

# Plán hodiny



2023-1-SK01-KA220-SCH-00015112

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                     |                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------|
| <b>Téma</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Bezpečnostné a digitálne nástroje                                                   |                                     |
| <b>Názov bloku</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Kybernetickí strážcovia: Skúmanie bezpečnosti prostredníctvom digitálnych nástrojov |                                     |
| <b>Veková kategória</b><br>9-16                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Trvanie (min)</b><br>100 minút                                                   | <b>Počet vyučovacích hodín</b><br>3 |
| <b>Vzdelávacie ciele zamerané na študenta (obsahové a výkonnostné štandardy)</b><br><b>Hlavný cieľ:</b> Pochopenie dôležitosti kybernetickej bezpečnosti. Študenti sa oboznámia s rôznymi typmi digitálnych bezpečnostných hrozieb a s tým, ako možno technológie využiť na ochranu informácií a údajov. 3D svet bude použitý na simuláciu scenárov kybernetickej bezpečnosti a študenti by mali byť schopní ich riešiť, najlepšie prácou v tímoch, podporou tímovej práce a inovatívneho riešenia problémov. |                                                                                     |                                     |
| <b>Didaktické materiály a didaktické techniky</b> <ul style="list-style-type: none"><li>Počítače s prístupom na internet alebo lokálnu sieť, na ktorej bude umiestnené prostredie 3D sveta.</li></ul>                                                                                                                                                                                                                                                                                                         |                                                                                     |                                     |
| <b>Zdroje/referencie (videá, metodiky)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                     |                                     |
| <b>Motivačná fáza</b><br>Trvanie (min): 10 minút                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                     |                                     |

Cieľom je vytvoriť úvod do digitálnej bezpečnosti a prinútiť študentov zamyslieť sa nad dôležitosťou ochrany informácií online. To sa dá dosiahnuť aktivitou vo virtuálnom svete, ktorá pripomína bludisko.

Študenti dorazia do veľkého bludiska, na začiatku ktorého bude označenie „Kybernetické bludisko“. Vnútri bludiska nájdu rôzne prekážky predstavujúce bežné bezpečnostné hrozby, ako sú phishingové e-maily, malware alebo hackovanie hesiel. Pri každej prekážke sa stretnú s výzvami, ako sú hádanky a kvízy, ktoré od nich budú vyžadovať, aby identifikovali spôsoby, ako sa týmto digitálnym hrozbám vyhnúť alebo ich zmierniť. Riešenie týchto výziev umožní študentom nájsť východ z bludiska.

### **Prieskumná fáza**

#### **Trvanie (min): 20 min**

Cieľom je povzbudiť študentov, aby preskúmali fungovanie nástrojov kybernetickej bezpečnosti a prostredníctvom interaktívneho učenia sa zoznámili s kľúčovými princípmi digitálnej bezpečnosti. Navrhovaná aktivita v tejto fáze má názov „Vytvorenie virtuálneho bezpečnostného systému“. Študenti by mali pracovať v tímoch na návrhu virtuálneho bezpečnostného systému pre fiktívnu spoločnosť alebo organizáciu, riešiť potenciálne bezpečnostné hrozby a navrhovať riešenia.

Študenti preskúmajú rôzne typy kybernetických hrozieb, ako sú vírusy, phishingové útoky a úniky údajov. Taktiež preskúmajú základné bezpečnostné nástroje, ako sú firewally, šifrovanie a viacfaktorové overovanie. Pomocou platformy virtuálneho sveta študenti vytvoria digitálnu reprezentáciu zabezpečeného kancelárskeho prostredia alebo dátového centra. Začlenia prvky, ako je prístup chránený heslom, šifrované dátové trezory a firewally. Tímy budú simulovať potenciálne narušenia bezpečnosti vo svojom virtuálnom svete (napr. hackeri sa pokúšajú ukradnúť údaje) a demonštrujú, ako ich bezpečnostný systém chráni organizáciu. Po dokončení návrhu každý tím prediskutuje bezpečnostné funkcie, ktoré sa rozhodli zahrnúť, a ako riešia konkrétne hrozby.

