

Plán lekce

2023-1-SK01-KA220-SCH-00015112



Téma	Bezpečnost a technologie	
Název bloku	<i>Zabezpeč svůj svět – aplikace pro bezpečné online chování</i>	
Věková kategorie 13 – 15	Trvání 135 minut	Počet vyučovacích hodin 3
Cíle vzdělávání zaměřené na žáka (obsahový a výkonový standard) Obsahový standard: • Principy bezpečného chování online. • Základy ochrany osobních údajů, phishing, hoaxy. Výkonový standard: • Navrhnout aplikaci vzdělávající o kyberbezpečnosti. • Identifikovat hrozby a způsoby ochrany. • Spolupracovat a reflektovat přínos řešení. Integrace předmětů: • Informatika, • Občanská výchova, • Český jazyk Dovednosti 21. století: • Kritické myšlení,		

- Digitální gramotnost,
- Spolupráce

Didaktické pomůcky a didaktická technika:

- Počítače s internetem,
- MIT App Inventor,
- Canva,
- Mobilní telefony

Reference / Zdroje (video, metodiky) :

- <https://appinventor.mit.edu>

Motivační fáze:

Trvání: 40 minut

„Co se může stát, když zapomeneme na bezpečí online?“

1. Úvodní video a diskuze:

- Učitel promítne video [Bezpečnost na internetu](#)
- Po zhlédnutí následuje moderovaná diskuse o nejčastějších hrozbách internetu – žáci sdílejí osobní zkušenosti s falešnými profily, podvodnými e-maily nebo nezabezpečenými stránkami.
- Učitel na tabuli zapisuje klíčová slova: *heslo, phishing, virus, kyberšikana, cookies, digitální stopa.*

1. Skupinová aktivita – „Co by se stalo, kdyby...“

- Skupiny vytvoří krátké scénáře popisující rizikové situace (např. zveřejnění hesla, kliknutí na neznámý odkaz, sdílení osobních dat).
- Ostatní hádají, jaké chyby se postavy dopustily a jak se jim mohly vyhnout.

1. Definování problému:

- Žáci společně formulují otázku: *„Jak by mohla mobilní aplikace pomoci lidem chovat se online bezpečněji?“*
- Učitel shrne, že cílem lekce bude navrhnout a vytvořit vzdělávací aplikaci, která upozorňuje na rizika internetu a učí správnému chování.

Expoziční fáze:

Trvání: 50 minut

Cíl:

Žáci pochopí základní principy kybernetické bezpečnosti a aplikují je při návrhu vlastní vzdělávací aplikace.

Rozvíjejí schopnost kombinovat teoretické poznatky o ochraně dat s praktickou tvorbou digitálního nástroje, který pomáhá předcházet rizikovému chování na internetu.

Integrace vědy:

Žáci propojují poznatky z občanské a mediální výchovy – pochopení pojmů *identita, důvěryhodnost, manipulace, odpovědnost online*.

Analyzují reálné příklady útoků (např. phishing, falešné soutěže, virální hoaxy).

Diskutují o tom, jak se technologie (např. dvoufaktorové ověřování, šifrování) využívají k ochraně uživatelů.

Cílem je ukázat, že principy bezpečnosti nejsou jen technické, ale také etické a společenské.

Integrace informatiky:

Žáci si osvojí základní principy vývoje mobilní aplikace v nástroji **MIT App Inventor**:

- práce s **generováním náhodných dat (hesel)**,
- tvorba **informačních bloků (bezpečnostní tipy, upozornění)**,
- implementace **interaktivních prvků (kvíz, tlačítko „Zjisti více“)**,
- základní podmíněné příkazy (*if – then*) reagující na odpovědi uživatele.

Tímto propojují digitální dovednosti s logickým myšlením a principy uživatelského rozhraní (UI/UX).

Aktivita:

Ukázka a analýza (10 min)

- Učitel předvede tvorbu jednoduchého generátoru hesel v MIT App Inventoru.
- Vysvětlí, proč silné heslo obsahuje velká/malá písmena, čísla a symboly.

Skupinová práce (30 min)

Žáci navrhují aplikaci s následujícími prvky:

- generátor silných hesel,
- krátké bezpečnostní tipy,
- mini kvíz o kyberbezpečnosti (3–5 otázek).

Učitel pomáhá s logikou bloků a testováním.

Testování a úpravy (10 min)

Žáci testují aplikace na telefonech, ověřují funkčnost a přehlednost rozhraní.

Skupiny diskutují, jak by jejich aplikace mohla pomoci spolužákům nebo rodičům.

Fixační fáze (upevňování a prohlubování):

Trvání: 45 minut

„Z bezpečnosti do praxe“

1. Prezentace výstupů:

- Každá skupina představí svůj prototyp aplikace, vysvětlí jeho funkce a přínos pro běžné uživatele.
- Ostatní žáci dávají zpětnou vazbu – co by aplikaci vylepšilo, co je přehledné, co chybí.

1. Vizuální shrnutí:

- Pomocí **Canvy** žáci vytvoří infografiku „5 pravidel pro bezpečný internet“, kterou lze vytisknout nebo zveřejnit na školním webu.

1. Reflexe:

Učitel otevře diskusi:

- Jak vám technologie pomáhá chránit se online?
- Co jste se naučili o svém vlastním chování na internetu?

Hodnocení žáka:

- Originalita a funkčnost aplikace (40 %)
- Porozumění bezpečnostním principům (30 %)
- Týmová spolupráce a prezentace (30 %)

Přílohy: