



MOBILE MONEY

Modulul 2

Securitate & Prevenire



Cofinanțat de
Uniunea Europeană

Acest proiect este finanțat de Uniunea Europeană. Conținutul prezentării reflectă exclusiv opiniile autorului (autorilor) și nu reprezintă în mod necesar poziția oficială a Uniunii Europene sau a Agenției Executive Europene pentru Educație și Cultură (EACEA). Uniunea Europeană și EACEA nu pot fi considerate responsabile pentru conținutul prezentat. Număr proiect: 2023-1-RO01-KA220-ADU-000157797





Parteneri



ZAVOD IZRIIS

Zavod IZRIIS, Slovenia



Asociația Four Change, Romania



E-SENIORS: INITIATION DES
SENIORS AUXNTIC
ASSOCIATION, France



GREEK UNIVERSITIES NETWORK

GUnet, Greece



NICIODATĂ SINGUR
prietenii vârstnicilor

Asociația Niciodata Singur –
Prietenii Varstnicilor, Romania



Fundació Gesmed Fundació de
la Comunitat Valenciana, Spain



Cofinanțat de
Uniunea Europeană



**MOBILE
MONEY**

Module

1. Competențe fundamentale în utilizarea tehnologiilor digitale

2. Securitate & Prevenire

3. Gestionarea unui cont bancar online

4. Soluții pentru a primi și trimite bani online

5. Utilizarea unui card bancar pentru achiziții online de bunuri și servicii

6. Efectuarea plăților online pentru taxe și facturi



Cofinanțat de
Uniunea Europeană



Secțiunea 1

Introducere

Obiective

La finalul acestei secțiuni, veți deține informații despre:

- ✓ Obiectivele de învățare și conținutul acestui modul de formare
- ✓ Metodologia de instruire utilizată și durata modului





Competențe

După finalizarea acestui modul:

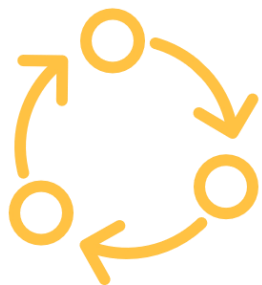
- Veți dobândi abilitățile necesare pentru a utiliza soluții de plată mobilă în siguranță și cu încredere:
 - ✓ Veți înțelege ce este securitatea online.
 - ✓ Veți înțelege ce înseamnă date personale și sensibile.
 - ✓ Veți înțelege noțiunile de confidențialitate și securitate.
 - ✓ Veți ști ce sunt spam-ul și phishing-ul prin e-mail și cum să reacționați la ele
- ✓ Veți cunoaște criteriile pentru a decide ce link-uri sunt sigure
- ✓ Veți cunoaște ce drepturi aveți în mediul online
- ✓ Veți înțelege ce este GDPR și de ce avem nevoie de el
- ✓ Veți ști cum să aplicați măsuri de securitate și de prevenire



Conținutul modulului de formare

1. Prezentarea sesiunii: durată, obiective, conținut și metodologie
2. Siguranță online, date personale, date sensibile, confidențialitate și securitate
3. Recunoașterea spam-ului și a phishing-ului și modalități de răspuns
4. Cunoașterea drepturilor dvs. online, exemplul GDPR
5. Cum vă protejați când intrați online
6. Test de verificare a cunoștințelor





Metodologie și Durată

Durată: 4 ore

- Sesiune față în față: 2 ore
- Pregătire online: 2 ore

Metodologie

- Sesiuni active și participative
- Sesiuni față în față:
 - ✓ Dialog
 - ✓ Joc de rol & Simulări
 - ✓ Lucru în echipă
- Pregătire online:
 - ✓ Videoclipuri selectate
 - ✓ Aplicarea practică a lucrurilor discutate în clasă
 - ✓ Activități de lucru în echipă
 - ✓ Simulări





Secțiunea 2

Siguranță online și date personale

Obiective

La finalul acestei secțiuni, veți ști:

- ✓ Ce este siguranța online
- ✓ Ce sunt datele personale și exemple ale acestora



Siguranța online

Când intră online, utilizatorii sunt expuși la multe **riscuri de securitate**. Odată ce un utilizator trimite date online (apeluri video sau mesaje vocale, e-mail sau numere de card de credit, site-uri web), acesta **nu are niciun control asupra persoanelor care au acces la aceste date**. Datele trec prin mai multe servere, routere și dispozitive unde orice hacker, furnizor de servicii sau agent guvernamental le poate accesa și citi.

Prin urmare, este extrem de important ca utilizatorii de internet să ia măsuri pentru:

- Protejarea **datelor lor personale sensibile**;
- Utilizarea instrumentelor și serviciilor online, cum ar fi criptarea datelor, care **asigură confidențialitatea și securitatea** informațiilor clienților atunci când comunică online cu aceștia.



Ce înseamnă date cu caracter personal?

Date cu caracter personal sunt orice informații specifice referitoare la o **persoană fizică vie, identificată sau identificabilă**.

Diverse informații care, împreună, pot fi folosite **pentru a identifica o anumită persoană**, sunt, de asemenea, date personale.



Exemple de date cu caracter personal

Date cu caracter personal sunt următoarele:

- Nume și prenume;
- Adresa de domiciliu;
- Adresa de email, cum ar fi
prenume.nume@companie.com;
- Date de localizare, cum ar fi funcția activată pe un telefon mobil);
- Numărul cărții de identitate;
- Adresa IP (Internet Protocol);
- Un ID de cookie;
- ID-ul de publicitate al telefonului tău;
- Date deținute de un spital sau de un medic, care pot contribui la identificarea certă a unei persoane.



Secțiunea 3

Date sensibile, confidențialitate și securitate

Obiective

După completarea acestei secțiuni, veți ști:

- ✓ Ce date cu caracter personal sunt considerate sensibile.
- ✓ Ce sunt datele personale sensibile și datele financiare.
- ✓ Ce reprezintă noțiunile de confidențialitate și securitate.
- ✓ Ce este confidențialitatea online și cum să fii în siguranță online.



Ce date cu caracter personal sunt considerate sensibile?

Următoarele date cu caracter personal sunt considerate „**sensibile**” și sunt supuse unor condiții specifice de prelucrare:

Date
personale
sensibile

- Date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice;
- Poze, videoclipuri;
- Apartenența la un sindicat;
- Date genetice, date biometrice, prelucrate în scopul identificării unei ființe umane;
- Date privind sănătatea;
- Date privind viața sexuală sau orientarea sexuală a unei persoane.



Date financiare sensibile

- Contul și parola pentru un sistem de e-banking
- Codul CCV, data expirării unui card de credit sau de debit
- Codul PIN al telefonului dvs. mobil

→ Exemple și exerciții



[Imagine redgreystock Freepik](#)



Ce este confidențialitatea?

Confidențialitatea se referă la:

- Modul în care **ne controlăm datele cu caracter personal** și
- modul în care **acestea sunt utilizate** de către cei care le-au primit, într-un mod securizat.

Cel mai des ne confruntăm cu **politicile de confidențialitate** atunci când ni se cere să le citim și să le acceptăm, când vizitează un site sau descarcăm o aplicație nouă pe telefonul mobil.



Ce este securitatea?

Securitatea se referă la **modalități de protejare a datelor personale** împotriva **accesului neautorizat**, fie pe dispozitivul dvs., pe serverul web de la distanță sau în timpul comunicării pe internet.

Este recomandat să utilizăm **controale de securitate** la nivel tehnic pentru a limita cine poate accesa informațiile. Aceste controale sunt în vigoare:

- Pe dispozitivele noastre (PC, tabletă, telefon mobil), de exemplu, aplicând actualizări ale sistemului de operare și ale software-ului, utilizând parole puternice;
- Pe serverul web de la distanță, de exemplu, utilizați parole puternice;
- Atunci când trimiteți informații pe internet, de exemplu, utilizați protocolul securizat **https**.



