



**information
matters**

Program de instruire **pentru cursuri online**

Modulul 9

Educație media și confidențialitate



Finanțat de Uniunea Europeană. Punctele de vedere și opiniile exprimate aparțin, însă, exclusiv autorului (autorilor) și nu reflectă neapărat punctele de vedere și opiniile Uniunii Europene sau ale Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.

Număr acord: 2022-1-BG01-KA220-ADU-000085514



**Cofinanțat de
Uniunea Europeană**

Conținut

Descriere pentru lecția online	4
Introducere	10
Rezultatele învățării	11
Cuvinte cheie	11
Subiecte	11
Termeni și definiții	12
Câteva resurse utile	14
Obiective de învățare	15
Setări/materiale/durată	16
Implementarea activității	16
Întrebări de reflecție	19
Activitate 2#: Păstrați informațiile personale în siguranță – povești despre confidențialitate	20
Obiective de învățare	20
Setări/materiale/durată	21
Implementarea activității	21
Recomandări pentru implementare	22
Întrebări de reflecție	23
Activitatea 3#: Servicii bancare online, fără teamă	24
Obiective de învățare	24
Setări/materiale/durată	25
Implementarea activității	25
Recomandări pentru implementare	27
Întrebări de reflecție	27

Evaluarea Modulului.....	28
Test pentru autoevaluare pentru modulul 9	28
Fisa de lucru	28
Proiect-Activitate	28
Chestionar	30
Validarea Modulului	30
ANEXA pentru Modulul 9	32
Activitate 1#: Cum să păstrați și să utilizați parolele în siguranță?	36
Activitate 2#: Păstrați informațiile personale în siguranță – povești despre confidențialitate	37
Activitatea 3#: Servicii bancare online fără teamă	40
QUIZ DE ALFABETIZARE MEDIA ȘI CONFIDENȚIALITATE	42
CHESTIONAR PRIVIND ALFABETIZAREA ȘI CONFIDENȚIALITATEA ÎN MASS-MEDIA	45

Descriere pentru lecția online

Bun venit la modulul despre alfabetizare media și confidențialitate. În acest modul, vom explora importanța protejării datelor cu caracter personal și a menținerii confidențialității în mediul online, în special pentru persoanele în vârstă. Până la sfârșitul acestui modul, veți avea o înțelegere mai profundă a problemelor de confidențialitate din era digitală și veți fi echipat cu strategii practice, menite să vă sprijine în protejarea informațiilor personale.



Definiții și exemple

- » **Datele personale** reprezintă orice informație care poate fi utilizată pentru a identifica o persoană. Include detalii precum numele, adresa, numărul de telefon, e-mailul, data nașterii și informații mai sensibile precum înregistrările financiare sau istoricul medical. Datele cu caracter personal sunt valoroase și ar trebui păstrate în siguranță, pentru a vă proteja de potențiale utilizări eronate sau de exploatare.
- » Este esențial să protejăm confidențialitatea acestor date împotriva partajării sau accesării de către părți neautorizate, deoarece acest lucru poate duce la furtul de identitate sau la alte forme de criminalitate cibernetică. Pentru a preveni atacul datelor cu caracter personal, trebuie să înțelegem cum să folosim setările de confidențialitate pe rețelele sociale și pe alte platforme online, să evităm partajarea informațiilor sensibile în rețele nesecurizate, să folosim parole puternice, precum și alte măsuri de securitate cibernetică.



- » **Confidențialitatea online** se referă la capacitatea de a controla și proteja informațiile dumneavoastră personale în timpul utilizării internetului. Aceasta implică păstrarea în siguranță a datelor dumneavoastră cu caracter personal, limitarea cantității de informații pe care le partajați online și conștientizarea faptului că cineva vă poate accesa activitățile online. Înțelegând confidențialitatea online, puteți menține un control mai mare asupra identității digitale și vă puteți proteja de amenințări online precum furtul de identitate, escrocherii sau supravegherea neautorizată.
- » **Amprenta digitală** este o urmă de informații pe care o lași în timp ce folosești dispozitive digitale și internetul. Acesta cuprinde activitățile dvs. online, inclusiv site-urile web pe care le vizitați, postările pe care le faceți pe rețelele sociale, comentariile pe care le lăsați și imaginile sau videoclipurile pe care le distribuiți. Amprenta digitală poate avea consecințe pe termen lung și poate fi folosită de alții pentru a-ți urmări comportamentul online, a-ți influența deciziile sau chiar a-ți determina credibilitatea. Înțelegerea amprenteii tale digitale este esențială pentru a menține o reputație online pozitivă și pentru a-ți proteja confidențialitatea.

În general, este important ca persoanele în vârstă să fie preocupate de protejarea vieții lor private în mediul digital. Rămânând informați, utilizând practici sigure și ținând cont de activitățile noastre online, putem minimiza riscurile potențiale și putem obține o experiență online mai sigură.

