

# JEJDA, NEMÁM V KAPSE OSOBNÍHO ŠPIÓNA?

Délka lekce: **40 minut** / Věk: **6.–7. třída**

Pozn.: V hodině je ideální pracovat se smartphony dětí přímo ve třídě.

## Děti se z této lekce dozví/připomenou si:

- ∞ Smartphone ukládá informace, ke kterým mohou přistupovat různé aplikace.
- ∞ Na majitele smartphonů mohou číhat rizika, pokud povolí aplikacím přístup ke všemu, oč žádají.
- ∞ Některá z těchto rizik jsou spojená s internetovou kriminalitou.

## Děti se naučí nebo si zopakují následující slova/koncepty:

- ∞ aplikace ve smartphonu
- ∞ informace ve smartphonu
- ∞ povolení přístupu aplikacím
- ∞ internetová kriminalita (ve smyslu např.: vykradení bankovního účtu nebo vydírání)

## Základní informace:

### Pouštěná videa:

- ∞ 17. díl „Špión nebo kamarád?“

### Co musí učitel zajistit před realizací lekce:

- ∞ podívat se na daný díl; doporučujeme přečíst i technický popis dílu
- ∞ přečíst si instrukce k této lekci
- ∞ na lekci je potřeba připravit si následující:
  - obyčejná tabule ve třídě
  - video ke spuštění
  - papíry a psací potřeby
  - pro úkol **2.3** si připravte Přílohu A k promítnutí nebo si ji přepište na tabuli a tu otočte tak, aby na ni na začátku hodiny nebylo vidět
  - pro úkol **3.2** je dobré, aby žáci měli své smartphony (případně abyste měli připraveno alternativní řešení)
  - pro aktivitu **4.** „Vymýšlení vlastní aplikace“:
    - papíry formátu A4
    - pastelky/fixy
    - papíry formátu A3

## Shrnutí děje 17. dílu:

Marwin z kouzelné koule „vyvěští“, co Kuba dělal cestou domů ze školy. Tyto informace Marwinovi zjistila aplikace „Doplňkov“, kterou Kubovi před pár dny poslal, protože Kuba přijal všechna přístupová oprávnění, jež aplikace chtěla. Marwin vezme Kubu do Datové Lhoty, kde mu na vlastní oči ukáže, co všechno se Doplňkov může v jeho telefonu dozvědět, a vysvětlí mu, že tyto informace lze snadno zneužít. Přitom se ukáže, že Kuba povolil přístup skoro ke všemu i dalším aplikacím, a tak kluci všechny zbytečné přístupy zakážou.

## Lekce v kostce:

- 1. fáze** – ÚVOD – Evokace na téma „aplikace v mém mobilu“ (5–10 min)
- 2. fáze** – 17. DÍL „ŠPIÓN NEBO KAMARÁD?“
  - Uvědomění I: Aplikace na smartphonu přistupují k našim informacím (10 min)
- 3. fáze** – AKTIVITA SE SMARTPHONY „K ČEMU MAJÍ APLIKACE V MÉM TELEFONU PŘÍSTUP?“
  - Uvědomění II: K čemu všemu mohou mít aplikace na našem mobilu přístup (10–15 min)
- 4. fáze** – UNPLUGGED AKTIVITA „VYMÝŠLENÍ VLASTNÍ APLIKACE“
  - Reflexe I: Zneužitelnost informací v telefonu (5 min)
- 5. fáze** – ZÁVĚR
  - Reflexe II: Stručné shrnutí hodiny (2–3 minuty)

## Průběh lekce:

### 1. fáze – Úvod

5–10 min

**Záměr fáze:** Evokace na téma „jaké aplikace žáci v mobilu používají“.

- 1.1.** Evokace – ptejte se děti: „Dnes se budeme zabývat aplikacemi ve smartphonech. Jaké aplikace používáte na smartphonu?“

Nechte děti vstávat a zapsat aplikaci na tabuli (část aplikací asi nebudete znát a nebudete vědět, jak se píšou). Nechte děti jednou dvěma větami vysvětlit, co daná aplikace dělá.

Aktivitu ukončete, jakmile budete mít na tabuli alespoň cca 8 aplikací.

