JEJDA, MŮJ POČÍTAČ MÁ VIR

Délka lekce: 40 minut

Cíl lekce

Cílem je děti naučit, jak počítačové viry mohou škodit našim počítačům, tabletům a smartphonům, a jak se proti počítačovým virům bránit.

DĚTI SE Z TÉTO LEKCE DOZVÍ:

- Počítačové viry škodí našim počítačům, tabletům a smartphonům a je zapotřebí se před nimi chránit.
- Antivir je program, který pomáhá chránit naše počítače, tablety a smartphony před viry.
- Pro správné fungování antiviru (a programů obecně) potřebujeme antivir, jakož i další programy, pravidelně aktualizovat.
- Ani aktualizovaný antivir neposkytuje stoprocentní ochranu – a hlavně už obvykle nedokáže napravit škodu, kterou viry nadělaly. Musíme se především v digitálním světě zodpovědně chovat.

Pozn.: Lekce uvádí i příklady, jak mohou různé druhy virů škodit – podle naší zkušenosti je toto téma zejména pro mladší děti velmi obtížné, a proto znalost různých druhů virů nepovažujeme za klíčový výstup lekce. Stejně tak je pro mladší děti často obtížné pochopit myšlenku, že antivir neposkytuje stoprocentní ochranu. Z naší zkušenosti jsou mladší děti většinou schopné pochopit pouze to, že vir škodí a antivir ochraňuje.

DĚTI SE NAUČÍ TATO NOVÁ SLOVA/KONCEPTY:

- počítačový vir
- antivir
- aktualizace

Základní informace

Pouštěná videa:

- 7. díl „Viry útočí“
- Talkshow „O virech“ (zhruba navazuje na 7. díl)

Pozn.: Pozor nenechte se zmást: to, že některé děti tráví na počítačových zařízeních velké množství času, ještě neznamená, že mají veliké znalosti!

Co musí učitel zajistit před realizací lekce:

- podívat se na video 7. díl – „Viry útočí“ a na talkshow „O virech“ a zkusit si stopovat jednotlivé ukázky
- přečíst si veškeré instrukce k této lekci
- na lekci je potřeba připravit si následující:
  - videa pro spuštění
  - vytisknutý průběh lekce
  - vytisknuté papíry s aktivitou
  - děti budou potřebovat tužku a gumu

Shrnutí děje 7. dílu – „Viry útočí“:

Kuba vchází do školy a zdálky slyší spolužáky, kteří se smějí. Kamarád Marwin mu vysvětlí, že se smějí jemu, protože viděli jeho směšné video s plyšovou okurkou (hračka). Kuba si není vědom, že by video natočil a rozeslal. Neví, co má teď dělat. Doma si všimne, že se mu sama zapnula webkamera a vydá se do Datové Lhoty zjistit, co za tím vězí. Setká se s počítačovými viry, které mu spustily webkameru a poté se videa zmocnily. Naštěstí se objeví Marwin. Začne se divit, proč Kuba nemá

spuštěný antivir. Kuba mu sdělí, že ho vypnul, protože mu vadilo, že se dlouho aktualizuje. Marwin Kubovi vysvětlí, že to už příště dělat nemá – bez aktualizovaného antiviru hrozí jeho počítači virová invaze. Zároveň Kubovi pomůže situaci zvládnout tím, že antivir spustí. Přitom Kubovi vysvětlí, jak viry dokázaly rozeslat video nahrané přes webkameru spolužákům.

Kapitoly talkshow:

- Viry
- Příklady počítačových virů
  - Špehouni („spyware")
  - Vyděrači („ransomware")
- Jak se viry dostaly ke Kubovi
- Viry a mobily

Pozn.: Záměrně nezařazujeme další typ virů, o kterých se v talkshow také mluví – těžební viry. Máme zkušenost, že těžební viry jsou pro většinu dětí těžko pochopitelné.

Lekce v kostce

1. fáze – ÚVOD – Seznámení se s tématem lekce (5 min)
2. fáze – 7. DÍL „VIRY ÚTOČÍ" – počítačový vir, antivir, aktualizace (15 min)
3. fáze – AKTIVITA „ODSTRAŇOVÁNÍ VIRU" (5 min)
4. fáze – TALKSHOW „O VIRECH" (10 min)
5. fáze – ZÁVĚR – Shrnutí a zopakování nových poznatků (5 min)

Průběh lekce

1. fáze – Úvod 5 min

Záměr fáze: Učitel představí téma a získá přehled o orientovanosti dětí v tématu.

1.1. Řekněte: „Dnes budeme mluvit o počítačových virech."

Položte dětem následující „rozehřívací" otázky:

- „Kdo jste se někdy setkal s počítačovým virem?"
- „Co je antivir?"
- „Kdo jste se setkal s aktualizacemi (v počítači nebo smartphonu)"?