Ce înseamnă siguranța online pentru persoanele în vârstă?

Confidențialitatea online și aplicarea unei game de inițiative de siguranță privind protecția datelor cu caracter personal și informațiile personale înseamnă:

- Să cunoască și să aplice reguli și principii de bază pentru siguranță, protecția vieții private și a informațiilor personale;
- A aplica setări de confidențialitate și permisiuni, cum ar fi cookie-urile;
- A fi conștient de instrumentele de urmărire;
- A fi conștient de amprenta dvs. digitală;
- A conștientiza strategiile și instrumentele utilizate în prezent pentru urmărirea, spionajul și intruziunea în sfera privată.



Cum vă puteți instrui participanții în vârstă despre alfabetizarea media și confidențialitatea?

- Puteți găsi conținuturi utile și link-uri suplimentare legate de alfabetizarea media și confidențialitatea în programul de formare.
- Realizați activități planificate pentru cursanții vârstnici, pentru a le facilita conștientizarea cu privire la confidențialitate. Prin realizarea și implementarea acestor activități de formare, vă puteți motiva și sprijini participanții să colecteze și să dezvolte abilitățile și competențele dorite în domeniul alfabetizării media și confidențialității. Exercițiile oferă oportunități de extindere a cunoștințelor în următoarele 3 domenii:
 - Cum să păstrați și să utilizați parolele în siguranță?
 - Cum să păstrați informațiile personale în siguranță?
 - Servicii bancare online, fără grijă.
- Petreceți suficient timp exersând o metodă pe care participanții dvs. o pot folosi cu încredere.
- Persoanele în vârstă se tem adesea de operațiunile bancare online, deoarece această abordare pare a fi prea nesigură pentru ei. Așa că scopul nostru este să abordăm temerile lor, astfel încât să putem înțelege în ce circumstanțe ar trebui să lucrăm.

- Dacă cunoașteți circumstanțele participanților dvs., puteți adapta poveștile și activitățile ulterioare în consecință.
- Motivați-vă cursanții să facă un rezumat al regulilor de siguranță, pentru a-și reaminti de ele la viitoarele lor activități online. Transmiteți această regulă într-un mod atrăgător și distribuiți-o participanților.

Felicitări pentru finalizarea Modulului 9 – Educație media și confidențialitate!

Amintiți-vă, rămânând informat, folosind practici sigure și ținând cont de activitățile dvs. online, puteți minimiza riscurile potențiale și puteți obține o experiență online mai sigură. Utilizați resursele oferite pentru a vă sprijini participanții să-și îmbunătățească cunoștințele și să-și continue călătoria spre a deveni alfabetizați media și conștienți de confidențialitate. Rămâneți vigilenți, fiți în siguranță și bucurați-vă de lumea digitală într-un mod responsabil.

Vă sfătuim să continuați cu lecția 10. Mult succes!



Introducere

Datele personale sunt orice informație care poate fi utilizată pentru a identifica o persoană. Este esențial să protejăm confidențialitatea acestor date împotriva partajării sau accesării de către părți neautorizate, deoarece acest lucru poate duce la furtul de identitate sau la alte forme de criminalitate cibernetică. Pentru a preveni furtul datelor personale, seniorii trebuie să înțeleagă cum să folosească setările de confidențialitate pe rețelele sociale și alte platforme online, să evite partajarea de informații sensibile prin rețele nesecurizate și să folosească parole puternice și alte măsuri de securitate pentru a-și proteja conturile.

În general, este important ca persoanele în vârstă să acționeze activ în protejarea vieții private în mediul digital. Rămânând informați, utilizând practici sigure și ținând cont de activitățile lor online, aceștia pot minimiza riscurile potențiale și pot obține o experiență online mai sigură.

Rezultatele învățării

Participantii vor putea înțelege importanța confidențialității și discuta posibilele vulnerabilități în utilizarea internetului și a dispozitivelor digitale. Ei vor dobândi de asemenea și informații despre protejarea și partajarea responsabilă a informațiilor personale. La nivel societal, va spori gradul de conștientizare cu privire la impactul dezinformării în sfera publică.

Cuvinte cheie

Date personale, confidențialitate online, amprentă digitală, igiena cibernetică, măsuri de precauție.

Subiecte

Confidențialitate online și aplicarea unei game de inițiative de siguranță privind protecția datelor cu caracter personal și informațiile personale:

- Reguli și principii de bază pentru siguranța, protecția vieții private și a informațiilor personale;
- Setări de confidențialitate și permisiuni cum ar fi cookie-uri, conștientizarea instrumentelor de urmărire, amprenta digitală;
- Conștientizarea strategiilor și instrumentelor utilizate în prezent pentru urmărirea, spionajul și intruziunea în sfera privată.

