# JEJDA, MOJE ZPRÁVY ČTE, KDO NEMÁ.

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

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

- Wi-Fi router („Wi-Fi krabička“) je zařízení, přes které se připojujeme k internetu; naše zařízení se k Wi-Fi routeru připojuje pomocí Wi-Fi signálu
- Hackovat lze prakticky jakékoli zařízení, které má v sobě počítač; ovšem nejsnáze to hackerům jde, pokud je zařízení připojené k internetu

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

- Wi-Fi router (coby „brána“ k internetu)
- hackování
- aktualizace
- IP adresa
- etický hacker

## Základní informace:

### Pouštěná videa:

- 15. díl „Kdo to heknul?“

### Co musí učitel zajistit před realizací lekce:

- podívat se na 15. díl; doporučujeme přečíst i technický popis dílu
- přečíst si instrukce k této lekci
- na lekci je potřeba připravit si následující:
  - video ke spuštění
  - tabule, fixy; promítací plocha
  - Wi-Fi router nebo alespoň jeho fotka
  - papíry a psací potřeby
  - vytištěné pracovní listy

## Shrnutí děje 15. dílu:

Většina školy se dozvěděla, že Linda má ráda tulipány, ale Linda to říkala jen na soukromém chatu. Jak k tomu mohlo dojít? Marwin, Kuba i Linda to jdou zjistit do Datové Lhoty. Všichni tři se po kratší cestě ocitnou na domácím Wi-Fi routeru. Ten je napaden hackovacím programem, jenž přesměrovává komunikaci z celé domácnosti na počítač neznámého útočníka, který si pak balíčky může prohlížet. Trojice se vydá dál na internet až do domácího Wi-Fi routeru útočníka. Na něm Linda odhalí, že hacker je Janáček starší. Marwin aktualizuje firmware domácího Wi-Fi routeru u Kuby a Lindy a změní na něm heslo. Aktualizací se odstraní Janáčkův záškodnický program.

## Lekce v kostce:

**1. fáze** – ÚVOD – Evokace na téma „Co je to hackování a kdo je hacker" (5 min)

**2. fáze** – 15. DÍL „KDO TO HEKNUL?"
– Uvědomění I: Ukázka, co hackeři dovedou (15–20 min)

**3. fáze** – UNPLUGGED AKTIVITA „CO JDE DOMA HACKNOUT"
– Uvědomění II: co všechno jde hacknout a proč by to někdo dělal (10–15 min)

**4. fáze** – ZÁVĚR – Reflexe (5 min)

## Průběh lekce:

### 1. fáze – Úvod 5 min

**Záměr fáze:** Evokace na téma hacker a hackování.

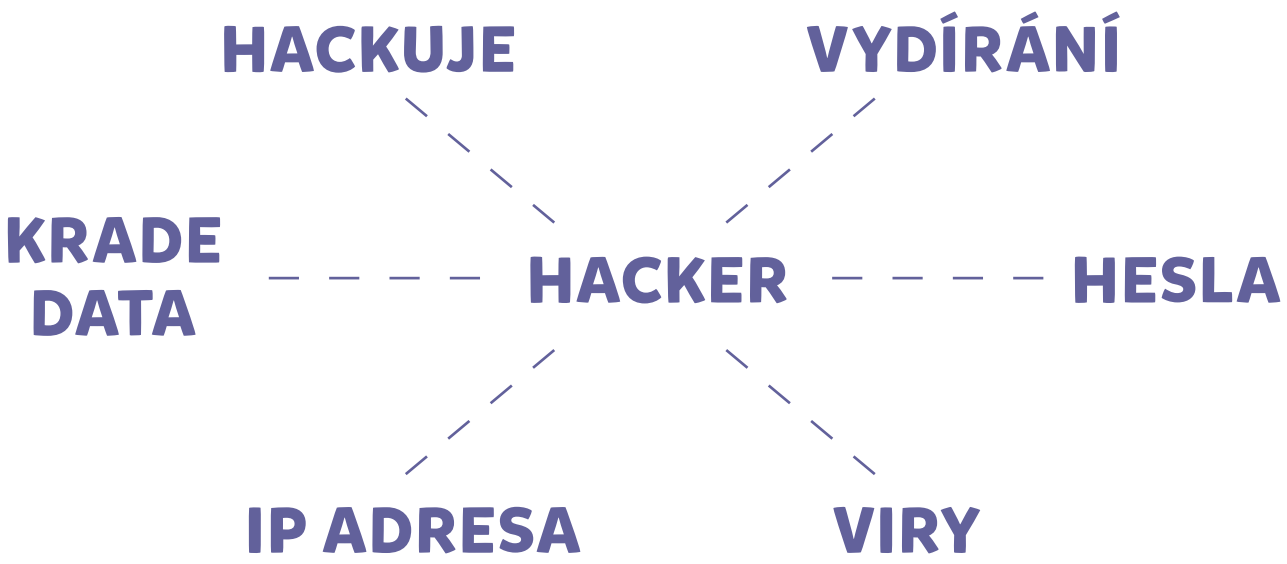
**1.1.** **Evokace** – vytvoření společné, jednoduché myšlenkové mapy (například na tabuli) na téma: „Hacker"

Řekněte: „Když řeknu hacker a hackování, co si pod tím představíte? Budu to psát na tabuli."

Podle odpovědí dětí vytvořte na tabuli jednoduchou myšlenkovou mapu.

*Pozn.:*

- *Myšlenková mapa může vypadat například následovně. Počítejte s tím, že mapa asi nebude příliš detailní a děti nejspíš nebudou znát koncept etických hackerů (viz dále). Někdy také děti budou znát určité slovo, ale nebudou rozumět, co přesně znamená (např. „hackuje zařízení").*




**1.2.** Uzavřete úvod:

„Na jeden ze způsobů, jak nás může někdo hacknout, a jak tomu zabránit, se půjdeme podívat do Datové Lhoty."

## 2. fáze – 15. díl „Kdo to heknul?“ 15 – 20 min

**Záměr fáze:** Uvědomění I: K jakým informacím se hacker umí dostat z pouhé nezabezpečené konverzace přes chat.

**2.1.** Otázka před spuštěním videa: „V díle zjistíme, že Linda se stala obětí hackera. Zjistěte z videa, kdo je hackerem.“

**2.2.** **Pusťte video „15. díl – Kdo to heknul?“**

**2.3.** Rozeberte odpověď na otázku: „Kdo byl hacker?“

**SPRÁVNÁ ODPOVĚĎ:** Janáček starší.

*Pozn.: Janáček ve skutečnosti není opravdovým hackerem, program na hacknutí routeru si mohl stáhnout z internetu. Celý problém pak tví v tom, že domácí Wi-Fi router u Lindy nebyl aktualizovaný a Linda neměla šifrovanou komunikaci s kamarádkami – proto bylo pro Janáčka tak jednoduché zprávy číst.*

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

| Otázka: | Pusťte: | Správná odpověď/poznámka: |
|---|---|---|
| Jaké zařízení bylo ve videu hacknuté? | 1:45 – 2:11 | Wi-Fi router v Kubově domácnosti.<br><br>*Pozn.: Děti budou spíše používat pojem Wi-Fi krabička, internetová krabička nebo modem.* |
| Jak je Wi-Fi router připojen k internetu? | | Typicky kabelem.<br><br>*Pokud máte možnost, **ukažte Wi-Fi router**, síťový kabel i napájecí kabel 230 V; nebo alespoň jejich fotku (Příloha A).*<br><br>*Pozn.: Děti správnou odpověď nemusí znát. Někdy si myslí, že internet je přiveden do Wi-Fi routeru pomocí elektrické sítě. Někdy si také myslí, že pokud má router dvě anténky, jedna se připojuje bezdrátově k družici a druhá vysílá signál po domácnosti. To také není pravda. Většinou je Wi-Fi router připojen kabelem, který vede „pod zem“ směrem ke „kabelové“ síti poskytovatele internetu. Někdy je celá domácnost připojena bezdrátově, ale pak je to buď prostřednictvím mobilních dat (Wi-Fi „krabička“ komunikuje s BTS vysílačem), nebo pomocí Wi-Fi v obci, pokud je tam zavedena, či výhledově pomocí družice (pak může vést z Wi-Fi routeru kabel do antény na domě, která je buď přes Wi-Fi signál připojena k obecnímu Wi-Fi routeru, nebo k satelitu na oběžné dráze).* |
| Co Marwin udělal, aby se problému zbavil? | 3:28 – 4:01 | Aktualizoval router a změnil na něj přihlašovací heslo.<br><br>*Zdůrazněte, že prakticky ve všech programech bývají **chyby**, kterých hackeři využívají, a firmy chyby odstraňují aktualizacemi. Také vypíchněte, že hesla přednastavená z výroby je třeba změnit.*<br><br>*Pozn.: IP adresa 192.168.1.1 bývá někdy lokální adresa domácího Wi-Fi routeru (někdy může být tato IP adresa i jiná).* |

