Co-funded by the European Union

FinPower

Module: SECURITATE ȘI SIGURANȚĂ ONLINE

Pregătit de: RightChallenge

PROJECT ID NUMBER: 2022-1-AT01-KA220-ADU-000087985

FinPower

Co-funded by the European Union

Table of Contents

OBIECTIVE DE ÎNVĂȚARE

Obiectivele de învățare ale acestui modul sunt diverse și concepute pentru a oferi participanților cunoștințe complete și abilități practice în domenii specifice.

Primul subiect este „Securitatea online". Acesta aprofundează domeniul securității online, subliniind riscurile comune precum furtul de identitate, tranzacțiile frauduloase și amenințările la adresa securității cibernetice. Acesta explică impactul financiar și emoțional al acestor riscuri asupra indivizilor, subliniind importanța protejării informațiilor personale.

A doua temă este „Cum să cumpărăm în siguranță online". Obiectivele-cheie includ înțelegerea riscurilor asociate cumpărăturilor online, identificarea metodelor comune de fraudă online și a criminalității cibernetice, evaluarea securității site-urilor web și a metodelor de plată și punerea în aplicare a strategiilor de protejare a informațiilor personale și financiare. De asemenea, cursanții vor fi instruiți să recunoască potențialele escrocherii online pentru a îmbunătăți protecția personală și a celor din jur.

În cele din urmă, tema „Care sunt metodele alternative de plată?" se axează pe înțelegerea, analizarea și utilizarea în siguranță a diferitelor metode alternative de plată, cum ar fi portofelele electronice, criptomonedele și plățile mobile. De asemenea, se pune accentul pe educarea participanților, în special a femeilor, cu privire la metodele de plată durabile, oferindu-le posibilitatea de a face alegeri financiare responsabile din punct de vedere ecologic și social.

În general, aceste obiective de învățare urmăresc să ofere participanților o înțelegere cuprinzătoare a fiecărui subiect și să îi doteze cu cunoștințele și abilitățile necesare pentru a naviga eficient în domeniu.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

SECURITATE ONLINE

Identificarea riscurilor comune de securitate

Potrivit FBI, după cum citează Kaspersky, **furtul de identitate** are loc atunci când cineva obține și utilizează în mod ilegal informațiile personale ale altei persoane (cum ar fi numele, numărul de asigurare socială, numărul cardului de credit sau detaliile contului bancar) pentru a comite fraude sau alte infracțiuni.

Exemple:

- Utilizarea neautorizată a informațiilor privind cardul de credit sau contul bancar al altei persoane pentru a face achiziții.
- Deschiderea de noi conturi de credit sau împrumuturi folosind identitatea altei persoane.
- Depunerea de declarații fiscale frauduloase folosind numere de securitate socială furate.

Tranzacțiile frauduloase implică achiziționarea, utilizarea sau transferul neautorizat sau înșelător de fonduri, bunuri sau alte active prin mijloace înșelătoare sau necinstite.

Exemple:

- Un escroc care se dă drept reprezentant legitim al unei companii și solicită plata unor servicii sau produse false.
- Acces neautorizat la un cont bancar sau la un card de credit pentru a efectua retrageri sau achiziții neautorizate.
- Facturi false sau scheme de facturare în care sunt trimise facturi pentru servicii care nu au fost niciodată prestate.

Amenințările la adresa securității cibernetice se referă la orice activități sau evenimente rău intenționate care încearcă să compromită confidențialitatea, integritatea sau disponibilitatea informațiilor și sistemelor digitale.

Exemple:

- Atacuri malware (de exemplu, viruși, ransomware, spyware) care infectează și compromit sistemele sau rețelele informatice.
- E-mailuri de tip phishing sau înșelăciuni prin inginerie socială concepute pentru a păcăli persoanele să dezvăluie informații sensibile sau să dea clic pe linkuri malițioase.
- Încălcări ale securității datelor prin care părți neautorizate obțin acces la informații sensibile stocate în baze de date sau servere.

Cum pot afecta aceste riscuri persoanele din punct de vedere financiar și emoțional?

Impactul financiar:

1. **Furtul de identitate:** Victimele furtului de identitate se pot confrunta cu pierderi financiare din cauza tranzacțiilor neautorizate, a împrumuturilor frauduloase sau a debitelor din conturile lor. De asemenea, acestea pot suporta cheltuieli legate de serviciile de soluționare a furtului de identitate și de taxele judiciare.
2. **Tranzacții frauduloase:** Persoanele afectate de tranzacții frauduloase pot suferi pierderi financiare directe în cazul în care li se fură fonduri sau se fac plăți neautorizate pe conturile lor. De asemenea, acestea pot suferi efecte financiare

indirecte, cum ar fi comisioane pentru descoperiri de cont sau cecuri fără acoperire.

3. **Amenințări la adresa securității cibernetice:** Victimele amenințărilor la adresa securității cibernetice pot suferi pierderi financiare ca urmare a furtului de informații financiare, a plății de răscumpărări pentru a recâștiga accesul la date criptate sau a costurilor asociate recuperării în urma încălcării securității datelor (de exemplu, investigații criminalistice, amenzi de reglementare, despăgubiri pentru clienți).

Impactul emoțional:

1. **Furtul de identitate**: Impactul emoțional al furtului de identitate poate fi semnificativ, provocând sentimente de încălcare, anxietate și neajutorare. Victimele pot experimenta stres și frustrare în timp ce parcurg procesul de raportare a furtului, de contestare a taxelor frauduloase și de restabilire a identității.
2. **Tranzacții frauduloase**: Persoanele afectate de tranzacții frauduloase pot experimenta sentimente de trădare și vulnerabilitate, în special dacă frauda implică o persoană de încredere. De asemenea, acestea pot simți o pierdere a controlului asupra securității lor financiare și a vieții private.
3. **Amenințări la adresa securității cibernetice**: Victimele amenințărilor la adresa securității cibernetice pot simți teamă, anxietate și neîncredere în siguranța informațiilor lor personale și a activităților online. De asemenea, pot avea un sentiment de vulnerabilitate și frustrare din cauza lipsei percepute de control asupra confidențialității și securității lor digitale.

Activitate: Discuții de grup privind breșe recente de securitate și impactul acestora asupra indivizilor și organizațiilor.

Această activitate urmărește să analizeze și să discute încălcările recente ale securității și impactul acestora asupra persoanelor și organizațiilor, inclusiv consecințele financiare și emoționale, lecțiile învățate și strategiile de prevenire.

Pas cu pas:

1. Împărțiți participanții în grupuri mici de 4-6 membri.

2. Atribuiți fiecărui grup un studiu de caz recent privind încălcarea securității sau un articol de presă pe care să îl analizeze. Exemplele includ încălcări ale securității datelor la companii importante, atacuri ransomware asupra organizațiilor din domeniul sănătății sau înșelătorii de tip phishing care vizează persoane fizice.

Se pot utiliza următoarele exemple:

Breșe de date la companii importante:

Breșa de date CAM4 (martie 2020): Serverul Elasticsearch al site-ului de streaming video pentru adulți CAM4 a fost violat, expunând peste 10 miliarde de înregistrări. Înregistrările compromise includeau nume complete, adrese de e-mail, orientare sexuală, transcrieri

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

ale chat-ului, transcrieri ale corespondenței prin e-mail, hash-uri ale parolelor, adrese IP și jurnale de plăți.

Breșa de date Yahoo (octombrie 2017): Yahoo a dezvăluit că o breșă din august 2013 a compromis 3 miliarde de conturi. Încălcarea a fost raportată pentru prima dată de Yahoo în timp ce se afla în negocieri pentru a se vinde către Verizon.

Breșa de date Aadhaar (martie 2018): Datele personale a peste un miliard de cetățeni din India stocate în cea mai mare bază de date biometrice din lume puteau fi cumpărate online.

Atacuri Ransomware asupra organizațiilor din domeniul sănătății:

University of Vermont (UVM) **Medical Centre** (octombrie 2020): Angajații Centrului Medical UVM nu au putut utiliza înregistrările medicale electronice (EHR), programele de salarizare și alte instrumente digitale vitale timp de aproape o lună. Multe intervenții chirurgicale au trebuit să fie reprogramate, iar pacienții cu cancer au trebuit să meargă în altă parte pentru tratament cu radiații.

Inova Health System: Inova Health System a fost unul dintre furnizorii de servicii medicale care au căzut victimă unui atac ransomware.

Escrocherii de tip phishing care vizează persoanele fizice:

Spear Phishing: Aceasta este o metodă de phishing țintită pe care infractorii cibernetici o folosesc pentru a vă fura informațiile prin substituirea unei surse de încredere.

HTTPS Phishing: Un infractor cibernetic vă păcălește să vă furnizați informațiile personale utilizând un site web rău intenționat.

Email Phishing: Unul dintre cele mai comune atacuri de phishing este email phishing-ul. Email phishing este atunci când un atacator cibernetic vă trimite un e-mail pretinzând că este altcineva în speranța că veți răspunde cu informațiile solicitate.

3. Furnizați grupurilor întrebări orientative pentru a facilita discuția:

- Care au fost circumstanțele și amploarea breșei de securitate?

- Ce impact financiar și emoțional a avut încălcarea asupra persoanelor și organizațiilor?

- Care au fost principalele lecții învățate în urma incidentului?

- Ce strategii sau măsuri ar fi putut fi implementate pentru a preveni încălcarea?

4.Acordați grupurilor 20-30 de minute pentru a revizui studiul de caz sau articolul, a discuta întrebările și a pregăti punctele-cheie pentru prezentare.

5.După timpul de discuție, reuniți-vă din nou ca grup întreg.

6.Fiecare grup prezintă un rezumat al constatărilor sale, subliniind aspectele cheie ale breșei de securitate, impactul acesteia, lecțiile învățate și măsurile preventive.

7.Încurajați discuțiile deschise și schimbul de idei între participanți.

8.Facilitați o sesiune de debriefing în care participanții reflectă asupra temelor comune, provocărilor și bunelor practici discutate în cadrul studiilor de caz.

9.Încheiați activitatea rezumând principalele concluzii și subliniind importanța conștientizării securității cibernetice și a măsurilor proactive în atenuarea riscurilor de securitate.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Importanța măsurilor de securitate

Înainte de a intra în tainele securității online, să înțelegem de ce protejarea informațiilor personale este atât de importantă. Informațiile personale, de la numele dvs. la detaliile financiare, joacă un rol crucial în viața noastră.

Acestea cuprind o gamă largă de date care pot fi utilizate pentru a identifica sau localiza o persoană. Acestea includ, dar nu se limitează la:

1. Numele
2. Adresa
3. Numărul de securitate socială (SSN)
4. Data nașterii
5. Adresa de e-mail.
6. Numărul de telefon.
7. Informații financiare (de exemplu, numere de card de credit, detalii ale contului bancar)
8. Informații medicale
9. Datele de identificare ale conturilor online (de exemplu, nume de utilizator, parole)

Protejarea acestor informații este extrem de importantă din următoarele motive:

- **Furtul de identitate**: Unul dintre cele mai semnificative riscuri asociate cu faptul că informațiile personale ajung în mâini greșite este furtul de identitate. Hoții de identitate pot utiliza informațiile personale furate pentru a deschide conturi frauduloase, pentru a face achiziții neautorizate sau chiar pentru a comite infracțiuni în numele victimei. Prejudiciul financiar și emoțional al furtului de identitate poate fi substanțial, deoarece victimele petrec adesea timp și resurse semnificative pentru a remedia daunele aduse creditului și reputației lor.
- **Frauda financiară**: Informațiile personale sunt adesea vizate de infractorii cibernetici care încearcă să comită fraude financiare. Aceasta poate implica accesul neautorizat la conturi bancare, fraude cu carduri de credit sau cereri frauduloase de împrumut folosind identități furate. Pierderile financiare rezultate în urma unei astfel de fraude pot fi devastatoare, afectând scorurile de credit ale persoanelor, stabilitatea financiară și încrederea în instituțiile financiare.
- **Încălcarea confidențialității**: Protejarea informațiilor personale este esențială pentru protejarea dreptului la viață privată al persoanelor fizice. Accesul neautorizat la datele cu caracter personal poate duce la încălcări ale dreptului la viață privată, atunci când informațiile sensibile sunt expuse unor părți neautorizate. Încălcările confidențialității pot duce la situații jenante, prejudicii de reputație și scăderea încrederii în organizațiile responsabile cu protejarea datelor cu caracter personal.

- **Consecințe juridice și de reglementare**: Organizațiile care nu protejează în mod adecvat informațiile personale se pot confrunta cu consecințe juridice și de reglementare. Legile privind protecția datelor, cum ar fi Regulamentul general privind protecția datelor (GDPR) în Europa sau California Consumer Privacy Act (CCPA) în Statele Unite, impun cerințe stricte pentru colectarea, stocarea și gestionarea datelor cu caracter personal. Nerespectarea acestor reglementări poate duce la amenzi semnificative, răspunderi juridice și afectarea reputației unei organizații.

Cele mai bune practici pentru protejarea informațiilor personale

Pentru a asigura securitatea informațiilor dvs. personale, urmați acești pași esențiali:

1. **Utilizați parole puternice**: Creați parole puternice și unice pentru fiecare cont online și schimbați-le în mod regulat. Evitați să utilizați parole ușor de ghicit sau să reutilizați parolele pentru mai multe conturi.

2. **Activați autentificarea cu doi factori (2FA):** Atunci când este posibil, activați autentificarea cu doi factori pentru a adăuga un nivel suplimentar de securitate conturilor dvs. online. 2FA solicită utilizatorilor să furnizeze o a doua formă de verificare, cum ar fi un cod trimis pe dispozitivul mobil, în plus față de parola lor.

3. **Fiți prudent cu informațiile personale**: Fiți prudent atunci când împărtășiți informații personale online sau la telefon. Evitați să furnizați informații sensibile dacă nu este necesar și verificați legitimitatea solicitărilor înainte de a partaja orice date.

4. **Asigurați-vă dispozitivele**: Asigurați-vă securitatea dispozitivelor, inclusiv a computerelor, smartphone-urilor și tabletelor, instalând software antivirus, activând firewall-uri și menținând software-ul la zi cu cele mai recente patch-uri de securitate.

5. **Informați-vă**: Rămâneți informat cu privire la escrocheriile comune și tacticile de phishing utilizate de infractorii cibernetici pentru a păcăli persoanele să dezvăluie informații personale. Fiți vigilent și sceptic cu privire la e-mailurile, apelurile telefonice sau mesajele nesolicitate care presupun cererea de informații personale sau plăți.

Prezentare generală a securizării conturilor și tranzacțiilor online pentru a preveni accesul neautorizat

În era digitală actuală, securizarea conturilor și tranzacțiilor online este de o importanță capitală pentru a proteja informațiile personale și financiare sensibile împotriva accesului neautorizat și a activităților frauduloase. Securizarea conturilor și tranzacțiilor online implică punerea în aplicare a unei combinații de măsuri preventive și de bune practici pentru a proteja împotriva diferitelor amenințări la adresa securității cibernetice, cum ar fi pirateria informatică, phishing-ul și furtul de identitate. Mai jos sunt prezentate componentele cheie ale securizării conturilor și tranzacțiilor online:

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Parole puternice:

1. Utilizați parole puternice și unice pentru fiecare cont online.
2. Evitați utilizarea de parole ușor de ghicit, precum „parola123" sau „123456".
3. Luați în considerare utilizarea unei fraze de acces compusă dintr-o combinație de litere, cifre și caractere speciale.
4. Actualizați în mod regulat parolele și evitați reutilizarea acestora pentru mai multe conturi.

Autentificare cu doi factori (2FA):

1.Activați autentificarea cu doi factori (2FA) ori de câte ori este disponibilă.

