O2 | Chytrá škola

# Jak chránit svá data

## Metodický rádce pro učitele

### 1. Východiska

K základům počítačové bezpečnosti patří zcela samozřejmě ochrana dat a informací nejrůznějšího typu a charakteru (osobní údaje, citlivé údaje, běžné informace, know how, obchodní tajemství, data podléhající utajení apod.). Základy zabezpečení počítače a mobilních dotekových zařízení (především smartphonů) by mělo být jedním z pilířů informační gramotnosti rozvíjené prostřednictvím základní školy.

V prostředí školy učíme žáky především:

1. Zásady technického zabezpečení počítače či mobilu
2. Zásady ochrany osobních dat v online prostředí (především v prostředí sociálních sítí)

### 2. Cíle výukových aktivit

Dlouhodobým cílem vzdělávání v této oblasti na úrovni ZŠ je vypěstovat u žáků základní bezpečnostní návyky a zautomatizovat je. Některé činnosti pak budou žáci vykonávat automaticky – například u nového počítače nainstalují antivir, automaticky se odhlásí z účtu, jakmile jej přestanou využívat atd.

Kromě samotného technického zajištění dat je velmi důležitá také **práce s daty v online prostředí** – především v prostředí sociálních sítí. Zde je důležité umět účet na sociální síti správně nastavit (veřejná, soukromá část).

# 3. Zásady ochrany dat

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

# Diskuze k pravidlům

Žáci rádi využívají nelegální software, případně legální software upravený pomocí různých druhů pirátských programů – utilit (tzv. cracky). Zde je nutné žákům vysvětlit, že virová hrozba může být ukryta právě v pirátských utilitách, které odstraňují původní zabezpečení hry či jiného programu.

# Otázky k diskuzi – stahování programů

1. **Stahujete v online prostředí hry?**
2. **A stahujete hry také nelegálně – např. z různých webových úložišť? A znáte názvy některých z nich?**
   *(Nejznámější je Uložto, Datoid, WebShare, HellSpy, RapidShare nebo třeba eSoubory.)*
3. **Má toto stahování nějaká rizika? Jaká?**

U her a dalších druhů počítačových programů, které jsou v prodeji, neplatí možnost stáhnout si toto dílo pro vlastní potřebu. Tedy stažení a využívání hry je nelegální. Velké množství kopií her či cracků také obsahuje různé druhy virů (na ně se zaměřujeme v jiném materiálu).

Protože se virové hrozby neustále mění, je nutné pružně reagovat a pravidelně aktualizovat operační systém pomocí různých druhů upgradů a „záplat“. Aktualizovaný systém logicky lépe vzdoruje kybernetickým hrozbám. Ze stejných důvodů je důležité aktualizovat i internetové prohlížeče a další služby, pomocí kterých vstupujeme do světa internetu.

# Otázky k diskuzi – antiviry

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

V posledních letech se stále častěji pro uchovávání dat využívají tzv. cloudové služby – vzdálená úložiště dat, ke kterým můžeme přistupovat odkudkoli. Ta mají velké množství výhod, ale současně mohou být bezpečnostními riziky.
Proto je důležité nesdílet pomocí cloudu externích společností data, která jsou citlivá a lze je zneužít (např. intimní fotografie, údaje o zdravotním stavu – dokumentaci apod.).

# Otázky k diskuzi – cloud

1. **Slyšeli jste někdy tyto názvy služeb: Dropbox, Google Drive, iCloud, OneDrive? K čemu se tyto služby používají?**
   *Jde o cloudové služby – úložiště dat, která jsou fyzicky umístěna v prostředí internetu a spravuje je konkrétní firma, třeba Google, Microsoft nebo Apple.*


2. **Jaké mají tyto služby výhody?**
   *K datům se dostaneme kdykoli, odkudkoli – třeba z tabletu či mobilu, nejsme závislí na funkčnosti našeho vlastního počítače. Při ztrátě dat (např. poškození našeho vlastního disku s daty) o data v cloudu nepřicházíme, máme je k dispozici.*

3. **Mají tyto služby i nějaké nevýhody?**
   *Všechny tyto služby jsou závislé na internetovém připojení – bez něj nedochází k synchronizování a aktualizování dat. Stejně tak data mohou uniknout do online světa – ať už tak, že uniknou přihlašovací údaje k účtům v dané službě, nebo dojde ke zkopírování samotných dat. V roce 2014 například Dropboxu uniklo více než 68 milionů přihlašovacích údajů – včetně hesel:*
   *https://computerworld.cz/securityworld/dropboxu-unikly-hesla-musite-je-zmenit-53268.*
   *Přestože je cloudový přenos dat stále více populární, k přenosu dat se dosud používají také USB flash disky. Jejich cena stále klesá a jsou tedy cenově dostupné, jejich kapacita je dostatečná, snadno se přenášejí a mají stylový design. Nicméně i flash disk může skrývat virovou hrozbu. Proto dodržujme zásadu, že do počítače neprověřené flash disky neznámého původu jednoduše nepatří – a pokud je chceme přesto použít, musíme mít vždy aktivní antivirovou kontrolu.*