| | | |
|---|---|---|
| Co dělal záškodnický program na Wi-Fi routeru u Kuby doma? | 2:05 – 2:20 | Panáčci vyměňovali (přelepovali) IP adresy příjemce. Zprávy pak chodily přes počítač hackera, který si je mohl přečíst.<br><br>*Připomeňte dětem, **co je IP adresa**: adresa v digitálním světě, kterou má každé zařízení připojené k internetu.*<br><br>*Pozn.: Počítač hackera pak pakety odešle původnímu adresátovi, takže pakety dorazí ke svému cíli. Můžete to vysvětlit pomocí metafory poštovní obálky: Hacker původní adresu přelepí lístečkem s hackerovou adresou, a až obálka dorazí k němu domů, lísteček odstraní a odešle dopis na původní adresu. Jedná se o útok typu „man in the middle".* |
| Pro druhou úroveň:<br><br>Mohl by číst Janáček starší Lindiny zprávy, kdyby používala šifrovanou komunikaci? | | Přímo zprávy by číst nemohl.<br><br>*Pozn.: Pokud se pro šifrování zpráv používá tzv. koncové neboli „end-to-end" šifrování např. WhatsAppem, pak se přímo k obsahu datových zpráv Janáček nedostane. Stále ale bude mít přístup například k cílovým IP adresám datových balíčků (tomu by šlo zabránit pokročilejšími systémy typu Tor). Pokud se šifruje pouze část cesty, může hacker podvrhnout i toto šifrování, proto je lepší používat koncové šifrování (ne vždy je to ale možné). Nezašifrované zprávy si hacker přečte rovnou. Šifrování jako takové doporučujeme probrat v jiné hodině.* |

*Tipy k ukazování Wi-Fi routeru pro 2. úroveň:*

- *Můžete ukázat, že Wi-Fi router má více ethernetových zásuvek, přičemž jedna obvykle vede „ven na internet" a další mohou vést k zařízením připojeným přes kabel doma. „Ven na internet" může znamenat například směrem k síťovému routeru poskytovatele internetu (nebo třeba k domácí anténě, pokud je domácnost připojena bezdrátově k obecnímu Wi-Fi routeru).*
- *Můžete třídu upozornit, že Wi-Fi komunikace funguje následovně: Wi-Fi router vyšle zprávu pomocí Wi-Fi signálu, který zachytí příslušné zařízení. Toto zařízení zprávu zpracuje a pošle odpověď Wi-Fi signálem zpátky. Tedy i zařízení v domácnosti slouží jako Wi-Fi přijímač i vysílač. Děti mohou mít miskoncepci, že Wi-Fi je něco jako „éter" (nebo „neviditelná voda"), který kolem sebe Wi-Fi router rozlévá, a zařízení v domácnosti pak tento éter zachytávají nebo přes něj posílají zprávy (jako by pak zařízení mohla po „neviditelné vodě" vyslat jakýmkoli směrem jakousi „loďku" – například dva mobily mezi sebou přímo).*
- *Náš Wi-Fi router je tedy vstupní branou na internet. Chceme-li vyhledat nějakou stránku, Wi-Fi router se spojí se serverem (přes složitou síť internetových kabelů a někdy částečně i bezdrátového spojení), na kterém je stránka uložená, pomocí IP adresy serveru.*
- *Ani pro 2. úroveň nedoporučujeme snažit se děti učit rozdíly mezi koncepty routeru, switche, hubu, modemu apod. – koncepty jsou pro děti příliš složité. Důležité je budovat představu „Wi-Fi krabičky", která je „branou k internetu", spíše než například formálně správnější představu „routeru" coby zařízení, které propojuje sítě, apod.*

