JAK CHRÁNIT SVÁ DATA

Metodický rádce pro učitele

1. Východiska

K základům počítačové bezpečnosti patří samozřejmě ochrana dat a informací – ať už jde o osobní údaje, citlivé i běžné informace, firemní know-how, obchodní tajemství nebo třeba utajované materiály. Základy zabezpečení počítače a dalších zařízení (mobil, tablet atd.) by měly být nedílnou součástí informační gramotnosti vyučované na základní škole.

V prostředí školy učíme žáky především:

- zásady technického zabezpečení počítače a mobilu
- zásady ochrany osobních dat v online prostředí (hlavně na sociálních sítí)

2. Cíle výukových aktivit

Dlouhodobým cílem vzdělávání v této oblasti na úrovni ZŠ je naučit žáky základní bezpečnostní návyky tak, aby je dělali automaticky. Například aby při nastavování nového počítače nainstalovali antivir, automaticky se odhlásili z účtu, když ho přestanou používat, a podobně.

Kromě samotného zabezpečení dat je důležitá také práce s nimi v online prostředí – především na sociálních sítích. Žáci by měli umět svůj účet správně nastavit (veřejná, soukromá část).

3. Zásady ochrany dat

1. Používejte legální software. Nelegální (pirátský) software může obsahovat viry.
2. Pravidelně aktualizujte operační systém.
3. Pravidelně aktualizujte programy, hlavně ty, které používáte k přístupu na internet.
4. Používejte a pravidelně aktualizujte antivirové programy.
5. Používejte firewall (v operačním systému, v routeru).
6. Používejte bezpečná hesla, bezpečné kontrolní otázky, případně dvoufázové ověřování.
7. Pro přenos dat nepoužívejte neznámé a neprověřené flash disky.
8. Osobní a citlivé údaje nenahrávejte na cloud.
9. Nejdůležitější data chraňte heslem (šifrovaný soubor).

Materiál vznikl ve spolupráci s projektem E-Bezpečí, Univerzita Palackého Olomouc

Diskuze k pravidlům

Žáci rádi používají nelegální software, případně legální software upravený pomocí různých druhů pirátských programů – utilit (tzv. cracky). V téhle části musíme žákům vysvětlit, že viry se často skrývají v pirátských programech, které odstraňují původní zabezpečení hry nebo jiného programu.

Otázky k diskuzi – stahování programů

1. **Stahujete hry?**
2. **A stahujete hry i nelegálně – např. z různých webových úložišť? A znáte názvy některých z nich?** *(Nejznámější je Datoid, WebShare.)*
3. **Má to nějaká rizika? Jaká?**

Placené hry a další počítačové programy si nemůžete stáhnout zadarmo mimo oficiální stránky prodejce. To je protizákonné. Spousta kopií her nebo cracků vám navíc může zavirovat počítač.

Protože se viry pořád mění a vyvíjí, měli bychom pravidelně aktualizovat operační systém, aby dokázal lépe vzdorovat kybernetickým hrozbám. Stejně tak je důležité aktualizovat i internetové prohlížeče a další služby, kterými vstupujeme do světa internetu.

Otázky k diskuzi – antiviry

1. **Znáte nějaký antivirový program, který je zdarma?**
   (Třeba Avast nebo Microsoft Security Essential.)
2. **Znáte názvy firem, od kterých byste si mohli antivirový program koupit?**
   (Avast, Eset, Avg, – součást Avastu, Kasperski, Norton…)

V dnešní době se pro uchovávání dat často používají tzv. cloudové služby – vzdálená úložiště dat, ke kterým můžeme přistupovat odkudkoli. Ta mají spoustu výhod, ale zároveň s sebou nesou i bezpečnostní rizika.

Proto bychom neměli sdílet na cloud externích společností data, která jsou citlivá a dají se zneužít (např. intimní fotografie, údaje o zdravotním stavu – dokumentaci apod.).

Otázky k diskuzi – cloud

1. **Slyšeli jste někdy o Dropbox, Google Drive, iCloud nebo OneDrive? K čemu se používají?**
   Jde o cloudová úložiště dat, jsou uložená na vzdálených serverech na internetu a spravuje je konkrétní firma – třeba Google, Microsoft nebo Apple.

2. **Jaké mají cloudová úložiště výhody?**
   Ke svým dokumentům, fotkám a jiným souborům se dostaneme kdykoli a odkudkoli – z počítače, tabletu i mobilu. Navíc nemusíme mít strach, že o data přijdeme, když ztratíme flashku nebo přestane fungovat náš pevný disk.

3. **Mají i nějaké nevýhody?**
   Bez připojení k internetu se ke svým datům nedostaneme. Druhou, možná ještě větší nevýhodou, je riziko úniku našich dat. Ať už přihlašovacích údajů nebo samotných souborů uložených na cloudu. V roce 2014 například Dropboxu uniklo víc než 68 milionů přihlašovacích údajů – včetně hesel: Hackeři ukradli 68 milionů hesel uživatelů Dropboxu. Mají i to vaše? - iDNES.cz.
   Někdy je proto lepší použít starý dobrý flashdisk. Ty mají dneska už dostačující kapacitu, můžeme si vybrat z nepřeberného množství designů a k tomu jsou poměrně levné. Bohužel si ale pořád musíme dávat pozor, abychom si do počítače nezanesli vir.