Termeni și definiții:

- **Date personale:** Datele personale se referă la orice informație care se referă direct sau indirect la o persoană. Include detalii precum numele, adresa, numărul de telefon, e-mailul, data nașterii și informații mai sensibile cum ar fi înregistrările financiare sau istoricul medical. Datele cu caracter personal sunt valoroase și ar trebui păstrate în siguranță pentru a vă proteja de potențiale utilizări eronate sau de exploatare.
- **Confidențialitate online:** se referă la capacitatea de a controla și de a proteja informațiile personale în timpul utilizării internetului. Aceasta implică păstrarea în siguranță a datelor dumneavoastră cu caracter personal, limitarea cantității de informații pe care le partajați online și conștientizarea a cine vă poate accesa activitățile online. Prin înțelegerea confidențialității online, vă puteți menține un control mai mare asupra identității digitale și vă puteți proteja de amenințări online precum furtul de identitate, escrocherii sau supravegherea neautorizată.

- **Amprenta digitală:** este urma de informații pe care o lași în urmă în timp ce folosești dispozitive digitale și internetul. Acesta cuprinde activitățile dvs. online, inclusiv site-urile web pe care le vizitați, postările pe care le faceți pe rețelele sociale, comentariile pe care le lăsați și imaginile sau videoclipurile pe care le distribuiți. Amprenta dvs. digitală poate avea consecințe pe termen lung și poate fi folosită de alții pentru a vă urmări online, pentru a vă influența deciziile sau chiar pentru a determina credibilitatea ta. Înțelegerea amprenteii tale digitale este esențială pentru a menține o reputație pozitivă online, precum și pentru a-ți proteja confidențialitatea.



Câteva resurse utile

 <https://www.digitaleseniorinnen.at/leistungen/know-how>

 <https://erwachsenenbildung.at/digiprof/mediathek/17725-studie-zu-bildung-und-digitalen-kompetenzen-im-alter.php>

 <https://cyberclever.eu/resources>

O scurtă animație despre navigarea online și confidențialitate:

 https://www.youtube.com/watch?v=zsboDBMq6vo&list=PL3cj0_EtKN4joc4Gt2IFzBMoZp4h5ty7o&t=51s



Activitate 1#: Cum să păstrați și să utilizați parolele în siguranță?

Obiective de învățare:

- Clarificați/repetăți scopul unei parole
- Aflați cum să găsiți parole sigure pentru dvs. fără să le scrieți
- Regulile pentru „cum vă puteți păstra parola în siguranță?”

Setări/materiale/durată

- note, pixuri și markere pentru participanți
- tablă online/șabloane de afișe (de ex <https://canva.com> și/sau hârtie mai mare pentru postere)
- 2 ore

Implementarea activității:

Pasul 1 – Introducere:

Ca o introducere la această activitate, cereți participanților să facă o listă cu domeniile online/site-urile web în care folosesc parolele. Poate fi transcris online (de ex. document partajat/tabletă albă/foaie de lucru/chat).

După aceea, puteți discuta în plen despre modul în care participanții au aflat despre parole și dacă au avut dificultăți în a-și reaminti respectivele parole.

Pasul 2:

Cereți participanților să cerceteze pe internet recomandările în legătură cu parole sigure.

Ei pot scrie regulile într-un document partajat sau pe o foaie de lucru (în acest caz, cereți-le să vi le trimită) iar dvs., în calitate de formator,

puteți prezenta mai târziu un poster cu cele mai importante reguli. Participanții pot imprima aceste reguli și le pot accesa în scop consultativ.

Sprijină activitatea cu feedback-ul tău cu privire la cele mai importante elemente ([Vezi Anexa](#)).

Pasul 3:

Oferiți participanților metode simple (vezi mai jos) despre cum să genereze și să observe parole sigure. Prezentați exemple cu propriile lor date, utilizând o persoană fictivă. (ex: Maria, o femeie de 76 de ani, care locuiește într-o casă de bătrâni în Viena la casa numărul 42, 4 nepoți, o pisică, mâncarea preferată este Wiener Schnitzel, culoarea preferată este albastru deschis).

Exemplul 1: MSchnitzelH42

- Gândește-te la mâncarea sau la legumele tale preferate (sau la un cuvânt special)
- Schimbați prima literă a acesteia cu prima literă a prenumelui dvs.
- Schimbați ultima literă cu prima literă a numelui dvs. de familie. Adăugați vârsta sau numărul de casă la început sau la sfârșit.
- Exemplu: „Maria Huber” a cărei mâncare preferată este „Snițel” și locuiește la numărul „42”.

Exemplul 2: 3!BabbiT@60

- Încercați un cuvânt pe care copilul dvs./nepotul dvs. nu l-a putut spune corect când era copil mic, de exemplu „babbit” în loc de „iepure”
- Adăugați numărul câți ani avea, de exemplu 3 și semnul exclamării „!” --> 3!babbit
- Faceți din primul „b” „B” mare și ultimul „t” cu „T” majusculă --> 3!BabbiT
- Apoi adaugă @60 la sfârșit pentru că aveai 60 de ani la momentul respectiv --> 3!BabbiT@60

Exemplul 3: Pntbcaloe2M

- Metoda primei litere: **P**arola **t**rebuie **s**chimbată **c**el puțin **o** dată **la 2** luni --> Ptscpodl2L
- Pentru acest exemplu, puteți folosi o frază/citate/linie dintr-o poezie etc. pe care probabil nu o veți uita niciodată.