*Tip k IP adrese pro 2. úroveň:*

- *Můžete napsat na tabuli, jak vypadá IPv4.*
- *Můžete upozornit i na nedostatek adres IPv4 a z toho plynoucí IPv6 resp. veřejné a neveřejné IP adresy a mechanismus NAT; pozor ale, že toto téma je poměrně pokročilé, zabere nějaký čas na vysvětlení a může být vhodnější ho probrat v jiné hodině.*

**2.4.** Vraťte se k myšlenkové mapě a nechte děti doplnit další informace.

*Tip: Osvědčilo se nám použít jinou barvu fixy/křídy.*

**2.5.** Upozorněte děti, že video ukazovalo jen jeden z mnoha způsobů hackování.

Zároveň jim řekněte, že existují i hodní hackeři, kterým říkáme **etičtí hackeři** (anglicky: white hat), a doplňte je do myšlenkové mapy.

*Pozn.: Žáci nejspíš nebudou znát pojem etický hacker. Etický hacker je zaměstnání v IT světě. Vysvětlete: „Etický hacker je člověk, který dokáže přemýšlet jako hacker a využívá přitom svoje znalosti legálně, aby pomáhal uživatelům nebo firmám s ochranou informací, hledáním slabých míst v zabezpečení a obecně obranou proti hackerům, kteří škodí."*

*Tip pro 2. úroveň: Pokud děti bezpečně vědí, co je server, můžete jim vysvětlit, že jiným oblíbeným hackerským kouskem je útok typu DDoS – distributed denial of service (česky lze přeložit zhruba jako: distribuované odepření služby). Jde o to, že server zahltíme obrovským množstvím požadavků z mnoha různých počítačů a server tak přestane být schopen zpracovávat požadavky běžných uživatelů. Představte si, že ve třídě místo toho, aby se děti hlásily, všechny najednou budou křičet na učitele svou otázku. Učitel (v pozici serveru) nedokáže pořádně odpovědět nikomu.*

## 3. fáze – Aktivita „Co jde doma hacknout" 10 – 15 min

**Záměr fáze**: Uvědomění II: Hacknout lze jakékoli zařízení, které obsahuje počítač. Jednodušší to je, pokud je zařízení připojeno přes internet. Je třeba být obezřetný a aktualizovat, protože hacker se může dostat k informacím, které lze zneužít.

**3.1.** Děti rozdělte do skupinek.

**3.2.** Každému dítěti rozdejte pracovní list. Zadejte pokyn: „Ve skupinkách se během 5 minut poraďte:

a) co za zařízení lze hacknout,

b) kde musí hacker fyzicky být, aby dané zařízení hacknul,

c) proč by to hacker dělal.

Každý žák si bude na svůj list dělat poznámky."

Polovině skupin zadejte část A, polovině část B.

*Pozn.:*

- *Každý žák má svůj pracovní list, aby si ho poté mohl založit do portfolia. Pokud portfolio nepoužíváte, postačí vám jeden list na skupinu.*
- *Podle úrovně své třídy můžete skupinkám zadat více či méně zařízení, než je v části A/B.*

**3.3.** Po pěti minutách se ptejte na jednotlivá zařízení a nechte děti odpovídat.

Směřovat byste měli k tomu, že **pokud zařízení obsahuje počítač, jde hacknout**. Pokud se zařízení připojuje k internetu, hacker může zařízení hacknout z internetu. Pokud se zařízení nepřipojuje k internetu, hacker se k němu musí dostat fyzicky.

*Poznámky ke konkrétním zařízením:*

- ***Chytré auto**: Obsahuje desítky počítačů, které tvoří několik malých počítačových sítí. Zařízení z těch sítí, které se připojují k internetu, lze hacknout po internetu. Výrobci aut se snaží dělat aktualizace (a pracovat s etickými hackery), sami se ale nemáme moc možností proti hackování auta bránit. Hacker může např. sledovat polohu auta, ale i například vypnout motor v jízdě na dálnici a spáchat teroristický čin[1]. 40 let staré auto počítače neobsahuje, a hacknout ho nemůžeme.*
- ***Wi-Fi router**: Viz 15. díl Datové Lhoty. Pokud hackneme Wi-Fi router, máme otevřenou bránu k zařízením v domácnosti, která se na Wi-Fi router připojují. To se týká i zařízení, která se připojují na Wi-Fi router, ale už nepřistupují dál k internetu.*