Pozn.: Podle toho, kolik toho děti umí předem, je vhodné upravit čas věnovaný vysvětlení jednotlivých pojmů. Znalosti dětí, s nimiž jsme se setkali v letech 2019 a 2020, byly obecně velmi malé až nulové.

Terminologická pozn.: Vyplatilo se nám používat pojmy vir a antivir, nikoli virus a antivirus – první dvojice byla pro děti srozumitelnější.

2. fáze – 7. díl „Viry útočí" 15 min

Záměr fáze: Děti se dozví (nebo si zopakují) základní definici počítačového viru; dozví se, co je antivir a co jsou aktualizace.

2.1. Před puštěním videa řekněte: „Více nám k tématu řekne díl seriálu Datová Lhota s názvem **Viry útočí**. Dozvíme se, co se Kubovi stalo, když byl jeho počítač napaden počítačovým virem. Po videu se vás zeptám: **Co je to ten počítačový vir a co nám může způsobit?**"

Pozn.: Máme zkušenost, že pro některé děti je jednodušší odpovědět na otázku „Co nám může vir způsobit?" než „Co je to počítačový vir?" a naopak. Proto pokládáme obě najednou.

2.2. **Pusťte celé video „7.díl – Viry útočí"**

2.3. Vyzvěte děti: „Rozmyslete si, co je to počítačový vir a co nám může způsobit."

Nechte děti přemýšlet asi minutu.

V rámci času, který je k dispozici, nechte odpovídat co nejvíce děti, které se hlásí. S odpověďmi se vám může hodit v další fázi pracovat.

SPRÁVNÁ ODPOVĚĎ: Vir je počítačový program, který škodí počítači.

Pozn.: Zatím není třeba dětem vysvětlovat, jak přesně může počítačový vir škodit, to bude předmětem další části lekce.

2.4. Řekněte: „Nyní se na některé věci podíváme trochu zblízka."

Pro úroveň 1:

Řekněte:	Pusťte:	Správná odpověď / poznámka:
Před spuštěním se zeptejte: „Zjistěte z videa, jak chránit náš počítač, tablet nebo smartphone před viry." **Po** stopnutí otázku zopakujte.	2:35 - 2:41	Potřebujeme antivir. To je program, který chrání naše zařízení před viry.
Před spuštěním se zeptejte: „Jakou chybu Kuba udělal?" **Po** stopnutí otázku zopakujte.	3:35 – 4:06	Kuba si rozklikl neznámý odkaz (link) na videohru a s ní si stáhnul do počítače vir. *Dětem je dobré zdůraznit, že než na něco kliknou, musí si ověřit, že jde o důvěryhodný odkaz – například zeptat se někoho, kdo počítačům rozumí.*
Před spuštěním se zeptejte: „Co slíbil Kuba Marwinovi?" **Po** stopnutí otázku zopakujte.	4:06 – 4:22	Že bude mít antivir vždy zapnutý a aktualizovaný.

Pozn.: Rozdíl mezi přístupem v úrovni 1 a 2 tkví zejména v tom, že pro úroveň 2 zdůrazňujeme, že ani aktualizovaný antivir neposkytuje stoprocentní ochranu – chceme zabránit falešnému pocitu bezpečí v případě nainstalovaného antiviru. Máme zkušenost, že pro úroveň 1 je tato myšlenka příliš složitá.

PRO ÚROVEŇ 2:

Řekněte:	Pusťte:	Správná odpověď / poznámka:
Před spuštěním se zeptejte: „Zjistěte z videa, jak chránit náš počítač, tablet nebo smartphone před viry." **Po** stopnutí otázku zopakujte.	2:35 – 2:41	Potřebujeme antivir. To je program, který **pomáhá** chránit naše zařízení před viry.
Před spuštěním se zeptejte: „Jakou chybu Kuba udělal?" **Po** stopnutí otázku zopakujte.	3:35 – 4:06	Kuba si rozklikl neznámý odkaz (link) na videohru a s ní si stáhnul do počítače vir. *Dětem je dobré zdůraznit, že ani antivir **není stoprocentní ochrana**, a než na něco kliknou, musí si v **každém případě** ověřit, že jde o důvěryhodný odkaz – například zeptat se někoho, kdo počítačům rozumí.*

Řekněte:	Pusťte:	Správná odpověď / poznámka:
Před spuštěním se zeptejte: „Co slíbil Kuba Marwinovi?“ **Po** stopnutí otázku zopakujte.	4:06 – 4:22	Že bude mít antivir vždy zapnutý a aktualizovaný.

2.5. Zeptejte se: „A co to ty aktualizace vlastně jsou?“

Naveďte děti v diskusi k tomu, že jde o novější verze programu: jejich vylepšení. Důležité je, že musíme aktualizovat nejen antivir, **ale i ostatní programy**.