Pasul 4

Discutați cu participanții ce ar trebui să facă dacă parola lor este folosită de altcineva sau furată. În principal, abuzul de parole trebuie raportat imediat coordonatorului site-ului web de pe care parola a fost furată.

Cercetați cu participanții sau încurajați-i să facă o cercetare despre modul în care aceste cazuri sunt tratate în țara lor. Există țări care au un Centru pentru Securitate Cibernetică de exemplu, unde aceste probleme pot fi raportate.

Recomandări pentru implementare

- » Este posibil ca participanții dvs. să fi folosit anterior reguli diferite pentru a aborda parolele. (De exemplu, au stocat parole în telefonul lor mobil/le-au notat într-un caiet și le-au păstrat pe birou, sau în Google Drive într-un document numit „parole și nume de utilizator”). Au nevoie de mai multă răbdare și timp pentru a lucra.
- » Acordați suficient timp exersând o metodă pe care participanții dvs. o pot folosi cu încredere. Puteți întreba unul câte unul dacă ar putea găsi o metodă bună de funcționare.
- » Puteți seta un memento pe telefoanele mobile sau în calendar la fiecare 2 luni pentru a schimba cele mai importante parole.

Întrebări de reflecție

- Ați găsit o metodă care vă ajută să faceți parole sigure?
- Care este cel mai bun mod de a vă observa parolele?
- Îți vei gestiona parola diferit în viitor? Cum?



Activitate 2#: Păstrați informațiile personale în siguranță – povești despre confidențialitate

Obiective de învățare:

- Să cunoască diferitele forme de criminalitate cibernetică
- Recunoască cele mai importante reguli în contextul securității confidențialității
- Cunoască diferența dintre rețelele securizate și cele nesecurizate
- Cunoască cum să-și protejeze intimitatea în spații deschise
- Fie atenți la activitățile online, pentru a obține o experiență online mai sigură

Setări/materiale/durată

- Note și pixuri pentru participanți
- tablă online
- 1,5 - 2 ore

Implementarea activității:

Pasul 1 – Introducere

Această activitate este destinată fie începătorilor care nu dețin prea multe informații despre confidențialitate, fie persoanelor în vârstă care s-ar putea să fi avut deja probleme cu aceste situații. Activitatea este, de asemenea, potrivită pentru a identifica reguli comune pentru o comunitate de persoane în vârstă.

Pasul 2

În cazul unei sesiuni în ritm propriu, cereți participanților să citească cele 3 povești.

În cazul unei sesiuni de grup online, organizați participanții în 3 grupuri. Dați grupurilor individuale 1-1 descrieri de caz (vezi Anexa). Grupurile ar trebui să discute temeinic poveștile, să răspundă la întrebările legate de acestea. În cazul lucrului individual, întrebările sunt aceleași.

Mai ales important este modul în care victimele pot evita incidentul nedorit data viitoare

Pasul 3

Participantii prezintă scenariile si răspunsurile lor elaborate în plen. Dacă lucrați cu un grup, dați celorlalte grupuri posibilitatea de a adăuga răspunsuri dacă consideră că este util.

Pasul 4

Cereți participanților să rezume cele mai importante reguli de comportament în cel puțin 5 puncte, pe baza scenariilor. Acest lucru poate ajuta la evitarea unor astfel de povești nedorite.

Recomandări pentru implementare

- » Dacă cunoașteți circumstanțele participanților dvs., puteți rescrie poveștile în consecință.
- » Dacă participanții/grupul dumneavoastră locuiesc împreună sau se întâlnesc regulat și au un asistent social, de exemplu într-un azil/club de bătrâni pentru bătrâni, încercați să vă consultați cu colegii pentru a rescrie scenariile în funcție de nevoile lor.

Întrebări de reflecție

- Ați învățat ceva util din aceste povești? Ați putea rezuma pe scurt?
- Există reguli pe care îți place să le spui prietenilor sau cunoscuților tăi?
- Care regulă este cea mai importantă pentru tine?





Activitatea 3#: Servicii bancare online, fără teamă

Obiective de învățare:

- Cunoașteți beneficiile serviciilor bancare online.
- Cunoașteți posibilitățile online banking.
- Înțelegerea importanței principalelor reguli ale online banking-ului, pentru a fi un utilizator informat.

Setări/materiale/durată

- calculatoare sau dispozitive personale (smartphone, tablete, laptopuri etc.) cu acces la internet
- marker, note, pixuri pentru participanți
- Min. 2 ore

Implementarea activității:

Pasul 1 – Introducere

Persoanele în vârstă se tem adesea de operațiunile bancare online, deoarece această abordare pare a fi prea nesigură pentru ei. Așa că scopul nostru este să abordăm temerile lor, astfel încât să putem înțelege în ce circumstanțe ar trebui să lucrăm.