1 Viz například https://www.youtube.com/watch?v=MK0SrxBC1xs.

- ***Chůvička připojená na Wi-Fi**: Lze hacknout přes Wi-Fi router po internetu, hacker se může dostat k zvukovému nebo obrazovému streamu a pak nás vydírat (tyto chůvičky vesměs mají webkameru a jsou umístěny v ložnicích). Doporučujeme se spíše těmto chůvičkám vyhýbat nebo je používat velmi obezřetně. Starší radiové chůvičky po internetu hacknout nelze.*
- ***Notebook s webkamerou**: Připojuje se k internetu, lze hacknout po internetu. Hacker se může dostat k citlivým údajům, např. k elektronickému bankovnictví. Může sledovat všechno, co na notebooku děláme. V důsledku nás pak může vykrást, vydírat. Našim kontaktům může zasílat spamy. Může náš notebook použít k nezákonným aktivitám (např. dalšímu hackerskému útoku). Notebook je třeba aktualizovat. Webkameru je třeba mít zalepenou/zakrytou, pokud ji zrovna nepoužíváme. (Některé novější notebooky už obsahují záklopky na webkamery.)*
- ***Chytrá TV**: Je obvykle připojena k internetu, takže lze hacknout po internetu. Pokud má ovládání hlasem, má automaticky zapnutý mikrofon, který lze zneužít k odposlouchávání. Hacker by také například mohl kontrolovat, jaký obsah televize pouští.*
- ***Mixér**: Novější modely sice mohou obsahovat počítač, ale k internetu se obvykle nepřipojují. Hacker by se tedy musel dostat přímo k mixéru – k nějakému skrytému vstupu, pomocí kterého lze nahrávat do počítače v mixéru data. Možnosti zneužití jsou značně omezené. Starší mixéry bez počítačů hacknout vůbec nelze.*
- ***Bojler s ovládáním na Bluetooth**: Pokud se nepřipojuje k internetu, lze hacknout jen na vzdálenost Bluetooth signálu. Hacker by teoreticky mohl kontrolovat spotřebu teplé vody a bojler například přehřát.*

**3.4.** Uzavřete ve smyslu: Je třeba být obezřetný, hackeři se můžou dostat skoro kamkoliv, **kde je počítač**, zejména pokud je počítač připojený k internetu – a proto aktualizujte a mějte silná hesla (a mějte antivirus a neklikejte na neznámé odkazy). Pokud to jde, používejte end-to-end šifrování.

*Pozn.: Hacker vs. virus: Hacker je člověk, virus je program. Hacker ale může počítačový virus využít k hackování.*

## 4. fáze – Reflexe 5–10 min

**Záměr fáze:** Děti by si měly zafixovat, že je třeba počítačová zařízení aktualizovat a zajímat se o to, jakým způsobem je naše komunikace šifrovaná.

**4.1.** Vyzvěte žáky k doplnění myšlenkové mapy. Pokud máte dost času, nechte děti překreslit si tuto mapu na druhou stranu pracovního listu.

*Tip: Myšlenkovou mapu mohou také děti kreslit do pracovního listu znovu samy na začátku další hodiny coby opakování.*

**4.2.** Nechte třídu odpovídat na následující otázky.

*Tip: Dotazování také můžete zařadit na začátek další hodiny coby opakování.*

| **Otázka:** | **Správná odpověď/poznámka:** |
|---|---|
| Jak se co nejlépe můžeme ubránit útokům hackerů? | • Mít aktualizovaný počítač včetně antiviru, a ideálně i domácí Wi-Fi router.<br>• Mít silná hesla včetně hesla k Wi-Fi routeru.<br>• Mít zakrytou webkameru, pokud ji zrovna nepoužíváme.<br>• Neinstalovat podezřelé programy/programy z neznámých zdrojů.<br>• Neklikat na podezřelé odkazy, např. v podezřelých mailech.<br>• Používat pro komunikaci aplikace s end-to-end šifrováním, pokud to jde.<br>• Používat dvoufaktorové ověření, pokud to jde.<br>*Pozn.: Nic ale není stoprocentní ochrana. Přirovnání: Když budeme dodržovat všechna pravidla silničního provozu, snižujeme tím pravděpodobnost, že se nám něco stane na ulici; stoprocentní jistotu ale nemáme, pokud chceme vyjít z domu ven.* |
| Jaká všechna zařízení může hacker hacknout? | Víceméně jakékoli **počítačové** zařízení (tj. obsahující počítač), pokud není úplně odříznuté od světa. |

