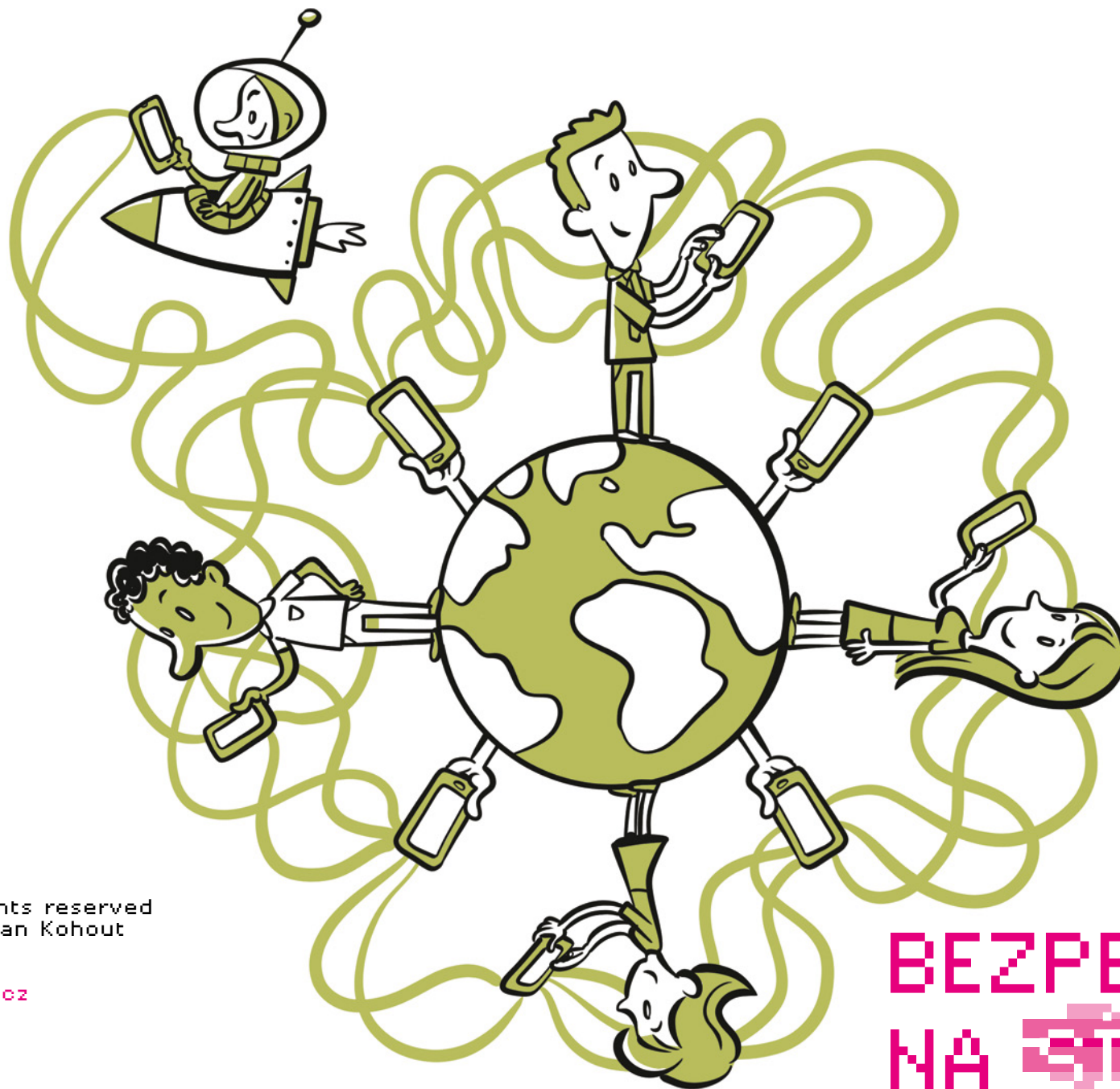


T...



T-Mobile Czech Republic
Copyright © 2018. All rights reserved
Text: Adam Maršál a Roman Kohout
Ilustrace: Petr Morkes
www.t-mobile.cz
www.internetembezpece.cz

T-Mobile
Pomáháme 

BEZPEČÍ NA SITI

Sláva internetu! Ale to ho máme užívat jen tak?

