarea perimetrului. Furnizați exemple specifice de măsuri de securitate centrate pe date, care pot proteja eficient informațiile sensibile chiar și în absența unei apărări puternice de perimetru.
2. Sunteți un profesionist în securitate IT responsabil pentru îmbunătățirea securității cibernetice în organizația dvs. Descrieți pașii pe care i-ați urma pentru a identifica și elimina datele redundante din sistemele de memorare a datelor ale organizației. Cum contribuie această practică la îmbunătățirea rezistenței securității cibernetice și a integrității datelor?
3. Într-un scenariu ipotetic, o companie s-a confruntat cu o breșă a datelor, în ciuda faptului că avea o apărare puternică în perimetru. Cum ar fi putut măsurile de securitate centrate pe date să atenueze sau să minimizeze impactul breșei? Oferiți informații despre strategiile cheie de securitate centrate pe date care ar fi putut face diferența în prevenirea sau răspunsul la incident.

Conducerea securității cibernetice și dezvoltarea culturii (MC 4.1.D.3)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Conducerea securității cibernetice și dezvoltarea culturii **Cod: MC 4.1.D.3**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	EXPERT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.66, 4.1.67):

- Pledați pentru investiții sporite în securitatea cibernetică și alocați resurse în mod eficient
- Fiți conștienți de importanța promovării unei mentalități de securitate la nivel de companie și a unei culturi a conștientizării securității cibernetice

Descriere

MC-ul „**Conducerea securității cibernetice și dezvoltarea culturii**” este un program cuprinzător, care dă posibilitatea participanților să susțină securitatea cibernetică în cadrul organizațiilor, să promoveze o cultură de conștientizare asupra securității și să conducă alocarea eficientă a resurselor pentru o rezistență cibernetică îmbunătățită. Dezvoltat în colaborare cu Comisia Europeană, acest curs transformator oferă participanților cunoștințele și abilitățile esențiale pentru a deveni lideri proactivi în securitatea cibernetică.

În peisajul digital care evoluează rapid, securitatea cibernetică a devenit un imperativ strategic pentru organizațiile de toate dimensiunile și din toate sectoarele de activitate. Primul modul al acestei MC analizează importanța investițiilor sporite în securitatea cibernetică.
Participanții vor obține informații despre amenințările cibernetice emergente, potențialele consecințe ale atacurilor cibernetice și importanța tot mai mare a alocării resurselor adecvate pentru a întări apărarea cibernetică. Prin studii de caz și discuții conduse de experți, cursanții vor explora cele mai bune practici pentru efectuarea de analize cost-beneficiu pentru a justifica investițiile în securitate cibernetică și pentru a alinia strategiile de securitate cu obiectivele organizaționale.

Al doilea modul se concentrează pe promovarea unei mentalități de securitate la nivel de companie și pe cultivarea unei culturi de conștientizare a securității cibernetice. Participanții vor aprofunda aspecte din psihologia comportamentului uman și impactul acestuia asupra securității cibernetice. Bazați pe aceste aspecte, cursanții vor dezvolta strategii pentru a implica și educa angajații de la toate nivelurile, pentru ca aceștia să devenă participanți activi la protejarea activelor digitale. Modulul va aborda tehnici eficiente de comunicare, metode de instruire antrenante și stabilirea unor politici și linii directoare solide de securitate cibernetică.
Participanții vor fi pregătiți pentru a implementa programe de conștientizare a securității, care să insufle o cultură proactivă de securitate și să ofere angajaților puterea să recunoască și să răspundă eficient la amenințările cibernetice.

Pe parcursul MC-ului, participanții se vor implica în ateliere interactive, jocuri de rol și simulări bazate pe scenarii. Ei vor învăța de la experții din industrie și liderii în securitate cibernetică. Acești specialiști își vor împărtăși experiențele și perspectivele în gestionarea inițiativelor de securitate cibernetică. Cursul pune accent pe aplicațiile practice și provocările din lumea reală, permițând participanților să-și dezvolte abilități de conducere în contextul securității cibernetice.

Ca parte a procesului de evaluare, participanților li se va cere să elaboreze un plan de conducere în domeniul securității cibernetice adaptat organizației lor. Acest plan va demonstra competența lor în susținerea investițiilor în securitate cibernetică, promovarea unei culturi de conștientizare în securitate și alocarea eficientă a resurselor pentru a răspunde nevoilor organizației în materie de securitate cibernetică.

După finalizarea cu succes a MC-ului „Conducerea securității cibernetice și dezvoltarea culturii”, participanții vor primi un certificat care atestă capacitățile lor de a conduce inițiative de securitate cibernetică, de a cultiva o cultură de conștientizare în securitate și de a-și direcționa organizația către reziliența cibernetică și reducerea riscurilor.

În concluzie, MC-il „Conducerea securității cibernetice și dezvoltarea culturii” oferă participanților expertiza și strategiile pentru a conduce eforturile de securitate cibernetică în cadrul organizațiilor. De la susținerea investițiilor strategice până la promovarea unei culturi de conștientizare în securitate, participanții vor deveni lideri eficienți și agenți de schimbare în domeniul securității cibernetice. Prin integrarea cunoștințelor tehnice cu abilitățile de conducere, acest program joacă un rol esențial în a se asigura că organizațiile fac față amenințărilor cibernetice și adoptă securitatea cibernetică ca un factor strategic pentru succesul lor pe termen lung.

Întrebări

1. În calitate de susținător al securității cibernetice, cum ați aborda directorii executivi sau conducerea pentru a sublinia importanța investițiilor sporite în securitatea cibernetică? Furnizați argumente și date specifice pentru a vă susține cazul.
2. Descrieți pașii pe care i-ați urma pentru a efectua o evaluare amănunțită a riscului de securitate cibernetică în cadrul organizației dvs. Cum ați folosi rezultatele evaluării pentru a aloca resurse în mod eficient pentru abordarea vulnerabilităților și a amenințărilor identificate?
3. Cum ați comunica angajaților - de la toate nivelurile organizației - importanța securității cibernetice? Furnizați exemple de strategii și metode de comunicare pe care le-ați folosi pentru a promova o mentalitate de securitate la nivel de companie și pentru a promova conștientizarea securității cibernetice.
4. În contextul promovării unei culturi a conștientizării securității cibernetice, cum ați concepe și implementa un program de formare în domeniul securității cibernetice pentru angajați? Ce subiecte ați include în program și cum ați asigura implicarea și participarea angajaților?
5. În calitate de lider în domeniul securității cibernetice, cum ați măsura succesul eforturilor dumneavoastră de a promova o cultură de conștientizare în securitate în cadrul organizației? Ce măsurători și indicatori cheie de performanță (KPI) ați folosi pentru a evalua eficacitatea inițiativelor de conștientizare în securitatea cibernetică?
6. Descrieți un scenariu în care organizația dvs. se confruntă cu constrângeri bugetare, dar există o nevoie presantă de a îmbunătăți securitatea cibernetică. Cum ați prioritiza inițiativele de securitate cibernetică și ce decizii ați lua pentru pentru alocarea resurselor, cu scopul pentru a aborda vulnerabilitățile critice, optimizând în același timp resursele disponibile?
7. În calitate de susținător al investițiilor sporite în securitatea cibernetică, cum ați aborda provocările organizaționale și rezistența părților interesate care ar putea să nu înțeleagă pe deplin importanța securității cibernetice? Cum ați construi consensul și sprijinul pentru propunerile dvs.?
8. Împărtășiți un exemplu de campanie sau inițiativă de conștientizare a securității cibernetice, de succes, pe care ați implementat-o în trecut. Explicați elementele cheie care au contribuit la succesul obținut și impactul pe care l-a avut asupra poziției generale de securitate a organizației.

Managementul securității datelor și conștientizarea cibernetică (MC 4.1.D.4)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul securității datelor și conștientizarea cibernetică **Cod: MC 4.1.D.4**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	EXPERT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.68, 4.1.69 și 4.1.70):

- Demonstrați-vă capacitatea de a clasifica datele în funcţie de prioritate şi importanţă
- Fiți conștient de importanţa autentificării prin doi factori (Two-factor Authentication) sau multi-factor (Multi-factor Authentication)
- Dați dovadă de prudență și vigilență atunci când utilizați platformele de social media

Descriere

MC-ul „**Managementul securității datelor și conștientizarea cibernetică**” este un program cuprinzător, conceput pentru a furniza cursanților cunoștințele și abilitățile necesare pentru a asigura securitatea datelor lor și pentru a promova conștientizarea cibernetică în diverse contexte. Acest program se concentrează pe trei aspecte critice ale siguranței și securității: clasificarea datelor, autentificarea cu doi sau mai mulți factori (MFA) și practicile sigure pentru rețelele sociale.

Datele sunt vitale pentru organizațiile moderne, iar securitatea lor are o importanță capitală. Primul modul al acestui MC se concentrează pe clasificarea datelor - practică fundamentală pentru protejarea informațiilor sensibile. Cursanții vor aprofunda conceptul de clasificare a datelor, înțelegând semnificația acestuia în prioritizarea și protejarea informațiilor pe baza sensibilității și criticității acesteia. Prin exemple din lumea reală și exerciții practice, participanții își vor demonstra capacitatea de a clasifica datele în funcție de prioritate și importanță.

Cel de-al doilea modul al acestui MC prezintă cursanților autentificarea cu doi factori sau cu mai mulți factori (MFA), o practică solidă de securitate care depășește parolele tradiționale. Cursanții vor explora diferitele forme de MFA, inclusiv coduri bazate pe SMS, aplicații de autentificare, verificare biometrică și jetoane hardware. Ei vor afla cum MFA adaugă un nivel suplimentar de protecție, solicitând utilizatorilor să folosească mai multe forme de identificare când accesează conturi sau sisteme sensibile. Participanții vor câștiga experiență practică în implementarea MFA pe diferite platforme și dispozitive, asigurându-se că își pot proteja în mod eficient identitățile online și activele digitale.

Modulul final subliniază importanța practicilor de precauție și vigilență în timpul utilizării platformelor de social media. Rețelele sociale au devenit o parte integrantă a vieții moderne, dar prezintă și riscuri semnificative de securitate dacă nu sunt utilizate în mod responsabil.
Cursanții vor fi îndrumați cu privire la cele mai bune practici pentru a-și securiza conturile de pe rețelele sociale, pentru a le proteja confidențialitatea și pentru a evita capcanele comune, cum ar fi partajarea excesivă a informațiilor personale. Ei vor explora, de asemenea, potențialele consecințe ale utilizării greșite a rețelelor sociale și vor învăța cum să recunoască și să răspundă la activitățile suspecte sau la încercările de phishing pe aceste platforme.

Pe parcursul programului, cursanții vor participa la activități interactive, studii de caz și chestionare, pentru a-și consolida înțelegerea conceptelor și a abilităților practice. Ei vor avea, de asemenea, acces la resurse și instrumente pentru a-și îmbunătăți cunoștințele despre securitatea datelor și conștientizarea cibernetică. Micro Credential oferă o experiență de învățare flexibilă, permițând participanților să progreseze în propriul ritm, în timp ce primesc îndrumări de la instructori experimentați.

După finalizarea cu succes a MC-ului „Managementul securității datelor și conștientizarea cibernetică”, cursanții vor primi un certificat care atestă competența lor în clasificarea datelor, implementarea MFA și practicile de social media sigure, făcându-le active valoroase pentru orice organizație care dorește să-și consolideze postura de securitate cibernetică.

În concluzie, MC-ul „Managementul securității datelor și conștientizarea cibernetică” este un program cuprinzător, conceput pentru a oferi cursanților cunoștințele și abilitățile esențiale necesare pentru a-și proteja datele și pentru a promova o cultură a conștientizării cibernetice. MC-ul se înscrie în necesitatea – în continuă creștere – ca indivizii și organizațiile să adopte măsuri de securitate proactive într-un peisaj digital evolutiv. Prin finalizarea acestui MC, cursanții vor proteja datele, vor securizarea conturile și vor fi vigilenți în interacțiunile online, contribuind la un mediu digital mai sigur.