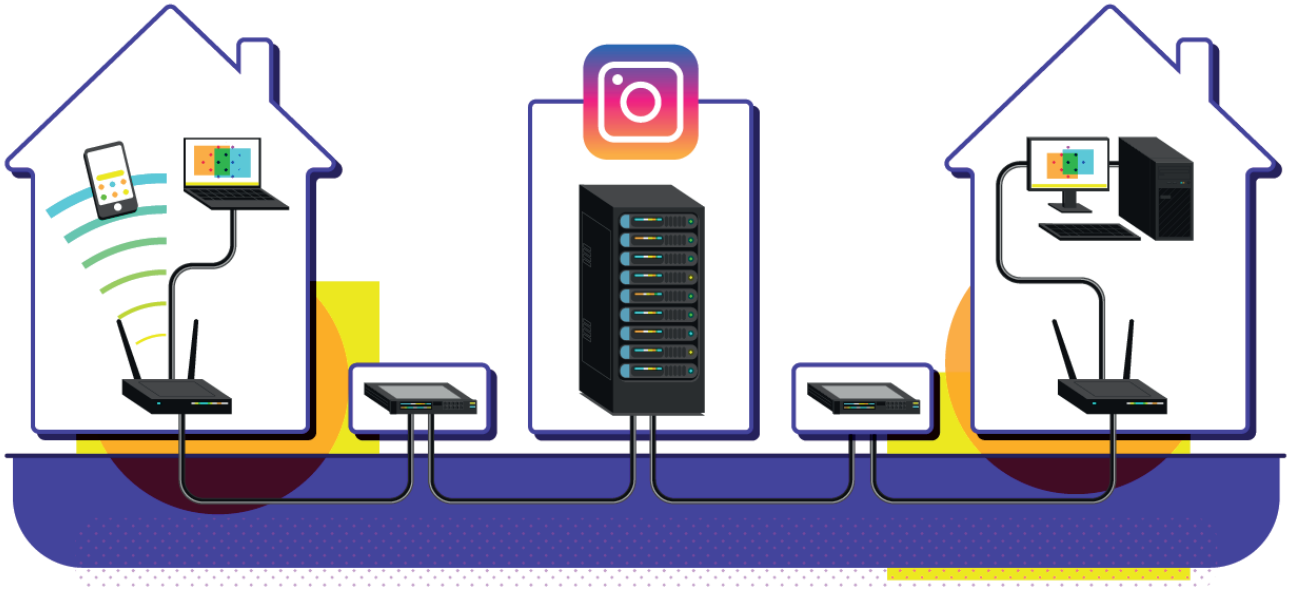
| | |
|---|---|
| Může hacker hacknout počítače, které řídí provoz v jaderné elektrárně? | Velmi těžko, protože tyto řídící počítače záměrně nejsou připojené k internetu a dostat se k nim fyzicky je pro člověka mimo elektrárnu velmi obtížné. Jaderné elektrárny jsou velmi dobře zabezpečené.<br><br>*Pozn.: Hacker by se musel do elektrárny vloupat nebo přesvědčit k záškodnické činnosti zaměstnance elektrárny – ti jsou ovšem velmi dobře prověřováni a jen tak by se k záškodnické činnosti přesvědčit nenechali. Smysl otázky je (kromě uklidnění) ukázat, že kritické systémy obvykle jsou dobře zabezpečené proti hacknutí, ale takové zabezpečení je náročné a drahé. Většina zařízení nemůže být zabezpečena na úrovni jaderné elektrárny.* |
| Lze otestovat, jestli je počítačový systém, například v bance, dobře zabezpečený proti hackerům? | Ano, pomocí speciálních testů, které dělají například etičtí („hodní“) hackeři. |

**4.3.** Vyzvěte skupinky žáků, aby každá řekla jednou větou jednu věc, která pro ně byla v dnešní hodině překvapivá/nová nebo kterou zatím nedělali a dělat začnou.

Nechte žáky tyto body zapsat na druhou stranu pracovního listu.