Na co si teda dál dávat pozor?

1. Neotvírejte přílohy e-mailů od neznámých odesílatelů. A pokud je opravdu potřebujete otevřít, zkontrolujte je nejdřív antivirovým programem.

2. Dávejte si pozor na e-maily, které vypadají, že jsou od vaší banky a chtějí, abyste se přihlásili do svého internetového bankovnictví. Často jde o podvod (phishing), kdy vás odkaz z e-mailu přesměruje na falešnou stránku, která vypadá jako pravá. Než někam zadáte přihlašovací údaje, ověřte si adresu webu.

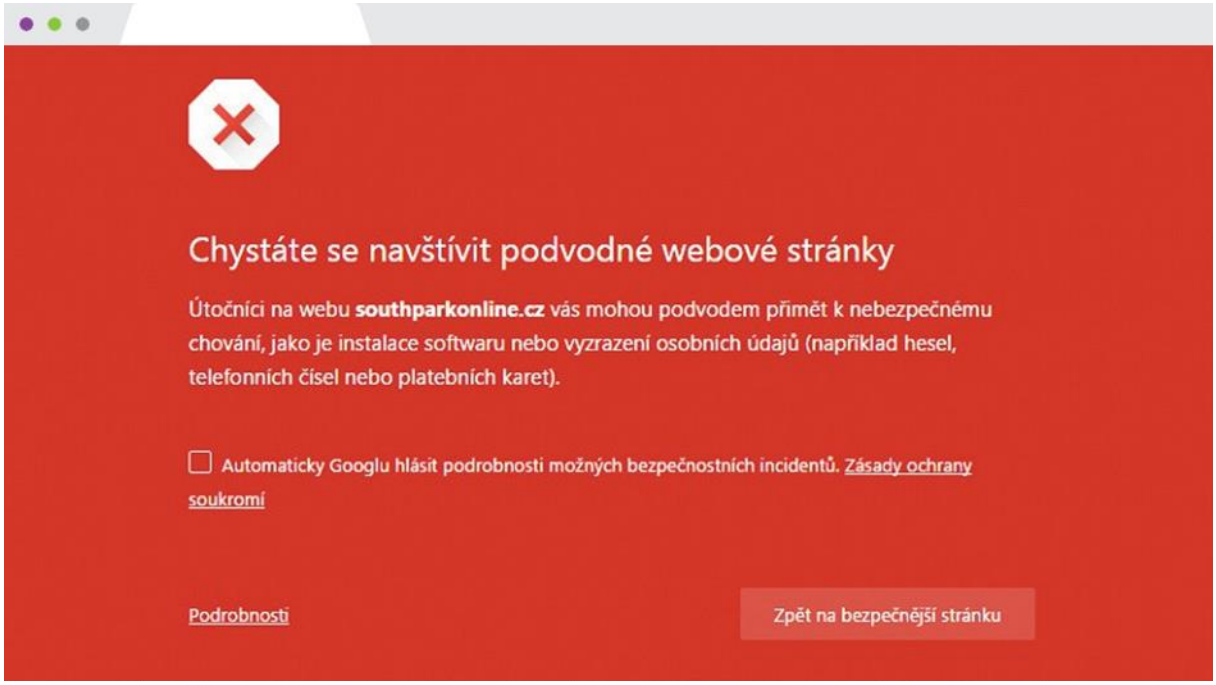
3. Neotevírejte stránky, které jsou označené jako podezřelé nebo nebezpečné. Mohly by obsahovat viry nebo jiný škodlivý software, který by mohl napadnout váš počítač.

4. Když už chcete z internetu odejít, nezapomeňte se ze všech účtů odhlásit. Zavření okna prohlížeče nestačí.

Svoje hesla ani PINy nikomu neprozrazujte a nikam si je nezapisujte. Případně k tomu použijte bezpečného správce hesel (např. LastPass). Volte zapamatovatelná, ale zároveň dostatečně bezpečná hesla. Zároveň nepoužívejte jedno univerzální heslo ke všem účtům.

Zavirovaný web

Prohlédněte si pozorně následující snímek obrazovky.
Jak byste se zachovali, kdyby se vám při otevírání stránky objevilo takové upozornění?



Ochrana osobních dat na sociálních sítích

Zásady ochrany osobních dat v prostředí sociálních sítí vychází z pravidel, která jsou definovaná v předchozí části textu.

1. Než začnete používat sociální síť, přečtěte si aspoň základní podmínky. Dozvíte se tam třeba, od kolika let je síť určená, co se děje s daty, která sdílíte, kdo za co zodpovídá, co se stane s vašimi daty po smazání účtu nebo co je na síti povolené a co ne.

