1. **Vytvořte plán hodiny, včetně úvodu, hlavní části, interakce s žáky, závěru a zpětné vazby.**

**Plán hodiny: Bezpečnost na internetu**

**Úvod (10 minut)**

1. **Přivítání a seznámení s tématem**:
   * Učitel přivítá žáky a představí téma hodiny.
   * Krátká diskuse: "Co si představujete pod pojmem bezpečnost na internetu?"
2. **Motivace**:
   * Učitel uvede několik příkladů rizik na internetu (např. kyberšikana, phishing, zneužití osobních údajů).
   * Promítnutí krátkého videa o bezpečnosti na internetu.

**Hlavní část (25 minut)**

1. **Prezentace klíčových pojmů**:
   * Vysvětlení pojmů jako kyberšikana, phishing, malware, soukromí na internetu.
   * Použití prezentace s obrázky a příklady.
2. **Praktické rady a tipy**:
   * Jak vytvořit silné heslo.
   * Jak rozpoznat podezřelé e-maily a odkazy.
   * Jak chránit své osobní údaje na sociálních sítích.
3. **Interaktivní aktivita**:
   * Rozdělení žáků do skupin a zadání úkolu: "Vytvořte plakát s pravidly bezpečného chování na internetu."
   * Každá skupina představí svůj plakát ostatním.

**Interakce s žáky (10 minut)**

1. **Diskuse a otázky**:
   * Učitel vyzve žáky k otázkám a diskusi o prezentovaných tématech.
   * Žáci mohou sdílet své vlastní zkušenosti a názory.

**Závěr (5 minut)**

1. **Shrnutí**:
   * Učitel shrne hlavní body hodiny.
   * Zdůraznění důležitosti bezpečného chování na internetu.

**Zpětná vazba (5 minut)**

1. **Reflexe**:
   * Učitel požádá žáky, aby napsali na papír jednu věc, kterou se dnes naučili, a jednu otázku, kterou ještě mají.
   * Učitel shromáždí papíry a na příští hodině odpoví na otázky.
2. **Požádejte AI o sestavení tabulky, která shrnuje klíčové pojmy či metody z vašeho**

**předmětu.**

| **Klíčový pojem/metoda** | **Popis** |
| --- | --- |
| **Kyberšikana** | Šikana, která probíhá prostřednictvím internetu, sociálních sítí nebo mobilních zařízení. |
| **Phishing** | Podvodná technika, kdy se útočník snaží získat citlivé informace (např. hesla, čísla kreditních karet) tím, že se vydává za důvěryhodnou osobu nebo organizaci. |
| **Malware** | Škodlivý software, který může poškodit nebo narušit počítačové systémy. |
| **Soukromí na internetu** | Ochrana osobních údajů a informací při používání internetu. |
| **Silné heslo** | Heslo, které je obtížné uhodnout, obvykle obsahuje kombinaci písmen, čísel a speciálních znaků. |
| **Rozpoznání podezřelých e-mailů** | Schopnost identifikovat e-maily, které mohou být podvodné nebo obsahovat škodlivé odkazy. |
| **Ochrana osobních údajů na sociálních sítích** | Praktiky a nastavení, které pomáhají chránit soukromí a bezpečnost uživatele na sociálních sítích. |
| **Vytvoření plakátu s pravidly bezpečného chování na internetu** | Skupinová aktivita, při které žáci vytvářejí vizuální pomůcku s pravidly pro bezpečné používání internetu. |

1. **Začleňte možné otázky (a odpovědi) pro ověření znalostí studentů.**

**Otázky a odpovědi**

1. **Co je kyberšikana a jak se jí můžeme bránit?**
   * **Odpověď**: Kyberšikana je šikana, která probíhá prostřednictvím internetu, sociálních sítí nebo mobilních zařízení. Můžeme se jí bránit tím, že nebudeme reagovat na provokace, budeme blokovat útočníky a hlásit nevhodné chování dospělým nebo administrátorům webových stránek.
2. **Co je phishing a jak ho rozpoznat?**
   * **Odpověď**: Phishing je podvodná technika, kdy se útočník snaží získat citlivé informace tím, že se vydává za důvěryhodnou osobu nebo organizaci. Phishingové e-maily často obsahují gramatické chyby, podezřelé odkazy nebo žádosti o osobní údaje.
3. **Jaké jsou znaky silného hesla?**
   * **Odpověď**: Silné heslo obsahuje kombinaci velkých a malých písmen, čísel a speciálních znaků. Mělo by být alespoň 12 znaků dlouhé a nemělo by obsahovat snadno uhodnutelné informace, jako je jméno nebo datum narození.
4. **Proč je důležité chránit své osobní údaje na sociálních sítích?**
   * **Odpověď**: Ochrana osobních údajů na sociálních sítích je důležitá, protože zabráníme jejich zneužití, krádeži identity nebo kyberšikaně. Měli bychom pečlivě nastavit soukromí na našich profilech a sdílet pouze informace, které jsou bezpečné.
5. **Jaké kroky můžeme podniknout, abychom se chránili před malwarem?**
   * **Odpověď**: Abychom se chránili před malwarem, měli bychom používat antivirový software, pravidelně aktualizovat operační systém a aplikace, neklikat na podezřelé odkazy a nestahovat soubory z nedůvěryhodných zdrojů.
6. **Co bychom měli dělat, pokud obdržíme podezřelý e-mail?**
   * **Odpověď**: Pokud obdržíme podezřelý e-mail, neměli bychom na něj reagovat ani klikat na odkazy. Měli bychom ho označit jako spam nebo phishing a nahlásit ho poskytovateli e-mailových služeb.
7. **Nechte AI vygenerovat grafické podklady k tématu hodiny.**

Obsah obrázku oblečení, nábytek, osoba, stůl

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obsah obrázku oblečení, muž, osoba, Lidská tvář

Obsah vygenerovaný umělou inteligencí může být nesprávný.Obsah obrázku oblečení, osoba, interiér, Vzdělávání

Obsah vygenerovaný umělou inteligencí může být nesprávný.