Întrebări

1. Cum ați determina prioritatea și importanța diferitelor tipuri de date în cadrul unei organizații? Furnizați exemple specifice de categorii de date și explicați cum le-ați clasifica.
2. Descrieți procesul de implementare a autentificării cu doi factori (2FA) sau a autentificării cu mai mulți factori (MFA) pentru un cont sau sistem online. Includeți pașii implicați și orice potențiale provocări sau considerații.
3. Explicați beneficiile utilizării autentificării cu doi factori sau cu mai mulți factori în comparație cu metodele tradiționale de autentificare cu un singur factor. Cum este sporită securitatea?
4. Furnizați exemple de situații în care utilizarea autentificării cu doi factori sau cu mai mulți factori ar fi deosebit de importantă și explicați de ce aceste scenarii necesită un nivel suplimentar de securitate.
5. Cum dați dovadă de precauție și vigilență atunci când folosiți platformele de social media? Descrieți anumite practici sau obiceiuri pe care le urmați pentru a vă proteja confidențialitatea și informațiile personale.
6. Identificați riscurile comune pentru securitatea rețelelor sociale, cum ar fi atacurile de phishing sau accesul neautorizat la conturi. Explicați strategiile pe care le aplicați pentru a atenua aceste riscuri și pentru a vă proteja prezența pe rețelele sociale.
7. Descrieți potențialele consecințe ale partajării informațiilor sensibile sau personale pe platformele de rețele sociale, fără setări de confidențialitate adecvate. Cum își pot persoanele să își protejeze datele în astfel de medii?
8. Cum pot organizațiile să promoveze conștientizarea securității cibernetice în rândul angajaților lor, în privința utilizării platformelor de social media atât la locul de muncă, cât și în mediul personal?
9. Imaginați-vă că găsiți un mesaj sau un link suspect pe o platformă de socializare. Ce pași ați lua pentru a verifica autenticitatea acestuia și pentru a vă asigura siguranța înainte de a vă implica?

Securitate cibernetică avansată și hacking etic (MC 4.1.D.5)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitate cibernetică avansată și hacking etic **Cod: MC 4.1.D.5**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	EXPERT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.71, 4.1.72):

- Aflați cum să folosiți și să angajați un hacker „pălărie albă” ("white hat" hacker) pentru evaluarea securității cibernetice
- Recunoașteți și apărați-vă împotriva tacticilor de inginerie socială

Descriere

MC-ul „Securitate cibernetică avansată și hacking etic” este un program extins și captivant, conceput pentru a înzestra cursanții cu cunoștințe și abilități avansate în recunoașterea și apărarea împotriva tacticilor de inginerie socială. În plus, participanții vor învăța cum să folosească tehnici de hacking etic, folosind hackeri de tip „pălărie albă” pentru evaluările de securitate cibernetică.

Prezentare generală a MC-ului:
Programul este împărțit în două module cuprinzătoare, fiecare concentrându-se pe aspectele esențiale ale securității cibernetice și ale hackingului etic. Cursanții vor beneficia de scenarii din lumea reală și exerciții practice, dobândind experiență practică în abordarea amenințărilor cibernetice sofisticate.

Modulul 1: Recunoașterea și apărarea împotriva tacticilor de inginerie socială
Acest modul oferă cursanților o înțelegere în profunzime a tacticilor de inginerie socială utilizate în mod obișnuit de către persoane rău intenționate pentru a exploata vulnerabilitățile umane.
Participanții vor învăța să recunoască aceste tehnici de manipulare și să dezvolte mecanisme de apărare eficiente pentru a se proteja împotriva atacurilor de inginerie socială.

1. Introducere în Ingineria Socială
   - Definiți ingineria socială și diferitele sale forme, inclusiv phishing-ul, pretextul, momeala, tailgating-ul și multe altele.
   - Înțelegeți aspectele psihologice care îi fac pe indivizi susceptibili la atacurile de inginerie socială.

2. Atacurile de phishing și falsificarea e-mailurilor
   - Identificați indicatorii comuni de phishing în e-mailuri și mesaje.
   - Analizați anteturile de e-mail pentru a detecta încercările de falsificare a e-mailurilor.
   - Practicați gestionarea sigură a e-mailurilor și raportarea e-mailurilor suspecte către autoritățile competente.

3. Pretextare și manipulare
   - Recunoașteți tacticile comune de pretext utilizate pentru a câștiga încredere și pentru a înșela victimele.
   - Dezvoltați strategii de verificare a autenticității cererilor și comunicărilor.

4. Momeli și Tailgating-uri
   - Înțelegeți conceptul de momeală și modul în care actorii rău intenționați folosesc oferte atrăgătoare pentru a compromite securitatea.
   - Implementați proceduri pentru a preveni accesul fizic neautorizat în zonele securizate prin tailgating.

5. Conștientizarea și instruirea în domeniul ingineriei sociale
   - Susțineți importanța cursurilor regulate de conștientizare a securității cibernetice pentru angajați și pentru indivizi.
   - Dezvoltați și implementați campanii de conștientizare a ingineriei sociale în cadrul organizațiilor.

6. Mecanisme de apărare și de răspuns la un incident
   - Creați planuri de răspuns la incident pentru a gestiona incidentele de inginerie socială.
   - Evaluați și îmbunătățiți mecanismele de apărare împotriva atacurilor de inginerie socială.

Modulul 2: Hacking etic și evaluări de tip „Pălărie albă” ("White Hat").
În acest modul, cursanții se vor aprofunda no'iunile dinn lumea hackingului etic, înțelegând metodologiile și instrumentele folosite de hackerii de tip „pălărie albă” pentru a efectua evaluări ale securității cibernetice. Accentul cade asupra utilizării tehnicilor de hacking etic pentru a identifica vulnerabilitățile și pentru a consolida postura de securitate cibernetică a unei organizații în mod proactiv.

1. Introducere în hacking-ul etic
   - Definiți hacking-ul etic și diferențiați-l de activitățile de hacking rău intenționat.
   - Înțelegeți considerentele etice și legale asociate cu evaluările hackingului etic.

2. Domeniul de aplicare și regulile de implicare
   - Definiți domeniul de aplicare și regulile de implicare pentru evaluările hackingului etic.
   - Elaborați linii directoare clare pentru efectuarea evaluărilor într-un mod controlat și sigur.

3. Amprentă și recunoaștere
   - Realizați amprentarea și recunoașterea pentru a aduna informații despre sistemele și rețelele țintă.
   - Utilizați instrumente și tehnici de inteligență open-source (OSINT) pentru a culege date.

4. Evaluarea vulnerabilității și testarea penetrației
   - Efectuați evaluări ale vulnerabilităților și teste de penetrare, pentru a identifica și exploata punctele slabe de securitate.
   - Raportați constatările și recomandați măsuri de remediere pentru a aborda vulnerabilitățile.

5. Testarea securității aplicațiilor web
   - Înțelegeți vulnerabilitățile comune ale aplicațiilor web și impactul acestora asupra securității.
   - Folosiți instrumente și metodologii pentru a evalua și a securiza aplicațiile web.

6. Evaluarea securității rețelei fără fir
   - Evaluați securitatea rețelei fără fir (wireless) și detectați potențialele vulnerabilități.
   - Implementați configurații securizate pentru rețelele wireless.

7. Ingineria socială în hacking-ul etic
   - Utilizați tehnici de inginerie socială în evaluările de hacking etic pentru a testa rezistența organizațională.
   - Discutați implicațiile etice și responsabilitățile asociate cu utilizarea ingineriei sociale în evaluări.

Evaluare și certificare:

MC-ul utilizează scenarii din viața reală și exerciții practice care evaluează capacitatea cursanților de a recunoaște și de a se apăra împotriva tacticilor de inginerie socială. În plus, cursanții își vor demonstra competența în utilizarea tehnicilor de hacking etic în timpul unei evaluări simulate de „pălărie albă". Finalizarea cu succes a programului va aduce participanților un certificat care validează expertiza cursanților în atenuarea amenințărilor de inginerie socială și evaluarea de hacking etic.

Concluzii:
MC-ul „Securitate cibernetică avansată și hacking etic" reprezintă o experiență de învățare aprofundată și practică, dând participanților cunoștințele și abilitățile necesare pentru a aborda amenințările cibernetice sofisticate. De la recunoașterea tacticilor de inginerie socială, până la efectuarea de evaluări de hacking etic, cursanții vor fi pregătiți să protejeze organizațiile de amenințările cibernetice și să contribuie la un mediu digital mai sigur.

Întrebări

1. Care sunt unele tactici comune de inginerie socială - utilizate de actorii rău intenționați - pentru a exploata vulnerabilitățile umane și cum se pot apăra indivizii împotriva unor astfel de tactici?
2. Cum ați folosi tehnici de hacking etic de tipul hacker cu „pălărie albă" pentru a evalua postura de securitate cibernetică a unei organizații? Furnizați un exemplu de scenariu în care hacking-ul etic poate fi utilizat în mod eficient.
3. Explicați importanța cursurilor de formare în conștientizarea ingineriei sociale pentru angajații din cadrul unei organizații. Cum poate o astfel de formare să contribuie la o cultură de securitate mai puternică?
4. În timpul unei evaluări a securității cibernetice de tipul hacker cu „pălărie albă", cum ați gestiona informațiile sensibile sau vulnerabilitățile descoperite în timpul evaluării pentru a menține practicile etice și a proteja organizația?
5. Descrieți rolul amprentei și recunoașterii într-o evaluare a hackingului etic. Cum pot aceste activități să ajute la identificarea potențialelor vulnerabilități în infrastructura de securitate a unei organizații?

Expert în securitatea cibernetică - Parole sigure și gestionarea accesului (MC 4.1.D.6)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Expert în securitatea cibernetică - Parole sigure și gestionarea accesului **Cod: MC 4.1.D.6**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	EXPERT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.73, 4.1.74):

- Deveniți capabili de a crea parole puternice și sigure pentru o securitate cibernetică îmbunătățită.
- Planificați strategii eficiente de gestionare a accesului, pentru a spori securitatea dispozitivelor folosite în afaceri și a datelor sensibile.

Descriere

Într-o era digitală aflată într-o evoluție rapidă, în care aproape fiecare aspect al interacțiunii umane este mediat prin platforme și dispozitive digitale, securitatea cibernetică a devenit o prioritate presantă. Apariția unor tehnologii precum inteligența artificială, cloud computing, Internetul lucrurilor (the Internet of Things) și învățarea automată, a amplificat semnificativ valoarea și vulnerabilitatea datelor. Această situație invită invariabil actori rău intenționați care sunt dornici să exploateze aceste vulnerabilități. Ca urmare, există o nevoie crescândă de practici eficiente de securitate cibernetică, care să includă o protecție robustă prin parolare și strategii extinse de gestionare a accesului.

Acest MC este conceput pentru a oferi o înțelegere aprofundată a securității cibernetice, cu un accent deosebit pe crearea unor parole solide și sigure, și pe implementarea unor strategii eficiente de gestionare a accesului. La finalizarea acestui program, participanții vor dobândi bazele esențiale în îmbunătățirea securității dispozitivelor folosite în afaceri și în protejarea datelor sensibile.

Modul: Crearea unei parole sigure
Semnificația protecției cu parolă, în ciuda naturii sale fundamentale, este adesea subestimată, ceea ce duce la riscuri de securitate considerabile. Parolele slabe sau reciclate devin ținte ușoare pentru infractorii cibernetici, care folosesc atacuri de tip “brute force” sau algoritmi sofisticați pentru a le sparge. În prima parte a acestui curs, participanții vor învăța despre principiile de bază ale creării de parole puternice și sigure, care includ utilizarea unei combinații de caractere speciale, litere și numere. Vor fi, de asemenea, prezentate strategii precum abținerea de la folosirea cuvintelor din dicționar, utilizarea autentificării cu doi factori și schimbarea frecventă a parolelor, pentru a consolida securitatea cibernetică.

Acest segment al MC-ului oferă participanților atât cunoștințe teoretice, cât și experiență practică în generarea de parole rezistente, care pot face față diferitelor tipuri de atacuri cibernetice. Folosind scenarii din lumea reală și studii de caz, vor fi evidențiate importanța parolelor sigure și repercusiunile compromiterii acestora. Participanții vor învăța să utilizeze instrumente de gestionare a parolelor, să implementeze o politică de parole sigure și să disemineze importanța parolelor puternice în rândul membrilor echipei lor.

Modul: Implementarea strategiilor de management al accesului
În afară de parole, un alt aspect critic al îmbunătățirii securității este implementarea unor strategii eficiente de gestionare a accesului. Aceasta include reglementarea legată de cine are acces la sisteme, definirea nivelului de acces și controlul a ceea ce poate face fiecare utilizator cu acel acces. Gestionarea inadecvată a accesului poate avea ca urmare ca datele și resursele sensibile să cadă în mâini neautorizate, ceea ce conduce la daune financiare și reputaționale substanțiale.

În această secțiune a cursului, participanții vor aprofunda strategiile de gestionare a accesului. Ei vor înțelege cum să atribuie și cum să gestioneze privilegiile de acces pe baza principiului cel mai mic privilegiu (PoLP), asigurându-se că utilizatorii au doar accesul necesar pentru a-și executa sarcinile. Vor fi abordate subiecte

precum controlul accesului bazat pe roluri (RBAC), verificarea identității utilizatorului, gestionarea sesiunilor, precum și auditul și monitorizarea activităților utilizatorilor. Această secțiune va examina, de asemenea, metode de gestionare a accesului la dispozitivele utilizate în afaceri și metode de gestionare a accesului privilegiat, pentru a preveni amenințările interne.

