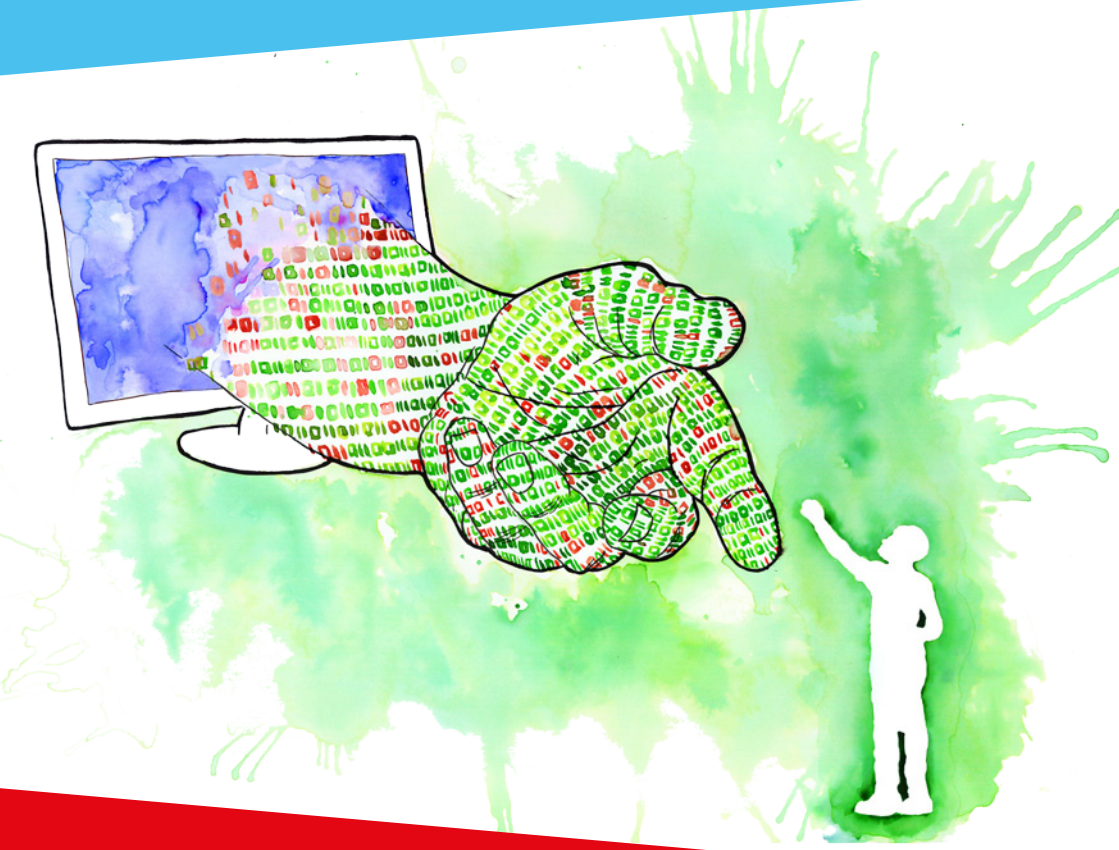
Roman Kohout
Sandra Kubíčková

Internetem Bezpečně



Příručka pro děti od 6 do 12 let

Internetem Bezpečně
Autor: Roman Kohout
Grafická úprava: Sandra Kubíčková
Úprava textu a korektura: Mgr. Marcela Chmarová
Vydal: you connected, z. s.
Počerny 146
360 17 Karlovy Vary
info@youconnected.cz
Tisk: AZUS Březová, s. r. o.
Vydání: Dotisk 1. vydání
Karlovy Vary 2018, říjen

ISBN 978-80-270-3101-6 (publikace)

ISBN 978-80-270-3102-3 (online pdf)

Publikaci je možné stáhnout na www.internetembezpecne.cz

Ahoj,

právě jsi otevřel první stranu malého průvodce Internetem Bezpečně, kterého jsem napsal pro tebe. Ptáš se, jak to můžu vědět, když tě ani neznám? Vím to, protože moje práce je často o tom, že je někdo nešťastný z událostí, které se mu staly na internetu (na facebooku, na WhatsAppu atd.). A tak chci předat dál důležité informace, které by měl znát každý. I ty.

Proto doufám, že v téhle knížce najdeš všechno, co potřebuješ umět, aby ses dokázal/a postarat o svoji bezpečnost na internetu. Nebo aby sis uměl/a poradit, pokud na tebe bude někdo na internetu zlý či nepříjemný. Nebo abys s tím uměl poradit kamarádce či kamarádovi, dědovi s babičkou, mladším sourozencům nebo třeba i rodičům.

Internet dnes máme všichni v telefonech, tabletech, počítačích atd. Většina z nás zde umí platit účty, sdílet fotky, „lajkovat" vše, co se nám líbí. Nejdůležitější je ale umět nejprve zabezpečit sebe a svůj počítač a vyhýbat se nebezpečí. Chraň svá tajemství dobrými hesly a chraň sám/sama sebe bezpečným chováním na internetu.

Není třeba se bát. Internet ti nabízí mnoho dobrého a užitečného. Jen je třeba mít se na pozoru a umět si (nechat) poradit.

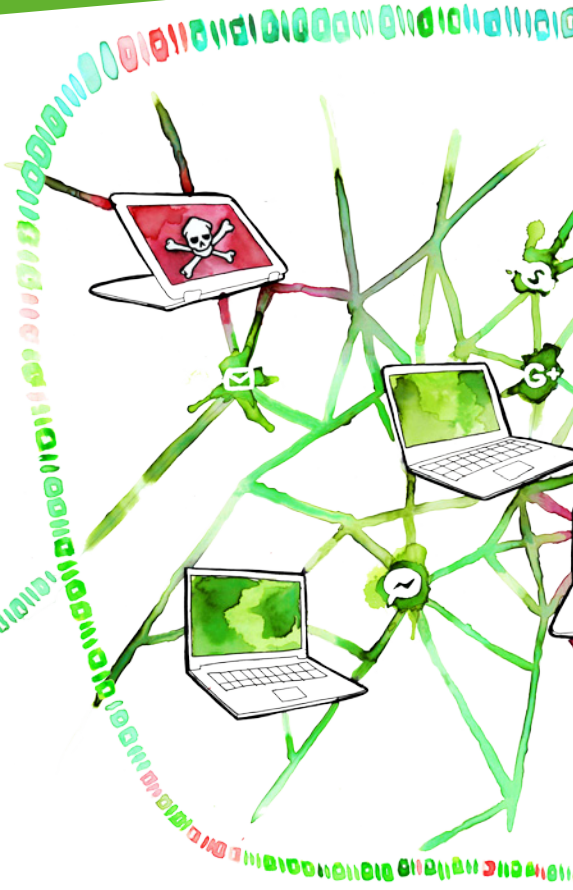
Roman Kohout
autor

Publikace byla vytištěna díky laskavé podpoře společnosti O_2

Obsah

Co je internet ?

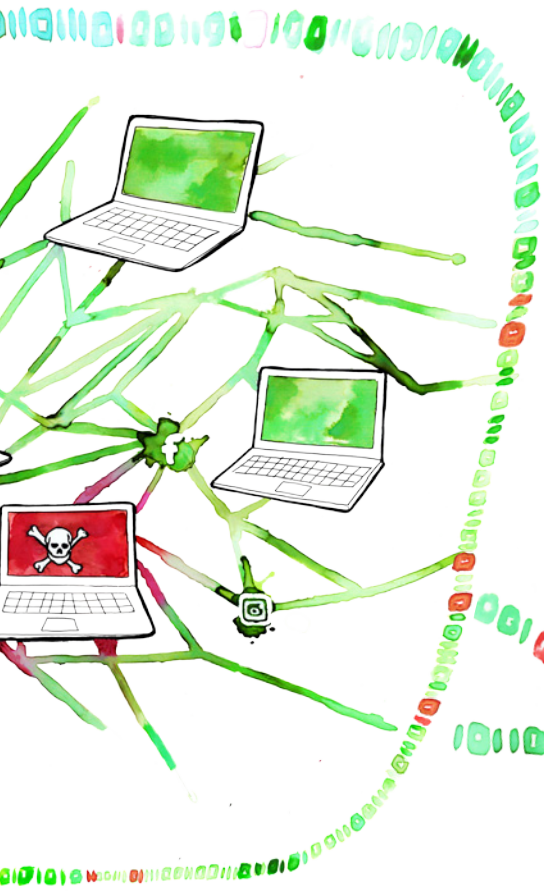
Představ si obrovské množství počítačů, které jsou vzájemně propojeny v jedné velké počítačové síti. A to je internet. Díky tomu můžeme komunikovat, posílat fotky nebo hrát počítačové hry s někým, kdo je právě teď na druhé straně planety. Není to úžasné?



I na internetu jsou však zlí lidé se špatnými úmysly ... Např. kradou důležitá data, peníze nebo tajemství, která pak mohou sdělit někomu dalšímu.

Před těmito lidmi je třeba být na pozoru. Pomůže ti s tím dodržování několika základních pravidel bezpečného chování na internetu - koukni na str. 31.

Na internetu je dnes možné dělat prakticky cokoliv: hrát počítačové hry, nakupovat a platit účty, sdílet fotografie a zážitky, posílat emaily, telefonovat, vyhledávat informace a mnoho dalších věcí. A většina z nás takto internet užívá.



Komunikuješ-li s kamarádem přes internet, nezapomeň, že mezi tvým a jeho počítačem je tedy ještě velké množství cizích počítačů, a ne všechny tyto počítače mají hodní lidé.

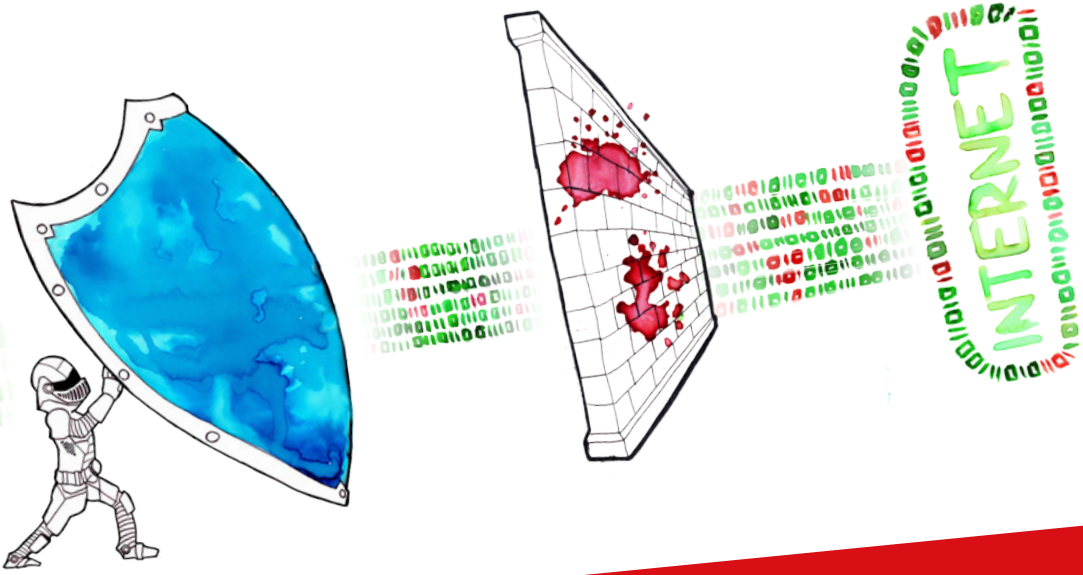
Jak správně zabezpečit počítač?

A obezřetnost ...

Buď opatrný. Než na něco klikneš, přečti si všechno, co je k tomu napsáno. Klidně třikrát. A neboj se někoho zeptat, pokud tomu nerozumíš.
Nikdo z nás neví všechno.

Heslo do počítače

Heslo tě chrání. Chrání tvá tajemství, tvá data - pokud si zvolíš špatné heslo, může toho někdo využít a tvá tajemství ukrást.



Základní zabezpečení počítače

Antivirový program

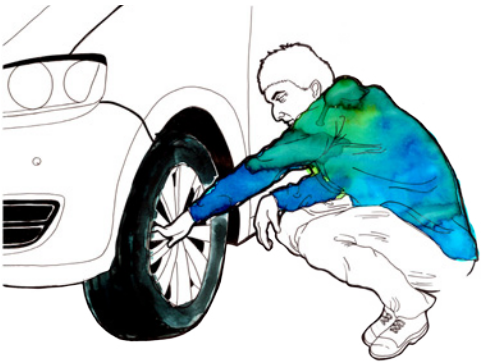
Kontroluje činnost všech programů ve tvém počítači. Ty se zlými úmysly (jako jsou počítačové viry) okamžitě zastaví nebo odstraní.

Firewall

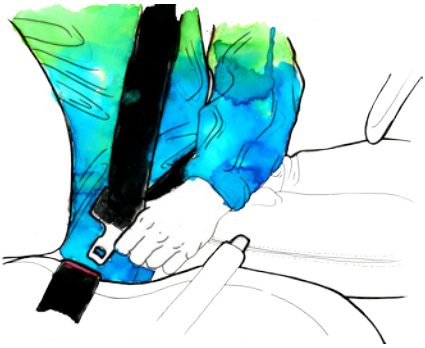
Úkolem firewallu je zablokovat „špatná“ data, která by se mohla chtít vloudit nenápadně do tvého počítače. A je v tom opravdu dobrý.

Než se vypravím na internet ...

Než se vypravíš autem:



Zkontroluj stav vozidla.



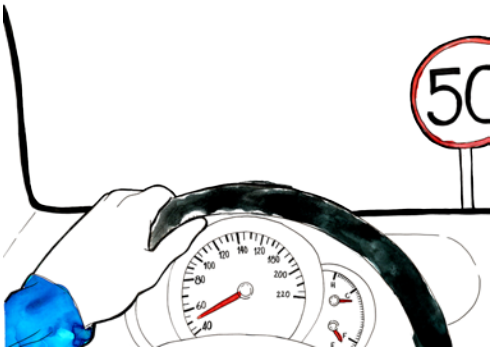
Mysli na svou bezpečnost.

Než se vypravíš na internet:

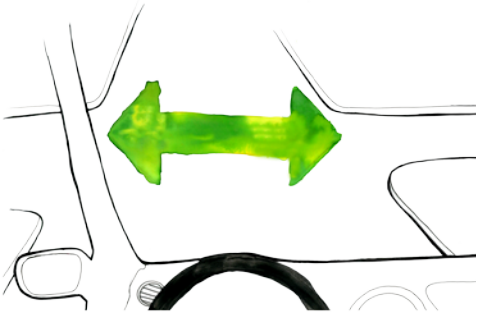
Zkontroluj zabezpečení počítače.

Nesděluj nikomu své osobní informace ani svá hesla.

Vypravit se na internet je podobné, jako se vypravit na cestu autem.



Dodržuj pravidla silničního provozu.



Než vjedeš do křižovatky, pořádně se rozhlédni.

Dodržuj pravidla bezpečného chování na internetu.

Než na cokoliv klikneš, pořádně si přečti, co potvrzuješ.