Pozn.: Naším hlavním cílem nyní je, aby děti pochopily, že je třeba programy, včetně antiviru, aktualizovat. Podrobnosti o fungování aktualizací rozebírá lekce „Co je to počítačový program“; tyto podrobnosti pro účely lekce „Počítačové viry“ nejsou důležité.

Pozn.: Pro mladší děti obvykle funguje následující metafora: Neustále vznikají nové počítačové viry. Aktualizace antiviru lze chápat jako vylepšení „bojových schopností“ antiviru proti těmto novým virům (nebo jako očkování proti nové nemoci).

3. fáze – Aktivita „Odstraňování viru“ 5 min

Záměr fáze: Podtrhnout skutečnost, že antivir sice odstraní počítačové viry, ale obvykle nemůže odstranit škodu, kterou vir napáchal.

3.1. Rozdejte dětem papíry s vytisknutou aktivitou (viz Příloha 1).

Řekněte: „Představte si, že toto je váš tablet, který napadnul vir. Nakreslete tento vir. Použijte pouze obyčejnou tužku.“

Nechte dětem jen tužky, protože vzápětí budou zase gumovat. Nechte jim na aktivitu jen 2–3 minuty, aby jim pak nebylo líto, že si musí vygumovat svůj dokonalý vir. Zejména u úrovně 2 stačí opravdu krátký čas.

Pozn.: Máme zkušenost, že i přes krátký čas je některým dětem trochu líto, že mají vir vygumovat. Můžeme toho didakticky využít: říct jim, že pokud jim vir smaže fotky apod., bude jim to také líto.

3.2. Řekněte: „Nyní si vezměte gumu a vir vygumujte. Vaše guma je jako antivir, který vir smaže.“

3.3. Až děti vygumují své viry, řekněte: „Podívejte se na váš tablet. Zmizel vir úplně nebo po něm na papíru zůstala nějaká stopa?“

SPRÁVNÁ ODPOVĚĎ: Na papíru zůstaly vrypy tužkou.

Řekněte: „Po viru skoro vždy zůstane nějaká stopa. Antivir vir smaže, podobně jako vaše guma. Ale už nenapraví to, co vir způsobil, stejně jako vy už nemůžete odstranit vrypy tužkou do papíru. Na příklad video s Kubou a okurkou je poslané po celé škole a smazat ho už nejde.“

4. fáze – Talkshow „O virech“ 10 min

Záměr fáze: Děti se dozví, že existuje více typů virů; dozví se příklady toho, co mohou v našem počítači viry napáchat a jaké nepříjemnosti nám způsobit.

4.1. Řekněte: „Pustíme si Kubovu talkshow, kde se dozvíme o virech pár věcí. Sledujte, co všechno viry umí.“

4.2. **Pusťte celé video Kubovy talkshow „O virech“**

4.3. Řekněte: „Nyní si zopakujeme pár důležitých bodů."

Pozn.: Pokud se chcete tématu věnovat déle, můžete nyní děti vyzvat, aby popsaly, co všechno mohou viry v počítači způsobit. Pokud máte času méně, pokračujte rovnou podle následující tabulky.

Řekněte	Pusťte	Správná odpověď / poznámka
Před spuštěním se zeptejte: „Jak mohou viry v počítači škodit?" **Po** stopnutí se zeptejte: „O jakých příkladech virů se ve videu hovořilo?	1:00 – 2:02	Špehovací viry (spyware) a viry vyděrači. *Zdůrazněte, že existují i další typy virů; toto byly jen ukázky. Máte-li čas, můžete koncepty znovu vysvětlit:* ∞ *Špehouni – vyšpehují, co na počítači děláte; mohou například zapnout webkameru nebo sledovat, co píšete na klávesnici (třeba heslo). Potom mohou vše poslat na internet. Mohou najít i vaše kontakty.* ∞ *Vyděrači – Potají zašifrují věci na vašem počítači a vy se k nim pak nedostanete, dokud nezaplatíte.*
Před spuštěním se zeptejte: „Jak se vir ke Kubovi dostal?" *Pozn.: To, že děti nemají klikat na neznámé odkazy, je důležitý koncept, proto se k němu vracíme podruhé (poprvé viz 2.4). Nemáte-li však čas, tuto ukázku přeskočte.*	4:20 – 4:31	Kuba si rozklikl neznámý odkaz na videohru a s ní si stáhnul do počítače vir. *Můžete zdůraznit, že pokud si někdo ve škole stáhnul Kubovo video a neměl aktualizovaný antivir, nejspíš se mu s videem do zařízení dostal i náš vir. Vir si lze stáhnout nejen s hrou, ale například i s videem.* Pro úroveň 2: Je vhodné zmínit, že žádná ochrana není absolutně spolehlivá. V ideálním případě je tedy potřeba kombinovat funkční antivir, aktualizace a neklikání na podezřelé odkazy.
Po stopnutí se zeptejte: „Může se vir dostat i na smartphone?"	4:31 – 5:21	Ano. I na smartphonu musíme mít aktualizovaný antivir.