La finalizarea acestui MC, participanții vor dobândi o înțelegere cuprinzătoare a practicilor eficiente de securitate cibernetică. Ei vor dobândi cunoștințele și abilitățile necesare pentru a genera parole sigure și pentru a implementa strategii robuste de gestionare a accesului, sporind, în consecință, securitatea dispozitivelor și a datelor sensibile ale organizației lor. În plus, aceștia vor fi bine poziționați pentru a propaga semnificația acestor practici în cadrul organizației lor, promovând o cultură de conștientizare și responsabilizare în materie de securitate cibernetică.

Combinând teoria cu exerciții practice și studii de caz, acest curs înzestrează participanții cu abilitățile de a naviga cu încredere în peisajul securității cibernetice din ce în ce mai complex. Ei vor fi bine pregătiți pentru a identifica în mod proactiv potențialele vulnerabilități de securitate și pentru a implementa strategii pentru a le contracara în mod eficient, asigurând integritatea, confidențialitatea și disponibilitatea activelor informaționale ale organizației lor.

Finalizarea acestui MC nu numai că va certifica competența participanților în securitatea parolelor și în gestionarea accesului, dar va sublinia și angajamentul lor de a rămâne la curent cu peisajul securității cibernetice în evoluție, făcându-i astfel o resursă de neprețuit pentru inițiativele de protecție a datelor, în organizațiile lor.

Întrebări

1. Care sunt caracteristicile cheie ale unei parole puternice și sigure și cum contribuie aceste componente la îmbunătățirea securității cibernetice?
2. Cum ajută utilizarea unei combinații de caractere speciale, litere și numere, într-o parolă, la prevenirea atacurilor cibernetice? Furnizați un exemplu de parolă robustă, urmând aceste principii.
3. Care este rolul autentificării cu doi factori în îmbunătățirea securității parolelor? Explicați cum acesta poate proteja un sistem chiar dacă o parolă este compromisă.
4. De ce este esențial să evitați utilizarea cuvintelor din dicționar în parole? Explicați cu ajutorul unui exemplu din lumea reală.
5. Explicați principiul celui mai mic privilegiu (PoLP) și rolul acestuia în gestionarea eficientă a accesului. Cum îmbunătățește aplicarea PoLP securitatea dispozitivelor deținute de companii și a datelor sensibile?
6. Ce este controlul accesului bazat pe roluri (RBAC) și cum poate ajuta implementarea acestuia la gestionarea accesului la date sensibile și la dispozitivele deținute de companie?
7. Cum contribuie verificarea identității utilizatorilor la strategia generală de gestionare a accesului? Furnizați un exemplu în care verificarea identității poate preveni o potențială încălcare a securității.
8. De ce sunr importante auditul și monitorizarea continuă a activităților utilizatorilor într-o strategie eficientă de management al accesului? Cum ajută la detectarea timpurie a potențialelor amenințări de securitate?
9. Discutați un scenariu în care gestiunea necorespunzătoare a accesului conduce la o încălcare a datelor. Cum ar fi putut fi prevenit acest lucru prin implementarea unor strategii eficiente de gestionare a accesului?

Conștientizarea în securitate cibernetică și gestionarea conturilor (MC 4.1.D.7)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Conștientizarea securității cibernetice și gestionarea conturilor **Cod: MC 4.1.D.7**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	EXPERT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.75, 4.1.76):

- Educați angajații cu privire la riscurile asociate cu utilizarea conturilor personale pentru sarcini legate de muncă și promovați importanța separării conturilor personale de cele de afaceri.
- Implementați un sistem de cont personal pentru fiecare angajat, pentru a stabili responsabilitatea clară a accesului la date sensibile și pentru a urmări eficient activitățile utilizatorilor.

Descriere

În era digitală, integrarea tehnologiei în operațiunile zilnice ale unei afaceri este omniprezentă, aducând cu ea o creștere a cantității de date sensibile care necesită protecție. Această schimbare de paradigmă necesită măsuri riguroase de securitate și o forță de muncă educată pentru a minimiza potențialul de amenințări cibernetice. Riscurile asociate cu amenințările cibernetice nu se limitează la atacatorii externi, ci pot veni adesea din interiorul organizației, intenționat sau involuntar, prin utilizarea greșită a conturilor personale pentru sarcini legate de muncă. Prin urmare, este crucial să educăm angajații cu privire la aceste riscuri și să implementăm un sistem care separă conturile personale de cele de afaceri.

Acest MC este conceput pentru a oferi participanților o înțelegere cuprinzătoare a riscurilor asociate cu utilizarea conturilor personale pentru sarcini legate de muncă și a importanței separării conturilor personale de cele de afaceri. Participanții vor învăța, de asemenea, să implementeze un sistem de cont-uri personale pentru fiecare angajat, pentru a stabili responsabilitatea clară la accesul la date sensibile și pentru a urmări eficient activitățile utilizatorilor.

Modul: Educarea angajaților cu privire la riscuri

Importanța securității cibernetice în spațiul de lucru nu poate fi subestimată. Cu toate acestea, un sistem de securitate este atât de puternic pe cât atât de slab este. Adesea, această verigă slabă este eroarea umană sau neglijența, în principal când angajații își folosesc conturile personale pentru sarcini legate de muncă. Această parte a cursului analizează riscurile asociate cu utilizarea conturilor personale în scopuri comerciale, inclusiv scurgerea de date, potențialul hacking și dificultatea de a urmări activitățile legate de muncă. Participanții vor afla despre exemple din lumea reală în care utilizarea greșită a conturilor personale a dus la încălcări semnificative de securitate. Ei vor înțelege implicațiile de anvergură ale unor astfel de încălcări, inclusiv potențialul de pierdere financiară, daune asupra reputației și pierderea încrederii între părțile interesate. Prin aceste lecții, participanții vor ajunge să aprecieze importanța critică a menținerii unor conturilor personale și de afaceri, separate, pentru a asigura securitatea și integritatea datelor sensibile.

Modul: Promovarea importanței separării conturilor personale și de afaceri

În al doilea segment al cursului, participanții vor învăța despre importanța de a avea conturi personale și de afaceri separate. Această separare este un element fundamental al unei strategii puternice de securitate cibernetică, deoarece permite un control mai bun asupra accesului la datele sensibile, o urmărire mai ușoară a activităților legate de muncă și o responsabilitate îmbunătățită. Participanții vor explora diferitele beneficii ale separării conturilor personale de cele de afaceri, inclusiv securitate sporită, piste de audit mai clare și control mai mare asupra accesului la date. Studiile de caz care prezintă avantajele unei astfel de separări, precum și capcanele de a nu face acest lucru, vor consolida și mai mult această înțelegere.

Modul: Implementarea sistemelor de cont personal

Segmentul final al cursului se va concentra pe implementarea sistemelor de cont personal pentru fiecare angajat. Participanții vor învăța cum să configureze conturile individuale de muncă pentru angajații lor, să stabilească reguli și linii directoare clare pentru utilizarea acestora și să implementeze sisteme de monitorizare pentru a urmări eficient activitățile utilizatorilor. Participanții vor învăța despre cele mai bune practici pentru configurarea și gestionarea sistemelor de conturi personale, inclusiv cum se gestionază integrarea și deconectarea, gestionarea permisiunilor de acces și auditarea activităților utilizatorilor. Ei vor înțelege, de asemenea, rolul acestor sisteme în menținerea responsabilității și în îmbunătățirea securității generale.

La finalizarea acestui MC, participanții vor avea o înțelegere profundă a importanței separării conturilor personale de cele de afaceri și a riscurilor asociate cu utilizarea conturilor personale pentru sarcini legate de muncă. Aceștia vor dobândi abilitățile de a implementa sisteme eficiente de conturi personale, asigurând o mai bună securitate a datelor și responsabilitatea în cadrul organizației lor.

Acest MC le va oferi oportunitatea de a înțelege cum o forță de muncă informată și educată poate acționa ca primă linie de apărare împotriva potențialelor amenințări la adresa securității cibernetice. Ei vor putea să sensibilizeze echipele lor despre importanța separării conturilor personale de cele de afaceri, contribuind astfel la crearea unei culturi conștiente de securitate în cadrul organizațiilor lor. Printr-o combinație de elemente teoretice, exemple din lumea reală și exerciții practice, participanții vor fi bine pregătiți pentru a anticipa potențialele riscuri de securitate și pentru a implementa strategii de atenuare. Finalizarea acestui MC va certifica înțelegerea cursanților cu privire la importanța separării și a gestionării conturilor și va reflecta angajamentul lor de a menține practici solide de securitate cibernetică în cadrul organizației lor, făcându-le active de neprețuit în inițiativele de protecție a datelor ale organizației lor.

Întrebări

1. Care sunt potențialele ariscuri sociate cu angajații care utilizează conturile personale pentru sarcini legate de muncă? Vă rugăm să oferiți un exemplu real care ilustrează aceste riscuri.
2. Explicați beneficiile separării conturilor personale de cele afaceri pentru angajați. Cum poate această separare să îmbunătățească postura de securitate cibernetică a unei organizații?
3. Ce măsuri poate lua o organizație pentru a educa angajații cu privire la pericolele utilizării conturilor personale pentru sarcini legate de muncă?
4. Cum ajută separarea conturilor personale de cele de afaceri la urmărirea mai eficientă a activităților legate de muncă?
5. Ce rol joacă educația angajaților în promovarea importanței separării conturilor personale de cele afaceri?
6. Descrieți o situație în care eșecul de a separa conturile personale și de afaceri a dus la o breșă de securitate. Cum ar fi putut fi prevenit acest lucru?
7. Ce elemente sunt cruciale în implementarea unui sistem de conturi personale pentru fiecare angajat?
8. Cum poate implementarea sistemelor de cont personal să stabilească o responsabilitate clară pentru accesul la datele sensibile?
9. Ce strategii poate folosi o organizație pentru a urmări eficient activitățile utilizatorilor atunci când folosește un sistem de conturi personale pentru angajați?

Managementul securității cibernetice - Protecția endpoint-urilor și păstrarea datelor (MC 4.1.D.8)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul securității cibernetice - Protecția endpoint-urilor și păstrarea datelor **Cod: MC 4.1.D.8**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	EXPERT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.77, 4.1.78):

- Cunoașteți cum să implementați, să gestionați și să întrețineți soluții de protecție a punctelor terminale pentru protejarea dispozitivelor și a rețelelor individuale în fața amenințărilor de securitate.
- Practicați politici de păstrare a datelor pentru a vă asigura că datele sunt păstrate doar pe durata necesară, minimizând riscul expunerii datelor și impactul potențial al incidentelor de securitate cibernetică.

Descriere

În domeniul extrem de dinamic al securității cibernetice, protecția endpoint-utilor, cum ar fi laptopurile, smartphone-urile și alte dispozitive wireless, reprezintă o componentă crucială în apărarea activelor digitale ale unei organizații, în fața amenințărilor de securitate. În același timp, politicile solide de păstrare a datelor pot juca un rol esențial în reducerea la minimum a riscului expunerii datelor și a impactului potențial al incidentelor de securitate cibernetică. Pentru a naviga prin complexitățile acestor domenii de securitate cibernetică, există o nevoie critică de profesioniști abili în implementarea și menținerea soluțiilor de protecție a punctelor terminale și în practicarea unor politici eficiente de păstrare a datelor.

Acest MC este conceput pentru a oferi participanților o înțelegere cuprinzătoare a strategiilor și practicilor implicate în protejarea dispozitivelor și a rețelelor individuale în fața amenințările de securitate. De asemenea, își propune să îi înzestreze pe cursanți cu abilitățile necesare pentru a implementa în mod eficient politicile de păstrare a datelor, asigurându-se că datele sunt păstrate doar pe durata necesară, reducând astfel riscul expunerii datelor.

Modul: Implementarea și întreținerea soluțiilor de protecție a endpoint-urilot

Endpoint-urile, ca porți către rețeaua unei organizații, sunt ținte principale pentru atacurile cibernetice. Asigurarea securității acestor dispozitive este o sarcină complexă care necesită cunoștințe și abilități de specialitate. Prima parte a acestui curs este dedicată înțelegerii importanței protecției punctelor terminale și a învățării modului de implementare și de întreținere eficientă a soluțiilor de protecție a terminalelor. Participanții vor aprofunda diferite tipuri de soluții de protecție a punctelor terminale, de la software antivirus și anti-malware până la firewall-uri și sisteme de detectare a intruziunilor. Ei vor înțelege rolul pe care îl joacă fiecare tip de soluție în apărarea împotriva diferitelor tipuri de amenințări cibernetice și cum să selecteze soluțiile adecvate pentru nevoile lor organizaționale specifice. În plus, ei vor afla despre cele mai bune practici pentru menținerea acestor soluții, inclusiv actualizări regulate de software și corecții, monitorizare continuă și răspuns prompt la potențialele amenințări. Prin scenarii din lumea reală și studii de caz, participanții vor înțelege consecințele protecției insuficiente a endpoint-urilot și rolul critic al actualizărilor în timp util și al monitorizării continue în menținerea unei apărări robuste împotriva amenințărilor cibernetice.

