

Plan de lecție



2023-1-SK01-KA220-SCH-00015112

Subiect	Securitate și instrumente digitale	
Titlu bloc	Gardienii cibernetici: Explorarea securității prin intermediul instrumentelor digitale	
Categorie de vârstă	Durată (min)	Numărul de ore de predare
9-16	100 de minute	3
Obiective educaționale orientate către elev (standarde de conținut și performanță)		
Scopul principal: Înțelegerea importanței securității cibernetice. Studenții vor învăța despre diferite tipuri de amenințări la adresa securității digitale și despre modul în care tehnologia poate fi utilizată pentru a proteja informațiile și datele. Lumea 3D va fi utilizată pentru a simula scenarii de securitate cibernetică, iar studenții ar trebui să fie capabili să le rezolve, de preferință lucrând în echipă, promovând munca în echipă și rezolvarea inovatoare a problemelor.		
Materiale didactice și tehnici didactice Calculatoare cu acces la internet sau la o rețea locală unde va fi găzduit mediul 3D World.		
Referințe/Surse (videoclipuri, metodologii)		
Faza motivațională		
Durată (min): 10 minute Obiectivul este de a realiza o introducere despre securitatea digitală și de a-i face pe elevi să reflecteze asupra importanței protejării informațiilor online. Acest lucru poate fi realizat printr-o activitate în lumea virtuală care seamănă cu un labirint.		
Elevii vor ajunge la un labirint imens, cu un indicator la început „Labirintul Lumii Cibernetice”. În interiorul labirintului vor găsi diferite obstacole care reprezintă amenințări comune de securitate, cum ar fi e-mailuri de phishing, programe malware sau piratarea parolilor. Pentru fiecare obstacol, vor întâlni provocări precum puzzle-uri și chestionare care le vor cere să identifice modalități de a evita sau atenua aceste amenințări digitale. Rezolvarea acestor provocări le va permite elevilor să găsească ieșirea din labirint.		
Faza exploratorie		
Durată (min): 20 min Obiectivul este de a încuraja studenții să exploreze modul în care funcționează instrumentele de securitate cibernetică, permițându-le să descopere principiile cheie ale securității digitale prin învățare interactivă. Activitatea propusă în această fază se numește „Construirea sistemului dvs. de securitate virtual”. Studenții ar trebui să lucreze în echipe pentru a proiecta un sistem de securitate virtual pentru o companie sau organizație fictivă, abordând potențialele amenințări de securitate și propunând soluții.		
Studenții vor explora diferite tipuri de amenințări cibernetice, cum ar fi viruși, atacuri de phishing și încălcări de date. De asemenea, vor cerceta instrumente de securitate de bază, cum ar fi firewall-uri, criptare și autentificare multi-factor. Folosind platforma lumii virtuale, studenții vor crea o reprezentare digitală.		

a unui mediu de birou securizat sau a unui centru de date. Acestea vor încorpora elemente precum acces protejat prin parolă, seifuri de date criptate și firewall-uri. Echipetele vor simula potențiale breșe de securitate în lumea lor virtuală (de exemplu, hackeri care încearcă să fure date) și vor demonstra modul în care sistemul lor de securitate protejează organizația. După finalizarea proiectării, fiecare echipă va discuta despre caracteristicile de securitate pe care au ales să le includă și despre modul în care acestea abordează amenințările specifice.

Următoarele sunt câteva elemente cheie care ar trebui incluse în activitatea planificată:

- Înțelegerea modului în care funcționează virușii, programele malware și alte amenințări cibernetice la nivel tehnic.
- Aplicarea instrumentelor de securitate precum criptarea, firewall-urile și protecția prin parolă.
- Proiectarea unui sistem de securitate virtual funcțional pentru a rezolva probleme din lumea reală.
- Calcularea cheilor de criptare, aratelor de transmitere a datelor sau determinarea gradului de securitate al unei parole.
- Crearea unei interfețe atractive și ușor de utilizat pentru sistemul de securitate.

Faza de fixare (consolidare și adâncire)

Durată (min): 30 min

Activitatea propusă se intitulează „Provocarea securității cibernetice: Protejarea viitorului”

Obiectivul este ca studenții să se confrunte cu o problemă reală de securitate cibernetică și să aibă sarcina de a proiecta o soluție digitală pentru a proteja o organizație sau un grup fictiv de un atac cibernetic.

Vor fi disponibile trei scenarii alternative:

- Proiectați un sistem de securitate pentru a proteja o casă inteligentă cu dispozitive conectate la internet (IoT), cum ar fi difuzoare inteligente, camere video și electrocasnice. Soluția trebuie să abordeze amenințări precum accesul neautorizat și încălcările de date.
- Elaborați un plan de securitate cibernetică pentru rețeaua unei școli, concentrându-vă pe protejarea datelor elevilor, prevenirea atacurilor cibernetice și asigurarea unei comunicări securizate între profesori, elevi și părinți. Creați o soluție de securitate cibernetică pentru o organizație din domeniul sănătății care gestionează date sensibile ale pacienților. Sistemul ar trebui să protejeze împotriva atacurilor cibernetice, a accesului neautorizat și a încălcărilor de date, asigurând în același timp confidențialitatea.

Pașii pentru elevi sunt următorii:

1. Elevii selectează un scenariu și identifică riscurile specifice de securitate cibernetică implicate (de exemplu, hacking, furt de date, ransomware).
2. Echipetele vor face brainstorming pentru soluții, luând în considerare ce instrumente de securitate cibernetică (de exemplu, criptare, firewall-uri, sisteme de autentificare) pot fi aplicate. Aceștia vor proiecta un prototip pe platforma lumii virtuale.
3. Folosind lumea virtuală, elevii vor simula un scenariu de atac cibernetic (de exemplu, un hacker care încearcă să pătrundă într-un sistem). Echipetele vor demonstra cum soluția lor de securitate protejează organizația de atac.
4. Echipetele prezintă clasei prototipul lor de securitate digitală, explicând cum funcționează și cum abordează amenințările reprezentate de scenariu. Feedback-ul din partea profesorului și a colegilor îi poate ajuta să își perfecționeze soluțiile.

Evaluarea studenților

- Participarea în labirintul virtual și găsirea ieșirii din acesta.
- Creativitatea și funcționalitatea sistemului de securitate digitală proiectat în lumea virtuală.
- Prezentări și capacitatea de a explica modul în care soluția lor de securitate abordează amenințări specifice folosind instrumente digitale.

Anexe:

Acest proiect a fost implementat cu sprijinul Comisiei Europene. Sprijinul acordat de Comisia Europeană pentru producerea acestei publicații nu constituie o aprobare a conținutului, care reflectă doar opiniile autorilor, iar Agenția și Comisia Națională nu pot fi trase la răspundere pentru nicio utilizare care ar putea fi făcută informațiilor conținute în aceasta.