*Pozn.: Dejte si pozor, ať nemáte na tabuli pouze aplikace jednoho druhu, například hry. Snažte se, aby děti vyjmenovaly různé aplikace, například sociální sítě, hry, mapy, vzdělávací aplikace, komunikátory, e-mailovou aplikaci atd. Případně sami nějakou aplikaci doplňte.*

*Tip: Pokud jste v počítačové laboratoři a učíte třídu pracovat v cloudovém prostředí, můžete nechat děti psát do společného dokumentu – každý jednu nebo dvě aplikace. Děti pak mohou hlasovat, kdo kterou aplikaci používá. Ale pozor, ať se moc nezdržíte.*

- 1.2.** Uzavřete úvod: „Teď se půjdeme podívat do Datové Lhoty na to, že ne všechny aplikace, které ve smartphonech máme, jsou vždy jen k našemu prospěchu.“

### 2. fáze – 17. díl „Špión nebo kamarád?“

10 min

**Záměr fáze:** Uvědomění I: Není dobré automaticky dávat všem aplikacím povolení přistupovat ke všem informacím, které chce aplikace využívat. Některé aplikace totiž mohou nějaké informace zneužít proti uživateli.

- 2.1.** Otázka před spuštěním videa: „Zjistěte z videa, kdo špiónil o Kubovi informace?“
- 2.2.** Pusťte video „17. díl – Špión nebo kamarád?“
- 2.3.** Rozeberte odpověď na otázku: „Zjistěte, kdo špiónil o Kubovi informace?“

**SPRÁVNÁ ODPOVĚĎ:** Marwin, díky aplikaci na úpravu fotek.

Ptejte se, a pokud budou děti tápat, pouštějte části videa podle následující tabulky.

Otázka:	Pustíte:	Správná odpověď/poznámka:
K jakým informacím mohou chtít aplikace přistupovat?	2:02 – 2:17	Například k poloze či našim souborům. <i>Pozn.: Stačí vyjmenovat pár věcí, další možnosti ukážete vzápětí.</i>
Aplikace mohou přistupovat k různým věcem, například těmto. <i>Promítněte Přílohu A (nebo otočte tabuli, kde máte Přílohu A přepsanou).</i> Jak lze zneužít přístupy k těmto věcem?	2:22 – 2:52	Pár příkladů: <ul style="list-style-type: none"><li>• Kamera, mikrofon, galerie – pořízení/stažení fotek nebo videí či zvukového záznamu bez vědomí uživatele; zjištění soukromých informací, vydírání, krádež</li><li>• GPS (poloha) – přístup k poloze, sledování uživatele: kdy nejsme doma a lze nás vykrást nebo kudy často chodíme a kde nás lze přepadnout</li><li>• Připojení k internetu – připojení k internetu na pozadí, odesílání informací z mobilu, zjišťování polohy podle okolních Wi-Fi sítí, ev. čerpání mobilních dat uživatele</li><li>• Bluetooth – ovládání mobilního telefonu pomocí Bluetooth; připojení k Bluetooth zařízením, s nimiž mobil pracuje; pokud má tuto aplikaci nainstalovanou hodně lidí, dá se použít i ke zjištění polohy uživatele</li><li>• Kontakty – zneužití k zasílání např. spamu nebo virů na kontakty oběti útoku – zprávy jsou zaslané z našeho čísla/účtu, takže vypadají důvěryhodně</li><li>• Provádění plateb – hry mohou zneužít na mikrotransakce při automatickém dokupování herních bonusů; v krajním případě krádež peněz z účtu oběti</li></ul> <p><i>Tip: Pokud bude debata chaotická, ptejte se na jednotlivé věci na tabuli a čtěte odpověď jednou větou.</i></p> <p><i>Pozn.: Mikrotransakce jsou většinou drobné platby v řádech korun. Používají se mj. ve hrách: hry je mohou za herní bonusy účtovat opakovaně (a někdy může jít i o výrazně větší jednorázové částky).</i></p>

*Pozn.: Připravte se na to, že děti mohou mít zmatek v tom, co je útok počítačového viru, útok hackera, přístup k datům a periferiím (tzn. obsah této lekce) a fakt, že na internetu zanecháváme datovou stopu, kterou internetové firmy zpeněžují. Nyní, v této hodině, se věnujeme jen jednomu ze způsobů, jak o nás mohou aplikace získávat více informací, než je nezbytně nutné, a jsme tak na pomezí hackování a zpeněžování naší datové stopy (podle toho, jaké informace o nás v dané situaci aplikace získávají a jak je využívají). Postupně je dobré dětem ozřejmit rozdíl mezi všemi výše uvedenými koncepty, ale je to práce na delší čas (viz ještě sekce 3.5 a modelová hodina o hackování a soukromí na internetu).*

#### 2.4. Zakočení fáze

Vraťte pozornost dětí zpět k tabuli se zapsanými aplikacemi. Zdůrazněte, že všechny tyto aplikace mohou přistupovat k informacím ze smartphonu, podobně jako jsme to viděli v Datové Lhotě. A podobně, jako jsme to viděli v Datové Lhotě, jim to můžeme zakázat.

