

++++
++++

FUTURE READY 5

DEZVOLTĂM COMPETENȚELE GENERAȚIILOR VIITOARE

Cursuri online gratuite dedicate copiilor de 10 - 14 ani din mediul rural și urban mic

SECURITATE CIBERNETICĂ

Acest booklet este destinat profesorilor care doresc să le ofere elevilor concepte fundamentale despre securitatea cibernetică. Materialul este structurat în mai multe lecții, fiecare concepută pentru o oră de curs de aproximativ 40-50 de minute. Lecțiile includ atât teorie detaliată, cât și activități practice pas cu pas pentru a stimula participarea activă a elevilor și dezvoltarea competențelor digitale sigure.



Proiectul Future Ready este dezvoltat de Simplon România și susținut de Societe Generale Global Solution Centre România ca parte din activitatea companiei de sprijinire a dezvoltării abilităților, nivelului de educație și integrării profesionale a grupurilor vulnerabile.



Global Solution Centre



LECȚIA 1: CE ESTE SECURITATEA CIBERNETICĂ ȘI DE CE ESTE IMPORTANTĂ?

OBIECTIVE:

- Înțelegerea conceptului de securitate cibernetică.
- Identificarea pericolelor din mediul online.
- Conștientizarea importanței protejării datelor personale.

CONȚINUT TEORETIC:

Definiția securității cibernetice:

Securitatea cibernetică se referă la protecția dispozitivelor, datelor și rețelelor împotriva atacurilor și amenințărilor digitale. Aceasta include măsuri de prevenire, detectare și reacție pentru a proteja utilizatorii de accesul neautorizat la informații sensibile.

Importanța securității cibernetice:

- Protejează informațiile personale (parole, conturi bancare, date confidențiale).
- Reduce riscul infectării dispozitivelor cu viruși și malware.
- Asigură o navigare sigură pe internet și protejează identitatea online.

Tipuri de atacuri cibernetice:

Ingineria socială este o tehnică de manipulare utilizată de atacatorii cibernetici pentru a determina o persoană să divulge informații confidențiale, cum ar fi parole, date bancare sau alte informații personale.

- **Phishing:** Emailuri și mesaje false care încearcă să obțină informații personale.
- **Hacking:** Acces neautorizat la conturi și sisteme informatice.
- **Virusuri și malware:** Programe dăunătoare care se instalează pe dispozitive pentru a fura date sau a provoca daune.
- **Atacuri DDoS:** Blocarea unui site prin trimiterea unui număr mare de cereri simultane, astfel încât acesta să devină inaccesibil utilizatorilor legitimi.
- **Atacuri prin link-uri periculoase:** Link-uri care duc la site-uri false și încearcă să-ți fure informațiile

ACTIVITATE PRACTICĂ:

Simulare de phishing:

1. Profesorul prezintă exemple de emailuri și mesaje suspecte.
2. Elevii identifică semnele unui atac de tip phishing.
3. Discută despre modalități de prevenire.

ÎNTREBĂRI DE REFLECȚIE:

- Ai primit vreodată un mesaj suspect?
- Cum poți verifica dacă un site sau un email este sigur?
- Ce măsuri ai putea lua pentru a-ți proteja conturile online?

LECTȚIA 2: PAROLE ȘI AUTENTIFICARE SIGURĂ

OBIECTIVE:

- Înțelegerea importanței parolelor sigure.
- Aplicarea regulilor pentru crearea unei parole puternice.
- Familiarizarea cu metodele de autentificare suplimentară.

CONȚINUT TEORETIC:

Cum alegem o parolă puternică?

- O parolă sigură trebuie să conțină cel puțin 12 caractere, incluzând litere mari și mici, cifre și simboluri.
- Evităm parolele comune sau ușor de ghicit, precum „123456”, „password” sau date personale evidente (nume, data nașterii).
- Fiecare cont trebuie să aibă o parolă unică pentru a evita compromiterea tuturor conturilor în cazul unui atac.

Importanța autentificării în doi pași (2FA):

- Pe lângă parolă, utilizatorul introduce un cod primit prin SMS, email sau aplicație.
- Aceasta adaugă un nivel suplimentar de securitate și face mult mai dificil accesul hackerilor la conturi.

Utilizarea unui manager de parole:

- Un serviciu care generează și stochează parole complexe.
- Exemple: LastPass, Bitwarden, 1Password, Google Password Manager.

ACTIVITATE PRACTICĂ:

Creare de parole sigure:

1. Elevii inventează o parolă sigură folosind regulile învățate.
2. Discută în grup despre dificultatea reținerii parolelor complexe.
3. Simulează folosirea unui manager de parole.