*Zbyde-li vám čas, z dalších typů škodlivých aplikací může být užitečné zmínit nechtěný **adware**: program, který nutí uživateli nechtěnou reklamu (například pomocí vyskakujících oken prohlížeče). Adware se typicky objeví, když bezmyšlenkovitě navštěvujeme neznámé stránky nebo stahujeme aplikace z neověřených zdrojů. Můžete také zmínit, že vir lze do počítače mimoděk nahrát z jakéhokoli přenosného média, třeba flashky.*

5. fáze – Závěr 5 min

Záměr fáze: Zopakování všech důležitých informací, prostor pro dotazy dětí.

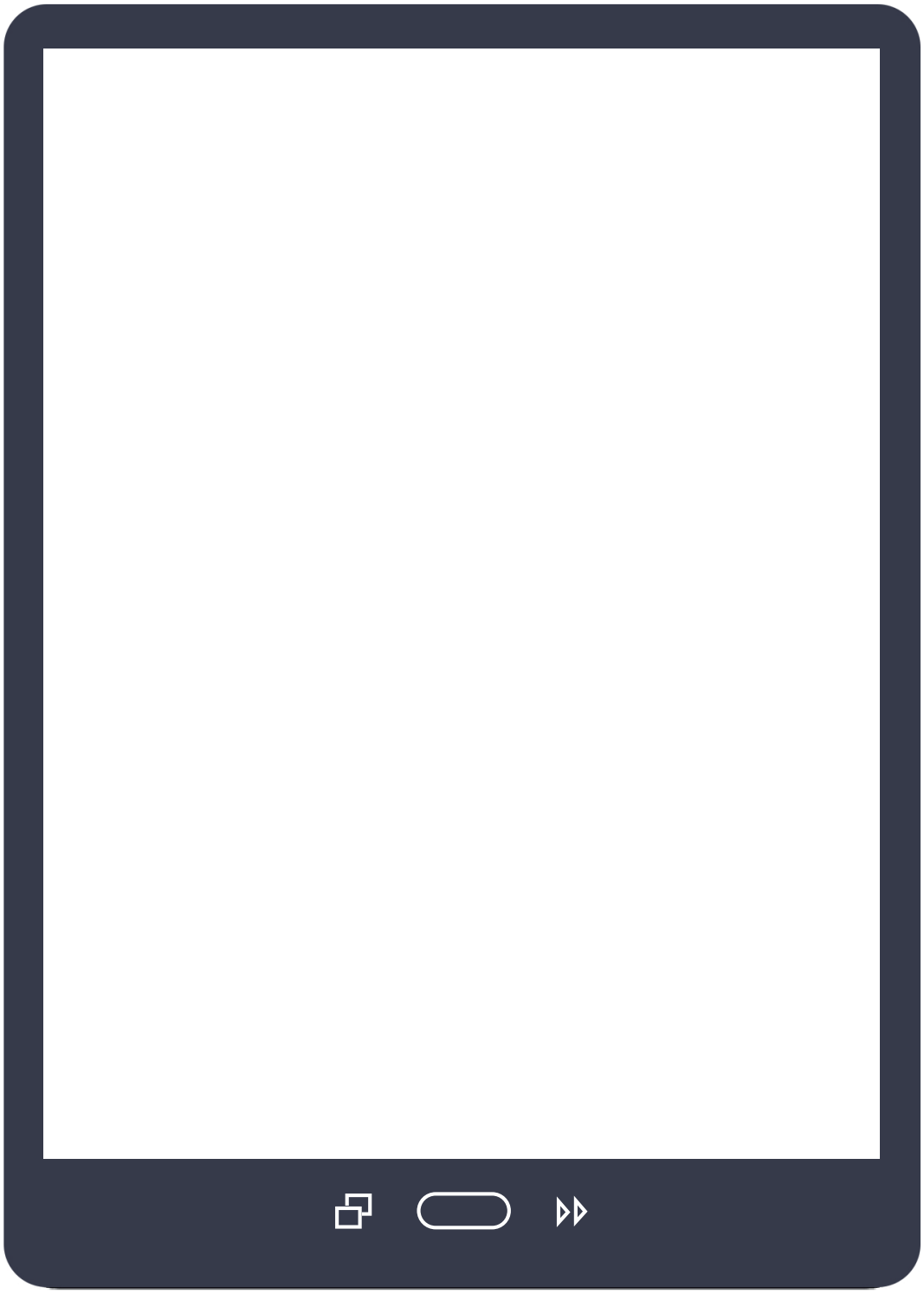
6.1. Otázky pro shrnutí

Uzavřete hodinu následujícími otázkami. Můžete je dětem postupně pokládat, nebo napsat či promítnout na tabuli. Starší děti si odpovědi mohou psát.

