



Bezpečnost on-line – Bezpečnostní zásady

♥ = 1. třída; ♥ = 2. třída; ♥ = 3. třída; ♥ = 4. třída; ♥ = 5. třída

1. Zásada: Odhlašujeme se z účtu ♥♥♥♥♥

2. Zásada: Školní počítač není pro zábavu ♥♥♥♥♥

Situace: Marián se ve školní učebně přihlásil pomocí hesla do školního počítače. Surfoval na internetu, hrál počítačové hry, vypracovával úkoly do školy. Poté zavřel prohlížeč a ostatní programy a odešel do další učebny.

Vyhodnocení: Marián se neodhlásil ze svého školního účtu, pouze zavřel všechny programy a od počítače odešel. Kdokoli, kdo po něm přijde k počítači, bude mít přístup do jeho školního účtu. Marián se měl během školní výuky počítačů věnovat pouze úkolům od učitele, neměl hrát počítačové hry nebo surfovat na internetu.

3. Zásada: Heslo si nikam nepíšeme ♥♥♥♥♥

Situace: Lexa umí skvěle pracovat s počítačem, a proto si vytvořil složité heslo obsahující malá i velká písmena a číslice. Aby heslo nezapomněl, napsal si ho na papírek na zadní stranu svého notebooku.

Vyhodnocení: Heslo nepatří ani na zadní stranu notebooku, ani na spodní stranu klávesnice ani do deníčku. Heslo si buď pamatujeme, sdílíme ho s rodiči nebo si ho uložíme do zamknutého poznámkového bloku v telefonu.

4. Zásada: Sociální sítě můžeme mít od 13 let ♥♥

5. Zásada: Na internetu si nepíšeme s cizími lidmi ♥♥

Situace: Františka chodí do 3. třídy a založila si účet na Tik Toku. Začala ho velmi aktivně používat, neustále přidávala nové příspěvky a chatovala se svými kamarády i s cizími lidmi. Jednoho dne ji začal posílat neznámý člověk nenávistné zprávy a nadával ji do komentářů. Františka se z toho zhroutila.

Vyhodnocení: Františka si vůbec neměla zakládat účet na Tik Toku, protože věková hranice pro jeho používání je 13 let, ale jí je pouze 8 let. Nezkušenému uživateli hrozí na sociálních sítích spousta nebezpečí. Františka si také na internetu neměla psát s cizími lidmi, které osobně nezná.

6. Zásada: Sociální sítě můžeme mít od 13 let ♥♥♥

7. Zásada: Na internetu si nepíšeme s cizími lidmi ♥♥♥

Situace: Františka chodí do 5. třídy a založila si účet na Tik Toku. Začala ho velmi aktivně používat, neustále přidávala nové příspěvky a chatovala se svými kamarády i s cizími lidmi. Jednoho dne ji začal posílat neznámý člověk nenávistné zprávy a nadával ji do komentářů. Františka se z toho zhroutila.

Vyhodnocení: Františka si vůbec neměla zakládat účet na Tik Toku, protože věková hranice pro jeho používání je 13 let, ale jí je pouze 10 let. Nezkušenému uživateli hrozí na sociálních sítích spousta nebezpečí. Františka si také na internetu neměla psát s cizími lidmi, které osobně nezná.



8. Zásada: Hesla si necháváme pro sebe 💙💛💚💜💖

Situace: Anita a Petra byly nejlepší kamarádky, a proto si sdílely veškerá tajemství. Znaly dokonce i svá hesla do telefonů. Jednou se velmi pohádaly a Petra se rozhodla Anitě pomstít. Když Anita nedávala pozor, dostala se Petra do jejího telefonu a odeslala z něj SMS „Jsem úplně blbá, ale na tebe nemám!“ na všechna čísla v telefonu. Anitě pak přišla spousta nehezkých odpovědí a musela všem, včetně rodičů, vysvětlovat že SMS nepsala ona.

Vyhodnocení: Nikdy ani nejbližším lidem nesdělujte svá hesla. Nikdy nevíme, jakým způsobem může tuto informaci daný člověk použít. Výjimku jsou naši rodiče.