Modul: Practicarea politicilor de păstrare a datelor

Un alt aspect vital al securității cibernetice este gestionarea ciclului de viață al datelor, în special perioada de timp în care datele sunt păstrate. A doua parte a cursului se concentrează pe politicile de păstrare a datelor și pe rolul acestora în reducerea riscului expunerii datelor. Participanții vor afla despre importanța păstrării datelor numai pe durata necesară și despre riscurile potențiale asociate cu păstrarea datelor mai mult decât este necesar. Aceștia vor analiza cerințele legale și de reglementare legate de păstrarea datelor și cum să le

încorporeze în politicile de păstrare a datelor ale organizației lor. În plus, participanții vor obține informații despre cele mai bune practici pentru implementarea și menținerea politicilor de păstrare a datelor, inclusiv audituri regulate, protocoale de ștergere automată a datelor și instruirea personalului. Ei vor înțelege rolul acestor politici în reducerea suprafeței pentru potențiale atacuri cibernetice și minimizarea impactului eventualelor incidente de securitate cibernetică.

La finalizarea acestui MC, participanții vor avea o bază solidă în două aspecte critice ale securității cibernetice: protecția punctelor terminale și păstrarea datelor. Ei vor dobândi cunoștințele și abilitățile necesare pentru a implementa și a menține soluții eficiente de protecție a punctelor terminale și politici de păstrare a datelor, sporind astfel securitatea dispozitivelor, rețelelor și datelor organizației lor. În plus, aceștia vor fi bine poziționați pentru a susține importanța acestor practici în cadrul organizației lor, promovând o cultură de conștientizare și responsabilitate în materie de securitate cibernetică.

Prin elemente teoretice, exerciții practice și studii de caz, acest curs va înzestra participanții cu abilitățile de a naviga cu încredere în peisajul securității cibernetice din ce în ce mai complex. Ei vor fi bine tregătiți pentru a identifica în mod proactiv potențialele vulnerabilități de securitate și pentru a implementa strategii pentru a le contracara în mod eficient, asigurând integritatea, confidențialitatea și disponibilitatea activelor informaționale ale organizației lor.

Finalizarea acestui MC va certifica competența participanților în protecția punctelor terminale și reținerea datelor, și va întări angajamentul lor de a rămâne la curent cu peisajul securității cibernetice în evoluție, făcându-i astfel o resursă de neprețuit pentru inițiativele de protecție a datelor ale organizației lor.

Întrebări

1. Care sunt componentele cheie ale unei soluții eficiente de protecție a endpoint-urilor? Cum funcționează aceste componente împreună pentru a proteja dispozitivele și rețelele individuale de amenințările de securitate?
2. Descrieți procesul de implementare a unei soluții de protecție a endpoint-urilor într-o organizație. Care sunt pașii implicați și care sunt factorii cheie de luat în considerare?
3. Cum pot contribui actualizările și corecțiile periodice (patches) la eficacitatea soluțiilor de protecție a punctelor terminale? Furnizați un exemplu real în care lipsa actualizărilor regulate a dus la o breșă a securității.
4. Explicați conceptul de politici de păstrare a datelor. Cum contribuie aceste politici la minimizarea riscului expunerii datelor?
5. Care este importanța stabilirii unei durate necesare pentru păstrarea datelor și care sunt riscurile potențiale ale păstrării datelor mai mult decât este necesar?
6. Cum influențează cerințele legale și reglementările politicile de păstrare a datelor? Dați un exemplu de reglementare care are impact asupra păstrării datelor și explicați cum.
7. Descrieți procesul de implementare a unei politici de păstrare a datelor în cadrul unei organizații. Care sunt pașii critici și ce provocări pot apărea în timpul implementării?
8. Cum poate practicarea unor politici eficiente de păstrare a datelor să minimizzez impactul potențial al incidentelor de securitate cibernetică? Oferiți un exemplu pentru a vă susține explicația.

Optimizarea browserului și gestionarea securității (MC 4.1.D.9)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Optimizarea browserului și gestionarea securității **Cod: MC 4.1.D.9**
Țara (Țările)/Regiunea (regiunile) emitentului	IRLANDA, ITALIA, CIPRU, GRECIA, ROMANIA http://dsw.projectsgallery.eu
Acordat de către organizația	Consorțiul DSW Număr proiect: **101087628**
Data emiterii	noiembrie 2023
Volumul de studiu necesar pentru a obține rezultatele învățării	Minim 3 – Maxim 8 ore
Nivelul certificat	EXPERT
Tipul de evaluare	Întrebări notate automat Număr de întrebări: 16 – 20 Scor de promovare: 75%
Forma de participare la activitatea de învățare	Asincron online
Modul de acreditare a cursului	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.1.79, 4.1.80):

- Optimizați-vă setările browser-ului și performanța pentru a îmbunătăți viteza și eficiența navigării.
- Personalizați setările de securitate ale browserului pentru a spori siguranța și confidențialitatea online.

Descriere

Browser-ul reprezintă interfața principală între utilizatori și Internet, oferind o poartă către cantități mari de informații și servicii. Ca atare, performanța și securitatea browser-ului pot influența semnificativ calitatea experienței online a unui utilizator. Prin urmare, este esențial pentru utilizatori să își optimizeze setările browser-ului pentru viteză și eficiență sporite, personalizând, de asemenea, setările de securitate pentru a promova siguranța și confidențialitatea online.

Aceat MC își propune să furnizeze participanții cunoștințele și abilitățile necesare pentru a optimiza setările browserului pentru îmbunătățirea vitezei și eficienței și pentru a personaliza setările de securitate pentru sporirea siguranței și confidențialității online. Cursul va acoperi toate aspectele legate de gestionarea browser-ului, de la înțelegerea diferitelor setări până la manipularea acestora, pentru a optimiza performanța și a spori securitatea.

Modul: Optimizarea browser-ului pentru viteză și eficiență sporite

În prima parte a cursului, participanții vor învăța despre numeroasele setări și caracteristici care pot afecta viteza și eficiența unui browser. Participanții vor aprofunda diferitele componente care influențează viteza de navigare, inclusiv gestionarea memoriei cache, controlul cookie-urilor și dezactivarea extensiilor inutile. Prin exerciții practice, cursanții vor învăța cum să ajusteze aceste setări pentru a optimiza performanța browserului și pentru a îmbunătăți experiența generală online. Importanța actualizărilor regulate ale browserului va fi, de asemenea, evidențiată, participanții învățând cum actualizările nu numai că oferă cele mai recente caracteristici și corecții de securitate, ci și îmbunătățesc adesea eficiența browserului. Exemplele din lumea reală vor sublinia și mai mult importanța actualizărilor regulate ale browserului și a gestionării adecvate a browser-ului pentru îmbunătățirea vitezei de navigare.

Modul: Personalizarea setărilor de securitate ale browser-ului pentru îmbunătățirea siguranței și a confidențialității

A doua parte a cursului se va axa pe setările de securitate ale browserului. Participanții vor învăța cum să personalizeze aceste setări pentru a spori siguranța și confidențialitatea online. De la înțelegerea rolului cookie-urilor în urmărirea online până la învățarea modului de implementare a diferitelor funcții de securitate, cum ar fi blocarea ferestrelor pop-up și navigarea privată, participanții vor dobândi o înțelegere profundă a setărilor de securitate ale browserului. Subiectele vor include, de asemenea, gestionarea parolelor salvate, activarea actualizărilor automate pentru corecțiile de securitate și înțelegerea conexiunilor securizate (HTTPS). Participanții vor învăța cum să gestioneze setările de confidențialitate pentru a controla cât de multe informații personale sunt partajate site-urilor web și cum să folosească modul incognito sau privat pentru confidențialitate suplimentară.

La finalul acestui MC, participanții vor înțelege modului de optimizare și gestionare a setărilor browserului

pentru îmbunătățirea vitezei, eficienței, siguranței și confidențialității. Cursanții vor putea să navigheze în mediul online cu mai multă încredere și control, asigurând o experiență de navigare sigură și eficientă.

Prin cunoștințe teoretice și exerciții practice, acest curs va permite participanților să înțeleagă nuanțele setărilor browserului și impactul acestora asupra vitezei, eficienței și securității. Aceștia vor obține, de asemenea, informații valoroase despre importanța gestionării browserului în contextul mai larg al siguranței și confidențialității online.

Finalizarea acestui MC va demonstra competența dobândită în optimizarea browserului și gestionarea securității. Cursul nu numai că le va îmbunătăți experiența online, ci le va furniza și abilitățile esențiale necesare în lumea digitală. Ei vor deveni cetățeni digitali mai competenți și responsabili, cunoscători în gestionarea interfeței lor online în mod eficient și în siguranță.

Întrebări

1. Care sunt câteva setări cheie care pot fi optimizate pentru a îmbunătăți viteza și eficiența unui browser? Dați exemple.
2. Cum influențează gestionarea memoriei cache performanța unui browser? Discutați despre implicațiile ștergerii memoriei cache a browserului asupra vitezei și eficienței navigării.
3. Care sunt riscurile potențiale asociate cu utilizarea setărilor implicite de securitate ale browserului? Cum poate personalizarea acestor setări să îmbunătățească siguranța și confidențialitatea online?
4. Descrieți rolul cookie-urilor în urmărirea online și în confidențialitate. Cum pot fi ajustate setările browserului pentru a gestiona cookie-urile în mod eficient?
5. Discutați despre importanța actualizărilor browserului atât în contextul optimizării performanței, cât și al securității. Dați un exemplu real în care lipsa actualizărilor browserului a dus la o încălcare a securității sau la scăderea performanței.
6. Cum poate afecta utilizarea extensiilor performanța și securitatea unui browser? Discutați câteva strategii pentru gestionarea eficientă a extensiilor.
7. Cum îmbunătățește navigarea privată sau modul incognito confidențialitatea online? În ce scenarii ar putea fi deosebit de benefic să utilizați această funcție?

DICȚIONAR DE TERMENI

MC – Microcredit (**M**icro-**c**redential)

LO – Rezultat al învățării (**L**earning **O**utcome)

K – Cunoștințe (**K**nowledge)

S – Aptitudini (Skills)

A – Atitudini (Attitudes)

UE – **U**niunea **E**uropeană

PC – Calculator personal (**P**ersonal **C**omputer)

Smartphone – Telefon inteligent

AI – Inteligență artificială (**A**rtificial **I**ntelligence)

Wi-Fi – Tehnologie de acces la internet fără fir (**WI**reless **FI**delity)

VPN – Rețea virtuală privată (Virtual Private Network)

HTTP – Protocol de transfer al hyper-text-ului (**H**yper**t**ext **T**ransfer **P**rotocol)

HTTPS – HTTP securizat (**H**ypertext **T**ransfer **P**rotocol **S**ecure)

e-mail – Poștă electronică (**e**lectronic **mail**)

2FA - Autentificarea cu 2 factori (Two-**F**actor **A**uthentication)

MFA - Autentificarea cu mai mulți factori (**M**ulti-**F**actor **A**uthentication)

PoLP – Accesul bazat pe cel mai mic privilegiu (**P**rinciple **o**f **L**east **P**rivilege)

RBAC – Accesul bazat pe roluri (**R**ole-**B**ased **A**ccess **C**ontrol)

GDPR – Reglementări generale privind protecția datelor (**G**eneral **D**ata **P**rotection **R**egulation)

WPS – Setare protejată a Wi-Fi-ului (**W**i-Fi **P**rotected **S**etup)

FTP – Protocol pentru transferul fișierelor (**F**ile **T**ransfer **P**rotocol)

SFTP – Protocol pentru transferul securizat al fișierelor (**S**ecure **F**ile **T**ransfer **P**rotocol)

IP – Protocol Internet (**I**nternet **P**rotocol)

DNS – Sistemul de nume al domeniului (***D**omain **N**ame **S**ystem)*

2FA - Autentificarea cu 2 factori (Two-**F**actor **A**uthentication)

MFA - Autentificarea cu mai mulți factori (**M**ulti-**F**actor **A**uthentication)

Jailbreaking-ul (pentru dispozitivele iOS) sau rooting-ul (pentru dispozitivele Android) - Procesul de eliminare a restricțiilor impuse de producător asupra sistemului de operare al dispozitivului. Acest lucru permite utilizatorilor să instaleze software neautorizat și să personalizeze dispozitivul în moduri care nu sunt oficial permise.