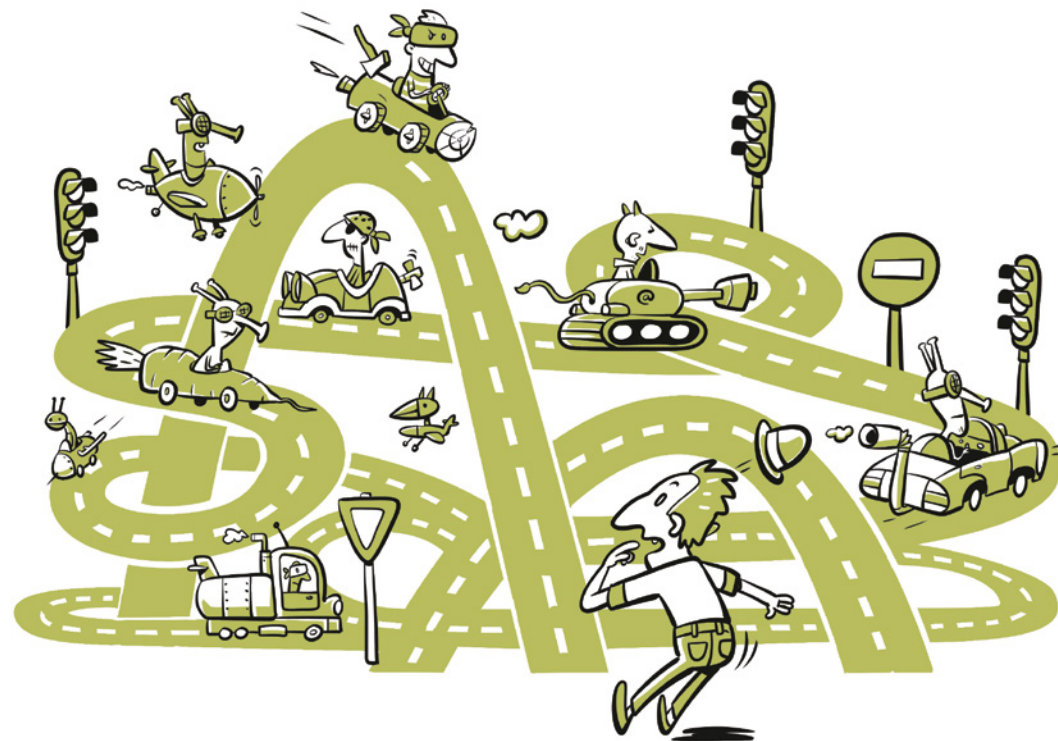
Téměř žádná činnost včetně té vaší se neobejde bez internetu. Připravili jsme proto pro vás pár rad, jak předejít případným potížím spojeným s jeho užíváním.

Nástrahy nehrozí jen počítačům, tabletům a chytrým telefonům, ale i na sociálních sítích. Víte, jak snadno se lze zmocnit nedostatečně zabezpečeného profilu nebo jakých věcí byste se měli ve světě virtuálních přátelství raději vyvarovat?

Internetem už směle plují i naše děti. Moderní rodič by měl vědět, co vše, světovou internetovou síť nevyjímaje, je může potkat, a poradit si, jak se k tomu postavit.

Naše doporučení vycházejí z knihy Internetem Bezpečně – Jak se nestat obětí virtuálního predátora od Romana Kohouta, který se v řadách Policie ČR věnuje vyšetřování kybernetické trestné činnosti.

Více informací naleznete na www.t-mobile.cz a www.internetembezpecne.cz.



Vždycky je lepší se trochu rozhlédnout,
než uděláte první krok. Všude člověk
může narazit. Ať už chcete, nebo ne,
týká se to i internetu.

REÁLNÝ SVĚT
A VIRTUÁLNÍ
MAJÍ K SOBĚ BLÍŽ,
NEŽ SI MYSLÍME



Uvědomujeme si rizika i na síti?
Zatímco v reálném světě jsme si vědomi
nástrah, jaké nás mohou potkat, ve
virtuálním prostředí se někdy chováme
jako malé děti.