9. Zásada: Heslo neobsahuje osobní údaje 💙💛💚💜

Situace: Oto se na programu o bezpečnosti na internetu dozvěděl, že je důležité používat silná hesla. Proto si doma vymyslel několik hesel. Jedno heslo vytvořil z jeho jména a data narození, v dalším hesle použil jméno jeho oblíbené hudební skupiny, další hesla obsahovala jména jeho domácích mazlíčků apod. Hesla si nastavil na všechny své účty (mobil, počítač, e-mail, YouTube, hry).

Vyhodnocení: Používání silného hesla je správná volba, ale heslo nesmí obsahovat žádné osobní údaje, jako je jméno a datum narození člena rodiny, kamaráda, kamarádky nebo mazlíčka. Heslo by také nemělo obsahovat naše zájmy, jako je oblíbený film, seriál, zpěvák, zpěvačka, koníček apod. Takové heslo je totiž snadněji uhodnutelné pro kohokoliv, kdo vás jen trochu zná.

10. Zásada: Používáme různá hesla 💙💛💚💜

Situace: Luiza se na programu o bezpečnosti na internetu dozvěděla, že je důležité používat silná hesla. Proto si doma nastavila na všech svých účtech (mobil, počítač, e-mail, YouTube, hry) jedno silné heslo, které obsahovalo malá i velká písmena a číslice a zároveň neobsahovalo žádný osobní údaj.

Vyhodnocení: Používání silného hesla je správná volba, ale používání jednoho stejného hesla do všech účtů je velmi nebezpečné. V případě, že by někdo získal toto heslo, přihlásí se pod stejným heslem ke všem ostatním účtům. Proto je důležité používat silných hesel několik, alespoň trochu pozměněných.

11. Zásada: Používáme různá hesla 💖

Situace: Luiza se na programu o bezpečnosti na internetu dozvěděla, že je důležité používat dvoufázové ověření. Proto si doma nastavila na svůj Tik Tok profil ověření přes e-mail, do kterého se přihlašuje stejným heslem jako do Tik Tok profilu.

Vyhodnocení: Dvoufázové ověření pomocí e-mailu je správná volba pouze pokud nepoužíváme stejné heslo k profilu s dvoufázovým ověřením a k e-mailu, pomocí kterého ověřujeme. V případě, že by někdo získal heslo k profilu, pak se pod stejným heslem přihlásí na e-mail a získá kód dvoufázového ověření.

12. Zásada: Heslo používáme i na telefonu 💙💛💚💜

Situace: Saša si svá hesla zapisovala do poznámkového bloku v mobilním telefonu. Na mobilním telefonu ale neměla žádný zámek ani heslo.

Vyhodnocení: Pokud není telefon zabezpečený, jde o velmi rizikové místo pro ukládání hesel (a nejenom pro ukládání hesel). K heslům (a ostatním datům) se může dostat kdokoli, kdo má nezabezpečený telefon v ruce. Zámek do telefonu by mělo být celé heslo, Touch ID nebo Face ID (určitě ne gesto nebo PIN). Heslo bychom také měli mít nastavené na přístup do poznámkového bloku, kde máme hesla uložená.



13. Zásada: Veřejnou Wi-Fi používáme opatrně ♥ ♥

Situace: Rodiče Sašu pomocí dětského internetového bankovníctví učí používat bankovní účet, na kterém má od nich nastřádané kapesné. Saša není fanouškem obědů ve školní jídelně, a tak se jednou rozhodla zajít si na oběd do fastfoodu. Připojila se zde na Wi-Fi a podívala se do svého internetového bankovníctví, aby věděla, kolik peněz má k dispozici.

