MICRO-CREDITE PENTRU SIGURANȚĂ
COMPETENȚA 4.2:
PROTECȚIA DATELOR PERSONALE ȘI A CONFIDENȚIALITĂȚII

DSW
DIGITAL SKILLS WALLET

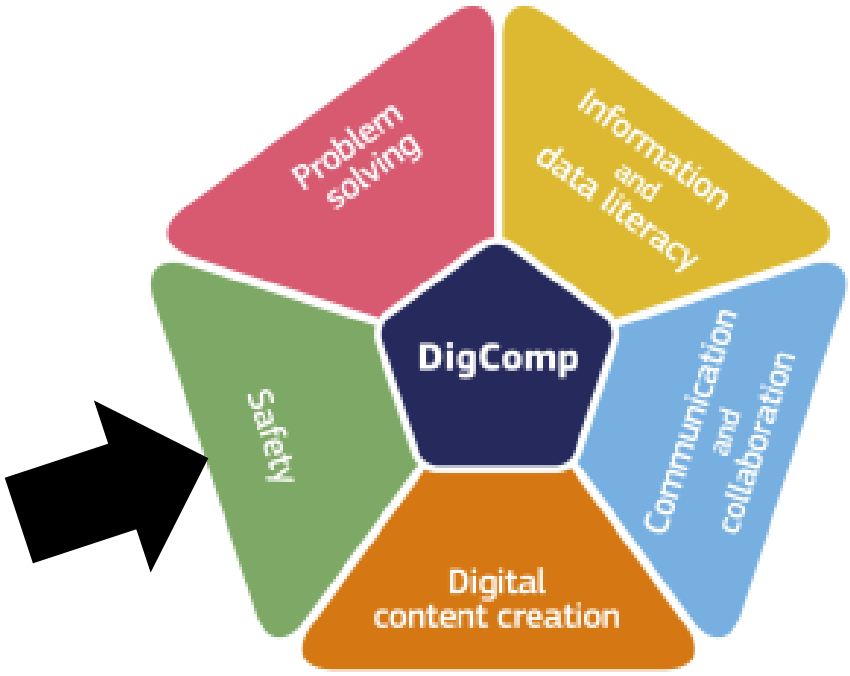
Co-funded by
the European Union

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.

DSW
DIGITAL SKILLS WALLET

Co-funded by the European Union

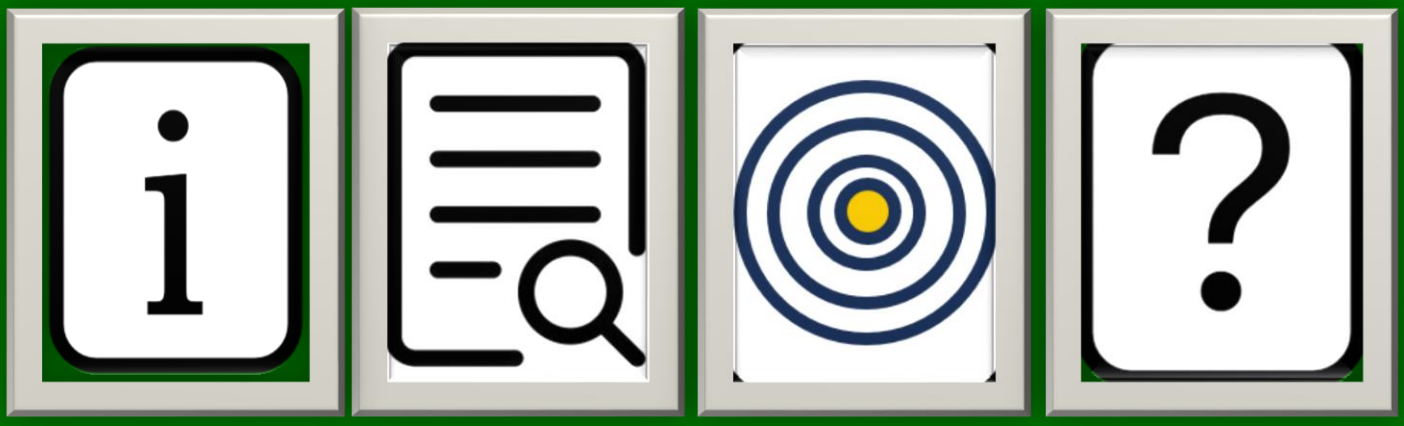
Micro-credite pentru competența 4.2: PROTECȚIA DATELOR PERSONALE ȘI A CONFIDENȚIALITĂȚII



Cuprins

NIVELUL DEBUTANT

(Nivelul 1 și Nivelul 2)



Înțelegerea extinsă a siguranței digitale și a securității tranzacțiilor (MC 4.2.A.1)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Înțelegerea extinsă a siguranței digitale și a securității tranzacțiilor Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.1 și 4.2.2):

- Recunoașterea importanței identificării electronice securizate pentru partajarea mai sigură a datelor cu caracter personal în tranzacții.
- Identificarea elementelor „politicii de confidențialitate" a serviciilor sau aplicațiilor.

Descriere

Pe măsură ce lumea digitală se extinde, importanța măsurilor de siguranță și securitate digitală escaladează, în special în partajarea și gestionarea datelor cu caracter personal. Acest MC validează o înțelegere profundă a rolului crucial al identificării electronice securizate și înțelegerea cuprinzătoare a politicilor de confidențialitate utilizate de diverse aplicații și servicii. Cunoașterea și conștientizarea sunt primii pași către asigurarea unor tranzacții online mai sigure și a unui mediu digital securizat.

Primul aspect major al siguranței digitale este identificarea electronică sigură. Aceasta reprezintă o „dovadă" digitală a identității care servește drept instrument de validare fiabil pentru tranzacțiile online. Esența acestui proces este de a asigura securitatea datelor partajate, garantând schimbul acestora cu destinatarul vizat. Joacă un rol important în tranzacțiile care implică persoane sau date confidențiale. Aceste tranzacții variază de la tranzacții financiare la schimburi de date din domeniul sănătății și comunicări profesionale. Prin urmare, utilizarea identificării electronice securizate este un aspect semnificativ al economiei digitale și modelează încrederea utilizatorilor în tranzacțiile digitale. În plus, identificarea electronică securizată formează baza politicilor de confidențialitate care protejează datele utilizatorilor și îi susțin drepturile.

Politicile de confidențialitate sunt centrale în menținerea încrederii în lumea digitală, asigurându-se că datele utilizatorilor sunt tratate cu grijă, respect și conformare legală. Există documente legale care detaliază modul în care aplicațiile sau serviciile adună, înmagazinează, protejează și partajează datele personale. O înţelegere robustă a acestor politici de confidențialitate conduce la decizii informate cu privire la utilizarea aplicaților sau a serviciilor și contribuie la menținerea autonomiei digitale. Printre componentele unei politici de confidențialitate, înțelegerea tipurilor de date colectate de o aplicație sau serviciu este crucială. Aceasta ar putea include informații personale, specificul dispozitivului sau datele despre comportamentul utilizatorului. Utilizatorii care înțeleg acest element pot să se asigure că sunt de acord cu tipurile de informații colectate. Ei pot evalua, de asemenea, dacă această colectare se aliniază cu utilizarea prevăzută a aplicației sau a serviciului, reducând astfel şansele de expunere nedorită a datelor.

La fel de importantă este înțelegerea motivului pentru care datele sunt colectate, adică scopul de colectare a datelor. Scopul ar putea include motive precum îmbunătățirea experienței utilizatorului, livrarea de conţinut personalizat, sau furnizarea de servicii. Înţelegerea acestor motive ajută la a evalua dacă acea colecție de date servește cele mai bune interese ale utilizatorului sau este în beneficiul furnizorului de servicii. Un alt aspect crucial îl reprezintă practicile de prelucrare și partajare a datelor. Această componentă elaborează călătoria datelor colectate, detaliind cum sunt acestea procesate, stocate și posibil partajate cu terți. De asemenea, include informație despre transferurile internaționale de date și depre datele prelucrate transfrontalier. Cunoștințele despre aceste practici le dau utilizatorilor puterea să evalueze riscurile potențiale și să facă alegeri informate cu privire la partajarea datelor cu caracter personal. Consimțământul este o piatră de temelie a reglementărilor privind protecția datelor. Este, prin urmare, vital să înțelegeți cum se obține consimțământul pentru colectarea și prelucrarea datelor de către o aplicație sau un serviciu. Acest lucru poate fi realizat prin metode explicite, cum ar fi casetele de selectare sau metode implicite, cum ar fi continuarea de a utiliza aplicația. Utilizatorii care înțeleg aceste procese pot să controleze mai bine consimţământul, sporind

puterea lor peste date personale. Drepturile utilizatorilor sunt parte integrantă a politicilor de protecție a datelor. Acesta include, de obicei,dreptul de a accesa, corecta, șterge sau restricționa prelucrarea informațiilor personale. Cunoașterea acestor drepturi permite utilizatorilor să exercite controlul asupra datelor lor, ceea ce poate duce la o încredere sporită în sfera digitală.

Un alt aspect critic al unei politici de confidențialitate este descrierea măsurilor de securitate luate pentru a proteja datele utilizatorului împotriva accesului neautorizat sau a utilizării greșite. O înțelegere clară a acestor măsuri poate ajuta utilizatorii să evalueze robustețea serviciului sau cadrul de securitate al aplicației și adecvarea acesteia pentru nevoile lor specifice. Înțelegerea perioadelor de păstrare a datelor, care specifică durata serviciului sau cât timp reține aplicația datele utilizatorului - înainte de a fi șterse sau anonimizate - este, de asemenea, crucială. Diferiți utilizatori pot avea diferite niveluri de confort în funcție de durata de păstrare a datelor, un factor semnificativ în alegerea serviciilor digitale sau aplicații. Dacă aplicația sau serviciul colaborează cu terți, politica de confidențialitate ar trebui să detalieze natura unor astfel de colaborări. Utilizatorii ar trebui să fie conștienți de aceste parteneriate, cum aceste parteneriate partajează și prelucrează suplimentar datele. În cazurile în care aplicația sau serviciul este adresat copiilor sau colectează date de la copii, aderarea la legile privind confidențialitatea copiilor devine un element vital al politicii de confidențialitate. Cunoașterea acestei conformități poate ajuta utilizatorii să ia decizii mai informate cu privire la astfel de aplicații sau servicii. În cele din urmă, modul în care sunt modificate sau actualizate politicile de confidențialitate sunt comunicate utilizatorilor, iar aceștia vor ști să contacteze serviciul sau aplicația pentru întrebări privind confidențialitatea datelor.

Acest MC înzestrează cursanții cu înțelegerea siguranței și a securității digitale în tranzacțiile de date. Le certifică cunoștințele privind identificarea electronică securizată și capacitatea de a identifica și a înțelege elementele explicate în mod obișnuit în politicile de confidențialitate. La finalizarea acestui MC, cursantul va fi bine pregătit pentru a-și proteja datele personale, pentru a naviga cu încredere în lumea digitală, și pentru a contribui la mediu digital mult mai sigur.

Întrebări

1. Ce este identificarea electronică sigură și de ce este crucială în tranzacțiile cu datele personale?
2. Cum contribuie identificarea electronică sigură la încrederea utilizatorilor în tranzacțiile digitale?
3. De ce este esențială o înțelegere cuprinzătoare a politicilor de confidențialitate în contextul siguranței și securitatății digitale?
4. Care sunt câteva tipuri tipice de date care ar putea fi colectate de către aplicații sau servicii ca parte a politicii lor de confidențialitate?
5. De ce este importantă înțelegerea scopului colectării datelor pentru utilizatorii aplicațiilor digitale sau a serviciilor?
6. Ce include de obicei componenta practicilor de prelucrare și partajare a datelor dintr-o politică de confidențialitate? De ce este important ca utilizatorii să înteleagă acest lucru?
7. Cum ar putea o aplicație sau un serviciu să obțină consimțământul unui utilizator pentru colectarea și prelucrarea datelor? De ce înțelegerea acestui lucru este crucială pentru utilizatorii?
8. Care sunt unele dintre drepturile utilizatorului evidențiate de obicei într-o politică de confidențialitate? De ce este important ca utilizatorii să le cunoască și să le înțeleagă?
9. Care este importanța înțelegerii măsurilor de securitate descrise într-o politică de confidențialitate?
10. De ce sunt importante cunoștințele despre perioadele de păstrare a datelor pentru utilizatori și cum ar putea influența acestea deciziile utilizatorilor de a folosi anumite servicii digitale sau aplicații?
11. Cum contribuie înțelegerea colaborărilor cu terțe părți și a notificărilor de actualizare a politicii la luarea deciziilor informate, cu privire folosirea aplicației sau a serviciului, de către utilizator?

Cunoștințe aprofundate despre siguranța datelor cu caracter personal și evaluarea riscurilor (MC 4.2.A.2)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Cunoștințe aprofundate despre siguranța datelor cu caracter personal și evaluarea riscurilor Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.3 și 4.2.4):

- Identificarea diferitelor tipuri de date cu caracter personal care ar putea fi expuse riscului (de exemplu, nume, e-mail, adresă, număr de telefon, număr de asigurări medicale din UE).
- Descoperirea beneficiilor și a riscurilor, înainte de a permite terților să prelucreze date cu caracter personal.

Descriere

Navigarea în peisajul digital a devenit o obișnuință în lumea modernă. Fiecare click, like și share contribuie la amprenta digitală a unei persoane, amplificând importanța siguranței datelor cu caracter personal. Delimitarea diferitelor tipuri de date cu caracter personal expuse riscului, în special pe platformele de social media, și evaluarea beneficiilor și a riscurilor prelucrării datelor de la terți, sunt abilități esențiale în domeniul securității și a pretecției datelor. Acest MC validează înțelegerea în profunzime a acestor aspecte cruciale și capacitatea lor de a lua decizii informate într-un mediu digital cât mai sigur.

Datele cu caracter personal constituie un spectru larg de informații care pot identifica sau se pot raporta la o anumită persoană. Aceste date pot fi identificatori generici, cum ar fi nume, e-mail adrese, adrese de domiciliu și numere de telefon, sau date mai sensibile, ca numere de asigurări de sănătate din UE, date de naștere, informații financiare și locuri de muncă Detalii. Odată cu dezvoltarea platformelor de social media, chiar și interesele personale, activitățile, și datele comportamentale au devenit o parte datelor cu caracter prsonal. Fiecare dată, când este partajată sau memorată, este susceptibilă la potenţialele riscuri de securitate și amenințări.
Importanța siguranței datelor cu caracter personal devine deosebit de evidentă pe rețelele sociale. Aceste platforme reprezintă o scenă pe care utilizatorii se pot exprima, interacționează cu ceilalți și accesează o multitudine de servicii. În acest fel, utilizatorii dezvăluie de cele mai multe ori o mulțime de date personale. Un simplu “like” pe o postare poate indica preferințele unei persoane, în timp ce un „check-in” poate expune date despre locație. Partajarea zilelor de naștere, a detaliilor despre familie sau chiar a fotografiilor pot dezvălui neintenționat informații sensibile. Astfel, utilizatorii devin vulnerabili la invadarea confidențialității sau chiar la furtul de identitate.

Înțelegerea tipurilor de date cu caracter personal expuse riscului pe rețelele sociale și posibilele repercusiuni ale expunerii lor constituie prima linie de apărare în siguranța digitală. De exemplu, dezvăluirea unei adrese de e-mail poate conduce primirea unor mesaje nesolicitate, iar expunerea informațiilor financiare ar putea avea rezultate mai grave, precum frauda financiară. Cunoașterea acestor riscuri evidențiază nevoia de a partaja judicios și de a gestiona atent datele personale pe rețelele sociale.
Cu toate acestea, responsabilitatea siguranței datelor cu caracter personal se extinde dincolo de individ. De asemenea, această responsabilitate aparține organizațiilor și serviciilor care manipulează astfel de date. Prin urmare, importanța politicilor de confidențialitate, a practicilor sigure de manipulare a datelor și a identificării electronice securizate, este foarte mare. Cunoașterea acestor măsuri permite utilizatorilor să se asigure că datele lor personale sunt tratate cu precauția și respectul necesare.

Ecosistemul digital modern implică adesea prelucrarea datelor de către terți, caz în care datele sunt partajate cu entități externe în diverse scopuri, ca îmbunătățirea calității serviciilor, personalizarea experienței utilizatorului, sau date analitice. Aceste parteneriate, pe lângă avantajele prezentate, vin și cu o serie de riscuri. Potențialul de încălcare a datelor și de apatiție a breșelor de date crește cu fiecare entitate suplimentară care

se ocupă de date. Fiecare parteneriat extern reprezintă un potențial punct de vulnerabilitate, prin care securitatea datelor ar putea fi compromisă. În plus, procesarea datelor de către terțe părți duce adesea la un grad de pierdere a controlului asupra datelor cu caracter personal. Având în vedere acestea considerații, capacitatea de a evalua beneficiile și riscurile înainte de a permite terților părți să prelucreze datele reprezintă o abilitate importantă în mentinerea siguranței datelor personale.
Această evaluare implică înțelegerea practicilor de prelucrare a datelor de către terți, a politicilor de confidențialitate și a măsurilor de securitate; necesită cunoașterea datelor care vor fi partajate, a modului de utilizare a acestora și a metodelor de protecție existente.
Familiarizarea cu drepturile utilizatorului, inclusiv dreptul de acces, corectare, ștergere sau restricționare a prelucrării datelor cu caracter personal este, de asemenea, esențială.
Adesea, prelucrarea datelor de către terți implică transferuri transfrontaliere de date, sporind complexitatea, prin diferitele reglementări care diferă de la o regiune la alta.
Prin urmare, o înțelegere clară a acestor aspecte este crucială pentru a lua decizii informate privind prelucrarea datelor de către terți și asigurarea securității datelor personale.
În concluzie, acest MC certifică cunoștințele și abilitățile cursanților în siguranța datelor cu caracter personal și evaluarea riscurilor. Cursanții vor avea capacitatea lor de a identifica diversetipuri de date cu caracter personal expuse riscului, în special pe platformele de social media, și de a evalua beneficiile și riscurile înainte de a autoriza prelucrarea datelor de către terți. Dobândind aceste, cursantul poate să-și gestioneze în mod activ datele personale, să navigheze în lumea digitală cu încredere și să contribuie la promovarea unui mediu digital mai sigur.

Întrebări

1. Care sunt diferitele tipuri de date personale care pot fi expuse pericolelor pe platformele de social media?
2. Ce riscuri potențiale de confidențialitate și securitate pot apărea prin partajarea publică a informațiilor personale sensibile pe rețelele sociale?
3. Care pot fi potențialele repercusiuni dacă date mai sensibile, cum ar fi numerele de asigurări de sănătate din UE sau datele financiare, sunt expuse pe rețelele sociale?
4. Cum poate prelucrarea datelor de către terți să îmbunătățească capacitățile serviciilor digitale?
5. Care sunt posibilele riscuri asociate cu prelucrarea datelor de către terți?
6. De ce este important să evaluăm beneficiile și riscurile înainte de a permite prelucrarea datelor de către terți?
7. Cum poate prelucrarea datelor de către terți să sporească vulnerabilitatea la încălcarea datelor?
8. Ce înseamnă pierderea controlului asupra datelor cu caracter personal în contextul prelucrării datelor de către terți?
9. Cum ajută înțelegerea practicilor de prelucrare a datelor, a politicilor de confidențialitate și a măsurilor de securitate ale terților la evaluarea beneficiilor și a riscurilor prelucrării datelor?
10. Care sunt drepturile utilizatorului în ceea ce privește prelucrarea datelor cu caracter personal și cum joacă ele un rol în prelucrarea datelor de către terți?
11. În ce fel, transferurile transfrontaliere de date, sporesc complexitatea prelucrării datelor de către terți?
12. Cum poate un individ să-și asigure siguranța datelor cu caracter personal în timp ce interacționează pe platformele de social media?
13. Care sunt unele dintre măsurile pe care organizațiile și serviciile le pot lua pentru a asigura siguranța datelor cu caracter personal, în special atunci când implică prelucrarea datelor de către terți?

Utilizarea avansată a aplicațiilor antivirus și personalizarea setărilor de confidențialitate (MC 4.2.A.3)

Specificații

Identificarea cursantului	Orice cetățean
Titlul micro-acreditării	Utilizarea avansată a aplicațiilor antivirus și personalizarea setărilor de confidențialitate **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.5 și 4.2.6):

- Discutarea rolului software-ului antivirus în protejarea împotriva programelor malware și exersați scanări antivirus regulate pe dispozitivele dvs.
- Personalizarea setărilor de confidențialitate de pe conturile Dvs. de rețele sociale, pentru a limita informațiile vizibile public.

Descriere

Într-o eră digitală în continuă evoluție, menținerea siguranței și securității nu înseamnă doar protejarea aspectelor fizice ale vieții noastre, ci și protejarea existenței noastre virtuale. Prezența software-ului antivirus pe dispozitive și personalizarea setărilor de confidențialitate pe conturile de rețele sociale au devenit componente integrante ale strategiilor extinse de securitate cibernetică. MC-ul “Mastery in Antivirus Application and Personal Privacy Setting Customization” atestă competența unei persoane de a folosi aceste instrumente pentru a-și securiza spațiile digitale.

Software-ul antivirus joacă un rol crucial în protecția dispozitivelor digitale împotriva diferitelor forme de software rău intenționat, cunoscut și sub numele de malware. Acest software funcționează prin scanarea, identificarea și eliminarea amenințărilor care pot compromite integritatea, funcționalitatea și securitatea dispozitivului. Virușii, viermii (worms), ransomware, spyware, adware și troieni sunt tipuri comune de malware, care pot provoca daune semnificative dispozitivelor digitale, de la coruperea și furtul datelor, până la defectarea totală a dispozitivului.

Cursantul trebuie să înțeleagă că scanările antivirus regulate ale dispozitivelor sale este un aspect fundamental al securității digitale. Scanările regulate vă ajută să vă asigurați că cele mai recente amenințări sunt identificate și tratate cu promptitudine, ceea ce este deosebit de important, având în vedere apariția continuă a noilor tipuri de malware. Scanările programate, alături de funcțiile de protecție în timp real oferite de multe programe antivirus, creează un sistem de apărare stratificat, care poate împiedica o mare varietate de atacuri malware, protejând astfel datele individuale, confidențialitatea și sănătatea generală a dispozitivelor lor.

Dincolo de utilizarea software-ului antivirus, abilitatea de a personaliza setările de confidențialitate pe conturile de rețele sociale, este o altă competență crucială, care contribuie la securitatea digitală a unei persoane. Platformele de social media sunt ținte comune pentru infractorii cibernetici datorită cantității mari de date personale pe care le dețin. Ca atare, setările de confidențialitate de pe aceste platforme trebuie tratate cu mare atenție, pentru a limita informațiile care sunt vizibile public și, astfel, potențial accesibile actorilor rău intenționați.

Personalizarea setărilor de confidențialitate pe platformele de social media implică înțelegerea și ajustarea unei game de comenzi care dictează vizibilitatea și accesibilitatea informațiilor personale, a postărilor, a datelor despre locația și conexiunile utilizatorului. Persoana trebuie să fie conștientă de faptul că aceste setări partajează adesea, în mod implicit, informații pe scară largă, așa că trebuie să gestioneze în mod proactiv aceste setări, pentru a restricționa diseminarea informațiilor personale. Limitarea audienței postărilor, revizuirea etichetelor de la prieteni, gestionarea setărilor de locație și controlul vizibilității listei de prieteni sunt câteva dintre acțiunile care pot spori semnificativ confidențialitatea pe platformele de social media.

Prin urmare, MC-ul "Utilizarea avansată a aplicațiilor antivirus și personalizarea setărilor de confidențialitate" certifică cunoștințele și abilitățile practice dobândite de către cursant, în securitatea cibernetică: utilizarea eficientă a software-ului antivirus pentru protejarea duspozitivelor împotriva programelor malware și personalizarea setărilor de confidențialitate pe rețelele sociale pentru a limita vizibilitatea publică a informațiilor personale.

Dobândirea acestor abilități le va permite cursanților să navigheze mai bine în lumea digitală, promovându-și securitatea și confidențialitatea într-un peisaj care este adesea plin de amenințări la adresa securității cibernetice.

Întrebări

1. Ce rol joacă software-ul antivirus în protecția dispozitivelor digitale?
2. Identificați și descrieți câteva tipuri comune de malware împotriva cărora software-ul antivirus vă poate proteja.
3. De ce este necesar să rulați scanări antivirus regulate pe dispozitivele dvs.?
4. Explicați conceptul de protecție în timp real în programele antivirus și modul în care aceasta contribuie la un sistem de apărare stratificat.
5. Cum contribuie personalizarea setărilor de confidențialitate pe platformele de social media la securitatea digitală a unei persoane?
6. Ce tipuri de informații pot deveni vizibile public dacă setările de confidențialitate ale rețelelor sociale nu sunt gestionate corespunzător?
7. Descrieți câteva măsuri care pot fi luate pentru a îmbunătăți confidențialitatea pe platformele de social media.
8. De ce este important să limităm audiența postărilor de pe platformele de social media?
9. Cum contribuie gestionarea setărilor de locație pe rețelele sociale la confidențialitatea utilizatorilor?
10. Explicați potențialele riscuri asociate cu necontrolarea vizibilității listei de prieteni pe platformele de social media.

Expertiză în gestionarea parolelor și utilizarea funcțiilor de securitate ale telefoanelor inteligente (smartphone-uri) (MC 4.2.A.4)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Expertiză în gestionarea parolelor și utilizarea funcțiilor de securitate ale telefoanelor inteligente (smartphone-uri) **Cod de utilizare: MC 4.2.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	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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.7 și 4.2.8):

- Testarea puterii parolelor dvs. folosind instrumente de gestionare a parolelor.
- Demonstrarea modului în care sunt folosite funcțiile de securitate încorporate ale smartphone-ului tău, cum ar fi blocarea ecranului, pentru a-ți proteja datele personale.

Descriere

Rata în creștere rapidă a digitalizării necesită măsuri de securitate extinse pentru a asigurarea siguranței datelor cu caracter personal. O dată cu progresul tehnologiei, securizarea datelor cu caracter personal nu se mai limitează doar la factorii fizici, externi, ci se extinde și la factorii virtuali, interni. MC-ul "Expertiză în gestionarea parolelor și utilizarea funcțiilor de securitate ale telefoanelor inteligente" validează abilitățile unei persoane în gestionarea parolelor folosind instrumente de gestionare a parolelor și în folosirea funcțiilor de securitate încorporate în smartphone-uri, pentru a-și proteja datele personale.

O parolă puternică este un factor cheie al securității conturilor online ale unei persoane și, prin extensie, a datelor sale personale. Parolele slabe pot fi sparte cu ușurință de către infractorii cibernetici, făcând conturile și datele personale ale unei persoane vulnerabile la accesul neautorizat și la utilizarea necorespunzătoare. Prin urmare, este esențial ca indivizii să testeze puterea parolelor lor, o sarcină care poate fi ușurată prin utilizarea instrumentelor de gestionare a parolelor.

Instrumentele de gestionare a parolelor îndeplinesc mai multe funcții care sporesc securitatea parolei. Acestea generează parole complexe și unice pentru fiecare cont, stochează aceste parole în siguranță și le completează automat în timpul autentificării, minimizând astfel riscul accesului neautorizat. Majoritatea managerilor de parole oferă, de asemenea, un test de putere a parolei, permițând individului să verifice robustețea parolelor lor împotriva potențialelor atacuri cibernetice. Înțelegerea și utilizarea acestor instrumente este o abilitate esențială în mediul digital actual, în care siguranța datelor cu caracter personal depinde în mare măsură de puterea parolelor.

În paralel, individul ar trebui să utilizeze caracteristicile de securitate încorporate în telefoanele inteligente, pentru a-și proteja datele personale. Într-o epocă în care smartphone-urile înmagazinează cantități mari de date cu caracter personal, lipsa securizării lor într-un mod adecvat poate duce la încălcări semnificative ale confidențialității. Caracteristicile de securitate încorporate, cum ar fi mecanismele de blocare a ecranului, oferă o primă linie de apărare împotriva accesului neautorizat.

Mecanismele de blocare a ecranului cuprind diferite forme de autentificare, inclusiv PIN-uri, modele, parole, recunoaștere facială și amprentele digitale. O persoană trebuie să înțeleagă beneficiile și limitările fiecărui tip de metodă de autentificare, pentru a o selecta pe cea care se potrivește cel mai bine nevoilor sale și oferă protecție maximă. De exemplu, în timp ce scanerele de recunoaștere facială și de amprentă oferă un nivel ridicat de securitate și confort, este posibil să nu funcționeze optim în toate condițiile. În schimb, codurile PIN, modelele și parolele sunt universal funcționale, dar pot fi vulnerabile dacă sunt slabe sau ușor de ghicit.

În concluzie, MC-ul "Expertiză în gestionarea parolelor și utilizarea funcțiilor de securitate ale telefoanelor inteligente" atestă cunoștințele abilitățile în aplicarea practicilor esențiale de securitate: utilizarea

instrumentelor de gestionare a parolelor pentru a spori securitatea parolelor și utilizarea eficientă a funcțiilor de securitate încorporate pentru smartphone-uri pentru a proteja datele personale. Deținerea acestor abilități sporește capacitatea individului de a naviga în lumea digitală în siguranță și cu încredere. Recunoașterea potențialelor vulnerabilități și implementarea unor măsuri de protecție robuste sunt cruciale pentru menținerea securității datelor cu caracter personal în era digitală.

Întrebări

1. Care este rolul puterii parolei în securizarea conturilor online și a datelor personale ale unei persoane?
2. Cum contribuie instrumentele de gestionare a parolelor la îmbunătățirea securității parolelor?
3. Care sunt câteva funcții cheie ale instrumentelor de gestionare a parolelor?
4. Explicați cum funcționează un test de putere a parolei în instrumentele de gestionare a parolelor.
5. De ce este important să folosim funcțiile de securitate încorporate ale smartphone-urilor pentru protecția datelor cu caracter personal?
6. Cum servește un mecanism de blocare a ecranului ca linie de apărare împotriva accesului neautorizat la smartphone-uri?
7. Identificați și descrieți diferitele tipuri de metode de autentificare disponibile în mecanismele de blocare a ecranului smartphone-ului.
8. Discutați avantajele și limitările utilizării recunoașterii faciale ca metodă de autentificare pentru blocarea ecranului smartphone-ului.
9. Cum contribuie PIN-urile, modelele și parolele la securitatea smartphone-urilor și care sunt potențialele vulnerabilități ale acestora?
10. Cum îmbunătățește utilizarea parolelor unice și complexe pentru fiecare cont securitatea datelor cu caracter personal?
11. Care sunt riscurile asociate cu utilizarea codurilor PIN, a modelelor și a parolelor slabe sau ușor de ghicit pentru autentificarea blocării ecranului smartphone-ului?

Expertiză în întreținerea parolelor și înțelegerea securității rețelei Wi-Fi publice (MC 4.2.A.5)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Expertiză în întreținerea parolelor și înțelegerea securității rețelei Wi-Fi publice **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.9 și 4.2.10):

- Modificarea periodică a parolei pentru a evita posibile breșe de date.
- Deducerea pericolelor utilizării rețelelor Wi-Fi publice, nesecurizate, în cazul tranzacțiilor care implică date personale.