Znáte základní pravidla pro bezpečí vašich zařízení připojených k internetu?

Nechránit majetek, nezamknout si dveře od bytu nebo předat cizímu člověku klíč od sejfu? Toho by se dopustil jen hlupák. Ale na netu mnohdy děláme totéž, jen si neuvědomujeme možné následky. Oba světy jsou si něčím podobné. A oba mají svá rizika. Zatímco ve městech navštěvujeme banky, obchody a kávéárny nebo se zastavíme na ulici na slovíčko se známým, na internetu nakládáme s financemi v e-bankách, nakupujeme v e-shopech nebo se s přáteli bavíme na sociálních sítích. Těžko si představíme, že bychom žili bez klíčů a bezpečnostních karet. Ale jsme takto zodpovědní i na netu?



Jak na to:

Používejte pouze aktualizovaný operační systém, nové verze aplikací i programů a vyhněte se nelegálnímu softwaru, s nímž si můžete nevědomky stáhnout i věci, které nechcete. Vždy si také rozmyslete, na co klikáte. I jedno stisknutí tlačítka může způsobit lavinu problémů.

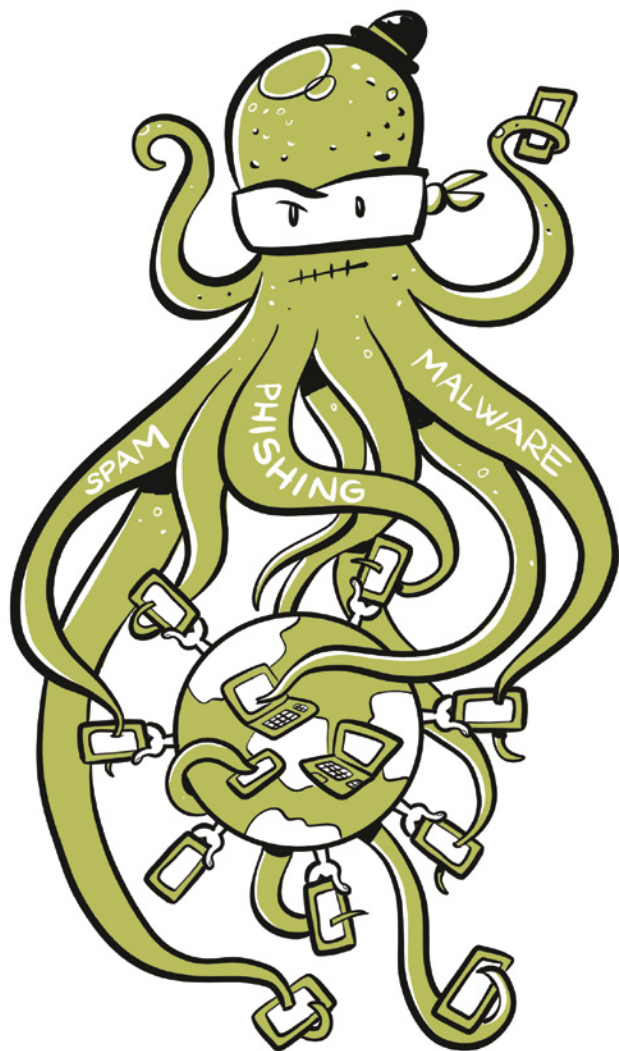
Dr. Netík říká:

Co vám můžou kybernetičtí piráti vzít?
Vaše fotky, bankovní konta, identitu, citlivé informace nebo profil na sociálních sítích.
To asi nechcete.



CO NA NÁS ČÍHÁ V HOUŠTI INTERNETU

2



Víte, co si na vás brousí zuby,
když se dost dobře nedíváte?
Na internetu je hodně dobrého.
Nekonečně užitečného.
Ale také špatného.

Spam

Nevyžádaná pošta, která s sebou často nese vir, falešnou výzvu nebo jiný závadný obsah

Co s tím?

- nebudte důvěřiví ke zprávám od cizích odesílatelů
- podezřelou poštu neotvírejte, mažte ji
- označte ji jako spam

Sociální inženýrství

Podvodná, manipulativní praktika, která po vás bude chtít, abyste si třeba nainstalovali „praktickou“ apku. Ta vás pak ale začne monitorovat...