Nasledujú niektoré kľúčové prvky, ktoré by mali byť zahrnuté v plánovanej aktivite:

- Pochopenie fungovania vírusov, malvéru a iných kybernetických hrozieb na technickej úrovni.
- Aplikácia bezpečnostných nástrojov, ako sú šifrovanie, firewally a ochrana heslom.
- Návrh funkčného virtuálneho bezpečnostného systému na riešenie problémov reálneho sveta.
- Výpočet šifrovacích kľúčov, rýchlosti prenosu dát alebo určenie bezpečnosti hesla.
- Vytvorenie pútavého a užívateľsky prívetivého rozhrania pre bezpečnostný systém.

## **Fáza fixácie (konsolidácia a prehĺbenie)**

### **Trvanie (min): 30 min**

Navrhovaná aktivita má názov „Výzva kybernetickej bezpečnosti: Ochrana budúcnosti“

Cieľom je, aby sa študenti stretli s reálnym problémom kybernetickej bezpečnosti a aby mali za úlohu navrhnúť digitálne riešenie na ochranu fiktívnej organizácie alebo skupiny pred kybernetickým útokom.

K dispozícii budú tri alternatívne scenáre:

- Navrhnete bezpečnostný systém na ochranu inteligentnej domácnosti so zariadeniami pripojenými na internet (IoT), ako sú inteligentné reproduktory, kamery a spotrebiče. Riešenie musí riešiť hrozby, ako je neoprávnený prístup a úniky údajov.
- Vypracovať plán kybernetickej bezpečnosti pre školskú sieť so zameraním na ochranu údajov študentov, predchádzanie hackerským útokom a zabezpečenie bezpečnej komunikácie medzi učiteľmi, študentmi a rodičmi.
- Vytvorte riešenie kybernetickej bezpečnosti pre zdravotnícku organizáciu, ktorá spracováva citlivé údaje o pacientoch. Systém by mal chrániť pred hackerskými útokmi, neoprávneným prístupom a únikmi údajov a zároveň zabezpečovať súkromie.

Kroky pre študentov sú nasledovné:

1. Študenti si vyberú scenár a identifikujú konkrétne riziká kybernetickej bezpečnosti (napr. hackerské útoky, krádež údajov, ransomvér).
2. Tímy brainstormujú riešenia a zvažujú, ktoré nástroje kybernetickej bezpečnosti (napr. šifrovanie, firewally, autentifikačné systémy) je možné použiť. Navrhnú prototyp na platforme virtuálneho sveta.
3. Pomocou virtuálneho sveta budú študenti simulovať scenár kybernetického útoku (napr. hacker sa pokúša preniknúť do systému). Tímy predvedú, ako ich bezpečnostné riešenie chráni organizáciu pred útokom.
4. Tímy predstavia triede svoj prototyp digitálnej bezpečnosti a vysvetlia, ako funguje a ako rieši hrozby, ktoré predstavuje daný scenár. Spätná väzba od učiteľa a kolegov im môže pomôcť spresniť ich riešenia.

### **Hodnotenie študentov**

- Účasť vo virtuálnom bludisku a hľadanie cesty z neho.
- Kreativita a funkčnosť digitálneho bezpečnostného systému navrhnutého vo virtuálnom svete.
- Prezentácie a schopnosť vysvetliť, ako ich bezpečnostné riešenie rieši konkrétne hrozby pomocou digitálnych nástrojov.

### **Prílohy:**

*Tento projekt bol realizovaný s podporou Európskej komisie. Podpora Európskej komisie na vypracovanie tejto publikácie nepredstavuje schválenie obsahu, ktorý odráža iba názory autorov, a Agentúra ani Národná komisia nenesú zodpovednosť za žiadne použitie informácií v nej obsiahnutých.*