2. 2FA adaugă un nivel suplimentar de securitate solicitând utilizatorilor să furnizeze o a doua formă de verificare, cum ar fi un cod trimis pe dispozitivul mobil, în plus față de parola lor.

3. Acest lucru ajută la prevenirea accesului neautorizat, chiar dacă parola este compromisă.

Comunicare securizată:

1. Asigurați-vă că tranzacțiile și comunicațiile online sunt efectuate pe canale securizate.

2. Căutați HTTPS în URL-ul site-ului și pictograma unui lacăt în bara de adrese a browserului, indicând faptul că conexiunea este criptată.

3. Evitați transmiterea de informații sensibile prin rețele Wi-Fi nesecurizate, deoarece acestea pot fi vulnerabile la interceptarea de către atacatori.

Actualizări periodice ale software-ului:

1. Păstrați software-ul, sistemele de operare și aplicațiile la zi cu cele mai recente patch-uri și actualizări de securitate.
2. Vulnerabilitățile din software-ul neactualizat pot fi exploatate de atacatori pentru a obține acces neautorizat la dispozitive și conturi.

Feriți-vă de atacurile de phishing:

1. Fiți atenți la e-mailurile, mesajele text sau apelurile telefonice de tip phishing care încearcă să păcălească utilizatorii să dezvăluie informații personale sau să dea clic pe linkuri malițioase.
2. Evitați să faceți clic pe linkuri sau să descărcați atașamente din e-mailuri suspecte sau nesolicitate.
3. Verificați legitimitatea solicitărilor de informații personale înainte de a furniza orice date sensibile.

Utilizați metode de plată sigure:

1. Atunci când efectuați tranzacții online, utilizați metode de plată sigure, cum ar fi cardurile de credit sau platformele de plată de renume care oferă protecție cumpărătorului.
2. Evitați să furnizați informații de plată către site-uri nesecurizate sau necunoscute.

Monitorizați activitatea contului:

1. Monitorizați în mod regulat activitatea contului și extrasele de cont pentru orice tranzacții neautorizate sau activități suspecte.
2. Raportați imediat orice tranzacție neautorizată sau activitate suspectă instituției financiare sau furnizorului de servicii respectiv.

Criptarea datelor:

1. Utilizați tehnologii de criptare pentru a proteja datele sensibile, atât în tranzit, cât și în repaus.
2. Criptarea bruiază datele pentru a le face ilizibile pentru utilizatorii neautorizați, protejându-le astfel de interceptare sau furt.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Explicații privind recunoașterea și evitarea înșelătoriilor pentru a ne proteja de pierderi financiare

Escrocheriile se prezintă sub diferite forme și pot viza persoanele prin diferite canale, inclusiv e-mailuri, apeluri telefonice, mesaje text și reclame online. Recunoașterea și evitarea înșelătoriilor este esențială pentru a vă proteja de pierderi financiare și alte consecințe negative. Iată o explicație a principalelor strategii de recunoaștere și evitare a înșelătoriilor:

Informați-vă:

1. Rămâneți informat cu privire la tipurile comune de escrocherii și scheme frauduloase, cum ar fi escrocheriile de tip phishing, escrocheriile legate de investiții și escrocheriile legate de loterii.

2. Fiți la curent cu cele mai recente tactici folosite de escroci pentru a înșela persoanele și a le exploata încrederea.

Fiți sceptic cu privire la comunicările nesolicitate:

1. Fiți precaut cu e-mailurile, apelurile telefonice sau mesajele text nesolicitate care vă cer informații personale sau financiare.
2. Evitați să răspundeți sau să faceți clic pe linkurile din comunicările nesolicitate, mai ales dacă acestea par suspecte sau prea bune pentru a fi adevărate.

Verificați legitimitatea solicitărilor:

1. Verificați legitimitatea solicitărilor de informații personale sau financiare înainte de a furniza orice date sensibile.
2. Contactați direct organizația folosind informațiile de contact oficiale pentru a confirma autenticitatea solicitărilor.

Evitați luarea de decizii pripite:

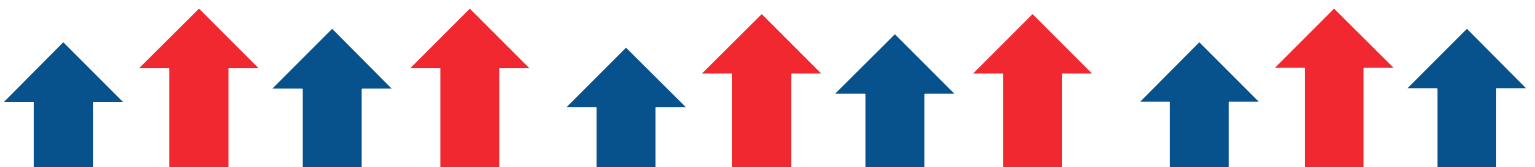
1. Evitați să luați decizii pripite sau să acționați impulsiv ca răspuns la tacticile de presiune utilizate de escroci.
2. Luați-vă timp să cercetați și să verificați ofertele sau oportunitățile înainte de a vă angaja financiar.

Protejați informațiile personale:

1. Protejați informațiile personale și financiare evitând să partajați date sensibile cu părți necunoscute sau neverificate.
2. Fiți precauți atunci când furnizați informații personale online, în special pe site-uri care nu sunt sigure sau de încredere.

Aveți încredere în instinctele dumneavoastră:

1. Aveți încredere în instinctele dvs. și feriți-vă de ofertele sau oportunitățile care par prea bune pentru a fi adevărate.
2. Dacă ceva vi se pare suspect sau nu pare în regulă, luați măsurile de precauție necesare și cereți sfatul unor surse de încredere.



FinPower

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Activitate: Scenariu de joc de rol în care cursanții prezintă securizarea conturilor și tranzacțiilor online

Obiectivul acestei activități de joc de rol este de a-i implica pe participanți într-un scenariu simulat în care își protejează conturile și tranzacțiile online. Prin participarea activă la exercițiul de joc de rol, participanții vor dobândi experiență practică în implementarea măsurilor de securitate pentru a preveni accesul neautorizat la conturile și tranzacțiile lor online.

Materiale necesare:

Sugestii pentru scenariul de joc de rol (pregătite în prealabil)

Recuzită (opțional)

Materiale de scris

Instrucțiuni:

Introducere (5 minute):

Prezentați scopul activității de joc de rol: să exersați securizarea conturilor și tranzacțiilor online pentru a preveni accesul neautorizat.

Explicați că participanții vor fi împărțiți în perechi sau grupuri mici pentru a juca diferite scenarii legate de securitatea online.

Atribuirea scenariilor (5 minute):

Împărțiți participanții în perechi sau grupuri mici.

Atribuiți fiecărei perechi/grup un scenariu specific de joc de rol legat de securizarea conturilor și tranzacțiilor online. Scenariile pot include:

Crearea unei parole puternice și activarea autentificării cu doi factori pentru un cont de e-mail.

Actualizarea setărilor de securitate pentru un cont bancar online.

Recunoașterea și evitarea tentativelor de phishing într-un e-mail sau mesaj text.

Verificarea legitimității unui site de cumpărături online înainte de a face o achiziție.

Pregătirea jocului de rol (10 minute):

Furnizați participanților o scurtă prezentare generală a scenariului care le-a fost atribuit, inclusiv obiectivele pe care trebuie să le atingă și orice acțiuni specifice pe care ar trebui să le întreprindă.

Scurtă prezentare generală:

a) Crearea unei parole puternice și activarea autentificării cu doi factori pentru un cont de e-mail: Participanții vor simula procesul de creare a unei parole puternice și de activare a autentificării cu doi factori pentru a spori securitatea unui cont de e-mail. Ei vor discuta despre strategiile de creare a unei parole sigure și de implementare a măsurilor suplimentare de autentificare pentru a preveni accesul neautorizat.

b) Actualizarea setărilor de securitate pentru un cont bancar online: Participanții vor face un joc de rol cu privire la pașii implicați în actualizarea setărilor de securitate pentru un cont bancar online. Ei vor revizui și ajusta setările de confidențialitate, vor seta alerte pentru activități suspecte și vor explora caracteristicile de securitate suplimentare oferite de platforma bancară online.

c) Recunoașterea și evitarea tentativelor de phishing într-un e-mail sau mesaj text: Participanții vor simula întâlnirea cu o tentativă de phishing într-un e-mail sau mesaj text și vor exersa recunoașterea semnelor de avertizare ale unei comunicări frauduloase. Ei vor discuta despre strategiile de verificare a legitimității mesajelor și de evitare a potențialelor înșelătorii.

d) Verificarea legitimității unui site de cumpărături online înainte de a face o achiziție: Participanții vor exemplifica procesul de verificare a legitimității unui site de cumpărături online înainte de a face o achiziție. Ei vor examina caracteristicile de securitate ale site-ului, cum ar fi criptarea SSL și opțiunile de plată securizate, și vor discuta strategii de identificare a comercianților online de încredere.

Încurajați participanții să facă un brainstorming împreună și să își planifice abordarea scenariului de joc de rol. Aceștia ar trebui să discute despre pașii pe care îi vor lua pentru a-și securiza eficient conturile și tranzacțiile online.

<u>Joc de rol (20 de minute):</u>

Participanții joacă scenariile care le-au fost atribuite, preluând rolurile persoanelor implicate (de exemplu, titulari de cont, reprezentanți ai serviciului clienți, hackeri).

Încurajați participanții să se angajeze într-un dialog și în acțiuni realiste pe măsură ce navighează în scenariu și pun în aplicare măsuri de securitate pentru a preveni accesul neautorizat.

Facilitatorii pot oferi îndrumare și sprijin, după caz, răspunzând la întrebări și oferind sugestii pentru a ajuta participanții să navigheze eficient prin scenarii.

<u>Debriefing și discuții (15 minute):</u>

După activitatea de joc de rol, reuniți-vă din nou ca un grup întreg pentru un debriefing și o discuție.

Invitați participanții să își împărtășească experiențele din timpul exercițiului de joc de rol, inclusiv orice provocări pe care le-au întâmpinat și modul în care le-au abordat.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Facilitați o discuție cu privire la principalele concluzii și lecții învățate din activitate, subliniind importanța securizării conturilor și tranzacțiilor online pentru a preveni accesul neautorizat.

Încurajați participanții să reflecteze asupra propriilor practici de securitate online și să identifice domenii de îmbunătățire pe baza scenariilor de joc de rol.

Concluzie (5 minute):

Rezumați principalele puncte discutate în timpul activității și consolidați importanța măsurilor proactive de securitate online.

Mulțumiți participanților pentru participare și implicarea lor în exercițiul de joc de rol.

Măsuri de securitate de bază

Măsurile de securitate de bază constituie fundamentul unei apărări solide împotriva amenințărilor digitale. Utilizarea de parole puternice și unice, activarea autentificării cu doi factori (2FA) și actualizarea periodică a software-ului și dispozitivelor sunt pași esențiali în protejarea conturilor online și a informațiilor personale. În secțiunile următoare, vom aprofunda fiecare dintre aceste metode, explorând importanța lor și oferind sfaturi practice pentru implementare.

Importanța utilizării parolelor unice puternice și metodele de creare a acestora

În era digitală de astăzi, parolele joacă un rol crucial în securizarea conturilor noastre online și a informațiilor sensibile. Cu toate acestea, prevalența amenințărilor cibernetice, cum ar fi atacurile de phishing, încălcările securității datelor și atacurile prin forța brută, subliniază importanța utilizării unor parole unice puternice pentru a ne proteja conturile de accesul neautorizat. Iată câteva motive pentru care utilizarea parolelor unice puternice este esențială:

1. **Prevenirea accesului neautorizat:** Parolele unice puternice acționează ca prima linie de apărare împotriva accesului neautorizat la conturile noastre online. Acestea fac mult mai dificil pentru infractorii cibernetici să ghicească sau să spargă parolele prin instrumente automate sau atacuri cu forță brută.

2. **Protejarea informațiilor personale:** Conturile online conțin adesea informații personale și financiare sensibile, cum ar fi detalii bancare, fișe medicale și comunicări personale. Utilizarea unor parole unice puternice ajută la protejarea acestor informații împotriva accesului neautorizat, reducând riscul de furt de identitate, fraudă financiară și încălcare a confidențialității.

3. **Atenuarea impactului încălcărilor securității datelor:** În cazul unei încălcări a securității datelor în care datele de autentificare sunt compromise, existența unor parole unice puternice pentru fiecare cont poate atenua impactul prin împiedicarea infractorilor cibernetici să acceseze alte conturi folosind aceleași date de autentificare. Această practică, cunoscută sub numele de igiena

parolelor, ajută la limitarea pagubelor și la limitarea expunerii la riscuri de securitate suplimentare.

4. **Conformitatea cu cele mai bune practici de securitate:** Parolele unice puternice se aliniază celor mai bune practici din industrie și ghidurilor de securitate cibernetică recomandate de organizații precum National Institute of Standards and Technology (NIST) și Cybersecurity and Infrastructure Security Agency (CISA). Respectarea acestor recomandări demonstrează un angajament față de securitatea online și ajută persoanele fizice și organizațiile să respecte reglementările și standardele relevante.

Metode de creare a parolelor unice puternice:

1. **Crearea de parole unice puternice** implică utilizarea unei combinații de caractere, inclusiv litere majuscule și minuscule, numere și simboluri speciale, pentru a face parolele mai rezistente la încercările de hacking. Iată câteva metode de creare a parolelor unice puternice:

2. **Fraze de acces**: În locul parolelor tradiționale, luați în considerare utilizarea frazelor de acces - combinații mai lungi de cuvinte sau fraze care sunt ușor de reținut, dar dificil de ghicit de către alții. Frazele de acces pot fi formate din cuvinte aleatorii, versuri de cântece, titluri de cărți sau fraze memorabile care au o semnificație personală.

3. **Combinații aleatorii de caractere**: Utilizați o combinație aleatorie de litere majuscule și minuscule, cifre și simboluri speciale pentru a crea o parolă unică. Evitați utilizarea unor modele sau secvențe ușor de ghicit, precum „123456" sau „parola", care sunt frecvent vizate de hackeri.

4. **Generatoare de parole**: Luați în considerare utilizarea instrumentelor generatoare de parole sau a funcțiilor integrate în software-ul de gestionare a parolelor pentru a crea parole unice puternice. Generatoarele de parole pot genera parole aleatorii de diferite lungimi și complexitate, făcându-le foarte sigure și greu de ghicit.

5. **Evitarea cuvintelor de dicționar:** Evitați utilizarea cuvintelor de dicționar sau a frazelor ușor de ghicit ca parole, deoarece acestea sunt susceptibile la atacurile de dicționar și la instrumentele de spargere a parolelor. În schimb, optați pentru combinații de caractere aleatorii sau fraze de acces care nu se regăsesc în dicționare sau în modele lingvistice comune.

6. Parole unice pentru fiecare cont: Asigurați-vă că fiecare cont online are o parolă unică pentru a preveni efectul de domino al unei singure parole compromise care duce la accesul neautorizat la mai multe conturi. Evitați utilizarea aceleiași parole pentru mai multe conturi, deoarece acest lucru crește riscul de breșe de securitate și compromisuri.

Prezentare generală a autentificării cu doi factori și rolul acesteia în îmbunătățirea securității conturilor

Autentificarea cu doi factori (2FA) este un nivel suplimentar de securitate utilizat pentru a proteja conturile online, dincolo de simplul nume de utilizator și parolă. Aceasta cere

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

utilizatorilor să furnizeze doi factori de autentificare diferiți pentru a-și verifica identitatea și a obține acces la conturile lor. Acești factori de autentificare se împart de obicei în trei categorii: ceva ce știți (de exemplu, o parolă), ceva ce aveți (de exemplu, un dispozitiv mobil sau un jeton hardware) și ceva ce sunteți (de exemplu, date biometrice precum amprentele digitale sau recunoașterea facială).