Explicați scopul și obiectivele de învățare ale acestei activități și acordați atenție recomandărilor.

Pasul 2

Cereți participanților să formeze grupuri mici. Aceste grupuri mici ar trebui să discute despre ce avantaje, dezavantaje și riscuri ale serviciilor bancare online le cunosc. Poate fi scris de către un participant sau pe o tablă/tabel/șablon online, sau le puteți cere să răspundă la această întrebare individual.

Dacă ai aveți ocazia, puteți discuta fiecare dintre aceste contribuții cu grupul în plen.

Pasul 3

Rugați toți participanții să cerceteze videoclipuri pe internet despre serviciile bancare online. Informațiile colectate pot fi adăugate la lista care a fost creată la pasul 2.

Pasul 4

Încurajează-ți participantul să aleagă câteva instituții bancare cu ale căror sisteme online ar dori să se familiarizeze. Desigur, puteți alege opțiunea de online banking a băncii lor individuale. Cercetarea video, cu tutoriale online este recomandată.

Pasul 5

Faceți un rezumat al regulii de siguranță (vezi Anexa).

Evidențiați ce se poate și ce nu poate fi cerut de la instituțiile bancare sau, în cazul cumpărăturilor online, de la utilizatori.

Transmiteți această regulă într-un mod atrăgător și distribuiți-o în grup. (e.g. editați un poster comun și furnizați-l ca trainer și împărtășiți participanților online)

Pasul 6

Discutați întrebările de reflecție cu participanții.

Recomandări pentru implementare

- » Scopul acestei activități nu este, în primul rând, de a convinge participanții să aleagă online banking, ci de a oferi informații pentru a-și depăși temerile față de această tehnică și pentru a împuternici persoanele să folosească online banking după ce s-au pregătit temeinic.
- » Dacă aveți ocazia, puteți organiza seminarii ulterioare în care participanții care au încercat serviciile bancare online își pot împărtăși primele experiențe.

Întrebări de reflecție

- Te simți mai în siguranță atunci când te gândești la online banking acum?
- Conceptul de online banking este mai clară pentru dvs. acum?
- Crezi că acum ai putea să utilizezi online banking cu mai multă încredere?
- Dacă vrei să încerci online banking, cui poți cere ajutor/sprijin?

Evaluarea Modulului

Test pentru autoevaluare pentru modulul 9

Chestionarul evaluează măsura în care au fost atinse obiectivele de formare.

 <https://forms.gle/kHphuJEzTt98SwpL8>

Fisa de lucru

Sunt formulate întrebări cheie, iar cursanții stabilesc ipoteze, elaborează proceduri pentru a-și testa ipotezele și își prezintă constatările. Răspunsurile lor oferă baza pentru discuții și identificarea posibilelor concepții greșite sau lacune în înțelegere.

 <https://forms.gle/ouLnaxijfTLS8WzL7>

Proiect-Activitate

Cursanții sunt capabili să rezolve o sarcină practică prin aplicarea creativă, independentă și orientată către rezultate a cunoștințelor, abilităților și competențelor dobândite.

Sarcinile proiectului pot fi rezolvate în grupuri mici (dacă modulele sunt finalizate într-un curs de formare)/sau individual.

Puteți găsi sugestii aici, sarcinile specifice proiectului trebuie să fie personalizate în funcție de nevoile și nivelul de cunoștințe al grupului țintă, precum și de obiectivele care trebuie atinse.

- Videoclipuri despre probleme de confidențialitate (în mod similar descrierilor elaborate la curs) în spații deschise. Opiniile/transferul de cunoștințe ale participanților pot fi adăugate și la sfârșitul filmelor. Aceste videoclipuri pot fi folosite ulterior ca materiale didactice.
- Organizați împreună cu participanții câteva evenimente comunitare de practică în comunitatea persoanelor în vârstă. Participanții, cu sprijinul tău, pot face prezentări mai scurte colegilor despre gestionarea parolelor sau online banking și împărtășesc câteva lecții practice pe care le-au dobândit deja.
- Pagina de socializare pentru persoanele în vârstă- susține creația unei pagini social media pentru persoanele în vârstă, unde sunt distribuite în mod regulat postări scurte despre cele mai importante probleme de confidențialitate. Participanții pot face mai întâi o listă de subiecte: cu cât sunt mai specifice, cu atât mai bine.

Chestionar

Cursanții vor răspunde la sfârșitul modulului pentru a măsura impactul general al programului de formare. Acestea pot fi compilate și sub formă de întrebări test cu mai multe răspunsuri posibile.