Jak se tomu vyhnout?

- nedůvěřujte výzvám
- ignorujte nabídky z nevyžádané pošty
- nikam a nikomu nikdy neposílejte své osobní údaje, čísla nebo data

Phishing

Falešná stránka, která vypadá stejně jako elektronické bankovníctví vaší banky s cílem vylákat z vás osobní údaje. Jeví se jako seriózní dialog, okno nebo dokument, do nějž důvěřivě vyrazíte to, co byste měli uchovat v tajnosti.

Jak nenaletět?

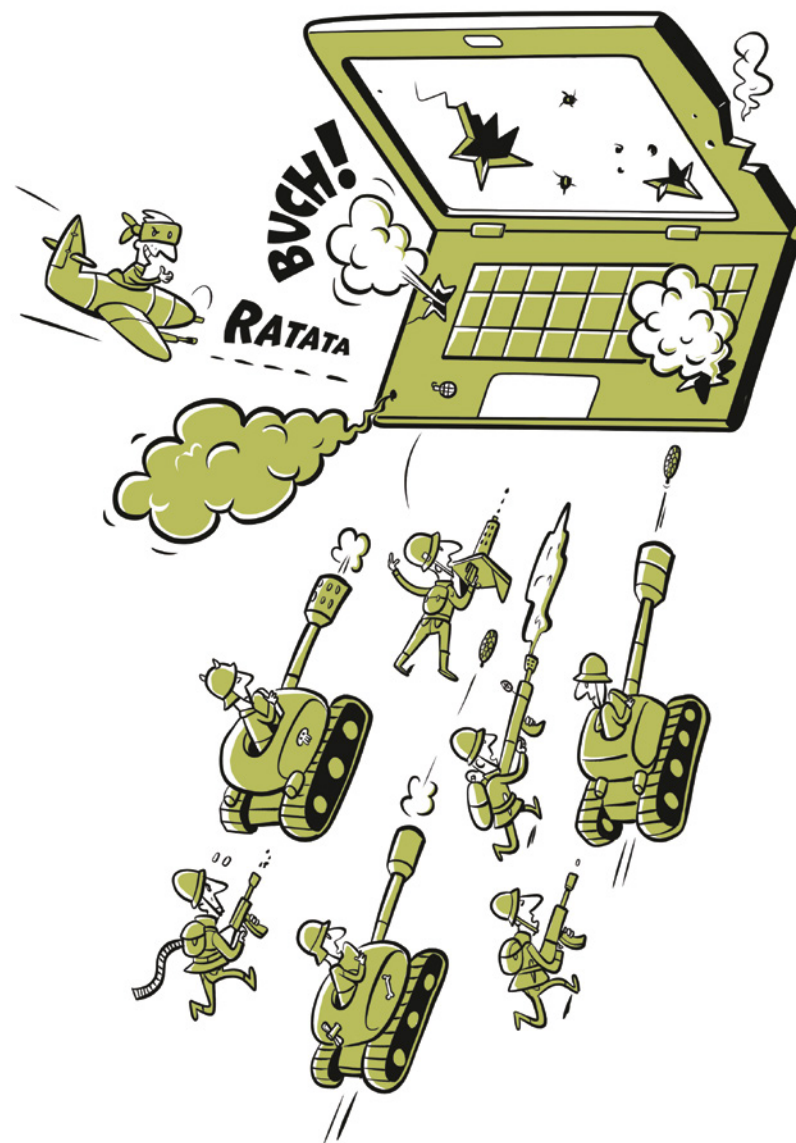
- kontrolujte webovou adresu stránky, z níž se někde přihlašujete. Sedí s tou, co běžně vídáte?
- nevypisujte žádné osobní údaje do formulářů, které vám přijdou mailem – seriózní instituce tohle nikdy neudělá

Malware

Zlý software, který má celou řadu podob. Může vniknout do vašeho systému, aby ho poškodil, ovládl jej, odcizil z něj data nebo vás sledoval. Chcete vědět víc? Otočte stránku!

JAKOU ŠKODU
VÁM ZPŮSOBÍ
NEJČASTĚJŠÍ
PŘÍPADY
MALWARU?