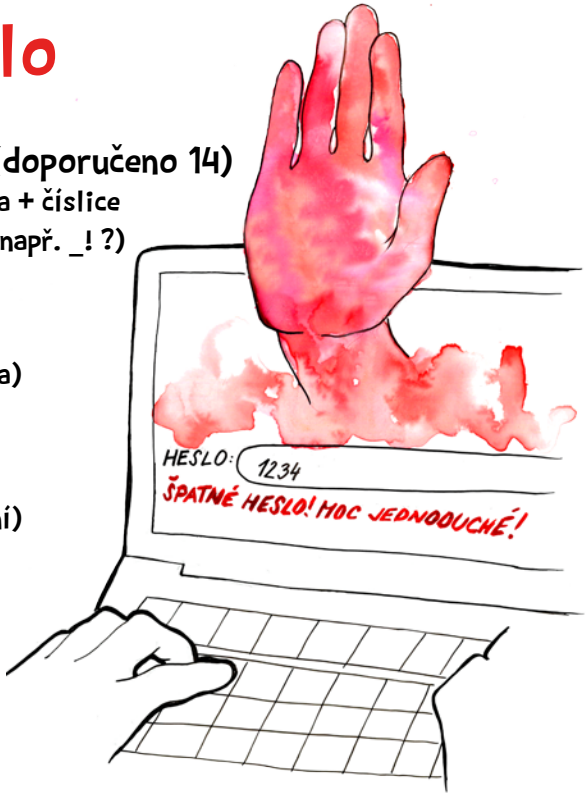
Heslo

Tvoje heslo je jako klíč od domu. Když je ten klíč kvalitní, nikdo si bez něj dveře do domu neotevře. Bude-li ale špatně zhotovený, nebude mít zloděj s otevřením dveří moc práce.

Bezpečné heslo by se proto mělo skládat ze znaků, které nikdo nezjistí ani neuhodne.

Bezpečné heslo

- má minimálně 8 znaků (doporučeno 14)
  malá písmena + velká písmena + číslice
  + má v sobě i speciální znak (např. _ ! ?)
- není uhodnutelné
  (jako je jméno tvého mazlíčka)
- není snadno zjistitelné
  (jako je datum tvého narození)
- není běžná posloupnost
  (jako je 12345, abcd)



Vytvoř si 3 okruhy hesel

1. okruh

router
heslo do počítače
heslo do mobilního telefonu nebo tabletu

Nejtajnější hesla z nejtajnějších ...

2. okruh

email
sociální sítě
(facebook, snapchat, instagram aj.)

Nikam je nepiš a nezapomínej se odhlašovat.

3. okruh

chaty
hesla do počítačových her
hesla do internetových obchodů

Také tajná hesla, ale měla by být jiná než předešlá.

Jak vytvořit heslo? Snadno!

Vymyslet neprůstřelné heslo není jen tak. A zapamatovat si ho - to vyžaduje hodně práce. Nebo ne?
Koukni na tenhle jednoduchý postup, jak na to:

NÁVOD

Vymysli si krátkou větu s číslovkou:

Můj pes má čtyři nohy a jeden ocas.

Z každého slova použij první písmeno a číslovky změň na čísla.

mpm4na1o

Některá písmena udělej velká.

MpM4Na1o <- hustokrutopřísné heslo :)

Jak si zapamatuješ více hesel? Stačí jedno trochu pozměnit, koukej!
ml_MpM4Na1o heslo do emailové schránky
MpM4Na1o_fb heslo do sociální sítě facebook
MpM4Na1o_game heslo do počítačové hry

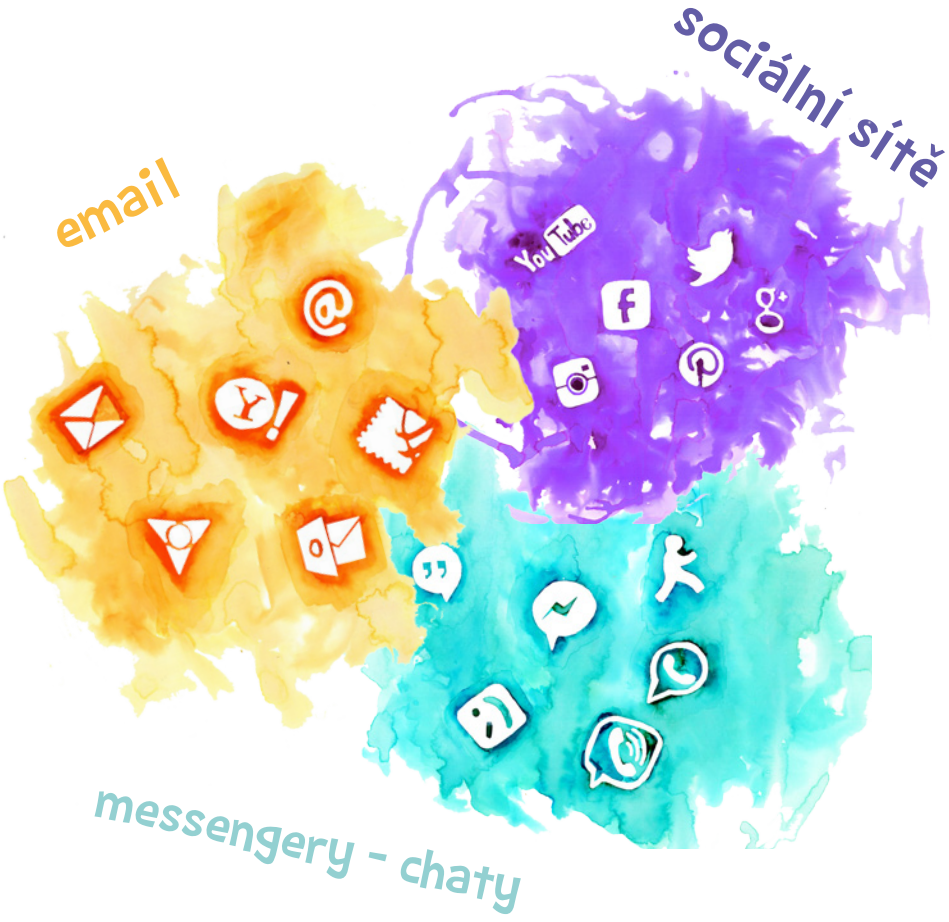
Nikdy, nikdy, nikdy!
Hesla nikdy nikomu neposílej přes internet (emailem apod.).
Hesla si nikam nepiš - zapamatuj si je.
Nepoužívej stejné heslo k více službám najednou.
Nikdy nenechávej heslo dlouho beze změny - pravidelně ho měň.