OTÁZKY	ODPOVĚDI
Co je to počítačový vir?	Program, který škodí počítačovým zařízením.
Jak se proti virům bránit?	Mít nainstalovaný antivir a aktualizovat programy (včetně antiviru).

OTÁZKY	ODPOVĚDI
Pro úroveň 2: Poskytne nám antivir stoprocentní ochranu proti virům?	Ne. Musíme se především zodpovědně chovat, například neklikat na podezřelé linky.
Může se počítačový vir dostat na smartphone?	Ano. *Pozn.: Dokonce na víceméně jakékoli počítačové zařízení, včetně skrytých počítačů nebo wifi.*
Co je to aktualizace? (v úrovni 1 lze vyměnit za: Je aktualizace pro antivir dobrá, nebo špatná?)	Stažení (z internetu) a nainstalování vylepšené verze programu. (Úroveň 1: Je dobrá; vylepšuje „bojové schopnosti“ antiviru.)
Napraví antivir škody, které vir napáchal.	Obvykle ne.

Příloha 1 – Aktivita „Odstraňování viru“



Doprovodné technické informace

Otázky, které se mohou objevit v souvislosti s výukou

Zasekává / zpomaluje se mi zařízení. Způsobil to vir?

Mohl to způsobit vir. Ale může to být třeba i tím, že má zařízení plný disk (paměťovou kartu) – je tam nainstalováno (postahováno) příliš mnoho programů nebo je tam příliš mnoho fotek, videí atp. Nebo je spuštěno příliš mnoho programů najednou. Nebo pokud se zařízení zasekává při spouštění konkrétního programu, může to být tím, že zařízení je pro tento program příliš pomalé.

Kdo vyrábí počítačové viry?

Lidé. Mohou je vyrábět pro zábavu, nebo záměrně: aby škodily uživatelům a přinášely zisk svým tvůrcům.

Mohu si nainstalovat jakýkoli antivir?

Pozor! Je dobré se poradit s někým, kdo tomu rozumí. Existuje mnoho antivirů, které jsou zadarmo, ale někdy se viry za antivir mohou maskovat! Existují také falešné antiviry: programy, které neškodí, ale zároveň ani neodstraňují viry (za takové falešné antiviry se často platí). Je třeba si dávat pozor, než si do zařízení něco nainstalujeme. Některé operační systémy mají zabudovaný vlastní antivir, ale je třeba si dát pozor na to, do jaké míry je kvalitní.

Kdo je to hacker?

Pozor, hacker (obvykle) není programátor počítačových virů. Hacker je obecně velmi dobrý programátor, který vytváří (obvykle ve svém volném čase) technologicky zajímavé a náročné „kousky", coby svého druhu umělec. „Kouskem" se dnes často rozumí proniknutí do cizího počítačového systému, ale může to znamenat i třeba tvorbu technologicky zajímavého zařízení. Hacker může mít dobré úmysly (snaží se proniknout do bankovního systému, aby zjistil jeho slabiny a nahlásil je), ale i špatné úmysly (snaží se proniknout do bankovního systému, aby ukradl peníze). Ano, hackeři mohou proniknout i do počítačových zařízení dětí. Většině takových průniků lze zabránit tím, že je zařízení adekvátně chráněno (aktualizovaný software, firewall, atd. – tato témata patří spíše na třetí stupeň).

Kdo mi může pomoci s mým zařízením (smartphonem, notebookem)?

Obvykle to bývá učitel informatiky, správce sítě nebo školní preventista, případně rodič či starší sourozenec. Bohužel v nemalém množství případů nikdo takový neexistuje.

Je počítačový vir jako nemoc a antivir jako lék?

Ano, i ne. Můžeme si to tak zjednodušeně představit (může to být přístupná metafora zejména pro mladší děti), ale je třeba vědět, že skutečné viry (bacily, nemoci apod.) nemohou nakazit počítač, a naopak počítačové viry jednak nejsou organismy a jednak nemohou nakazit člověka/zvíře. Počítač nakažený virem není nemocný, je spíš porouchaný. Podobně je to s paralelou mezi léky a antivirem. Pokud si navíc představíme antivir coby lék, je vhodné si ho představit zároveň jako preventivní lék, abychom se nenakazili, a zároveň i lék, který léčí, když pacient nemoc dostane.

Mohu si nahrát vir z flashky?

Ano, z jakéhokoli přenosného média. Pokud máme zavirovaný například notebook a připojíme k němu flashku, některé viry se na flashku umí nahrát a pak se z flashky přehrát na jiný počítač. Je to další způsob, jakým se viry mohou šířit.

Rozšiřující otázky

Co „těží" těžební viry?

Využívají (těží) kapacitu počítače: například na rozesílání spamů nebo těžení bitcoinů (a jiné elektronické měny).