3



Jistěže jsme o tom už mnohokrát
slyšeli. Ale pro pořádek si to
shrňme. Třeba vám to pomůže
utřídit informace, které byste
o škodlivém softwaru chtěli říct
vlastním dětem.

Malware má celou řadu podob

Počítačový vir

Šíří se v přílohách mailů se spustitelnými soubory. Má za cíl poškodit váš systém, ale v současnosti jej snadno odhalí antivirový program.

Počítačový červ

Jeho zákeřnost spočívá ve schopnosti se samostatně replikovat a šířit dál, aby poškodil vaše data.

Trojan

Dostane se do vašeho systému přes zdánlivě neškodný nebo užitečný program. Často se jeví dokonce opačně jako např. antivir, který vás vybízí ke stažení a instalaci. Pokud to dopustíte, bude se snažit získat moc nad vaším zařízením, získat vaše data nebo ovládat běžící systémy.

Keylogger

Sleduje a zaznamenává klávesy, které stisknete. Kybernetický útočník tak může získat uživatelská jména s hesly nebo číslo platební karty a následně je zneužít.

Botnet

Bude chtít k síti „zotročených“ zařízení připojit i váš počítač, aby jej zapojil do další kybernetické kriminality. Bez vaší vůle se tak třeba začnou odesílat spamy na všechny adresy ve vašem adresáři.

Ransomware

Škodlivý software, který zašifrováním zamezí přístup k určitým souborům. Útočník po vás bude požadovat „výkupné“ výměnou za to, že vám soubor zpřístupní nebo odemkne.

Dr. Netík říká:

Jak se bránit malwaru? Používejte antiviry.
Nestahujte programy z neověřených zdrojů.
Neotvírejte přílohy nevyžádané pošty,
i kdyby vám slibovaly, že se rázem ocitnete
v ráji na zemi.



HLÍDEJTE SI
MOBILY

4



Na net jsou připojeny i chytré telefony, rizika se nevyhýbají ani jim.

Dr. Netík říká:

Co dělat při ztrátě mobilu? Změňte hesla na všech účtech i v aplikacích a zrušte spárování platební karty s těmito účty.



1 Věci, které byste měli vědět, než do mobilu začnete instalovat nějakou aplikaci

2 Do mobilu instalujte výhradě aplikace z aplikačního obchodu operačního systému

Všechny jiné kroky mohou být nebezpečné.

3 Vir se vám do mobilu nedostane sám

Vnikne vám tam jedině tak, že si ho sami nainstalujete třeba prostřednictvím falešné aplikace. Návštěvou stránky nebo otevřením mailu se vám do zařízení nedostane.

4 Riziko se dá poznat

Pokud je nějaká stránka závadná, telefon ji sám o sobě nerozezná. Falešné stránky nebo aplikace se často samy prozradí kvůli použití nespisovné češtiny nebo gramatickým chybám. Dejte si pozor na všechny pochybné výzvy a v žádném případě se jimi neřidte. Instrukce nevedou k nápravě (fiktivního) problému, ale k jeho zažehnutí.

Máte virus, co bude dál?

Nejspíš to nijak nepocítíte. Virus bývá nenápadný a spíš se skrývá. Ale může o vás získávat informace, které pak posouvá dál třeba kvůli reklamě. Často se projeví zpomalením systému. Nejrychlejší obranou je uvedení přístroje do továrního nastavení.