Příklady nejhorších hesel

1. 12456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball
11. welcome
12. 123456890
13. abc123
14. 111111
15. 1qaz2wsx
16. dragon
17. master
18. monkey
19. letmein
20. login
21. princess
22. qwertyuiop
23. solo
24. passw0rd
25. starwars

Internetová komunikace

Internet ti nabízí široké možnosti komunikace.
I tady ale platí jistá pravidla, která je potřeba znát.



Desatero bezpečné komunikace

1. Ignoruj neslušné zprávy a neodpovídej na ně. Nikdy.
2. Pokud s někým nechceš komunikovat, nekomunikuj.
3. Zprávy od neznámých osob hned smaž. Může to být podvodník nebo se ve zprávě může nacházet počítačový vir.
4. Na profilech sociálních sítí nikdy neuváděj své telefonní číslo, rodné číslo nebo adresu.
5. Své telefonní číslo nebo adresu nikomu neposílej ani v soukromé zprávě. Ten, kdo ji chce, může být někdo úplně jiný, než sám/sama říká, že je.
6. Nedomlouvej si schůzky přes internet. Na schůzku domluvenou přes internet nechoď, aniž bys o tom řekl někomu dalšímu.
7. Nikomu neposílej své nahé fotografie, protože můžou být rozesílány dalším lidem. Pokud po tobě někdo chce intimní fotografii, přestaň s ním ihned komunikovat.
8. Mysli na své digitální já - mysli dvakrát, než na internet napíšeš něco nevhodného nebo urážlivého.
9. Při používání webové kamery buď opatrný, kdokoli může na druhé straně hovor nahrávat.
10. Uzamkni svůj počítač nebo telefon, pokud s ním dál nebudeš pracovat. Nastav si automatické uzamknutí při delší nečinnosti.

Kyberšikana

Kyberšikana je, když ...

... útočník využívá internet a mobilní technologie pro to, aby mohl někomu ublížit: zesměšnit ho, ztrapnit, ohrozit nebo zastrašit.

Kyberšikana je třeba:

- posílání urážlivých a zastrašujících zpráv nebo pomluv
- natáčení videí nebo pořizování fotek a jejich zveřejnění na internetu bez souhlasu aktérů
- vytvoření webové stránky, která uráží, pomlouvá nebo ponižuje
- krádež identity
- provokování a napadání uživatelů v diskuzních fórech
- odhalování cizích tajemství
- vydírání pomocí moderních technologií
- obtěžování a pronásledování pomocí moderních technologií

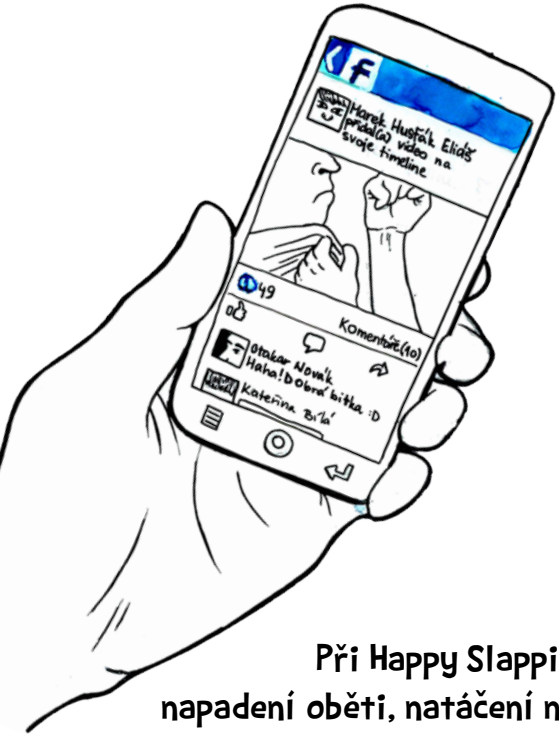
Znaky kyberšikany:

- útočník se domnívá, že je anonymní – ALE NENÍ TOMU TAK!
- na internetu nerozhoduje fyzická síla – šikanovat tu může klidně i „slabší silnějšího“
- nevíš, kdy a kde přijde útok
- v šíření kyberšikany pomáhá útočníkovi „publikum“
- není snadné rozeznat dopady kyberšikany na oběť
- kyberšikana může být způsobena i neúmyslně – jako nepovedený vtip
- často je spojena s tradiční šikanou