Securitate și Confidențialitate

- Securitatea se referă la **protejarea datelor**, în timp ce confidențialitatea se referă la **protejarea identității utilizatorilor**.

De exemplu, personalul spitalelor și clinicilor utilizează sisteme securizate pentru a comunica cu pacienții despre starea lor de sănătate, în loc să trimită informații prin intermediul conturilor personale de e-mail. Acest tip de comunicare este un exemplu de securitate.

- Pe de altă parte, politica și reglementările privind confidențialitatea ar putea limita accesul la dosarele medicale ale pacienților la **anumiți membri ai personalului spitalului**, cum ar fi medicii, asistentele și asistenții medicali.

- **Este posibil să existe securitate fără confidențialitate.**

Într-adevăr, de exemplu, datele cu caracter personal pot fi transmise și stocate în siguranță pe un site web, dar site-ul web le poate vinde în continuare.

- **Nu este posibil să existe confidențialitate fără securitate.**

Într-adevăr, de exemplu, un hacker ar putea obține acces neautorizat la dispozitivul dvs., la serverul web sau la datele transmise și v-ar putea fura datele personale.



Secțiunea 3

Spam și phishing

Obiective

După completarea acestei secțiuni, veți ști:

- ✓ Ce sunt spam-ul și phishing-ul
- ✓ Cum să identificați spam-ul
- ✓ Când un link poate fi accesat în siguranță



[Imagine vectorjuice Freepik](#)



Cofinanțat de
Uniunea Europeană

Ce sunt spam-ul și phishing-ul

Cu siguranță ați primit e-mailuri enervante de la un **expeditor necunoscut**, de obicei de natură comercială.

Aceste **e-mailuri pot fi periculoase** deoarece pot conține link-uri care conduc la site-uri de phishing, site-uri care găzduiesc programe malware sau care conțin programe malware ca atașament.

Prin urmare, **nu deschideți niciun fișier și nu apăsați click pe niciun link în aceste cazuri**. Nu divulgați niciodată datele dvs. personale, detaliile contului de e-banking (orice nume de utilizator, parolă) sau detaliile cardului dvs. de credit/debit, cum ar fi data expirării și cele 3 cifre ale codului CCV.

Aceasta practică se numește **phishing (a pescui)**: infractorii trimit e-mailuri cu aspect oficial pentru a vă păcăli să dezvăluiți detalii care pot fi folosite pentru furtul de identitate.



Cum identific spam-ul?

Un e-mail este suspect dacă conține unul sau mai multe dintre următoarele elemente:

- Greșeli gramaticale și de ortografie
- E-mailuri într-o limbă străină
- Numele expeditorului lipsește
- Nevoia urgentă de acțiune - în special combinată cu o amenințare



- Invitația de a introduce date personale (de exemplu PIN)
- Solicitarea de a deschide un fișier



Ce să faceți sau ce să nu faceți?

- ✓ Evitați să deschideți fișiere din e-mailuri dacă acestea nu au fost scanate de un program antivirus.
- ✓ Nu uitați să vă deconectați, mai ales dacă utilizați un computer public comun.
- ✓ Ștergeți toate e-mailurile de la persoane necunoscute.
- ✓ Nu răspundeți niciodată la spam!
- ✓ Nu dați clic pe niciun link din e-mailurile spam!





Activitate: Este link-ul sigur de accesat?

Decideți dacă link-ul este sigur pentru accesare:

Să presupunem că primiți un e-mail de la o bancă care vă cere să accesați un link precum cel de mai jos și să trimiteți date personale, cum ar fi numele de utilizator, parolele și detaliile cardului de credit.