Jaké další typy virů existují?

Například **Trojské koně**. Jedná se o viry, které byly záměrně vpraveny do programů, které se tváří (a často i fungují) úplně normálně. Mohou například pustit na počítač další viry nebo škodit velmi specifickým způsobem: třeba schválně kazit matematické výpočty, díky kterým se potom pokazí výroba nějakého zařízení. Existují i viry, které dokážou **poškodit hardware**, například tak, že rychle vypínají a zapínají harddisk. Některé viry také dělají z počítačů tzv. **„zombies"**: takové počítače fungují jako normálně, ale hacker nad nimi může kdykoli převzít kontrolu a provést z nich kybernetický útok (například na banku – podezření potom padne nikoli na hackera, ale na majitele zombie počítače).

Obecně existují i další typy škodlivých programů mimo viry. Někdy se pro tyto programy používá pojem **malware** („malicious software") – toto téma je nad rámec této lekce.
Další informace například (dostupnost zdrojů ověřena 28. 4. 2020):

- knihy.nic.cz/files/edice/bud_panem_sveho_prostoru.pdf
- o2chytraskola.cz/video/25
- internetembezpecne.cz/internetem-bezpecne/malware/
- avg.com/en/signal/what-is-a-computer-virus

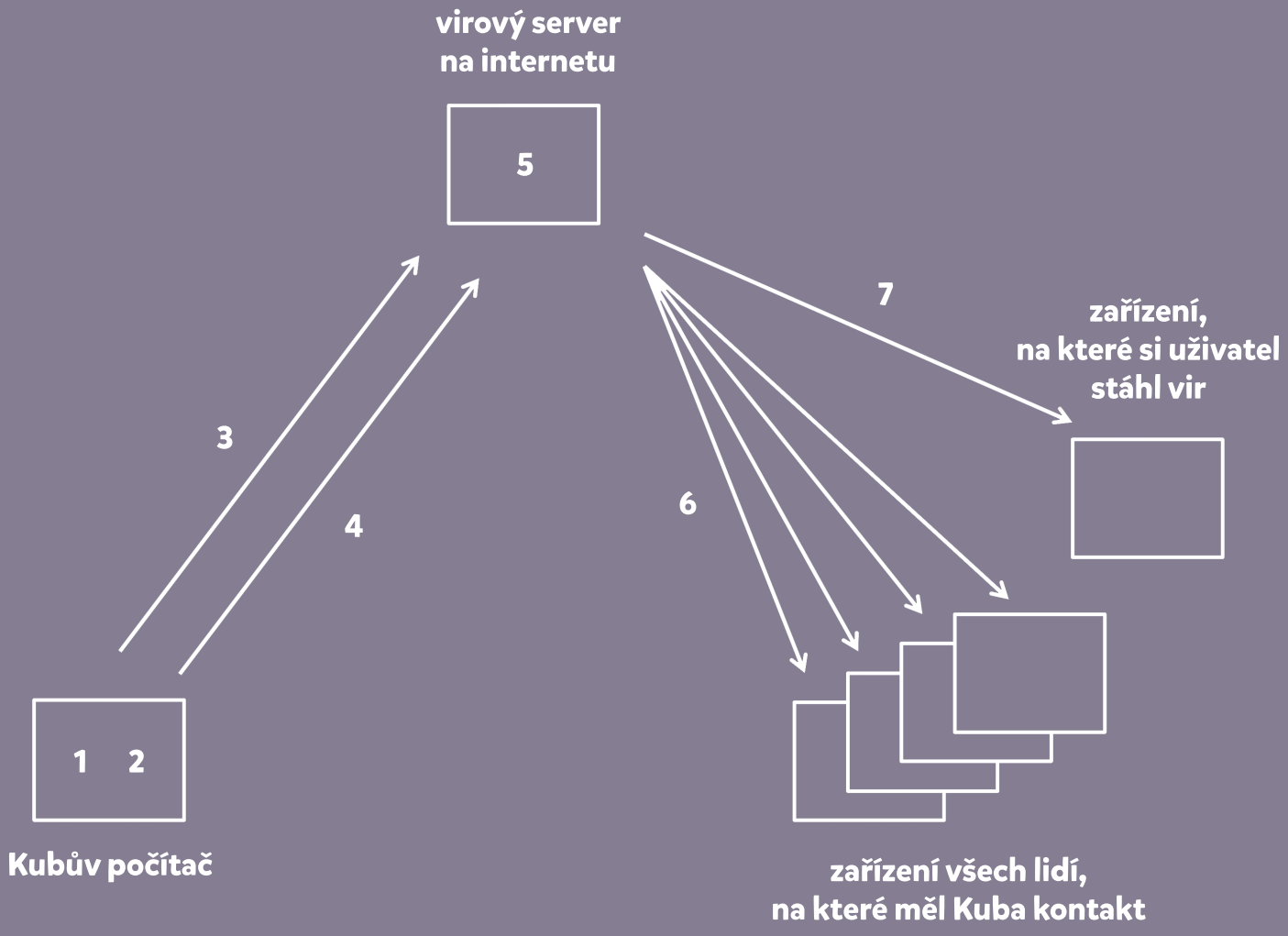
Jak přesně funguje „návnada" (talkshow: 3:26)?