Descriere

Pe măsură ce platformele digitale continuă să se integreze în fiecare fațetă a vieții moderne, accentul pus pe menținerea securității cibernetice a crescut considerabil. MC-ul "Expertiză în întreținerea parolelor și înțelegerea securității rețelei Wi-Fi publice" certifică capacitatea unei persoane de a naviga și de a înțelege două aspecte critice ale siguranței personale digitale: importanța modificării periodice a parolelor și înțelegerea riscurilor asociate cu rețelele Wi-Fi publice nesecurizate.

Integritatea identității digitale și securitatea datelor cu caracter personal sunt strâns legate de puterea și menținerea parolelor. Parolele acționează ca primă linie de apărare împotriva accesului neautorizat la conturile și informațiile personale. Prin urmare, nu este important doar să creați parole robuste, greu de ghicit, dar este crucial să le și modificați periodic. Schimbările regulate ale parolei pot împiedica accesul neautorizat pe termen lung, chiar dacă parola a fost compromisă anterior fără știrea persoanei. Prin urmare, abilitatea de a gestiona și schimba parolele la intervale regulate este un factor cheie în reducerea riscului potențialelor încălcări ale datelor.

Pe lângă întreținerea parolei, MC-ul se concentrează pe înțelegerea de către o persoană a pericolelor inerente utilizării rețelelor Wi-Fi publice, nesecurizate. Rețelele Wi-Fi publice, în special cele fără protocoale de conectare securizate, prezintă riscuri semnificative de securitate. Rețelele nesecurizate sunt ținte principale pentru infractorii cibernetici, care pot intercepta cu ușurință datele transmise prin rețea. Acest lucru devine deosebit de îngrijorător atunci când aceste rețele sunt utilizate pentru tranzacții care implică date personale sau informații sensibile.

Cursanții trebuie să deducă diferitele riscuri asociate cu astfel de rețele, care includ, dar nu se limitează, la atacuri de tip „Man-in-the-Middle", snooping și sniffing, distribuirea de malware și chiar amenințarea hotspot-urilor rău intenționate care se mascchează în rețele legitime. Înțelegerea acestor pericole evidențiază importanța evitării unor astfel de rețele atunci când folosiți date personale, sensibile sau când optați pentru măsuri de protecție, cum ar fi rețelele private virtuale (VPN) pentru a cripta transmisiile lor de date.

În concluzie, MC-ul "Expertiză în întreținerea parolelor și înțelegerea securității rețelei Wi-Fi publice" certifică abilitățile și cunoștințele – dobîndite de către cursant - asupra aspectelor vitale ale securității datelor personale. Schimbarea regulată a parolelor reduce semnificativ riscul de încălcare a datelor, în timp ce recunoașterea pericolelor utilizării rețelelor Wi-Fi publice nesecurizate subliniază nevoia de vigilență și precauție în securitatea datelor. Aceste cunoștințe și capacitatea de a le aplica în mod eficient furnizează cursanților abilitățile necesare pentru a naviga în peisajul digital în siguranță, protejându-și informațiile personale de potențialele amenințări cibernetice.

Întrebări

1. Cum contribuie schimbarea regulată a parolelor la securitatea datelor cu caracter personal?
2. Care sunt riscurile potențiale în cazul în care o persoană nu își modifică periodic parolele?
3. De ce rețelele Wi-Fi publice nesecurizate sunt considerate o amenințare la adresa securității datelor cu caracter personal?
4. Puteți explica unele dintre riscurile specifice asociate cu utilizarea rețelelor Wi-Fi publice, nesecurizate, pentru tranzacții care implică date personale?
5. Ce este un atac „Man-in-the-Middle” și ce legătură are acesta cu utilizarea rețelelor Wi-Fi publice, nesecurizate?
6. Descrieți conceptul de „snooping și sniffing” în contextul rețelelor Wi-Fi nesecurizate.
7. Cum are loc distribuția de malware în contextul rețelelor Wi-Fi publice?
8. Ce este un hotspot rău intenționat și cum reprezintă el o amenințare pentru securitatea datelor?
9. Cum pot măsurile de protecție precum rețelele private virtuale (VPN) să atenueze riscurile asociate cu utilizarea rețelelor Wi-Fi publice?

Expertiză în eticheta conținutului digital și în securitatea datelor personale (MC 4.2.A.6)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Expertiză în eticheta conținutului digital și securitatea datelor cu caracter personal **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.11 și 4.2.12):

- Diferențierea conținutului digital adecvat de cel neadecvat pentru partajarea pe conturile de rețele sociale.
- Discuții despre importanța protejării datelor cu caracter personal în timpul utilizării platformelor digitale.

Descriere

“Expertiză în eticheta conținutului digital și în securitatea datelor personale” este un MC care validează înțelegerea exinsă de către o persoană a comportamentului online adecvat și natura critică a siguranței datelor cu caracter personal în universul digital. Pe măsură ce lumea se îndreaptă către o digitalizare crescândă, înțelegerea modului de a interacționa cu platformele digitale, în special rețelele sociale, și menținerea vigilenței asupra protecției datelor cu caracter personal, au devenit imperative atât în sfera personală, cât și în cea profesională.

O componentă integrală a acestei expertize implică capacitatea de a distinge între conținutul adecvat și cel nepotrivit/neadecvat pentru difuzarea pe rețelele sociale. O dată cu omniprezența rețelelor sociale, indivizii împărtășesc în mod regulat anecdote personale, puncte de vedere și diverse forme de informații online. În timp ce acest lucru oferă sentimentul de comunitate globală și încurajează dialogul, introduce simultan nevoia de prudență în a decide ce conținut să partajăm.

Ce face diferența între un conținut și unul nepotrivit, depinde în mare măsură de mai mulți factori, incluzând cercurile sociale și profesionale ale individului, platforma social media în cauză, obiceiurile culturale și normele din societate. Factorii care delimitează, de obicei, granița dintre conținutul adecvat și cel neadecvat/nepotrivit includ sensibilitatea informațiilor, potențialul de a provoca vătămări sau stres și nivelul de confort al individului sau al publicului. Prin urmare, indivizii trebuie să evalueze natura conținutului și să evalueze adecvarea acestuia înainte de a-l distribui.

În plus, indivizii trebuie să fie conștienți de potențialele consecințe care pot apărea din partajarea anumitor tipuri de conținut. Acestea ar putea include deteriorarea reputației personale, pierderea locului de muncă, încălcarea vieții private și chiar repercusiuni legale în anumite situații. Acest lucru evidențiază importanța aplicării gândirii critice și a prudenței atunci când decideți ce conținut digital să distribuiți pe platformele de social media.

Un alt element de bază al MC-ului subliniază importanța critică a protejării datelor personale în timpul interacțiunii cu platformele digitale. Menținerea securității datelor cu caracter personal este o piatră de temelie a păstrării confidențialității personale și a prevenirii potențialelor amenințări, cum ar fi frauda de identitate, escrocheriile financiare și intruziunea neautorizată în conturile personale. Diferite forme de informații personale, de la cele financiare până la datele de identificare, sunt transmise și memorate pe o serie de platforme digitale, făcându-le susceptibile la intruziunile cibernetice.

Înțelegerea potențialelor ramificații ale încălcării datelor și cunoașterea modului de protecție împotriva unor astfel de evenimente este o abilitate crucială. Aceasta include utilizarea tehnicilor de parole puternice, actualizarea regulată a software-ului de securitate, precauția față de e-mailurile sau link-urile dubioase și exercitarea discreției cu privire la informațiile partajate pe platformele de social media. Conștientizarea și

implementarea acestor practici sporesc în mod semnificativ protecția datelor cu caracter personal și promovează o experiență digitală mai sigură.

În concluzie, "Expertiză în eticheta conținutului digital și în securitatea datelor personale" este un MC care validează capacitatea și înțelegerea unei persoane de a distinge conținutul digital adecvat pentru partajarea lui și de a-și proteja datele cu caracter personal. MC-ul certifică capacitatea individului de a-și gestiona prezența digitală în mod responsabil și de a acorda prioritate siguranței datelor. Această înțelegere și competență sunt esențiale în menținerea unui mediu digital respectuos și sigur. Capacitatea de a gestiona în mod corespunzător conținutul digital și de a proteja datele cu caracter personal nu este doar un indiciu al competenței digitale, ci demonstrează și respectul pentru drepturile digitale și confidențialitatea proprie și a celorlalți. Joacă un rol esențial în formarea unei comunități digitale mai sigure, mai responsabile și mai respectuoase.

Întrebări

1. Puteți explica de ce este esențial să faceți diferența între conținutul potrivit și cel nepotrivit, în vederea partajării acestuia pe rețelele sociale?
2. Cum ar putea, un anumit context, cum ar fi obiceiurile culturale, normele din societate, să influențeze considerarea unui conținut ca fiind adecvat pentru a fi distribuit pe platformele de socializare?
3. Care sunt posibilele consecințe ale partajării de informații inadecvate sau sensibile pe platformele de social media?
4. De ce este important să protejăm datele personale în timpul utilizării platformelor digitale?
5. Puteți descrie unele amenințări potențiale care apar datorită protecției inadecvate a datelor cu caracter personal pe platformele digitale?
6. Ce măsuri pot lua indivizii pentru a-și proteja datele personale pe platformele digitale?
7. Cum contribuie actualizarea regulată a software-ului de securitate la protecția datelor cu caracter personal?
8. De ce este esențial să exercitați discreție atunci când partajați informații pe platformele de social media?
9. În opinia dumneavoastră, cum contribuie capacitatea unui individ de a gestiona în mod corespunzător conținutul digital și de a proteja datele personale la comunitatea digitală în ansamblu?

Expertiză în gestionarea confidențialității digitale și practici sigure de comerț electronic (MC 4.2.A.7)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Expertiză în gestionarea confidențialității digitale și practici sigure de comerț electronic **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.13 și 4.2.14):

- Validarea măsurilor adecvate pentru a proteja datele cu caracter personal înainte de a le partaja pe platformele digitale.
- Efectuarea de tranzacții online după ce s-au luat măsurile adecvate de siguranță și de securitate.

Descriere

“Expertiză în gestionarea confidențialității digitale și practici sigure de comerț electronic” este un MC vizează o înțelegere extinsă și o implementare practică a măsurilor de protecție a datelor cu caracter personal pe platformele digitale și executarea în siguranță a tranzacțiilor online. În lumea de astăzi, în care interacțiunile digitale le înlocuiesc rapid pe cele tradiționale, expertiza în siguranța digitală a apărut ca o cerință critică. Protecția datelor sensibile și personale este un factor cheie al încrederii digitale, asigurând interacțiuni personale și profesionale fluide și sigure în lumea virtuală.

MC-ul subliniază două rezultate semnificative ale învățării.

Primul se referă la strategiile riguroase necesare pentru protejarea datelor cu caracter personal înainte de difuzarea acestora pe platformele digitale. Datele cu caracter personal sunt un termen umbrelă, care include nu numai detalii de identificare de bază, cum ar fi numele și informațiile de contact, ci și date extrem de sensibile, cum ar fi datele financiare, informațiile de asistență medicală și multe altele. În absența unor măsuri de securitate robuste, astfel de informații pot deveni o țintă profitabilă pentru infractorii cibernetici, ducând la încălcări neautorizate de date, la furtul de identitate și la utilizarea abuzivă a datelor cu caracter personal.

Din acest motiv, adoptarea unor măsuri stricte de siguranță pentru protecția datelor cu caracter personal este esențială. Măsurile includ generarea și utilizarea de parole complexe, unice, care sunt greu de piratat, permițând autentificarea cu doi factori sau cu mai mulți factori, pentru a oferi un nivel suplimentar de securitate, și menținerea unui nivel ridicat de precauție cu privire la cantitatea și tipul de informații partajate în domenii digitale publice. Acest lucru necesită o înțelegere a pericolelor asociate cu partajarea excesivă și a importanței discreției în forumurile digitale publice.

În plus, este de o importanță capitală să efectuați, regulat, audituri și ajustări ale setărilor de confidențialitate pe diferite platforme digitale. Setările de confidențialitate acționează ca prima linie de apărare în protejarea datelor cu caracter personal, împotriva accesului neautorizat, și ar trebui administrate strategic și cu atenție. Pentru o protecție sporită, în special în timpul accesării rețelelor Wi-Fi publice, se recomandă utilizarea rețelelor private virtuale (VPN). VPN-urile asigură un canal securizat, criptat pentru transmiterea datelor, ceea ce face mult mai dificil pentru entitățile neautorizate să intercepteze și să acceseze datele. Aceste măsuri colective susțin în mod semnificativ mecanismul de apărare împotriva amenințărilor cibernetice, asigurând astfel o experiență de navigare online mai sigură și consolidând confidențialitatea personală.

Al doilea rezultat de învățare de bază al MC-ului vizează efectuarea de tranzacții online sigure, utilizând protocoale adecvate de siguranță și securitate. Odată cu proliferarea platformelor digitale, o multitudine de tranzacții, de la comerțul electronic și plățile facturilor, până la servicii bancare online și gestionarea portofoliului, s-au mutat online. În consecință, asigurarea securității acestor tranzacții a devenit o preocupare critică.

Pentru a efectua tranzacții online în siguranță, este important să folosiți numai site-uri web caracterizate de un prefix HTTPS, care indică natura criptată a transmiterii datelor între browserul utilizatorului și site-ul web. Auditurile regulate ale tranzacțiilor bancare sunt, de asemenea, recomandate pentru a facilita detectarea detectarea din timp a tranzacțiilor neautorizate și rezolvarea acestora. Implementarea autentificării cu doi factori sau cu mai mulți factori pentru tranzacțiile online oferă un nivel suplimentar de securitate, necesitând mai mult de o metodă de verificare a identității utilizatorului.

În plus, partajarea datelor sensibile prin rețele nesecurizate ar trebui evitată, deoarece aceste rețele constituie, de cele mai mute ori, o țintă ușoară pentru atacurile cibernetice. Prin adoptarea acestor măsuri de siguranță, riscul de fraudă sau de acces neautorizat poate fi redus semnificativ, asigurând o experiență tranzacțională online sigură și fără întreruperi.

În concluzie, MC-ul "Expertiză în gestionarea confidențialității digitale și practici sigure de comerț electronic" certifică înțelegerea aprofundată și abilitățile practice ale unui individ în adoptarea de măsuri stricte pentru protecția datelor cu caracter personal și în efectuarea de tranzacții online sigure. Aceste abilități nu sunt doar cruciale pentru siguranța digitală personală, dar contribuie și la crearea unui ecosistem digital mai sigur pentru toți. Abilitatea de a naviga pe platformele digitale în siguranță, de a proteja datele personale și de a efectua tranzacții online sigure demonstrează un nivel ridicat de inițiere în mediile digitale și de responsabilitate în era digitală de astăzi.

Întrebări

1. Care este importanța parolelor unice și complexe în contextul managementului confidențialității digitale?
2. Cum îmbunătățește autentificarea cu doi factori sau cu mai mulți factori securitatea datelor cu caracter personal pe platformele digitale?
3. Care ar trebui să fie considerentele cheie în timpul schimbului de informații pe platformele digitale publice?
4. De ce este esențial să auditați și să ajustați în mod regulat setările de confidențialitate pe diferite platforme digitale?
5. Cum îmbunătățește o rețea privată virtuală (VPN) securitatea, în special atunci când accesați rețele Wi-Fi publice?
6. De ce este important să efectuați tranzacții online numai pe site-uri web caracterizate de un prefix HTTPS?
7. Cum contribuie monitorizarea regulată a extraselor bancare la securizarea tranzacțiilor online?
8. Care sunt riscurile asociate cu partajarea datelor sensibile prin rețele nesecurizate și cum pot fi atenuate aceste riscuri?
9. Cum contribuie principiile managementului confidențialității digitale și practicile sigure de comerț electronic la un ecosistem digital mai sigur?

Schimbul securizat de date și practici de tranzacții online (MC 4.2.A.8)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Schimbul securizat de date și practici de tranzacții online **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.15 și 4.2.16):

- Discuții despre importanța evitării site-urilor web nesigure atunci când manipulați informații despre card.
- Stabilirea măsurilor adecvate pentru a verifica dacă persoanele cu care urmează să partajați date sensibile sunt de încredere.

Descriere

“Schimbul securizat de date și practici de tranzacții online” este un MC care certifică înțelegerea și aplicarea extinsă a metodelor de protejare a datelor personale și financiare în timpul tranzacțiilor online, împreună cu strategiile care ne pot asigura de încrederea persoanelor, înainte de a partaja cu acestea informații sensibile. MC-ul certifică capacitatea de a naviga în peisajul digital în siguranță, de a lua decizii bine informate care asigură protecția datelor și de a îmbunătăți, per total, experiența online a utilizatorului.

Unul dintre rezultatele esențiale ale învățării se axează pe importanța evitării site-urilor web nesigure atunci când sunt procesate informațiile despre carduri. Acest element este o componentă esențială a procesului de efectuare a tranzacțiilor online; elementul are o importanță critică, având în vedere explozia la nivel global a cazurilor de infracțiuni cibernetice și breșe ale datelor. Ori de câte ori o persoană procesează informații despre card pe o platformă online, datele devin susceptibile de a fi interceptate sau piratate dacă site-ul nu dispune de protocoalele de securitate adecvate.

Site-urile web nesigure au adesea măsuri de securitate slabe sau inexistente, ceea ce le face posibile porți de acces pentru infractorii cibernetici, pentru a obține acces neautorizat la datele sensibile. Tranzacțiile pe astfel de site-uri web pot expune informațiile despre carduri acestor entități, ceea ce are consecințe dăunătoare, cum ar fi fraudă financiară, furt de identitate și pierderi economice semnificative.

Cursantul trebuie să fie competent în identificarea unor astfel de site-uri web nesigure, caracterizate de obicei prin lipsa HTTPS în adresa lor URL, prin absența unui simbol de lacăt care indică o conexiune sigură sau prin avertismente de la browserele web despre securitatea site-ului. Alegând în mod conștient să furnizeze informații despre carduri numai pe platforme sigure și de încredere, cursanții pot reduce considerabil riscul potențialelor amenințări cibernetice. Aceste platforme au protocoale de criptare robuste, asigurându-se că, chiar dacă datele sunt interceptate, ele rămân ilizibile și, prin urmare, inutile pentru hackeri.

Al doilea rezultat cheie al învățării se referă la stabilirea de măsuri pentru a verifica fiabilitatea persoanelor înainte de a partaja cu acestea date sensibile. Odată cu creșterea schimburilor de date în sfera digitală, asigurarea faptului că destinatarii datelor sensibile sunt de încredere devine crucială pentru prevenirea accesului neautorizat sau a utilizării abuzive a datelor.

Verificarea poate fi un proces în mai multe etape. Inițial, se pot solicita documente oficiale de identificare sau acreditări/credențiale pentru a confirma identitatea persoanei. Comunicarea directă cu persoana poate fi, de asemenea, benefică în înțelegerea intenției acesteia și în stabilirea unui anumit grad de încredere. Cu toate

acestea, doar acești pași pot să nu fie suficienți, mai ales în scenariile care implică schimbul de date pe platforme digitale.

Aici, folosirea canalelor de comunicații sigure pentru schimbul de date poate adăuga un nivel de securitate. Aceste canale folosesc tehnici de criptare, pentru a se asigura că datele, dacă sunt interceptate, nu pot fi citite fără cheia de decriptare corectă. În plus, atunci când partajați date cu organizațiile, revizuirea politicilor lor de confidențialitate și a măsurilor de securitate poate oferi o perspectivă asupra modului în care datele vor fi gestionate, memorate și partajate. Înainte de partaja datele, obținerea consimțământului explicit de la persoană este un pas critic. Acest lucru asigură că destinatarul este conștient de datele pe care le primește, de scopul datelor și de responsabilitatea lor în protejarea acestora.

Utilizarea acestor măsuri poate ajuta la asigurarea protecției datelor și la reducerea semnificativă a riscului potențialelor încălcări ale datelor sau al accesului neautorizat.

În concluzie, "Schimbul securizat de date și practici de tranzacții online" certifică înțelegerea avansată și abilitățile practice ale unei persoane în navigarea în siguranță în lumea digitală. De la recunoașterea site-urilor web nesigure și a practicilor securizate de partajare a datelor până la înțelegerea importanței verificării încrederii înainte de schimbul de date, acest MC reprezintă un angajament față de siguranța și responsabilitatea digitală, un aspect indispensabil în era interacțiunilor digitale în creștere.

Această expertiză nu numai că ajută la securizarea datelor cu caracter personal, dar contribuie și în mod semnificativ la creșterea încrederii digitale generale și la crearea unui mediu online mai sigur pentru toți utilizatorii.

Întrebări

1. De ce este important să evitați site-urile web nesigure atunci când procesați informații despre card și care sunt riscurile potențiale dacă nu faceți acest lucru?
2. Ce caracteristici ar putea indica faptul că un site web nu este sigur pentru procesarea informațiilor despre card?
3. Cum pot platformele sigure și de încredere să vă protejeze informațiile cardului în timpul tranzacțiilor online?
4. De ce este crucială verificarea încrederii persoanelor înainte de a le partaja date sensibile?
5. Ce măsuri pot fi luate pentru a verifica încrederea unei persoane înainte de a partaja ce aceasta date sensibile?
6. Cum pot canalele de comunicații sigure să sporească siguranța schimbului de date?
7. De ce este esențial să revizuim politicile de confidențialitate și măsurile de securitate ale organizațiilor înainte de a partaja date cu acestea?
8. Care este rolul consimțământului explicit în procesul de partajare a datelor și de ce este important?
9. Cum contribuie înțelegerea și practicarea schimbului de date securizat și a practicilor de tranzacții online la siguranța și încrederea digitală generală?

Protecția datelor utilizatorilor în browsere-le web (MC 4.2.A.9)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Protecția datelor utilizatorilor în browsere-le web MC 4.2.A.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.17 și 4.2.18):

- Explicații despre ce este un cookie și cum vă poate afecta datele sensibile.
- Explicarea conceptul de „mod incognito” sau „navigare privată” în browserele web și modul de utilizare al acestuia.

Descriere

MC-ul “Protecția datelor utilizatorilor în browsere-le web” certifică cunoștințe de profunzime și capacitatea extinsă de a naviga pe internet folosind browsere (instrumente de navigare) și strategii de navigare care asigură protecția datelor sensibile ale utilizatorilor. Accentul cade pe stăpânirea conceptelor cheie, cum ar fi înțelegerea cookie-urilor web și implicațiile utilizării navigării private sau în „modul incognito”.

Primul rezultat al învățării se concentrează pe conceptul de „cookie”. Cookie-urile sau cookie-urile HTTP sunt fișiere mici care sunt memorate pe calculatorul unui utilizator atunci când acesta vizitează un site web. Aceste fișiere sunt folosite de către site-ul web pentru a reține informații despre vizită, cum ar fi preferințele utilizatorului, informațiile de conectare sau articolele dintr-un coș de cumpărături. Prin salvarea acestor informații, site-urile web pot oferi o experiență personalizată a utilizatorului și pot face vizitele ulterioare mai eficiente. Cu toate acestea, în timp ce aceste module cookie contribuie în mod semnificativ la confortul utilizatorului, ele pot prezenta, de asemenea, potențiale riscuri pentru confidențialitatea utilizatorului și securitatea datelor sensibile.

Cookie-urile pot fi clasificate în general în două tipuri: cookie-uri de sesiune și cookie-uri persistente. Cookie-urile de sesiune, sau cookie-urile tranzitorii, sunt temporare și sunt șterse când utilizatorul își închide browserul. Ele sunt utilizate în principal pentru sarcini precum întreținerea unui coș de cumpărături sau amintirea acțiunilor unui utilizator în cadrul unei sesiuni de navigare. Pe de altă parte, cookie-urile persistente rămân pe computerul utilizatorului chiar și după ce acesta și-a închis browserul. Aceste module cookie sunt folosite pentru a reține preferințele și comportamentul utilizatorului pe o perioadă lungă de timp și sunt cele mai frecvent asociate cu preocupările legate de confidențialitate.

Cookie-urile terță parte (third-party cookies), o submulțime a modulelor cookie persistente, sunt discutabile în privința confidențialității datelor. Spre deosebire de cookie-urile “first-party”, care sunt setate de site-ul web pe care îl vizitează un utilizator, cookie-urile terță parte sunt setate de către alte domenii, nu de către domeniul vizitat. Aceste cookie-uri sunt adesea folosite pentru publicitate online și pot urmări obiceiurile de navigare ale unui utilizator pe mai multe site-uri web. Această capacitate de a urmări comportamentul utilizatorilor a ridicat îngrijorări semnificative cu privire la confidențialitate și securitatea datelor.

Având în vedere acest lucru, înțelegerea modului de gestionare și control al setărilor cookie-urilor este crucială. Majoritatea browsere-lor web oferă opțiuni pentru a bloca cookie-urile de la terți, pentru a șterge toate cookie-urile sau pentru a alerta utilizatorul când este setat un cookie. Prin gestionarea activă a acestor setări, utilizatorii își pot proteja datele sensibile și își pot menține confidențialitatea online.

Al doilea rezultat de învățare se adâncește în conceptul de „mod incognito” sau „navigare privată”. Aceasta este o caracteristică - disponibilă în majoritatea browserelor web - care permite unui utilizator să navigheze pe

internet fără ca browserul să stocheze informații precum istoricul de navigare, istoricul căutărilor sau cookie-urile. Când un utilizator deschide o nouă fereastră incognito sau o sesiune de navigare privată, browserul creează o sesiune temporară separată, care este izolată de sesiunea principală de navigare și de datele utilizatorului.

Cu toate acestea, în timp ce navigarea privată poate împiedica alți utilizatori ai aceluiași dispozitiv să vă vadă activitatea de navigare, aceasta nu vă face invizibil pe internet.

Site-urile web vizitate, furnizorii de servicii de internet și administratorii de rețea pot urmări în continuare activitățile de navigare. Acest lucru este important de reținut, deoarece mulți oameni cred în mod eronat că navigarea privată oferă anonimat complet și protecție online.

În general, MC-ul "Protecția datelor utilizatorilor în browsere-le web" vizează complexitatea gestionării datelor utilizatorilor în timp ce navighează în peisajul digital. De la înțelegerea rolului cookie-urilor până la a ști cum și când să utilizați navigarea privată, MC-ul reprezintă un angajament față de siguranța digitală și față de confidențialitate. Aceste cunoștințe sunt esențiale pentru promovarea unui mediu digital sigur și de încredere, permițând utilizatorilor să interacționeze cu platformele online cu încredere și responsabilitate.

Întrebări

1. Ce este un cookie, în contextul browserelor web, și cum funcționează?
2. Care este diferența dintre cookie-urile de sesiune și cookie-urile persistente? Oferiți exemple de utilizare a acestora.
3. Explicați conceptul de cookie-uri terță parte și de ce sunt asociate cu probleme de confidențialitate.
4. Cum pot utilizatorii să gestioneze și să controleze setările cookie-urilor în browserele lor web pentru a-și proteja datele sensibile?
5. Ce este „modul incognito" sau „navigare privată" și cum diferă de navigarea obișnuită?
6. Cum ajută „modul incognito" sau „navigare privată" la protejarea confidențialității utilizatorilor?
7. Care sunt limitările „modului incognito" sau ale „navigării private" în ceea ce privește protejarea confidențialității utilizatorilor?
8. Cum afectează „modul incognito" sau „navigarea privată" memorarea și utilizarea cookie-urilor?
9. Discutați de ce înțelegerea cookie-urilor și a „modului incognito" este esențială pentru confidențialitatea și securitatea datelor.
10. Cum poate înțelegerea și gestionarea cookie-urilor să contribuie la o experiență personalizată a utilizatorului?
11. Explicați modul în care utilizarea „modului incognito" sau „navigare privată" afectează reținerea datelor utilizatorilor.

Inițiere în siguranța digitală și în confidențialitate (MC 4.2.A.10)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Inițiere în siguranța digitală și în confidențialitate **Cod: MC 4.2.A.10**
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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.19 și 4.2.20):

- Testarea cunoștințelor despre politicile de confidențialitate ale site-urilor web vizitate frecvent.
- Recomandarea – către prieteni și familie – a celor mai bune practici pentru siguranța online.

Descriere

În lumea contemporană, o dată cu prezența extinsă a tehnologiei digitale în viața de zi cu zi, înțelegerea complexității confidențialității și a siguranței digitale constituie o necesitate, nu un lux. Acest MC este conceput pentru a oferi cursanților cunoștințele și abilitățile necesare pentru a naviga în peisajul digital complex cu încredere, asigurându-se că interacțiunile lor online sunt ghidate de principiile confidențialității și ale securității.

Primul rezultat al învățării din acest MC vizează capacitatea cursanților de a înțelege și de a evalua critic politicile de confidențialitate ale site-urilor web vizitate frecvent. Politicile de confidențialitate, în esență, servesc ca un contract legal între operatorul unui site web și utilizatorii sau vizitatorii acestuia, delimitând diferiți parametri, cum ar fi tipurile de date colectate, scopul colectării, modul în care datele sunt memorate, utilizate și eventual partajate. Aceste politici, de cele mai multe ori, sunt trecute cu vederea sau nu sunt complet înțelese de către utilizatori, ceea ce duce la partajarea involuntară a informațiilor personale și la potențiale încălcări ale confidențialității.

Pentru a atenua astfel de situații, cursanții vor aprofunda studiul diferitelor politici de confidențialitate, vor recunoaște componentele lor critice și vor învăța cum să le interpreteze implicațiile în scenarii din lumea reală. Această înțelegere formează baza luării deciziilor informate cu privire la interacțiunile cu site-urile web și gestionarea eficientă a amprentei digitale. Acest prim scop urmărit în cadrul MC-ului va oferi cursanților capacitatea de a evalua în mod critic aceste politici, testându-și cunoștințele față de o serie de scenarii diferite din lumea reală, asigurându-se astfel că nu numai că își pot proteja datele personale, ci și pot respecta drepturile de confidențialitate digitală ale altora.

Al doilea rezultat al învățării din acest MC se concentrează pe pledoaria pentru siguranța digitală, o cerință critică în era digitală actuală. Ca parte a unei comunități online mai mari, este esențial să extindem responsabilitatea siguranței digitale dincolo de noi înșine, împărtășind aceste cunoștințe cruciale și altora. Înțelegând și implementând cele mai bune practici pentru siguranța online, persoanele pot ghida prietenii și familia în promovarea unei prezențe online sigure și securizate.

Aceste bune practici includ sfaturi privind crearea de parole solide, recunoașterea și evitarea înșelătoriilor de tip phishing, securizarea rețelelor de la domiciliu, utilizarea canalelor de comunicare criptate și reducerea cantității de informații personale partajate online. Pentru a împărtăși în mod eficient aceste practici, cursanții trebuie să înțeleagă temeinic raționamentul din spatele fiecărei recomandări și contribuția acesteia la îmbunătățirea siguranței generale online. Procedând astfel, ei nu numai că se protejează, ci joacă și un rol crucial în cultivarea unui mediu online mai sigur pentru toată lumea.