Juice jacking – Atac cibernetic care implică accesul neautorizat și manipularea dispozitivelor prin porturile de încărcare USB.

Atac de tip brute-force – Atac în care care hackerii încearcă automat o serie de combinații pentru a ghici o parolă

Endpoint - Orice dispozitiv care se conectează la o rețea, cum ar fi computere desktop, laptopuri, telefoane mobile, tablete și servere

Phishing - Tip de atac cibernetic proiectat să inducă oamenii în eroare pentru a dezvălui informații confidențiale.

DOMENIUL DE COMPETENȚĂ: SIGURANȚĂ

DOMENIUL COMPETENȚEI: SIGURANȚĂ (4)		
COMPETENȚĂ: PROTECTIA DISPOZITIVELOR (4.1)		
1	La nivel elementar și cu indrumare, eu pot să:	• **identific** moduri simple de a proteja dispozitivele și conținutul digital • **diferențiez** riscuri simple și amenințări în mediile digitale • **aleg** măsuri simple de siguranță și securitate • **identific** moduri simple de a avea în vedere fiabilitatea și confidențialitatea
2	La nivel elementar, autonom și cu îndrumări adecvate acolo unde este necesar, eu pot să:	• **identific** moduri simple de a proteja dispozitivele și conținutul digital • **diferențiez** riscuri simple și amenințări în mediile digitale • **urmez** măsuri simple de siguranță și securitate • **identific** moduri simple de a avea în vedere fiabilitatea și confidențialitatea
3	Pe cont propriu și rezolvând probleme simple, eu pot să:	• **indic** moduri bine definite și de rutină, pentru protejarea dispozitivelor mele și a conținutului digital • **diferențiez** riscuri bine definite și de rutină și amenințări din mediile digitale • **selectez** măsuri de siguranță și securitate, bine definite și de rutină. • **indic** moduri bine definite și de rutină, pentru a avea în vedere fiabilitatea și confidențialitatea
4	Independent, în conformitate cu nevoile mele proprii și rezolvând probleme bine-definite, care nu sunt de rutină, eu pot să:	• **organizez** moduri prin care să protejez dispozitivele mele și conținutul digital • **diferențiez** riscurile și amenințările din mediile digitale • **selectez** măsuri de siguranță și de securitate • **explic** moduri de a avea în vedere fiabilitatea și confidențialitatea
5	Îndrumând alte persoane, eu pot să:	• **aplic** diferite moduri de a proteja dispozitivele și conținutul digital • **diferențiez** o varietate de riscuri și amenințări în mediile digitale • **aplic** măsuri de siguranță și de securitate • **utilizez** diferite moduri de a avea în vedere fiabilitatea și confidențialitatea

6	La nivel avansat, în funcție de nevoile mele și ale altora, și în contexte complexe, eu pot să:	• **aleg** cea mai adecvată protecţie pentru dispozitive și conţinutul digital • **deosebesc** riscurile și amenințările din mediile digitale • **aleg** cele mai adecvate măsuri de siguranță și de securitate • **evaluez** cele mai adecvate moduri de a avea în vedere fiabilitatea și confidențialitatea
7	La nivel înalt de specializare, eu pot să:	• **creez soluții la probleme complexe** cu definiție limitată, care sunt legate de protecția dispozitivelor și a conţinutului digital, de gestionarea riscurilor și a amenințărilor, de aplicarea măsurilor de siguranță și de securitate, și de fiabilitate și de confidențialitate în mediile digitale • **integrez** cunoştinţele mele pentru a contribui la practica și cunoștințele profesionale, și pentru a-i ghida și pe alții în protejarea dispozitivelor
8	La cel mai avansat și specializat nivel, eu pot să:	• **creez soluții pentru a rezolva probleme complexe** cu mulți factori care interacționează, probleme legate de protejarea dispozitivelor și a conţinutului digital, de gestionarea riscurilor și a amenințărilor, de aplicarea măsurilor de siguranță și de securitate, și de fiabilitate și de confidențialitate în mediile digitale • **propun noi** idei și procese în acest domeniu de competență

INTRODUCERE:

Inițierea în siguranță și securitate cuprinde aptitudinile și cunoştinţele necesare la protecția dispozitivelor, a conţinutului digital, și a datelor personale, și înţelegerea riscurilor și a amenințărilor prezente în mediile digitale. În lumea interconectată de astăzi, în care tehnologia este omniprezentă, cultivarea practicilor de siguranță digitală este esențială pentru a te proteja pe tine și pe alții de potențialele atacuri.

La nivel elementar, cu indrumare, cursanții pot identifica moduri simple de a-și proteja dispozitivele și conţinutul digital. Cursanții vor aplica practicile de a folosi parole sigure şi vor recunoaște importanța a folosind diferite puternice parole pentru variat servicii on-line. Ei vor putea diferenția riscuri elementare și amenințări în mediile digitale, cum ar fi furtul de identitate, escrocherii și atacurile malware. În plus, ei vor învăța să aleagă măsuri simple de siguranță și securitate și să conștientizeze importanța confidențialității și a fiabilității.

Pe măsură ce cursanții avansează spre nivelul intermediar, ei câștigă autonomie și pot urma, în mod independent, măsuri simple de siguranță și securitate. Ei înțeleg importanța de a-și menține dispozitivele și aplicațiile actualizate, la zi, pentru a atenua vulnerabilitățile de securitate. Mai mult, ei învață despre autentificarea cu doi factori și îmbunătățește aceasta protecţia lor digitală.

Avansând la nivelul intermediar, cursanții pot indica modalități bine definite și de rutină pentru a-și proteja dispozitivele și conținutul digital. Ei pot discerne riscuri bine definite și de rutină și amenințările din mediile digitale. Ei selectează și aplică măsuri de siguranță și securitate bine definite și de rutină. Ei inteleg importanţa criptării datelor sensibil și pot răspunde în mod corespunzător la breșele de securitate.

La nivelul avansat, cursanţii demonstrează o deplină înţelegere a măsurilor de siguranță și securitate digitală. Ei pot aplica metode variate pentru a-și proteja, în mod eficient, dispozitivele și conținutul digital. Cursanții diferențiază o gamă largă de riscuri și amenințări în mediile digitale și folosesc, în consecinţă, măsurile adecvate de siguranță și securitate. În plus, ei vor stăpâni cunoştinţele necesare pentru a-i ghida și pe alții în adoptarea practicilor de protecţie.

La cel mai înalt nivel de specializare, cursanții vor putea crea soluții inovative la probleme complexe privind protejarea dispozitivelor, gestionarea riscurilor și a amenințărilor, și aplicarea măsurilor de siguranță și securitate în mediile digitale. Expertiza dobândită le va permite să contribuie la practicile și cunoştinţele profesionale; cursanții vor deveni, astfel, resurse valoroase pentru îndrumarea altora în a-și proteja dispozitivele și conţinutul digital.

În final, la cel mai avansat nivel de specializare, cursanţii vor fi capabili să conceapă soluții sofisticate pentru problemele complexe, cu mai multe fațete, din siguranța și securitatea digitale. Cursanții vor putea propune idei inovatoare și procese, pentru a îmbunătăți domeniul, promovând practici de protecţie de

ultimă oră.
În diverse cazuri de utilizare - scenarii din lumea reală, cursanții vor exersa practic inițierea în siguranța și securitatea digitală. Ca urmare, un astfel de angajat va putea să securizeze conturile de social media ale corporației în care lucrează, să detecteze și să abordeze riscurile, să-și instruiască colegii în cela mai bune practici. În mediul educațional, va putea să mențină în siguranță platformele digitale de învățare, să identifice potenţialele amenințări, și să-și ajute colegii să navigheze în condiții de siguranță pe aceste platforme.

CERINȚE PRELIMINARE

1. Cunoştinţe elementare despre Internet, incluzând funcțiile lui și cum facilitează acesta schimburile de date între calculatoare.
2. Înţelegerea importanței unor parole puternice împreună cu cunoștințe despre modul de gestionare și protejare a acestora în siguranță.
3. Cunoştinţe despre practicile online sigure, cum ar fi evitarea utilizării Wi-Fi-lor publice când realizează activități sensibile sau precauția în partajarea informațiilor personale pe net.
4. Conștientizarea autentificării cu doi factori și cum le permite aceasta să sporeascp securitatea conturilor online.
5. Cunoştinţe elementare în organizarea și gestionarea în siguranță a conţinutului digital și a fișierelor.

ANEXĂ - COMPETENȚA 4.1. – PROECȚIA DISPOZITIVELOR

DOMENIUL DE COMPETENȚĂ: SIGURANȚĂ (4) COMPETENȚĂ: PROTECȚIA DISPOZITIVELOR (4.1)			
Rezultatele învățării	Nivel	K – S - A	Explicaţie
1. Recunoașteți importanța utilizării parolelor unice pentru diferite conturi online, pentru sporirea securității.	L1	K	Înțelegeți că utilizarea de parole puternice, diferite, pentru fiecare cont, contribuie la reducerea riscului de compromitere a mai multor conturi în cazul în care o parolă este expusă. Înțelegeți că având parole unice și puternice pentru fiecare cont, se reduce probabilitatea ca numeroase conturi să fie compromise în cazul în care o parolă devine publică.
2. Promovați o atitudine de vigilență și de conștientizare a mediului înconjurător	L1	A	Încurajând indivizii să fie conștienți de mediul înconjurător, cursanții vor dezvolta o atitudine de vigilență și atenție la potențiale riscuri sau amenințări din mediul digital. Această conștientizare sporită poate contribui la siguranța și securitatea personală, permițând indivizilor să răspundă în mod corespunzător la orice situații sau pericole neașteptate pe care le pot întâlni.
3. Identificați semnele comune ale încercărilor de phishing și învățați cum să evitați să deveniți victima unor astfel de escrocherii.	L1	K - S	Recunoașteți e-mailurile, mesajele sau site-urile web suspecte care ar putea încerca să vă înșele pentru a dezvălui informații personale sau credențiale de conectare.
4. Recunoașteți e-mailurile, mesajele sau site-urile web suspecte care ar putea încerca să vă înșele pentru a dezvălui informații personale sau credențiale de conectare.	L1	K	Enumerați avantajele instalării unui software antivirus de încredere pentru a detecta și elimina programele dăunătoare de pe dispozitivele dvs.
5. Aplicați abilitățile de a vă securiza dispozitivul când acesta este nesupravegheat.	L1	S	Învățând să aplice abilitățile de a-și securiza dispozitivele atunci când acestea sunt nesupravegheate, cursanții pot lua măsuri proactive pentru a preveni accesul neautorizat sau utilizarea necorespunzătoare. Câteva măsuri pot fi blocarea dispozitivului cu o parolă, PIN sau autentificare biometrică, activarea blocării automate a ecranului atunci când dispozitivul este inactiv și precauția de a lăsa dispozitivele în locuri publice. Implementarea acestor măsuri ajută la protejarea datelor sensibile și asigură că dispozitivul rămâne în siguranță de potențiale amenințări de securitate atunci când dispozitivul este nesupravegheat.

6. Descrieți importanța securizării rețelelor de acasă prin parole puternice și protocoale de criptare.	L1	K	Explicați în ce mod setarea unor parole Wi-Fi puternice parola și activarea protocoalelor de criptare ajută la împiedicane accesului neautorizat la rețeaua dvs.
7. Identificați riscurile asociate cu folosirea retelelor Wi-Fi publice	L1	K - S	Recunoaşteți că retelele Wi-Fi publice pot fi nesigure; de aceea, folosirea parolelor în rețelele Wi-Fi publice este de evitat.
8. Descrieți modul în care revizuirea și ajustarea setărilor de confidențialitate poate ajuta la controlul informațiilor partajate pe dispozitive și conturi online.	L1	K	Explicați importanța verificării și actualizării regulate a setărilor de confidențialitate pentru a gestiona informațiile personale partajate cu aplicațiile și serviciile.
9. Enumerați potențialele amenințări reprezentate de riscurile digitale și importanța de a rămâne informați cu privire la securitatea cibernetică.	L1	K	Enumerați diferitele tipuri de riscuri digitale, cum ar fi phishingul, programele malware și ingineria socială și necesitatea de a rămâne informat pentru a vă proteja împotriva acestora.
10. Descrieți pașii pe care trebuie să îi urmați, dacă un dispozitiv este pierdut sau furat, pentru a vă proteja datele personale și confidențialitatea.	L1	K - S - A	Când un dispozitiv este pierdut sau furat, acțiunea imediată protejează informațiile sensibile. Persoana trebuie mai întâi să raporteze furtul la poliție și apoi să utilizeze funcțiile de blocare de la distanță pentru a securiza dispozitivul; trebuie să schimbe rapid parolele pentru conturile accesibile pe dispozitiv, folosind instrumente de urmărire pentru a încerca locația. Informarea persoanelor aflate la contactele personale și profesionale vă ajută să vă protejați împotriva comunicării neautorizate; puteți face o reclamație la asigurator. Viteza este esențială pentru a minimiza daunele potențiale.
11. Recunoașteți importanța dezactivarii serviciilor de rețea inutile și a programelor din fundal (background) de pe dispozitivele Dvs., pentru a reduce potențialele suprafețe de atac.	L2	K	Înțelegeți că dezactivarea serviciilor de rețea inutile și a programelor din fundal (background) pot ajuta la minimizarea riscului de vulnerabilități de securitate.