<http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnyTLRIk2703ToIFpo2vd2MKt5gB6dY/2FnC6T5iVsCdbcug7l6pkTad-2FBfACSlC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpny-asDvdva>

- 1. Nu vă grăbiți, gândiți-vă de două ori și decideți dacă acest link este sigur de accesat.*
- 2. Gândiți-vă la motivele pentru care ați luat această decizie.*





Activitate: Este sigur să vizitați acest link? (2)

Răspunsul: Acest link **nu este sigur** din mai multe motive:

- Acesta utilizează http în loc de https.
- Numele de domeniu nu este legat de numele oficial al băncii.
- Link-ul este suspect de lung.
- Numele de domeniu al linkului este diferit de numele de domeniu al adresei de email a expeditorului.
- O bancă reală nu va solicita niciodată nume de utilizator, parole sau detalii ale cardului de credit.



Secțiunea 4

Drepturile tale online

Obiective

După completarea acestei secțiuni, veți ști:

- ✓ Care vă sunt drepturile și obligațiile digitale
- ✓ Ce este GDPR și de ce avem nevoie de el



Suntem cetățeni digitali!

Cetățenii digitali se pot bucura de drepturi privind viața privată, securitatea, accesul și incluziunea, libertatea de exprimare.

Cu toate acestea, odată cu aceste drepturi vin și anumite responsabilități, cum ar fi chestiuni etice, nevoia de empatie și alte asemenea responsabilități, pentru a asigura un mediu digital sigur pentru toți.



*Acum suntem cu toții
conectați prin internet, ca niște
neuroni într-un creier uriaș.*

Stephen Hawking

[Imagine storyset Freepik](#)



Ce este GDPR și cine trebuie să îl respecte?

Ce este GDPR?

- **Regulamentul General de Protecția Datelor (GDPR)** este un regulament al Uniunii Europene care a fost pus în aplicare la 25 mai 2018 și care impune organizațiilor să protejeze datele cu caracter personal și să respecte dreptul la viață privată al oricărei persoane aflate pe teritoriul UE.

Cine trebuie să se conformeze GDPR?

- Orice organizație care prelucrează date cu caracter personal ale persoanelor din UE.
- „**Prelucreare**” este un termen larg care acoperă aproape orice se poate face cu datele: colectare, stocare, transmitere, analiză etc.
- „**Datele cu caracter personal**” sunt orice informații care se referă la o persoană, cum ar fi nume, adrese de e-mail, adrese IP, culoarea ochilor, convingeri politice etc.



Cine este obligat să respecte GDPR-ul?

Chiar dacă o organizație nu are nicio legătură directă cu UE, dar prelucrează datele cu caracter personal ale persoanelor din UE (de exemplu, prin urmărirea activității pe site-ul său web), aceasta tot trebuie să respecte GDPR.

GDPR nu se limitează la societățile cu scop comercial.



[Imagine pch.vector Freepik](#)



Este GDPR ceva pozitiv?

- GDPR există pentru a vă proteja drepturile în calitate de utilizator.
- Este bine să știți cu ce sunteți de acord și ce înseamnă un modul cookie.
- Gestionarea corectă a utilizatorilor vulnerabili nu este doar o cerință a legii, ci și un lucru corect din punct de vedere social și o mișcare de afaceri inteligentă.



[Imagine Freepik](#)



Secțiunea 5

Cum vă puteți proteja în avans

Obiective

După completarea acestei secțiuni, veți ști:

- ✓ Cum vă puteți proteja prin identificarea site-urilor sigure, a link-urilor, a modulelor cookie, a consimțământului



[Imagine vectorjuice](#) [Freepik](#)

Câteva exemple pentru a fi în siguranță (1/3)

- Evitați să plătiți pe cineva prin transfer bancar, Western Union, ordin de plată sau carduri cadou. Escrocii solicită adesea aceste tipuri de plăți, deoarece acestea nu lasă urme.
- Nu împărtășiți niciodată parolele dvs. cu nimeni online. Doar cu persoane de încredere!
- Fiți sceptici cu privire la orice lucru urgent. Escrocii doresc adesea să acționați înainte de a avea timp să vă gândiți critic la situație. Amintiți-vă să faceți o pauză și poate să vă îndepărtați de calculator în loc să intrați în panică dacă aveți impresia că ceva este suspect și nu sunteți sigur cum să procedați.
- Apăsați imediat pe X sau Nu pentru a închide orice site web sau pop-up despre viruși sau tombole cu premii.