Cele două rezultate ale învățării – vizate prin acest MC - urmăresc să consolideze în mod semnificativ inițierea în siguranța digitală și în confidențialitate, permițând cursanților să se protejeze și să contribuie pozitiv la

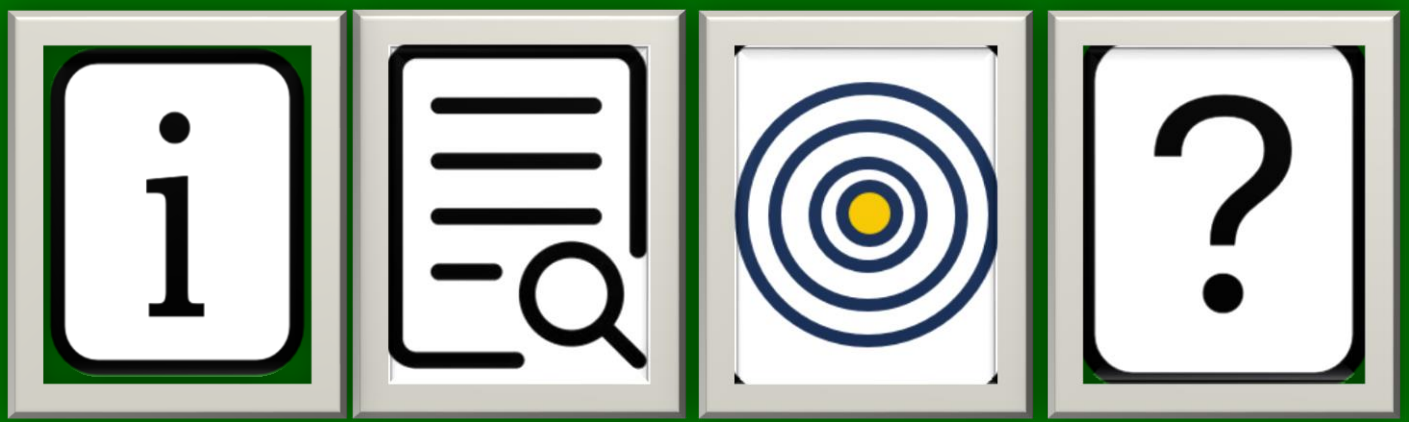
siguranța celorlalți în lumea digitală. Acest MC urmărește o înțelegere extinsă a politicilor de confidențialitate și a celor mai bune practici pentru siguranța online, și o aplicare a acestor cunoștințe dobândite de către cursanți într-un mod practic, semnificativ și influent. Peisajul digital ar putea fi complex, dar cu abilitățile și cunoștințele dobândite prin acest MC, navigarea - în siguranță și cu încredere – în internet devine o sarcină fezabilă.

Întrebări

1. Care este rolul unei politici de confidențialitate pe un site web?
2. Cum vă pot influența politicile de confidențialitate ale site-urilor web interacțiunea cu acestea?
3. Care sunt posibilele implicații ale neînțelegerii politicii de confidențialitate a unui site web?
4. De ce este important să împărtășiți cunoștințele despre practicile de siguranță online cu prietenii și familia?
5. Care sunt componentele critice care trebuie căutate în politica de confidențialitate a unui site web?
6. Cum poate contribui înțelegerea politicii de confidențialitate a unui site web la gestionarea amprentei Dvs. digitale?
7. Dați un exemplu pentru cea mai bună practică pentru siguranța online pe care ați recomanda-o unui prieten sau unui membru al familiei.
8. Cum contribuie parolele robuste la siguranța online și cum ați sfătui pe cineva să creeze o astfel de parolă?
9. Ce pași ați recomanda unei persoane pentru a o ajuta să-și securizeze rețeaua de acasă?
10. Descrieți un scenariu în care lipsa de înțelegere a politicii de confidențialitate a unui site web ar putea duce la o violare a confidențialității.
11. Ce măsuri pot lua utilizatorii pentru a reduce cantitatea de informații personale pe care le distribuie online?
12. Ce sunt înșelătoriile de tip phishing și cum pot oamenii să le recunoască și să le evite?
13. Cum pot canalele de comunicare criptată să sporească siguranța online și când ar trebui utilizate?

NIVELUL INTERMEDIAR

(Nivelul 3 și Nivelul 4)



Conștientizare în domeniul securității cibernetice și protecția datelor cu caracter personal (MC 4.2.B.1)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Conștientizare în domeniul securității cibernetice și protecția datelor cu caracter personal **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.21 și 4.2.22)

- Recomandarea – către prieteni și familie - celor mai bune practici pentru siguranța online.
- Identificarea acțiunilor adecvate care trebuie luate atunci când datele personale sunt utilizate abuziv pe platformele de social media.

Descriere

În universul digital de astăzi, importanța deținerii unor cunoștințe extinse despre siguranța online și protecția datelor nu a fost niciodată mai mare. MC-ul "Conștientizare în domeniul securității cibernetice și protecția datelor cu caracter personal" este meticulos proiectat pentru a oferi cursanților aceste cunoștințe indispensabile.

Programul acoperă în mod complex două domenii esențiale ale siguranței online și ale strategiilor de utilizare abuzivă a datelor pe platformele de rețele sociale, cu scopul de a crea cetățeni digitali informați și alertați.

Prima zonă crucială de învățare a MC-ului "Conștientizare în domeniul securității cibernetice și protecția datelor cu caracter personal" implică cultivarea unei abilități nuanțate de a ghida prietenii și familia cu privire la cele mai bune practici pentru siguranța online. Pe fondul creșterii numărului de amenințări digitale, care includ atacuri cibernetice, escrocherii online și hărțuire cibernetică, este vital ca utilizatorii să fie familiarizați cu măsurile de protecție. MC-ul urmărește să cultive abilitățile necesare pentru a analiza caracteristicile de siguranță și de securitate ale diverselor platforme digitale, pentru a recunoaște potențialele pericolele și pentru a sugera soluții pentru a reduce vulnerabilitățile. Deținând aceste abilități, cursanții se pot proteja de amenințările digitale și pot acționa ca membri activi pentru siguranța online în comunitățile lor. Acest aspect al programului consolidează importanța acțiunii colective în promovarea unui mediu digital sigur.

A doua componentă esențială de învățare a MC-ului "Conștientizare în domeniul securității cibernetice și protecția datelor cu caracter personal" este gestionarea strategică și răspunsul la utilizarea abuzivă a datelor cu caracter personal pe platformele de social media. Creșterea exponențială a rețelelor sociale a condus la o multitudine de preocupări legate de confidențialitate și securitate. Utilizarea greșită a datelor cu caracter personal, de la furtul de identitate la partajarea neautorizată a datelor și chiar exploatarea comercială, este, din păcate, obișnuită. Prin urmare, este imperativ ca persoanele fizice să poată discerne când datele lor personale au fost compromise și să poată lua contramăsurile adecvate. Acest MC îi ajută pe cursanți să își perfecționeze abilitățile necesare pentru a-și gestiona în mod eficient persoanele online, pentru a-și reglementa amprenta digitală, pentru a recunoaște semnele de utilizare abuzivă a datelor cu caracter personal și pentru a lua măsuri corective adecvate, cum ar fi raportarea încălcărilor, blocarea accesului neautorizat și protejarea datelor cu caracter personal.

Un aspect suplimentar de învățare în acest MC este introducerea în aspectele etice și legale ale siguranței și securității digitale. Această introducere îi va ajuta pe cursanți să înțeleagă rețeaua complexă de legi și reglementări care guvernează domeniul siguranței și securității digitale, permițându-le să le folosească pentru a-și proteja identitățile online și datele personale. Înțelegerea legalității interacțiunilor digitale ajută la promovarea cetățeniei digitale responsabile și informate.

Prin integrarea celor două obiective esențiale de învățare, MC-ul "Conștientizare în domeniul securității cibernetice și protecția datelor cu caracter personal" prezintă o perspectivă detaliată și atotcuprinzătoare asupra siguranței digitale și a protecției datelor. Scopul este de a firniza cursanților instrumentele și cunoștințele necesare pentru a-și asigura propria protecție în sfera digitală și pentru a disemina această înțelepciune în comunitatea lor. Drept urmare, cei care finalizează acest program vor fi adepți în a gestiona diversele provocări și oportunități ale lumii digitale, navigând în peisajul online în siguranță și cu încredere.

În concluzie, MC-ul "Conștientizare în domeniul securității cibernetice și protecția datelor cu caracter personal" constituie un instrument vital pentru oricine dorește să manevreze prin lumea digitală în siguranță și cu încredere. Încurajând o înțelegere profundă a acestor domenii cruciale, cursanții nu numai că își vor asigura propria siguranță digitală, ci și vor contribui în mod semnificativ la conturarea unui mediu digital mai sigur pentru toți. Prin abordarea sa cuprinzătoare și detaliată, acest program abordează nevoia presantă de educație privind siguranța digitală în lumea noastră din ce în ce mai conectată.

Întrebări

1. Care sunt unele dintre principalele amenințări digitale menționate în acest MC și care este importanța recunoașterii acestor amenințări?
2. Ce competențe își propune să dezvolte MC-ul pentru a ajuta persoanele să evalueze siguranța și securitatea diferitelor platforme digitale?
3. Cum pot persoanele dotate cu cunoștințele din acesă MC să contribuie la promovarea unui mediu digital sigur în comunitățile lor?
4. Care sunt potențialele forme de utilizare abuzivă a datelor cu caracter personal pe platformele de rețele sociale și de ce este important să le recunoaștem?
5. Care sunt acțiunile recomandate pe care persoanele fizice le pot întreprinde atunci când identifică utilizarea greșită a datelor lor personale pe rețelele sociale?
6. În ce moduri MC-ul îi ajută pe cursanți să-și gestioneze în mod eficient persoanele online?
7. Cum instruiește MC-ul persoanele să își reglementeze amprentele digitale?
8. Cum contribuie înțelegerea aspectelor etice și legale ale siguranței și securității digitale la o cetățenie digitală informată, conform MC-ului?
9. Cum pot persoanele fizice să folosească legile și reglementările care guvernează siguranța și securitatea digitală pentru a-și proteja identitățile online și datele personale?
10. În ce mod pregătește MC-ul cursanții să facă față diverselor provocări și oportunități ale lumii digitale?
11. Cum contribuie MC-ul la modelarea unui mediu digital mai sigur pentru noi toți, în conformitate cu obiectivele programului?

Cetățenie digitală și competență în securitatea online (MC 4.2.B.2)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Cetățenie digitală și competență în securitatea online **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.23, 4.2.24 și 4.2.25):

- Utilizarea identificării electronice pentru serviciile furnizate de autoritățile publice și sectorul de afaceri.
- Acordarea de prioritate protecției datelor atunci când utilizați rețelele sociale în scopuri profesionale sau educaționale.
- Recunoașterea escrocheriilor online și dezvoltarea unui scepticism sănătos față de ofertele nesolicitate online.

Descriere

În lumea în care trăim, observăm o dependență din ce în ce mai mare de instrumentele și platformele digitale; ca urmare, nevoia ca indivizii să devenă bine pregătiți în practicile de siguranță și securitate online a devenit primordială. MC-ul "Cetățenie digitală și competență în securitate online" își propune să ofere cursanților cunoștințele și abilitățile necesare pentru a naviga în siguranță, responsabil, în lumea digitală. Acest MC abordează trei domenii de bază - utilizarea identificării electronice (e-ID), protecția datelor în timpul utilizării rețelelor sociale profesionale sau educaționale și recunoașterea și scepticismul în privința înșelătoriilor online.

Primul rezultat al învățării din acest MC este înțelegerea și utilizarea eficientă a identificării electronice când folosim servicii oferite de autoritățile publice și de sectoarele de afaceri. Proliferarea serviciilor online într-o gamă largă de domenii, de la bancar la educație, necesită utilizarea unor metode de identificare sigure.

Identificarea electronică (e-ID) oferă o modalitate sigură și eficientă de a verifica online identitatea unei persoane, eliminând necesitatea metodelor de identificare fizică. Cu toate acestea, utilizarea e-ID-urilor aduce și provocări unice în ceea ce privește asigurarea confidențialității și a securității datelor. Prin intermediul acestui MC, cursanții vor dobândi o înțelegere aprofundată a sistemelor e-ID, incluzând principiile funcționării lor, beneficiile și potențialele riscuri de securitate. Programul analizează, de asemenea, cele mai bune practici pentru utilizarea e-ID-urilor, cum ar fi cum să păstrați datele e-ID în siguranță și ce să faceți în cazul unui potențial furt de identitate sau a unor încălcări ale datelor.

Ce este e-ID?

Identificarea electronică, denumită adesea e-ID, este o soluție digitală pentru dovada identității. Aceasta capătă o importanță din ce în ce mai mare, într-o lume în care tranzacțiile și interacțiunile sunt din ce în ce mai des efectuate online.

E-ID-urile sunt omoloagele digitale ale cărților și documentelor fizice de identitate. Acestea autentifică identitatea utilizatorului, permițând tranzacții și interacțiuni online sigure. Utilizarea e-ID-urilor se extinde în diferite sectoare, cuprinzând servicii furnizate atât de către autoritățile publice, cât și de către entitățile de afaceri.

În sectorul public, identificarea electronică poate simplifica și securiza procese, cum ar fi declarații de impozit, cererea de beneficii, votul și alte activități civice.

Guvernele din întreaga lume implementează sisteme e-ID pentru a asigura identitățile digitale ale cetățenilor lor, facilitând astfel furnizarea eficientă a serviciilor publice.

În sectorul de afaceri, utilizarea identificării electronice este răspândită în mai multe domenii. De exemplu, în industria bancară și financiară, e-ID-ul este utilizat pentru verificarea identității - pentru a preveni frauda în timpul tranzacțiilor-, pentru crearea unui cont și și pentru accesul la serviciile financiare. În sectorul comerțului electronic, e-ID poate ajuta la asigurarea tranzacțiilor sigure de bunuri și servicii, protejând atât consumatorii, cât și întreprinderile de fraudă. În domeniul sănătății, identificarea electronică poate fi utilizată pentru a accesa în siguranță dosarele personale de sănătate, pentru a programa întâlniri și pentru a efectua consultații de telesănătate.

În ciuda utilizării pe scară largă și a beneficiilor aduse, identificarea electronică aduce, de asemenea, o serie de provocări. Cele mai importante dintre acestea sunt preocupările privind confidențialitatea și securitatea datelor. E-ID-urile, dacă nu sunt protejate corespunzător, pot fi susceptibile la accesul neautorizat, hacking sau chiar furt de identitate. Prin urmare, utilizatorii trebuie să înțeleagă mecanismele sistemelor e-ID, memorarea securizată și gestionarea credențialelor e-ID-lor, precum și procedurile care trebuie urmate în caz de suspiciune sau de compromis.

MC-ul “Cetățenie digitală și competență în securitatea online” recunoaște importanța e-ID în lumea digitală modernă. Acesta își propune să furnizeze cursanților o înțelegere aprofundată a principiilor funcționării e-ID-urilor, a beneficiilor sale, a potențialelor riscuri de securitate și a celor mai bune practici pentru utilizarea în siguranță a e-ID-urilor. Cursanții sunt educați cu privire la nuanțele menținerii securității datelor lor de identificare electronică și pașii pe care trebuie să îi urmeze în cazul în care bănuiesc că datele lor au fost compromise.

Investind timp în înțelegerea identificării electronice și a aspectelor de securitate aferente acesteia, persoanele pot valorifica potențialul serviciilor digitale, asigurându-se în același timp că identitățile lor sunt protejate. MC-ul urmărește să furnizeze cursanților cunoștințele și instrumentele necesare pentru a naviga în această zonă complexă, dar esențială a lumii digitale.

Al doilea rezultat al învățării este înțelegerea și prioritizarea protecției datelor, în timpul utilizării rețelelor sociale în scopuri profesionale sau educaționale. O dată cu utilizarea crescândă a platformelor de social media pentru muncă și educație, securitatea datelor personale și profesionale nu a fost niciodată mai crucială. Acest MC educă cursanții cu privire la riscurile potențiale asociate cu utilizarea profesională sau educațională a rețelelor sociale, cum ar fi scurgerile neintenționate de date sau utilizarea greșită a datelor de către terți. De asemenea, oferă instruire cuprinzătoare privind setările de confidențialitate, practicile de partajare securizată a datelor și gestionarea amprentelor digitale. În plus, cursanții vor dobândi o înțelegere profundă a legilor și reglementărilor relevante privind protecția datelor, cum ar fi Regulamentul general privind protecția datelor (GDPR), permițându-le să-și înțeleagă drepturile și responsabilitățile privind protecția datelor.

Al doilea rezultat de învățare al microcreditelor “Cetățenie digitală și competență în securitatea online”de cetățenie digitală și competență în securitate online se învârte în jurul înțelegerii și prioritizării protecției datelor în timpul utilizării rețelelor sociale în scopuri profesionale sau educaționale. Acest accent este de o importanță capitală într-o epocă în care platformele de social media sunt esențiale pentru multe aspecte ale vieții, inclusiv munca și educația.

Platformele de social media, în timp ce oferă oportunități de conectivitate, schimb de informații și colaborare, pot prezenta, de asemenea, riscuri substanțiale de confidențialitate. Aceste riscuri sunt deosebit de pronunțate atunci când aceste platforme sunt utilizate în scopuri profesionale sau educaționale. De exemplu, persoanele ar putea împărtăși informații sensibile legate de locul de muncă sau de instituția lor de învățământ, expunându-se, fără să știe, la scurgeri sau încălcări ale datelor (breșe de date).

Înțelegerea acestor riscuri potențiale este un aspect crucial al acestui rezultat al învățării. Cursanții vor fi educați despre amenințările comune la securitatea datelor asociate cu utilizarea rețelelor sociale profesionale sau educaționale, cum ar fi accesul neautorizat la conturi, scurgerile neintenționate de date și utilizarea greșită a datelor de către terți.

În plus, cursanții sunt învățați despre importanța protecției datelor pe rețelele sociale și sunt introduși în strategii eficiente pentru a-și proteja informațiile. Aceasta include învățarea despre setările de confidențialitate pe diferite platforme, cunoașterea despre ce informații să partajeze și ce informații să păstreze private și înțelegerea implicațiilor amprentelor lor digitale. Cursanții sunt, de asemenea, încurajați să dezvolte obiceiul de a verifica și actualiza în mod regulat setările de confidențialitate în conformitate cu nivelurile și cerințele lor de confort.

Mai mult, acest rezultat al învățării urmărește introducerea cursanților în aspectele legale ale protecției datelor. Acest lucru ar putea implica studierea unor reglementări precum Regulamentul general privind protecția datelor (GDPR) și înțelegerea modului în care aceste reglementări le protejează drepturile online. Astfel de cunoștințe sunt de neprețuit în mediul profesional sau educațional, unde respectarea legilor privind protecția datelor este adesea obligatorie.

În plus, programul oferă informații despre cele mai bune practici pentru partajarea în siguranță a datelor și interacțiunea profesională cu alte persoane pe aceste platforme. Sunt acoperte aspecte precum comunicarea securizată, partajarea în siguranță a fișierelor și a documentelor și recunoașterea și evitarea link-urilor sau atașamentelor potențial periculoase.

Înțelegerea și prioritizarea protecției datelor în timpul utilizării rețelelor sociale în scopuri profesionale sau educaționale este o abilitate complexă, dar vitală în era digitală de astăzi. Prin stăpânirea acestui rezultat al învățării, cursanții pot utiliza cu încredere și în siguranță rețelele sociale pentru progresul lor profesional și educațional, asigurându-se în același timp că datele lor personale rămân în siguranță.

Al treilea rezultat de învățare se concentrează pe recunoașterea înșelătoriilor online și pe dezvoltarea unui scepticism sănătos față de ofertele nesolicitate online. În era digitală, înșelătoriile au devenit din ce în ce mai sofisticate, ceea ce face esențial ca indivizii să rămână vigilenți și sceptici față de potențialele amenințări. Acest MC oferă o imagine de ansamblu asupra tipurilor comune de escrocherii online, cum ar fi phishingul, programele malware și furtul de identitate. De asemenea, în instruiește pe cursanți în strategiile practice pentru identificarea înșelătoriilor, inclusiv recunoașterea e-mailurilor, link-urilor și a site-urilor web suspecte și verificarea autenticității ofertelor nesolicitate. Programul oferă, de asemenea, îndrumări cu privire la ce trebuie făcut dacă cineva este victima unei escrocherii, inclusiv mecanisme de raportare și pașii de urmat pentru a atenua daunele.

Cel de-al treilea rezultat al învățării din MC-ul “Cetățenia digitală și competența în securitatea online” se concentrează pe recunoașterea înșelătoriilor online și pe cultivarea unui scepticism sănătos față de ofertele

nesolicitate online. Această înțelegere este crucială în peisajul digital de astăzi, în care înșelătoriile și activitățile frauduloase sunt din ce în ce mai sofisticate și omniprezente.

Înșelătoriile online vin sub mai multe forme și exploatează adesea lipsa de cunoștințe a persoanelor despre practicile sigure pe internet. Printre cele mai frecvente escrocherii se numără încercările de phishing, în care escrocii se maschează în entități legitime pentru a păcăli utilizatorii să dezvăluie informații personale și frauda cu taxă și câștiguri mari (advanced fee fraud), în care escrocii promit profituri mari în schimbul unei taxe inițiale. Alte escrocherii pot implica loterii sau premii false, piețe online frauduloase sau chiar escrocherii romantice care îi exploatează pe cei singuri și vulnerabili.

În acest MC cursanții sunt familiarizați cu diferitele tipuri de escrocherii online și modul de funcționare a acestora; învață să recunoască semnele înșelătoriilor, care pot include comunicări nesolicitate, tactici de presiune, oferte prea bune pentru a fi adevărate, solicitări de informații sensibile și metode de plată neobișnuite.

În plus, cursanții vor învăța despre instrumentele și strategiile de verificare a autenticității ofertelor nesolicitate. Acestea pot include tehnici precum verificarea adresei de e-mail sau a adresei URL a expeditorului pentru anomalii, cercetarea online a ofertei sau a expeditorului, contactarea directă a presupusului expeditor printr-o metodă verificată și să nu facă click/să nu selecteze pe linkuri sau atașamente suspecte.

O parte cheie a acestui rezultat de învățare este stimularea unui sentiment de scepticism sănătos față de ofertele nesolicitate online. Cursanții sunt încurajați să pună la îndoială legitimitatea ofertelor neașteptate și să își facă întotdeauna timp pentru a verifica înainte de a se implica. Li se reamintește că entitățile legitime rareori, sau chiar niciodată, solicită informații sensibile sau plăți prin e-mail sau mesaj text.

Cursanților li se oferă, de asemenea, îndrumări cu privire la ce trebuie să facă dacă sunt victimele unei înșelătorii. Aceasta include pași imediați, cum ar fi contactarea băncii sau a companiei cardului de credit, schimbarea parolelor și raportarea înșelătoriei către organele locale de aplicare a legii și platformele online. Ei sunt, de asemenea, educați cu privire la măsurile pe termen lung, cum ar fi monitorizarea rapoartelor lor de credit pentru a identifica semnele unui furt de identitate.

Abilitatea de a recunoaște înșelătoriile online și de a menține un scepticism sănătos față de ofertele nesolicitate online este o abilitate esențială pentru navigarea în lumea digitală. Prin acest rezultat al învățării, indivizii sunt echipați cu cunoștințele și instrumentele pentru a se proteja de escrocherii online, contribuind la un mediu online mai sigur și mai sigur.

Pe scurt, MC-ul “Cetățenie digitală și competență în securitatea online” le furnizează cursanților o înțelegere extinsă asupra a trei aspecte critice ale siguranței și securității online - identificarea electronică, protecția datelor pe rețelele sociale și escrocheriile online. Prin finalizarea acestui program, cursanții vor fi dotați cu cunoștințele și abilitățile necesare pentru a naviga în siguranță în lumea digitală, a-și proteja datele personale și profesionale și a susține practici digitale sigure și responsabile în comunitățile lor.

Acest program aprofundat și detaliat necesită un angajament semnificativ din partea cursanților, dar promite să furnizeze cunoștințe și abilități esențiale care devin din ce în ce mai esențiale în lumea digitală modernă. Pe măsură ce viețile noastre devin din ce în ce mai împletite cu tehnologiile digitale, acest MC reprezintă o investiție critică în siguranța și securitatea digitală individuală și colectivă.

Întrebări

1. Ce este identificarea electronică (e-ID) și de ce este importantă în lumea digitală de astăzi?
2. Care sunt potențialele riscuri de securitate asociate cu utilizarea e-ID și cum pot fi atenuate acestea?
3. Explicați cele mai bune practici pentru utilizarea în siguranță a e-ID-ului.
4. Ce pași ar trebui urmați în cazul în care o persoană suspectează că datele sale de identitate electronică au fost compromise?
5. De ce este crucială protecția datelor atunci când utilizați rețelele sociale în scopuri profesionale sau educaționale?
6. Prezentați câteva amenințări - la securitatea datelor asociate cu utilizarea profesională sau educațională a rețelelor sociale – întâlnite în mod frecvent.
7. Cum își poate gestiona un individ amprenta digitală în mod eficient pe platformele de social media?
8. Descrieți rolul legilor și al reglementărilor, cum ar fi GDPR, în protecția datelor pe rețelele sociale.
9. Care sunt cele mai bune practici pentru partajarea în siguranță a datelor pe platformele de rețele sociale în scopuri profesionale sau educaționale?
10. Definiți înșelătoriile online și oferiți exemple de tipuri obișnuite de escrocherii pe care oamenii le pot întâlni online.
11. Care sunt unele semnale roșii sau semne de înșelătorie online de care ar trebui să fie conștienți oamenii?
12. Explicați tehnicile de verificare a autenticității ofertelor nesolicitate online.
13. Discutați despre importanța dezvoltării unui scepticism sănătos față de ofertele nesolicitate online.
14. Ce pași imediați ar trebui urmați de către o persoană care este victima unei escrocherii online?
15. Care sunt măsurile pe termen lung pe care oamenii le pot lua după ce au căzut victimele unei escrocherii online?

Cele mai bune practici de securitate cibernetică și evaluarea comportamentului online (MC 4.2.B.3)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Cele mai bune practici de securitate cibernetică și evaluarea comportamentului online **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.26 și 4.2.27):

- Instalarea și actualizarea software-ului de securitate necesar, pe calculatorul și smartphone-ul Dvs.
- Evaluarea obiceiurilor online în funcție de riscul lor de securitate.

Descriere

În era digitală actuală, în care utilizarea dispozitivelor tehnologice - cum ar fi calculatorele și smartphone-urile - a devenit o obișnuință zilnică, înțelegerea practicilor de securitate cibernetică și managementul comportamentului online sunr de o importanță vitală. Programul MC “Cele mai bune practici de securitate cibernetică și evaluarea comportamentului online” se concentrează pe aceste două elemente cheie, instruind cursanții să-și pregătească dispozitivele digitale prin măsuri de securitate adecvate și să-și evalueze obiceiurile online în contextul riscului de securitate.

Primul rezultat al învățării implică instruirea cursanților pentru a-și pregăti eficient calculatorele și smartphone-urile prin instalarea și actualizarea regulată a software-ului de securitate esențial. Dispozitivele tehnologice fac parte integrantă din viața noastră, memorând date sensibile, de la informații personale până la documente profesionale. Prin urmare, asigurarea securității acestor dispozitive devine primordială.

Instalarea software-ului de securitate este un prim pas vital în protejarea acestor dispozitive. Software-ul de securitate constituie un zid de apărare împotriva diferitelor amenințări online, cum ar fi viruși, malware, ransomware și spyware. Gama de software de securitate include, printre altele, programe antivirus, firewall-uri, antispyware și instrumente de criptare. Acest rezultat al învățării vizează înțelegerea diferitelor tipuri de software de securitate, a rolurilor specifice acestora și a importanței menținerii celor mai recente versiuni.

Actualizarea regulată a software-ului de securitate este la fel de critică. Amenințările cibernetice evoluează în mod constant, în mod regulat, apar noi tipuri de viruși și programe de tip malware. Pentru a combate aceste amenințări care evoluează continuu, furnizorii de software de securitate lansează actualizări regulate, corecții (patch-uri) și îmbunătățiri ale programele lor. Aceste actualizări conțin îmbunătățiri importante și noi mijloace de apărare împotriva amenințărilor identificate recent.

Programul vizează înțelegerea procesului de actualizare a riscurilor asociate cu software-ul de securitate învechit și a importanței menținerii la zi a întregului software, inclusiv a sistemelor de operare, a browsere-lor web și a aplicațiilor.

În plus, cursul abordează și alte practici de securitate, cum ar fi crearea de parole puternice, autentificarea cu doi factori și obiceiurile de navigare în siguranță.

MC-ul își propune să construiască o bază solidă pentru asigurarea securității calculatorelor și a smartphone-urilor prin instalare și actualizări regulate ale software-ului relevant.

Securitatea software este un termen larg care include o varietate de aplicații dezvoltate pentru a proteja calculatorele și smartphone-urile de amenințările digitale. Aceasta include programe antivirus concepute pentru a identifica, eradica și apăra împotriva virușilor și a altor tipuri de malware, firewall-uri care gestionează și blochează accesul neautorizat la dispozitive, software anti-spyware care protejează împotriva colectării

neautorizate de date și instrumente de criptare care securizează datele transformându-le în un format care poate fi decriptat numai cu cheia corespunzătoare.

Acest rezultat al învățării se concentrează pe transmiterea de cunoștințe despre importanța fiecărui tip de software în menținerea securității dispozitivului. De asemenea, subliniază necesitatea unei abordări coezive de securitate în care diferite tipuri de software care creează în mod colectiv o barieră de securitate extinsă.

Frecvența actualizării tuturor software-ului de securitate instalate este un alt element esențial al securității dispozitivului. O dată cu natura în continuă evoluție a amenințărilor cibernetice și a noilor tipuri de viruși și programe malware care apar în mod constant, furnizorii de software de securitate lansează în mod obișnuit actualizări care includ îmbunătățiri, rezolvarea problemelor existente și noi apărări împotriva acestor amenințări în evoluție. Menținând software-ul de securitate actualizat, utilizatorii pot asigura o apărare optimă pentru dispozitivele lor împotriva amenințărilor.

Acest rezultat al învățării include și alte măsuri de securitate, cum ar fi actualizările periodice ale sistemului de operare și ale aplicațiilor, practicile securizate de parole, autentificarea cu doi factori și obiceiurile de navigare în siguranță, care formează împreună un protocol de securitate extinsă pentru a apăra utilizatorii de majoritatea amenințărilor digitale.

Al doilea rezultat al învățării implică dezvoltarea abilităților de a evalua obiceiurile online legate de riscul de securitate. Internetul, deși este o resursă vastă, adăpostește și potențiale amenințări de securitate. Obiceiurile online ale unei persoane pot influența semnificativ expunerea la aceste amenințări.

Acest rezultat al învățării îi instruiește pe cursanți cu privire la conceptul de risc în contextul comportamentului online. Oferă o privire de ansamblu asupra comportamentelor online cu risc ridicat, cum ar fi click-urile pe link-uri necunoscute, utilizarea rețelelor Wi-Fi nesecurizate și partajarea online a informațiilor sensibile. De asemenea, evidențiază obiceiurile cu risc scăzut care sporesc securitatea online, cum ar fi să vizitați doar site-urile web securizate prin HTTPS, să vă deconectați de la conturi atunci când nu le utilizați și să actualizați regulat setările de confidențialitate.