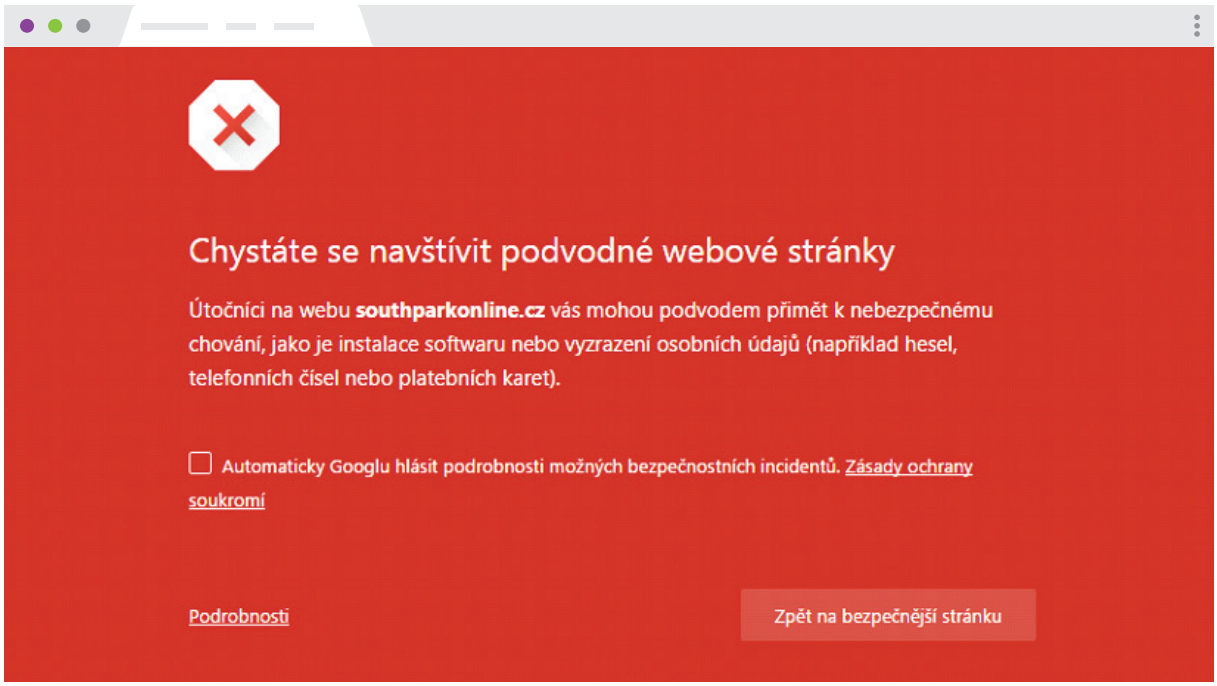
## Na co si tedy dále dávat pozor?

1. Neotvírejte přílohy e-mailů, které k vám dorazily od neznámých osob. Pokud je nutně potřebujete otevřít, zkontrolujte před otevřením soubory antivirovým programem. Dávejte si pozor na e-maily, které přicházejí z vaší banky a které vás informují o tom, že je třeba se přihlásit do vašeho internetového bankovnictví. V řadě případů může jít o podvod
(tzv. phishing), v rámci kterého vás odkaz v e-mailu přesměruje na podvrženou stránku – kopii vašeho bankovnictví. Ověřujte si pečlivě adresu v příkazovém řádku internetového prohlížeče.
2. Na internetu neotevírejte stránky, které jsou označeny jako podezřelé (či obsahující nebezpečný obsah). Jejich prostřednictvím může být váš počítač infikován.
3. Po ukončení práce na internetu se odhlaste – pouhé zavření internetového prohlížeče nestačí.
4. Svá osobní hesla a PINy nikomu neprozrazujte a nikam je nezapisujte, volte takové heslo, které je bezpečné a zároveň si jej dokážete zapamatovat nebo je dokážete dohledat ve „správci hesel". Ke klíčovým službám jako e-mail nebo sociální sítě využívejte různá hesla, nepoužívejte jedno univerzální heslo.

**Navazující aktivita**

## Zavirovaný web

Prohlédněte si pozorně následující screen obrazovky.
Jak byste se zachovali, kdyby se vám při otevírání stránky objevila následující obrazovka?