 <https://forms.gle/dNLYiZTz4eMqCqq6>

Validarea Modulului

La sfârșitul Modulului, cursanții vor fi dobândit

Cunoștințe:

Cursanții sunt capabili să:

- înțeleagă sensul datelor cu caracter personal și al confidențialității,
- identifice diferite forme de criminalitate cibernetică,
- gestioneze în mod conștient setările lor individuale pe diverse platforme,
- știe exact ce condiții minime sunt necesare pentru a evalua un site web securizat,
- aplice cunoștințe solide despre gestionarea parolelor și a aplicațiilor bancare online.

Aptitudini:

Cursanții sunt capabili să:

- folosească parole sigure în mod conștient
- recunoască cazurile în care intimitatea cuiva este încălcată.
- raporteze organizațiilor corespunzătoare dacă observă că parolele sau datele lor au fost manipulate greșit.
- Controleze propriile activități online într-un mod responsabil.

Competențe:

Cursanții sunt capabili să:

- gestioneze propriile parole și datele personale în mod responsabil,
- susțină și să apere intimitatea propriei persoane,
- respecte confidențialitatea altor utilizatori,
- utilizeze avantajele aplicațiilor și site-urilor online fără teamă, dar cu atenție.



ANEXA pentru Modulul 9

Educație media și confidențialitate

Test de nivel de intrare - Educație media și confidențialitate

Întrebarea 1: Este sigur să utilizați aceeași parolă pentru mai multe conturi online.

- a. Adevărat
- b. Fals

Întrebarea 2: Care dintre următoarele este o practică recomandată pentru protejarea informațiilor personale online?

- a. Partajarea de informații personale pe platformele de social media.
- b. Păstrarea informațiilor personale salvate pe calculatoare publice.
- c. Actualizarea regulată a setărilor de confidențialitate pe conturile de rețele sociale.
- d. Făcând clic pe atașamente de e-mail necunoscute.

Întrebarea 3: Serviciile bancare online nu sunt sigure pentru persoanele în vârstă.

- a. Adevărat
- b. Fals

Întrebarea 4: Setările de confidențialitate permit persoanelor să controleze cine își poate accesa informațiile personale pe platformele de rețele sociale.

- a. Adevărat
- b. Fals

Correct answers:

Întrebarea 1: b) Fals

Întrebarea 2: c) Actualizarea regulată a setărilor de confidențialitate pe rețelele sociale

Întrebarea 3: b) Fals

Întrebarea 4: a) Adevărat

Test de nivel de ieșire - Educație media și confidențialitate

Întrebarea 1: Setările de confidențialitate și permisiunile, cum ar fi cookie-urile, nu au niciun impact asupra protecției informațiilor personale online.

- a. Adevărat
- b. Fals

Întrebarea 2: Care dintre următoarele NU este o regulă de bază pentru asigurarea confidențialității online și protecției informațiilor personale?

- a. Evitați partajarea informațiilor personale pe platformele de social media
- b. Folosiți parole puternice și unice pentru diferite conturi online
- c. Faceți clic pe linkuri suspecte sau descărcați fișiere din surse necunoscute
- d. d) Păstrați software-ul și programele antivirus actualizate

Întrebarea 3: Serviciile bancare online sunt o opțiune sigură pentru persoanele în vârstă, iar acestea ar trebui să se simtă încrezătoare în utilizarea acestora.

- a. Adevărat
- b. Fals

Întrebarea 4: Care dintre următoarele acțiuni poate ajuta la păstrarea în siguranță a datelor cu caracter personal?

- a. Folosind aceeași parolă pentru mai multe conturi online.
- b. Partajarea de informații personale pe platformele de social media.
- c. Deschiderea atașamentelor de e-mail sau clic pe linkuri suspecte.
- d. Actualizarea regulată a parolelor și utilizarea parolelor sigure și unice pentru fiecare cont online.

Răspunsuri corecte:

Întrebarea 1: b) Fals

Întrebarea 2: c) Faceți clic pe linkuri suspecte sau descărcați fișiere din surse necunoscute

Întrebarea 3: a) Adevărat

Întrebarea 4: c) Actualizarea regulată a parolelor și utilizarea parolelor sigure și unice pentru fiecare cont online.

Activitate 1#: Cum să păstrați și să utilizați parolele în siguranță?

Pasul 2

Link-uri pentru parola de siguranță:

 <https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/1/>

 <https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password>

 <https://terranovasecurity.com/how-to-create-a-strong-password-in-7-easy-steps/>

 <https://www.rhsb.com/your-passwords-hackable/>

Activitate 2#: Păstrați informațiile personale în siguranță – povești despre confidențialitate

Scenariul 1:

Bill se întâlnește cu vechii săi prieteni și colegi într-o cafenea de două ori pe săptămână. Între timp, a vrut să discute ceva cu alte persoane de pe site-urile de socializare. S-a autentificat cu parola lui simplă și până acum spunea câteva litere cu voce tare pentru a se asigura că face totul bine. Prietenii lui s-au uitat și la telefonul său mobil. Ulterior, s-a dus la toaletă și și-a lăsat telefonul mobil pe masă pentru că nu a vrut să-l ia cu el ca să nu îl ude. Când s-a întors, prietenii lui erau ocupați să discute pe telefonul său mobil. Ce s-ar putea întâmpla mai departe?

