

SECURITATEA FINANCIARĂ ÎN MEDIUL DIGITAL

SCOP	Identificarea modalităților de evitare a fraudei financiare în mediul digital
TEMA DIN PROGRAMĂ ȘCOLARĂ/ CURRICULUM PENTRU EDUCAȚIA TIMPURIE LA CARE POATE FI CONECTATĂ	<i>Calitatea în turism și alimentație</i>
GRUPUL ȚINTĂ	Elevii claselor a IX-a
NIVEL DE DIFICULTATE	Mediu
LOCUL DE DESFAȘURARE	Sala de clasă
FORMA DE ORGANIZARE A ACTIVITĂȚII	Frontal, pe echipe
MATERIALELE NECESARE	Flipchart, hârtie, creioane colorate, laptop-uri, tablă inteligentă, conexiune la internet
TIMPUL NECESAR	20 minute

RESURSE

- umane: elevii claselor a IX-a;
- de timp: 20 min;
- de documentare:

https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_ro

[https://ro.wikipedia.org/wiki/Ban_\(mijloc_de_plat%C4%83\)](https://ro.wikipedia.org/wiki/Ban_(mijloc_de_plat%C4%83))

<https://support.microsoft.com/ro-ro/topic/ce-este-s-e-c-u-r-i-t-a-t-e-a-c-i-b-e-r-n-e-t-i-c-%C4%83-8b6efd59-41ff-4743-87c8-0850a352a390>

<https://comunitate.orange.ro/t5/altele-internet-%C8%99i-tv/top-100-cele-mai-vulnerabile-parole-in-2019/m-p/20421>

CE VA ÎNVĂȚA / CE VA
ȘTI SĂ FACĂ ELEVUL
LA SFÂRȘITUL
ACTIVITĂȚII

Să identifice caracteristicile de securitate financiară în mediul digital;

Să identifice modalitățile sigure de a crea parole pentru aplicațiile financiare;

Să verifice dacă un magazin online este sigur;

Să utilizeze în condiții de siguranță cardul în mediul on-line.

DESCRIEREA ACTIVITĂȚII PAS CU PĂS

Pasul 1. Se distribuie fișa de documentare (Anexa 1) despre securitatea cibernetică. Elevii trebuie să definească securitatea cibernetică pe baza fișei de documentare și să identifice cei trei stâlpi de securitate cibernetică (Acronimul "CIA"- Confidențialitate, Integritate, Access).

Pasul 2.

Utilizarea internetului ar trebui să fie sigură. Răspundeți următoarelor întrebări:

1. Cât de sigur este dispozitivul tău? De exemplu , telefon mobil, computer, tabletă.
2. Ce conexiune la internet folosești?
3. Ce programe de calculator și aplicații pentru telefon utilizați?
4. Cât de sigure sunt parolele tale?

Pasul 3.

Experții în securitate recomandă evitarea parolelor care sunt ușor de ghicit. O parolă puternică trebuie să conțină cel puțin 8 caractere diferite. Creați o parolă utilizând: numere, litere mari,

litere mici, simboluri. Notați-o pe flipchart pentru a verifica dacă îndeplinește condițiile unei parole sigure.

NU utilizați în parolă: date importante, numele persoanelor apropiate sau animalelor de companie, numere de telefon, denumirile așezărilor, nume populare de companii.

De exemplu, Samsung.

Astfel de parole nu sunt sigure.

Parole ușor de ghicit, cum ar fi 123456, qwerty, Parole etc. Puteți găsi exemple de parole greșite pe site-ul web <https://comunitate.orange.ro/t5/altele-internet-%C8%99i-tv/top-100-cele-mai-vulnerabile-parole-in-2019/m-p/20421>

Pasul 4.

Cum se verifică siguranța magazinului online?

Vreți să achiziționați mobilier pentru pensiunea „Bucovina de altă dată” și trebuie să comandați de pe următorul site: <https://www.evohoreca.ro/mobilier-horeca>

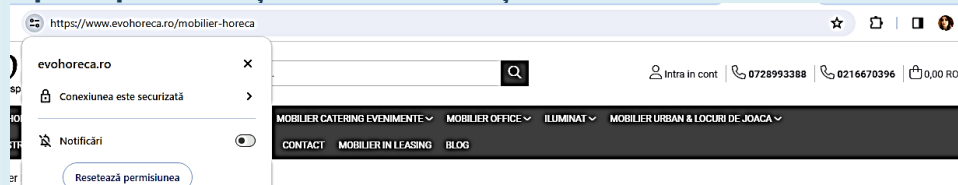
1. Uită-te la adresa site-ului magazinului online! Verifică dacă îndeplinește următoarele condiții înainte de a demara procedura de achiziție:

O adresă de site securizată începe cu https://

O adresă de site web nesigură începe cu http://

2. Veți vedea o pictogramă de lacăt pe pagina de pornire a unui magazin online securizat.

Apasa pe ea! Veți vedea informațiile de securitate ale site-ului.



**NOȚIUNI/ TERMENI DE
EDUCAȚIE
FINANCIARĂ**

Securitate financiară în mediul digital, securitatea dispozitivelor electronice, parole sigure, siguranța magazinului on-line, utilizarea cardului on-line.

FIȘĂ DE DOCUMENTARE

Ce este securitatea cibernetică?

Securitatea cibernetică, numită și securitate digitală, este practica de a proteja informațiile, dispozitivele și activele digitale. Între acestea se numără informațiile personale, conturile, fișierele, fotografiile și chiar banii.

Acronimul „CIA” este utilizat adesea pentru a reprezenta cei trei stâlpi de securitate cibernetică.

Confidențialitate - păstrarea secretelor și asigurarea că doar persoanele autorizate vă pot accesa fișierele și conturile.

Integritate - asigurându-vă că informațiile dumneavoastră sunt ceea ce ar trebui să fie și că nimeni nu a inserat, modificat sau șters lucruri fără permisiunea dvs. De exemplu, modificarea rău intenționată a unui număr într-o foaie de calcul.

Access – Vă asigură că vă puteți accesa informațiile și sistemele atunci când este necesar. Un exemplu de problemă de acces ar fi un atac de tip refuz-serviciu, în care atacurile vă inunda sistemul cu traficul de rețea pentru a face accesarea aproape imposibilă; sau ransomware care vă criptează sistemul și vă împiedică să îl utilizați.

Realizat de: Prof. Andrieș Andreea Claudia

Revizuit de: prof. dr. Vranciu Livia Elena, profesor metodist pentru discipline din aria curriculară Tehnologii