Câteva exemple pentru a fi în siguranță (2/3)

- Sunați o persoană dragă sau căutați sfaturi online.
- Căutați pe Google pentru a vedea dacă alte persoane au raportat astfel de escrocherii.
- Asigurați-vă că site-urile web au **https://** listat în fața lor. Litera „s” indică faptul că site-ul este securizat. Numele ar trebui să aibă și un mic lacăt lângă el.
- Feriți-vă de tot ceea ce pare prea frumos ca să fie adevărat.
- Luați în considerare activarea autentificării cu multi-factor (factori multipli). Aceasta vă cere fie să introduceți un cod (trimis prin SMS sau e-mail), fie să utilizați o aplicație pentru a vă conecta la unele dintre conturile dvs., inclusiv rețelele sociale sau portalurile bancare. Acest lucru poate împiedica hackerii să se conecteze.



Câteva exemple pentru a fi în siguranță (3/3)

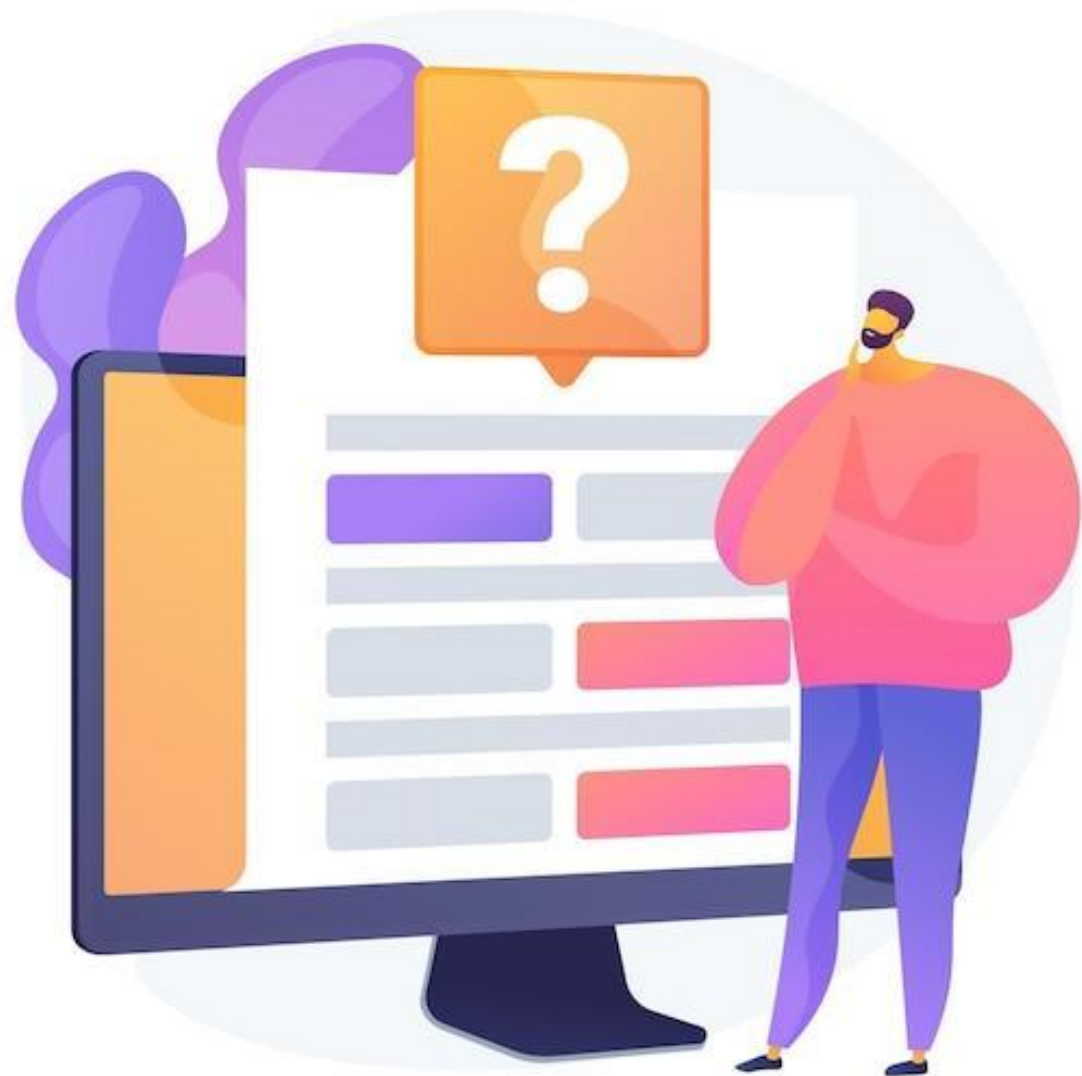
- Se pot lua mai multe măsuri de precauție pentru a evita escrocheriile.
- Nimeni nu trebuie să se teamă să continue să folosească internetul, atâta timp cât deține cunoștințele necesare pentru a-l utiliza în siguranță.
- Găsiți un spațiu sigur în comunitatea sau cercul dvs. social, unde vă simțiți confortabil să discutați despre aceste probleme fără teama de a fi judecați.