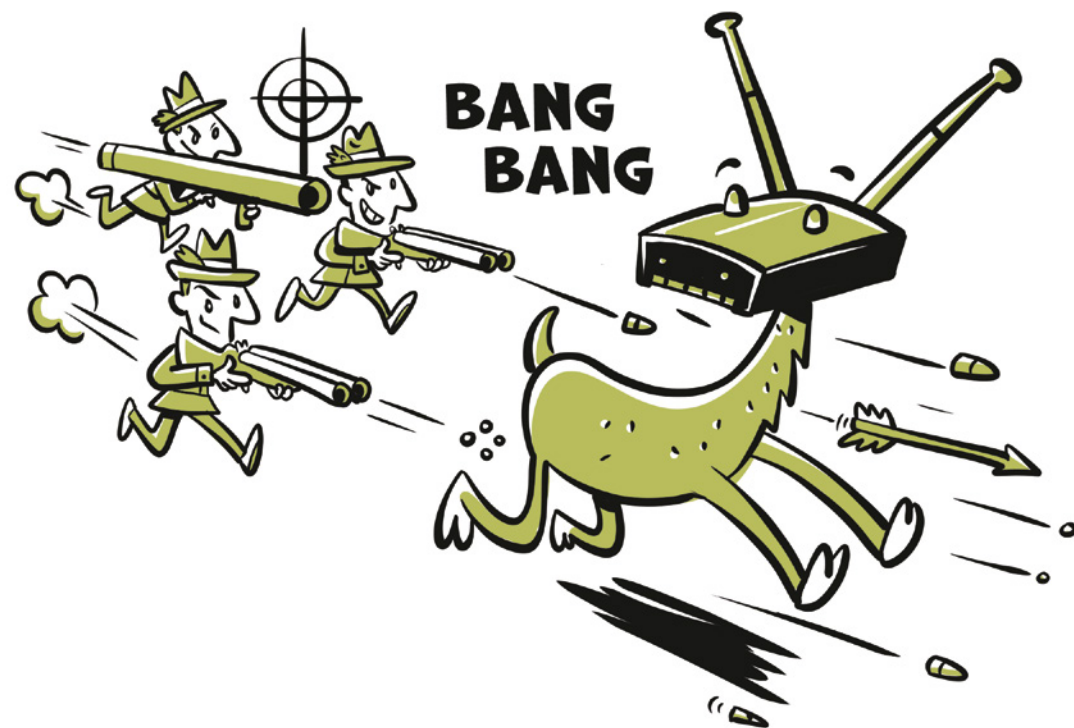
Dr. Netík říká:

V Česku stovkám lidí vyskočilo na displeji smartphonu okno se sdělením, že jejich mobil je zavirován a osobní data budou ztracena, pokud si ihned nepořídí antivir v ceně 99 Kč za týden. Pokud by se vám něco takového stalo, nic nepotvrzujte, protože právě to by vedlo k zavirování. Stačí zařízení restartovat a po restartu zavřít všechny záložky v prohlížeči.



5

ZABEZPEČTE SI INTERNET



Nezabezpečený domácí router si přímo říká o útok. Chvíli vám to může procházet, ale je otázkou času, kdy se na stopu vaší Wi-Fi pustí kybernetičtí pytláci. Připojí se na ni bez vašeho vědomí a vyčkají, až jim sami odevzdáte svá citlivá data. Jak tomu předejít?

1

3 kroky pro zabezpečení domácí sítě:

Zabezpečte svůj router

- to je ta krabička s anténou, která umožňuje, že vám doma chodí Wi-Fi
- změňte heslo pro administraci
- aktualizujte firmware

2

Zabezpečte svou Wi-Fi

- změňte název a heslo
- heslo musí být dostatečně silné (viz kapitola 7)
- zašifrujte síť šifrovacím protokolem WPA2. Pokud jej váš router neumí, je čas koupit nový. Vaše komunikace a data nejsou chráněny!

3

Rozhodněte o tom, kdo se na vaši Wi-Fi připojí

- na Wi-Fi routeru můžete nastavit, aby síť byla přístupná jen vašemu počítači, mobilům nebo dalším zařízením ve vaší domácnosti podle jejich MAC adresy
- znamená to, že se připojí jen tato zařízení, nebo můžete dokonce některá výslovně zakázat
- drtivá většina moderních routerů umí vysílat dvě Wi-Fi sítě. Využijte toho! První, třeba pod názvem domácí, bude sloužit pro členy domácnosti a druhá, pojmenovaná jako hosté, pro návštěvníky. Ti tak neuvidí nasdílená zařízení a data ve vaší počítačové síti

Neumíte si s některým z těchto kroků poradit?

Není to nic složitého. Obrátte na prodejny T-Mobile, kde vám rádi poradí.