**Záměr fáze:** Uvědomění II. Praktická ukázka, k čemu mohou mít aplikace na smartphonu přístup.

- 3.1.** Vysvětlíte, že některé informace ve smartphonech pomáhají aplikacím být účinnější (a bez některých by určité aplikace vůbec nefungovaly). Často jde o informace z periférií smartphonu, jako je třeba kamera, mikrofon nebo GPS (například Mapám se hodí přístup k informacím o poloze telefonu). Může jít ale o přístupy třeba ke kontaktům nebo o přístup k připojení pomocí mobilních dat na pozadí.
- 3.2.** Zadejte dětem úkol: „Zjistěte ve svém telefonu, k jakým informacím mají přístup aplikace napsané na tabuli, tedy které jste sepsaly na začátku hodiny.“

*Tip: V telefonu s Androidem v. 12 nebo 13 tuto informaci najdete: Nastavení → Aplikace → Správa aplikací → Vyberete aplikaci, která vás zajímá → Oprávnění aplikace (zde uvidíte, k čemu aplikace přístup má povolený/nepovolený).*

*V telefonu s iOS 16 tuto informaci najdete: Nastavení → Vyberete aplikaci, která vás zajímá → Přístup aplikace k datům (zde uvidíte, k čemu aplikace přístup má povolený/nepovolený). Postup může být mírně odlišný podle typu a verze operačního systému.*

*Pozn.: Někteří ve třídě nemusí mít svůj smartphone. V takovém případě se hodí použít školní nebo mít postup připravený na slajdech. Není vhodné, aby si děti půjčovaly své osobní smartphony či používaly telefon učitele; tato zařízení obsahují osobní data.*

- 3.3.** Vyzvěte žáky, že mohou **sdílet** (pokud chtějí) informaci o nějaké aplikaci, která na jejich telefonu měla přístup k něčemu, co nepotřebovala.
- 3.4.** Upozorněte žáky, že přístup lze často povolovat i **jednorázově**, když to opravdu v daný moment aplikace potřebuje.

*Tip: Když se děti budou bát, že toho „vypnou moc“, sdělte jim, že mohou příslušné přístupy opět povolit, jakmile se jim bude zdát, že aplikace nefunguje, jak má. Aplikace na to, že jí chybí přístupy, většinou sama upozorní.*

*Při instalaci neznámých aplikací je dobré číst recenze před stažením aplikace (např. na App Store nebo Google Play) a neinstalovat z nedůvěryhodných zdrojů.*

- 3.5.** Sdělte žákům: „Pozor, že i když zakážete aplikacím přistupovat k věcem, které nepotřebují, stejně o vás **internetové firmy sbírají data** – například na webech pomocí cookies. V dnešní hodině jde o to, aby o nás nesbíraly aplikace víc informací, než je nezbytně nutné.“

*Pozn.: Jedna věc je, když si děti stáhnou z internetu podezřelou aplikaci, kterou vytvořil někdo s nekalými úmysly. Takové aplikace je třeba se ihned zbavit. Druhá věc je, že někdy nás zneužívají i aplikace, které působí legálně a chceme je používat (například zmíněné hry – automatické mikrotransakce za herní bonusy). Třetí věc je, že zanecháváme datovou stopu na internetu, kterou zpeněžují internetové firmy – za věci, které jsou jakoby zadarmo, platíme informacemi o sobě. To se týká jak našeho pohybu na webových stránkách, tak i používání našeho mobilu. Je dobré, aby si toto žáci postupně osvojili, ale nejde to všechno zvládnout v této hodině.*

- 3.6.** Ujistěte se na závěr, že děti odložily své smartphony.

**Záměr fáze:** Reflexe I: Upevnění informace, k čemu mohou mít aplikace na smartphonu přístup a jak toho mohou využívat.

4.1. Položte dvě kontrolní otázky:

Otázka:	Správná odpověď/poznámka:
Proč navigace do auta potřebuje znát GPS polohu?	Aby uživatel neustále viděl svůj postup na vytyčené cestě.
Můžu povolit přístup k placení (resp. povolit „nákupy v aplikaci“) hře, kterou jsem si právě nainstaloval?	Raději ne; může se jednat o aplikaci, která je mi pomocí mikrotransakcí za herní bonusy apod. schopna vybrat účet. <i>Pozn.: Aplikace nemusí mít přímo přístup k číslu kreditní karty apod., ale pomocí jiné aplikace (např. App Store) může provádět platby.</i>

4.2. Žáky rozdělte na skupiny.