Importanța autentificării cu doi factori:

1. **Securitate sporită**: 2FA îmbunătățește în mod semnificativ securitatea contului prin adăugarea unui nivel suplimentar de protecție dincolo de o simplă parolă. Chiar dacă un hacker reușește să obțină parola unui utilizator, acesta va avea nevoie de acces la al doilea factor (de exemplu, un dispozitiv mobil sau date biometrice) pentru a se autentifica cu succes și a obține acces la cont.

2. **Protecție împotriva furtului de parole**: Furtul parolei este o metodă frecvent utilizată de hackeri pentru a obține acces neautorizat la conturile online. Prin solicitarea unei a doua forme de autentificare, 2FA reduce riscul de acces neautorizat, chiar dacă parolele sunt compromise.

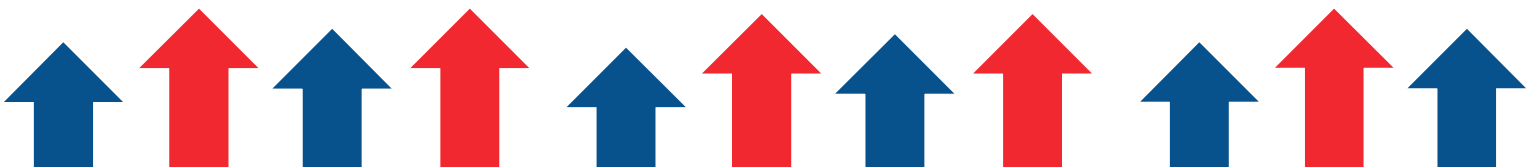
3. **Reducerea riscului de acces neautorizat**: 2FA reduce riscul de acces neautorizat la conturi, în special în cazul reutilizării parolelor sau al parolelor slabe. Chiar dacă parola unui utilizator este compromisă din cauza unei încălcări a securității datelor sau a unui atac de phishing, factorul suplimentar de autentificare adaugă un nivel suplimentar de securitate.

4. **Conformitatea cu standardele de securitate**: Multe organizații și organisme de reglementare recomandă sau solicită utilizarea 2FA ca parte a protocoalelor lor de securitate. Conformitatea cu aceste standarde contribuie la asigurarea faptului că datele și resursele sensibile sunt protejate în mod adecvat împotriva accesului neautorizat.

5. **Conștientizarea și controlul utilizatorului**: 2FA sporește conștientizarea și controlul utilizatorului asupra securității contului, oferind un nivel suplimentar de apărare împotriva accesului neautorizat. Utilizatorii sunt împuterniciți să ia măsuri proactive pentru a-și proteja conturile și datele.

Metode de autentificare cu doi factori:

1. **Coduri prin mesaje text (SMS)**: Un cod de verificare este trimis pe dispozitivul mobil al utilizatorului prin mesaj text, pe care acesta trebuie să îl introducă împreună cu parola pentru autentificare.
2. **Aplicații de autentificare**: Utilizatorii pot instala aplicații de autentificare precum Google Authenticator, Microsoft Authenticator sau Authy pe dispozitivele lor mobile. Aceste aplicații generează parole unice în funcție de timp (TOTP) pe care utilizatorii le introduc împreună cu parola lor pentru autentificare.
3. **Jetoane hardware**: Unele organizații emit jetoane hardware care generează coduri de autentificare. Utilizatorii trebuie să dețină jetonul fizic pentru a se autentifica.
4. **Autentificare biometrică**: Unele sisteme acceptă metode de autentificare biometrică, cum ar fi amprentele digitale, recunoașterea facială sau recunoașterea vocală ca al doilea factor.



Importanța actualizării periodice a software-ului și a dispozitivelor pentru a reduce vulnerabilitățile de securitate

Importanța actualizării regulate a software-ului și a dispozitivelor pentru reducerea vulnerabilităților de securitate nu poate fi supraestimată. Iată câteva motive cheie pentru care este crucială:

1. **Remedierea vulnerabilităților de securitate**: Actualizările software includ adesea patch-uri care abordează vulnerabilități de securitate cunoscute. Aceste vulnerabilități pot fi exploatate de infractorii cibernetici pentru a obține acces neautorizat la sisteme, a fura informații sensibile sau a întrerupe serviciile. Actualizările regulate contribuie la asigurarea faptului că aceste vulnerabilități sunt abordate prompt, reducând riscul de exploatare.

2. **Protejarea împotriva exploatărilor**: Infractorii cibernetici dezvoltă în mod constant noi tehnici și exploatări pentru a viza software-ul și dispozitivele. Prin menținerea la zi a software-ului și a dispozitivelor, utilizatorii se pot proteja împotriva vulnerabilităților și exploatărilor nou descoperite. Acest lucru contribuie la menținerea integrității și securității sistemelor și datelor.

3. **Menținerea conformității**: În multe industrii, conformitatea cu reglementările și standardele legate de securitatea cibernetică este obligatorie. Actualizarea periodică a software-ului și a dispozitivelor este adesea o cerință a acestor reglementări și standarde. Nerespectarea acestor cerințe poate duce la sancțiuni, amenzi sau alte consecințe juridice.

4. **Îmbunătățirea stabilității și a performanței**: Actualizările software nu abordează doar vulnerabilitățile de securitate, ci includ și îmbunătățiri ale stabilității și performanței. Prin menținerea la zi a software-ului și a dispozitivelor, utilizatorii pot beneficia de fiabilitate sporită, performanță mai rapidă și funcționalitate îmbunătățită.

5. **Protejarea împotriva programelor malware și a atacurilor cibernetice**: Software-ul și dispozitivele neactualizate sunt mai vulnerabile la infecțiile malware și la atacurile cibernetice. Infractorii cibernetici exploatează adesea vulnerabilitățile cunoscute ale software-ului învechit pentru a distribui malware, cum ar fi ransomware, viruși sau spyware. Actualizările regulate ajută la protejarea împotriva acestor amenințări prin eliminarea lacunelor de securitate.

6. **Mențineți suportul furnizorului**: Furnizorii de software oferă de obicei asistență și întreținere pentru produsele lor pentru o perioadă limitată. Pe măsură ce software-ul ajunge la sfârșitul ciclului său de viață, furnizorii pot înceta să mai lanseze actualizări și patch-uri, lăsând utilizatorii vulnerabili la amenințările de securitate. Actualizarea periodică a software-ului și a dispozitivelor asigură faptul că utilizatorii continuă să beneficieze de asistența furnizorului și de protecție împotriva vulnerabilităților de securitate.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Activitate: Atelier practic despre crearea de parole puternice și activarea autentificării cu doi factori pe diverse platforme online

Obiectivul acestui atelier este de a educa participanții cu privire la importanța creării de parole puternice și a activării autentificării cu doi factori (2FA) pentru a spori securitatea conturilor lor online. Participanții vor învăța cum să creeze și să gestioneze parole puternice și să configureze 2FA pe diferite platforme online.

Materiale necesare:

Calculatoare sau dispozitive mobile cu acces la internet pentru fiecare participant

Diapozitive de prezentare sau broșuri privind crearea de parole puternice și activarea 2FA

Exemple de platforme online care acceptă 2FA (de exemplu, Google, Facebook, Twitter, site-uri bancare)

Materiale de scris

Instrucțiuni:

Introducere (10 minute):

Urați bun venit participanților la atelier și prezentați importanța creării de parole puternice și a activării autentificării cu doi factori (2FA) pentru a spori securitatea online.

Oferiți o prezentare generală a agendei atelierului și a obiectivelor de învățare.

Prezentare privind crearea de parole puternice (15 minute):

Prezentați o scurtă introducere generală a caracteristicilor parolelor puternice, inclusiv lungimea, complexitatea și unicitatea.

Furnizați sfaturi și orientări pentru crearea de parole puternice, cum ar fi utilizarea unei combinații de litere majuscule și minuscule, cifre și caractere speciale.

Demonstrați tehnici de gestionare a parolelor, cum ar fi utilizarea managerilor de parole pentru generarea și stocarea în siguranță a parolelor puternice.

De exemplu:

1Password: Cunoscut pentru securitatea sa imbatabilă și tonele de funcții suplimentare. Este o alegere de top pentru majoritatea utilizatorilor și este deosebit de bun pentru familii.

Dashlane: Oferă servicii extra remarcabile, cum ar fi monitorizarea dark web și un VPN2 rapid. De asemenea, este cunoscut pentru gestionarea premium a parolelor.

RoboForm: Un manager de parole accesibil, cu o securitate bună și capacități puternice de completare a formularelor.

Keeper: Manager de parole extrem de sigur, cu aplicații intuitive și prețuri flexibile.

NordPass: Cunoscut pentru gestionarea sigură a parolelor și este deosebit de bun pentru administratorii de conturi de afaceri.

Bitwarden: Cunoscut pentru gestionarea gratuită a parolelor.

Aceste managere de parole vă pot ajuta să creați parole unice și puternice pentru fiecare dintre conturile dvs. online și vă pot alerta cu privire la eventualele scurgeri de date. Toate sunt fie complet gratuite, fie foarte necostisitoare. Vă rugăm să rețineți că, deși aceste administratoare de parole oferă servicii similare, caracteristicile exacte și prețurile pot varia. Este întotdeauna o idee bună să consultați site-urile lor oficiale pentru informații cât mai exacte și actualizate.

Activitate practică: Crearea de parole puternice (20 de minute):

Împărțiți participanții în perechi sau grupuri mici.

Furnizați participanților o listă de conturi online obișnuite (de exemplu, e-mail, rețele sociale, servicii bancare) și rugați-i să creeze parole puternice pentru fiecare cont.

Încurajați participanții să aplice intrucțiunile privind crearea parolelor discutate anterior și să se asigure că fiecare parolă este unică și greu de ghicit.

Circulați printre grupuri pentru ajutor și îndrumare, după caz.

Prezentare privind activarea autentificării cu doi factori (2FA) (15 minute):

Prezentați un rezumat general al autentificării cu doi factori (2FA) și rolul acesteia în consolidarea securității conturilor online.

Explicați diferitele tipuri de metode 2FA, cum ar fi codurile SMS, aplicațiile de autentificare și jetoanele hardware.

Furnizați instrucțiuni pas cu pas pentru activarea 2FA pe diferite platforme online, inclusiv exemple de platforme care acceptă 2FA

Activitate practică: Activarea autentificării cu doi factori (2FA) (20 de minute):

Instruiți participanții să aleagă o platformă online care acceptă 2FA (de exemplu, Google, Facebook, Twitter, site web bancar).

Ghidați participanții prin procesul de activare a 2FA pe platforma aleasă, utilizând instrucțiunile pas cu pas furnizate.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Încurajați participanții să își folosească dispozitivele mobile sau computerele pentru a urmări și activa 2FA pe conturile lor.

Ajutor și asistență pentru depanare, după caz.

Încheiere și discuții (10 minute):

Adunați participanții pentru o scurtă recapitulare și discuție.

Treceți în revistă principalele concluzii ale atelierului, inclusiv importanța creării de parole puternice și a activării autentificării cu doi factori (2FA) pentru a spori securitatea online.

Încurajați participanții să își împărtășească experiențele și orice provocări pe care le-au întâmpinat în timpul activităților practice.

Oferiți resurse suplimentare și sprijin participanților care doresc să afle mai multe despre cele mai bune practici de securitate online.

Concluzie:

Mulțumiți participanților pentru participarea și implicarea lor în atelier.

Reamintiți-le participanților să aplice cunoștințele și competențele dobândite pentru a-și securiza conturile online și a-și proteja informațiile personale.

Încurajați participanții să împărtășească cunoștințele nou dobândite cu prietenii, familia și colegii pentru a promova practici mai bune de securitate online.

Recunoașterea înșelătoriilor

Mai jos sunt explorate tipurile comune de înșelăciuni, caracteristicile acestora și semnalele de alarmă la care trebuie să fiți atenți.

E-mailurile de phishing sunt e-mailuri frauduloase care par a proveni de la organizații sau persoane legitime, dar sunt concepute pentru a păcăli destinatarii să dezvăluie informații sensibile, precum parole, nume de utilizator, numere de carduri de credit sau alte informații personale. Aceste e-mailuri conțin adesea linkuri către site-uri web false sau atașamente malițioase.

Exemplu: În 2016, o înșelătorie de phishing foarte răspândită a vizat utilizatorii Gmail prin trimiterea de e-mailuri care păreau să provină de la Google, solicitând utilizatorilor să facă clic pe un link către o pagină falsă de autentificare Google. Utilizatorii care și-au introdus datele de autentificare pe pagina falsă au furnizat din greșeală informațiile de autentificare atacatorilor, care au obținut apoi acces neautorizat la conturile lor.

Schemele Ponzi sunt scheme de investiții frauduloase care promit randamente ridicate investitorilor cu riscuri mici sau inexistente. Într-o schemă Ponzi, investitorii timpurii primesc randamente din investițiile investitorilor târzii, mai degrabă decât din profiturile legitime. Pe măsură ce schema se dezvoltă, operatorul poate utiliza fonduri de la noii investitori pentru a plăti randamente investitorilor anteriori, creând iluzia rentabilității.

Exemplu: Una dintre cele mai faimoase scheme Ponzi din istorie a fost orchestrată de Bernie Madoff, care a înșelat investitorii cu miliarde de dolari pe parcursul mai multor decenii. Madoff le promitea investitorilor randamente ridicate și constante prin intermediul firmei sale de investiții, dar, în schimb, folosea fondurile noilor investitori pentru a plăti randamente investitorilor existenți. Schema s-a prăbușit în cele din urmă în 2008, provocând pierderi financiare masive pentru mii de investitori.

Escrocheriile în domeniul investițiilor implică scheme sau oferte frauduloase care promit randamente ridicate ale investițiilor, dar care, în cele din urmă, duc la pierderi financiare pentru investitori. Aceste escrocherii vizează adesea persoanele care doresc să își investească banii în oportunități care par prea frumoase pentru a fi adevărate.

Exemplu: În ultimii ani, escrocheriile privind investițiile în criptomonede au devenit din ce în ce mai răspândite. Escrocii pot promova oferte inițiale de monede (ICO) false sau oportunități de investiții în criptomonede false, promițând randamente ridicate cu riscuri minime. Aceste escrocherii sunt concepute pentru a păcăli investitorii să își trimită banii escrocilor, ceea ce duce la pierderi financiare pentru victime.

Caracteristici ale fiecărui tip de înșelătorie și semnale de alarmă la care trebuie să fii atent

1. Emailuri de phishing:

Caracteristici:

1. E-mailurile de phishing par adesea să provină de la organizații legitime, cum ar fi bănci, platforme de social media sau agenții guvernamentale.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

2. De obicei, acestea conțin mesaje urgente sau alarmante care solicită destinatarilor să ia măsuri imediate, cum ar fi să dea clic pe un link sau să furnizeze informații sensibile.

3. E-mailurile de phishing pot include logo-uri, mărci sau adrese de e-mail false care imită surse legitime pentru a înșela destinatarii.

Semnale de alarmă la care ar trebui să fii atent:

1. **Salutări generice:** E-mailurile de phishing folosesc adesea saluturi generice precum „Stimate client" în loc să se adreseze destinatarilor pe nume.

2. **Solicitări urgente**: E-mailurile de phishing pot conține solicitări urgente de informații personale, de verificare a contului sau de acțiune imediată pentru a evita consecințele.

3. **Link-uri suspecte**: Feriți-vă de link-urile din e-mailuri care vă direcționează către site-uri necunoscute sau URL-uri care nu corespund domeniului expeditorului.

4. **Gramatică și ortografie proaste**: E-mailurile de phishing conțin adesea greșeli de ortografie și gramatică, formatări neobișnuite sau limbaj ciudat care pot indica faptul că nu provin dintr-o sursă legitimă.

5. **Solicitări de informații personale**: De obicei, organizațiile legitime nu solicită prin e-mail informații sensibile precum parole, numere de asigurări sociale sau detalii despre conturi.