Prin acest program, cursanții își dezvoltă capacitatea de a-și analiza în mod critic obiceiurile online, de a distinge între comportamentele cu risc ridicat și cele cu risc scăzut și de a face ajustările necesare pentru a le spori siguranța online. Acest rezultat al învățării nu acoperă doar obiceiurile personale, ci se extinde și la comportamentul profesional, subliniind importanța obiceiurilor online sigure în protejarea nu doar a persoanelor, ci și a locurilor de muncă și a instituțiilor.

Acțiunile și obiceiurile pe care le adoptă oamenii în timp ce sunt online le afectează în mod semnificativ susceptibilitatea la amenințările cibernetice. Anumite practici, cum ar fi navigarea numai pe site-uri web securizate prin HTTPS, folosirea de parole puternice și distincte și deconectarea de la conturi atunci când nu sunt utilizate, pot reduce considerabil riscul de a fi victima unor amenințări cibernetice.

Pe de altă parte, acțiunile cu risc ridicat, cum ar fi click-ul pe linkuri din e-mailuri necunoscute, utilizarea rețelelor Wi-Fi nesecurizate și dezvăluirea excesivă de informații personale online pot crește în mod semnificativ acest risc.

În acest rezultat al învățării, indivizii sunt învățați să-și evalueze critic comportamentul online. Aceștia sunt instruiți să recunoască comportamentele care i-ar putea expune la riscuri și sunt instruiți cu cunoștințele necesare pentru a-și ajusta obiceiurile care le îmbunătățesc securitatea.

În mod crucial, această analiză nu se limitează la obiceiurile personale. Cursul acoperă, de asemenea, impactul comportamentului online într-un context de muncă. Odată cu dependența tot mai mare de platformele digitale la locul de muncă, practicile online sigure au devenit esențiale pentru protejarea nu doar a persoanelor, ci și a întreprinderilor și instituțiilor.

În concluzie, MC-ul "Cele mai bune practici de securitate cibernetică și evaluarea comportamentului online" le dă cursanților puterea să-și îmbunătățească securitatea digitală prin pregătirea eficientă a dispozitivelor lor și printr-o examinare atentă a obiceiurilor lor online. Prin finalizarea acestui program, persoanele nu numai că își vor îmbunătăți propria securitate digitală, ci vor contribui și la o comunitate digitală mai sigură. Oferă o înțelegere cuprinzătoare și o stăpânire a securității cibernetice personale, creând cetățeni digitali responsabili, bine pregătiți pentru a naviga în peisajul digital în siguranță.

Întrebări

1. Care este semnificația instalării software-ului de securitate pe dispozitive tehnologice precum calculatore și smartphone-uri?
2. Ce tipuri de software de securitate sunt disponibile și care sunt rolurile lor specifice în protejarea dispozitivelor digitale?
3. De ce este esențial să păstrați software-ul de securitate actualizat? Cum contribuie actualizările periodice la securitatea cibernetică?
4. Care sunt unele dintre riscurile asociate cu utilizarea software-ului de securitate învechit?
5. Dincolo de actualizarea software-ului de securitate, care sunt alte practici importante pentru a asigura securitatea dispozitivelor digitale?
6. Cum contribuie crearea de parole sigure și autentificarea cu doi factori la securitatea generală a dispozitivului?
7. Cum influențează acțiunile și obiceiurile unei persoane - în timp ce este online - susceptibilitatea la amenințările cibernetice?
8. Care sunt exemplele de comportamente online cu risc ridicat și cu risc scăzut în contextul securității cibernetice?
9. Cum se poate evalua în mod critic comportamentul online pentru a identifica potențiale riscuri de securitate?
10. De ce este important să facem ajustările necesare la obiceiurile online pentru a spori siguranța?
11. În ce moduri pot proteja obiceiurile online sigure nu doar indivizii, ci și locurile de muncă și instituțiile?
12. Cum contribuie acest MC la crearea de cetățeni digitali responsabili?
13. Cum îmbunătățesc cunoștințele - dobândite în acest MC – la securitatea digitală personală și cum contribuie acestea la o comunitate digitală mai sigură?

Confidențialitate digitală extinsă, siguranța copiilor și competență în navigarea în siguranță (MC 4.2.B.4)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Confidențialitate digitală extinsă, siguranța copiilor și competență în navigarea în siguranță **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.28, 4.2.29 și 4.2.30) :

- Discuții despre faptul că prelucrarea datelor cu caracter personal este supusă reglementărilor locale precum GDPR.
- Cunoașterea despre existența browsere-lor adaptate copiilor și manifestarea preocupărilor pentru siguranța online a copiilor prin utilizarea sau recomandarea acestor browsere.
- Diferențierea între site-urile web sigure și cele nesigure atunci când navigați.

Descriere

MC-ul “Confidențialitate digitală extinsă, siguranța copiilor și competență în navigarea în siguranță” este un program cu mai multe fațete, care aprofundează înțelegerea și abilitățile cursanților cu privire la trei domenii cruciale ale siguranței digitale: legile privind protecția datelor cu caracter personal, instrumentele de internet sigure pentru copii și identificarea site-urilor web sigure și nesigure..

Programul analizează aspectul critic al prelucrării datelor cu caracter personal și reglementările sale pertinente. Având în vedere volumul de date cu caracter personal care circulă online, importanța legilor privind protecția vieții private, precum Regulamentul general privind protecția datelor (GDPR) este substanțială. GDPR, o lege strictă privind confidențialitatea și securitatea implementată în Uniunea Europeană, are implicații ample pentru gestionarea datelor pe tot globul. Acest program oferă rezultate cuprinzătoare ale învățării centrate pe GDPR și legi similare care sunt concepute pentru a proteja datele personale. Aceasta include înțelegerea scopului și a elementelor cheie ale acestor reglementări, recunoașterea drepturilor persoanelor vizate și identificarea responsabilităților operatorilor de date.

Prelucrarea datelor cu caracter personal se referă la orice acțiune efectuată asupra datelor cu caracter personal, inclusiv colectarea, înregistrarea, organizarea, structurarea, memorarea, adaptarea sau modificarea, preluarea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

Reglementarea prelucrării datelor cu caracter personal a devenit extrem de importantă o dată cu creșterea digitalizării serviciilor și activităților. Legi precum Regulamentul general privind protecția datelor (GDPR) în Uniunea Europeană au fost create pentru a proteja confidențialitatea și datele personale ale cetățenilor.

GDPR a fost adoptat în 2016 și a intrat în vigoare în 2018. Este considerată una dintre cele mai dure legi privind confidențialitatea și securitatea din lume; deși a fost elaborat și adoptat de Uniunea Europeană, impune obligații organizațiilor oriunde, atâta timp cât acestea vizează sau să colecteze date referitoare la persoane din UE.

Regulamentul se bazează pe mai multe principii care privesc prelucrarea datelor cu caracter personal. Acestea includ legalitatea, corectitudinea și transparența, limitarea scopului, minimizarea datelor, acuratețea, limitarea memorării, integritatea și confidențialitatea, responsabilitatea.

Conform GDPR, persoanele au mai multe drepturi, printre care:

1. Dreptul de a fi informat: Persoanele fizice au dreptul de a fi informate cu privire la colectarea și utilizarea datelor lor personale.

2. Dreptul de acces: Persoanele fizice au dreptul de a-și accesa datele personale și informațiile suplimentare.

3. Dreptul la rectificare: Persoanele fizice au dreptul ca datele cu caracter personal inexacte să fie rectificate sau completate dacă acestea sunt incomplete.

4. Dreptul la ștergere (cunoscut și sub numele de „dreptul de a fi uitat”): Persoanele fizice au dreptul la ștergerea datelor cu caracter personal.

5. Dreptul de a restricționa prelucrarea: Persoanele fizice au dreptul de a solicita restricționarea sau suprimarea datelor lor personale.

6. Dreptul la portabilitatea datelor: Acest lucru permite persoanelor fizice să obțină și să-și refolosească datele personale în propriile scopuri în cadrul diferitelor servicii.

7. Dreptul de a se opune: În anumite circumstanțe, persoanele fizice au dreptul de a se opune prelucrării datelor lor personale.

8. Drepturi în legătură cu luarea automată a deciziilor și crearea de profiluri: Persoanele fizice au dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv pe profilare, care produce efecte juridice în privința lor sau le afectează semnificativ în mod similar.

În plus, programul se concentrează, de asemenea, pe impactul acestor reglementări asupra utilizării zilnice a internetului, explorând modul în care aceste legi influențează modul în care datele personale sunt colectate, stocate și prelucrate. Această înțelegere este esențială nu numai pentru protejarea propriilor informații digitale, dar contribuie și la menținerea unor standarde înalte de confidențialitate în mediile online profesionale și personale.

O altă arie pe care se concentrează acest MC este siguranța copiilor pe internet. Datorită numărului din ce în ce mai mare de copii care accesează internetul, necesitatea instrumentelor digitale adaptate copiilor nu a fost niciodată mai crucială. Browser-ele adaptate copiilor le oferă acestora un mediu mai sigur și mai controlat pentru a explora internetul, prin restricționarea accesului la potențialul conținut dăunător și prin asigurarea confidențialității utilizatorului tânăr.

MC-ul pune un accent puternic pe înțelegerea acestor instrumente, detaliind modul în care funcționează, caracteristicile lor cheie și beneficiile pe care le aduc pentru a asigura o experiență de internet mai sigură pentru copii. Aceste cunoștințe se dovedesc esențiale pentru persoanele implicate în activitățile online ale copiilor, cum ar fi părinții, educatorii și tutorii.; le dă putere să recomande sau să utilizeze aceste browsere, promovând astfel în mod activ și permițând o utilizare mai sigură a internetului în rândul copiilor.

Browserele adaptate copiilor, cunoscute și sub numele de browsere sigure pentru copii, sunt browsere web concepute special pentru a fi utilizate de către copii. Aceste browsere acordă prioritate siguranței online, oferind un mediu în care copiii pot explora internetul în siguranță, fără riscul de a da peste conținut neadecvat sau de a cădea pradă amenințărilor online. Utilizarea acestor browsere demonstrează un angajament față de siguranța copiilor online și poate fi recomandată părinților, educatorilor sau îngrijitorilor ca instrument de promovare a utilizării sigure și pozitive a internetului.

Una dintre caracteristicile principale ale browserelor prietenoase pentru copii este filtrarea conținutului. Această funcție împiedică accesul la site-uri web care conțin materiale explicite, violente sau neadecvate, blocându-le automat. Unele browsere adaptate copiilor folosesc o abordare de tip listă albă, în care pot fi accesate numai site-urile web aprobate în prealabil. Alții folosesc un sistem de tip listă neagră, în care anumite site-uri dăunătoare sau neadecvate sunt blocate. Mulți folosesc o combinație a ambelor.

Unele browsere adaptate copiilor includ, de asemenea, funcții de gestionare a timpului, permițând adulților să stabilească limite pentru timpul pe care îl pot petrece copiii online. Acestea ajută la prevenirea dependenței de internet.

O altă caracteristică comună acestor browsere o reprezintă interfețele utilizator simplificate, cu butoane mai mari și cu meniuri simplificate, prin care utilizatorii tineri navighează mai ușor. Unele oferă chiar indicii vizuale și auditive pentru a ghida experiențele de navigare ale copiilor.

Confidențialitatea este un alt aspect critic al browserelor adaptate copiilor. Nu colectează date cu caracter personal și nu permit reclame de la terți, ceea ce este crucial în era preocupărilor legate de confidențialitatea digitală. De asemenea, adesea integrează instrumente și resurse educaționale, oferind un mediu online productiv pentru învățare.

Câteva exemple de browsere adaptate copiilor sunt Zoodles, KidzSearch și KIDOZ. Aceste platforme oferă copiilor un mediu sigur și controlat pentru a explora internetul, pentru a învăța lucruri noi și pentru a se distra online.

Promovarea utilizării browser-elor adaptate copiilor este un pas important în asigurarea siguranței online pentru copii. Este o parte a cetățeniei și conștientizării digitale, arătând preocuparea și responsabilitatea pentru experiențele online ale copiilor. Prin utilizarea sau recomandarea acestor browsere, se poate contribui la un mediu online mai sigur pentru cei mai vulnerabili utilizatori de internet.

Este important să rețineți că, deși browserele adaptate copiilor sunt un instrument excelent pentru siguranța online, ele ar trebui utilizate împreună cu supravegherea activă a adulților și cu îndrumările despre comportamentul online sigur. Combinația dintre tehnologie și educație este cea mai bună abordare pentru a menține copiii în siguranță în online.

Rezultatul final al învățării critice al programului se concentrează pe diferențierea dintre site-urile web sigure și nesigure. Cu numeroase amenințări potențiale la adresa securității cibernetice, este esențial ca utilizatorii de internet să poată identifica și diferența între site-urile web care oferă o conexiune sigură, criptată și cele care nu fac acest lucru.

Trebuie înțelese principiile conexiunilor securizate, recunoscute indiciile vizuale asociate site-urilor web securizate (cum ar fi protocoalele HTTPS și simbolul lacătului) și înțelese potențialele riscuri ale navigării pe site-urile web nesigure. Se utilizează instrumente pentru evitarea potențialele amenințări, cum ar fi malware, phishing și furtul de date, sporind considerabil siguranța persoanei și securitatea datelor sale personale în timpul navigării online.

Conexiunile securizate constituie o parte fundamentală a navigării sigure pe web, în special atunci când se interacționează cu site-uri web care necesită informații sensibile, cum ar fi site-urile bancare online sau de cumpărături. Înțelegerea principiilor conexiunilor securizate ajută persoanele să facă diferența între site-urile

web sigure și cele nesigure, deci ajută la atenuarea riscului de furt de date sau a altor activități rău intenționate.

O conexiune securizată la un site se realizează prin protocolul cunoscut sub numele de HTTPS (Hypertext Transfer Protocol Secure). Aceasta este o versiune de HTTP-ului care funcționează în combinație cu un alt protocol, SSL (Secure Sockets Layer) sau cu succesorul său, TLS (Transport Layer Security), pentru a transporta datele în siguranță.

Când un utilizator vizitează un site web cu o conexiune HTTPS, browser-ul utilizatorului va forma o conexiune securizată cu serverul site-ului web. Această conexiune este criptată, ceea ce înseamnă că orice date transferate între dispozitivul utilizatorului și server (cum ar fi parole, numere de card de credit sau alte informații personale) nu pot fi citite sau modificate cu ușurință de către o terță parte. Criptarea are loc folosind un certificat SSL sau TLS, pe care serverul site-ului îl oferă.

Pentru a identifica o conexiune securizată la un site web, există mai multe indicii vizuale pe care utilizatorii ar trebui să le caute în browserul lor web:

1. Adresa URL a site-ului web: Un site web securizat va avea „https://” la începutul adresei URL. „S” înseamnă „securizat” și este indicatorul cheie al unei conexiuni securizate.

2. Pictograma lacăt: Cele mai multe browsere web moderne afișează o pictogramă cu un lacăt în bara de adrese atunci când utilizatorul vizitează un site web securizat. Dacă faceți click pe lacăt, veți obține adesea informații suplimentare despre securitatea site-ului web.

3. Informații despre certificat: făcând click pe pictograma lacăt, utilizatorii pot accesa informații despre certificatul SSL sau TLS al site-ului, inclusiv cine l-a emis și cât timp este valabil.

4. Sigiliul site-ului (website seal) web: Unele site-uri web securizate afișează un sigiliu de securitate, care este un indicator vizual furnizat de entitatea care a emis certificatul SSL sau TLS.

5. Bara verde de adrese: în unele browsere, bara de adrese sau numele proprietarului site-ului web va deveni verde pentru site-urile deosebit de sigure care au un certificat SSL de validare extinsă (EV).

Este important de reținut că, deși aceste indicii vizuale indică faptul că a fost stabilită o conexiune sigură, ele nu garantează că site-ul în sine este sigur sau că nu conține conținut rău intenționat. Utilizatorii ar trebui să fie în continuare precauți atunci când introduc informații personale online.

În esență, MC-ul este un program complet care vizează pregătirea temeinică a cursanților pentru a naviga în siguranță în lumea digitală. Perfecționându-și cunoștințele și abilitățile în domeniile cruciale ale reglementărilor privind datele personale, în siguranța copiilor online și în identificarea site-urilor web securizate, cursanții se pot proteja mai bine pe ei înșiși și pe alții, promovând un peisaj digital mai sigur pentru toți. Finalizarea acestui program înseamnă nu doar competență personală, ci și capacitatea de a contribui semnificativ la o societate digitală mai sigură.

Întrebări

1. Care este scopul legilor privind protecția datelor cu caracter personal, cum ar fi Regulamentul general privind protecția datelor (GDPR)?

2. Cum se aplică GDPR organizațiilor din afara Uniunii Europene?
3. Care sunt câteva dintre principiile cheie privind prelucrarea datelor cu caracter personal în conformitate cu GDPR?
4. Puteți enumera și explica pe scurt drepturile pe care le au persoanele în conformitate cu GDPR?
5. Cum influențează legile privind protecția vieții private, cum ar fi GDPR, modul în care datele personale sunt colectate, stocate și procesate zilnic?
6. Care este rolul și importanța browser-elor adaptate copiilor în asigurarea siguranței online pentru copii?
7. Care sunt unele dintre caracteristicile cheie ale browsere-lor adaptate copiilor care le fac potrivite pentru copii?
8. Numiți câteva browsere adaptate copiilor și discutați cum contribuie acestea la crearea unui mediu online mai sigur pentru copii.
9. Cum abordează browserele adaptate copiilor problemele de confidențialitate?
10. Cum se stabilește o conexiune sigură la un site web și de ce este importantă?
11. Ce înseamnă HTTPS și ce indică prezența acestuia în cadrul adresei URL a unui site web?
12. Ce ne indică prezența unei pictograme lacăt din bara de adrese a unui browser?
13. Ce este un sigiliu de securitate pe un site web și ce reprezintă acesta?
14. Cum indică culoarea unei bare de adrese sau numele proprietarului site-ului web nivelul de securitate al unui site web?
15. De ce este încă important să fiți precauți atunci când introduceți informații personale online, chiar dacă sunt prezente indicii vizuale ale unei conexiuni securizate?

Securitate digitală avansată și competență în criptare (MC 4.2.B.5)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitate digitală avansată și competență în criptare **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.31, 4.2.32 și 4.2.33):

- Identificarea mesajelor de e-mail suspecte care pot conține încercări de phishing sau programe malware.
- Utilizarea măsurilor avansate de securitate pentru a proteja datele personale pe conturile de rețele sociale.
- Înțelegerea conceptului de criptare și a rolului criptării în protejarea informațiilor personale.

Descriere

MC-ul "Securitate digitală avansată și competență în criptare" este un program care vizează practicile proactive de securitate cibernetică în era digitală din prezent. Se concentrează pe trei domenii critice ale siguranței online și securității datelor: identificarea activităților suspecte de e-mail, securizarea datelor personale pe platformele de social media și înțelegerea conceptului de criptare.

Primul rezultat de învățare se concentrează pe identificarea activităților suspecte de e-mail care ar putea fi încercări de phishing sau diseminare de malware. Prevalența e-mailului ca instrument de comunicare a făcut din acesta o țintă frecventă pentru infractorii cibernetici și, prin urmare, înțelegerea modului de detectare și gestionare a acestor potențiale amenințări este crucială. Programul oferă cursanților abilitățile necesare pentru a discerne e-mailurile legitime de cele rău intenționate, evidențiind indicatorii comuni ai e-mailurilor de phishing sau ai celor care transportă malware. Acestea pot include atașamente nesolicitate, urgență în tonul mesajului, greșeli de ortografie sau greșeli gramaticale și incongruențe în informațiile despre expeditorul e-mailului.

E-mailul a devenit o formă omniprezentă de comunicare atât în mediul personal, cât și în cel profesional. Cu toate acestea, utilizarea pe scară largă a făcut din poșta electronică și o țintă frecventă pentru infractorii cibernetici care folosesc tehnici înșelătoare, cum ar fi phishingul sau distribuirea de programe malware, pentru a înșela destinatarii, adesea cu scopul de a fura informații sensibile sau de a compromite sistemele de securitate.

Phishing-ul este un tip de atac cibernetic în care atacatorul se deghizează într-o entitate sau persoană cunoscută, într-un e-mail sau altă comunicare, pentru a distribui link-uri sau atașamente rău intenționate care pot îndeplini o varietate de funcții, inclusiv furtul credențialelor de conectare sau informații bancare, instalarea de programe malware sau blocarea utilizatorului până când acesta plătește o răscumpărare pentru recuperarea datelor.

În acest MC, cursanții sunt învățați cum să recunoască semnele phishing-ului și a altor activități rău intenționate din e-mail. De exemplu, e-mailurile de phishing încearcă adesea să creeze un sentiment de urgență sau teamă, încurajând destinatarul să facă click pe un link sau să deschidă un atașament fără a sta prea mult pe gânduri. Aceste e-mail-uri conțin, de cele mai multe ori, salutări generice, greșeli de ortografie și greșeli gramaticale și, adesea, adresa de e-mail a expeditorului nu se va potrivi cu organizația pe care se presupune că o reprezintă.

Programele malware, sau software-ul rău intenționat, se referă la orice program sau fișier care este dăunător pentru un utilizator de computer. Programele malware includ viruși de computer, viermi (worms), cai troieni (Trojan horses) și programe spion (spyware). Aceste programe rău intenționate pot îndeplini o varietate de funcții, inclusiv furtul, criptarea sau ștergerea datelor sensibile, modificarea sau deturnarea funcțiilor de calcul de bază și monitorizarea activității utilizatorilor pe computer fără permisiunea acestora.

E-mailurile pot fi folosite pentru a distribui programe malware în mai multe moduri, inclusiv prin atașamente sau link-uri încorporate. E-mailul poate părea că provine de la o sursă de încredere, cum ar fi un prieten sau o companie cunoscută, și îndeamnă destinatarul să deschidă un atașament sau să facă click pe un link. Odată ce utilizatorul a întreprins această acțiune, malware-ul poate fi instalat pe sistemul său.

În acest MC cursanții sunt învățați cum să identifice potențialele amenințări malware din e-mailuri: vor înțelege ce tipuri de fișiere sunt folosite, de obiecei, pentru a transmite malware (cum ar fi fișierele .exe sau .zip), vor învăța despre pericolul de a face click pe link-uri necunoscute și despre importanței menținerii software-ului antivirus actualizat.

Programul subliniază importanța de a trata întotdeauna cu prudență e-mailurile nesolicitate, în special pe cele prin care se solicită informații sensibile, pe cele care îndeamnă la o acțiune rapidă, pe cele care au un design neprofesional sau exprimări gramatical incorecte sau pe cele care conțin atașamente nesolicitate. Recunoscând aceste semnale roșii, utilizatorii își pot reduce semnificativ riscul de a deveni victime ale atacurilor de tip phishing sau malware.

În general, capacitatea de a identifica activitățile suspecte de e-mail este o abilitate crucială în era digitală modernă. Poate proteja persoanele și organizațiile de încălcări ale datelor/breșe de date, pierderi financiare și alte consecințe grave asociate atacurilor cibernetice. MC-ul furnizează cursanților cunoștințele și abilitățile necesare pentru a naviga în lumea digitală în siguranță și eficient, încurajând o societate digitală mai sigură și mai atentă la aspectele de confidențialitate. Aceste cunoștințe pot atenua în mod semnificativ riscul de încălcare a datelor sau alte amenințări cibernetice care ar putea compromite securitatea digitală a utilizatorului.

În era rețelelor sociale, programul abordează și protecția datelor cu caracter personal pe aceste platforme, ca al doilea rezultat al învățării. Chiar dacă aceste platforme oferă numeroase beneficii, ele ridică și preocupări substanțiale legate de confidențialitate. Programul vizează o înțelegere aprofundată a măsurilor avansate de securitate care pot fi luate pentru a proteja informațiile personale pe platformele de social media. Acestea includ instrucțiuni despre cele mai bune practici, cum ar fi stabilirea de parole puternice, unice, activarea autentificării cu mai mulți factori, limitarea partajării informațiilor sensibile, înțelegerea și gestionarea eficientă a setărilor de confidențialitate și recunoașterea și evitarea potențialelor escrocherii sau activități frauduloase.

Rețelele sociale au modificat fundamental modul în care oamenii comunică, împărtășesc informații și interacționează. Utilizarea rețelelor sociale în viața de zi cu zi a introdus preocupări semnificative cu privire la confidențialitatea și securitatea datelor. Având în vedere cantitatea mare de date personale partajate pe aceste platforme, utilizatorii devin adesea ținte pentru infractorii cibernetici. Infractorii urmăresc și exploateaza breșele de date, furtul de identitate sau alte forme de criminalitate cibernetică.

În acest MC, al doilea rezultat al învățării vizează înțelegeriea și implementarea măsurilor avansate de securitate pentru a proteja informațiile personale pe platformele de social media. Aceste platforme includ, dar nu se limitează la, Facebook, Instagram, Twitter, LinkedIn și Snapchat.

Unul dintre aspectele principale este crearea și gestionarea parolelor puternice și unice. O parolă robustă constituie o primă linie de apărare utilizatorului împotriva accesului neautorizat. Programul detaliază elementele parolelor puternice, care implică, de obicei, combinații de litere mari și mici, numere și simboluri, care nu sunt ușor de ghicit (cum ar fi „parola123” sau „qwerty”). În plus, programul încurajează utilizarea de parole diferite pentru duverse platformele folosite de către utilizator, pentru a preveni situația în care compromiterea unei parole pe o platformă să afecteze și conturile de pe celelalte platforme utilizate.

Pe lângă practicile unor parole solide, programul subliniază importanța activării autentificării cu mai mulți factori (MFA) pe conturile de rețele sociale. MFA adaugă un nivel suplimentar de securitate, solicitând utilizatorilor să furnizeze cel puțin doi sau mai mulți factori de verificare pentru a obține acces la un cont, ceea ce îngreunează accesul potențialilor intruși.

Programul subliniază, de asemenea, importanța înțelegerii și gestionării eficiente a setărilor de confidențialitate pe platformele de social media. Utilizatorii partajează adesea informații sensibile pe aceste platforme, fără să-și dea seama că postările, comentariile, aprecierile, distribuirile și chiar detaliile personale pot fi vizibile pentru un public mai larg decât și-au propus. Programul oferă o înțelegere aprofundată a setărilor de confidențialitate, îndrumând cursanții cum să controleze cine le poate vedea informațiile și cum pot fi partajate informațiile.

Mai mult, programul acoperă identificarea și evitarea înșelătoriilor și a activităților frauduloase întâlnite frecvent pe rețelele sociale. Acestea pot include încercări de phishing, mesaje înșelătoare, solicitări frauduloase de prietenie sau reclame înșelătoare.

La finalizarea acestui MC, cursanții vor deține cunoștințe profunde despre modul în care să își protejeze datele personale pe platformele de social media. Cunoștințele și abilitățile dobândite nu numai că vor contribui la securitatea digitală personală a cursanților, dar vor influența și cultura siguranței online și a confidențialității datelor. Acest rezultat al învățării este un aspect esențial al asigurării bunăstării digitale a indivizilor și a comunităților, promovând un peisaj social media mai sigur și mai conștient de aspectul legat de confidențialitate. Aceste cunoștințe ajută la asigurarea utilizării în siguranță a platformelor de social media, protejând utilizatorii împotriva încălcării datelor și a potențialului furt de identitate.

În a treia parte, programul analizează conceptul de criptare și rolul său primordial în protejarea informațiilor personale. MC-ul vizează o înțelegere aprofundată a modului în care funcționează criptarea, ca măsură de securitate. Metodele de criptare transformă datele într-un format care nu poate fi citit. Descifrarea mesajului sau a datelor transmise poate fi realizară doar cu cheia de decriptare corectă. MC-ul explorează în continuare diferitele forme de criptare, cum ar fi criptarea simetrică și asimetrică, și contextele în care sunt aplicate. Această înțelegere permite indivizilor să aprecieze rolul criptării în menținerea confidențialității și a integrității datelor, fie că este vorba de comunicații personale, tranzacții de afaceri sau de un peisaj digital mai larg. Criptarea este un aspect critic al securității cibernetice și al confidențialității datelor. Este un proces care convertește textul sau datele care pot fi citite, cunoscute sub numele de text simplu, într-o versiune codificată numită text cifrat, care poate fi decodificată/decriptată doar de către cei care dețin cheia de decriptare corespunzătoare. Scopul principal al criptării este de a proteja confidențialitatea datelor digitale memorate în sistemele informatice sau transmise prin internet sau alte rețele de calculatoare.

Criptarea funcționează prin folosirea de algoritmi complecși pentru a transforma/amesteca datele. Există două tipuri principale de criptare: simetrică și asimetrică.

1. Criptarea simetrică: în criptarea simetrică, aceeași cheie este utilizată atât pentru criptare, cât și pentru decriptare. Aceasta înseamnă că emițătorul și destinatarul trebuie să aibă, amândoi, aceeași cheie. Cel mai comun tip de criptare simetrică este Advanced Encryption Standard (AES), care este aprobat de către Guvernul SUA și de către reglementările europene pentru criptarea informațiilor clasificate, atât la standardele de criptare de grad civil, cât și militar. Standardele actuale prevăd ca informațiile criptate cu o cheie de lungime de minimum 256 de biți - AES 256 (lungimea cheii în biți) - să fie etichetate ca fiind „securizate".

2. Criptare asimetrică: Criptarea asimetrică, cunoscută și sub numele de criptare cu cheie publică, utilizează două chei în loc de una. Cheia publică, care este cunoscută de toată lumea, este folosită pentru criptare, în timp ce cheia privată, care este ținută secretă de destinatar, este folosită pentru decriptare. Cel mai comun tip de criptare asimetrică este algoritmul RSA. Criptarea asimetrică este adesea folosită în comunicațiile securizate, cum ar fi protocoalele SSL și TLS (https://), care asigură transmisia de date pe internet. Standardele internaționale indică o lungime minimă a cheii de 2048 de biți pentru a considera criptarea „securizată".

Diferența uriașă în lungimea cheii (256 biți față de 2048 biți) dintre cheile simetrice și asimetrice se bazează pe algoritmului asimetric RSA care are nevoie de produsul a două numere prime mari (notate cu "p" și „q") pentru a crea nucleul cheilor asimetrice (notat cu „n", unde n este produsul dintre p și q). Lucrând cu numere prime de 5, 6 sau mai multe cifre, universul statistic va fi mult mai mare decât cel al numerelor naturale.

Una dintre utilizările principale ale criptării este protejarea integrității datelor în timpul transmisiei. Când datele sunt criptate, acestea devin ilizibile pentru oricine fără cheia de decriptare, asigurându-ne astfel că datele nu pot fi interceptate și citite în timpul transmisiei. Acest lucru este deosebit de important atunci când transmiteți date sensibile, cum ar fi numere de card de credit sau informații personale, prin internet.

O altă utilizare crucială a criptării este protejarea datelor memorate. Prin criptarea fișierelor sau a unui întreg dispozitive de memorare externă, utilizatorii se pot asigura că, în cazul în care datele sunt furate sau accesate fără autorizație, acestea vor rămâne ilizibile și, prin urmare, inutile pentru partea neautorizată.