Raspunsuri posibile:

- Dacă prietenii de pe chat nu au menționat că nu sunt proprietarul telefonului mobil, acest lucru poate duce la neînțelegeri neplăcute.
- Ar putea fi trimise și mesaje deranjante.
- Conexiunile importante pot fi anulate sau pot fi realizate cele nedorite.

Datele importante pot fi stocate pe un telefon mobil deblocat, ce ar putea fi folosit de utilizatorii rău intenționați, în scopuri nedorite.

Recomandări:

- Nu lăsați niciodată telefonul mobil nesupravegheat.
- Utilizați o parolă puternică
- Nu rostiți niciodată datele cu voce tare în locuri publice.

Scenariul 2:

Sylvia își folosea laptopul în camera comunității. Georg a avut niște vizitatori, dar ea nu-i cunoștea. Sylvia s-a conectat la laptop, pentru a vorbi cu prietenii ei și pentru a împărtăși câteva fotografii din vacanța cu nepoții ei. Daniel și Michael, vizitatorii, priveau tot timpul la laptopul ei. După o oră, Sylvia a vrut să bea un pahar cu apă și s-a dus la bucătărie. Și-a lăsat laptopul pe masă. A schimbat câteva vorbe cu ceilalți în bucătărie și s-a întors în 10 minute. Seara primise deja 6 mesaje urâte de la prieteni, după conversația plăcută de după-amiază. Ce s-ar putea întâmpla?

Raspunsuri posibile:

- Vizitatorii au trimis mesaje prietenilor Sylviei.
- Sylvia probabil nu s-a dezabonat de la chat.
- Probabil că nu are o parolă pe care să o introducă pe laptop sau este prea slabă.

Recomandări:

- Nu lăsați niciodată dispozitivele personale nesupravegheate
- Utilizați o parolă sigură
- Publicați regulile comunității în spații deschise

Scenariul 3

Dorothea plecase cu prietena ei la un restaurant, pentru prânz. Erau doar câteva locuri, așa că doi bărbați le-au rugat să stea la celălalt capăt al mesei. După 15 minute au avut ocazia să se așeze la o altă masă și să lase bărbații în urma lor. Dar puțin mai târziu Dorothea a observat că și-a lăsat geanta cu telefonul mobil pe cealaltă masă. Nu avea un cod complicat (1234) și online banking-ul său era deschis, pentru că a verificat dacă are destui bani în cont chiar înainte de prânz. Ce s-ar putea întâmpla mai departe?

Raspunsuri posibile:

- Din păcate, în acest caz, toate datele de conectare pot fi furate, iar în cel mai rău caz, datele bancare ale Sylviei pot fi folosite pentru a-și transfera banii și contul integral într-un alt cont sau pentru a plăti sume mici sau mari, în mod regulat de aici. Ea ar trebui să schimbe imediat toate detaliile de conectare, eventual interzicând utilizarea contului pentru o perioadă scurtă de timp.

Recomandări:

- Nu lăsați niciodată dispozitivele personale nesupravegheate
- Utilizați o parolă sigură
- Dacă nu sunteți sigur că vă veți supraveghea întotdeauna instrumentele, nu utilizați aplicații sensibile în spații deschise (de exemplu, online banking și alte servicii online importante) și deconectați-vă când ați terminat de utilizat. În acest caz, nu stocați niciodată parolele pe dispozitivul dvs. personal.

Activitatea 3#: Servicii bancare online fără teamă

Pasul 5:

Ce pot face pentru a-mi păstra banii și identitatea în siguranță?

În general, operațiunile bancare online sunt sigure, dar există pași pe care îi puteți lua pentru a vă îngriji banii și identitatea:

- » **Utilizați o parolă puternică**, care evită cuvintele, numerele sau modelele de tastatură obișnuite (cum ar fi „parolă” sau „123456”). Nu includeți în parola dvs. informații personale, cum ar fi numele dvs., data nașterii sau detaliile oricărui membru al familiei. [Faceți clic aici](#) pentru a afla mai multe despre cum să alegeți o parolă puternică.
- » **Nu utilizați aceleași parole pentru conturi diferite.**