2. Scheme Ponzi:

Caracteristici:

1. Schemele Ponzi promit randamente ridicate ale investițiilor cu un risc minim.

2. Ele se bazează pe un aflux continuu de noi investitori pentru a plăti randamentele investitorilor existenți, în loc să genereze profituri legitime din investiții.

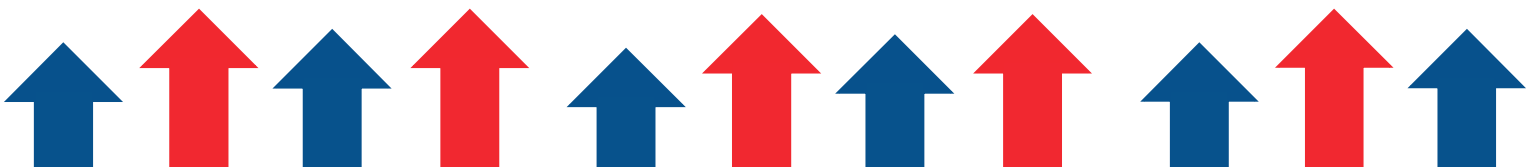
3. Schemele Ponzi utilizează adesea strategii de investiții complexe sau jargon financiar pentru a deruta investitorii și a crea iluzia legitimității.

Semnale de alarmă la care ar trebui să fii atent:

1. **Randamente nerealiste:** Fiți precauți cu privire la oportunitățile de investiții care promit în mod constant randamente ridicate cu riscuri mici sau inexistente.

2. **Lipsa de transparență:** Schemele Ponzi sunt adesea lipsite de transparență cu privire la modul în care sunt utilizate sau investite fondurile investitorilor.

3. **Presiunea de a investi:** Escrocii pot recurge la tactici de vânzare sub presiune pentru a convinge persoanele să investească rapid, fără a acorda timp suficient pentru diligență sau cercetare.



4. **Lipsa înregistrării sau a reglementării:** Oportunitățile de investiții legitime sunt de obicei înregistrate la autoritățile de reglementare și supuse supravegherii. Schemele Ponzi pot să nu fie înregistrate sau reglementate corespunzător.

3. Escrocherii privind investițiile:

Caracteristici:

1. Escrocheriile privind investițiile pot implica oferte sau oportunități frauduloase legate de acțiuni, proprietăți imobiliare, criptomonede sau alte produse financiare.

2. Escrocii pot folosi informații false sau înșelătoare pentru a convinge persoanele să investească bani.

3. Escrocheriile privind investițiile promit adesea randamente ridicate cu un efort sau un risc minim, profitând de dorința persoanelor de a obține profituri rapide.

Semnale de alarmă la care ar trebui să fii atent:

1. **Oferte nesolicitate:** Fiți atenți la ofertele de investiții nesolicitate primite prin e-mail, apeluri telefonice, social media sau reclame online.

2. **Lipsa documentației:** Oportunitățile de investiții legitime oferă de obicei documente sau materiale de informare care prezintă detaliile, riscurile și condițiile investiției. Feriți-vă de oportunitățile cărora le lipsește documentația sau transparența corespunzătoare.

3. **Presiunea de a acționa rapid:** Escrocii pot face presiuni asupra persoanelor pentru a lua rapid decizii de investiții, fără a acorda timpul necesar pentru o diligență adecvată sau pentru cercetare.

4. **Randamente garantate:** Fiți sceptici cu privire la oportunitățile de investiții care garantează randamente ridicate sau promit un risc minim. Toate investițiile prezintă un anumit grad de risc, iar oportunitățile de investiții legitime nu garantează profituri.

Activitate: Analiza e-mailurilor de phishing și identificarea elementelor cheie care indică faptul că acestea sunt frauduloase

Obiectivul acestei activități este de a educa participanții cu privire la elementele cheie ale e-mailurilor de phishing și cum să le identifice ca fiind frauduloase. Participanții vor analiza e-mailuri de phishing din viața reală și vor identifica semnalele de alarmă care indică faptul că acestea sunt înșelătorii.

Materiale necesare:

1. Imprimări sau copii digitale ale unor e-mailuri de phishing reale (asigurați-vă că aceste e-mailuri nu conțin linkuri sau atașamente malițioase)

2. Tablă sau flipchart

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

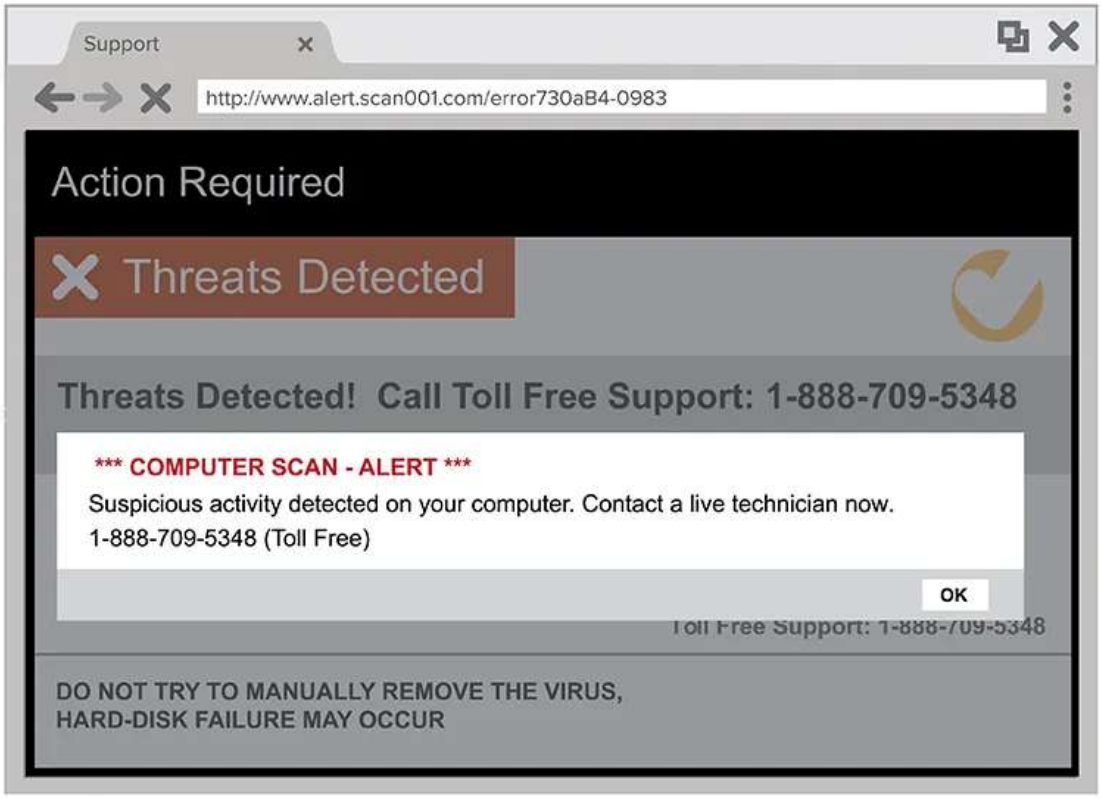
3. Materiale de scris

Exemple:

1. Emailuri de phishing cu suport tehnic

Folosind tactici înfricoşătoare în e-mailuri şi pop-up-uri, escrocii păcălesc victimele să creadă că au nevoie de asistență tehnică. Escrocii se pot da drept Microsoft - cel mai fraudat brand în 2023 [*] - sau Geek Squad de la Best Buy pentru a vă convinge că există o problemă cu dispozitivul dumneavoastră.

Cum funcționează escrocheriile de asistență tehnică:



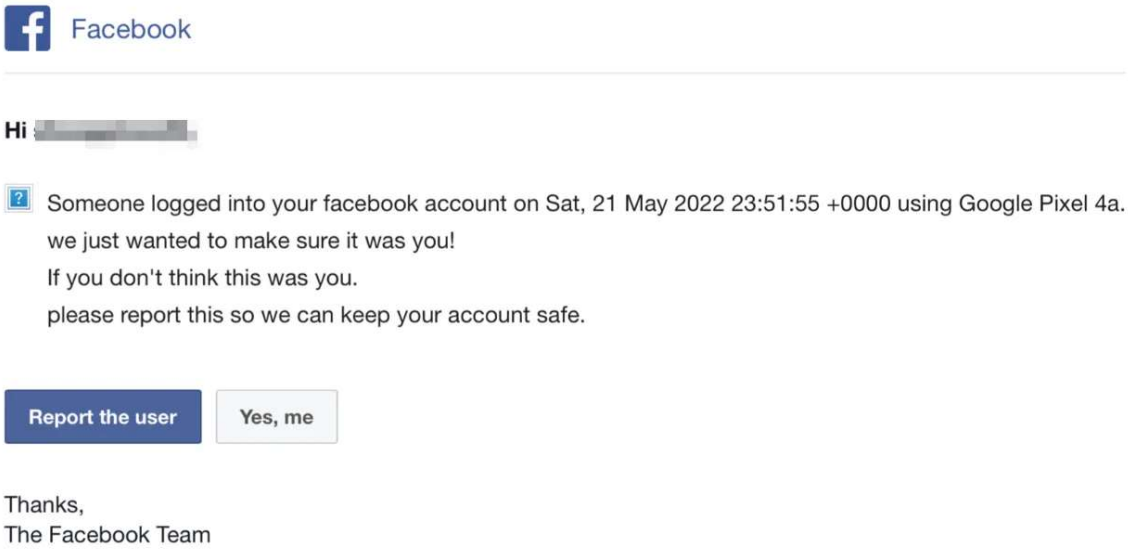
- Escrocii folosesc un limbaj foarte tehnic sau vag în materie de securitate cibernetică pentru a vă speria, deruta și dezarma.
- Aceștia vă pot factura pentru reparații false ale dispozitivului sau ale software-ului sau vă pot vinde actualizări sau garanții inutile.
- S-ar putea să vă îndemne să faceți clic pe atașamente malițioase sau să vizitați un site web pentru a vă furniza informațiile.

- Ar putea solicita acces de la distanță la computerul dvs. pentru a remedia presupusele probleme, permițându-le să instaleze programe malware sau ransomware.

E-mailuri de phishing din rețelele sociale

În această înșelătorie, e-mailul de phishing provine de la o presupusă echipă de asistență pentru social media, cum ar fi Instagram sau LinkedIn. Mesajul imită un avertisment tipic sau o notificare de cont pentru a părea autentic și a vă atrage atenția.

E-mail fals de alertă de conectare care imită Facebook, cu un CTA pentru „Raportați utilizatorul".



Exemplu de înșelătorie prin phishing pe rețelele sociale. Sursa: Reddit.

Cum funcționează înșelăciunile de tip phishing în rețelele sociale:

- Acest e-mail înșelător conține un link de phishing pentru verificarea sau autentificarea în contul dvs.
- Dacă faceți clic pe link, puteți descărca programe malware sau spyware sau puteți accesa o pagină de autentificare falsificată.
- Odată ce au informațiile despre contul dvs., escrocii se pot conecta și vă pot bloca accesul sau pot folosi datele de conectare în altă parte dacă v-ați reutilizat parola.

Instrucțiuni:

Introducere (5 minute):

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

1. Urați bun venit participanților la activitate și explicați scopul: analizarea e-mailurilor de phishing și identificarea elementelor-cheie care indică faptul că acestea sunt frauduloase.

2. Oferiți o prezentare generală a e-mailurilor de phishing și a importanței de a le putea recunoaște pentru a vă proteja împotriva amenințărilor cibernetice.

Prezentarea elementelor-cheie ale e-mailurilor de phishing (10 minute):

1. Realizați o scurtă prezentare generală a elementelor-cheie ale e-mailurilor de phishing, inclusiv caracteristicile comune și semnalele de alarmă.
2. Discutați elemente precum salutul generic, solicitările urgente, linkurile sau atașamentele suspecte, gramatica și ortografia greșite și solicitările de informații personale.

Analiza e-mailurilor de phishing (30 de minute):

1. Împărțiți participanții în grupuri mici.
2. Distribuiți fișe sau afișați copii digitale ale unor e-mailuri de phishing reale pentru ca fiecare grup să le analizeze.
3. Instruiți participanții să examineze cu atenție e-mailurile de phishing și să identifice elementele-cheie care indică faptul că acestea sunt frauduloase.
4. Încurajați participanții să discute constatările lor în cadrul grupurilor lor și să noteze semnalele de alarmă pe care le identifică.

Discuții în grup (15 minute):

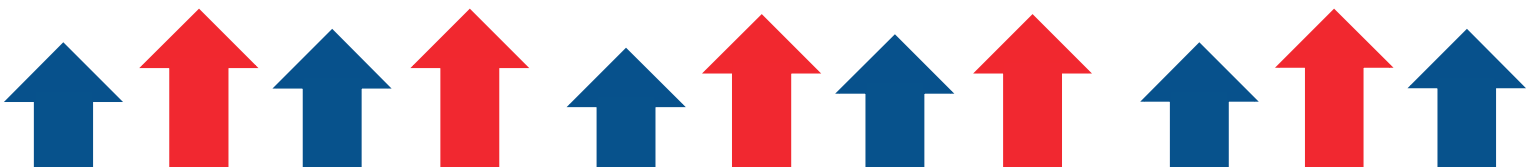
1. Reîntruniți din nou întregul grup și invitați fiecare grup să își împărtășească observațiile și constatările rezultate în urma analizării e-mailurilor de phishing.
2. Facilitați o discuție privind semnalele de alarmă comune și elementele-cheie ale e-mailurilor de phishing identificate de participanți.
3. Utilizați o tablă sau un flipchart pentru a documenta semnalele de alarmă și elementele-cheie identificate de participanți.

Reflecție și concluzii (10 minute):

1. Conduceți o sesiune de reflecție în care participanții își împărtășesc gândurile și ideile dobândite în urma analizării e-mailurilor de phishing.
2. Discutați strategiile de protecție împotriva atacurilor de phishing, cum ar fi verificarea adreselor de e-mail ale expeditorilor, evitarea apăsării pe link-uri sau atașamente suspecte și raportarea tentativelor de phishing către autoritățile competente.
3. Rezumați principalele concluzii și subliniați importanța vigilenței și a scepticismului atunci când aveți de-a face cu e-mailuri nesolicitate.

Concluzie:

1. Mulțumiți participanților pentru participarea lor la activitate și pentru contribuțiile lor la discuție.
2. Încurajați participanții să aplice cunoștințele și competențele dobândite pentru a identifica și a se proteja împotriva e-mailurilor de phishing în viața personală și profesională.



Importanța conștientizării securității cibernetice

Conștientizarea securității cibernetice este extrem de importantă pentru a te proteja de diverse amenințări online. Înțelegerea strategiilor utilizate de infractorii cibernetici pentru a înșela persoanele, cum ar fi tentativele de phishing, este esențială pentru menținerea siguranței și securității digitale. Recunoscând tacticile comune de phishing și distingându-le de e-mailurile legitime, indivizii pot reduce riscurile de a deveni victime ale atacurilor cibernetice.

Strategii de recunoaștere a tentativelor de phishing și de diferențiere a acestora de e-mailurile legitime

Tentativele de phishing au adesea ca scop înșelarea destinatarilor pentru ca aceștia să divulge informații sensibile sau să dea clic pe linkuri malițioase. Prin utilizarea următoarelor strategii, indivizii își pot spori capacitatea de a identifica și contracara tentativele de phishing:

Verificați adresa de e-mail a expeditorului: Verificați cu atenție adresa de e-mail a expeditorului pentru a vă asigura că aceasta corespunde domeniului oficial al organizației sau persoanei care pretinde că a trimis e-mailul. Fiți atenți la adresele de e-mail care utilizează nume de domeniu greșit ortografiate sau suspecte.