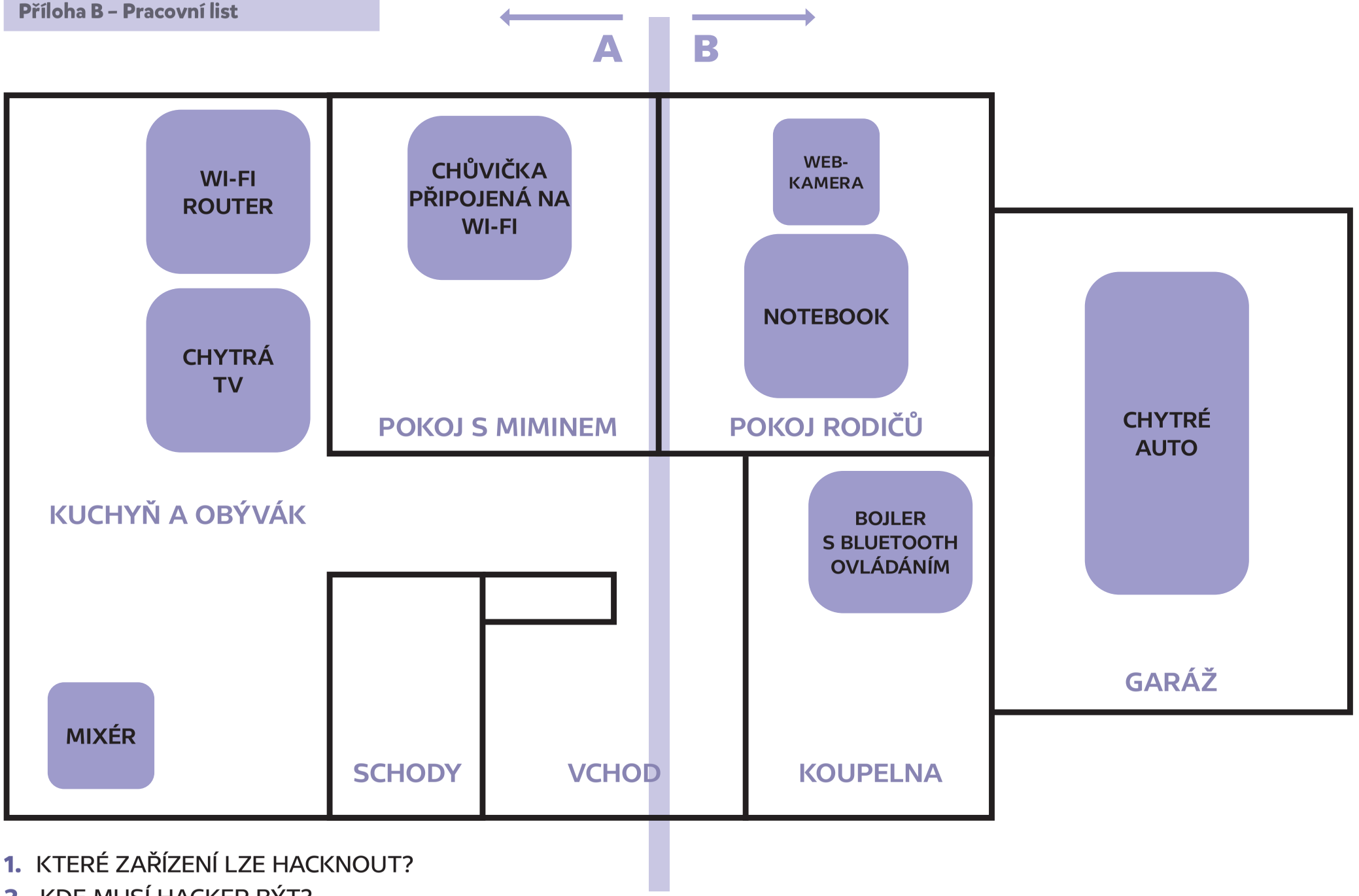
## Příloha A – Jak se připojujeme na internet?

**Internet** je **celosvětová síť** propojených počítačů. Velmi zjednodušeně vypadá takto:



Vidíme zde dvě domácnosti, v nichž mohou být uživatelská zařízení: mobily, tablety, počítače a tak dále. Konkrétně zde jsou tato zařízení připojena přes Wi-Fi nebo kabelem k **Wi-Fi routeru**. Wi-Fi router je většinou připojený k internetu **kabelem**.