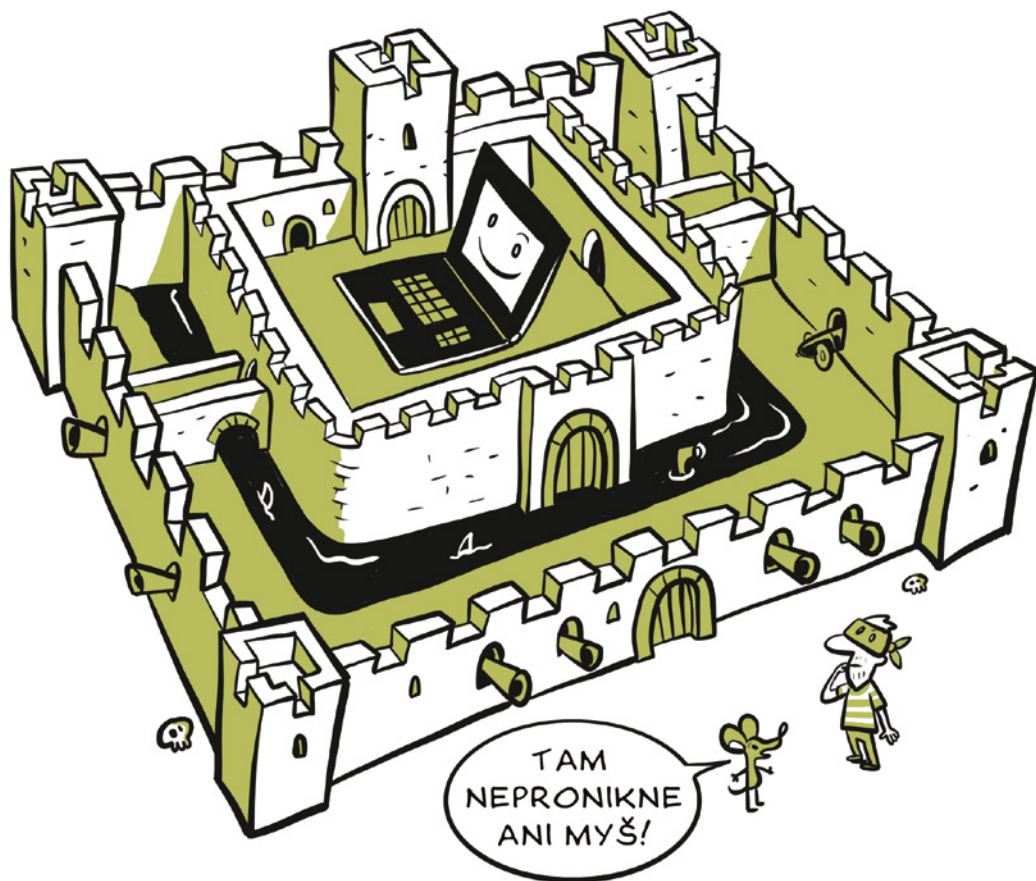
Dr. Netík říká:

Co pro vás znamená bezpečné připojení? Že se na vaši síť bez vašeho povolení nepřihlásí někdo nepovolaný. Jen tak budete mít v bezpečí veškerá data, hesla, osobní fotografie, videa nebo záznamy. Nezvaný host ve vaší síti by vám mohl třeba podstrčit falešnou webovou stránku té legitimní (např. přihlášení do e-banky).



ZABEZPEČTE SI SVÁ ZAŘÍZENÍ

6



Jestli se vše zlé vyhne obloukem vašim zařízením, není otázkou šťastné náhody, ale odpovědné prevence. Není to žádná věda, zvládne to i váš pes (pokud se aspoň trochu motá kolem IT).

1

Více bariér = více bezpečí

Pořídte si antivir

Protože denně vznikne až několik desítek nových škodlivých virů, které můžou vaše zařízení napadnout. Antivir je včas odhalí, eliminuje a odstraní z vašeho zařízení.

2

Aktivujte firewall

Protože tak bude pod kontrolou datový tok do vašeho počítače. Firewall ho usměrňuje a v případě potřeby ho dokáže i zastavit. Do vašeho počítače tak nepustí to, co tam nemá být.

3

Zálohujte si data

Protože to je pořád nejjistější způsob, jak o ně nepřijít. Data není jen tak nějaký IT pojem – jsou to fotky z vaší svatby, fotky vašich dětí, když udělaly první krok... Chtěli byste je jednou provždy ztratit jen proto, že jste si neudělali čas na to je bezpečně uložit?