Dacă ați fost deja victima unei înșelătorii, iată câteva măsuri pe care le puteți lua:

- Sunați la bancă. Aceasta vă poate îngheța contul astfel încât nimeni să nu vă poată accesa fondurile și vă poate emite un nou card de debit. Dacă banii au fost deja furați, puteți vedea dacă banca poate anula acele tranzacții și vă poate returna fondurile.
- Luați în considerare depunerea unei plângeri la poliție.



Test de verificare a cunoștințelor



1. Care dintre următoarele parole este cea mai puternică?

Un singur răspuns este corect!

A. John1234

B. John1990

C. John051190

D. J0Hn!2nO



2.Care dintre următoarele reprezintă date personale?

Un singur răspuns este corect!

A. Adresa IP

B. Adresa de e-mail

C. Toate

D. Cookies ID în browser



3. Când pictograma cu lacăt apare în browser, înseamnă că browser-ul a blocat pagina deoarece nu este sigură.

Da, afirmația este corectă.

Nu, afirmația este greșită.



4. Care dintre următoarele NU sunt date personale sensibile:

Un singur răspuns este corect!

A. Poze

B. Adresa de domiciliu

C. Informații legate de sănătate

D. Opinii politice



**5. Poate fi expeditorul un indicator al
faptului că un e-mail este spam?**

Da

Nu



6. Ce nu trebuie să faceți niciodată dacă primiți un e-mail spam?

Un singur răspuns este corect!

A. Să ștergeți acest e-mail

B. Să verificați expeditorul

C. Să verificați linia de referință

D. Să răspundeți și să întrebați dacă este spam





IMOBILE
MONEY

Felicitări!
Ați completat acest modul!



**Cofinanțat de
Uniunea Europeană**

Acest proiect este finanțat de Uniunea Europeană. Conținutul prezentării reflectă exclusiv opiniile autorului (autorilor) și nu reprezintă în mod necesar poziția oficială a Uniunii Europene sau a Agenției Executive Europene pentru Educație și Cultură (EACEA). Uniunea Europeană și EACEA nu pot fi considerate responsabile pentru conținutul prezentat.

Număr proiect: 2023-1-RO01-KA220-ADU-000157797