Verificați dacă există saluturi generice: E-mailurile de phishing folosesc adesea saluturi generice precum „Stimate client" sau „Stimate utilizator" în loc să se adreseze destinatarilor pe nume. E-mailurile legitime de la organizații de renume se adresează de obicei destinatarilor pe nume.

Căutați solicitări urgente sau amenințări: E-mailurile de phishing conțin adesea solicitări urgente sau amenințări menite să creeze un sentiment de urgență și să exercite presiuni asupra destinatarilor pentru ca aceștia să ia măsuri imediate. Fiți atenți la e-mailurile care amenință cu consecințe dacă nu răspundeți rapid sau nu furnizați informații personale.

Examinați link-urile și URL-urile: Treceți cursorul mouse-ului peste hyperlink-urile din e-mailuri (fără a da clic) pentru a previzualiza URL-ul de destinație. Verificați dacă URL-ul corespunde site-ului oficial al organizației de la care se pretinde că provine. Fiți atenți la URL-urile scurtate sau la URL-urile care redirecționează către site-uri necunoscute sau suspecte.

Evitați să faceți clic pe atașamente: Fiți precauți cu privire la atașamentele e-mailurilor, mai ales dacă acestea provin din surse necunoscute sau neașteptate. E-mailurile de phishing pot conține atașamente malițioase care pot instala programe malware pe dispozitivul dvs. sau vă pot compromite securitatea.

Verificați solicitările de informații personale: Fiți sceptici cu privire la e-mailurile care solicită informații sensibile precum parole, numere de asigurări sociale, detalii ale cardurilor de credit sau acreditări de cont. Organizațiile legitime nu solicită de obicei informații sensibile prin e-mail.

Verificați dacă există greșeli de ortografie și gramatică: E-mailurile de phishing conțin adesea greșeli de ortografie și gramatică, o structură neobișnuită a frazei sau un

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

limbaj ciudat care pot indica faptul că nu provin dintr-o sursă legitimă. Feriți-vă de e-mailurile cu un limbaj de proastă calitate.

Fiți precaut în cazul solicitărilor sau ofertelor neobișnuite: Fiți suspicioși cu privire la e-mailurile care oferă recompense neașteptate, premii sau oferte care par prea bune pentru a fi adevărate. De asemenea, e-mailurile de phishing pot solicita destinatarilor să participe la sondaje, concursuri sau oferte care necesită informații personale sau tranzacții financiare.

Aveți încredere în instinctele dumneavoastră și fiți sceptic: Dacă un e-mail vi se pare ciudat sau suspect, aveți încredere în instinctele dumneavoastră și fiți prudent. Este mai bine să fiți sceptic și să verificați legitimitatea unui e-mail înainte de a lua orice măsură.

Utilizați software de securitate și filtre de e-mail: Instalați un software antivirus de încredere și filtre de e-mail pentru a ajuta la detectarea și blocarea tentativelor de phishing. Aceste instrumente pot ajuta la identificarea e-mailurilor suspecte și la protejarea împotriva conținutului malițios.

Sfaturi pentru a evita să faceți clic pe linkuri suspecte sau să descărcați atașamente din surse necunoscute

Verificați identitatea expeditorului: Înainte de a da clic pe orice link sau de a descărca atașamente, verificați identitatea expeditorului. Asigurați-vă că e-mailul sau mesajul provine de la o sursă legitimă și nu de la un expeditor necunoscut sau suspect.

Verificați adresa de e-mail: Examinați cu atenție adresa de e-mail a expeditorului. Fiți atenți la adresele de e-mail care utilizează nume de domenii greșit scrise sau suspecte, deoarece acestea pot indica tentative de phishing.

Treceți peste linkuri pentru a previzualiza URL-urile: Treceți cursorul mouse-ului peste hyperlink-urile din e-mailuri sau mesaje (fără a da clic) pentru a previzualiza URL-ul de destinație. Verificați dacă URL-ul corespunde cu site-ul oficial al organizației de la care se pretinde că provine. Fiți atenți la URL-urile scurtate sau la URL-urile care redirecționează către site-uri necunoscute sau suspecte.

Evitați e-mailurile sau mesajele nesolicitate: Feriți-vă de e-mailurile sau mesajele nesolicitate de la expeditori necunoscuți, mai ales dacă acestea conțin linkuri sau atașamente. Ștergeți sau ignorați astfel de e-mailuri pentru a evita potențialele riscuri de securitate.

Feriți-vă de solicitările urgente sau suspecte: Fiți precauți cu e-mailurile sau mesajele care conțin solicitări urgente sau amenințări, cum ar fi avertismente privind suspendarea contului, acțiuni în justiție sau consecințe financiare. Escrocii

folosesc adesea urgența pentru a exercita presiuni asupra destinatarilor și a-i determina să dea clic pe linkuri malițioase sau să descarce fișiere atașate.

Verificați conținutul cu expeditorul: Dacă primiți un e-mail sau un mesaj cu linkuri sau atașamente de la un expeditor cunoscut, dar conținutul pare suspect, verificați legitimitatea conținutului împreună cu expeditorul printr-un canal de comunicare separat (de exemplu, apel telefonic sau mesaj text).

Utilizați software antivirus și filtre de e-mail: Instalați software antivirus și filtre de e-mail de încredere pe dispozitivele dvs. pentru a ajuta la detectarea și blocarea conținutului rău intenționat, inclusiv a link-urilor și atașamentelor suspecte. Mențineți software-ul antivirus și filtrele de e-mail actualizate pentru o eficiență maximă.

Informează-te cu privire la tacticile comune de phishing: Rămâneți informați cu privire la tacticile și strategiile comune de phishing utilizate de infractorii cibernetici pentru a păcăli persoanele să dea clic pe link-uri malițioase sau să descarce atașamente. Informează-te pe tine și membrii echipei tale cu privire la cele mai recente tendințe și tehnici de phishing.

Fiți precauți pe rețelele sociale și în aplicațiile de mesagerie: Fiți precauți atunci când faceți clic pe linkuri sau descărcați atașamente de pe platformele de social media, aplicațiile de mesagerie sau alte platforme online. Escrocii folosesc adesea aceste platforme pentru a distribui linkuri de phishing și programe malware.

Raportați activitatea suspectă: Dacă primiți un e-mail sau un mesaj suspect care conține linkuri sau atașamente, raportați-l departamentului IT al organizației dumneavoastră sau autorităților competente. Raportarea activității suspecte poate ajuta la protejarea altor persoane de a deveni victime ale înșelătoriilor de tip phishing.

Importanța păstrării confidențialității informațiilor personale pe platformele social media

Păstrarea confidențialității informațiilor personale pe platformele social media este esențială din mai multe motive:

Protecție împotriva furtului de identitate: Informațiile personale partajate pe social media, cum ar fi numele complet, data nașterii, adresa și datele de contact, pot fi exploatate de hoții de identitate pentru a vă fura identitatea. Cu aceste informații, infractorii pot deschide conturi frauduloase, pot solicita carduri de credit sau pot comite alte forme de fraudă financiară în numele dumneavoastră.

Prevenirea hărțuirii și hărțuirii cibernetice: Împărtășirea prea multor informații personale pe rețelele de socializare vă poate face vulnerabil la urmărirea și hărțuirea

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

cibernetică. Persoanele rău intenționate vă pot folosi informațiile personale pentru a vă localiza, pentru a vă monitoriza activitățile sau pentru a vă hărțui online sau în viața reală.

Evitarea înșelătoriilor online și a atacurilor de phishing: Infractorii cibernetici folosesc adesea informațiile personale partajate pe rețelele de socializare pentru a lansa atacuri de phishing sau escrocherii direcționate. Aceștia vă pot folosi datele personale pentru a crea mesaje sau e-mailuri convingătoare, păcălindu-vă să dezvăluiți informații sensibile sau să cădeți în capcana unor scheme frauduloase.

Protecția reputației și a vieții private: Schimbul de informații sensibile sau nepotrivite pe rețelele de socializare vă poate afecta reputația și viața privată. Angajatorii, colegii, membrii familiei și alte persoane pot avea acces la profilurile dvs. de social media, iar conținutul inadecvat ar putea avea consecințe negative asupra vieții dvs. profesionale și personale.

Prevenirea atacurilor de inginerie socială: Platformele de social media sunt frecvent utilizate de infractorii cibernetici pentru atacuri de inginerie socială, prin care aceștia manipulează utilizatorii pentru a dezvălui informații confidențiale sau pentru a efectua acțiuni care compromit securitatea. Limitând cantitatea de informații personale pe care le partajați pe rețelele de socializare, reduceți riscul de a deveni victime ale tacticilor de inginerie socială.

Securitate online sporită: Păstrarea confidențialității informațiilor personale pe platformele social media contribuie la îmbunătățirea securității dvs. online globale. Aceasta reduce probabilitatea accesului neautorizat la conturile dvs., minimizează riscul de furt de identitate și fraudă și vă protejează confidențialitatea și amprenta digitală.

Activitate: Sesiune interactivă privind identificarea și evitarea link-urilor și atașamentelor suspecte în scenarii de e-mail simulate.

Obiectivul acestei activități este de a instrui participanții cu privire la identificarea și evitarea link-urilor și atașamentelor suspecte din e-mailuri prin intermediul unor scenarii simulate. Participanții se vor angaja în exerciții interactive pentru a analiza conținutul e-mailurilor, pentru a identifica semnalele de alarmă și pentru a lua decizii în cunoștință de cauză cu privire la apăsarea pe linkuri sau descărcarea atașamentelor.

Materiale necesare:

1. Scenarii simulate de e-mail
2. Tablă sau flipchart
3. Materiale de scris
4. Calculatoare sau dispozitive mobile cu acces la internet (opțional)

Instrucțiuni:

Introducere (5 minute):

1. Urați bun venit participanților la sesiunea interactivă privind identificarea și evitarea linkurilor și atașamentelor suspecte din e-mailuri.
2. Explicați scopul activității: sporirea gradului de conștientizare și a competențelor participanților în ceea ce privește recunoașterea tentativelor de phishing și protejarea împotriva amenințărilor cibernetice.

Prezentare privind semnalele de alarmă și cele mai bune practici (10 minute):

1. Faceți o scurtă prezentare a semnalelor de alarmă și a celor mai bune practici pentru identificarea linkurilor și atașamentelor suspecte din e-mailuri.
2. Discutați caracteristicile comune ale e-mailurilor de phishing, cum ar fi salutul generic, solicitările urgente, URL-urile suspecte și solicitările de informații personale.
3. Analizați cele mai bune practici pentru a evita să dați clic pe linkuri sau să descărcați atașamente din surse necunoscute sau suspecte.

Scenarii simulate de e-mail (30 de minute):

1. Împărțiți participanții în grupuri mici.
2. Distribuiți scenarii simulate de e-mail fiecărui grup. Fiecare scenariu ar trebui să includă un e-mail cu un link sau un atașament care poate fi suspect.

De exemplu:

E-mail legitim de la o bancă:

```
Subiect: Extrasul dvs. lunar este gata
De la: noreply@yourbank.com

Stimate client,

Extrasul dvs. lunar este acum disponibil în contul dvs. bancar online.
Vă rugăm să vă conectați la contul dvs. pentru a vizualiza extrasul.

Toate cele bune,
Banca dvs.
```

Email de phishing care se prezintă drept o bancă:

```
Subiect: Urgent: Cont suspendat
De la: support@yourbank-security.com

Stimate client,
```

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Am detectat o activitate neobișnuită în contul dumneavoastră. Contul dvs. a fost suspendat. Vă rugăm să faceți clic pe link-ul de mai jos pentru a vă verifica identitatea și a vă restabili contul.

Faceți clic aici pentru a vă restabili contul.

Toate cele bune,
Banca dvs.

În acest caz, e-mailul folosește un limbaj urgent pentru a speria destinatarul și a-l determina să facă clic pe link. Adresa de e-mail a expeditorului este, de asemenea, suspectă și nu este e-mailul oficial al băncii.

Email legitim de la un coleg:

Subiect: Note de întâlnire
De la: colleague@yourcompany.com

Bună ziua,

Vă rugăm să găsiți notele de ședință atașate.

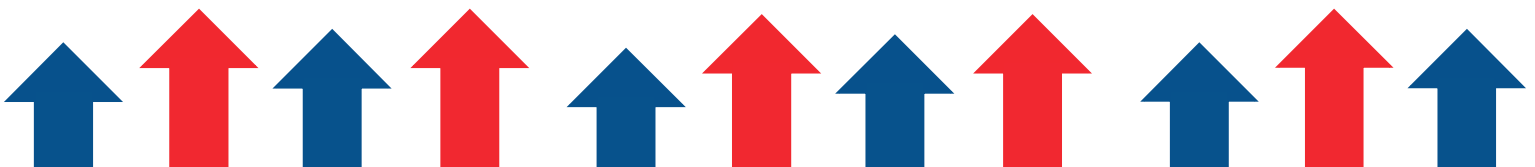
Toate cele bune
Coleg

Email de phishing care se dă drept un coleg:

Subiect: Urgent: Factură scadentă
De la: colleage@yourcompany.com

Bună,

Factura pentru furnizorul nostru este scadentă. Vă rugăm să consultați factura atașată și să efectuați plata imediat.



Toate cele bune,
Coleg

În acest caz, e-mailul folosește un limbaj urgent și solicită destinatarului să întreprindă o acțiune care nu face parte din activitatea sa obișnuită. Adresa de e-mail a expeditorului conține, de asemenea, o greșeală de tipar, care poate fi un semn al unei tentative de phishing.

1. Instruiți participanții să analizeze cu atenție conținutul e-mailului, să identifice semnalele de alarmă și să decidă dacă să facă clic pe link sau să descarce atașamentul.
2. Încurajați participanții să discute observațiile lor și procesul de luare a deciziilor în cadrul grupurilor lor.

Discuții în grup (15 minute):

1. Reuniți-vă din nou în grup și invitați fiecare grup să își împărtășească analiza scenariilor de e-mail simulate.
2. Facilitați o discuție cu privire la semnalele de alarmă identificate de participanți și la raționamentul din spatele deciziilor lor de a da clic pe linkuri sau de a descărca atașamente.
3. Folosiți o tablă albă sau un flipchart pentru a consemna principalele concluzii și perspective ale discuției.

Reflecție și concluzii (10 minute):

1. Conduceți o sesiune de reflecție în cadrul căreia participanții își împărtășesc gândurile și perspectivele obținute în urma sesiunii interactive.
2. Discutați strategiile de evitare a tentativelor de phishing și de protecție împotriva amenințărilor cibernetice în comunicațiile prin e-mail de zi cu zi.
3. Rezumați principalele concluzii și subliniați importanța vigilenței și a scepticismului atunci când aveți de-a face cu linkuri și atașamente suspecte în e-mailuri.

Concluzii:

1. Mulțumiți participanților pentru participarea lor activă la sesiunea interactivă.
2. Încurajați participanții să aplice cunoștințele și abilitățile dobândite pentru a identifica și evita link-urile și atașamentele suspecte în comunicările lor prin e-mail.
3. Oferiți resurse suplimentare și sprijin participanților care doresc să afle mai multe despre cele mai bune practici de securitate cibernetică.

Integrarea studiilor de caz

Exemple reale de persoane care cad victime înșelăciunilor financiare.