2. Pro přihlášení si nastavte bezpečné heslo, které nepoužíváte nikde jinde (třeba na e-mailu). Pokud to jde, zapněte si dvoufázové ověření, například heslo a ověření přes mobil.

3. I když sociální sítě požadují, aby si uživatelé nahráli reálnou fotografii obličeje, z důvodu ochrany soukromí doporučujeme, aby děti použily jiný typ fotky. Třeba abstraktní obrázek nebo fotku oblíbeného zvířete.

Materiál vznikl ve spolupráci s projektem E-Bezpečí, Univerzita Palackého Olomouc

4. Na sociální sítě nepatří žádné fotky ani videa sexuálního charakteru (materiály, na kterých je dítě částečně, nebo dokonce úplně obnaženo). Takový obsah jde snadno zneužít.

5. Nikdy se neobnažujte před webkamerou! Můžete se stát terčem kybernetického útoku známého jako webcam trolling.

6. Chraňte své soukromí a oddělte soukromé informace (vidíte je jenom vy a vaši „přátelé“) od těch veřejných.

7. Pečlivě zvažujte, koho si přidáváte do přátel a komu zpřístupňujete svůj profil. Přidávejte si opravdu jen ty lidi, které opravdu znáte. Zároveň si dávejte pozor na falešné profily.

8. Dávejte si pozor na podvodníky. Neodesílejte žádné SMS ani nikomu neposkytujte údaje o svém bankovním účtu. Ani pokud vás o to prosí kamarád nebo kamarádka. Jejich účet mohl být napadený.

9. Nesdílejte nepravdivé informace – vždy si je nejdřív ověřte. Pokud chcete sdílet hoax, označte ho tak, aby ostatní věděli, že se nejedná o fakta.

10. Na sociálních sítích se chovejte podle pravidel netikety a vyhněte se agresivním projevům.

Otázky k diskuzi – sociální sítě

1. **Od kolika let si můžeš založit účet na Facebooku nebo Instagramu? Splňuješ tuhle podmínku?**
   Řešení: Správná odpověď je 13 let, ale v České republice je to 15 let (kvůli nařízení Evropské unie: GDPR). Diskuze může být zaměřena např. na to, že uživatelé můžou lhát o svém věku – pokud dítě lže o svém věku a vydává se za starší, i dospělý může lhát a vydávat se za dítě. Musíme si proto prověřit, s kým komunikujeme.

2. **Ze kterého zařízení se na sociální síť připojuješ? Počítač, notebook, tablet, mobil?**
   Řešení: V posledních letech pořád víc lidí používá k procházení sociálních sítí mobil. Ten ale často není vůbec zabezpečený (třeba antivirem). Navíc je snáz zjistitelná tvoje poloha. V tom lepším případě ti bude síť jenom nabízet líp cílenou reklamu. V horším případě může tvoje poloha skončit v rukou lidí, kteří ji můžou zneužít třeba k vyhledání tvých osobních informací nebo k různým formám sledování.

3. **Máš nějaké účty na sociálních sítích? Kolik jich je a máš i nějaký falešný profil?**
   Řešení: Žáci by měli pochopit, že stejně jako mají falešné účty někteří z nich, můžou mít takové účty i ostatní. Mělo by to vést k větší opatrnosti při přijímání přátelských žádostí a komunikaci online, protože je důležité si ověřovat, kdo je na druhé straně.

Materiál vznikl ve spolupráci
s projektem E-Bezpečí,
Univerzita Palackého Olomouc

4. **Kolik máš na Facebooku přátel a sledujících na Instagramu? Znáš každého z nich osobně? Jak zjistíš, že jsou opravdu tím, za koho se vydávají?**
   Řešení: Diskutujte s žáky, jestli a jaký vnímají rozdíl mezi skutečnými a online přáteli.

5. **Kolik máš hesel? Používáš jedno na všechno, nebo máš pro každou službu jiné?**
   Řešení: Žáci by měli pochopit, že pokud unikne heslo z jednoho zdroje – v případě univerzálního hesla získá útočník přístup i k ostatním účtům. Pro sociální sítě by tedy měli používat jiné heslo než např. do e-mailu. Můžete je seznámit s pravidly pro tvorbu hesla, správcem hesel, uvést příklady slabých a silných hesel atd.

6. **Jaké osobní údaje o tobě prozradí tvoje působení na internetu? Můžou se ostatní dozvědět něco i o tvé rodině, domácím mazlíčkovi nebo třeba o tom, jakou techniku máš doma? Jdou takové informace nějak zneužít?**
   Řešení: Otázka cílí na hodnotu informací. Děti sdílejí různé údaje – jméno, adresu, věk, fotografie, ale třeba i citlivé informace o tom, kdy jedou na dovolenou (a byt je tím pádem prázdný), jaké mají doma technické vybavení (lákadlo pro zloděje), jestli mají domácího mazlíčka apod.

Aktualizace 31. ledna 2025.