

Vzdělávací obor: Informatika

Očekávaný výsledek učení: INF-INF-003-ZV9-012

Vybírá pro své potřeby hardware, software a způsob připojení digitálních zařízení do sítě na základě porozumění jejich vlastnostem.

Popis úrovně Na Cestě

- Vysvětlí fungování počítače z hlediska jeho základních dílů (procesor, operační paměť, úložiště/disky).
- Volí typ zařízení (stolní počítač, notebook, tablet, chytrý telefon) podle jeho využití.
- Vysvětlí roli operačního systému při využívání počítače a zvládá základy ovládání jednoho běžně využívaného operačního systému.
- Rozzná typ sítě, do které je zařízení připojeno, vysvětlí princip jejího fungování (LAN, Internet, Wi-Fi, Bluetooth, mobilní síť).
- Identifikuje nejčastější problémy hardware, software a počítačové sítě.
- Získává informace o technologiích z různých zdrojů, učí se rozpoznávat nepřesné formulace a úmyslné manipulace.

Můj bezpečný mobil

Úvod / kontext / anotace

Zadání pro žáky

Zajistěte bezpečné nastavení prostředí mobilního telefonu.

1. Výběr zařízení

Jaký mobil nebo tablet je nejlepší pro školní práci? Jaké funkce by měl mít (výkon, úložiště, zabezpečení)?

2. Přihlášení a zabezpečení

Proč používat silné heslo a dvoufázové ověření (např. SMS kód, otisk prstu, rozpoznání obličeje)?

3. Oprávnění aplikací

Jak zjistit, které aplikace opravdu potřebuješ? Jak správně nastavit oprávnění, aby aplikace neměly zbytečný přístup k tvým osobním údajům (např. fotky, poloha, mikrofón)?

4. Ochrana před nebezpečím

Jak poznáš podezřelou aplikaci? Co dělat, když aplikace požaduje příliš mnoho oprávnění? Jak chránit mobil před hackery a viry?

5. Správa dat

Proč je dobré mazat nepotřebné aplikace a pravidelně zálohovat důležitá data?

6. Týmový úkol

Vytvořte stručný návod pro spolužáky:

- Jak bezpečně nastavit telefon?
- Jak chránit osobní údaje?
- Co dělat, když ztratíš mobil?

Popis ověřování

Učitel sleduje, zda žák:

- Vybere vhodné mobilní zařízení pro školní účely s ohledem na jeho výkon, operační systém a bezpečnostní funkce.
- Správně nastaví oprávnění pro aplikace na mobilním zařízení, a to tak, aby aplikace měly přístup pouze k nezbytným funkcím.
- Identifikuje rizikové aplikace a ví, jak nastavit ochranu před nebezpečnými aplikacemi nebo hrozbami.
- Bezpečně spravuje data na mobilním zařízení a zálohuje důležitá školní data.
- Vytvoří bezpečnostní průvodce pro spolužáky, který obsahuje doporučení pro správné nastavení mobilních zařízení a aplikací.

Ukázka řešení

Bezpečné nastavení mobilu – řešení

1. **Výběr zařízení**
Nejlepší pro školní práci: Tablet nebo telefon s velkým displejem, dlouhou výdrží baterie dostatečným úložištěm.
Důležité parametry: Rozšířený operační systém (Android/iOS), podpora bezpečnostních aktualizací.
Zabezpečení: Ideálně čtečka otisků prstů nebo rozpoznání obličeje.
2. **Přihlášení a zabezpečení**
Silné heslo: Kombinace písmen, čísel a speciálních znaků.
Dvoufázové ověření: Nastavit ověřování přes SMS, e-mail nebo biometriku (otisk prstu, obličej).
3. **Oprávnění aplikací**
Instalovat jen ověřené aplikace. Povolovat pouze nezbytný přístup (např. poznámky nepotřebují polohu). Oprávnění lze upravit v nastavení.
4. **Ochrana před nebezpečím**
Nepoužívat aplikace s podezřelými oprávněními. Stahovat jen z oficiálních obchodů. Pravidelně aktualizovat systém a aplikace.
5. **Správa dat**
Mazat nepotřebné aplikace. Důležitá data zálohovat na cloud nebo externí disk.
6. **Týmový úkol**

Zdroje

KYSELA, J. Vlastní práce, 2025. Nepublikovaný materiál.