12. Fiți atenți la securitatea dispozitivului fizic, în special în locuri publice, pentru a preveni furtul și accesul neautorizat	L2	S	Dezvolta-ți-vă obiceiul de a fi atenți la securitatea dispozitivelor Dvs. mobile și de a le ține sub observație în locuri publice, pentru a descuraja furtul.
13. Aplicați practici sigure de partajare a ecranului în timpul întâlnirilor virtuale sau a colaborărilor la distanță, pentru a proteja informațiile sensibile de accesul sau expunerea neautorizate	L2	S	Pentru a preveni accesarea sau expunerea informațiilor sensibile către părți neautorizate în timpul întâlnirilor virtuale sau al colaborărilor de la distanță, este esențial să urmați procedurile de partajare securizată a ecranului. Vă puteți asigura că numai publicul vizat poate vedea conținutul partajat și să evitați orice potențiale încălcare a confidențialității sau a datelor prin utilizarea procedurilor sigure de partajare a ecranului. Acest lucru poate presupune utilizarea unor platforme de întâlnire securizate cu restricții încorporate de partajare a ecranului, alegerea conținutului pe care să-l prezinte cu precauție și urmărirea cine are acces la ecranul partajat. Puteți păstra confidențialitatea datelor dvs. sensibile, păstrați integritatea acestora și preveniți ca acestea să ajungă în mâini greșite, respectând aceste măsuri de siguranță.
14. Cunoașteți importanța revizuirii și a eliminării periodice a informațiilor Dvs. Personale, stocate în bazele de date din rețelele sociale, pentru a vă proteja confidențialitatea conținutului digital	L2	K	Fiți conștienți de necesitatea de a verifica și gestiona în mod regulat informațiile personale stocate în conturile de pe rețele sociale, pentru a menține confidențialitatea.
15. Implementați controale parentale și software-uri de filtrare pentru a proteja copiii de conținutul neadecvat și de riscurile online	L2	S	Configurați controlul parental și software-ul de filtrare atunci când este necesar, pentru a crea un mediu online mai sigur pentru copii.

16. Înțelegeți riscurile asociate cu descărcarea de programe sau aplicații din surse neoficiale sau terțe	L2	K	Cunoașteți că descărcarea din surse neoficiale poate expune dispozitivul dvs. la riscuri de software rău intenționat și de securitate.
17. Evitați utilizarea dispozitivelor afectate de jailbreaking sau rooting, deoarece aceste metode pot ocoli măsurile de securitate și pot compromite siguranța datelor Dvs.	L2	S	Alegeți să nu utilizați dispozitive cu jailbreaking sau rooting, pentru a menține integritatea caracteristicilor de securitate ale dispozitivului.
18. Cunoașteți importanța ștergerii și aruncării în siguranță a dispozitivelor vechi pentru a preveni recuperarea datelor dvs. de către alții	L2	K	Înțelegeți necesitatea de a șterge corect datele de pe dispozitivele vechi pentru a asigura confidențialitatea datelor.
19. Utilizați criptarea pentru a proteja datele sensibile de pe dispozitivele dvs., în special pentru datele stocate pe dispozitive mobile și stocarea în masă amovibilă.	L2	S	Implementați programe de criptare pentru a proteja datele sensibile, acordând o atenție deosebită dispozitivelor mobile și a dispozitivelor de memorare externă.
20. Înțelegeți riscurile asociate cu transmiterea sau stocarea informațiilor personale pe dispozitive și potențialul de încălcare a datelor	L2	K	Fiți conștient că stocarea informațiilor sensibile, cum ar fi detaliile cardului de credit sau numerele de asigurări medicale din UE, pe dispozitive, vă poate expune la furtul de identitate dacă dispozitivul este compromis.

21. Gestionați cu precauție linkurile suspecte și evitați descărcarea fișierelor din surse necunoscute pentru a vă proteja dispozitivele de potențialele amenințări malware.	L3	S - A	Înțelegeți riscurile asociate cu click-ul pe link-uri suspecte și descărcarea fișierelor din surse nesigure.
22. Realizați cât este de important să realizați periodic de copii de rezervă ale datelor (data backup) pentru a vă proteja împotriva pierderii datelor și/sau a defectării dispozitivului.	L3	K	Înțelegeți că efectuarea regulată a copiilor de siguranță a fișierelor asigură faptul că datele importante sunt în siguranță și pot fi recuperate în cazul unor evenimente neașteptate.
23. Învățați că dispozitivele pierdute sau furate pot fi urmărite, blocate sau șterse, folosind instrumente bazate pe web, disponibile gratuit	L3	K	Rețineți că dispozitivele vin cu instrumente încorporate, care vă pot ajuta să le urmăriți și să le securizați de la distanță sau să ștergeți datele în cazul pierderii sau furtului dispozitivului.
24. Utilizați cu pricepere funcțiile de urmărire, de blocare și de ștergere pentru a vă proteja datele și confidențialitatea, în cazul în care dispozitivul este pierdut sau furat	L3	S	Utilizați funcțiile de urmărire, blocare și ștergere a dispozitivului, în mod eficient, pentru a proteja informațiile sensibile în cazul pierderii dispozitivului.

25. Înțelegeți importanța deconectarii la sfârșitul sesiunilor dvs. de internet sau la terminarea lucrului în aplicații, pentru a vă proteja informațiile personale împotriva accesului neautorizat.	L3	K	Rețineți că deconectarea după utilizarea serviciilor online vă asigură că conturile dvs. rămân în siguranță și datele dvs. sunt protejate.
26. Înțelegeți cum să gestionați permisiunile aplicațiilor pentru a vă proteja confidențialitatea și fiți conștienți de datele colectate de aplicațiile de pe dispozitivele dvs.	L3	S	Utilizați permisiunile aplicațiilor în mod judicios și citiți cu atenție termenii și condițiile înainte de acceptarea acestora.
27. Practicați deprinderile de navigare în siguranță, cum ar fi evitarea site-urilor web suspecte și utilizarea conexiunilor HTTPS, pentru a reduce riscul de malware și furtul de date.	L3	S	Implementați practici de navigare sigură pentru a proteja dispozitivele și datele, de potențialele amenințări cibernetice, în timpul lucrului online
28. Recunoașteți importanța menținerii dispozitivelor în siguranță din punct de vedere fizic, în special în locuri publice, pentru a preveni furtul și accesul neautorizat.	L3	K	Recunoașteți necesitatea de a fi vigilenți cu privire la securitatea dispozitivului și de a păstra dispozitivele la vedere pentru a evita potențialele furturi sau manipulări.
29. Identificați riscurile potențialului de furt de date sau instalării de malware atunci când utilizați stațiile publice de încărcare.	L3	K - S	Fiți conștienți de potențialele riscuri de securitate atunci când utilizați stațiile publice de încărcare și luați măsuri de precauție pentru a proteja dispozitivele de astfel de riscuri.

30. Fiți capabil să implementați un manager de parole pentru a stoca și a genera în siguranță parole complexe, pentru diferite conturi online, reducând riscul de încălcare a securității legate de parole.	L3	S	Utilizați un instrument de gestionare a parolelor (un manager de parole/password manager tool) pentru a genera și gestiona parole puternice și unice pentru fiecare cont online, sporind securitatea generală.
31. Implementați caracteristici de securitate specifice dispozitivului, cum ar fi autentificarea biometrică sau criptarea dispozitivului, pentru a îmbunătăți protecția datelor sensibile.	L4	S	Configurați autentificarea biometrică sau criptarea dispozitivului pentru a consolida securitatea dispozitivului și pentru a proteja informațiile personale.
32. Înțelegeți riscurile utilizării pe dispozitivele Dvs. a unor software-uri învechite sau neacceptate și importanța actualizării sau înlocuirii unui astfel de software pentru a menține securitatea.	L4	K	Fi conștient de cel Securitate riscuri pozat de folosind învechit software și cel nevoie la Actualizați sau a inlocui aceastacu versiuni acceptate. Fiți conștienți de riscurile de securitate care apar la utilizarea software-ului învechit și de necesitatea actualizării sau înlocuirii acestuia cu versiuni acceptate.
33. Identificați activitățile suspecte de pe dispozitivele dvs., cum ar fi ferestrele pop-up neașteptate sau descărcarea neobișnuită a bateriei; acestea pot indica potențiale malware sau încălcări de securitate.	L4	K - S	Recunoașteți semnele unui dispozitiv care a fost compromis și luați măsurile necesare pentru a aborda potențialele amenințări de securitate.

34. Evaluați caracteristicile de securitate ale diferitelor dispozitive și alegeți cele mai sigure opțiuni, în funcție de nevoile și cazurile de utilizare specifice.	L4	A	Atunci când doriți să faceți o achiziție, cercetați cu atenție caracteristicile de securitate inerente ale dispozitivului. Evaluați standardele de criptare, mecanismele de autentificare și frecvența actualizărilor de securitate. Reflectați asupra cerințelor dvs. unice: aveți nevoie de verificare biometrică avansată sau de autentificare cu mai mulți factori? De asemenea, luați în considerare feedback-ul din partea experților în tehnologie și a utilizatorilor obișnuiți. Echilibrarea securității cu nevoile dumneavoastră specifice asigură protecție și funcționalitate optime. Siguranța datelor dvs. depinde de alegerile informate.
35. Recunoașteți importanța revizuirii și gestionării periodice a permisiunilor aplicațiilor, pentru a limita accesul la datele personale și pentru a proteja confidențialitatea.	L4	K	Revizuirea și gestionarea în mod regulat a permisiunilor pentru aplicații crucială. Fiind proactiv, puteți preveni accesul neautorizat la date, păstrându-vă confidențialitatea. Verificările periodice asigură că sunt acordate numai permisiunile esențiale, minimizând riscurile. De exemplu, o aplicație pentru notițe are nevoie de locația dvs.? Probabil că nu. Limitând accesul inutil, nu numai că protejați informațiile sensibile, dar și sporiți apărarea dispozitivului împotriva potențialelor încălcări. Proteja-ți-vă confidențialitatea, fiind vigilenți.
36. Extindeți măsurile de securitate a dispozitivului Dvs. pentru a include medii de lucru la distanță, asigurând protecția datelor și canale de comunicare securizate.	L4	KS	Lucrul în afara mediilor tradiționale de birou poate expune datele sensibile la noi amenințări. Pentru a vă adapta, asigurați-vă conexiuni criptate, în special când sunteți conectat la un Wi-Fi public. Actualizați în mod regulat și faceți backup pentru date. Folosiți parole puternice, unice, și activați autentificarea cu doi factori atunci când este posibil. Limitați accesul la dispozitiv doar pentru personalul necesar și instalați software de securitate fiabil. În setările de la distanță, securitatea proactivă a dispozitivului este crucială pentru a proteja informațiile vitale.
37. Promovați conștientizarea securității în rândul colegilor sau al membrilor familiei, educându-i cu privire la cele mai bune practici pentru securitatea dispozitivelor și a comportamentul online sigur.	L4	A	Promovați conștientizarea securității dispozitivelor și încurajați un comportament online responsabil în rândul colegilor sau al membrilor familiei.