Criptarea joacă un rol vital în numeroase domenii, cum ar fi: securitatea internetului, sistemele de comunicații, bănci și finanțe, asistența medicală și multe altele. Este un pilon fundamental al comunicației digitale sigure și al memorării datelor, împiedicând accesul neautorizat și menținând integritatea și confidențialitatea datelor.

Cu toate acestea, este esențial să rețineți că, deși criptarea poate îmbunătăți în mod semnificativ securitatea datelor, nu este infailibilă; ar trebui utilizată ca parte a unei abordări mai ample a securității cibernetice, care include bune practici digitale, utilizarea rețelelor securizate și actualizările regulate de software.

În esență, programul "Securitate digitală avansată și competență în criptare" este conceput pentru a îmbunătăți înțelegerea și capacitățile cursantului cu privire la aspectele cruciale ale siguranței digitale și ale securității datelor. După finalizarea MC-ului, cursanții vor avea o pregătire temeinică în identificarea și atenuarea potențialelor amenințări online, în protecția datelor personale în mediile de social media și în înțelegerea rolului vital al criptării în securizarea informațiilor digitale. Această competență nu este doar benefică doar pentru cursant, ci poate contribui în mod semnificativ la o societate digitală mai sigură.

Întrebări

1. Care sunt câteva caracteristici care indică, de obicei, un e-mail de tip phishing?

2. Puteți explica termenul „malware” și să enumerați câteva dintre tipurile acestuia?
3. Cum puteți identifica o potențială amenințare de malware într-un e-mail?
4. Care este importanța de a trata e-mailurile nesolicitate cu prudență?
5. Care sunt elementele unei parole puternice, unice?
6. Puteți explica conceptul de autentificare multifactor și importanța acestuia în rețelele sociale?
7. Cum pot fi gestionate eficient setările de confidențialitate pe platformele de social media?
8. Ce tipuri de escrocherii sau activități frauduloase sunt frecvent întâlnite pe rețelele sociale?
9. De ce este importantă criptarea în protejarea informațiilor personale?
10. Puteți explica diferența dintre criptarea simetrică și asimetrică?
11. Care este rolul criptării în transmiterea datelor?
12. Cum ajută criptarea la protejarea datelor stocate?
13. De ce ar trebui considerată criptarea ca parte a unei abordări mai ample a securității cibernetice?
14. Care este rolul criptării în sistemele de securitate și comunicații pe internet?
15. Cum contribuie o bună înțelegere a securității poștei electronice la o societate digitală mai sigură?
16. În ce moduri gestionarea eficientă a parolelor pe platformele de social media sporește securitatea datelor cu caracter personal?
17. Cum îmbunătățește înțelegerea criptării capacitățile cuiva în ceea ce privește siguranța digitală și securitatea datelor?
18. Puteți oferi exemple de situații în utilizarea criptării simetrice este mai avantajoasă față de utilizarea criptării asimetrice și invers?
19. Cum diferă gestionarea cheilor în ceea ce privește criptarea simetrică și asimetrică și care sunt implicațiile acestor diferențe în ceea ce privește securitatea și comoditatea?
20. Puteți explica funcționarea algoritmului Advanced Encryption Standard (AES) utilizat în criptarea simetrică și a algoritmului RSA utilizat în criptarea asimetrică?
21. Ce diferențiază algoritmii de criptare simetrică (cum ar fi AES) de cei de criptare asimetrică (cum ar fi RSA) din punct de vedere a securității și a performanței lor?

Elemente avansate de protecție a datelor cu caracter personal și analiza confidențialității (MC 4.2.B.6)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Elemente avansate de protecție a datelor cu caracter personal și analiza confidențialității **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.34, 4.2.35):

- Recunoașterea potențialelor riscuri ale partajării datelor personale pe rețelele de socializare și luarea măsurilor de precauție necesare.
- Compararea politicilor de confidențialitate ale diferitelor aplicații sau servicii pentru a determina practicile lor de colectare a datelor.

Descriere

MC-ul "Elemente avansate de protecție a datelor cu caracter personal și analiza confidențialității" vizează întărirea înțelegerii de către cursanți a confidențialității datelor, a practicilor personale de securitate cibernetică și a drepturilor lor ca cetățeni digitali. Acest program subliniază relevanța practicilor proactive și informate în mediul digital, cu un accent deosebit pe riscurile potențiale ale partajării datelor personale pe platformele de social media, și pe capacitatea de a evalua și compara practicile de colectare a datelor din diverse aplicații și servicii digitale.

În prima parte a MC-ului, cursanții vor explora potențialele riscuri legate de partajarea datelor personale pe platformele de social media. În ciuda numeroaselor avantaje de comunicare și conectare pe care le oferă platformele de social media, ele prezintă și amenințări semnificative legate de confidențialitatea și securitatea datelor. Natura omniprezentă a acestor platforme și schimbul amplu de informații cu caracter personal îi fac pe utilizatori vulnerabili la activitățile criminale cibernetice: breșe de date, furt de identitate și alte infracțiuni cibernetice.

Rezultatul învățării 1: Recunoașterea potențialelor riscuri ale partajării datelor personale pe rețelele sociale și luarea măsurilor de precauție necesare.

Platformele de social media au devenit o parte integrantă a vieții de zi cu zi. Cu toate acestea, deoarece indivizii partajează o cantitate substanțială de informații personale pe aceste platforme, există riscuri considerabile asociate cu confidențialitatea și securitatea datelor. Programul vizează o înțelegere aprofundată a modului în care infractorii cibernetici exploatează aceste platforme și utilizatorii lor. De exemplu, infractorii cibernetici folosesc adesea tehnici de phishing pentru a atrage utilizatorii să dezvăluie informații sensibile sau exploatează setările slabe de confidențialitate pentru a obține acces neautorizat la datele personale.

MC-ul prezintă strategiile și măsurile preventive pe care utilizatorii le pot lua pentru a-și proteja datele personale pe aceste platforme. Cursanții învață cum să folosească setările de confidențialitate în mod eficient, la persoane necunoscute și să înțeleagă implicațiile geoetichetării (geotagging) și a înregistrărilor publice (public check-ins).

Mai mult, programul acoperă importanța evaluării critice a aplicațiilor conectate la platformele de social media, deoarece acestea au adesea acces la informațiile personale și pot să nu adere la aceleași standarde de confidențialitate ca platforma în sine.

Ca răspuns la aceasta, cursanții sunt ghidați prin cele mai bune practici pentru a-și proteja informațiile personale pe aceste platforme. Curriculumul include discuții despre înțelegerea modului în care datele partajate pot fi utilizate corect sau greșit, despre importanța gestionării efective a setărilor de confidențialitate

pentru a limita cine poate vedea conținutul lor partajat și despre conceptul de amprentă digitală și impactul său pe termen lung. Aceste discuții urmăresc să insufle cursanților o conștientizare a potențialelor ramificații ale partajării nediscriminate de date pe astfel de platforme.

Al doilea rezultat al învățării este centrat pe dezvoltarea abilităților cursanților de a evalua și de a compara în mod critic politicile de confidențialitate ale diferitelor aplicații și servicii digitale. Având în vedere peisajul digital actual în care datele sunt considerate o marfă foarte valoroasă, o gamă largă de aplicații și servicii colectează frecvent date despre utilizatori, justificând că o fac în scopul îmbunătățirii experiențelor utilizatorilor. Aceste practici generează preocupări notabile de confidențialitate.

Rezultatul învățării 2: compararea politicilor de confidențialitate ale diferitelor aplicații sau servicii pentru a determina practicile lor de colectare a datelor

Acest rezultat al învățării se concentrează pe dotarea cursanților cu capacitatea de a evalua și de a compara în mod critic politicile de confidențialitate și practicile de colectare a datelor ale diferitelor aplicații și servicii digitale. Odată cu apariția erei digitale, datele au devenit un activ valoros, iar multe companii folosesc strategii bazate pe date pentru a îmbunătăți experiența utilizatorului, adesea în detrimentul confidențialității utilizatorilor.

MC-ul vizează înțelegerea terminologiei și a cadrelor legale utilizate în politicile de confidențialitate, recunoașterea modului în care datele sunt colectate, stocate și partajate și identificarea controlului pe care utilizatorii îl au asupra datelor lor. Programul discută exemple practice de politici de confidențialitate, evidențiind diferite politici și modul în care companiile pot utiliza datele colectate.

Programul îi instruiește pe cursanți în domeniul reglementărilor majore privind protecția datelor, cum ar fi Regulamentul general privind protecția datelor (GDPR), oferindu-le o înțelegere clară a drepturilor lor cu privire la datele personale.

Ca rezultat al acestui MC, cursanții nu numai că vor dobândi o înțelegere aprofundată a potențialelor riscuri asociate cu partajarea datelor cu caracter personal pe rețelele de socializare, dar își vor dezvolta și abilitățile necesare pentru a evalua și compara în mod critic diverse practici de colectare a datelor și diferite politici de confidențialitate ale serviciilor digitale.

În acest context, cursanții sunt învățați cum să discearnă ce tipuri de date colectează aceste servicii și aplicații, cum sunt utilizate, stocate și potențial partajate aceste informații și ce control au utilizatorii asupra datelor lor personale; implică înțelegerea politicilor de confidențialitate și a termenilor acordurilor de servicii, adesea complexe și lungi, pe care mulți utilizatori le acceptă fără o examinare amănunțită. Instruirea din acest MC acoperă, de asemenea, cadre de reglementare precum Regulamentul general privind protecția datelor (GDPR), care oferă consumatorilor drepturi și protecții stricte cu privire la datele lor personale.

După finalizarea MC-ului “Elemente avansate de protecție a datelor cu caracter personal și analiza confidențialității” cursanții vor avea o înțelegere aprofundată a potențialor riscuri și a măsurilor preventive necesare legate de partajarea datelor cu caracter personal pe rețelele sociale. De asemenea, aceștia își vor antrena capacitatea de a evalua și compara în mod critic colectarea datelor și practicile de confidențialitate ale diferitelor servicii digitale. Aceste competențe se extind dincolo de beneficiul personal, încurajând o societate digitală mai informată, mai responsabilă și mai conștientă de confidențialitate.

Întrebări

1. Care sunt unele riscuri comune asociate cu partajarea datelor personale pe platformele de social media?
2. Cum pot setările de confidențialitate de pe platformele de socializare să protejeze datele personale?
3. Ce măsuri de precauție ar trebui luate atunci când se acceptă cereri de prietenie sau urmăritori (followeri) pe rețelele sociale?
4. Care sunt potențialele implicații ale etichetării geografice (geotagging) și ale înregistrărilor publice (public check-in) pe rețelele sociale?
5. Cum pot aplicațiile terță parte conectate la platformele de social media să prezinte un risc pentru datele personale?
6. De ce este important să citiți și să înțelegeți politicile de confidențialitate ale serviciilor digitale?
7. De ce termeni cheie și cadre juridice ar trebui să fim conștienți atunci când evaluăm politicile de confidențialitate?
8. Cum poate un utilizator să identifice tipurile de date colectate de către un serviciu, așa cum este detaliat în politica sa de confidențialitate?
9. Ce aspecte ale stocării și partajării datelor ar trebui să căutați într-o politică de confidențialitate?
10. Cum afectează reglementările precum GDPR drepturile unui utilizator cu privire la datele personale?
11. Cum poate o comparație a politicilor de confidențialitate între diferite servicii să ajute un utilizator să facă alegeri informate cu privire la serviciile pe care să le folosească?

Securitate avansată a datelor cu caracter personal și confidențialitate (MC 4.2.B.7)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitate avansată a datelor cu caracter personal și confidențialitate **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.36, 4.2.37 și 4.2.38):

- Descrierea conceptului de comunicare criptată și valotizarea confidențialității prin alegerea aplicațiilor de comunicare care oferă criptare end-to-end.
- Adoptarea celor mai bune practici pentru protejarea datelor cu caracter personal în diverse contexte online.
- Investigarea anomaliilor în dispozitivele dvs. care ar putea indica o încălcare a confidențialității.

Descriere

Pe măsură ce lumea trece rapid la platformele digitale, programul “Securitate avansată a datelor cu caracter personal și confidențialitate” oferă cursanților o înțelegere holistică a securității datelor cu caracter personal în sfera online. Printr-o explorare aprofundată a comunicării criptate, a practicilor de protecție a datelor cu caracter personal și a detectării încălcării confidențialității, programul furnizează abilitățile și cunoștințele necesare pentru a asigura interacțiuni digitale sigure.

Pentru început, comunicarea criptată formează piatra de temelie a comunicării online sigure, servind drept prim rezultat al învățării. Criptarea este un instrument de securitate puternic care maschează informațiile pentru a preveni accesul neautorizat. Comunicarea criptată folosește această tehnologie pentru a proteja informațiile pîn timpul transmiterii lor de la expeditor la destinatar, asigurându-se că, conținutul rămâne confidențial și își menține integritatea.

Programul pune accent pe conceptul de criptare end-to-end, o formă specială de criptare, în care doar utilizatorii care comunică pot citi mesajele. În principiu, împiedică potențialele persoane care interceptează datele/mesajele transmise – inclusiv furnizorii de telecomunicații, furnizorii de internet și chiar furnizorul de servicii însuși – să poată accesa cheile criptografice necesare pentru a decripta conversația. Această măsură avansată de securitate este folosită de multe aplicații moderne de comunicații, pentru a proteja confidențialitatea utilizatorilor.

Se realizează o analiză în profunzime a unor aplicații de comunicații criptate, cum ar fi Signal, WhatsApp și Telegram. Aceste aplicații sunt diferite prin nivelul de securitate, politicile de confidențialitate și protocoalele de criptare pe care le utilizează. MC-ul, însă, nu promovează o aplicație față de cealaltă. În schimb, subliniază importanța luării deciziilor în cunoștință de cauză, bazându-ne pe evaluarea nevoilor de confidențialitate, pe înțelegerea politicilor de confidențialitate și pe înțelegerea standardelor de criptare ale fiecărei aplicații.

Al doilea rezultat al învățării furnizează cursanților o înțelegere extinsă a celor mai bune practici pentru protejarea datelor personale în diverse contexte online. Programul subliniază faptul că fiecare platformă sau serviciu online necesită o abordare unică a protecției datelor datorită funcționalității sale distincte, a politicilor de confidențialitate și a măsurilor de securitate.

Odată cu omniprezența tranzacțiilor online, platformele de comerț electronic au devenit un hotspot pentru infractorii cibernetici. Prin urmare, programul evidențiază importanța opțiunilor de plată sigure, utilizarea platformelor autorizate și precauția împotriva partajării de informații financiare sensibile.

Platformele de social media, având în vedere acoperirea extinsă și capacitatea lor de a difuza rapid informații, facilitează adesea, din neatenție, răspândirea datelor cu caracter personal. Prin urmare, înțelegerea setărilor de confidențialitate, discernământul cu privire la acceptarea solicitărilor de conectare și precauțiile în privința informațiilor partajate, fac parte din acest modul.

E-mailul și alte instrumente profesionale de comunicare, adesea folosite pentru partajarea datelor profesionale sensibile, necesită, de asemenea, practici de securitate stricte. Programul ghidează cursanții prin procesele de stabilire a parolelor puternice, identificarea e-mailurilor de phishing și partajarea responsabilă a datelor în aceste contexte.

Al treilea rezultat al învățării din acest MC se referă la detectarea potențialelor încălcări ale confidențialității. Anomaliile dispozitivelor, cum ar fi blocările sau opririle neașteptate ale sistemului, performanțele scăzute, anunțurile pop-up excesive (pop-up ads), aplicațiile nerecunoscute sau consumarea mult mai rapidă a bateriei, ar putea indica o încălcare a confidențialității.

În acest sens, programul insuflă o înțelegere a diferitelor instrumente și metode de securitate cibernetică, cum ar fi software-ul antivirus, firewall-urile și sistemele de detectare a intruziunilor, care pot identifica și gestiona aceste amenințări. Programul îi educă în continuare pe cursanți despre cum să-și auditeze în mod regulat dispozitivele și conturile online pentru modificări neașteptate și cum să ia măsuri corective în cazul unei încălcări, cum ar fi schimbarea parolelor, deconectarea de la internet sau contactarea profesioniștilor în securitate cibernetică.

În esență, programul "Securitate avansată a datelor cu caracter personal și confidențialitate" cultivă o înțelegere cuprinzătoare a securității online și a confidențialității datelor. Până la sfârșitul programului, cursanții vor avea abilitățile de a comunica în siguranță online, de a-și proteja datele personale pe diverse platforme și de a identifica potențialele încălcări ale confidențialității și de a răspunde la acestea în mod eficient.

Acest program constituie o dovadă a necesității unei culturi mai largi a securității digitale și a conștientizării confidențialității în societatea noastră din ce în ce mai interconectată. Abilitățile și cunoștințele dobândite aici nu se limitează doar la beneficiul personal. De asemenea, contribuie la crearea unor spații digitale mai sigure pentru toată lumea, ajutând comunitățile să prospere în era digitală. Într-o lume în care granița dintre digital și fizic se estompează continuu, asigurarea siguranței digitale nu mai este un lux, ci o necesitate. Acest program MC semnifică un pas important în acest sens, încurajând capacitatea de a naviga cu încredere în lumea digitală, protejându-te atât pe tine, cât și pe ceilalți, de potențialele amenințări cibernetice.

Întrebări

1. Care este scopul comunicării criptate în contextul securității online?
2. Explicați conceptul de criptare end-to-end și importanța acestui rip de criptare în păstrarea confidențialității.
3. Comparați protocoalele de criptare utilizate în aplicațiile Signal, WhatsApp și Telegram.
4. De ce este crucial să înțelegem și să evaluăm politicile de confidențialitate ale diverselor aplicații de comunicare?
5. Care sunt cele mai bune practici pentru protejarea datelor cu caracter personal pe platformele de

comerț electronic?

6. Discutați considerentele cheie pentru protejarea datelor cu caracter personal pe platformele de social media.
7. Care sunt unele măsuri care pot fi luate pentru a spori securitatea instrumentelor profesionale de comunicare precum e-mailul?
8. Identificați și explicați trei anomalii ale dispozitivelor care ar putea indica o încălcare a confidențialității.
9. Cum pot ajuta instrumentele de securitate cibernetică, cum ar fi software-ul antivirus și firewall-urile, la identificarea potențialelor încălcări ale confidențialității?
10. Discutați pașii implicați în efectuarea unui audit al dispozitivelor și al conturilor online pentru încălcări ale confidențialității.
11. Ce măsuri ar trebui luate în cazul detectării unei încălcări a confidențialității?
12. Cum contribuie cunoștințele și practicile privind securitatea datelor cu caracter personal la cultura generală a securității digitale?
13. Cum contribuie asigurarea siguranței digitale personale la comunitatea digitală mai largă și la bunăstarea acesteia?

Managementul confidențialității digitale și interacțiunea online sigură (MC 4.2.B.8)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul confidențialității digitale și interacțiunea online sigură **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.39, 4.2.40):

- Diferențierea tuturor tipurilor de „cookie” și înțelegerea modului în care acestea pot fi utilizate de site-uri web pentru stocarea datelor utilizatorilor.
- Prioritizarea conturilor online în funcție de sensibilitatea informațiilor pe care le dețin.

Descriere

MC-ul “Managementul confidențialității digitale și interacțiunea online sigură” vizează înțelegerea extinsă a două domenii principale ale siguranței digitale și securității datelor: diferențierea diverselor tipuri de „cookie” și utilizarea lor în stocarea datelor pe site-uri web și clasificarea conturilor online în funcție de sensibilitatea informațiilor pe care le conțin.

Programul pornește într-o explorare a lumii nuanțate a „cookie-urilor” – fișiere mici pe care site-urile web le trimit și le stochează pe dispozitivele utilizatorilor pentru a reține detalii specifice despre vizită. Cookie-urile au devenit componente integrante ale experienței de navigare pe web, influențând modul în care utilizatorii interacționează cu site-urile, informațiile pe care site-urile și le amintesc și tipurile de reclame pe care le văd utilizatorii. Cu toate acestea, nu toate modulele cookie sunt la fel, iar înțelegerea diferitelor tipuri de cookie-uri varietăți este crucială pentru gestionarea confidențialității online și a securității datelor.

Cookie-urile sunt mici fragmente de date stocate pe computerul unui utilizator de către browser-ul web în timpul navigării pe un site web. Ele joacă un rol esențial în îmbunătățirea experienței utilizatorului prin faptul că își amintesc informații despre vizita utilizatorului, cum ar fi informațiile de conectare, preferințele de limbă și alte setări. Dar, în timp ce cookie-urile oferă comoditate, ele pot prezenta și preocupări legate de confidențialitate, deoarece pot urmări activitatea de navigare și pot colecta date despre comportamentul online al utilizatorilor.

Diferite tipuri de cookie-uri au scopuri diferite, iar înțelegerea acestora poate ajuta persoanele să își gestioneze mai bine confidențialitatea online:

1. Cookie-uri de sesiune: acestea sunt cookie-uri temporare care sunt șterse atunci când un utilizator își închide browser-ul web. Acestea sunt folosite pentru a reține acțiunile utilizatorului într-o sesiune de navigare, cum ar fi articolele adăugate într-un coș de cumpărături pe un site de comerț electronic. Aceste module cookie de obicei nu ridică probleme majore de confidențialitate, deoarece nu urmăresc activitatea utilizatorului pe mai multe sesiuni sau site-uri.
2. Cookie-uri persistente: spre deosebire de modulele cookie de sesiune, modulele cookie persistente rămân pe computerul unui utilizator chiar și după ce acesta închide browser-ul. Acestea sunt folosite pentru a reține preferințele și acțiunile unui utilizator în mai multe sesiuni de navigare, cum ar fi preferințele de aspect al site-ului sau informațiile de conectare. Deoarece urmăresc activitatea în timp, pot ridica probleme legate de confidențialitate, în special în cazurile în care colectează informații sensibile.
3. Cookie-uri securizate: acestea sunt transmise prin conexiuni criptate (HTTPS), făcându-le mai sigure decât cookie-urile obișnuite; împiedică interceptarea datelor transmise de către părți neautorizate.

4. Cookie-uri numai HTTP (HTTP-only cookies): aceste module cookie nu pot fi accesate prin scripturi la nivel client, cum ar fi JavaScript. Acest lucru le face mai sigure împotriva anumitor tipuri de atacuri, cum ar fi atacurile cross-site scripting (XSS), care folosesc scripturi rău intenționate pentru a fura cookie-urile și informațiile pe care le dețin.
5. Cookie-uri terță parte (Third-party cookies): acestea sunt create de către alte domenii decât cel pe care îl vizitează la un moment dat utilizatorul; sunt adesea folosite pentru publicitatea online și pot urmări activitatea unui utilizator pe multe site-uri, ridicând preocupări semnificative privind confidențialitatea.

Înțelegând aceste diferite tipuri de cookie-uri, persoanele pot lua decizii mai informate cu privire la confidențialitatea lor online. De exemplu, ar putea alege să blocheze cookie-urile terță parte pentru a preveni urmărirea pe mai multe site-uri sau ar putea să-și șteargă în mod regulat cookie-urile pentru a elimina cookie-urile persistente și pentru a limita cantitatea de date care pot fi colectate despre istoricul lor de navigare.

În plus, înțelegerea cookie-urilor poate ajuta persoanele să interpreteze politicile de confidențialitate ale site-ului web, care dezvăluie adesea tipurile de cookie-uri pe care le folosește un site și cum anume le folosește. Aceste cunoaștințe permit utilizatorilor să facă alegeri mai informate cu privire la utilizarea unui site și la modul în care își setează setările de confidențialitate.

În cele din urmă, înțelegerea implicațiilor cookie-urilor poate încuraja obiceiuri online mai sănătoase. De exemplu, recunoașterea faptului că cookie-urile pot urmări activitatea online ar putea motiva persoanele să folosească instrumente de îmbunătățire a confidențialității, cum ar fi blocarea reclamelor sau rețelele private virtuale (VPN), sau să folosească browsere axate pe confidențialitate sau motoare de căutare care nu urmăresc activitatea utilizatorului.

Cookie-urile joacă un rol critic în internetul modern, dar ridică și probleme legate de confidențialitate. Înțelegând diferitele tipuri de module cookie și modul în care site-urile web le utilizează, persoanele pot lua măsuri proactive pentru a-și gestiona confidențialitatea online, cum ar fi ajustarea setărilor browser-ului, ștergerea regulată a modulelor cookie, utilizarea instrumentelor de îmbunătățire a confidențialității și luarea unor decizii mai informate cu privire la site-urile web pe care să le folosească. Acest lucru poate duce la o experiență online mai sigură și mai atentă la aspectul confidențialității.

Al doilea rezultat major al învățării din acest program se referă la prioritizarea conturilor online pe baza sensibilității informațiilor pe care le dețin. În era digitală de astăzi, foarte multe persoane au numeroase conturi online, începând de la cele de pe platformele de social media, până la servicii bancare online și cumpărături. Fiecare din aceste conturi stochează cantități variate de informații personale.

Prioritizarea conturilor online pe baza sensibilității informațiilor pe care le dețin este un pas esențial către menținerea confidențialității și a securității în sfera digitală. Majoritatea persoanelor de astăzi operează numeroase conturi online într-o gamă largă de servicii.

Acestea pot include profiluri de rețele sociale, conturi de e-mail, servicii bancare online, platforme de comerț electronic, servicii de abonament, dosare de sănătate și multe altele. Fiecare dintre aceste conturi păstrează cantități diferite de informații personale și, prin urmare, prezintă niveluri diferite de risc, dacă este compromis.

Procesul de prioritizare implică evaluarea impactului potențial sau a daunelor care ar putea să apară dacă o persoană neautorizată ar obține acces la fiecare cont specific.

Iată câteva elemente de luat în considerare atunci când prioritizați conturile:

1. Informații financiare: serviciile bancare online, conturile de card de credit sau orice servicii care au detaliile dvs. financiare (cum ar fi PayPal sau site-urile de cumpărături) ar trebui să fie în fruntea listei Dvs. de priorități. O încălcare a acestor conturi/breșă poate duce la pierderi financiare și la furt de identitate.
2. Conturi de e-mail: Contul Dvs. principal de e-mail, mai ales dacă este folosit pentru recuperarea parolelor de la alte reprezintă o prioritate ridicată. Accesul neautorizat la e-mailul Dvs. poate duce la un efect de domino al spargerilor de date, deoarece poate fi folosit pentru resetarea parolelor și obținerea accesului la alte conturi.
3. Documente medicale: orice cont care conține informații sensibile despre sănătate este extrem de important, deoarece o spargere de date aici ar putea conduce la încălcări grave ale confidențialității și la o posibilă utilizare greșită a informațiilor medicale personale.
4. Conturi profesionale: acestea includ e-mailuri de serviciu, conturi legate de profesia Dvs. sau orice platformă care conține datele Dvs. profesionale. Compromiterea acestor conturi ar putea avea ca urmări pierderea proprietății intelectuale și deteriorarea reputației profesionale.
5. Conturi pe rețelele sociale: chiar dacă ar putea să nu pară la fel de critice precum conturile financiare sau profesionale, conturile din rețele sociale dețin o mulțime de informații personale care pot fi exploatate pentru furtul de identitate sau utilizate pentru a vă viza pe Dvs. și/sau contactele Dvs. în atacurile de phishing.

După identificarea și prioritizarea conturilor, este necesară aplicarea unor strategii pentru a spori securitatea acestor conturi:

- Utilizarea de parole puternice, unice pentru fiecare cont. Luați în considerare utilizarea unui manager de parole pentru a le urmări.
- Activarea autentificării cu doi factori (2FA) sau autentificarea cu mai mulți factori (MFA) ori de câte ori este posibil.
- Monitorizarea și actualizarea în mod regulat setărilor de securitate.
- Acordarea unei atenții sporite la partajarea online a informațiilor, în special a datelor sensibile.

Înțelegerea sensibilității informațiilor deținute de diferite conturi și luarea măsurilor adecvate în funcție de nivelul de risc implicat este o practică esențială pentru a menține informațiile personale în siguranță. Prin prioritizarea conturilor online în funcție de sensibilitatea datelor pe care le dețin, persoanele își pot aloca eforturile de securitate în mod eficient, concentrându-se pe protejarea conturilor care ar putea cauza cele mai multe daune în cazul în care au fost compromise.

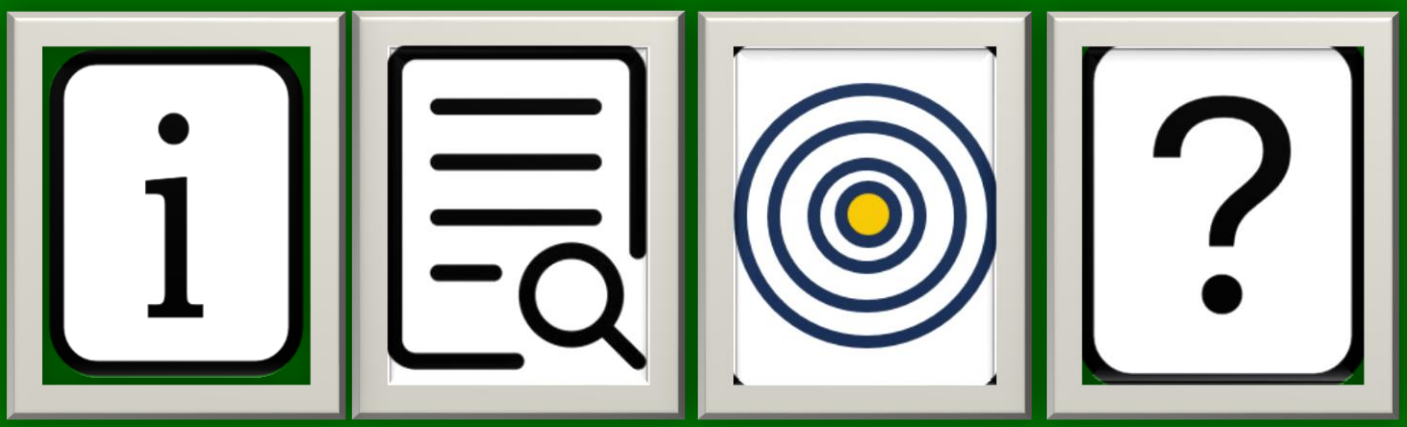
În concluzie, acest MC furnizează cursanților cunoștințe critice despre funcționalitățile cookie-urilor și despre nevoia de a prioritiza conturile online pe baza sensibilității datelor, permițându-le să navigheze în lumea digitală cu o conștientizare și competență sporite. Cu aceste abilități, persoanele își pot proteja mai bine informațiile personale, pot contribui la o cultură mai largă a confidențialității datelor și pot promova o societate digitală mai sigură.