# Ochrana osobních dat na sociálních sítích

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

1. **Před vstupem do prostředí sociální sítě bychom měli znát alespoň obecné podmínky užívání dané služby, ve kterých je stanoven např. věkový limit pro užívání služby, pravidla definující, co se stane s daty v případě jejich sdílení, jaké je rozdělení odpovědnosti, co se stane s daty po smazání účtu, jaké aktivity v prostředí sítě můžeme a nesmíme dělat apod.**
2. **Pro vstup do sociální sítě je třeba zvolit bezpečné heslo, které bychom neměli používat pro vstup do jiných služeb, třeba e-mailu. Univerzální hesla používá přibližně polovina uživatelů sociálních sítí. Pokud to sociální síť umožňuje, volíme vícefázové ověřování (např. současně heslo a ověření pomocí mobilního telefonu).**
3. **Ačkoli sociální sítě vyžadují, aby si uživatelé nahráli jako profilové foto skutečně reálnou fotografii vlastního obličeje focenou zepředu, z důvodu ochrany osobních údajů však doporučujeme, aby dítě volilo fotografii jinou – klidně abstraktní, zvířecí aj.**
4. **Do prostředí sociálních sítí nepatří fotografie či videa sexuálního charakteru (materiály, na kterých je dítě částečně či zcela obnaženo). Tyto materiály jde snadno zneužít k útoku na dítě i dospělého.**
5. **Nikdy se v online prostředí neobnažujte před webkamerou! Můžete se stát terčem kybernetického útoku s využitím tzv. webcam trollingu (podrobněji v jiných materiálech).**
6. **Chraňte si soukromí a oddělte informace, které budou veřejné (viditelné všem), od informací, které budou soukromé (uvidíte je pouze vy a vaši „přátelé" – typické např. pro fotoalba).**
7. **Zvažte, koho si přidáváte mezi přátele. Uvědomte si, že v online prostředí existuje velké množství podvržených profilů (fake profily) a váš internetový kamarád nemusí být tím, za koho se vydává. Mezi přátele si přidávejte především ty, které znáte z reálného světa, případně ty, u kterých jste si prověřili identitu (viz materiál věnovaný seznamování v online prostředí).**
8. **Nereagujte na žádosti svých online přátel k odesílání různých druhů esemesek (často placené/předplacené služby), rovněž neposkytujte uživatelům sociální sítě údaje o svém bankovním účtu či kreditní kartě.**
9. **Nesdílejte informace, které jsou nepravdivé – vše si ověřujte. Pokud budete sdílet hoax, označte jej tak, ať je zřejmé, že jde o skutečně o hoax – třebas vtipný a zajímavý.**
10. **V prostředí sociální sítě se chovejte podle pravidel netikety. Omezte agresivní projevy.**

# Otázky k diskuzi – sociální sítě

1. **Od kolika let je povolen vstup do sociální sítě Facebook a Instagram? Splňuješ tento limit?**
   *Řešení: Odpověď je 13 let, ale podle nově zavedené legislativy vláda odhlasovala posun na 15 let věku – soulad s GDPR). Diskuze může být zaměřena např. na to, že uživatelé mohou lhát o svém věku – pokud dítě lže o svém věku a vydává se za starší, dospělý může lhát a vydávat se za dítě. Tedy je nutné prověřit si, s kým komunikujeme.*

2. **Ze kterého zařízení se na sociální síť připojuješ? Počítač, notebook, tablet, mobil?**
   *Řešení: V posledních letech rapidně roste počet uživatelů, kteří se díky datovým tarifům připojují k sociálním sítím z mobilních zařízení. Problém je, že mobilní zařízení často nejsou zabezpečená – třeba antivirem. Navíc při vstupu do sociální sítě o sobě dítě prozradí další osobní/citlivý údaj: svou polohu. Sociální síť zachytí, odkud se připojuje, a podle toho dítěti nabízí reklamu cílenou na daný region.*

3. **Pokud máš účet na sociálních sítích, kolik jich máš? Máš i nějaký falešný?**
   *Řešení: Otázka je cílená, aby dítě pochopilo, že stejně jako má falešné účty ono samo, mohou mít falešné účty i ostatní přátelé.*

4. **Kolik máš ve svém profilu přátel? Znáš každého z nich osobně? Jak si ověřuješ, že jsou skutečně těmi, za koho se vydávají?**
   *Řešení: Zde je dobré rozjet diskuzi na téma, jaký je rozdíl mezi online přáteli a skutečnými „reálnými" přáteli – zda žáci vnímají rozdíly.*

5. **Kolik máš hesel? Jedno univerzální, nebo více hesel, každé pro jinou službu?**
   *Řešení: Žáci musí pochopit, že pokud unikne heslo třeba jen z jednoho zdroje – v případě univerzálního hesla získá útočník přístup i k ostatním účtům žáka. Tj. pro sociální sítě volit heslo, které není využíváno např. pro vstup do e-mailu. Žáky lze seznámit samozřejmě s pravidly pro tvorbu hesla, uvést příklady typických „slabých" hesel, připomenout možnost využít program „správce hesel" (password manager) apod.*

6. **Které osobní údaje se o tobě uživatelé mohou dozvědět? A dozví se něco i o tvé rodině, domácím mazlíčkovi nebo třeba o tom, jakou techniku máš doma? Jde některý z nich zneužít?**
   *Řešení: Otázka cílí na hodnotu informací. Děti sdílejí různé údaje – jméno, adresu, věk, fotografie, ale třeba také citlivé informace o tom, kdy jedou na dovolenou (a byt je tím pádem prázdný), jaké mají technické vybavení (lákadlo pro zloděje), zda mají domácí zvíře apod.*