Schema Ponzi a lui Bernie Madoff:

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Una dintre cele mai cunoscute escrocherii financiare din istorie a fost orchestrată de Bernie Madoff. Madoff a condus o schemă Ponzi timp de mai multe decenii, promițând randamente ridicate investitorilor. El a atras mii de investitori, inclusiv persoane fizice, organizații caritabile și investitori instituționali, oferind randamente constante și profitabile. Cu toate acestea, în loc să investească fondurile așa cum a promis, Madoff a folosit banii noilor investitori pentru a plăti randamentele investitorilor existenți. Schema s-a prăbușit în cele din urmă în 2008, provocând pierderi de miliarde de dolari pentru investitori. (Hayes, 2023)

Frauda cu avans:

Frauda cu onorariu anticipat, cunoscută și sub denumirea de **înșelătoria 419 sau înșelătoria cu prințul nigerian**, este o înșelătorie financiară obișnuită care vizează persoanele prin e-mail sau alte canale de comunicare. În cadrul unei scheme de fraudă cu avans, escrocii promit o sumă mare de bani în schimbul unei plăți inițiale mici sau a unei taxe. Victimele sunt ademenite cu promisiuni de moștenire, câștiguri la loterie sau oportunități de afaceri, dar sfârșesc prin a pierde bani în favoarea escrocilor. (Grigutytė & Grigutytė, 2023)

Analiza strategiilor care ar fi putut fi utilizate pentru a evita să cadă pradă acestor escrocherii

Schema Ponzi a lui Bernie Madoff:

Due Diligence: Investitorii ar fi putut să efectueze un due diligence amănunțit înainte de a-și investi banii în Bernie Madoff. Aceasta ar fi presupus verificarea legitimității firmei de investiții, analizarea situațiilor financiare și solicitarea de audituri independente de la terți.

Să pună la îndoială randamentele nerealiste: Investitorii ar fi trebuit să pună la îndoială randamentele nerealiste și constante promise de firma de investiții a lui Madoff. Randamentele constant ridicate cu un risc minim ar fi trebuit să ridice semnale de alarmă și să determine investigații suplimentare.

Escrocherii cu e-mail de tip phishing:

Verificați identitatea expeditorului: Verificați întotdeauna identitatea expeditorului înainte de a răspunde la e-mailurile care solicită informații personale sau financiare. Organizațiile legitime nu vor solicita informații sensibile prin e-mail.

Scrutați URL-urile și link-urile: Treceți cu privirea peste hyperlink-urile din e-mailuri pentru a verifica URL-ul de destinație înainte de a da clic. Fiți atenți la URL-urile care nu corespund site-ului oficial al organizației sau care conțin domenii suspecte.

Escrocherii privind investițiile în criptomonede:

Cercetați oportunitățile de investiții: Efectuați cercetări amănunțite înainte de a investi în criptomonede sau de a participa la oferte inițiale de monede (ICO). Verificați legitimitatea proiectului, a membrilor echipei și a documentelor tehnice pentru a evita investițiile în scheme frauduloase.

Evitați randamentele nerealiste: Fiți sceptici cu privire la oportunitățile de investiții care promit în mod constant randamente ridicate cu un risc minim. Investițiile în criptomonede, ca orice altă investiție, comportă riscuri inerente, iar randamentele garantate ar trebui privite cu suspiciune.

Frauda comisioanelor în avans:

Fiți sceptic cu privire la ofertele nesolicitate: Feriți-vă de e-mailurile sau mesajele nesolicitate care promit sume mari de bani în schimbul unei plăți inițiale mici sau a unei taxe. Fiți prudent și puneți la îndoială legitimitatea unor astfel de oferte.

Cercetați și verificați: Cercetați oferta și verificați identitatea expeditorului sau a organizației înainte de a răspunde. Oportunitățile de afaceri legitime nu necesită de obicei plăți sau taxe în avans.

Frauda privind investițiile:

Verificați oportunitățile de investiții: Efectuați cercetări amănunțite cu privire la oportunitățile de investiții și verificați legitimitatea firmei de investiții sau a consilierului. Verificați înregistrările de reglementare, licențele și istoricul disciplinar pentru a vă asigura credibilitatea.

Evitați tacticile de vânzare cu presiune ridicată: Fiți atenți la oportunitățile de investiții care utilizează tactici de vânzare cu presiune ridicată sau care vă forțează să luați decizii rapide. Oportunitățile de investiții legitime oferă timp pentru o analiză și o analiză corespunzătoare.

Activitate: Prezentare în grup privind analiza cazurilor reale de escrocherie financiară și propunerea de măsuri preventive.

Obiectivul acestei activități este de a aprofunda înțelegerea de către participanți a cazurilor reale de escrocherie financiară, de a analiza factorii care au contribuit la aceste escrocherii și de a propune măsuri preventive pentru a se proteja împotriva unor escrocherii similare în viitor.

Materiale necesare:

1. Lista cazurilor reale de escrocherie financiară (menționate mai sus)
2. Materiale de prezentare (diapozitive, materiale pentru distribuire, etc.)
3. Materiale de scris
4. Proiector sau ecran (dacă se folosesc diapozitive)

Instrucțiuni:

Introducere (10 minute):

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Urați bun venit participanților la prezentarea de grup privind analiza cazurilor reale de escrocherie financiară și propunerea de măsuri preventive.

Explicați scopul activității: analizarea cazurilor reale de escrocherie financiară, identificarea modelelor și vulnerabilităților comune și propunerea de măsuri preventive pentru a reduce riscul unor escrocherii similare.

Selectarea cazurilor de escrocherie (10 minute):

1. Împărțiți participanții în grupuri mici.
2. Furnizați fiecărui grup o listă de cazuri reale de escrocherii financiare din care să aleagă. Aceste cazuri ar trebui să acopere o varietate de escrocherii financiare, cum ar fi schemele Ponzi, frauda în investiții, escrocherii prin phishing etc.
3. Cereți fiecărui grup să selecteze un caz de escrocherie pe care să îl analizeze și să îl prezinte.

Cercetare și analiză (30 de minute):

1. Alocați timp fiecărui grup pentru a cerceta și analiza cazul de înșelătorie selectat.
2. Încurajați grupurile să examineze detaliile cazului de escrocherie, inclusiv autorii, victimele, metodele utilizate, semnalele de alarmă, impactul și consecințele.
3. Îndemnați grupurile să identifice modele comune, vulnerabilități și factori care au contribuit la succesul escrocheriei.

Măsuri preventive (30 de minute):

1. După analizarea cazului de înșelătorie, instruiți fiecare grup să facă un brainstorming și să propună măsuri preventive pentru a se proteja împotriva unor înșelătorii similare în viitor.
2. Încurajați grupurile să ia în considerare o serie de măsuri preventive, inclusiv reforme de reglementare, educația consumatorilor, campanii de sensibilizare, soluții tehnologice și măsuri de aplicare a legii.
3. Fiecare grup ar trebui să pregătească o listă de măsuri preventive și să le prioritizeze în funcție de eficacitatea și fezabilitatea lor.

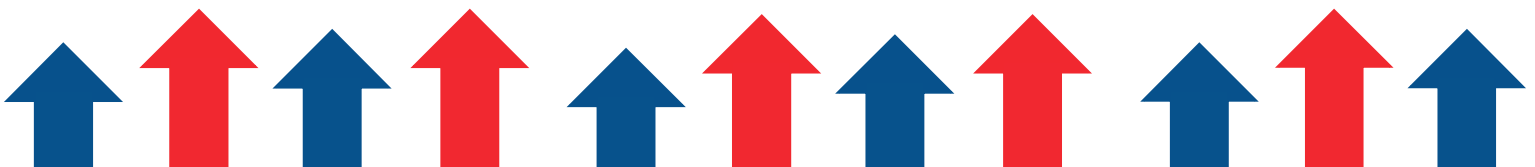
Prezentări de grup (40 de minute):

1. Alocați timp fiecărui grup pentru a-și prezenta analiza cazului de înșelătorie și pentru a propune măsuri preventive.
2. Încurajați grupurile să utilizeze materiale de prezentare (diapozitive, foi volante etc.) pentru a-și susține prezentările.
3. După fiecare prezentare, facilitați o scurtă sesiune de întrebări și răspunsuri pentru a permite celorlalți participanți să pună întrebări și să ofere feedback.

Discuții și reflecții (20 de minute):

1. Încheiați prezentările de grup cu o sesiune de discuții și reflecții.
2. Încurajați participanții să discute temele comune, perspectivele și lecțiile învățate din cazurile de înșelăciune și măsurile preventive propuse.
3. Facilitați o discuție privind importanța măsurilor proactive în prevenirea escrocheriilor financiare și protejarea consumatorilor și investitorilor.

Concluzie (10 minute):



1. Mulțumiți participanților pentru participare și contribuțiile lor la prezentările de grup.
2. Rezumați principalele concluzii și idei desprinse din activitate.
3. Subliniați importanța vigilenței continue, a educației consumatorilor și a eforturilor de reglementare în combaterea escrocheriilor financiare.

Practicarea

Activitate de învățare autodirijată

Sugerați participanților să afle mai multe despre subiecte și sugerați câteva lecturi suplimentare, cum ar fi:

Furtul de identitate, tranzacțiile frauduloase și amenințările la adresa securității cibernetice:

1. Identity Theft Resource Centre (https://www.idtheftcenter.org/) - Oferă informații, resurse și asistență pentru victimele furtului de identitate.
2. Federal Trade Commission (FTC) Identity Theft website (https://www.identitytheft.gov/) - Oferă îndrumări pas cu pas privind prevenirea, detectarea și recuperarea furtului de identitate.

Importanța măsurilor de securitate și Măsuri de securitate de bază:

1. StaySafeOnline.org (https://staysafeonline.org/) - Oferă resurse și sfaturi pentru siguranța online și conștientizarea securității cibernetice.
2. Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/) - Oferă resurse, sfaturi și bune practici de securitate cibernetică pentru persoane și organizații.

Recunoașterea înșelătoriilor și conștientizarea securității cibernetice:

1. FBI Internet Crime Complaint Centre (IC3) (https://www.ic3.gov/) - Permite utilizatorilor să raporteze infracțiuni pe internet și oferă resurse pentru prevenirea criminalității informatice.
2. Better Business Bureau (BBB) Scam Alerts (https://www.bbb.org/scamtracker) - Oferă alerte privind înșelăciunile, sfaturi și resurse pentru consumatori și întreprinderi.

Studii de caz privind escrocherii reale și strategii de evitare:

1. Securities and Exchange Commission (SEC) (https://www.sec.gov/) - Oferă resurse și informații privind educația investitorilor, alertele și acțiunile de aplicare a legii.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

2. Consumer Financial Protection Bureau (CFPB) (https://www.consumerfinance.gov/) - Oferă resurse și instrumente pentru consumatori, inclusiv alerte privind fraudele și rapoarte privind escrocheriile financiare.

Test de evaluare

Test: Identificarea riscurilor comune de securitate și recunoașterea caracteristicilor înșelătoriilor

Instrucțiuni:

1. Citiți cu atenție fiecare întrebare și selectați cel mai bun răspuns.
2. Alegeți opțiunea care reprezintă cel mai bine răspunsul corect.
3. La sfârșitul testului, numărați-vă scorul pentru a vedea cât de bine v-ați descurcat.

Ce este furtul de identitate?

1. Un tip de malware care infectează computerele și fură informații personale.
2. Utilizarea neautorizată a informațiilor personale ale altcuiva pentru a comite fraude sau alte infracțiuni.
3. O înșelătorie financiară care implică scheme de investiții frauduloase.
4. O amenințare la adresa securității cibernetice care vizează conturile bancare online.

Care dintre următoarele este o caracteristică a e-mailurilor de phishing?

1. Salutări personalizate adresate destinatarului pe nume.
2. Solicitări de informații sensibile precum parole sau numere de carduri de credit.
3. Adrese de e-mail legitime ale expeditorului care corespund domeniului oficial al organizației.
4. Sigle și mărci oficiale ale organizațiilor de încredere.

Ce este o schemă Ponzi?

1. Un tip de atac de tip phishing care vizează persoane fizice prin e-mailuri frauduloase.
2. O înșelătorie de investiții care promite randamente ridicate investitorilor cu riscuri minime.
3. O amenințare la adresa securității cibernetice care exploatează vulnerabilitățile din software sau sisteme.
4. Un tip de malware conceput pentru a fura informații personale de pe computere.

Care este scopul autentificării cu doi factori?

1. Să securizeze conturile online prin solicitarea mai multor forme de verificare.
2. Pentru a preveni atacurile de phishing prin criptarea comunicațiilor prin e-mail.
3. Pentru a proteja împotriva furtului de identitate prin monitorizarea rapoartelor de credit.
4. Să detecteze și să elimine programele malware de pe dispozitivele infectate.

Care dintre următoarele este un semnal de alarmă pentru o potențială înșelătorie?

1. Solicitări urgente de informații personale sau acțiuni imediate.
2. E-mailuri personalizate care se adresează destinatarului pe nume.
3. Sigle și mărci oficiale de la organizații de încredere.
4. Solicitări de feedback sau sondaje din surse de încredere.

Care este importanța actualizărilor periodice de software și a întreținerii dispozitivelor?

1. Pentru a vă proteja împotriva atacurilor de phishing și a infecțiilor malware.
2. Pentru a securiza conturile online cu parole puternice.
3. Pentru a preveni furtul de identitate și frauda financiară.
4. Pentru a atenua vulnerabilitățile de securitate și a proteja împotriva amenințărilor informatice.

Care dintre următoarele NU este o caracteristică comună a oportunităților legitime de investiții?

1. Garantarea unor randamente ridicate cu un risc minim.
2. Înregistrare și supraveghere reglementară corespunzătoare.
3. Documentație transparentă care prezintă detaliile și riscurile investiției.
4. Presiunea de a lua decizii de investiții rapide, fără diligența necesară.

Care este semnificația păstrării confidențialității informațiilor personale pe platformele social media?

1. Pentru a se proteja împotriva furtului de identitate și a hărțuirii cibernetice.
2. Pentru a preveni atacurile de phishing și infecțiile cu programe malware.
3. Pentru a securiza conturile online cu autentificare cu doi factori.
4. Pentru a evita vulnerabilitățile software și problemele de întreținere a dispozitivelor.

Răspunsuri:

b) Utilizarea neautorizată a informațiilor personale ale altcuiva pentru a comite fraude sau alte infracțiuni.

b) Solicitări de informații sensibile precum parole sau numere de carduri de credit.

b) O înșelătorie de investiții care promite randamente ridicate investitorilor cu riscuri minime.

a) Pentru a securiza conturile online prin solicitarea mai multor forme de verificare.

a) Solicitări urgente de informații personale sau acțiuni imediate.

d) Pentru a atenua vulnerabilitățile de securitate și a proteja împotriva amenințărilor cibernetice.

a) Randamente ridicate garantate cu risc minim.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

a) Pentru a proteja împotriva furtului de identitate și a hărțuirii cibernetice.

Punctaj:

- **8 răspunsuri corecte:** Excelent! Aveți o înțelegere solidă a riscurilor comune de securitate și a caracteristicilor înșelătoriilor.
- **5-7 răspunsuri corecte:** Bună treabă! Aveți o bună înțelegere a conceptelor, dar ați putea beneficia de o revizuire suplimentară.
- **4 sau mai puține răspunsuri corecte:** Luați în considerare revizuirea materialului pentru a vă îmbunătăți înțelegerea riscurilor comune de securitate și a caracteristicilor înșelătoriilor.

CUM SĂ CUMPĂRAȚI ONLINE ÎN SIGURANȚĂ

Introducere în cumpărăturile online

Obiectivul principal al acestui subdomeniu este de a familiariza cursanții cu caracteristicile și avantajele cumpărăturilor online. Cumpărăturile online oferă o modalitate convenabilă de a face cumpărături din confortul propriei case. În cadrul acestui subdomeniu, participanții vor explora diverse aspecte ale site-urilor de cumpărături online și vor parcurge etapele achiziționării unui articol online - fără a finaliza tranzacția. Obiectivul este de a oferi o experiență practică pentru a înțelege procesul și caracteristicile efectuării unei achiziții online, fără a efectua tranzacția finală.