Întrebări

1. Definiți cookie-urile în contextul navigării pe internet și explicați funcția lor principală.
2. Diferențiați cookie-urile de sesiune de cookie-urile persistente. Cum diferă funcționalitățile lor?
3. Care este semnificația cookie-urilor securizate? De ce sunt considerate mai sigure decât cookie-urile obișnuite?
4. Descrieți cookie-urile numai HTTP (HTTP-only cookies)și discutați despre modul în care acestea oferă securitate suplimentară.
5. Ce sunt cookie-urile terță parte (third-party cookies) și de ce ar putea fi considerate o problemă de confidențialitate?
6. Cum ajută înțelegerea diferitelor tipuri de cookie-uri la gestionarea confidențialității online?
7. Cum pot cunoștințele despre cookie-uri să ajute o persoană în interpretarea politicii de confidențialitate a unui site web?
8. Descrieți câteva strategii pentru gestionarea cookie-urilor în vederea îmbunătățirii confidențialității online.
9. Explicați importanța prioritizării conturilor online pe baza sensibilității informațiilor pe care le conțin.
10. Ce factori ar trebui luați în considerare atunci când acordați prioritate conturilor online pentru confidențialitate și securitate sporite?
11. Discutați riscurile asociate cu compromiterea conturilor online cu prioritate ridicată, cum ar fi cele care dețin informații financiare sau informații medicale.
12. Care pot fi potențialele consecințe ale unei încălcări a conturilor profesionale?
13. De ce este important să luați în considerare conturile de pe rețele sociale în timp ce acordați prioritate conturilor online, chiar dacă acestea nu conțin date sensibile evidente?
14. Descrieți pașii pe care îi veți urma pentru a îmbunătăți securitatea conturilor online cu prioritate ridicată.
15. Cum contribuie practica de prioritizare a conturilor online pe baza sensibilității datelor la siguranța generală a informațiilor personale și la confidențialitatea datelor?

NIVELUL AVANSAT

(Nivelul 5 și Nivelul 6)



Securitatea dispozitivelor personale și cele mai bune practici (MC 4.2.C.1)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea dispozitivelor personale și cele mai bune practici **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.41, 4.2.42):

- Evaluarea și compararea diferitelor 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.
- Evitarea utilizării 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 extins, practic, conceput pentru a furniza cursanților cunoștințele și abilitățile esențiale pentru a-și proteja dispozitivele și datele personale într-o lume din ce în ce mai interconectată. Avizat de către Comisia Europeană, acest program prezintă participanților instrumente și tehnici practice pentru a evalua și pentru a selecta cele mai eficiente soluții software de securitate, cum ar fi programe antivirus și firewall-uri, adaptate la dispozitivul și la nevoile lor specifice de securitate.

În primul modul, cursanții pătrund în profunzime în 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 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 susțină cele mai bune practici și să susțină utilizarea instrumentelor de gestionare a parolelor (password managers) pentru a memora și gestiona în siguranță parole complexe pentru diferite conturi online.

Pe parcursul MC-ului, cursanților li se prezintă studii de caz din lumea reală și scenarii de securitate cibernetică, permițându-le să aplice cunoștințele nou dobândite în situații practice. Aceștia sunt încurajați să analizeze critic potențialele riscuri de securitate și să elaboreze strategii proactive pentru a atenua eficient amenințările.

După finalizarea cu succes a MC-ului „Securitatea dispozitivelor personale și cele mai bune practici", participanții vor dobândi un certificat prestigios din partea Comisiei Europene, care confirmă faptul că stăpânesc cunoștințele teoretice și abilitățile practice în securizarea dispozitivelor și gestionarea parolelor. Înarmați cu aceste competențe, cursanții vor fi pregătiți pentru a-și proteja cu încredere dispozitivele și datele personale de amenințările cibernetice, contribuind la un mediu digital mai sigur și mai sigur pentru ei și pentru cei din jurul lor.

Întrebări

1. Întrebare despre evaluarea soluțiilor software de securitate: „Sunteți în procesul de selectare a software-ului de securitate pentru laptop-ul Dvs., pe care îl utilizați în principal pentru activități

bancare online și activități profesionale. 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 și nevoile Dvs. specifice?"

2. Întrebare despre promovarea securității parolelor: „Discutați despre cele mai bune practici de securitate a parolelor cu colegii Dvs. Unul dintre ei sugerează utilizarea unor informații ușor de urmărit, cum ar fi datele de naștere sau cuvinte comune, în parole. Cum ați susține evitarea utilizării acestor informații și cum ați promovați practicile unor parole mai puternice? Oferiți motive și exemple pentru a vă susține argumentul."
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 ar trebui să îi urmați pentru a îmbunătăți 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 parolei și cele mai bune practici (MC 4.2.C.2)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea parolei și cele mai bune practici **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.43, 4.2.44 și 4.2.45):

- Înțelegerea importanței evitării utilizării cuvintelor din dicționar sau a modelelor comune în parole pentru a preveni atacurile brutale.
- Recunoașterea riscului utilizării aceleiași parole în mai multe conturi și a importanței utilizării parolelor unice pentru fiecare cont.
- Recunoașterea importanței actualizării periodice a parolelor și a evitării reutilizării parolelor vechi.

Descriere

MC-ul „Securitatea parolei și cele mai bune practici" este un program extins, specializat, creat cu meticulozitate pentru a oferi cursanților cunoștințe și abilități avansate în protejarea identităților digitale prin practici solide de parolare. Acest program, aprobat de distinsa Comisie Europeană, analizează în profunzime subiectul complex al securității parolelor, futnizând participanților expertiza necesară pentru ca aceștia să poată crea, gestiona și menține parole puternice și unice, care să le întărească prezența online împotriva potențialelor amenințări.

În primul modul, cursanții explorează vulnerabilitățile asociate cu utilizarea cuvintelor din dicționar sau a modelelor/tiparelor (patterns) comune în parole. Prin studii de caz ilustrative și exemple din lumea reală, cursanții dobândesc o înțelegere profundă a modului în care astfel de practici fac conturile lor susceptibile la atacuri brutale. Înarmați cu aceste cunoștințe, participanții vor fi îndrumați cu privire 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 în mai multe conturi. Cursanții sunt expuși la scenarii revelatoare care evidențiază efectul de domino al reutilizarii parolelor, în care un singur cont compromis poate conduce la o mulțime de încălcări ale securității, în cascadă. Prin exerciții interactive, cursanții înțeleg importanța primordială a adoptării parolelor unice pentru fiecare cont, protejându-ți astfel activele digitale și menținând o apărare fortificată împotriva adversarilor cibernetici.

În modulul final, cursanții se concentrează pe semnificația indispensabilă a actualizării regulate a parolelor și pe evitarea reutilizării parolelor vechi. Ei înțeleg modul în care aceste practici contribuie la o poziție de securitate în continuă evoluție, fortificându-și activele digitale împotriva amenințărilor cibernetice emergente. Angajându-se în activități practice și simulări, participanții internalizează principiile managementului eficient al parolelor, sporindu-și astfel pregătirea de a se adapta la provocările de securitate aflate în continuă evoluție.

Pe parcursul MC-ului, cursanții beneficiază de un mediu de învățare dinamic și interactiv, facilitat de experți din industrie și de profesioniști experimentați în securitate cibernetică. Cursanții parcticipă activ la exerciții practice și simulări din viața reală, aplicându-și, cu încredere, cunoștințele noi în interacțiunile digitale de zi cu zi.

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

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

În concluzie, MC-ul „Securitatea parolei și cele mai bune practici” este un program transformator, care nu furnizează doar cunoștințe teoretice, ci și cunoștințe și abilități practice aplicabile pentru a-și consolida identitățile digitale și pentru a-și proteja datele personale de tărâmul în continuă dezvoltare al amenințărilor cibernetice. MC-ul este indicat atât profesioniștilor care doresc să-și îmbunătățească perspicacitatea în domeniul securității cibernetice, cât și utilizatorilor obișnuiți care aspiră să-și protejeze tărâmurile digitale cu cea mai mare competență.

Întrebări

1. Întrebare despre complexitatea parolelor: „De ce este esențial să evitați utilizarea cuvintelor din dicționar sau a modelelor comune în cadrul parolelor? Cum îmbunătățesc aceste practici securitatea conturilor dumneavoastră și previn atacurile brutale? Furnizați exemple pentru a vă susține răspunsul.”
2. Întrebare bazată pe scenariu privind reutilizarea parolei: „Ați folosit aceeași parolă atât pentru conturile dvs. de e-mail, cât și pentru conturile bancare online. Care sunt potențialele riscuri asociate cu această practică? Cum poate practica de a folosi parole unice pentru fiecare cont să atenueze aceste riscuri și să vă sporească, per total, 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 scenariul privind schimbarea parolei: „Să presupunem că nu ți-ai schimbat parolele pentru conturile de rețele sociale de peste un an. Ce riscuri ar putea apărea din această cauză? 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 compromisului 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 potențialelor consecințe ale acestei încălcări de securitate? Ce pași suplimentari ați urma 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 neglijeri? Cum ați remedia situația și ați preveni apariția similară a situației în viitor?"

Gestionarea securizată a dispozitivelor și eficiența datelor (MC 4.2.C.3)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Gestionarea securizată a dispozitivelor și eficiența datelor **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.46, 4.2.47):

- Utilizarea cu pricepere a unui program de compresie pe un dispozitiv pentru a reduce volumul de date, asigurând stocara și transmisia eficientă.
- Capabilitatea de a configura setările dispozitivului pentru a se bloca automat sau a se deconecta după o perioadă de inactivitate, pentru a preveni accesul neautorizat.

Descriere

MC-ul "Gestionarea securizată a dispozitivelor și eficiența datelor" este un program cuprinzător, de ultimă oră, conceput meticulos pentru a furniza cursanților abilitățile esențiale în gestionarea în siguranță a dispozitivelor și în optimizarea eficienței datelor. Avizat de prestigioasa Comisie Europeană, acest program furnizează participanților cunoștințele necesare pentru a naviga cu încredere în peisajul digital, asigurându-se că dispozitivele lor rezistentă în fața potențialelor amenințări de securitate, dar sunt și eficiente în gestionarea datelor.

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

Al doilea modul analizează în profunzime aspectul primordial al securității dispozitivului prin mecanisme automate de blocare și deconectare. Cursanții vor căpăăta deprinderi în configurarea setărilor dispozitivului pentru implementarea funcțiilor de blocare sau deconectare automată pe timpul perioadelor de inactivitate.

Înarmați cu aceste cunoștințe, cursanții își întăresc în mod eficient dispozitivele împotriva accesului neautorizat, protejând informațiile sensibile și datele personale de potențialele încălcări ale securității. Implementarea cu pricepere a acestor măsuri permit cursanților să păstreze controlul asupra punctelor de acces ale dispozitivelor lor, promovând un mediu digital rezistent și sigur.

Pe parcursul MC-ului, 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 eficiența datelor.

După finalizarea cu succes a MC-ului „Gestionarea securizată a dispozitivelor și eficiența datelor", participanții obțin un certificat din partea Comisiei Europene, care le recunoaște competența în a-și securiza dispozitivele și a optimiza gestionarea datelor. Înarmați cu aceste abilități avansate, cursanții sunt pregătiți să îmbrățișeze peisajul digital în evoluție cu încredere, contribuind la un ecosistem digital mai sigur, mai productiv.

Pe scurt, MC-ul „Gestionarea securizată a 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 iscusința digitală, acest program pregătește cursanții să fie navigatori pricepuți pe tărâmului digital, asigurându-se că dispozitivele lor rămân în siguranță, iar 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 urmat și beneficiile - în ceea ce privește reducerea volumului de date și depozitarea eficientă - la care vă așteptați după comprimarea fișierului.”
2. Întrebare bazată pe scenariul despre setările de blocare a dispozitivului: „Imaginați-vă că vă folosiți frecvent dispozitivul în locuri publice și că sunteți îngrijorat de accesul neautorizat la acesta, atunci când este lăsat nesupravegheat. Cum ați configura cu pricepere setările dispozitivului pentru a se bloca automat după o perioadă de inactivitate? Descrieți pașii pe care i-ați urma și potențialele beneficii de securitate ale implementării acestei caracteristici.”
3. Întrebare de gândire critică privind eficiența datelor: „Să presupunem că aveți spațiu de stocare limitat pe un dispozitiv și că 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 pentru îmbunătățirea experienței digitale globale?

Siguranța digitală și manipularea securizată a datelor (MC 4.2.C.4)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Siguranța digitală și manipularea securizată a datelor Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.48, 4.2.49 și 4.2.50):

- Cunoașterea riscurilor de a utiliza funcțiile de conectare automată pentru site-urile web sau aplicațiile care memorează informații personale.
- Utilizarea metodelor securizate de transfer de fișiere, cum ar fi SFTP sau stocarea securizată în cloud, pentru schimbul de fișiere sensibile între dispozitive.
- Recunoașterea potențialor riscuri ale utilizării de software sau aplicații necunoscute pe dispozitivele personale

Descriere

MC-ul „Siguranța digitală și manipularea securizată a datelor” este un program cuprinzător și de perspectivă, conceput pentru a furniza 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 furnizează participanților cunoștințele necesare pentru ca aceștia să poată lua decizii în cunoștință de cauză, să susțină practicile sigure și să-și protejeze - în mod eficient - informațiile digitale.

În primul modul, cursanții vor înțelege în profunzime riscurile asociate cu funcțiile de conectare automată. Prin exemple din lumea reală și studii de caz, participanții devin foarte conștienți de potențialele implicații ale permiterii site-urilor web sau aplicațiilor să stocheze automat informații personale. Înarmați cu 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 a-și păstra confidențialitatea digitală.

Al doilea modul se concentrează pe metodele securizate de transfer 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 face schimb 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 încălcării datelor.

Modulul final evidențiază potențialele riscuri ale utilizării de software sau aplicații necunoscute pe dispozitivele personale. Participanții explorează pericolele asociate cu descărcarea și rularea software-ului provenit din surse neverificate. Recunoscând aceste riscuri, cursanții își sporesc vigilența digitală și sunt precauți pe parcursul evaluării și a utilizării unor noi aplicații, protejându-și dispozitivele de potențialele malware și vulnerabilități de securitate.

Pe parcursul MC-ului, cursanții sunt antrenați în activități practice, simulări și discuții interactive, permițându-li-se astfel să internalizeze cele mai bune practici în domeniul siguranței digitale și al gestionării securizate a datelor. Finalizarea cu succes a programului nu numai că le conferă cursanților o certificare prestigioasă din partea Comisiei Europene, dar le dă și puterea să facă alegeri responsabile și informate în interacțiunile lor digitale, contribuind la un mediu digital cât mai sigurpentru 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

au fost instruiți să susțină practicile sigure, să protejeze datele sensibile și să promoveze siguranța digitală în diverse contexte, având un impact pozitiv în sferele lor personale și profesionale.

Întrebări

1. Întrebare de conștientizare a riscurilor privind funcțiile de conectare automată: „Explicați potențialele riscuri ale utilizării funcțiilor de conectare automată pentru site-uri web sau aplicații care stochează informații personale. Cum vă pot compromite aceste funcții confidențialitatea și securitatea digitală? Furnizați exemple de scenarii în care dezactivarea conectării automate ar fi recomandabilă. "
2. Întrebare care susține și justifică folosirea metodelelor 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 fișiere sensibile între dispozitive. Includeți 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: „Veți întâlni cu 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 implicați în utilizarea software-ului necunoscut și descrieți pașii pe care i-ați lua pentru a-i evalua legitimitatea și securitatea înainte de a continua.”

Securitatea dispozitivelor și protecția datelor (MC 4.2.C.5)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea dispozitivelor și protecția datelor Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.51, 4.2.52):

- Recunoașterea importanței dezactivării Bluetooth-ului pe dispozitivele personale atunci când acestea nu sunt utilizate.
- Capacitatea de a efectua scanări de viruși pe dispozitive de stocare externe.

Descriere

Micro-Credit-ul „Securitatea dispozitivelor și protecția datelor” este un program concentrat, practic, menit să înzestreze cursanții cu abilitățile esențiale pentru a-și proteja dispozitivele și datele de potențiale amenințări de securitate. Avizat de către prestigioasa Comisie Europeană, acest program furnizează participanților cunoștințele și capacitățile nenesare pentru a-și întări dispozitivele împotriva vulnerabilităților legate de Bluetooth și pentru a efectua scanări de viruși pe dispozitivele de stocare externe.

În primul modul, cursanții explorează riscurile asociate conectivității de tip Bluetooth atunci când acestea sunt lăsate în modul activ pe dispozitivele lor, mai ales atunci când dispozitivele nu sunt utilizate. Prin exemple din lumea reală și studii de caz, participanții devin foarte conștienți de potențialele vulnerabilități de securitate care pot apărea din cauza conexiunilor Bluetooth. Ei înțeleg importanța dezactivării Bluetooth-ului atunci când nu este utilizat în mod activ, reducându-se, astfel, riscul accesului neautorizat sau al încălcării datelor/breșelor de date.

Al doilea modul se concentrează pe practica critică de a efectua scanări de viruși pe dispozitivele de memorie externă. Participanților li se prezintă informațiile despre potențialele riscurile asociate cu utilizarea mediilor de stocare externe (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 stocare infectate. Prin dobândirea de abilități practice în efectuarea de scanări de viruși pe mediile de memorare externă, cursanții pot detecta și atenua în mod proactiv amenințările, asigurându-se că dispozitivele și datele lor rămân în siguranță.

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

După finalizarea cu succes a MC-ului „Securitatea dispozitivelor și protecția datelor”, participanții dobândesc cunoștințe solide, validându-și competențele în a-și securiza dispozitivele și 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 concluzie, MC-ul „Securitatea dispozitivelor și protecția datelor” este un program transformator, care furnizează cursanților cunoștințe și abilități practice în securitatea dispozitivelor și protecția datelor. Participanții devin gardieni proactivi ai dispozitivelor și datelor lor digitale, fiind bine pregătiți pentru a atenua riscurile de securitate și pentru a promova un mediu digital mai sigur pentru ei și pentru ceilalți.

Întrebări

1. Întrebare bazată pe scenariul despre securitatea Bluetooth: „Imaginați-vă că tocmai ați terminat de utilizat Bluetooth-ul pentru a vă conecta dispozitivul la un difuzor fără fir (wireless speaker). Ce pași ați urma pentru a asigura securitatea dispozitivului dvs. după deconectarea de la difuzor? Explicați potențialele riscuri din situația în care Bluetooth-ul rămâne activat pe perioada când nu este utilizat și furnizați motivele pentru care este esențial să dezactivați Bluetooth-ul în astfel de cazuri."
2. Evaluarea aptitudinilor practice privind scanarea virușilor: „Primiți o unitate USB de la un coleg; USB-ul 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 pe dispozitivul de stocare 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: „Plănuiți să transferați unele fișiere de pe calculatorul personal pe un hard disk extern în scopul de a efectua o copie de rezervă (backup). Cum v-ați asigura că dispozitivul de stocare extern nu conține programe malware sau viruși care v-ar putea infecta computerul în timpul procesului de transfer? Discutați despre importanța de a realiza scanări ale virușilor pe dispozitivelor de stocare externă și despre modul în care această practică contribuie la protecția generală a datelor și la securitatea dispozitivului.”

Instruire extinsă și implementare în domeniul securității (MC 4.2.C.6)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Instruire extinsă și implementare în domeniul securității Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.53, 4.2.54 și 4.2.55):

- Înțelegerea importanței instruirii angajaților cu privire la tehnicile de securitate IT.
- Dezvoltarea unor măsuri extinse de securitate fizică pentru a proteja activele organizaționale.
- Conștientizarea importanței conceptului de autentificare în doi factori (2FA) și a rolului acestuia în introducerea unui strat suplimentar de protecție pentru conturile online.

Descriere

MC-ul „Instruire extinsă și implementare în domeniul securității" este un program extins, specializat, conceput pentru a înzestra cursanții cu cunoștințele și abilitățile necesare pentru a asigura practici de securitate solide în cadrul organizațiilor.
Avizat de prestigioasa 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 pătrund în profunzime 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 privire la protejarea datelor, la identificarea potențialelor amenințări și a răspunsului la incidentele de securitate.

Al doilea modul subliniază importanța măsurilor extinse 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-urilor, 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, care adaugă unui nivel suplimentar de protecție față 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 această practică esențială de securitate.

Pe parcursul MC-ului, cursanții se angajează în scenarii practice, exerciții de joc 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 extinsă și implementare în domeniul securității", participanții dobândesc cunoștințe valoroase, validându-și expertiza în îmbunătățirea securității organizaționale. Înarmați cu acest set cuprinzător 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.
Pe scurt, MC-ul „Instruire extinsă și implementare în domeniul securității" este un program care instruiește cursanții să abordeze în mod proactiv provocările de securitate din organizații. Participanții apar ca 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 de formare: „Ca trainer în securitate IT, descrieți pașii pe care i-ați urma pentru a proiecta un program eficient de instruire - cu privire la tehnicile de securitate IT - pentru angajați. Cum ați adapta instruirea la 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 avantajele 2FA: „Explicați conceptul de autentificare cu doi factori (2FA) unei persoane nefamiliare cu termenul. 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 legată de scenariul ales pentru a instrui și 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, supravegherea și managementul vizitatorilor, asigurând astfel o protecție maximă pentru activele organizației”.
6. Implementarea și promovarea 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 acesteia pentru a asigura o utilizare pe scară largă."
7. 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 și diferențiați 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 scenariile specifice în care o metodă ar putea fi mai potrivită decât cealaltă. ”

Conștientizarea securității cibernetice și protecția dispozitivelor (MC 4.2.C.7)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Conștientizarea securității cibernetice și protecția dispozitivelor Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.56, 4.2.57 și 4.2.58):

- Cunoașterea modului de diagnosticare și să depanare a problemelor de securitate pe dispozitivele personale, identificând eventualele programe malware sau încercări de acces neautorizat.
- Înțelegerea potențialelor pericole ale stocării parolelor în browser-ele web și a importanței utilizării instrumentelor de gestionare a parolelor.
- Elaborarea unui plan personal de conștientizare a securității cibernetice pentru a rămâne informat cu privire la amenințările actuale și pentru a adopta cele mai bune practici de protejare a dispozitivelor și a datelor personale.

Descriere

MC-ul „Conștientizarea securității cibernetice și protecția dispozitivelor” este un program cuprinzător, practic, conceput pentru a oferi cursanților cunoștințele și abilitățile esențiale în materie de securitate cibernetică. Acest program se concentrează pe trei aspecte vitale ale securității cibernetice, pentru a asigura protecția dispozitivelor și a datelor personale.

În primul modul, participanții aprofundează practica diagnosticării și a remedierii problemelor de securitate pe dispozitivele personale. Prin simulări interactive și scenarii din viața reală, cursanții dobândesc experiență în identificarea potențialelor infecții malware, în detectarea încercărilor de acces neautorizat și în 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 browser-ele web și rolul esențial al instrumentelor dedicate de gestionare a parolelor. Cursanții explorează vulnerabilitățile asociate stocării parolelor în 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 a stoca 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, cum să urmărească actualizările din industrie și cum să rămână vigilenți împotriva amenințărilor cibernetice emergente. Cultivând o mentalitate proactivă și implementând cele mai bune practici de securitate, participanții își creează o apărare solidă împotriva potențialelor atacuri cibernetice și a încălcării datelor.

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

După finalizarea cu succes a MC-ului „Conștientizarea securității cibernetice și protecția dispozitivelor”, participanții primesc certificarea. Această recunoaștere le validează competența în diagnosticarea problemelor

de securitate, în utilizarea tehnicilor de gestionare a parolelor sigure și în dezvoltarea unui plan proactiv de conștientizare a securității cibernetice.

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

Întrebări

1. Observați că computerul dumneavoastră funcționează mai lent decât de obicei și primiți frecvent reclame pop-up (pop-u ads) enervante în timp ce navigați pe internet. Ce problemă de securitate ați putea bănui că există și ce pași ați urma pentru a depana și a rezolva această problemă?
2. Explicați potențialele pericole ale stocării parolelor în browser-ele web și cum vă poate compromite aceasta securitatea online. Care sunt beneficiile utilizării instrumentelor 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 faceți click pe 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 de a cădea 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 datelor dumneavoastră personale. Includeți acțiuni specifice pe care le veți întreprinde, cum ar fi abonamentul la surse de știri privind securitatea cibernetică, activarea autentificării cu doi factori și actualizarea regulată a software-ului dispozitivului dvs.

Măsuri avansate de securitate pentru dispozitive și sisteme personale (MC 4.2.C.8)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Măsuri avansate de securitate pentru dispozitive și sisteme personale **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.59, 4.2.60):

- Utilizarea software-lui antivirus și anti-malware recunoscute, pe dispozitivele personale, pentru a detecta și elimina potențialele amenințări.
- Implementarea controalelor de acces pentru a reglementa și pentru a restricționa intrarea în sisteme, conturi sau profiluri personale, asigurând o mai bună securitate și confidențialitate.

Descriere

MC-ul „Măsuri avansate de securitate pentru dispozitive și sisteme personale" este un program specializat, conceput pentru a furniza cursanților cunoștințe teoretice și practice despre tehnicile avansate de securitate, pentru a-și proteja dispozitivele personale și profilurile digitale. Acest curs extins 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 adopta 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 obțin informații despre detectarea și eliminarea potențialelor amenințări care pot compromite integritatea dispozitivelor lor. Scenariile din lumea reală și simulările practice le permit 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 construiesc o apărare solidă împotriva amenințărilor digitale și își îmbunătățesc postura generală de securitate cibernetică.

În cel de-al doilea modul, participanții aprofundează domeniul controalelor de acces și 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 datele, aplicațiile și identitățile online în mod eficient. În plus, modulul subliniază importanța menținerii parolelor puternice și unice pentru a consolida mecanismele de control al accesului, atenuând, astfel, riscul accesului neautorizat și potențialele încălcări ale datelor/breșe de date.

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

După finalizarea cu succes a Micro Credential „Măsuri avansate de securitate pentru dispozitive și sisteme personale", participanții vor primi un certificat care le validează competența în adoptarea și în implementarea măsurilor avansate de securitate, întărindu-le credibilitatea în peisajul securității digitale.

În concluzie, MC-ul „Măsuri avansate de securitate pentru dispozitive și sisteme personale" furnizează cursanților expertiza necesară pentru a-și proteja în mod eficient viața digitală. Înarmați cu o înțelegere mai profundă a software-ului de securitaterecunoscut, a controalelor avansate de acces și a practicilor de parole

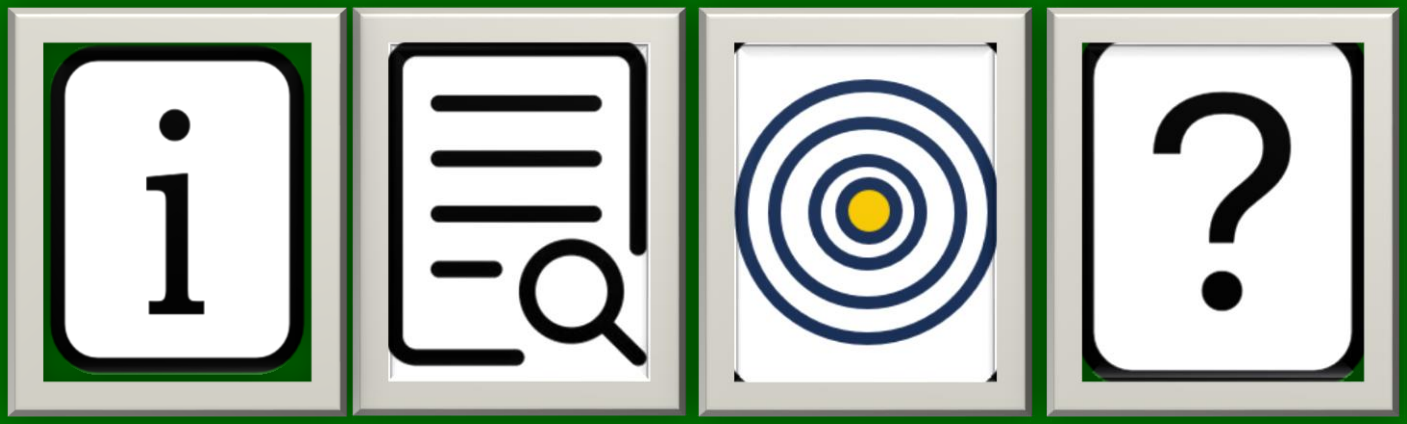
sigure, participanții vor deveni gardieni adepți ai dispozitivelor și sistemelor lor personale, promovând un ecosistem digital mai sigur pentru ei înșiși și pentru societate în ansamblu.

Întrebări

1. De ce este important să 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, a selecta și a instala – pe acest dispozitiv - software antivirus și anti-malware.
4. Sunteți responsabil pentru securizarea unei aplicații bazate pe web utilizată de angajații organizației în care lucrați. Descrieți cum ați implementa controalele de acces pentru a reglementa și pentru a restricționa accesul la diferitele caracteristici și funcționalități ale aplicației. Includeți metodele specifice de control al accesului pe care le-ați utiliza și rațiunea din spatele alegerilor dvs.

NIVELUL EXPERT

(Nivelul 7 și Nivelul 8)



Managementul riscurilor de securitate cibernetică și conștientizarea personalului (MC 4.2.D.1)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul riscurilor de securitate cibernetică și conștientizarea personalului **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.61, 4.2.62 și 4.2.63):

- Înțelegerea importanței organizării de cursuri anuele de formare pentru conștientizarea personalului cu privire la securitatea cibernetică.
- Analiza și clasificarea potențialele riscuri de securitate cibernetică pe baza impactului și probabilității lor de apariție.
- Examinarea și actualizarea regulată a politicilor și a procedurilor legate de securitatea cibernetică.

Descriere

MC-ul „Managementul riscurilor de securitate cibernetică și conștientizarea personalului" este un program extins, conceput pentru a furniza participanților experiența 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 cursurilor de formare de 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 comune de securitate cibernetică și cele mai bune practici, cursanții pot adapta 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 aprofunda analiza și categorizarea 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 actualizării periodice a politicilor și a procedurilor de securitate cibernetică. Participanții vor explora cele mai bune practici pentru crearea și menținerea politicilor de securitate cibernetică extinsă 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 apărarea în securitatea cibernetică a organizației lor.

Pe parcursul MC-ului, cursanții vor fi evaluați printr-o combinație de chestionare, studii de caz și sarcini practice, care le evaluează capacitatea de a aplica cunoștințele dobândite în scenarii din lumea reală. Participanții vor înțelege în profunzime managementul riscului de securitate cibernetică și rolul cursurilor de formare a conștientizării 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 în încurajarea unei culturi de conștientizare a securității în rândul personalului, contribuind la îmbunătățirea practicilor de securitate cibernetică în diverse organizații.

În concluzie, MC-ul „Managementul riscurilor de securitate cibernetică și conștientizarea personalului” le furnizează cursanților cunoștințele și abilitățile necesare pentru a analiza în mod eficient riscurile de securitate cibernetică, pentru a concepe programe de instruire a personalului vizate și pentru a menține politici și proceduri de securitate cibernetică la zi. Prin împuternicirea persoanelor să ia măsuri proactive împotriva amenințărilor cibernetice, acesă MC joacă un rol esențial în consolidarea rezistenței digitale a organizațiilor din diverse industrii.

Întrebări

1. De ce este esențială pentru organizații organizarea anuală de cursuri de formare în conștientizarea 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 postura de securitate a organizației?
4. Sunteți un profesionist în securitate IT însărcinat cu desfășurarea unui curs 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 de risc al securității cibernetice pentru o instituție financiară. Analizați un scenariu ipotetic de risc de securitate cibernetică, clasificând riscurile în funcție de impactul și 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 management-ul datelor redundante (MC 4.2.D.2)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitatea cibernetică centrată pe date și management-ul datelor redundante **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.64, 4.2.65):

- Acordați mai multă atenție măsurilor de securitate centrate pe date, nu vă bazați doar pe apărarea perimetrului.
- Demonstrarea cunoștințelor și a abilităților de a identifica și a elimina datele redundante, în vederea îmbunătățirii securității cibernetice.