4.3. Řekněte:

- ∞ „Dnes si zkusíme zahrát na hackery a vymyslíme si vlastní zlou aplikaci. Vymyslete aplikaci, která by mohla uživatele zaujmout, ale potají chce zneužít nějakého přístupu v mobilu.“
- ∞ „Zamyslete se, k jakým periferiím či informacím má mít aplikace přístup.“

Nechte žáky pracovat 2–3 minuty.

4.4. Nechte žáky jednou dvěma větami představit několik aplikací.

*Tip: Můžete zmínit konkrétní příklad skutečně existující nesolidní aplikace: Nejjasnější svítilna. Aplikace pracuje se světlem mobilu, ale sbírá osobní data a prodává je třetím stranám; požaduje oprávnění přistupovat např. i k úložišti a poloze. Aplikace je stále dostupná na Google Play.*

**Záměr fáze:** Reflexe II: Hlavní myšlenky z dnešní hodiny.

5.1. Nechte každou skupinku říct jednou větou pro mladšího spolužáka nějaký tip z dnešní hodiny.

ODPOVĚDI:

Mělo by zaznívat například:

- ∞ Aplikace mohou zneužít informace z tvého telefonu.
- ∞ Kontroluj, k čemu mají tvé aplikace přístup.
- ∞ Zakaž přístupy, které aplikace nepotřebuje.
- ∞ Nestahuj aplikace z neprověřených zdrojů.

*Tip: Děti můžete nechat některé odpovědi zapsat a uložit do portfolia. Pokud máte ve škole mobilní zóny, můžete tam nejlepší odpovědi vyvěsit.*

*Tip: Problematice se více věnuje následující bakalářská práce z roku 2016: [https://is.muni.cz/th/dvrl1/Bc\\_prace\\_Tesarova.pdf](https://is.muni.cz/th/dvrl1/Bc_prace_Tesarova.pdf)*

**Kamera**

**Bluetooth**

**Fotogalerie**

**Kontakty**

**Mikrofon**

**Přístup k internetu**

**GPS (poloha)**

**Provádění plateb**

## Technický popis 17. dílu:

Marwin připravil pro Kubu překvapení: z křišťálové koule pozná, co Kuba poslední dobou dělal nebo nedělal. Kuba tuší, že jde o trik – jak ho ale Marwin provedl? Marwin vysvětlí, že Kubu špehovala aplikace Doplnkov na smartphonu (od 1:17), protože jí Kuba povolil přístup k informacím z jiných aplikací a periférií telefonu (1:35–1:45).

Přímo v Datové Lhotě pak vidíme, že panáčky z Doplnkova si chodí pro informace do jiných míst v Datové Lhotě, například pro textové dokumenty (2:05), informace o poloze telefonu (2:07), hudební soubory (2:11) nebo fotky (2:15). Marwin upozorní, že takové informace lze snadno zneužít (2:22–2:52).

Naštěstí stačí zakázat Doplnkovu přístup k informacím, které nepotřebuje (3:00–3:24; potřebuje pouze přístup k obrázkům, s nimiž se v aplikaci pracuje – 3:08–3:21). Důsledek je okamžitý – panáčky z Doplnkova už žádné informace, k nimž nemají mít přístup, nedostanou (3:26–3:37). Ukáže se ale, že Kuba povolil přístup dalším aplikacím, a to skoro ke všemu (od 3:38). I to je třeba zakázat (3:46–4:07).

Po návratu kluků z Datové Lhoty projeví o aplikaci Doplnkov zájem Linda (od 4:16), která ale na rozdíl od Kuby ví, že jí musí omezit přístup k většině informací z telefonu.

## Technická poznámka:

V díle není zobrazeno, že informace, které zjistí Doplnkov, tato aplikace pošle přes internet Marwinovi. Na jejich základě potom mohl Marwin předvést na začátku dílu svůj kouzelnický „trik“.

Modelové lekce připravili a na školách vyzkoušeli: Cyril Brom, Anna Drobná, Tereza Hannemann, Pavel Ježek, Ondřej Petíř.

Děkujeme za připomínky k lekcím pro 2. sérii Datové Lhoty [29. 12. 2023]: Štěpánka Baierlová, Eva Kloudová, Hana Kuciánová, Michala Radotínská, Radek Šmíd, Jan Vais, Petr Vincena.

Děkujeme Jitce Šídové ze ZŠ Veronského náměstí v Praze, Heleně Lazarové ze ZŠ Hrabina v Českém Těšíně, Štěpánce Baierlové ze ZŠ Labyrinth v Brně a Petře Ogurekové ze ZŠ Byšice, které nám pomohly s rozsáhlým testováním a jejichž cenné rady jsme do modelových hodin zapracovali. Děkujeme i ZŠ Jungmannovy sady a všem dalším školám, které nám s testováním pomohly.