Happy Slapping

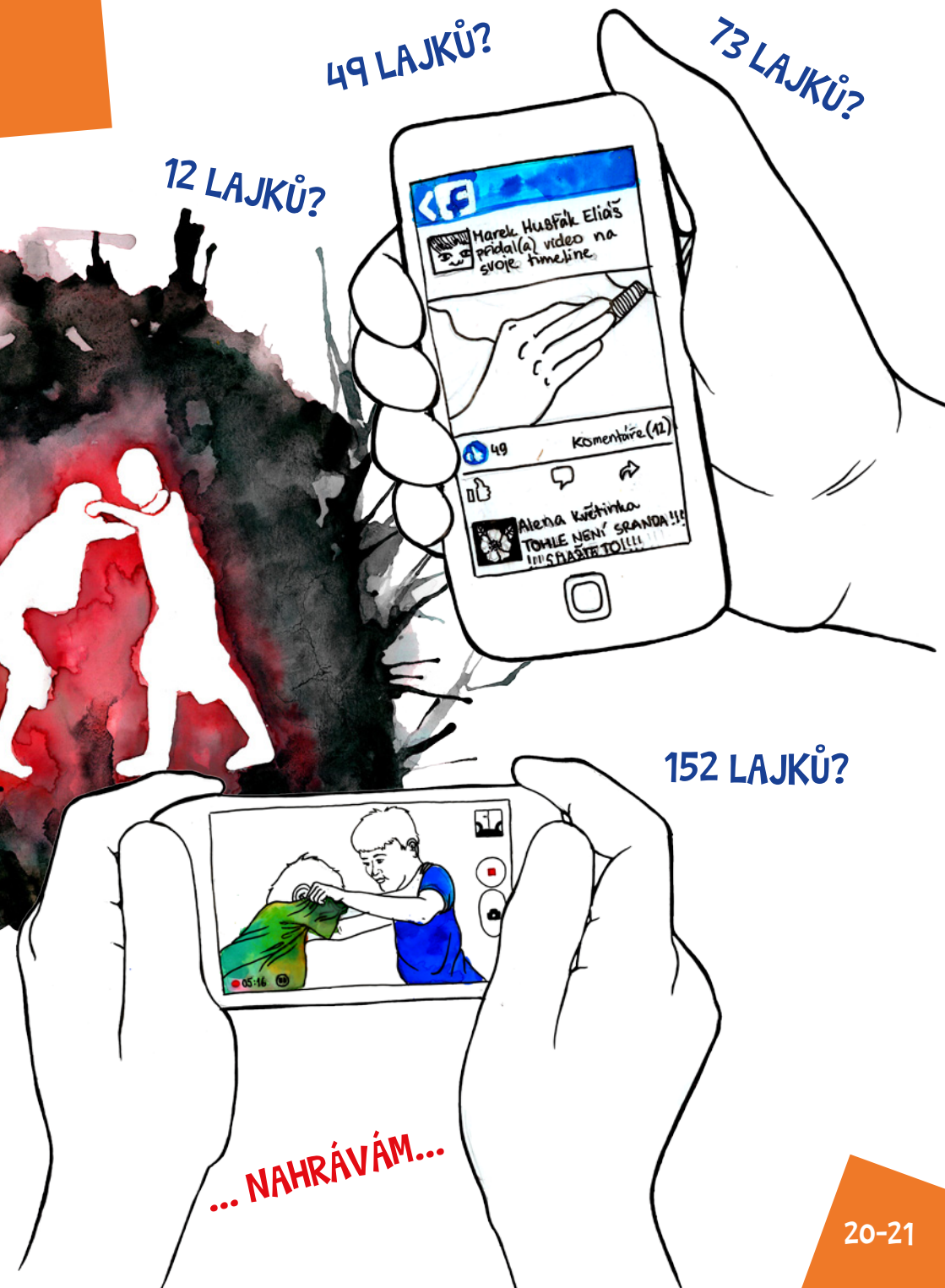
Happy Slapping je, když ...

... útočník fyzicky napadá oběť
a pořizuje záznam tohoto násilí
na telefon, tablet atd.
... a tento záznam dál šíří
(mobilem, na facebooku apod.).



Nikdy to není „jen hra“

Při Happy Slappingu může být TRESTNÉ všechno:
napadení oběti, natáčení napadení (pořizování záznamu),
pozorování a neohlášení násilí, jeho sdílení a jiné šíření!


49 LAJKŮ?
73 LAJKŮ?
12 LAJKŮ?
Marek Hubřák Eliáš přidal(a) video na svoje timeline
49
Komentáře (12)
Alena Květinka
TOHLE NENÍ SRANDA!!!
!!! SMAŽTE TO!!!!
152 LAJKŮ?
05:16
... NAHRÁVÁM...