38. Recunoașteți potențialele riscuri legate de deschiderea arhivelor zip sau rar provenite din surse necunoscute sau care nu sunt de încredere.	L4	K	Evitați să deschideți atașamente de e-mail sau să descărcați fișiere de pe site-uri web dacă nu aveți încredere în expeditor sau în sursă. Acest lucru previne riscul de a descărca arhive zip sau rar periculoase sau care ar putea conține software dăunător sau viruși.
39. Dezvoltați obiceiul de a vă asigura siguranța suporturilor hardware portabile și a dispozitivelor șterse, evitând să aveți încredere în dispozitivele sau conținuturile media nesigure.	L4	A	Înainte de a utiliza o unitate flash USB sau un hard disk extern, inspectați-l vizual pentru orice deteriorare fizică sau pentru alte semne suspecte. De asemenea, luați în considerare scanarea conținutului media cu un software antivirus de încredere, pentru a preveni răspândirea potențialelor amenințări de securitate pe dispozitivele dvs.
40. Explicați riscurile asociate descărcării de aplicații care provin din surse necunoscute și importanța utilizării magazinelor oficiale de aplicații.	L4	K	Descărcarea aplicațiilor din surse necunoscute vă poate expune dispozitivul la programe malware dăunătoare.
41. Evaluați și comparați diferite soluții software de securitate, cum ar fi programe antivirus și firewall-uri, pentru a le selecta pe cele mai eficiente pentru dispozitivul și nevoile dvs. specifice.	L5	S	Cercetați și comparați diferite programe antivirus pe baza caracteristicilor, a recenziilor și a eficacității acestora, pentru a le alege pe cele mai potrivite pentru calculatorul Dvs.

42. Evitați să utilizați informații sensibile sau ușor de urmărit/detectabile în parole, pentru a le spori puterea și securitatea.	L5	A	Încurajați prietenii și colegii să creeze parole puternice care nu includ informații ușor de ghicit, cum ar fi zile de naștere, nume sau expresii obișnuite.
43. Înțelegeți importanța evitării utilizării cuvintelor din dicționar sau a tiparelor/pattern-lor comune în parole, pentru a preveni atacurile de tip “brute force”	L5	K	Rețineți că utilizarea cuvintelor simple din dicționar sau a modelelor/tiparelor previzibile în parole le poate face vulnerabile la instrumentele automate de spargere a parolelor.
44. Recunoașteți riscul utilizării aceleiași parole pentru mai multe conturi și importanța utilizării parolelor unice pentru fiecare cont.	L5	K	Generați parole puternice care conțin un amestec de litere mari și mici, numere și caractere speciale, pentru fiecare dintre conturile dvs.
45. Recunoașteți importanța actualizării periodice a parolelor și evitați reutilizarea parolelor vechi.	L5	K	Rețineți că schimbarea regulată a parolelor ajută la atenuarea riscurilor asociate cu potențialele încălcări ale datelor sau cu conturile compromise.
46. Utilizați cu pricepere un program de compresie pe dispozitivul Dvs., pentru a reduce volumul de date, asigurând memorarea și transmisia eficientă.	L5	S	Implementați un algoritm de compresie pentru a reduce dimensiunea datelor, facilitând memorarea și partajarea informațiilor.

47. Fiți capabil să configurați setările dispozitivului pentru a se bloca sau deconecta automat după o perioadă de inactivitate, pentru a preveni accesul neautorizat.	L5	S	Setați smartphone-ul sau laptopul Dvs. să se blocheze automat după o scurtă perioadă de inactivitate, pentru a vă proteja datele de privirile indiscrete.
48. Cunoașteți riscurile utilizării funcțiilor de conectare automată pentru site-urile web sau în aplicațiile care memorează informații personale	L5	K	Înțelegeți că activarea funcțiilor de conectare automată poate economisi timp, dar poate reprezenta un risc de securitate în cazul în care cineva obține accesul fizic la dispozitiv.
49. Utilizați metode securizate pentru transferul fișierelor, cum ar fi SFTP sau memorarea securizată în cloud, pentru a transfera fișiere sensibile între dispozitive.	L5	A	Încurajați colegii sau prietenii să folosească metode sigure de transfer ale fișierelor, pentru a partaja documente confidențiale, fără a le compromite securitatea
50. Recunoașteți riscurile potențiale ale utilizării de software sau aplicații necunoscute pe dispozitivele dvs.	L5	S	Când întâlniți un nou software sau o aplicație cu care nu sunteți familiarizat, este esențial să fiți precaut și să luați în considerare consecințele potențiale, înainte de a o instala pe dispozitiv. Utilizarea unui software necunoscut poate prezenta mai multe riscuri pentru securitatea și funcționalitatea dispozitivului Dvs. Unele dintre aceste riscuri includ programe malware, modificări nedorite, probleme de confidențialitate, etc.
51. Recunoașteți importanța dezactivării Bluetooth pe dispozitivele Dvs., atunci când nu sunt utilizate	L6	K	Înțelegeți că dezactivarea Bluetooth-ului atunci când acesta nu este necesar vă ajută să reduceți potențialele riscuri de securitate și să economisiți durata de viață a bateriei pe dispozitivul Dvs.
52. Fiți capabil să efectuați scanări de viruși pe dispozitive de memorare externe	L6	KS	Dobândiți cunoștințele și abilitățile necesare pentru a scana de viruși dispozitivele de memorare externe, cum ar fi unități USB sau hard disk-uri. Procedând astfel, puteți identifica și elimina potențialii viruși sau programe malware care pot fi prezenți pe mediile de stocare, protejându-vă dispozitivele de posibile infecții și de coruperea datelor.

53. Înțelegeți importanța instruirii angajaților cu privire la tehnicile de securitate IT	L6	KA	Dețineți cunoștințele și abilitatea de a conduce cursuri de formare în domeniul securității IT pentru angajați. Astfel, le puteți transmite cunoștințele și abilitățile esențiale pentru a identifica și a răspunde eficient la amenințările de securitate cibernetică. Această instruire dă putere angajaților să adopte cele mai bune practici, să protejeze informațiile sensibile și să contribuie la un mediu de lucru mai sigur.
54. Dezvoltați măsuri cuprinzătoare de securitate fizică pentru a proteja activele organizaționale	L6	A	Cu cunoștințele dumneavoastră despre principiile de securitate fizică, veți proiecta și implementa măsuri de securitate robuste pentru a proteja activele fizice ale organizației, inclusiv clădirile, echipamentele și informațiile sensibile. Aplicându-vă abilitățile, puteți efectua evaluări ale riscurilor, puteți instala sisteme de control al accesului, camere de supraveghere și sisteme de alarmă, precum și să stabiliți proceduri sigure de intrare și ieșire. Această abordare proactivă va asigura protecția infrastructurii fizice a organizației față de accesul neautorizat, furt, vandalism și alte amenințări fizice. Promovând conștientizarea securității în rândul angajaților și al părților interesate, creați un mediu de lucru mai sigur, atenuând riscurile potențiale și îmbunătățiți postura generală de securitate a organizației.
55. Fiind conștienți de importanța conceptului de autentificare în doi factori (2FA) și de rolul acestui tip de autentificare în furnizarea unui nivel suplimentar de protecție pentru conturile online.	L6	A	Descrieți modul în care 2FA adaugă un nivel suplimentare de securitate a parolelor, care ce îngreunează accesul persoanelor neautorizate la conturi.
56. Diagnosticați și depanați problemele de securitate pe dispozitivele dvs., identificând eventualele programe malware sau încercările de acces neautorizat.	L6	S	Investigați și rezolvați cu pricepere incidentele de securitate pentru a vă proteja dispozitivele de potențiale amenințări.
57. Înțelegeți potențialele pericole ale stocării parolelor în browserele web și importanța utilizării instrumentelor dedicate de gestionare a parolelor.	L6	K	Rețineți că stocarea parolelor în browserele web poate să nu fie la fel de sigură ca utilizarea aplicațiilor de gestionare a parolelor.

58. Elaborați un plan personal de conștientizare a securității cibernetice pentru a rămâne informat cu privire la amenințările actuale și pentru a adopta cele mai bune practici pentru a proteja dispozitivele și datele personale.	L6	A	Creați un plan personalizat de securitate cibernetică pentru a fi la curent cu amenințările și pentru a proteja dispozitivele și datele personale.
59. Instalați pe dispozitivele personale software antivirus și anti-malware recunoscut, pentru a detecta și elimina potențialele amenințări.	L6	S	Asigurați-vă securitatea dispozitivelor personale prin instalarea și actualizarea regulată a software-lui antivirus și anti-malware recunoscute. Acest software va scana în mod activ dispozitivele pentru potențiale amenințări, cum ar fi viruși, programe malware și alte programe rău intenționate. Dacă sunt detectate amenințări, software-ul le va elimina imediat, protejându-vă dispozitivele și datele de pericole. Actualizările regulate asigură că software-ul dumneavoastră antivirus și anti-malware poate detecta și combate în mod eficient cele mai recente și emergente amenințări, oferindu-vă o apărare puternică împotriva potențialelor riscuri de securitate cibernetică.
60. Implementați controale de acces pentru a reglementa și a restricționa intrarea în sisteme, conturi sau profiluri personale, asigurând o mai bună securitate și confidențialitate	L6	S	Prin folosirea controalelor de acces, puteți gestiona și limita cine are permisiunea de a vă accesa sistemele, conturile sau profilurile personale. Acest lucru ajută la protejarea informațiilor sensibile și previne accesul persoanelor neautorizate. Utilizând tehnici precum parolele, autentificarea cu doi factori și controlul accesului bazat pe roluri, puteți îmbunătăți securitatea generală a activelor Dvs. digitale. Controlul accesului minimizează, de asemenea, riscul de încălcare a datelor, furtul de identitate și utilizarea neautorizată a informațiilor personale. În consecință, mențineți un nivel mai ridicat de confidențialitate, integritate și disponibilitate a resurselor Dvs., întărindu-vă apărarea în securitatea cibernetică.
61. Înțelegeți importanța organizării anuale a unor cursuri de formare pentru conștientizare a personalului cu privire la securitatea cibernetică	L7	K - S - A	Demonstrați cunoștințele, abilitățile și atitudinea de a organiza și a desfășura sesiuni anuale de formare a personalului, axate pe securitatea cibernetică. Prin desfășurarea acestor sesiuni de instruire, vă asigurați că toți angajații sunt educați cu privire la cele mai recente amenințări de securitate cibernetică, cele mai bune practici și politicile companiei. Acest lucru ajută la creșterea gradului de conștientizare în rândul membrilor personalului, dându-i puterea să recunoască potențiale riscuri, să evite capcanele comune și să contribuie în mod activ la un mediu de lucru sigur și vigilent. Cursurile regulate de formare și conștientizare a personalului sporesc importanța securității cibernetice în cadrul organizației și promovează o cultură conștientă de securitate în rândul angajaților.

62. Analizați și clasificați potențialele riscuri de securitate cibernetică pe baza impactului și a probabilității lor de apariție	L7	S	Ca parte a unui exercițiu de evaluare a riscurilor, vă veți demonstra cunoștințele (K) despre amenințările și vulnerabilitățile de securitate cibernetică cu care se confruntă în mod obișnuit organizațiile. Veți putea identifica și recunoaște riscuri specifice, cum ar fi atacuri de phishing, infecții cu programe malware și încercări de acces neautorizat. Aplicându-vă abilitățile (S), veți evalua impactul potențial și probabilitatea fiecărui risc asupra sistemelor informaționale și a datelor organizației. Prin clasificarea riscurilor în niveluri de severitate ridicate, medii sau scăzute, veți prioritiza eforturile de atenuare, alocând resurse, în mod eficient, pentru a aborda mai întâi cele mai critice riscuri. Această abordare demonstrează o atitudine proactivă (A) față de securitatea cibernetică, asigurând că organizația este bine pregătită pentru a se proteja împotriva potențialelor amenințări și pentru a minimiza impactul incidentelor de securitate.
63. Examinați și actualizați în mod regulat politicile și procedurile legate de securitatea cibernetică	L7	KSA	În calitate de profesionist în securitate cibernetică, veți revizui și actualiza politicile și procedurile de securitate cibernetică pentru a se alinia la cele mai bune practici și reglementări actuale. Această abordare proactivă are consecințele că organizația menține o poziție puternică de securitate și poate răspunde eficient la amenințările emergente.
64. Subliniați măsurile de securitate centrate pe date, în loc să vă bazați doar pe apărarea perimetrului	L7	A	În calitate de avocat al securității cibernetice, veți acorda prioritate protecției datelor în sine, în loc să vă concentrați exclusiv pe securizarea perimetrului rețelei organizației. Această abordare implică implementarea criptării, a controalelor de acces și clasificarea a datelor pentru a proteja informațiile sensibile, chiar dacă perimetrul rețelei este încălcat. Punând accent pe securitatea centrată pe date, organizația se poate asigura că datele rămân în siguranță în orice moment, indiferent dacă sunt memorate, transmise sau accesate de către personal autorizat. Această atitudine proactivă față de protecția datelor îmbunătățește rezistența generală a securității cibernetice a organizației și reduce riscul de încălcare a datelor și accesul neautorizat la informațiile critice.
65. Demonstrați-vă cunoștințele și abilitățile pentru a identifica și a elimina datele redundante, pentru a îmbunătăți securitatea cibernetică	L7	K - S	În calitate de practician în securitate cibernetică, veți fi competent în recunoașterea datelor redundante memorate în sistemele și bazele de date ale organizației. Aplicând cunoștințele Dvs., puteți evalua impactul și riscurile potențiale asociate cu datele redundante, cum ar fi costurile crescute de memorare și expunerea la breșele datelor. Folosindu-vă abilitățile, veți identifica și veți elimina în mod eficient înregistrările, fișierele sau informațiile sensibile duplicate, inutile. Această abordare proactivă optimizează gestionarea datelor, reduce suprafața de atac și îmbunătățește securitatea cibernetică globală, reducând la minimum punctele potențiale de vulnerabilitate.
66. Pledați pentru investiții sporite în securitatea cibernetică și alocați resursele în mod eficient	L7	S - A	În calitate de profesionist în securitate cibernetică, veți susține în mod activ alocarea mai multor resurse financiare și timp pentru consolidarea eforturilor organizației în domeniul securității cibernetice. Folosindu-vă abilitățile, puteți evalua situația actuală de securitate cibernetică și puteți identifica domeniile care necesită investiții suplimentare, cum ar fi instrumente avansate de securitate, formarea angajaților și auditurile de securitate. Prin alocarea eficientă a resurselor, puteți spori capacitatea organizației de a detecta, preveni și răspunde la amenințările cibernetice, reducând astfel riscul de încălcare a securității și de compromitere a datelor. Această atitudine proactivă față de cheltuile mai mari pentru securitatea cibernetică reflectă angajamentul de a proteja activele digitale ale organizației și de a menține o apărare puternică împotriva potențialelor atacuri cibernetice.