Răsfoirea magazinelor online

În acest subdomeniu, obiectivul este de a aprofunda înțelegerea de către cursanți a cumpărăturilor online prin accentuarea aspectului de navigare a magazinelor online

fără a fi necesară efectuarea unei achiziții. Accentul se pune pe explicarea faptului că cursanții pot explora magazinele online, pot vizualiza articole și pot naviga prin diferite categorii fără a se angaja să cumpere ceva. Acest lucru permite persoanelor să se obișnuiască cu aspectul și caracteristicile diferitelor magazine online, să înțeleagă modul în care sunt prezentate produsele și cum este structurat procesul de cumpărare. Prin simpla navigare, cursanții se pot familiariza cu interfața utilizatorului, cu funcționalitățile de căutare și cu experiența generală a cumpărăturilor online, fără presiunea de a face o achiziție. Această explorare practică este esențială pentru sporirea încrederii și înțelegerii lor în mediul de cumpărături online.

Activitatea 1 - Navighează pe un magazin online

Obiectivele acestei activități cuprind furnizarea unei experiențe practice pentru cursanți în vederea navigării pe o platformă de cumpărături online și înțelegerea etapelor esențiale implicate în efectuarea unei achiziții. Aceasta ar trebui inițiată prin instruirea cursanților să acceseze internetul și să viziteze un site web specific, cum ar fi Amazon. Explorând pagina de pornire și învățând să utilizeze caracteristicile sale, cum ar fi caseta de căutare, filele departamentului și navigarea prin categorii precum „Cadouri" și „Cărți", cursanții se vor familiariza cu aspectul și funcționalitățile site-ului.

Activitatea urmărește să ilustreze procesul de rafinare a căutărilor cu ajutorul opțiunilor de filtrare și de manevrare între pagini. În plus, accentul se pune pe clarificarea procedurii pas cu pas de achiziționare a unui articol online, de la găsirea articolului la adăugarea acestuia în coșul de cumpărături, la finalizarea comenzii, introducerea detaliilor de livrare și, în final, efectuarea plății. Această prezentare pas cu pas este menită să demistifice și să familiarizeze cursanții cu procesul secvențial al unei achiziții online, imitând pașii implicați într-o experiență fizică de cumpărături.

Pas cu pas

1. Rugați cursantul să deschidă Internetul.

2. Cereți-i cursantului să meargă la www.amazon.es (sau altă țară)

3. Explicați pagina de pornire Amazon:

- Caseta de căutare.

- File de departament

4.Explorați pagina de pornire.

5.Rugați cursantul să facă clic pe fila Cadouri și sub categoria Cadouri să aleagă Cărți

6.Explorați pagina de rezultate a cărții.

7.Explicați că puteți utiliza opțiunile de filtrare din stânga pentru a vă rafina căutarea.

8.Faceți clic pe butonul înapoi al browserului pentru a reveni la pagina de pornire.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Achiziționarea unui articol online

Obiectivul acestui subtematic este de a familiariza cursanții cu etapele esențiale ale procesului de achiziționare a unor articole prin intermediul cumpărăturilor online. Explicația începe prin asemănarea procesului de achiziție digitală cu cel al unui magazin fizic, împărțind pașii într-o secvență simplă. Inițial, cursanților li se prezintă pașii fundamentali care implică găsirea articolului dorit din magazinul online, adăugarea acestuia în coșul virtual de cumpărături, trecerea la casa de marcat, introducerea detaliilor de livrare necesare și finalizarea tranzacției prin efectuarea plății. Prin încadrarea procesului de cumpărare online în acest mod, se urmărește simplificarea și demistificarea etapelor, facilitând înțelegerea și parcurgerea de către cursanți a experienței de cumpărături online, similar cu rutina lor familiară de cumpărături în magazin. Această abordare structurată urmărește să consolideze încrederea și înțelegerea cursanților, permițându-le să se implice în mod eficient și sigur în tranzacțiile online.

Activitatea 2 - Cumpărați un e-book Kindle online

Scopul principal al acestei activități este de a-i ghida pe cursanți prin etapele unei achiziții online pe un site de cumpărături, subliniind factorii cruciali pentru o experiență de cumpărare online sigură și autentică. Cursanții ar trebui să fie direcționați către un site web desemnat, cum ar fi Amazon, unde pot explora pagina de pornire în timp ce evaluează în mod critic autenticitatea acesteia. Considerațiile importante includ verificarea afișării pe site a unei adrese poștale, a unui număr de telefon și a unei politici de returnare vizibile.

Procesul de achiziție pas cu pas este navigat și susținut de către formator, care explică fiecare fază, subliniind măsurile cheie de securitate, cum ar fi adresa web care începe cu „https", indicând o tranzacție sigură. Cursanților trebuie să li se reamintească faptul că nu fac de fapt o achiziție, dar dacă ar face-o, ar introduce detaliile de plată și ar primi o confirmare. În plus, activitatea cuprinde o explicație a opțiunilor de plată precum cardul de credit și PayPal. După exercițiu, cursanții ar trebui încurajați să utilizeze butonul „înapoi" al browserului pentru a reveni la pagina de pornire, cu avertismentul că astfel se șterg toate informațiile introduse pe site, consolidând importanța securității online și a protecției datelor. Acest exercițiu cuprinzător are ca scop educarea cursanților cu privire la identificarea semnelor unui site web autentic, înțelegerea procesului de plată securizată și accentuarea practicilor de navigare sigură în timpul cumpărăturilor online.

Pas cu pas

Explicați cursantului dvs. că va vizita un site de cumpărături și va parcurge pașii de achiziționare a unui articol online, dar nu va cumpăra nimic.

1.Cereți-i cursantului să meargă la www.amazon.es (sau altă țară)

2.Explorați pagina de pornire - **IMPORTANT**:

- Site-ul este autentic?

- Site-ul afișează o adresă poștală și un număr de telefon?

- Există o politică de returnare?

1. Cereți-i cursantului să urmeze pașii unei achiziții.
2. Explicați fiecare pas pe parcurs.
3. Când ajunge la pagina de plăți a site-ului, rugați-l să se uite la adresa web - aceasta ar trebui să înceapă cu https - **IMPORTANT** Verificați dacă adresa web din browser începe cu https (și nu cu http) - aceasta înseamnă că se utilizează un anumit tip de securitate atunci când se gestionează banii dumneavoastră.
4. Explicați cursantului dvs. că, dacă intenționează să achiziționeze produsul, va completa acum detaliile de plată și va primi confirmarea achiziției. (nu o faceți!)
5. Explicați opțiunile de plată.

Card de credit ; PayPal

1. Când exercițiul este finalizat, rugați cursantul să folosească butonul înapoi al browserului pentru a reveni la pagina de pornire. **Notă:** Utilizarea butonului înapoi al browserului va șterge orice informație furnizată pe site.

Escrocherii romantice online

Escrocheriile romantice online sunt un tip necinstit și viclean de criminalitate informatică în care escrocii profită de atașamentele emoționale ale victimelor pentru a le jefui de bani. Pentru a câștiga încrederea și apropierea victimelor credulilor, escrocii adoptă frecvent identități false și par a fi interesați romantic de acestea. Acești infractori folosesc strategii creative, cum ar fi crearea de povești captivante și prezentarea lor ca parteneri perfecți, pentru a face victimele să creadă că sunt în siguranță.

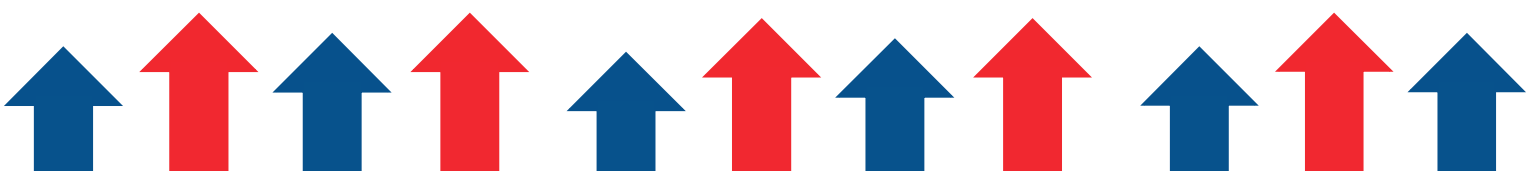
Odată ce încrederea a fost construită, escrocii pot profita de sentimentele victimei pentru a o constrânge să trimită bani sau să dezvăluie date financiare sau personale sensibile. Poveștile de viață exagerat de dramatice sau fără cusur, reticența de a se întâlni personal, declarațiile pripite de dragoste sau devotament și cererile de ajutor financiar sunt semnale de alarmă ale fraudelor romantice online. Pentru a reduce probabilitatea de a deveni victimă a acestor scheme frauduloase, este esențial să dați dovadă de atenție, scepticism și vigilență atunci când participați la interacțiuni online. Escrocheriile de dragoste online profită de emoțiile și încrederea oamenilor.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

FinPower

Co-funded by the European Union

Activitatea 3 - Depistarea înșelătoriilor legate de relațiile amoroase online



Activitatea are ca scop educarea participanților cu privire la identificarea semnelor de avertizare ale potențialelor fraude în domeniul întâlnirilor online. Se pune accentul pe recunoașterea semnalelor de alarmă, cum ar fi o persoană excesiv de perfectă, evitarea întâlnirilor față în față, exprimarea rapidă a dragostei și cererile de asistență financiară. În plus, oferă sfaturi concise privind siguranța, susținând efectuarea de verificări online, abținerea de la împărtășirea informațiilor personale și încrederea în propriile instincte atunci când nu se simte bine în legătură cu o relație.

Activitatea încurajează discuțiile deschise, permițând participanților să pună întrebări și să răspundă la întrebări în timp ce își împărtășesc opiniile, preocupările și experiențele personale sau observate cu privire la înșelăciunile legate de relațiile amoroase online. Acest schimb interactiv promovează conștientizarea și pregătirea împotriva activităților potențial frauduloase din cadrul întâlnirilor online, permițând persoanelor să navigheze în aceste relații cu mai multă prudență și sensibilitate.

Pas cu pas

Discutați câteva red flags tipice care ar putea indica o fraudă la întâlnirile online. Acestea ar putea consta în:

-**Prea perfectă pentru a fi adevărată:** Dacă persoana pare extrem de perfectă sau dacă povestea ei de viață pare prea dramatică, fiți precaut.

- Evitarea întâlnirilor față în față: Este un semnal de alarmă dacă cealaltă persoană inventează în mod constant motive pentru a evita întâlnirile în persoană.

- **Declarații rapide de dragoste:** Ar putea fi un indiciu dacă își arată dragostea sau devotamentul extrem de devreme în relație.

- Cereri de bani: Nu dați niciodată bani și nu divulgați detalii financiare unui străin pe care nu l-ați văzut în persoană.

1.Dați câteva scurte sfaturi de siguranță:

- Efectuați întotdeauna o verificare online a trecutului unei persoane pentru a căuta orice discrepanțe.

Nu împărtășiți nicio informație personală: Păstrați-vă pentru dumneavoastră adresa de domiciliu, informațiile bancare și numărul de securitate socială.

Dacă ceva vi se pare ciudat, aveți încredere în instinctele dumneavoastră; probabil că așa este. Îmbrățișați-vă instinctul.

2.Oferiți tuturor șansa de a pune întrebări și de a răspunde la întrebări. Încurajați cursanții să își discute opiniile, îngrijorările și orice experiențe personale sau observate cu înșelăciunile romantice online.

Activitatea 4 - Un videoclip despre cumpărături sigure

Obiectivul acestei activități este de a-i ghida pe cursanți în recunoașterea și punerea în aplicare a măsurilor de siguranță atunci când se angajează în cumpărături online.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Activitatea ar trebui să înceapă cu îndrumarea cursanților să viziteze www.getsafeonline.org, urmată de navigarea la secțiunea „Watch Videos" și selectarea videoclipului „Shopping Online". După finalizarea videoclipului, cursanții ar trebui să fie instruiți să acceseze www.easons.com și să evalueze critic site-ul web răspunzând la întrebări specifice: dacă site-ul afișează o politică de confidențialitate și dacă prezintă o adresă de contact.

Această activitate urmărește să încurajeze cursanții să se implice în resursele educaționale privind siguranța online și apoi să își aplice practic cunoștințele prin evaluarea măsurilor de securitate și a transparenței unui site de cumpărături real. Prin combinarea cunoștințelor teoretice din materialul video cu o evaluare practică a site-ului web, cursanții pot discerne și identifica în mod activ măsurile de siguranță esențiale de care trebuie să țină seama în timpul cumpărăturilor online. Acest proces facilitează o experiență de învățare practică, consolidând importanța politicilor de confidențialitate și a informațiilor de contact pentru o experiență sigură de cumpărături online.

METODE ALTERNATIVE DE PLATĂ

Introducere în metodele alternative de plată

Metodele de plată convenționale, cum ar fi numerarul și cardurile de credit, pot fi dăunătoare pentru societate și pentru mediu. Acest subdomeniu abordează acest aspect prin evidențierea metodelor de plată de substituție, denumite metode de plată alternative, cum ar fi:

- **Portofelele digitale**: Prin eficientizarea tranzacțiilor online și eliminarea nevoii de monedă forte și facturi pe hârtie, aceste carduri electronice promovează un sistem financiar fără hârtie.
- **Plățile mobile**: Pentru o gamă largă de servicii și mărfuri, aceste servicii, care sunt rulate pe dispozitive mobile, preiau rolul metodelor tradiționale de plată, precum numerarul sau cardurile.
- **Criptomonedele**: Folosind tehnologia blockchain, monedele digitale descentralizate și sigure permit tranzacții fără a fi nevoie de bănci centrale, reducând posibil dependența de instituțiile financiare stabilite.

Metodele alternative de plată se referă la modalitățile netradiționale de efectuare a tranzacțiilor financiare în afara numerarului sau a cardurilor de credit/debit. Aceste metode au câștigat popularitate datorită confortului, accesibilității și, adesea, integrării lor în platformele digitale. Cardurile preplătite, transferurile bancare, portofelele digitale, criptomonedele, programele de fidelizare, cardurile locale și opțiunile de plată amânată sunt doar câteva dintre posibilitățile care intră în această categorie. Datorită ușurinței de utilizare și securității lor, epidemia a accelerat și mai mult acceptarea lor.

- **Impactul asupra mediului și societății**: Utilizarea metodelor alternative de plată pentru tranzacțiile digitale are mai multe avantaje.

- **Avantaje ecologice**: Tranzacțiile digitale se caracterizează printr-un consum mai redus de hârtie, un impact mai mic asupra emisiilor de carbon și o mai bună eficiență energetică. Ele diminuează daunele pe care producția și tranzitul monedelor fizice le provoacă mediului.
- **Impactul criptomonedelor** asupra societății poate fi văzut în capacitatea lor de a reduce drastic costurile de tranzacționare, de a accelera tranzacțiile și de a încuraja incluziunea financiară, în special în comunitățile marginalizate. Acest lucru contribuie la sprijinirea economiilor locale și la furnizarea de servicii financiare persoanelor care nu au acces la instituțiile tradiționale.

Datorită mai multor considerente, tranzacțiile digitale reprezintă o opțiune mai ecologică decât tranzacțiile în monedă tradițională, care au efecte majore asupra mediului.

- **Diminuarea impactului asupra mediului**: Producția, distribuția și tipărirea monedei fizice au toate un traseu substanțial pe hârtie care contribuie la pierderea copacilor. Utilizarea pe scară largă a banilor de hârtie are efecte negative asupra mediului, cum ar fi defrișările și creșterea emisiilor de gaze cu efect de seră. În plus, transportul banilor la bănci și bancomate contribuie la creșterea consumului de combustibil și a emisiilor generate de deplasarea mașinilor.