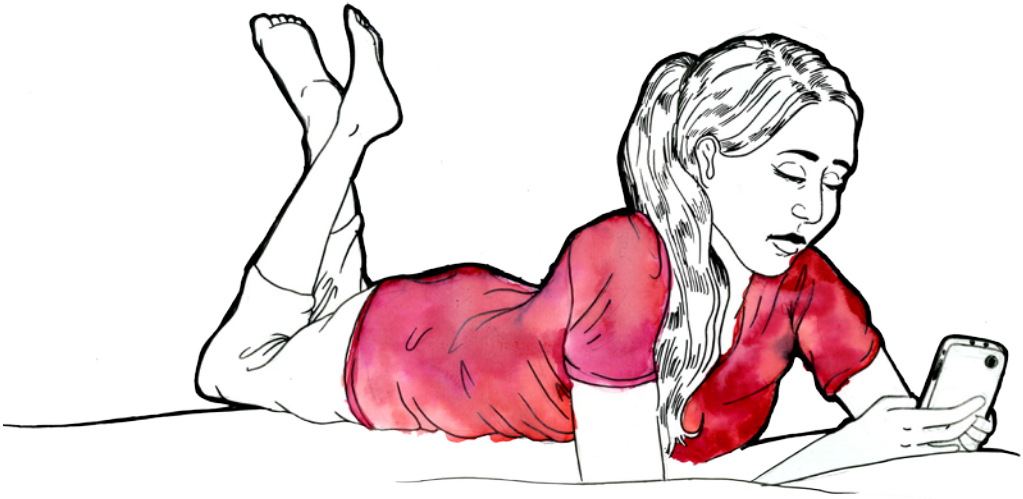
Sexting

Sexting je, když ...

... si někdo píše o sexuálních tématech např. na facebooku nebo posílá svoje nahé fotky a videa pomocí počítače, chytrého telefonu, tabletu atd.

Jakékoliv šíření sextingu může být trestné!

Na žádost o takové fotky/videa nebo informace nikdy nereaguj! Prostě si s takovým člověkem přestaň psát. A řekni o něm dospělákům! Třeba tím zachráníš někoho jiného.



Nikdy nevíš, kdo je na druhé straně.

Na internetu se lidé často vydávají za někoho jiného.
Takový člověk může vaše dopisování, fotky a videa zneužít.
Třeba je zveřejní na internetu – kdykoliv se mu zachce!
A bohužel není možné je „smazat“ nebo jinak odstranit.

Také je může použít k vydírání – může to být kybergroomer
(podívej se na stranu 24 – 25).

DĚJE SE TO?
NAJDI ODVAHU A ŘEKNI TO!

Kybergrooming

Kybergrooming je, když ...

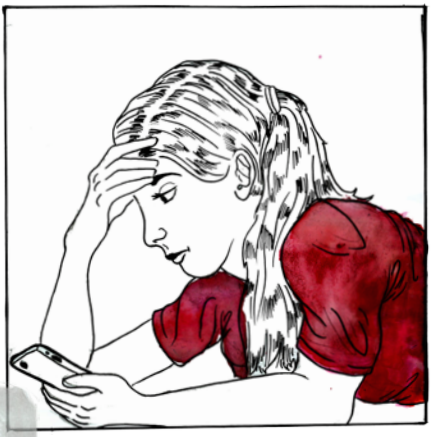
... si útočník vymýšlí a lže oběti pro to, aby přišla sama na osobní schůzku. Zde jí chce ublížit nebo ji chce sexuálně zneužít. Většinou se snaží komunikovat chatováním na facebooku.

Útočník se snaží různými způsoby získat důvěru oběti.

Jak to kybergroomer dělá?

- chválí, lichotí a předstírá zájem
- chce, aby se mu oběť se vším svěřovala
- pomlouvá její rodiče, kamarády atd. (aby ji „měl“ jen pro sebe)
- snaží se ji podplatit: novým mobilem, penězi, dobitím kreditu atd.
- chce ji mít „v hrsti“ tím, že získá její nahé fotky, videa apod.
- udělá cokoliv, aby přišla na osobní schůzku
- může ji různě vydírat, aby ji donutil přijít (např. chce její fotky a videa poslat rodičům)
- na osobní schůzce ji ublíží, zneužije ji nebo znásilní
- dál ji může vydírat, aby to nikomu neříkala

DĚJE SE TO?
NAJDI ODVAHU A SVĚŘ SE!

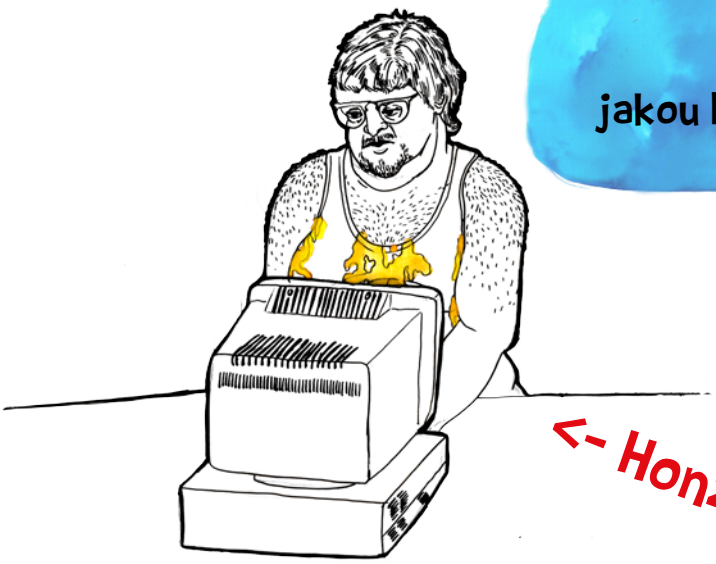


Ahoj, jsem Honza a je mi 12 let, nechceš si se mnou psát?

Ahoj, já jsem Anička, proč ne...

Hodně se mi líbíš, pošleš mi nějakou svoji fotku?

Díky, jakou bys chtěl ...???