67. Fiți conștienți de importanța de a promova mentalitatea de securitate la nivel de companie și de a promova o cultură a conștientizării securității cibernetice	L7	A	Conducând prin exemplu, veți inspira angajații de la toate nivelurile să acorde prioritate securității cibernetice în activitățile lor zilnice. Comunicând în mod regulat importanța securității și oferind exemple reale de amenințări cibernetice și impactul potențial al acestora, veți cultiva o mentalitate de securitate la nivel de companie. Încurajând angajații să raporteze orice probleme de securitate sau incidente, veți crea un mediu în care toată lumea joacă un rol activ în protejarea activelor digitale și a datelor sensibile ale companiei. Această abordare proactivă va contribui la o cultură de securitate puternică, în care practicile de securitate devin înrădăcinate în ADN-ul organizației, sporind rezistența generală a securității cibernetice.
68. Demonstra-ți-vă capacitatea de a clasifica datele în funcție de prioritate și importanță	L7	KS	Veți dobândi abilitățile de a evalua și a clasifica datele în diferite niveluri de prioritate, cum ar fi critice, sensibile și publice. Această clasificare permite organizației să aloce resurse de securitate în mod eficient, asigurându-se că datele cele mai valoroase și sensibile primesc o protecție sporită. Înțelegând importanța clasificării datelor, puteți implementa măsuri de securitate adecvate pentru a proteja informațiile critice de potențialele amenințări cibernetice.
69. Recunoașteți importanța autentificării cu doi factori sau cu mai mulți factori	L7	KS	Cunoscând diferite metode de autentificare, veți configura autentificarea cu doi factori (Two-factor Authentication) sau cu mai mulți factori (MFA - Multi-factor Authentication) pentru diferite conturi și sisteme. Prin aplicarea abilităților dvs., veți configura MFA pentru a solicita un pas suplimentar de verificare, cum ar fi o parolă unică sau o scanare a amprentei digitale, în plus față de parola obișnuită. Această abordare proactivă îmbunătățește securitatea conturilor sensibile, deoarece adaugă un nivel suplimentar de protecție împotriva accesului neautorizat, reducând riscul unor atacuri cibernetice de succes, cum ar fi phishing-ul sau breșele/încălcarea parolei.
70. Dați dovadă de prudență și vigilență atunci când utilizați platformele de social media	L7	A	Prin adoptarea unei atitudini precaute față de utilizarea rețelelor sociale, veți fi atent la informațiile pe care le partajați, la setările de confidențialitate pe care le aplicați și la conexiunile pe care le acceptați. Această abordare proactivă vă ajută să vă protejați datele personale și informațiile sensibile de potențiale amenințări precum furtul de identitate, ingineria socială și escrocheriile cibernetice. Fiind conștienți de riscurile asociate cu partajarea excesivă sau cu acceptarea cererilor de prietenie de la persoane necunoscute, puteți menține o prezență online mai sigură și puteți reduce probabilitatea de a deveni victima unor încălcări de securitate în rețelele sociale.
71. Învățați cum să angajați un hacker de tip „pălărie albă” (white-hat hacker) pentru a evalua securitatea cibernetică	L8	KA	Înțelegeți beneficiile angajării unui hacker cu „pălărie albă”, cunoscut și ca hacker etic, pentru a efectua evaluări de securitate cibernetică și pentru a identifica potențialele vulnerabilități în sistemele organizației dvs. Angajând un astfel de profesionist, vă puteți testa și întări în mod proactiv apărarea, asigurându-vă că potențialele deficiențe de securitate sunt descoperite înainte ca hackerii rău intenționați să le poată exploata. Această abordare ajută la îmbunătățirea poziției de securitate cibernetică a organizației Dvs. și minimizează riscul apariției breșelor de date și a atacurilor cibernetice.

72. Recunoașteți și apărați-vă împotriva tacticilor de inginerie socială	L8	KS	Dobândiți cunoștințe despre tacticile de inginerie socială utilizate de către actorii rău intenționați și dezvoltați abilități pentru a identifica și a răspunde în mod corespunzător la astfel de încercări, sporind rezistența generală a securității cibernetice.
73. Fiți capabil să creați parole puternice și sigure, pentru o securitate cibernetică îmbunătățită	L8	A	Dobândiți cunoștințe despre principiile creării de parole puternice pentru a consolida securitatea cibernetică. Dezvoltați abilitățile de a genera parole cu minim 12 caractere, care conțin litere mari, litere mici, numere și simboluri speciale. Implementarea acestor practici crește complexitatea parolelor, făcându-le mai puțin susceptibile la atacuri de tip "brute force" și îmbunătățind semnificativ securitatea generală a contului.
74. Planificați strategii eficiente de gestionare a accesului pentru a spori securitatea dispozitivelor deținute de întreprindere și a datelor sensibile.	L8	S	În calitate de proprietar al unei afaceri, asigurarea unei gestionări adecvate a accesului este crucială pentru menținerea securității dispozitivelor și a datelor sensibile ale organizației dvs. Deținând drepturi de administrare gestionate și restricționând angajații să instaleze software neautorizat sau să acceseze anumite date din rețea, puteți minimiza riscul unor potențiale încălcări de securitate și compromisuri. Această abordare proactivă vă ajută să vă protejați afacerea de accesul neautorizat, față de scurgerile de date și față de potențialele amenințări cibernetice. Controlând cu atenție accesul la resursele și datele esențiale, puteți menține un mediu IT sigur și robust, protejându-vă afacerea și activele sale valoroase de potențiale daune.
75. Educați angajații cu privire la riscurile asociate cu utilizarea conturilor personale pentru sarcini legate de muncă și promovați importanța separării conturilor personale de cele de afaceri.	L8	A	Este esențial ca angajații să fie conștienți de riscurile pe care le implică utilizarea conturilor lor personale pentru sarcini legate de muncă. Utilizarea conturilor personale în scopuri comerciale poate expune informațiile sensibile ale companiei la potențiale amenințări de securitate și încălcări ale datelor. Educând angajații cu privire la aceste riscuri și promovând practica de separare a conturilor personale de cele afaceri, puteți contribui la protejarea datelor organizației Dvs. și la protejarea acestora împotriva accesului sau expunerii neautorizate. Încurajarea angajaților să folosească conturi de serviciu dedicate și adoptarea practicilor de conectare securizate poate reduce semnificativ șansele ca informațiile confidențiale să fie compromise, asigurând securitatea și integritatea globală a operațiunilor dvs. de afaceri.
76. Implementați un sistem de conturi personale pentru fiecare angajat, pentru a stabili responsabilitatea clară pentru accesul la date sensibile și pentru a urmări eficient activitățile utilizatorilor.	L8	A	Prin crearea de conturi personale individuale pentru fiecare angajat, creați un sistem clar și trasabil pentru monitorizarea persoanelor care accesează anumite informații și la ce oră. Această abordare personalizată îmbunătățește securitatea prin atribuirea unor acțiuni și responsabilități specifice angajaților individuali, permițându-vă să identificați mai ușor orice posibile încălcări de securitate sau activități neautorizate. Cu conturile personale create, puteți monitoriza activitățile utilizatorilor, puteți urmări încercările de conectare și puteți revizui jurnalele de acces la date pentru a vă asigura că numai personalul autorizat are acces la datele sensibile. Acest nivel crescut de responsabilitate vă întărește măsurile generale de securitate cibernetică și vă ajută să vă protejați afacerea de potențialele amenințări interne sau de accesul neautorizat la informații critice.
77. Cunoșteți cum să implementați, să gestionați și să întrețineți	L8	S	Protecția endpoint-urilor se referă la un set de măsuri de securitate concepute pentru a proteja dispozitivele individuale, cum ar fi computerele, laptopurile și dispozitivele mobile, de amenințările de securitate cibernetică. Asigurând protecția punctelor terminale, implementați antivirus, anti-malware, firewall și alte instrumente de

soluții de protecție a endpoint-urilor, pentru a proteja dispozitivele și rețelele individuale față de amenințările de securitate.			securitate pe fiecare dispozitiv pentru a vă proteja împotriva software-ului rău intenționat, a accesului neautorizat și a încălcării datelor. Aceste soluții ajută la detectarea și blocarea potențialelor amenințări, asigurând că dispozitivele sunt mai puțin susceptibile la infecții cu malware, furtul de date și atacurile cibernetice. Implementarea și actualizarea regulată a măsurilor de protecție a punctelor terminale vă întărește postura generală de securitate și creează un mediu de calcul mai sigur pentru angajați și pentru datele organizației.
78. Practicați politici de păstrare a datelor pentru a vă asigura că datele sunt păstrate doar pentru durata necesară, minimizând riscul expunerii datelor și impactul potențial al incidentelor de securitate cibernetică.	L8	A	Adoptarea politicilor de păstrare a datelor ajută la gestionarea eficientă a datelor și la reducerea riscului de încălcare a datelor. Dacă nu păstrați datele mai mult decât este necesar, minimizați cantitatea de informații personale expuse riscului în cazul unui atac cibernetic sau al unei încălcări a datelor. Această practică duce, de asemenea, la eliberarea spațiului de stocare, la optimizarea stocării datelor și la eficientizarea proceselor de gestionare a datelor. Revizuirea și eliminarea periodică a datelor inutile asigură că informațiile sensibile sunt protejate în mod adecvat și reduce probabilitatea accesului neautorizat sau a scurgerilor de date. Drept urmare, postura de securitate cibernetică a organizației este consolidată și respectarea reglementărilor privind protecția datelor este menținută.
79. Optimizați-vă setările și performanța browserului pentru a îmbunătăți viteza și eficiența navigării.	L8	S	Ajustând setările și configurațiile browserului, îi puteți îmbunătăți performanța, rezultând experiențe de navigare mai rapide și mai fluide. Acest lucru poate implica ștergerea memoriei cache și a cookie-urilor, dezactivarea extensiilor inutile și actualizarea browserului la cea mai recentă versiune. Luarea acestor pași va crește viteza browserului dvs., făcându-l mai receptiv și mai eficient în gestionarea conținutului web și reducând timpul de încărcare a paginilor web. În plus, optimizarea browserului poate duce, de asemenea, la îmbunătățirea securității și a confidențialității prin eliminarea potențialelor vulnerabilități și reducerea riscului de urmărire sau de colectare a datelor prin cookie-uri.
80. Personalizați setările de securitate ale browserului pentru a spori siguranța și confidențialitatea online.	L8	S	Personalizarea setărilor de securitate ale browserului vă permite să vă adaptați experiența de navigare în funcție de preferințele dvs. specifice de securitate și confidențialitate. Prin ajustarea setărilor precum confidențialitatea, blocarea ferestrelor pop-up, gestionarea cookie-urilor și nivelurile de securitate, puteți consolida capacitatea browserului dvs. de a vă proteja împotriva diferitelor amenințări online și urmărirea datelor. De exemplu, activarea setărilor stricte de confidențialitate poate limita cantitatea de informații colectate de site-urile web despre dvs., în timp ce activarea blocarelor pop-up ajută la prevenirea reclamelor nedorite sau a conținutului potențial rău intenționat. Făcând aceste ajustări, puteți spori securitatea browserului dvs., făcându-l mai rezistent la potențiale riscuri cibernetice și protejându-vă datele personale în timpul interacțiunilor online.