Descriere

MC-ul „Securitatea cibernetică centrată pe date și management-ul datelor redundante ” este un program de ultimă oră, conceput pentru furniza participanților tehnici avansate de securitate cibernetică centrate pe protejarea datelor, deoarece datele reprezintă cel mai important activ pentru orice organizație. Acest curs cuprinzător se concentrează pe două competențe cheie care abordează provocările moderne de securitate cibernetică.

În peisajul dinamic al amenințărilor de astăzi, apărarea perimetrului tradițional nu mai este suficientă pentru a proteja datele sensibile 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, tokenizarea, 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 încălcării datelor/breșelor de date și a atacurilor cibernetice.

Al doilea modul este dedicat managementului datelor redundante, un aspect crucial al securității cibernetice, din păcate - adesea trecut cu vederea. Participanții vor învăța cât de important este să identifice și să elimine datele redundante, pentru a minimiza suprafața de atac și pentru a îmbunătăți integritatea datelor. Prin exerciții practice, cursanții vor dezvolta abilitățile de a efectua audituri ale datelor, de a detecta, de a elimina datele redundante și de a eficientiza sistemele de stocare a datelor. Această abordare proactivă nu numai că îmbunătățește securitatea cibernetică, ci și promovează eficiența datelor, reducând costurile de stocare și îmbunătățind practicile de gestionare a datelor.

Pe parcursul MC-ului, participanții vor fi evaluați folosind o combinație de sarcini practice, exerciții de auditare a datelor și evaluări bazate pe scenarii. Ei vor avea ocazia să-și aplice cunoștințele în incidente - de securitate cibernetică - simulate, demonstrându-și competența în implementarea măsurilor de securitate centrate pe date și gestionarea datelor redundante.

După finalizarea cu succes a Micro Credentialului „Securitatea cibernetică centrată pe date și management-ul datelor redundante”, participanții vor primi un certificat 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 management-ul datelor redundante” furnizează participanților 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 stocare a datelor, acest program joacă un rol crucial în consolidarea rezistenței securității cibernetice și în promovarea

eficienței datelor în cadrul organizațiilor din diferite sectoare. Participanții vor fi bine pregătiți să navigheze în peisajul securității cibernetice și să devină active valoroase în protejarea datelor sensibile de amenințările cibernetice aflate în continuă evoluție.

Întrebări

1. Explicați conceptul de securitate centrată pe date și modul în care aceasta diferă de cea care se bazează 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 securitatea IT și sunteți responsabil pentru îmbunătățirea securității cibernetice în organizația dvs. Descrieți pașii pe care i-ați urma pentru a identifica și a elimina datele redundante din sistemele de stocare 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 de date, chiar dacă avea implementate sisteme puternice de securitate perimetrală. 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 4.2.D.3)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Conducerea securității cibernetice și dezvoltarea culturii **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.66, 4.2.67):

- Promovarea necesitpții investițiilor sporite în securitatea cibernetică și alocarea în mod eficient a resurselor
- Cnștientizarea importanței de a promova o mentalitate de securitate la nivel de companie și de a promova o cultură a conștientizării securității cibernetice

Descriere

MC-ul „Conducerea securității cibernetice și dezvoltarea culturii" este un program extins care dă posibilitatea participanților să susțină securitatea cibernetică în cadrul organizațiilor, să promoveze o cultură conștientă de securitate și să conducă alocarea eficientă a resurselor pentru o reziliență cibernetică îmbunătățită. Dezvoltat în colaborare cu Comisia Europeană, acest curs transformator furnizează participanților cunoștințele și abilitățile esențiale pentru a deveni lideri proactivi în securitatea cibernetică.

Într-un peisaj digital care evoluează rapid, securitatea cibernetică a devenit un imperativ strategic pentru organizațiile de toate dimensiunile, din toare sectoarele.

Primul modul al acestui MC analizează importanța investițiilor sporite în securitatea cibernetică. Participanții vor obține informații despre amenințările cibernetice emergente, despre potențialele consecințe ale atacurilor cibernetice și despre importanța tot mai mare a alocării resurselor adecvate cu scopul de 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 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 studia în profunzime psihologia comportamentului uman și impactul acestuia asupra securității cibernetice. Dobândind aceste cunoștințe, cursanții vor putea dezvolta strategii în care să implice și să educe angajații – de la toate nivelurile - pentru a deveni participanți activi la protejarea activelor digitale. Modulul va aborda tehnici eficiente de comunicare, metode de instruire antrenante și va stabili politici și linii directoare solide de securitate cibernetică.
Participanții vor fi pregătiți pentru a implementa programe de conștientizare a securității care insuflă o cultură proactivă de securitate și oferă angajaților puterea să recunoască și să răspundă eficient la amenințările cibernetice.

Pe parcursul MC-ului, participanții se vor implica în ateliere interactive, exerciții de joc de rol și simulări bazate pe scenarii. Ei vor învăța de la experți din industrie și lideri în securitate cibernetică, care 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 abilitățile de conducere în contextul securității cibernetice.

Ca parte a procesului de evaluare, participanților li se va cere să elaboreze un plan de conducere - adaptat organizației lor - în domeniul securității cibernetice. Acest plan va consolida competența cursanților în susținerea investițiilor în securitate cibernetică, în promovarea unei culturi conștiente de securitate și în

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 oficial din partea UE. Acest certificat atestă capacitățile lor de a conduce inițiative de securitate cibernetică, de a cultiva o cultură conștientă de securitate și de a-și direcționa organizația către reziliența cibernetică și reducerea riscurilor.

În concluzie, MC-ul „Conducerea securității cibernetice și dezvoltarea culturii" furnizează participanților expertiza și strategiile necesare pentru a conduce eforturile de securitate cibernetică în cadrul organizațiilor. De la susținerea investițiilor strategice până la promovarea unei culturi conștiente de 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 rămân în fața 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 în care lucrați. Cum ați folosi rezultatele evaluării pentru a aloca în mod eficient resursele necesare pentru a aborda vulnerabilitățile și amenințările identificate?
3. Cum ați comunica importanța securității cibernetice angajaților de la toate nivelurile organizației? 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 conștientă de securitate în cadrul organizației? Ce metrici și indicatori cheie de performanță (KPI) ați folosi pentru a evalua eficacitatea inițiativelor de conștientizare a securității cibernetice?
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 - de alocare a resurselor pentru a aborda vulnerabilitățile critice – ați adopta, 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. Dați 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 său și impactul pe care l-a avut asupra poziției generale de securitate a organizației.

Managementul siguranței datelor și conștientizarea cibernetică (MC 4.2.D.4)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul siguranței datelor și conștientizarea cibernetică **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.68, 4.2.69 și 4.2.70):

- Demonstrarea capacității de a clasifica datele în funcţie de prioritatea şi importanţa lor
- Recunoașterea importanţei autentificării cu 2 factori (Two-factor Authentication) sau a autentificării cu mai mulți factori (Multi-factor Authentication)
- Adoptarea unei atitudini de prudență și vigilență în cazul utilizării platformelor de social media

Descriere

MC-ul „Managementul siguranței datelor și conștientizarea cibernetică" este un program extins, conceput cu scopul de a furniza cursanților cunoștințele și abilitățile necesare pentru a asigura securitatea datelor 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 (2FA) sau mai mulți factori (MFA) și practicile sigure pentru rețelele sociale.

Datele sunt vitale pentru organizațiile moderne, iar securitatea lor este de o importanță capitală. Primul modul al acestui MC se concentrează pe clasificarea datelor, o practică fundamentală pentru protejarea informațiilor sensibile. Cursanții vor aprofunda conceptul de clasificare a datelor, înțelegând semnificația acestuia în prioritizarea și protejarea informațiilor, în funcție de cât de sensibile sau critice sunt acestea. 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 MC-ului prezintă cursanților metodele 2FA (autentificarea cu doi factori) și MFA (autentificarea cu mai mulți factori), ambele metode implementând o practică solidă de securitate, care o depășește pe cea a parolelor tradiționale. Cursanții vor explora diferitele forme de MFA, incluzând coduri transmise prin SMS, aplicații de autentificare, verificare biometrică și jetoane hardware(hardware tokens). Cursanții vor înțele modul în care MFA adaugă un nivel suplimentar de protecție, prin faptul că solicită utilizatorilor să furnizeze mai multe forme de identificare înainte de a accesa 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 adoptării unor practicii 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 în cazul în care 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 saula încercările de phishing pe aceste platforme.

Pe parcursul programului, cursanții se vor implica în activități interactive, studii de caz și chestionare pentru a-și consolida înțelegerea conceptelor și a abilităților practice prezentate. Ei vor avea, de asemenea, acces la resurse și instrumente pentru a-și îmbunătăți cunoștințele despre securitatea datelor și conștientizarea cibernetică. MC-ul oferă o experiență de învățare flexibilă, permițând participanților să progreseze în propriul

ritm, îndrumați de experți și instructori experimentați.

După finalizarea cu succes a MC-ului „Managementul siguranței datelor și conștientizarea cibernetică”, cursanții vor primi o recunoaștere certificată din partea Uniunii Europene. Această certificare atestă competența lor în clasificarea datelor, implementarea MFA și practicile de social media sigure. Atfel, cursanții devin active valoroase pentru orice organizație care dorește să-și consolideze poziția de securitate cibernetică.

În concluzie, MC-ul „Managementul siguranței datelor și conștientizarea cibernetică” este un program cuprinzător, conceput pentru a furniza 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 abordarea în care ca indivizii și organizațiile au din ce în ce mai multă nevoie să adopte măsuri de securitate proactive într-un peisaj digital în continuă evoluție. Prin completarea acestui MC, cursanții vor fi capabili să își protejeze datele personale și pe cele ale organizației din care fac parte, să securizeze conturile și să fie vigilenți în interacțiunile lor online, contribuind la un mediu digital sigur și securizat pentru toți.

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 pentru un 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 pot 2Fa și MFA să sporească securitatea?
4. Furnizați exemple de situații în care utilizarea 2FA sau MFA ar fi deosebit de importantă. Explicați cauzele pentru care aceste scenarii necesită un nivel suplimentar de securitate.
5. Cum păstrați atitudinea 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 folosite 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 rețelele sociale, care apar în cazul în care setările de confidențialitate nu sunt 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 - cu privire la utilizarea platformelor de social media atât la locul de muncă, cât și în mediul personal?
9. Imaginați-vă că întâlniți un mesaj sau un link suspect pe o platformă de socializare. Ce pași ați urma pentru a verifica autenticitatea acestuia și pentru a vă asigura siguranța înainte de a vă implica?

Securitate cibernetică avansată și hacking etic (MC 4.2.D.5)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Securitate cibernetică avansată și hacking etic **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.71, 4.2.72):

- Cunoașterea modului în care se folosește un hacker „pălărie albă” ("white hat" hacker) pentru evaluările securității cibernetice
- Recunoașterea tacticilor de inginerie socială și apărarea împotriva acestora

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?

Stăpânirea securității cibernetice - Parole sigure și gestionarea accesului (MC 4.2.D.6)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Stăpânirea securității cibernetice - Parole sigure și gestionarea accesului **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.73, 4.2.74):

- Capacitatea de a crea parole puternice și sigure pentru o securitate cibernetică îmbunătățită.
- Planificarea strategiilor eficiente de gestionare a accesului aplicate cu scopul de 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 brutale 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 securității cibernetice și gestionarea conturilor (MC 4.2.D.7)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Conștientizarea securității cibernetice și gestionarea conturilor **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.75, 4.2.76):

- Educarea angajaților cu privire la riscurile asociate cu utilizarea conturilor personale pentru sarcini legate de muncă și promovarea importanței de a separara conturile personale de cele de afaceri.
- Implementarea 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 dispozitivelor/punctelor finale și păstrarea datelor (MC 4.2.D.8)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Managementul securității cibernetice - Protecția punctelor finale și păstrarea datelor **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.77, 4.2.78):

- Cunoașterea modului de implementare, de gestionare și de întreținere a soluțiilor de protecție a punctelor terminale pentru protejarea dispozitivelor și a rețelelor individuale în fața amenințărilor de securitate.
- Practicarea politicilor de păstrare a datelor pentru a fi siguri 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 punctelor finale, 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 punctelor finale

Punctele finale, 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 punctelor finale 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 punctelor finale? 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 punctelor finale 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 4.2.D.9)

Specificații

Identificarea cursantului	Orice cetățean
Titlul și codul micro-creditului	Optimizarea browserului și managementul securității **Cod: MC 4.2.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
Forma de participare la activitatea de învățare	Peer Review (Evaluare de către colegi)

Rezultatele învăţării

Rezultatele învățării (ref. LO 4.2.79, 4.2.80):

- Optimizarea setărilor browser-ului și a performanțelor cu scopul de a îmbunătăți viteza și eficiența navigării.
- Personalizarea setărilor 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

PIN – Număr de identificare personală (**P**ersonal **I**dentification **N**umber)

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)

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

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

SSID – Identificator al mulțimii de servicii (**S**ervice **S**et **I**dentifier)

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)*

DoH (**D**NS-**o**ver-**H**TTPS)

DoT (**D**NS-**o**ver-**T**LS)

DNSSEC (**D**omain **N**ame **S**ystem **Sec**urity Extensions)

Fake news – știri false

ANEXĂ – COMPETENȚA 4.2 PROTECȚIA DATELOR PERSONALE ȘI A CONFIDENȚIALITĂȚII

DOMENIUL DE COMPETENȚĂ: SIGURANȚĂ (4) COMPETENȚĂ: PROTECTIA DATELOR PERSONALE ȘI A CONFIDENȚIALITĂȚII (4.2)			
Rezultatul învățării	Nivel	K – S - A	Explicație
1. Recunoașterea importanței identificării electronice securizate pentru partajarea mai sigură a datelor cu caracter personal în tranzacții.	L1	K	Identificarea electronică sigură este esențială pentru partajarea în siguranță a datelor cu caracter personal în tranzacțiile online. De exemplu, utilizarea modului de autentificare cu doi factori (2FA) introduce un nivel suplimentar de securitate, reducând riscul de accesare neautorizată a informațiilor sensibile.

2. Identificarea elementelor „politicii de confidențialitate” a serviciilor sau aplicațiilor.	L1	K - S	Politicile de confidențialitate conțin elemente esențiale pentru asigurarea transparenței și a conformității cu regulile de protecție a datelor. Aceste elemente includ: Tipuri de date colectate: Acest secțiune explică categoriile de date, despre utilizator, pe care o aplicație sau serviciu le colectează, ca de exemplu, informații despre dispozitivul folosit și utilizarea datelor. Scopul în care sunt colectate datele: Sunt evidențiate motivele pentru care sunt colectate datele, ca de exemplu, furnizarea de servicii, îmbunătățirea experienței utilizatorului sau livrarea de conținut personalizat. Practici de prelucrare și partajare a datelor: Aceste politici detaliază cum vor fi prelucrate datele, cum vor fi memorate și partajate cu terțe părți; pot include, de asemenea, informații despre transferurile de date și prelucrările trans-frontaliere. Consimţământul utilizatorului: Acest element explică modul în care utilizatorul își dă consimțământul pentru colectarea și prelucrarea datelor. Trebuie să implice un consimțământ explicit, acordate prin casetele de selectare (checkboxes) sau consimțământul implicit, prin utilizarea aplicației. Drepturile utilizatorului: Sunt evidențiate drepturile utilizatorilor în privința datelor, incluzând drepruei de a accesa, modifica, șterge sau restricționa prelucrarea informațiilor lor personale. Măsuri de securitate: Politica de confidențialitate descrie măsurile de securitate implementate în vederea la protejării datelor utilizatorului față de accesul neautorizat, breșe, sau abuzuri. Perioada de retenție (păstrare) a datelor: Această secțiune precizează cât timp păstrează datele despre urilizator o aplicație sau un serviciu și când aceste date sunt șterse sau devin anonime. Utilizarea de către terțe servicii: Dacă aplicația sau serviciul integrează servicii de la terți sau partajează date cu aceștia, acest element explică natura unor astfel de colaborări. Confidențialitatea copiilor (dacă este cazul): Dacă aplicația sau serviciul se adresează copiilor sau

			colectează date ale acestora, sunt necesare informații suplimentare despre conformitatea cu legile de confidențialitate pentru copii. Politica de notificări despre actualizări: Politica trebuie să stabilească modul în care utilizatorii vor fi informați în privința modificărilor sau a actualizărilor politicii de conformitate. Informații de contact: Politica confidențialității furnizează utilizatorului informațiile de contact, astfel încât acesta să poată adresa întrebări sau reclamații despre confidențialitatea datelor.
3. Identificarea diferitelor tipuri de date cu caracter personal care ar putea fi expuse riscului (de exemplu, nume, e-mail, adresă, număr de telefon, număr de asigurări medicale din UE).	L1	K - S	Pe platformele de social media, diverse tipuri de date personale ar putea fi în pericol (nume, aderesă de e-mail, adresă de domiciliu, numere de telefon, numere ale asigurării de sănătate din UE, date de naștere, informații financiare, detalii despre locul de muncă, informații despre interesele sau activitățile personale. Utilizatori ar trebui să fi precaut când partajează astfel de informații sensibile în mod public, pentru a evita potenţiale riscuri de confidențialitate și securitate.
4. Descoperirea beneficiilor și a riscurilor, înainte de a permite terților să prelucreze date cu caracter personal.	L1	S	Cântărirea beneficiilor și a riscurilor, înainte de a permite terțelor părți prelucrarea datelor personale este esenţială pentru a asigura confidențialitatea și securitatea datelor. În timp ce parteneriatul cu terți poate oferi avantaje, cum ar fi servicii îmbunătățite și capabilități extinse, acesta aduce, de asemenea, potențiale riscuri, cum ar fi breșele de date și pierderea controlului asupra informațiilor sensibile.
5. Discutarea rolului software-ului antivirus în protejarea împotriva programelor malware și realizarea unor scanări antivirus periodice pe dispozitivele de lucru	L1	K - S	Software-ul antivirus joacă un rol crucial în protejarea împotriva programelor malware prin detectarea, blocarea și îndepărtarea software-ului rău intenționat din dispozitivele de lucru. Realizarea unor scanări antivirus regulate ale dispozitivelor, în mod proactiv, la identificarea și eliminarea potențialelor amenințări, asigurând securitatea și integritatea datelor și a bună funcționare a dispozitivelor. Practicând această abordare proactivă, utilizatorii pot reduce în mod semnificativ riscul infectării cu programe malware și își pot salva active digitale.

6. Personalizarea setărilor de confidențialitate de pe conturile din rețele sociale, pentru a limita informațiile vizibile public.	L1	S	Personalizarea setărilor de confidențialitat pe conturile de social mass-media este esenţială în limitarea vizibilității informațiilor publice, asigurând că doar conținutul dorit este partajat cu publicul vizat și reducând riscul de acces neautorizat la datele personale. Prin personalizarea setărilor de confidențialitate, utilizatorii pot avea un control mai bun al prezenței lor online și își pot proteja în mod eficient confidențialitatea.
7. Testarea puterii parolelor personale folosind instrumente de gestionare a parolelor.	L1	A	Testarea puterii unei parole se realizează folosind ofline instrumente pentru managementul parolelor, pentru a vă asigura că parolele sunt puternice și sigure. Aceste instrumente ajută la identificarea parolelor slabe și furnizează recomandări pentru crearea unor parole mai puternici, sporind, astfel, securitatea online generală.
8. Demonstrarea modului în care sunt folosite funcțiile de securitate încorporate ale smartphone-ului personal, cum ar fi blocarea ecranului, pentru protecția datelor personale.	L1	S	Pentru a utiliza caracteristicile de securitate incoprporate în smartphone-ul personal, se merge la setările dispozitivului, se selectează opțiunea Securitate ("Security") sau Blocarea ecranului "Lock screen" și se selectează/setează o metodă puternică de blocare a ecranului, cum ar fi PIN, parolă, tipar/model (pattern) sau metodă biometrică (amprentă sau recunoaștere facială). Astfel, datele personale vor fi protejate împotriva accesului neautorizat și vă veți asigura că numai proprietarul smatphone-ului îl poate debloca și accesa informațiile sensibile.
9. Modificarea periodică a parolei pentru a evita posibile breșe de date/încălcări ale datelor.	L1	S - A	Modificarea periodică a parolelor este importantă pentru a minimiza riscul încălcării datelor. Schimbarea parolelor cu regularitate previne accesarea neautorizată a contului și îmbunătățește, per total, sexcuritatea online.
10. Deducerea pericolelor utilizării rețelelor Wi-Fi publice, nesecurizate, în cazul tranzacțiilor care implică date personale.	L1	K - S	Utilizarea rețelelor Wi-Fi publice nesecurizate pentru tranzacții care implică date personale aduce cu sine pericole semnificative; poate expune informațiile sensibile la potențiali ascultători, poate conduce la interceptarea datelor, la furtul identității, sau la accesul neautorizat la conturile financiare, personale. De aceea, este esențial să se evite utilizarea rețelelor Wi-Fi publice pentru tranzacțiile sensibile; pentru a asigura securitatea și confidențialitatea datelor se vor utiliza rețele securizate sau VPN-uri.

11. Diferențierea conținutului digital adecvat de cel neadecvat în vederea partajării pe conturile din rețele sociale.	L2	K - S	Conținutul digital adecvat partajării pe conturile din rețelele sociale trebuie să conțină postări pozitive și respectuoase, care să respecte liniile directoare ale platformei. Sunt admise, de asemenea, actualizări, informări și conținut inspirațional. Conținutul inadecvat partajării include materiale ofensatoare, instigări la ură, partajarea informațiilor personale fără consimțământ și încălcări ale dreptului de autor.
12. Discuții despre importanța protejării datelor cu caracter personal în timpul utilizării platformelor digitale.	L2	K	Înțelegerea importanței protejării datelor cu caracter personal în timpul utilizării platformelor digitale este crucială protejarea confidențialității, prevenirea furtului de identitate și evitarea potențialelor daune. Datele personale, cum ar fi nume, adrese, detalii financiare și informații de contact, sunt valoroase și pot fi folosite - de către actori rău intenționați - pentru diverse activități frauduloase. Prin prioritizarea protecției datelor, persoanele fizice pot menține controlul asupta informațiilor lor și pot reduce riscul încălcării datelor sau a accesului neautorizat, asigurând o experiență online securizată și sigură.
13. Validarea măsurilor adecvate pentru a proteja datele cu caracter personal înainte de a le partaja pe platformele digitale.	L2	A	Pentru a proteja datele personale înainte de a le partaja pe platformele digitale, se utilizează parole puternice și unice, se activează autentificarea cu doi factori (2FA) și este indicat să fiți precauți cu privire la informațiile partajate public. Revizuirea periodică și ajustarea setărilor de confidențialitate pentru a controla accesul la date, utilizarea VPN-urilor în loc de a folosi rețelele Wi-Fi publice sporesc și ele securitatea și previn accesul neautorizat, asigurând o experiență online mai sigură.
14. Efectuarea de tranzacții online după ce s-au luat măsurile adecvate de siguranță și de securitate.	L2	S	Luând măsuri adecvate de siguranță și securitate, persoanele fizice pot desfășura cu încredere transzacții online. Aceste măsuri includ utilizarea site-urilor web securizate cu HTTPS, autentificarea cu 2 factori (2FA), monitorizarea petiodică a extraselor de cont și evitarea partajării informațiilor sensibile prin rețele nesecurizate. Ținând cont de aceste măsuri de precauție, riscul fraudelor sau al accesului neautorizat este minimizat, permițând o experiență online fără griji, mai sigură.
15. Discuții despre importanța de a evita accesarea site-urilor web nesigure atunci când manipulați informații despre card.	L2	K	Înțelegerea despre importanţa evitării site-uri web nesigure când se manipulează informații despre card este esențială protejarea datelor personale și financiare. Site-urile web nesigure pot bloca măsurile de securitate adecvate; astfel, persoanele devin vulnerabile la încălcarea datelor și la accesul neautorizat. Evitând aceste site-uri web și oferind informații despre carduri doar pe platforme sigure și de încredere, persoanele se pot proteja față de potenţialele fraude, față de furtul de identitate, și pierderile financiare, asigurând o experienţă online mai sigură.

16. Stabilirea măsurilor adecvate pentru a verifica dacă persoanele cu care urmează să partajați date sensibile sunt de încredere.	L2	S - A	Pentru a verifica gradul de încredere a unor persoane înainte de a partaja date sensibile cu ele, trebuie cerute documente oficiale de identificare sau credențiale care să le confirme identitatea, sau să comunicați direct cu aceste persoane în vederea stabilirii încrederii sau să utilizați canale sigure de comunicații pentru schimbul de date. În plus, sunt recomandate revizuirea politicilor de de confidențialitate și a măsurilor de securitate în cazul partajării de date cu companii sau platforme online și obținere consensului explicit al persoanelor înainte de a partaja datele. Aceste măsurile ajută la asigurarea protecției datelor și la reducerea riscului de posibile încălcări ale datelor sau acces neautorizat.
17. Explicarea noțiunii de cookie și înțelegerea despre cum vă poate afecta un cookie datele sensibile.	L2	K	Un cookie (cookie HTTP) este un mic fișiere memorat pe dispozitivul unui utilizator atunci când persoana vizitează un site web. Cooki-urile sunt, în general, inofensive și utilizate în diverse scopuri. Totuși, ele pot afecta datele sensibile dacă sunt utilizate greșit, urmărind comportamentul și preferințele utilizatorului, credențialele de conectare, prezentând astfel un risc pentru confidențialitatea datelor dacă aceste informații sunt accesate de către părți neautorizate sau utilizate în scopuri rău intenționate.
18. Explicarea conceptul de „mod incognito” sau „navigare privată” în browser-ele web și modul de utilizare al acestuia.	L2	K	„Modul incognito” sau „navigare privată” este o caracteristică a browsere-lor web care permite utilizatorilor să navigheze în internet fără să alveze istoricul de navigare, cooki-uri sau date despre site-uri pe dispozitivele lor. Pentru utilizarea acestui mod de navigare, se deschide browser-ul web și se activează modul de navigare privată, -care se găsește de obicei în setări sau în meniu - și se pornește navigarea. După ce închideți fereastra de navigare privată, toate datele din acea sesiune vor fi șterse, iar experiența de navigare este privată și sigură.
19. Testarea cunoștințelor despre politicile de confidențialitate ale site-urilor web vizitate frecvent.	L2	A	Acest LO este vital pentru inițierea în mediul digital și pentru securitatea cibernetică. Subliniază importanța înțelegerii și a evaluării critica a politicilor de confidențialitate pentru a proteja datele personale. Acest obiectiv ajută cursanții să ia decizii informate despre activitățile lor online și încurajează practici onine mai sigure.
20. Recomandarea – către prieteni și familie – a celor mai bune practici pentru siguranța online.	L2	A	Pentru a asigura siguranța online, se recomandă utilizarea parolelor puternice și unice, care să permită doi factori dev autentificare (2FA), evitarea selectării link-urilor suspecte sau descărcarea atașamentelor din surse necunoscute, actualizări regulate de software și dispozitive atitudinea de a fi precaut în ceea ce privește partajarea informațiilor personale pe net. Recomandați prietenilor și familiei să se informeze asupra celor mai recente amenințări de pe net și să adopte practici responsabile de protecție datelor, pentru a-și salva confidențialitatea și securitatea în timpul utilizării platformelor digitale.

21. Identificarea acțiunilor adecvate care trebuie luate atunci când datele personale sunt utilizate abuziv pe platformele de social media	L3	K - S	Atunci când datele personale sunt utilizate în mod greșit pe platformele de rețele sociale, se raportează cu promptitudine echipei de asistență sau moderatorilor platformei. Se examinează și se modifică setările de confidențialitate pentru a limita accesul la informațiile personale. Dacă este necesar, se schimbă parolele pentru a preveni accesul neautorizat.
22. Dezvoltarea unei atitudini de precauție când faceți click pe link-uri din e-mailuri sau mesaje, și învățarea despre vizualizarea destinației reale a link-ului.	L3	A	Dezvoltarea unei atitudini de prudență, atunci când faceți click pe linkuri din e-mailuri sau mesaje, este crucială pentru a evita să cădeți victima înșelătoriilor de tip phishing sau a programelor malware. Se trece întotdeauna cursorul peste link-uri pentru a vedea destinația lor reală înainte de a face click pe link-uri, pentru a vă asigura că duc la site-uri web legitime și sigure.
23. Utilizarea identificării electronice pentru serviciile furnizate de autoritățile publice și sectorul de afaceri	L3	S	Utilizarea identificării electronice (eID) pentru serviciile furnizate de autoritățile publice și sectorul de afaceri oferă numeroase beneficii în ceea ce privește eficiența, securitatea și confortul utilizatorului. Prin adoptarea soluțiilor de identificare electronică, persoanele fizice pot accesa online diverse servicii guvernamentale și private fără a fi nevoie de vizite fizice sau documente. Autentificarea eID asigură verificarea securizată a identității, reducând riscul de fraudă și accesul neautorizat la informațiile sensibile. În plus, eficientizează procesele, accelerează furnizarea de servicii și promovează o experiență mai simplă și mai ușor de utilizat pentru cetățeni și clienți care interacționează atât cu entitățile publice, cât și cu cele private.
24. Acordarea de priorități protecției datelor atunci când utilizați rețelele sociale în scopuri profesionale sau educaționale.	L3	S	Prioritizarea protecției datelor în timpul utilizării rețelelor sociale în scopuri profesionale sau educaționale, prin: configurarea setărilor de confidențialitate, atitudine selectivă cu privire la conținutul partajat și activarea autentificării cu doi factori (2FA) pentru securitate sporită. Păstrarea vigilenței împotriva tentativelor de phishing, limitarea informațiilor personale din profiluri și precauție la permisiunile aplicațiilor terță parte pentru a proteja datele sensibile și pentru a asigura o experiență online mai sigură.
25. Recunoașterea escrocheriilor online și dezvoltarea unui scepticism sănătos față de ofertele nesolicitate online.	L3	K - A	Cunoștințele despre înșelătoriile online și dezvoltarea unui scepticism sănătos față de ofertele nesolicitate este esențial pentru a vă proteja de fraudă și furtul de identitate. A fi precaut și a verifica legitimitatea ofertelor înainte de a furniza informații personale sau de a efectua orice tranzacție financiară poate ajuta la evitarea situației în care cădeți victime înșelătoriilor și la asigurarea siguranței online.