- **Eficiența energetică a tranzacțiilor digitale**: Pe de altă parte, tranzacțiile digitale executate electronic necesită mai puțină energie și echipamente fizice substanțiale. Pentru a reduce efectul lor total asupra mediului, majoritatea tranzacțiilor digitale sunt gestionate în centre de date care sunt alimentate din surse de energie regenerabile. Aceste instalații sunt concepute pentru a fi cât mai eficiente din punct de vedere energetic posibil, reducând semnificativ impactul lor asupra emisiilor de carbon.

Criptomonedele prezintă mai multe avantaje potențiale, în special pentru populațiile defavorizate care caută servicii financiare:

- **Costuri de tranzacționare mai mici**: Băncile și companiile de remitențe percep frecvent comisioane ridicate pentru transferurile internaționale tradiționale de bani. Aceste cheltuieli sunt reduse considerabil de criptomonede, făcând transferurile internaționale de bani mai rezonabile.

- **Tranzacții mai rapide**: Comparativ cu sistemele bancare obișnuite, tranzacțiile cu criptomonede se remarcă prin rapiditatea lor. Această viteză este deosebit de importantă pentru persoanele care depind de transferuri în timp util pentru a acoperi costurile zilnice sau urgențele neprevăzute.

- **Incluziunea financiară și economiile locale**: prin furnizarea de servicii financiare persoanelor care nu au acces la instituțiile bancare tradiționale, criptomonedele pot reduce decalajele financiare din localitățile îndepărtate sau sărace. Această strategie atotcuprinzătoare poate stimula considerabil economia regională și poate oferi persoanelor defavorizate mai multă influență.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Tipuri de metode alternative de plată

Metodele alternative de plată se referă la o varietate de metode netradiționale de tranzacții financiare care oferă clienților mai multe alternative pentru efectuarea plăților.

Câteva exemple de metode alternative de plată sunt:

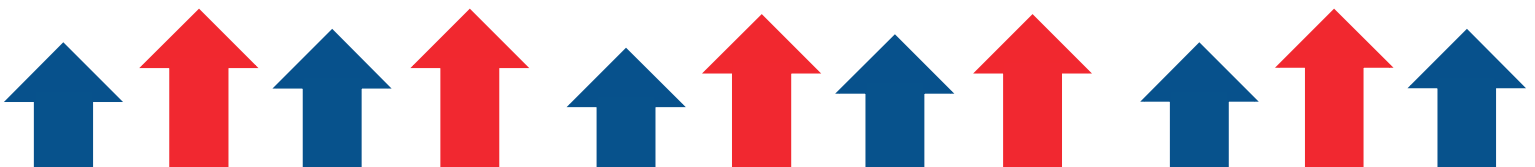
- **Carduri preplătite**: Acestea sunt carduri care sunt preîncărcate cu o anumită sumă de bani și pot fi utilizate pentru a face cumpărături până când soldul este epuizat.
- **Transferuri bancare**: Această metodă permite consumatorilor să plătească bunuri și servicii online utilizând transferuri online directe din contul lor bancar.
- **Portofele digitale**: Acestea sunt software sau hardware care permit utilizatorilor să efectueze plăți electronice. Acestea pot fi utilizate pentru a stoca mai multe metode de plată, cum ar fi cardurile de credit și conturile bancare, și pot fi folosite pentru a face achiziții online sau în magazine.
- **Criptomonede**: Acestea sunt monede digitale sau virtuale care utilizează criptografia pentru securitate și funcționează independent de o bancă centrală. Acestea pot fi utilizate pentru a face achiziții online sau în magazinele care le acceptă ca formă de plată.
- **Programe de loialitate**: Aceste programe permit consumatorilor să câștige puncte sau recompense pentru efectuarea de cumpărături la un anumit comerciant sau brand. Punctele sau recompensele pot fi apoi răscumpărate pentru reduceri sau produse gratuite.
- **Carduri locale**: Acestea sunt carduri de credit sau de debit care sunt emise de bănci sau instituții financiare locale și pot fi utilizate numai într-o anumită țară sau regiune.
- **Opțiuni de plată amânată și în rate**: Aceste opțiuni permit consumatorilor să amâne plata pentru o achiziție sau să o plătească în rate în timp.

Activitatea 1: Diferite tipuri de metode alternative de plată

Scopul principal al acestei activități este de a pune la dispoziția cursanților o broșură detaliată care prezintă și explică o serie de opțiuni de plată diferite. Este furnizată o scurtă descriere pentru fiecare metodă, care include carduri preplătite, transferuri bancare, portofele digitale, criptomonede, programe de fidelizare, carduri locale și opțiuni de plată întârziată. Obiectivul este de a oferi cursanților o înțelegere de bază a diferitelor mecanisme de plată, subliniind numeroasele beneficii, caracteristici și situații în care fiecare abordare ar putea fi utilă. La sfârșitul activității, cursanții ar trebui să aibă o înțelegere de bază a opțiunilor alternative de plată, care să le permită să evalueze posibilele utilizări și avantaje ale fiecărei metode în diverse situații financiare.

Pas cu pas

1. Distribuiți fișa de lucru cursanților.
2. Întrebați cursanții dacă au folosit oricare dintre aceste metode de plată și, dacă da, cum a fost experiența lor.



Activitatea 2: Beneficii și dezavantaje

Obiectivele acestei activități sunt de a promova gândirea critică și participarea participanților la cântărirea avantajelor și dezavantajelor diferitelor opțiuni de plată. Pe tablă sau flipchart, se creează o zonă organizată, încurajând participarea la o conversație în grup. Scopul exercițiului este de a investiga și de a înțelege avantajele și dezavantajele diferitelor opțiuni alternative de plată.

Prin intermediul acestui exercițiu, cursanții pot identifica avantajele utilizării acestor strategii, inclusiv mai multă flexibilitate, o bază mai largă de consumatori și posibile economii de costuri pentru întreprinderi. În același timp, ei se gândesc la posibilele dezavantaje, cum ar fi adoptarea limitată de către întreprinderi, cerința de a avea mai multe opțiuni de plată și gradele diferite de protecție împotriva fraudei oferite de diferitele alternative. Utilizând această comparație, cursanții înțeleg complexitatea sistemelor de plată alternative și factorii care trebuie luați în considerare.

Pas cu pas

Cereți cursanților să își împărtășească opiniile cu privire la beneficiile și dezavantajele utilizării metodelor alternative de plată și scrieți-le pe partea corespunzătoare a tabloului (a se vedea exemplele de mai sus).

Utilizați tabla albă

Ghid pentru un formator: Avantaje și dezavantaje

Aspecte precum securitatea, ușurința în utilizare, costurile, disponibilitatea și eventualele stimulente sunt frecvent în centrul discuțiilor privind avantajele și dezavantajele mai multor sisteme de plată alternative. Prin examinarea aprofundată a acestor factori, cursanții vor avea cunoștințele necesare pentru a pune în balanță avantajele și dezavantajele utilizării metodelor alternative de plată. Această înțelegere facilitează luarea unor decizii în cunoștință de cauză cu privire la aplicarea acestora în diverse tranzacții financiare.

Utilizarea altor metode de plată are mai multe avantaje. Clienților, atunci când vine vorba de cumpărături, acestea le oferă mai multe opțiuni și libertate. Prin utilizarea metodei de plată alese, ei pot, de asemenea, să ajute companiile să atragă clienți din întreaga lume. În plus, prin utilizarea altor modalități de plată, firmele pot fi în măsură să reducă costurile de procesare a cardurilor de credit.

Cu toate acestea, utilizarea opțiunilor alternative de plată poate prezenta unele dezavantaje. De exemplu, clienții ar putea fi nevoiți să aibă la dispoziție mai multe alternative de plată, deoarece nu toate întreprinderile acceptă toate tipurile de metode alternative de plată. În plus, nu toate celelalte opțiuni de plată oferă același grad de protecție împotriva fraudei ca și cardurile de credit.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

Activitatea 3: Securitatea și confidențialitatea utilizării metodelor alternative de plată.

Această activitate își propune să abordeze problemele de confidențialitate și securitate asociate cu utilizarea metodelor alternative de plată. Ea explorează pericolele posibile ale utilizării diferitelor metode de plată, inclusiv frauda, furtul de identitate și încălcarea securității datelor. În cadrul discuției se subliniază importanța adoptării de măsuri preventive pentru reducerea acestor riscuri. Aceste măsuri preventive includ revizuirea periodică a situațiilor financiare pentru a depista nereguli, utilizarea autentificării cu doi factori pentru a se proteja împotriva preluării conturilor și asigurarea că destinatarii plăților sunt legitimi înainte de a transfera bani. Scopul este de a oferi consumatorilor tactici utile pentru a reduce problemele legate de securitate și confidențialitate atunci când utilizează alte metode de plată.

Pas cu pas

Discutați implicațiile utilizării metodelor alternative de plată asupra securității și confidențialității, cum ar fi riscul de fraudă, încălcarea securității datelor și furtul de identitate.

Rezumați punctele-cheie abordate în lecție și subliniați importanța utilizării metodelor alternative de plată în condiții de siguranță și securitate.

Încurajați cursanții să pună orice întrebări pe care le au cu privire la subiect.

Ghid pentru un formator:

Implementarea sistemelor alternative de plată este condiționată de păstrarea securității și a confidențialității. Este esențial să se garanteze securitatea acestor tehnici pentru a se proteja împotriva furtului de identitate, a fraudei și a încălcărilor care implică informații personale. Este esențial să se înțeleagă protocoalele de criptare și securitate care protejează aceste opțiuni de plată.

Riscul de fraudă: Metodele alternative de plată introduc noi oportunități pentru activități frauduloase. Spre deosebire de sistemele de plată tradiționale, aceste metode pot avea măsuri de securitate mai puțin stricte, ceea ce le face vulnerabile la tranzacții neautorizate sau la preluarea conturilor. Utilizatorii trebuie să fie precauți atunci când își împărtășesc informațiile de plată și să fie conștienți de eventualele tentative de phishing sau înșelăciuni.

Încălcări ale securității datelor: Platformele alternative de plată stochează informații financiare sensibile, cum ar fi detaliile cardurilor de credit sau numerele conturilor bancare. În cazul unei încălcări a securității datelor, aceste informații ar putea fi compromise, ducând la pierderi financiare și furturi de identitate. Companiile care oferă servicii alternative de plată trebuie să acorde prioritate măsurilor robuste de securitate pentru a proteja datele utilizatorilor de accesul neautorizat sau de atacurile cibernetice.

Furtul de identitate: Metodele alternative de plată cresc riscul de furt de identitate, deoarece acestea solicită adesea utilizatorilor să furnizeze informații personale pentru crearea și verificarea contului. Infractorii cibernetici pot exploata vulnerabilitățile acestor

sisteme pentru a fura identitatea utilizatorilor și a se angaja în activități frauduloase. Utilizatorii ar trebui să dea dovadă de prudență atunci când împărtășesc informații personale online și să își monitorizeze periodic conturile pentru a depista orice activitate suspectă.

Utilizatorii își pot consolida confidențialitatea, pot lua decizii în cunoștință de cauză și își pot dezvolta încrederea în utilizarea acestor tehnologii, fiind conștienți de procedurile de securitate și de orientările privind confidențialitatea legate de aceste modalități. Subtema se referă la furnizarea către cursanți a informațiilor de care au nevoie pentru a evalua caracteristicile de securitate și confidențialitate ale mai multor opțiuni de plată alternative.

Aceste modalități de plată oferă clienților mai multe opțiuni și flexibilitate atunci când fac achiziții, dar există șansa să apară fraude, furturi de identitate și încălcări ale securității datelor.

Opțiunile de plată alternative pot avea efecte asupra confidențialității și securității. Aceste metode de plată oferă clienților mai multe opțiuni și mai multă flexibilitate în efectuarea cumpărăturilor, dar există posibilitatea să apară fraude, furturi de identitate și încălcări ale securității datelor.

Atunci când utilizează metode de plată alternative, consumatorii pot lua câteva măsuri de siguranță pentru a reduce aceste pericole. De exemplu, aceștia ar trebui să își auditeze periodic situațiile financiare pentru a descoperi orice nereguli. În plus, pentru a se proteja împotriva preluărilor de conturi care pot duce la fraudarea plăților, ei trebuie să activeze autentificarea cu doi factori. Înainte de a trimite bani, clienții ar trebui, de asemenea, să confirme destinația plății lor.

CONCLUZII

Acest modul a oferit participanților cunoștințe esențiale și abilități practice în domeniul securității online și al educației financiare. Prin explorarea unor subiecte precum riscurile de securitate online, cumpărăturile online în condiții de siguranță și metodele alternative de plată, participanții au dobândit cunoștințe privind protejarea eficientă a informațiilor personale și financiare. Modulul urmărește să ofere indivizilor posibilitatea de a lua decizii în cunoștință de cauză și de a adopta practici financiare sigure și durabile în era digitală de astăzi.

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. Project Number: 2022-1-AT01-KA220-ADU-000087985

REFERINȚE

- Anti-Phishing Working Group (APWG). (n.d.). Retrieved from https://www.apwg.org/
- Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). Retrieved from https://www.cisa.gov/
- Federal Trade Commission (FTC). (n.d.). Retrieved from https://www.ftc.gov/
- Grigutytė, M., & Grigutytė, M. (2023, December 27). Nigerian Prince scam: what is it and how it works. NordVPN. https://nordvpn.com/pt/blog/nigerian-prince-scam/
- Hayes, A. (2023, December 20). Bernie Madoff: Who He Was, How His Ponzi Scheme Worked. Investopedia. https://www.investopedia.com/terms/b/bernard-madoff.asp
- Krebs on Security. (n.d.). Retrieved from https://krebsonsecurity.com/
- SANS Institute. (n.d.). Retrieved from https://www.sans.org/
- Age Action. (n.d.). For All Older People. https://www.ageaction.ie
- Better Business Bureau. (2021). How to Protect Yourself When Shopping Online. https://www.bbb.org/article/tips/11205-bbb-tip-how-to-protect-yourself-when-shopping-online
- ESL Lesson Plans | Your English Pal. (2022, February 3). Your English Pal. https://www.yourenglishpal.com
- Federal Trade Commission. (2021). Online Shopping Tips. https://www.consumer.ftc.gov/articles/online-shopping-tips
- Get Safe Online | The UK's leading Online Safety Advice Resource. (2023, November 1). Get Safe Online. https://www.getsafeonline.org/)
- Kaspersky. (2021). Safe Online Shopping: 10 Tips to Avoid Scams. https://www.kaspersky.com/resource-center/online-safety/safe-online-shopping
- Norton. (2021). Online Shopping Safety Tips: How to Shop Online Safely. https://us.norton.com/internetsecurity-online-shopping-safety-tips-how-to-shop-online-safely.html
- Jackson, W. (2023, July 10). William Jackson | Data security policies: Necessary but not sufficient. Route Fifty. https://www.route-fifty.com/cybersecurity/2007/12/william-jackson-data-security-policies-necessary-but-not-sufficient/308532/
- K. (2023, March 10). Keeping Your money Safe Online. YouTube. https://www.youtube.com/watch?v=EL0_zRfpEnQ
- Marsh, L. (2023, November 3). How To Avoid Payment Fraud As A Property Manager. Forbes. https://www.forbes.com/sites/forbescommunicationscouncil/2023/11/03/how-to-avoid-payment-fraud-as-a-property-manager/?sh=455340a03362
- Mileva, G. (2023, October 26). Everything You Need to Know About Alternative Payment Methods in 2024. Influencer Marketing Hub. https://influencermarketinghub.com/alternative-payment-methods/
- Online Payment Processing Solution. (n.d.). GoCardless. https://gocardless.com/
- Payne, K. (2023, July 18). Axos Bank Review. Investopedia. https://www.investopedia.com/axos-bank-review-4802090
- What are the risks of digital payments? (2020, February 5). World Economic Forum. https://www.weforum.org/agenda/2015/02/what-are-the-risks-of-digital-payments/

FinPower

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. Project Number: 2022-1-AT01-KA220-ADU-000087985