ÎNTREBĂRI DE REFLECȚIE:

- Ce parole folosești în prezent? Sunt sigure?
- Cum ai putea îmbunătăți securitatea conturilor tale?
- Ce ai învățat despre autentificarea în doi pași?

LECȚIA 3: PROTEJAREA DATELOR PERSONALE ȘI CYBERBULLYING-UL

OBIECTIVE:

- Identificarea informațiilor personale care trebuie protejate.
- Conștientizarea riscurilor partajării excesive online.
- Aplicarea măsurilor pentru un comportament digital responsabil.

CONȚINUT TEORETIC:

Ce informații NU ar trebui să împărtășim online?

- Date personale precum adresa de acasă, numărul de telefon, CNP-ul, datele cardurilor bancare.
- Parole și informații de securitate ale conturilor online.
- Fotografiile sensibile sau informații care pot fi folosite împotriva noastră.

Cum verificăm dacă un site este sigur?

- Verificăm dacă adresa URL începe cu „https://” și dacă are un certificat de securitate valabil (extensia s).
- Analizăm prezența recenziilor și a informațiilor de contact legitime.
- Evităm site-urile care solicită date personale fără justificare.
- Verificăm dacă are trust marks - imagini sau sigle care arată că au îndeplinit diverse cerințe de securitate și confidențialitate

Ce este cyberbullying-ul?

Cyberbullying-ul este o formă de agresiune online care poate avea un impact emoțional puternic. Se manifestă prin atacuri verbale repetate, răspândirea de informații false sau jenante, și excluderea intenționată din grupuri online.

Tipuri de cyberbullying:

- Mesaje și comentarii jignitoare: Insulte și amenințări prin rețele sociale, mesaje text sau emailuri.
- Distribuirea de informații false sau jenante: Răspândirea de minciuni pentru a afecta reputația unei persoane.
- Excluderea intenționată din grupuri online: Marginalizarea unei persoane prin eliminarea sa din comunități digitale.
- Impersonare: Crearea unui cont fals în numele unei persoane pentru a o discredita.
- Sexting și revenge porn: Trimiterea sau distribuirea fără permisiune a imaginilor intime, ceea ce poate duce la umilire și probleme legale.
- Hărțuirea repetată: Mesaje insistente și agresive trimise constant unei persoane.

Impactul cyberbullying-ului:

- Studiile arată că 54% dintre tinerii cu vârste între 12-17 ani s-au simțit afectați emoțional sau jigniți în mediul virtual.
- 40% dintre adolescenți sunt expuși la conținut care promovează autovătămarea sau sinuciderea.

Cum ne protejăm împotriva cyberbullying-ului?

- Nu răspunde provocărilor – reacțiile emoționale pot încuraja agresorii.
- Salvează dovezile – capturile de ecran pot fi utile pentru a raporta incidentul.
- Blochează și raportează utilizatorul – majoritatea platformelor permit blocarea agresorilor și raportarea conținutului ofensator.
- Discută cu un adult de încredere – profesorii, părinții sau consilierii școlari te pot ajuta să gestionezi situația.

Setările de confidențialitate pe rețelele sociale

- Controlează cine poate vedea postările tale – folosește setările de confidențialitate pentru a limita accesul la informațiile personale.
- Evită etichetarea automată în poze – aceasta poate expune informații despre tine fără consimțământul tău.
- Restricționează accesul la profil pentru persoane necunoscute – nu accepta cereri de prietenie de la persoane pe care nu le cunoști.

ACTIVITATE PRACTICĂ:

Analiză de profil online:

1. Elevii își verifică setările de confidențialitate pe o platformă socială.
2. Identifică informațiile pe care ar trebui să le protejeze mai bine.
3. Prezintă în fața clasei ce schimbări au făcut pentru a-și proteja datele.

Analiză de situație:

1. Profesorul prezintă un caz real de cyberbullying.
2. Elevii identifică tipul de cyberbullying din exemplu și discută despre impact.
3. În grupuri, propun soluții pentru gestionarea situației.

ÎNTREBĂRI DE REFLECȚIE:

- Ce informații ai partajat online fără să-ți dai seama?
- Cum îți poți proteja mai bine datele personale?
- Ce impact are dezinformarea asupra deciziilor tale online?
- Ai asistat vreodată la cyberbullying?
- Cum ai putea ajuta pe cineva care trece printr-o astfel de experiență?
- De ce este important să avem un comportament etic online?