<- Honzík

Kyberstalking

Kyberstalking je, když ...

... útočník někomu neustále píše zprávy nebo ho jinak kontaktuje (zasíláním SMS, na zdi facebooku, na chatu, pomocí instant messengerů apod.), nebo jej pomocí moderních technologií neustále sleduje.

Jak se to odehrává?

Útočník chce oběti znepříjemnit život. A tak:

- nevhodně komentuje její příspěvky na zdi facebooku atd.
- otravuje častým zasíláním SMS, emailů nebo zpráv z chatů
- pořád sleduje, s kým se stýká a s kým si píše
- může obtěžovat zprávami i její kamarády

DĚJE SE TO?
NAJDI ODVAHU A ŘEKNI TO!

Hoax

Hoax je, když ...

... někdo vyšle do internetového světa falešnou zprávu, mystifikaci, novinářskou kachnu, poplašnou zprávu, výmysl nebo kanadský žert.

Hoax vzniká, když někdo chce:

- pobavit
- vyvolat strach
- šířit falešnou radu
- manipulovat s názory lidí
- poškodit instituci, značku, firmu, výrobek
- ohromit, zaujmout, přilákat pozornost
- vystřelit si z důvěřivých uživatelů

Jakým způsobem se ke mně hoax dostane?

Hoax byl dříve hodně rozesílán emailem, avšak v současné době je šířen spíše skrze sociální sítě jako je facebook nebo messengery jako je WhatsApp.

Jak poznáš, co je hoax? Zjisti si to!

Na internetu kolují tisíce hoaxů. Proto každou informaci ověř. Využij internetové vyhledávače (seznam.cz, google.com) nebo navštiv www.hoax.cz. Zde se falešným zprávám přímo věnují.

Jak se bránit???

UKONČI KOMUNIKACI

Pokud je na tebe na internetu někdo zlý, hned s ním přestaň komunikovat. A řekni to na něj.

NEBLOKUJ ANI NEMAŽ ZPRÁVY OD ÚTOČNÍKA

Pokud je na internetu někdo zlý, policie by to měla vědět - a k usvědčení podvodníka nebo jiné zlé osoby potřebuje důkazy.

OZNAM NEPŘÍJEMNOU ZKUŠENOST

Pokud se ti nelíbí, jak se k tobě někdo na internetu chová, přestaň okamžitě komunikovat a svěř se se svým problémem.

BUĎ HRDINA

Pokud se dozvíš, že byl někdo přes internet zlý na tvého kamaráda, a ten to nechce oznámit, udělej to za něj. Pomůžeš mu.

Kam se obrátit?

Stalo se ti na internetu něco, z čeho máš špatný pocit? Najdi odvahu a řekni to!

Běž za dospělákem!

Za dospělákem, kterému věříš: může to být máma/táta, učitel/ka, brácha/ségra, školní psycholog, trenér atd.
Požádej je o pomoc!
(a vezmi tuhle knížku s sebou)

Neboj se jít na policii!

Nebo jim zavolej - 158 (a oni přijedou za tebou).
Věř mi, že ti určitě pomůžou.

Pokud nevíš, za kým jít, zavolej na Linku bezpečí - 116 111 (je to zdarma).

Desatero bezpečného internetu

1. Na internet se připojuj pouze z důvěryhodného zdroje. Doma řádně zabezpeč svůj router a při připojení na volné wifi síti nikdy nezadávej svá hesla.
2. Udržuj svůj počítač nebo telefon aktualizovaný - operační systém, programy (zejména internetový prohlížeč), antivir.
3. Programy instaluj pouze z důvěryhodného zdroje.
4. Nastav si automatické zamykání svého počítače nebo telefonu při delší nečinnosti.
5. Užívej silná hesla ke každé službě a NIKOMU je nesděluj - ani blízké osobě. A nikam si je nepiš!
6. Pečlivě nastav svá zabezpečení, kontroluj nastavení soukromí a možnosti sdílení tvého obsahu na facebooku a jiných sociálních sítích.
7. Ověřuj informace. Internet není vševědoucí - každá informace nemusí být pravdivá.
8. Přemýšlej, než klikneš. Před každým potvrzením si vždy přečti veškeré podmínky.
9. Chraň své osobní údaje - nikomu je na internetu nesděluj (svou adresu, datum narození atd.).
10. Neotevírej zprávy od cizích lidí - hlavně přílohy v emailech nebo chatech. Může v nich být vir.

Desatero bezpečného internetu

Internetem Bezpečně

Internetem Bezpečně
Autor: Roman Kohout
Grafická úprava: Sandra Kubíčková
Úprava textu a korektura: Mgr. Marcela Chmarová
Vydal: you connected, z. s., Počerny 146, 360 17 Karlovy Vary
info@youconnected.cz
Tisk: AZUS Březová, s. r. o.
Vydání: první
Karlovy Vary 2017, prosinec
ISBN 978-80-270-3101-6 (publikace)

ISBN 978-80-270-3102-3 (online pdf)
Publikaci je možné stáhnout na www.internetembezpecne.cz

Zdroje:
www.hoax.cz
www.wikipedia.org
www.nebudobet.cz
www.bezpecnyinternet.cz
Roman Kohout, Mgr. Radek Karchňák - Bezpečnost v online prostředí
(ISBN 978-80-260-9543-9)

Příručka pro děti od 6 do 12 let