26. Instalarea și actualizarea software-ului de securitate necesar, pe calculatorul și smartphone-ul personal	L3	S - A	Pregătirea calculatorului și a smartphone-ului pentru o securitate sporită se realizează prin instalarea și actualizarea regulată a software-ului de securitate necesar, cum ar fi programe antivirus și firewall. Aceste măsuri ajută la protejarea dispozitivelor în fața programelor malware, a virușilor și a altor amenințări online, asigurând o experiență online mai sigură.
27. Evaluarea obiceiurilor online în funcție de riscul lor de securitate.	L3	A	Este esențial ca persoanele să-și evalueze în mod regulat propriile obiceiuri online și să ia măsurile necesare pentru a minimiza riscurile de securitate, cum ar fi utilizarea parolelor puternice, activarea autentificării cu doi factori și evitarea partajării informațiilor sensibile cu surse necunoscute sau care nu sunt de încredere.
28. Discuții despre faptul că prelucrarea datelor cu caracter personal este supusă reglementărilor locale precum GDPR.	L3	K	Prelucrarea datelor cu caracter personal este supusă reglementărilor locale precum GDPR, asigurând protecția confidențialității datelor. Organizațiile trebuie să respecte cerințele GDPR atunci când manipulează datele cu caracter personal ale persoanelor fizice în UE.
29. Cunoașterea despre existența browsere-lor adaptate copiilor și manifestarea preocupărilor pentru siguranța online a copiilor prin utilizarea sau recomandarea acestor browsere.	L4	K - S	Părinții ar trebui să fie conștienți de existența browsere-lor adaptate copiilor, concepute pentru a oferi copiilor un mediu online mai sigur. Folosirea sau recomandarea acestor browsere, ajută la protejarea copiilor privind accesarea conținutului neadecvat și le asigură copiilor siguranța online în timp ce explorează lumea digitală.
30. Diferențierea între site-urile web sigure și cele nesigure atunci când navigați.	L3	K - S	Site-urile web securizate folosesc HTTPS în adresele URL și afișează o pictogramă de lacăt în bara de adrese a browserului, indicând faptul că, conexiunea dintre utilizator și site este criptată, asigurând astfel protecția datelor. Site-urile web nesigure nu au HTTPS în adresele URL și pot afișa un avertisment „Nesecurizat”, indicând că datele transmise între utilizator și site-ul web nu sunt criptate, prezentând riscuri potențiale pentru securitatea datelor.

31. Identificarea mesajelor suspecte de e-mail care pot conține încercări de phishing sau programe malware.	L4	K - S	Identificarea mesajelor suspecte de e-mail care conțin încercări de phishing sau programe malware se realizează prin căutarea unor expeditori necunoscuti, printr-un limbaj imperativ/urgent sau amenințător, a unor linkuri suspecte, a solicitărilor de informații sensibile, prin atașamente neașteptate și salutări generice și evitarea de a face click pe orice conținut îndoielnic. Este recomandat să verificați legitimitatea expeditorului printr-un alt canal sau să contactați direct organizația.
32. Utilizarea măsurilor avansate de securitate pentru a proteja datele personale pe conturile de rețele sociale.	L4	S - A	Aplicarea unor măsuri avansate de securitate pentru a proteja datele personale pe conturile de pe rețelele de socializare include activarea autentificării în doi factori (2FA), revizuirea și ajustarea regulată a setărilor de confidențialitate, utilizarea parolelor puternice și unice, precauția cu permisiunile aplicațiilor de la terțe părți și vigilenta împotriva tentativelor de phishing. În plus, se va evita partajarea publică a informațiilor sensibile, se vor limita datele personale pe profiluri și tebuie să vă informați despre cele mai recente funcții de confidențialitate și riscurile potențiale de pe platformele de socializare. Prin combinarea acestor măsuri, se poate îmbunătăți în mod semnificativ securitatea datelor personale și se poate puteți menține un control mai mare asupra confidențialității online.
33.Înțelegerea conceptului de criptare și a rolului criptării în protejarea informațiilor personale.	L4	K - S - A	Criptarea este procesul de conversie a datelor într-o formă codificată, cu scopul de a preveni accesul neautorizat. Rolul său în protejarea informațiilor cu caracter personal este de a se asigura că datele rămân în siguranță și confidențiale, chiar dacă sunt interceptate de părți neautorizate, protejând astfel confidențialitatea și menținând integritatea datelor.
34. Recunoașterea potențialelor riscuri ale partajării datelor personale pe rețelele de socializare și luarea măsurilor de precauție necesare.	L4	K	Recunoașterea potențialelor riscuri ale partajării datelor cu caracter personal pe rețelele sociale este esențială pentru a proteja confidențialitatea și a preveni utilizarea abuzivă a datelor. Unele riscuri includ furtul de identitate, hărțuirea cibernetică, atacurile de tip phishing și accesul neautorizat la informații sensibile. Măsurile de precauție necesare includ configurarea setărilor de confidențialitate, a fi selectiv în ceea ce privește conținutul partajat, utilizarea parolelor puternice, activarea autentificării cu doi factori și evitarea partajării publice a datelor sensibile. Fiind informate cu privire la riscurile potențiale și implementând aceste măsuri de precauție, persoanele se pot bucura de o experiență online mai sigură și mai sigură pe platformele de social media.

35. Compararea politicilor de confidențialitate ale diferitelor aplicații sau servicii pentru a determina practicile lor de colectare a datelor.	L4	K - S - A	Pentru a analiza politicile de confidențialitate ale diferitelor aplicații sau servicii, în privința practicilor lor de colectare a datelor, se vor examina tipurile de date colectate, scopul colectării datelor, practicile de procesare și partajare a datelor, consimțământul utilizatorului, măsurile de securitate și perioada de păstrare a datelor. Se verificăi dacă politicile respectă drepturile utilizatorului, utilizarea serviciilor de către terțe părți, confidențialitatea copiilor (dacă este cazul) și actualizările cu privire la modificările politicii.
36. Descrierea conceptului de comunicare criptată și valotizarea confidențialității prin alegerea aplicațiilor de comunicare care oferă criptare end-to-end.	L4	K - A	Comunicarea criptată presupune codificarea mesajelor astfel încât numai destinatarii vizați să le poată descifra, asigurând confidențialitatea și securitatea datelor. Pentru protejarea confidențialității, se aleg aplicații de comunicare care oferă criptare end-to-end, care asigură că mesajele sunt accesibile numai expeditorului și destinatarului, minimizând riscul accesului neautorizat la conversațiile sensibile.
37. Adoptarea celor mai bune practici pentru protejarea datelor cu caracter personal în diverse contexte online.	L4	K - A	Cele mai bune practici pentru protejarea datelor cu caracter personal online includ utilizarea parolelor puternice, activarea autentificării în doi factori, actualizarea regulată a software-ului, precauție față de link-uri și atașamente, revizuirea setărilor de confidențialitate, limitarea partajării informațiilor personale, utilizarea rețelelor securizate, monitorizarea conturilor și copii de rezervă (backup) a datelor.
38. Investigarea anomaliilor în dispozitivele Dvs. care ar putea indica o încălcare a confidențialității.	L4	S	Pentru a vă proteja confidențialitatea, fiți vigilenți și investigați orice anomalie în dispozitivele dvs., cum ar fi utilizarea neașteptată a datelor, ferestre pop-up neobișnuite, aplicații necunoscute sau încercări de acces neautorizat. Dacă observați orice activitate suspectă, luați măsuri imediate, cum ar fi rularea de scanări antivirus, actualizarea software-ului de securitate și schimbarea parolelor, pentru a vă proteja datele personale și pentru a preveni potențialele încălcări ale confidențialității.
39. Diferențierea tuturor tipurilor de „cookie” și înțelegerea modului în care acestea pot fi utilizate de site-uri web pentru stocarea datelor utilizatorilor.	L4	K - S	Site-urile web folosesc cookie-uri de sesiune pentru stocarea temporară a datelor în timpul unei sesiuni de navigare, cookie-uri persistente pentru stocarea datelor pe termen mai lung și cookie-uri de la terți pentru urmărirea comportamentului utilizatorilor și publicitate direcționată. Utilizatorii ar trebui să fie precauți cu privire la colectarea datelor și își pot gestiona setările cookie-urilor în browserele lor, pentru a controla confidențialitatea și a limita urmărirea.

40. Prioritizarea conturilor online în funcție de sensibilitatea informațiilor pe care le dețin.	L4	S	Prioritizarea conturilor online, în funcție de sensibilitatea informațiilor pe care le dețin, este extrem de importantă. Este necesară connsolidarea măsurilor de securitate, cum ar fi folosirea parolelor puternice și activarea autentificării cu doi factori, pentru conturile cu date mai sensibile, pentru a asigura o protecție mai bună împotriva accesului neautorizat.
41. Evaluarea eficacității măsurilor de securitate în salvarea datelor personale pe plarformele digitale.	L5	A	Eficacitatea măsurilor de securitate în protejarea datelor cu caracter personal pe platformele digitale depinde de puterea măsurilor implementate și de receptivitatea platformei la amenințările emergente. Măsurile de securitate robuste, cum ar fi criptarea, autentificarea cu mai mulți factori și actualizările regulate contribuie la o mai bună protecție a datelor, dar monitorizarea continuă și conștientizarea utilizatorilor sunt esențiale pentru a asigura eficacitatea continuă.
42. Aplicarea pașilor necesari pentru a șterge memoria cache și istoricul de navigare din browsere web și aplicații.	L5	S	Ștergerea memoriei cache și a istoricului de navigare îmbunătățește confidențialitatea și securitatea online prin eliminarea fișierelor temporare și a datelor stocate de browser-ul web, reducând riscul accesului neautorizat la informațiile sensibile și minimizând urmărirea activității utilizatorilor pe site-urile web.
43. Enumerarea potențialelor riscuri asociate cu partajarea informațiilor sensibile pe conturile publice din rețelele sociale.	L5	K	Potențialele riscurile asociate cu partajarea informațiilor sensibile pe conturile publice din rețelele sociale includ furtul de identitate, încălcarea confidențialității, înșelătoriile direcționate și urmărirea cibernetică, precum și expunerea informațiilor personale către un public mai larg, ceea ce poate duce la o atenție nedorită sau la utilizarea abuzivă a datelor. Este esențială adoptarea unei atitudini precaute cu privire la tipul de conținut partajat pe platformele publice pentru a proteja confidențialitatea și securitatea personală.
44. Descrierea implicațiilor juridice ale manipulării greșite a datelor cu caracter personal pe platformele de social media.	L5	K	Manipularea greșită a datelor cu caracter personal pe platformele de socializare poate duce la consecințe legale, cum ar fi amenzi, penalități și procese civile pentru încălcarea legilor privind protecția datelor, precum și deteriorarea reputației și pierderea oportunităților de afaceri din cauza pierderii încrederii utilizatorilor. Respectarea reglementărilor privind protecția datelor și practicile responsabile de manipulare a datelor sunt esențiale pentru a evita aceste implicații legale.
45. Crearea și aplicarea politicilor de protecție a datelor în cadrul unei organizații sau a unei comunități.	L5	A	Pentru a crea și a aplica politici de protecție a datelor, a efectua o evaluare, a dezvolta politici clare, a le comunica părților interesate, a implementa proceduri și a revizui și actualiza în mod regulat politicile, este necesar să numiți un responsabil cu protecția datelor, să integrați confidențialitatea prin proiectare și să asigurați conformitatea terților pentru a construi încrederea și a proteja datele în cadrul organizației sau comunității.

46. Formularea de strategii pentru a răspunde la breșe de date și minimizarea impactului	L5	A	Ca răspuns la breșele de date, implementați un plan de răspuns rapid la incident, incluzând proceduri de izolare, de investigare și de notificare. Reduceți impactul informând prompt persoanele afectate, cooperând cu autoritățile de reglementare, efectuând evaluări amănunțite și îmbunătățind măsurile de securitate pentru a preveni vbreșele viitoare.
47. Examinarea importanței securizării rețelei Wi-Fi de acasă și schimbarea numelui (SSID) și cunoștințe despre setarea unei parole puternice pentru Wi-Fi și dezactivarea WPS-ului.	L5	S	Securizareai rețelei Wi-Fi de acasă schimbând numele (SSID) și setând o parolă puternică pentru a preveni accesul neautorizat; dezactivarea Wi-Fi Protected Setup (WPS) pentru a minimiza potențialele vulnerabilități de securitate și pentru a asigura un mediu Wi-Fi mai sigur.
48. Diagnosticarea potențialelor puncte slabe în setarea confidențialității datelor personale.	L5	S	Pentru a diagnostica potențialele puncte slabe în configurarea confidențialității datelor, trebuie revizuite măsurile și practicile de securitate, cum ar fi folosirea parolelor puternice și unice, activarea autentificării cu doi factori, actualizarea regulată a software-ului și revizuirea permisiunilor aplicațiilor. În plus, trebuie evaluat modul în care sunt gestionate datele personale, cum ar fi partajarea lor pe rețelele sociale sau cu terțe părți și identificarea domeniior susceptibile la îmbunătățiri pentru consolidarea confidențialității generale a datelor.
49. Informarea despre cele mai recente probleme de confidențialitate și soluții, discuții cu persoane competente, pentru a-ți dezvolta și proteja rețeaua cinste”	L5	A	Pentru a fi la curent cu cele mai recente preocupări și soluții de confidențialitate, este necesar să vă conectați cu alți utilizatori competenți care vă împărtășesc interesele. Implicarea în discuții, participarea la ateliere sau participarea la forumuri online cu persoane care au aceleași opinii, pot ajuta la obținerea unor informații valoroase și la aflarea celor mai bune practici pentru îmbunătățirea confidențialității și a securității datelor.
50. Validarea autenticității și a siguranței descărcărilor digitale.	L5	A	Pentru a valida autenticitatea și siguranța descărcărilor digitale, trebuie să descărcați fișiere din surse recunoscute și oficiale. Verificați adresa URL a site-ului web, verificați semnăturile digitale sau sumele de verificare (checksums) furnizate de către dezvoltator și utilizați un software antivirus de încredere pentru a scana fișierele descărcate pentru malware înainte de a le deschide sau instala.

51. Recunoașterea responsabilităților și a obligațiior legale ale organizațiilor și companiilor în manipularea datelor cu caracter personal.	L6	K	Organizațiile au responsabilitățile legale de a trata datele personale în mod etic, transparent și sigur, în conformitate cu legile și reglementările privind protecția datelor. Organizațiile și companiile pot pot trase la răspundere pentru încălcarea datelor și pentru nerespectarea legilor privind protecția datelor și se pot confrunta cu amenzi, penalități sau acțiuni legale dacă manipulează în mod defectuos datele cu caracter personal.
52. Sublinierea rolului setărilor de confidențialitate pentru dispozitivele de tip "casă inteligentă" (smart home devices) și dezvoltarea unei atitudini de precauție în utilizarea acestora, ținând cont de implicațiile privind confidențialitatea.	L6	S - A	Înțelegerea rolului setărilor de confidențialitate pentru dispozitivele de tip casă inteligentă pentru a controla datele pe care le colectează și le partajează. Dezvoltarea unei atitudini de precauție pe timpul utilizătii acestora, luând în considerare potențialele implicații ale confidențialității; configurarea setărilor de confidențialitate pentru protecția datelor personale și pentru a menține controlul asupra confidențialității.
53. Organizarea de evaluări complete ale riscurilui pentru a identifica potențiale riscuri legate de confidențialitatea datelor.	L6	A	Efectuarea unor evaluări complete ale riscului este crucială pentru a identifica în mod eficient potențialele riscuri de confidențialitate a datelor. Acestea sjută organizațiile să identifice în mod proactiv vulnerabilitățile, să evalueze potențialele impacturi și să implementeze măsurile de protecție adecvate pentru a protejarea datelor personale.
54. Observarea rolului factorilor umani în securitatea cibernetică și aplicarea conștientizării ingineriei sociale și a contramăsurilor în interacțiunile digitale.	L6	K	Aprecierea rolului factorilor umani în securitatea cibernetică implică înțelegerea faptului că, comportamentul și acțiunile umane pot avea un impact semnificativ asupra securității datelor. Dezvoltând conștientizarea ingineriei sociale și implementând contramăsuri, cum ar fi precauția în ceea ce privește partajarea informațiilor personale online, verificarea legitimității mesajelor și a solicitărilor și rămânând informați cu privire la cele mai recente tactici de phishing, persoanele se pot proteja de amenințările cibernetice și pot contribui la un mediu digital mai sigur.

55. Prioritizarea confidențialității și a securității, ca valori fundamentale.	L6	S	Prioritizarea confidențialității și a securității datelor ca valori fundamentale este esențială pentru protejarea informațiilor sensibile, protejarea încrederii utilizatorilor și asigurarea conformității cu legile privind protecția datelor. Făcând din confidențialitatea și securitatea datelor o prioritate, persoanele și organizațiile pot crea un mediu digital mai sigur și pot menține confidențialitatea și integritatea datelor cu caracter personal.
56. Examinarea prezenței știrilor false și dezvoltarea unei atitudini critice față de informațiile din online.	L6	K - A	Înțelegeți că există știri false și fiți critic atunci când întâlniți informații online, verificând sursele, verificând mai multe referințe credibile și fiți precauți în privința distribuirii de informații neverificate. Dezvoltarea unei atitudini critice ajută la prevenirea răspândirii dezinformării și contribuie la o comunitate online mai informată și mai responsabilă.
57. Inventarierea și gestionarea amprentei digitale pe mai multe platforme și servicii.	L6	S	Inventariați și gestionați amprenta digitală, revizuind și evaluând informațiile pe care le-ai partajat pe diverse platforme și servicii. Actualizați în mod regulat setările de confidențialitate, limitați datele personale pe care le partajați și luați în considerare ștergerea sau dezactivarea conturilor care nu mai sunt necesare, pentru a vă reduce prezența online și pentru a vă îmbunătăți confidențialitatea.
58. Explorarea măsurilor proactive pentru a proteja datele personale și confidențialitatea online; prevenirea potențialelor amenințări.	L6	S	Pentru a proteja în mod proactiv datele personale și confidențialitatea online, utilizați parole puternice, activați autentificarea cu doi factori (2FA), actualizați periodic software-ul și dispozitivele, fiți precaut cu link-urile și atașamentele, revizuiți setările de confidențialitate, limitați partajarea informațiilor personale, utilizați rețelele securizate, educați despre amenințările online și monitorizați în mod regulat conturile pentru activități neautorizate. Adoptarea acestor măsuri îmbunătățește confidențialitatea și securitatea online, reducând riscul de încălcare a datelor și furtul de identitate.
59. Deducerea potențialelor riscuri și consecințe ale breșelor de date pe platformele de social media.	L6	K - S	Încălcările de date/breșele de date de pe platformele de social media pot avea un impact semnificativ asupra utilizatorilor, incluzând furtul de identitate, pierderi financiari și deteriorarea reputației. În 2018, o încălcare a datelor pe Facebook a expus datele personale a peste 50 de milioane de utilizatori. Aceste date ar putea fi folosite de infractori pentru a comite furt de identitate, fraudă și alte infracțiuni.

60. Investigarea vulnerabilităților de securitate a platformelor digitale și recomandări de îmbunătățiri.	L6	S	Pentru a investiga vulnerabilitățile de securitate din platformele digitale, se efectuează evaluări amănunțite de securitate, cum ar fi teste de penetrare și revizuiri ale codului. Se identifică punctele slabe, cum ar fi software-ul învechit, metodele de autentificare nesigure sau criptarea inadecvată a datelor. Apoi sunt recomandate îmbunătățiri, cum ar fi actualizări regulate de securitate, mecanisme de autentificare puternice și implementarea protocoalelor de criptare pentru sporirea securității platformei și pentru protejarea datelor utilizatorilor.
61. Detectarea amenințărilor avansate de securitate cibernetică și potențialul lor impact asupra datelor personale.	L7	S	Amenințările avansate de securitate cibernetică, cum ar fi programele malware sofisticate, ransomware-ul și atacurile de phishing direcționate, pot avea consecințe grave asupra datelor personale. Aceste amenințări pot conduce la acces neautorizat, încălcări ale datelor/breșe ale datelor, furt de identitate și fraudă financiară, compromițând informațiile sensibile și provocând pierderi financiare, daune ale reputației și tulburări emoționale pentru persoanele ale căror date sunt expuse. Pentru a se proteja împotriva unor astfel de amenințări, utilizatpeii trebuie să rămână vigilenți, să utilizeze măsuri de securitate solide și să acorde prioritate confidențialității datelor în activitățile lor online. Organizațiile ar trebui, de asemenea, să investească în instrumente avansate de securitate cibernetică și în formarea angajaților pentru a proteja datele personale de amenințările cibernetice sofisticate.
62. Explicați conceptul de adresă IP și rolul acesteia în activitatea online.	L7	K - S - A	O adresă IP este o etichetă numerică unică atribuită fiecărui dispozitiv de pe internet, utilizată pentru comunicare și schimb de date. Joacă un rol crucial în rutarea datelor și urmărirea activităților utilizatorilor online, motiv pentru care protejarea adresei IP este importantă pentru menținerea confidențialității și a securității online.
63. Reamintirea conceptului DNS, cum poate afecta DNS-ul confidențialitatea. Schimbarea DNS-ului pe calculator, pe router sau pe modem.	L7	K - S	Sistemul de nume al domeniului (DNS) traduce numele de domenii în adrese IP pe internet; poate afecta confidențialitatea, deoarece furnizotul de servicii internet al utilizatorului poate înregistra solicitările DNS. Confidențialitatea poate fi îmbunătățită confidențialitatea modificând setările DNS de pe calculator sau de pe router, pentru a utiliza servere DNS mai sigure, axate pe confidențialitate.

64. Studiul conceptul de metadate în fișierele digitale și păstrarea confidențialității eliminând metadatele din fișiere înainte de a le partaja online.	L7	K - A	Metadatele sunt informații suplimentare stocate în fișiere digitale, cum ar fi fotografii sau documente, care pot dezvălui detalii precum locația, data și dispozitivul utilizat. Pentru protejarea confidențialității, metadatele trebuie eliminate din fișiere, înainte de a partaja fișierele online; astfel, se previne divulgarea neintenționată a informațiilor sensibile.
65. Dezvoltarea preocupării pentru securizarea comunicațiilor prin e-mail. Criptarea e-mail-ulilor.	L7	A	Dezvoltarea unei preocupări pentru securitatea comunicațiilor prin e-mail recunoscând riscurile potențiale ale accesului sau interceptării neautorizate: pentru a îmbunătăți securitatea e-mailurilor, e-mailurile trebuie criptae utilizând servicii de e-mail securizate sau instrumente de criptare. În acest fel, numai destinatarii vizați pot citi conținutul, iar informațiile sensibile vor fi ferite de privirile indiscrete.
66. Înțelegerea riscurilor permisiunilor aplicațiilor mobile, auditarea și limitarea periodică a permisiunilor pe smartphone-ul personal.	L7	K - S	Înțelegerea riscurilor permisiunilor aplicațiilor mobile: unele aplicații pot solicita accesul la date sensibile sau la caracteristici ale dispozitivului care nu sunt necesare pentru funcționalitatea lor. Auditarea și limitarea periodică a permisiunile aplicațiilor pe smartphone-ul personal reduc potențialele riscuri de confidențialitate și constituie asigurarea că aplicațiile accesează numai datele și funcțiile de care au, într-adevăr, nevoie.
67. Evidențierea beneficiilor și a riscurilor autentificării biometrice și dezvoltarea unei abordări prudente în ceea ce privește utilizarea caracteristicilor biometrice ca măsuri de securitate.	L7	K - S - A	Autentificarea biometrică oferă acces convenabil și securizat prin utilizarea trăsăturilor biologice unice, cum ar fi amprentele digitale sau recunoașterea facială. Cu toate acestea, utilizarea funcțiilor biometrice necesită precauție, deoarece acestea pot crea probleme de confidențialitate în cazul în care sunt compromise sau manipulate greșit. Pentru o mai bună protecție, combinați autentificarea biometrică cu alte măsuri de securitate.
68. Înțelegerea unor cazuri juridice legate de confidențialitatea datelor și a implicațiilor acestora.	L7	K	Un caz legal notabil legat de confidențialitatea datelor este „Facebook, Inc. împotriva Comisiei Federale pentru Comerț (FTC),” în care Facebook s-a confruntat cu o amendă de 5 miliarde de dolari pentru manipularea greșită a datelor utilizatorilor. Cazul a evidențiat importanța reglementărilor privind protecția datelor și potențialele consecințe pentru companiile care nu reușesc să adere la angajamentele de confidențialitate și securizarea datelor utilizatorilor.

69. Extrapolarea viitorului confidențialității datelor pe baza progreselor tehnologice și a peisajului juridic în evoluție.	L7	K	Viitorul confidențialității datelor se va concentra în continuare, probabil, pe progresele tehnologice din criptare, pe stocarea sigură a datelor și pe autentificare a utilizatorilor, pentru a proteja datele personale. În plus, peisajul juridic în evoluție poate aduce reglementări mai stricte privind protecția datelor, o aplicare sporită și o mai mare conștientizare în rândul persoanelor și a organizațiilor cu privire la importanța protejării informațiilor personale în era digitală.
70. Modificarea configurațiilor dispozitivului și ale rețelei pentru o confidențialitate optimă a datelor.	L7	S	Modificarea configurațiilor dispozitivelor și ale rețelei activând funcții de securitate precum firewall-uri, VPN-uri și autentificarea cu doi factori și actualizarea periodică a software-ul pentru a asigura confidențialitatea optimă a datelor și protecția împotriva potențialelor amenințări cibernetice. Implementarea acestor măsuri poate îmbunătăți în mod semnificativ securitatea dispozitivelor și a rețelei, protejând datele personale și activitățile online.
71. Discutarea conceptelor DoH, DoT și DNSSEC, și despre cum pot acestea să îmbunătățească confidențialitatea și securitatea împotriva programelor malware.	L8	K	DoH (DNS-over-HTTPS), DoT (DNS-over-TLS) și DNSSEC (Domain Name System Security Extensions) sunt protocoale concepute pentru a îmbunătăți confidențialitatea și securitatea în comunicarea DNS. DoH și DoT criptează interogările DNS, prevenind interceptarea prin ascultare și potențialele interceptări ale datelor DNS; DNSSEC adaugă un nivel de validare și autentificare răspunsurilor DNS, reducând riscul de falsificare DNS și îmbunătățind integritatea generală a datelor și protecția împotriva atacurilor malware și phishing.
72.Interpretarea cercetărilor de ultimă oră privind protecția datelor și aplicarea lor în scenarii din lumea reală.	L8	K - S - A	Interpretarea cercetărilor de ultimă oră în domeniul protecției datelor implică a fi informat cu privire la cele mai recente progrese în criptare, anonimizare a datelor, partajarea securizată a datelor și a tehnicilor de păstrare a confidențialității. Aplicarea acestor cunoștințe în scenarii din lumea reală implică implementarea măsurilor de ultimă generație de protecție a datelor în organizații, asigurarea conformității cu legile privind confidențialitatea datelor și adoptarea celor mai bune practici pentru a proteja informațiile sensibile de potențiale breșe și acces neautorizat. Procedând astfel, companiile pot spori încrederea clienții, își pot proteja reputația și pot îmbunătăți securitatea generală a datelor în peisajul digital de astăzi.
73. Cunoștințe de utilizarea a unui VPN atât pentru rețelele cu acces local (domestice), cât și pentru rețelele publice.	L8	S	Pentru a configura un VPN pentru rețelele cu acces local (domestice), cât și pentru rețelele publice, se selectează un furnizor recunoscut de servicii VPN, se instalează clientul VPN pe dispozitivel și se realizeză conectarea la locația de server dorită, pentru o comunicare sigură și criptată. Utilizarea unui VPN asigură confidențialitatea datelor și protecția împotriva potențialelor amenințări atunci când sunt accesate resursele locale de la distanță (remote) sau sunt utilizate rețele Wi-Fi publice.

74. Detectarea și răspunsul la atacurile cibernetice sofisticate care vizează datele personale.	L8	S	Pentru a detecta și a răspunde la atacurile cibernetice sofisticate care vizează datele personale, se utilizează măsuri avansate de securitate, cum ar fi sisteme de detectare a intruziunilor, instrumente de informații despre amenințări și monitorizare continuă pentru a identifica cu promptitudine potențialele amenințări. Implementarea unor planuri de răspuns la incident pentru a atenua impactul atacurilor și pentru a securiza datele personale împotriva accesului neautorizat, asigurând o abordare proactivă a securității cibernetice.
75. Analizarea compromiterii avansate a datelor, cu scopul de a le înțelege metodele și vulnerabilitățile.	L8	S	Discuțiile despre compromiterea avansată a datelor implică analiza tehnicilor utilizate de către infractorii cibernetici pentru a obține acces neautorizat la informații sensibile și identificarea vulnerabilităților din sistemele în care au apărut breșele de securitate. Înțelegând metodele și punctele slabe, organizațiile își pot consolida măsurile de securitate și pot proteja mai bine datele personale de viitoarele amenințări cibernetice.
76. Explorarea beneficiilor de confidențialitate ale descentralizării și cunoașterea modului de utilizare a platformelor și a serviciilor descentralizate.	L8	S	Aprecierea beneficiilor de confidențialitate ale descentralizării implică înțelegerea faptului că platformele și serviciile descentralizate distribuie datele pe mai multe noduri, reducând riscul unui singur punct de eșec și sporind confidențialitatea datelor. Învățând să utilizeze platformele descentralizate, cursanții vor avea un control mai mare asupra datelor lor, deoarece minimizează dependența de entitățile centralizate, atenuează riscurile de confidențialitate și promovează un mediu digital mai sigur și privat.
77. Încorporarea abordărilor inovatoare - de protecție a datelor personale - în tehnologiile emergente.	L8	A	Conducerea abordărilor inovatoare pentru protejarea datelor personale în tehnologiile emergente necesită eforturi proactive pentru a integra principiile confidențialității prin proiectare, pentru a implementa tehnici robuste de criptare și a asigura că protecția datelor consrituie o prioritate în dezvoltarea noilor tehnologii. Prin adoptarea unor strategii progresiste, se pot aborda provocările unice generate de tehnologiile emergente și se poate menține confidențialitatea datelor ca aspect fundamental al progresului digital.
78. Elaborarea un plan extins de conștientizare a securității cibernetice în protecția datelor personale.	L8	A	Dezvoltarea unui plan extins de conștientizare a securității cibernetice pentru protecția datelor cu caracter personal prin educarea persoanelor cu privire la amenințările cibernetice comune, promovarea practicilor de parole puternice, creșterea gradului de conștientizare cu privire la phishing și ingineria socială, încurajând actualizări regulate de software și subliniind importanța confidențialității datelor în toate activitățile online. Implementarea acestui plan va permite persoanelor să își protejeze în mod proactiv datele personale și să contribuie la un mediu online mai sigur.

79. Învățarea conceptului de „apărare în profunzime” în securitatea cibernetică și aprecierea importanței implementării mai multor straturi de securitate.	L8	K - S - A	„Apărare în profunzime” în securitatea cibernetică se referă la strategia de implementare a mai multor straturi de măsuri de securitate pentru protecția împotriva diferitelor tipuri de amenințări cibernetice. Apreciind importanța acestor straturi, cum ar fi firewall-urile, software-ul antivirus, criptarea și controalele de acces, persoanele și organizațiile își pot îmbunătăți semnificativ poziția generală de securitate cibernetică și își pot proteja mai bine datele sensibile de potențiale încălcări.
80. Sprijinirea demersurilor pentru promovarea unei protecții mai puternice a confidențialității datelor și a practicilor digitale etice.	L8	A	A sprijini demersurile care susțin o protecție mai puternice a confidențialității datelor și a practicilor digitale etice implică promovarea activă a conștientizării cu privire la importanța confidențialității datelor, sprijinirea implementării unor reglementări solide de confidențialitate și stabilirea unui exemplu pozitiv prin aderarea la standardele etice în activitățile online. Prin susținerea acestor inițiative, se poate crea un mediu digital mai sigur și mai respectuos pentru persoane și organizații.