- » **Nu partajați niciodată parola completă sau numărul PIN.**
Băncile nu vă vor cere niciodată codul PIN sau parola completă – în schimb, vă vor cere anumite numere sau litere, de exemplu, primul și al treilea caracter.
- » **Deconectați-vă întotdeauna de la sesiunea dvs. bancară online,** mai ales dacă utilizați un dispozitiv partajat. Dacă utilizați un computer public, cum ar fi un computer de bibliotecă, fiți deosebit de precauți – este posibil să nu aibă nivelul potrivit de software de securitate. Dacă aveți nevoie, întrebați personalul bibliotecii pentru mai multe informații.
- » **Utilizați numai rețele Wi-Fi securizate pentru a vă accesa serviciile bancare online.** Dacă utilizați o rețea publică, cum ar fi cele din cafenele sau gări, este posibil ca persoanele din aceeași rețea să vă acceseze detaliile.
- » **Verificați-vă soldul și tranzacțiile în mod regulat.** Dacă există o tranzacție pe care nu o recunoașteți, raportați-o imediat băncii.
- » **Verificați în mod regulat dacă datele dumneavoastră personale sunt corecte și actualizate.**

Resursă:

 [Servicii bancare online pentru persoanele în vârstă | Vârsta Marea Britanie](#)

QUIZ DE ALFABETIZARE MEDIA ȘI CONFIDENȚIALITATE



Acest test face parte din Programul de formare Information Matters (cofinanțat de Programul Erasmus+ al Uniunii Europene), Modulul 9 - Media Literacy & Privacy for Older People. (Vă rugăm să alegeți răspunsul corect.) (Informații pentru formatori: răspunsurile corecte sunt marcate cu x, nu uitați să adaptați testul pentru grupul dvs. țintă.)

» Parola mea

- a. trebuie generată de mine (X)
- b. este generată pentru mine, de către asistenții mei sociali/medici/rudele/asistentă

» O parolă

- a. o nu poate fi schimbată niciodată
- b. o trebuie schimbată regulat. (X)

» Se recomandă schimbarea parolelor importante

- a. o cel puțin o dată la 2 luni
- b. o cel puțin anual
- c. o cel puțin la fiecare 2 ani



» O parolă puternică ar trebui să conțină

- a. litere mici (x)
- b. litere mari (x)
- c. doar majuscule
- d. caractere speciale (x)
- e. doar caractere speciale
- f. numere (x)
- g. min. 8 caractere (x)
- h. max. 8 caractere
- i. datele personale
- j. numele mamei mele

» Ar trebui întotdeauna să

- a. păstrez parola aproape de computerul meu sau alte dispozitive
- b. păstrez parolele secrete (X)
- c. împărtășesc parola cu asistentul meu social/asistenta/rudele/prietenii.

» Când îmi folosesc dispozitivele mobile în spații deschise,

- a. trebuie să-l dau prietenului meu pentru a-l urmări când am altceva de făcut
- b. nu ar trebui să-l las niciodată deblocat, astfel încât nimeni să nu aibă acces la datele mele (X)
- c. sunt mai în siguranță decât acasă.

- » **Dacă vreau să aranjez ceva cu banca mea,**
 - a. banca nu va cere codul PIN complet sau parola. (X)
 - b. banca îmi va cere codul PIN complet și parola.
- » **Este în regulă, să accesezi online banking**
 - a. de pe un computer privat sigur de acasă (X)
 - b. de pe rețelele publice, cum ar fi cafenelele sau gările
- » **Este ok**
 - c. să folosesc aceeași parolă pentru conturile mele
 - d. Să utilizez întotdeauna parole diferite pentru conturile mele (X)

CHESTIONAR PRIVIND ALFABETIZAREA ȘI CONFIDENȚIALITATEA ÎN MASS-MEDIA



Acest chestionar face parte din Programul de formare Information Matters (cofinanțat de Programul Erasmus+ al Uniunii Europene), Modulul 9 - Educație media și confidențialitate pentru persoanele în vârstă.

Information Matters

- » **Conținutul de formare despre alfabetizarea media și confidențialitatea a îndeplinit așteptările dvs.?**
 - a. da
 - b. nu
- » **A fost adecvat conținutul de prezentări/explicații și activități?**
 - a. da
 - b. nu
- » **Ai învățat ceva nou?**
 - a. da
 - b. nu



Dacă da, vă rugăm să furnizați mai multe detalii despre cunoștințele/competențelor dumneavoastră. Eu pot sa...

Dacă nu, vă rugăm să furnizați detalii despre cunoștințele/aptitudinile/competențelor lipsă:

» **Cursul a fost practic / ușor de aplicat?**

- a. da
- b. nu

» **Ați observat vreun impact pozitiv al acestui curs asupra problemelor dvs. de confidențialitate? Le puteți specifica?**

» **Pe baza acestei pregătiri, ați fi interesat să vă antrenați în alte abilități?**

- a. da
- b. nu

» **Aveți sugestii pentru a îmbunătăți acest curs?**

Dacă da/nu, vă rugăm să furnizați mai multe detalii, de ce?





information matters

contact@informationmatters.eu

Finanțat de Uniunea Europeană. Punctele de vedere și opiniile exprimate aparțin, însă, exclusiv autorului (autorilor) și nu reflectă neapărat punctele de vedere și opiniile Uniunii Europene sau ale Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.

Număr acord: 2022-1-BG01-KA220-ADU-000085514



**Cofinanțat de
Uniunea Europeană**