V našem seriálu postupoval špehovací vir tímto způsobem (viz schéma):

1. Zapnul webkameru a začal nahrávat.
2. Zjistil kontakty na Kubovy kamarády.
3. Odeslal nahraná videa na virový server.
4. Odeslal kontakty na virový server.
5. Na virovém serveru bylo vytvořeno vtipné video (tzn. kousek z toho, co bylo přes webkameru nahráno) a návnada (fotka). V tomto případě vtipné video a návnadu vytvořil člověk, ale v některých případech by oboje mohlo být vyrobeno i automaticky.
6. Návnada byla odeslána Kubovým kamarádům (jejichž kontakty má virový server z kroku 2 a 4).
7. Pokud se někdo nechal zlákat návnadou, stáhnul si vir.

Kuba si ovšem původně nahrál do počítače vir společně se „Superhrou" – návnadou tedy v jeho případě byla „Superhra".

Postup špehovacího viru:



Co dělat, když mám zavirovaný počítač?
Antivir může umět vir odstranit, ale častěji bývá vhodnější zachránit data (texty, fotografie atd.) a počítač celý přeinstalovat.

Co by třeba mohly dělat viry v blízké budoucnosti?

Například: Dnes již existují programy, které mohou například vytvořit video s člověkem, jenž říká věci, které nikdy neřekl. Pro tvorbu takového videa potřebujeme mít s tímto člověkem nahraná jiná videa. Náš špehovací vir by taková videa například mohl nahrát – a na virovém serveru by bylo automaticky vytvořeno video, jak Kuba říká něco, co nikdy neřekl.

Hlavní funkce antiviru

- Umí rozpoznat viry. Lze si to představit tak, že psi ze seriálu mají „brýle poznání", pomocí kterých viry odhalí. Jednou z funkcí aktualizací je i přinášet neustále vylepšené „brýle poznání", kterými rozpozná antivir nové viry.
- Umí odstranit (izolovat, zablokovat) vir, jakmile ho pozná.
- Antivir neumí odstranit škody, které vir napáchal (až na výjimky). Například pokud vir pouze zpomaluje počítač, odstraněním viru je odstraněn i problém: zpomalování. Ale pokud vir něco způsobí (rozešle video, zašifruje soubory, zjistí heslo), antivir škodu neodstraní. Antivir funguje jako prevence a lék na základní příčinu (vir), ale nikoli lék na následky „nemoci".

Co antivir v zařízení dělá – podrobněji

Správně nainstalovaný antivir zejména:
- Má seznam podezřelých webových stránek (IP adres); varuje, pokud je chceme navštívit. Seznam si aktualizuje díky aktualizacím. Podezřelá stránka je například ta, kterou málo lidí navštěvuje (pozor: ne vždy musí stránka, před kterou antivir varuje, skutečně obsahovat viry).
    - Podezřelé stránky mohou například provádět „phishing" – jde o stránky, které vypadají jako známé stránky, ale ve skutečnosti například lákají z uživatele hesla.
- Zná vzorce chování známých virů; varuje, pokud takové chování u určitého programu rozpozná. Seznam vzorců chování si aktualizuje díky aktualizacím.
- Umí podle obecných znaků chování virů (např. program se připojuje na internet, aniž by to byl prohlížeč nebo hra) označit jako vir i program, se kterým se nikdy předtím nesetkal. Může se ale splést a označit nezávadný program.
- Podle vzorců chování nebo obecných znaků hledá viry:
    - na disku/paměťové kartě, ale jenom na vyžádání, nebo když mu řekneme, aby jednou za čas disk/paměťovou kartu prohledal.
    - v datech, která vstupují do počítače: typicky coby přílohy zpráv, po stažení z internetu nebo třeba z flashky; musíme ho ale správně nastavit (například „propojit" s emailovým klientem).
- Programy, které podezírá z toho, že jsou viry, umí zavřít do „virového trezoru" a poté odeslat na server výrobce antiviru k podrobné analýze. Výrobce antiviru poté může připravit novou aktualizaci, do které vloží „signaturu" (tzn. poznávací znaky) nově objeveného viru.
- Může odhalený vir i odstranit z počítače.

Tipy pro dospělé

1) Jmenujte rodinného/školního „správce počítačové bezpečnosti".