Uprostřed vidíme **servery** (v tomto případě jde o servery aplikace Instagram). Servery jsou důležité počítače, které nám poskytují veškeré služby internetu (třeba posílání zpráv na Instagramu nebo streamování na Twitchi) a ukládají naše data, která na internet pošleme. Takových serverů jsou na světě miliony. Více viz: https://internet4kids.mff.cuni.cz/jak-funguje-internet-vysvetleni/




1. KTERÉ ZAŘÍZENÍ LZE HACKNOUT?
2. KDE MUSÍ HACKER BÝT?
3. PROČ BY TO HACKER DĚLAL?

# PROSTOR PRO TVOJE POZNÁMKY

HACKOVÁNÍ



Hlavní myšlenky dnešní hodiny

1) .....

2) .....

3) .....

4) .....

5) .....

## Technický popis 15. dílu:

Většina školy se dozvěděla, že Linda má ráda tulipány, ale Linda to říkala jen na soukromém chatu (0:32, 0:59). Jak k tomu mohlo dojít? Marwin si myslí, že Lindě někdo hacknul počítač, protože ho nemá aktualizovaný (1:16), ale Linda ho vyvede z omylu – aktualizovaný ho má (1:22). Nezbývá než se podívat, v čem je problém, do Datové Lhoty – a tentokrát i s Lindou.

Všichni tři se ocitnou v síťovém ovladači (Síťově) na notebooku Lindy (1:44–1:47), odkud rychle zamíří po sběrnici (koleje s vozíčkem) na síťovou kartu notebooku (1:48–1:57). Odsud se dostanou bezdrátově na síťovou kartu domácího Wi-Fi routeru (1:58) a do jeho operační paměti (2:05–2:28). Zde se ukáže, že domácí Wi-Fi router je napaden hackovacím programem, který přesměrovává (2:07–2:20) veškerou komunikaci z celé domácnosti na počítač neznámého útočníka, který si pak balíčky může prohlížet (balíčky se zprávami školního chatu nejsou šifrované, jak znázorňuje jejich žlutá barva a absence zámečku).

Trojice se vydá dál na internet až do domácího Wi-Fi routeru útočníka – udělá to tak, že sleduje, kam balíčky s přelepenou IP adresou přes internet putují (2:29–2:45). Na Wi-Fi routeru útočníka Linda nahlédne do nešifrované komunikace ze školního chatu (3:04), čímž odhalí, že hacker je Janáček starší. Marwin nachystá (mimo záběr) past na Janáčka: poté, co se přes prohlížeč připojí Janáček na internet, začne jeho Wi-Fi router posílat na Janáčkův počítač falešný HTML kód fiktivní webové stránky „Nešmíruj Janáčku" (4:26). Nakonec Marwin aktualizuje firmware domácího Wi-Fi routeru u Kuby a Lindy (3:33–3:47) a změní na něm heslo (3:58). Aktualizací se odstraní záškodnický program od Janáčka.

## Technická poznámka:

V díle byl zobrazen pouze jeden z mnoha typů hackování. Je založen na tom, že se internetová komunikace z hacknutého Wi-Fi routeru přepošle „odbočkou" útočníkovi, který si ji může prohlédnout, než ji pošle na původní místo určení (je to podobné, jako když tajná policie čte cizí poštu). Celá komunikace tak trvá o chvilku déle, ale nakonec zprávy dorazí na místo určení. Janáček starší má přitom přístup k veškeré komunikaci z hacknutých domácností: tedy například i k tomu, jaké webové stránky si prohlíží rodiče Kuby a Lindy.

Pokud se pro šifrování zpráv používá tzv. koncové neboli „end-to-end" šifrování speciální aplikací, pak se přímo k obsahu datových zpráv Janáček nedostane. Stále ale bude mít přístup například k cílovým IP adresám datových balíčků (tomu by šlo zabránit pokročilejšími kryptografickými systémy typu Tor). Pokud se šifruje pouze část cesty, může hacker podvrhnout i toto šifrování, proto je lepší používat koncové šifrování (ne vždy je ale koncové šifrování možné).

Janáček starší nemusel program na hacknutí routeru sám naprogramovat. Takový program se dá stáhnout a hackovat tak mohou i méně ICT zdatní jedinci…

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]: Štepánka 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.