

PROTEJAREA INFORMAȚIILOR PERSONALE ȘI FINANCIARE

16+

SUBIECT: Literație Digitală, Educația Consumatorului

TEMA LECȚIEI: Cum să protejați informațiile personale și financiare online

DURATA: 60 minute

OBIECTIVE DE ÎNVĂȚARE:

Obiectivele principale ale lecției:

Conștientizarea importanței protejării informațiilor personale și financiare online, înțelegerea amenințărilor potențiale și învățarea unor strategii eficiente pentru protejarea împotriva fraudei online și a furtului de identitate.

Competențe dobândite:

- Cunoașterea principalelor amenințări la adresa securității cibernetice (de exemplu, phishing, malware, încălcări ale securității datelor).
- Abilitatea de a recunoaște activitățile, e-mailurile și site-urile web suspecte.
- Conștientizarea practicilor online sigure atunci când se împărtășesc informații personale sau financiare.

MATERIALE/RESURSE NECESARE:

Modulul 5 DIGI-CIVIS

(<https://www.digi-civis.eu/e-learning>);

Proiector și computer pentru prezentare; Acces la internet pentru demonstrație.

Exemple de e-mailuri de phishing, site-uri false.

METODE/TEHNICI:

- Discuții în grupuri mici
- Reflecție personală și autoevaluare
- Discuții în clasă și feedback
- Joc de rol

PREZENTAREA GENERALĂ A PLANULUI DE LECȚIE

PREGĂTIREA LECȚIEI:

- Pregătiți slide-urile de prezentare din MODULUL 5 DIGI-CIVIS.
- Găsiți exemple de e-mailuri de phishing, site-uri frauduloase și site-uri sigure pentru a le prezenta în timpul lecției.
- Creați fișe de lucru care să ghideze elevii prin crearea de parole puternice și identificarea tentativelor de phishing.

DESFĂȘURAREA LECȚIEI:

- Introducere în amenințările online (10 minute): Explicați amenințările online comune (phishing, programe malware, încălcări ale securității datelor) și de ce protejarea informațiilor personale și financiare este esențială.
- Recunoașterea atacurilor de phishing (10 minute): Prezentați exemple de e-mailuri de phishing și site-uri web frauduloase. Discutați despre semnele de avertizare, cum ar fi URL-urile suspecte și solicitările urgente de informații.
- Cele mai bune practici pentru protecție (15 minute): Predați crearea unei parole puternice, utilizarea autentificării cu doi factori și evitarea Wi-Fi-ului public pentru tranzacțiile sensibile. Demonstrați cum să verificați securitatea site-urilor web (de exemplu, „https”, pictograma lacăt).
- Activitate practică „Crearea de parole puternice” (10 minute): Ghidați elevii prin crearea de parole sigure și arătați cum se evaluează gradul de putere.
- Discutarea studiului de caz (10 minute): Treceți în revistă o încălcare a securității datelor din viața reală, discutați impactul acesteia și modul în care practici de securitate mai bune ar fi putut-o preveni.
- Reflecție (5 minute): Elevii identifică o măsură pe care o vor lua pentru a-și îmbunătăți propria securitate online.

INFORMAȚII SUPLIMENTARE:

EU OP, [Shoppingul online în UE](#)
[EU E- Raport Comercial 2023](#)
[Schema DMA](#)
Fiți în siguranță!

ANEXE:

[Protecția datelor în UE \(Video\)](#)
[Literație financiară \(video\)](#)

TEMĂ PENTRU ACASĂ:

Elevii vor face un audit de securitate al propriilor conturi online și vor scrie o reflecție de o pagină cu privire la ceea ce au descoperit și la măsurile pe care le-au luat pentru a-și îmbunătăți securitatea online.

EVALUARE:

Revizuirea temei pentru acasă pentru a evalua capacitatea elevului de a aplica principiile securității online.