Rodina: Může to být někdo z rodiny nebo i mimo. Jakmile ale kdokoli z vaší rodiny používá zařízení typu tablet, smartphone, PC, notebook, hračky připojující se k internetu nebo k jinému počítači … jakmile máte wifi, měli byste se zajímat o to, zda všechna zařízení ve vaší rodině jsou řádně zabezpečena. To zahrnuje i adekvátní antivir (pozor na to, že byste měli stahovat jen antivir od společnosti, které důvěřujete: většina „antivirů", které jsou ke stažení na internetu, jsou ve skutečnosti různé škodlivé programy nebo rovnou viry).
Škola: Určete někoho, za kým mohou zajít děti, když mají bezpečnostní problém se svým počítačovým zařízením. Nezřídka nemá z rodiny dětem kdo poradit.

2) Buďte dětem vzorem.

Mějte svá zařízení zabezpečena a dejte to dětem na vědomí. To zahrnuje i instalaci antiviru na smartphony.

3) Zkuste se sami o virech a antivirech naučit více.

Můžete k tomu použít například materiály od CZ.NIC (viz výše, otázka „Jaké máme další typy virů?") nebo z webu Internetem bezpečně (https://www.internetembezpecne.cz/ke-stazeni/, kniha „Internetem Bezpečně: web offline").

Technický popis 7. dílu „Viry útočí“

Mimo díl se stalo toto: Kubovi se při každém (nebo téměř každém – řekněme jednou denně) spuštění počítače začal aktualizovat antivir. Aktualizace chvíli trvá – například proto, že se obvykle musí z internetu stáhnout pro aktualizaci data. Kubovi čekání vadilo, a tak celý antivir vypnul (2:41). Kdyby vypnul jen aktualizace antiviru, antivir by zůstal spuštěný, pouze by přestal „vylepšovat své bojové schopnosti“. Ale Kuba vypnul antivir úplně. (V seriálu operační systém Kubu upozorňuje, že je antivir vypnutý, na 1:00.)

Následně si Kuba stáhl novou Superhru. Odkaz na ni mu přišel ve zprávě od kamarádů (3:50). Superhra je opravdu zábavná hra, jenže její součástí je i špionážní vir („spyware“). Kdyby měl Kuba aktualizovaný antivir, tento by ho pravděpodobně v okamžiku, kdy by Kuba kliknul na tlačítko „Zahájit stahování“ (šipka v okně na 3:51), upozornil, že za odkazem na Superhru se skrývá vir.
Z dílu nevíme, co všechno vir u Kuby na počítači napáchal, ale dvě věci víme jistě: a) zkopíroval si kontakty na jeho kamarády z nějaké aplikace na posílání zpráv, b) zapínal Kubovi webkameru, nahrával ho a jeho nahrávky rozesílal kamarádům (jak to přesně udělal – viz „Jak přesně funguje návnada“). Tímto způsobem se děti ve škole dozvěděly, že si Kuba oblíbil plyšovou okurku, kterou vyhrál v soutěži v 5. díle.

Marwinovi se v Datové Lhotě podařilo spustit antivir (2:55) a s jeho pomocí odhalit vir v Superhře (3:40). Podařilo se zabránit, aby vir odeslal **nové** video (tzn. video, které se v tomto díle nahrávalo zhruba od 1:06) a vir z Kubova počítače smazat. Staré video s okurkou, kterým díl začíná, ale zůstalo rozesláno – antivir nemá žádnou moc ho z internetu a ze zařízení Kubových spolužáků smazat. Stejně tak nebyl zničen server viru (viz otázka „Jak přesně funguje návnada“ výše) – vir pokračuje ve své škodlivé činnosti: na serveru zůstává původní Kubovo video a kontakty na jeho kamarády… a zřejmě i stovky dalších podobných videí dětí či dospělých. Přitom pokud někdo z Kubových spolužáků Kubovo původní video s okurkou stáhnul a sám neměl zapnutý a aktualizovaný antivir, náš vir se dostal na zařízení tohoto spolužáka. Pokud tento spolužák nemá zalepenou kameru, brzy bude následovat Kubův osud…

Technická poznámka:
Vir coby počítačový program má Kuba v notebooku jen jeden. V seriálu vidíme více „postaviček virů“ – to jsou jednotlivá vlákna téhož programu (téhož viru).

Modelové lekce připravili a na školách vyzkoušeli: Cyril Brom, Anna Drobná, Tereza Hannemann, Pavel Ježek.
Modelové lekce recenzovali: Daniela Benešová, Miroslava Černochová, Michala Radotínská, Petra Sobková, Jan Vais, Tomáš Zahoř [15. 5. 2020]
Děkujeme paní Jitce Šídové ze ZŠ Veronského náměstí v Praze a paní Heleně Lazarové ze ZŠ Hrabina v Českém Těšíně, které nám pomohly s rozsáhlým testováním a jejichž cenné rady jsme do modelových hodin zapracovali.