Vyhodnocení: Používání veřejné Wi-Fi (restaurace, obchody, letiště apod.) je velmi nebezpečné. Kdokoliv, kdo je k této Wi-Fi síti také připojen, může odposlouchávat ostatní zařízení na síti. Proto se na veřejné Wi-Fi nikdy nepřihlašujeme (zadané heslo může získat útočník), nepoužíváme internetové bankovníctví (útočník by zjistil všechny informace o našem účtě) a nenavštěvujeme nevhodné stránky (útočník nás může vydírat). Nejlepším řešením je místo veřejné Wi-Fi používat mobilní data.

14. Zásada: Neklikáme na podezřelé odkazy ♥ ♥

Situace: Otovi (13 let) přišla nová zpráva od kamarádky na Instagramu. Poslala mu odkaz. Oto si myslel, že jde asi o nějakou vtipnou stránku nebo zajímavost, a proto na odkaz klikl. V tu chvíli začaly z jeho Instagramu neuvěřitelnou rychlostí odcházet zprávy všem jeho přátelům se stejně závadným obsahem a odkazem na nebezpečnou stránku. Dřív, než se Oto stihl vzpamatovat z šoku, někdo ho nahlásil a jeho profil byl zablokován.

Vyhodnocení: Nikdy neklikáme na podezřelé odkazy od neznámých lidí ani od přátel. Neklikáme ani na podezřelé bannery a reklamy. Hrozí, že jedním kliknutím se do našeho zařízení dostane škodlivý program, který může napáchat spoustu nepříjemností.

15. Zásada: Nenavštěvujeme nebezpečné stránky ♥

Situace: Ludvík se naučil crackovat placené programy, hry, filmy a seriály na pirátských stránkách. Má doma nadupaný počítač, a tak stahuje všechno, co ho jen trochu zajímá. Během několika měsíců měl už ale pětkrát hacknutý počítač a pokaždé si musel měnit všechna hesla, dvakrát zakládat nový Steam účet na hry a jednou dokonce přeinstalovat celý počítač, takže ztratil všechna data.

Vyhodnocení: Stahujete v online prostředí hry? Stahujete hry také nelegálně – např. z různých webových úložišť? Znáte názvy některých z nich? (Ulož.to, The Pirate Bay, Datoid, WebShare, HellSpy, RapidShare nebo eSoubory) Má toto stahování nějaká rizika? Jaká? Crackování her je nejenom nemorální a nelegální, ale dokonce i nebezpečné. Na pirátských stránkách se velmi často objevují soubory, které obsahují malware. Uživatelé, kteří často crackují a neumí se dostatečně chránit, trpí častými hackerskými útoky. Jak se můžeme malwaru bránit? (antimalware, pravidelná aktualizace operačního systému i všech programů).



16. Zásada: Používáme jeden antivirus ♥

Situace: Silvia má ve svém telefonu stažené tyto aplikace: Gmail, Spotify, Messenger, WhatsApp, Avast Antivirus, Google Mapy, YouTube, Instagram a Tik Tok. Jednoho dne při brouzdání internetem na Silviu vyskočilo varovné okénko, že její telefon obsahuje tři viry. Silvia se zděsila a rychle stáhla Eset Antivirus, aby mohla viry odstranit. Program Eset ji neustále hlásil, že má v telefonu jeden malware, kterého se nemohla zbavit.

Vyhodnocení: Silvia již v telefonu měla nainstalovaný Avast Antivirus. Není možné mít nainstalovaných více antivirů na jednom zařízení současně. Antiviry se navzájem vidí jako malware a snaží se ho zbavit, mezitím se ale do zařízení může dostat skutečný malware. Při brouzdání internetem také nevěřte falešným reklamám, které vás informují, že vaše zařízení obsahuje viry. Jde o poplašné zprávy, které se snaží do vašeho zařízení právě nějaký ten virus propašovat. Jediný, kdo může hlásit, že vaše zařízení obsahuje malware, je antivirus.

Licence

Toto dílo – Bezpečnost on-line - Příloha Bezpečnostní zásady je licencován pod licencí Creative Commons Uvedte původ-Zachovejte licenci 4.0. Autorem je Lukáš Havelka.

Licenční podmínky navštivte na adrese <https://creativecommons.org/licenses/by-sa/4.0/legalcode.cs>.