4

Pravidelně aktualizujte operační systém

Protože je tvořen z miliónů řádků programového kódu, kde kybernetičtí útočníci hledají chyby, aby je mohli využít k ovládnutí celého systému. Pravidelné aktualizace tyto chyby opravují.

**VYTVÁŘEJTE SILNÁ
HESLA. VŽDY
A KE VŠEMU**

7

Dr. Netík říká:

Silné heslo si nejlépe vytvoříte pomocí slovní mnemotechnické pomůcky jako: ms07lsobj5n1 (mam skodu Oktavku 7 let starou co bere jenom 5 na 100).



Heslo je jako zámek na dveřích. Některé rozloupne bytař hned, na jiných si vyláme zuby. Postavte nekalostem na síti do cesty pevné dveře se silným zámkem. Vytvářejte silná hesla!

Jak vypadá silné heslo

- má aspoň 10 znaků
- jsou v něm písmena i číslice
- minimálně jedno písmeno je velké
- obsahuje minimálně jeden symbol (?, *, #, +)

A které lze snadno uhádnout?

- jména blízkých
- jména mazlíčků
- samostatná slova
- data narození
- běžné posloupnosti (1234...)
- symboly nebo čísla na začátku

Za jak dlouho speciální program prolomí vaše heslo?

4 znaky: 4,8 s
6 znaků: 11 hodin
8 znaků: 10 let
9 znaků: 1 000 let
10 znaků: 91 800 let

Pozn.: Znakem rozumíme užití malého či velkého písmena, číslice nebo symbolu.

Dr. Netík říká:

Budete se divit, ale nejčastější hesla na internetu jsou stále 123456 a password.



VÍTE, ŽE JSTE PO
PŘIHLÁŠENÍ K FREE
Wi-Fi JAKO NAZÍ
V TRNÍ?





Na volném připojení může trochu zkušenější sígr sledovat vaše kroky na internetu, jako kdyby seděl přímo vedle vás.

1

Na free Wi-Fi obezřetně

Rozlišujte, kam se hlásíte

Když už používáte veřejné Wi-Fi (free Wi-Fi), přemýšlejte, na jaké služby se hlásíte. Například návštěvu elektronického bankovníctví nebo internetovou platbu nechte až na zabezpečenou domácí Wi-Fi.

2

Žraloci číhají

Existují aplikace, které zaznamenají veškerou komunikaci se všemi Wi-Fi sítěmi v dosahu.

3

Dali byste z ruky platební kartu?

Na netu se vám to přitom stane, ani nevíte... Pachatel může odchytnout např. vaši komunikaci s e-shopem a díky tomu se v budoucnu vydávat za vás – a bezplatně „nakoupit“ na váš účet!

Dr. Netík říká:

Jakmile nakládáte s penězi, hlásíte se do internetového bankovníctví nebo něco nakupujete kartou, dělejte to jen na zabezpečené Wi-Fi.



9

**ALE FACEBOOK JE
PŘECE BEZPEČNÝ.
NEBO SNAD NE?**



I mezi vašimi přáteli jsou oběti kybernetického zločinu. Co to znamená? Že vám nehrozí nebezpečí jen tak od někoho, ale třeba právě od vašich známých.

Jak si pohlídat profil na sociálních sítích

- buďte kritičtí k výzvám k přijetí přátelství od lidí, které neznáte a s nimiž ani nemáte společné přátele
- ignorujte žádosti o přátelství od cizích krásků s cizími jmény a nahlaste je jako spam (samo se nabídne – stačí kliknout)
- neotvírejte odkazy, které vám přišly bez komentáře, a to i na Messengeru. Může dojít k ovládnutí vaší identity a jejímu využití k dalšímu šíření spamu – proces se spustí a už se nedá zastavit
- nepřihlašujte se ke službám nebo hrám prostřednictvím svého profilu
- ignorujte žádosti o zaslání peněz, a to i od přátel, stejně jako soutěže o podezřele výhodné produkty jako třeba super letenky, kam se máte přihlásit pod svým profilem
- neuvádějte na svých profilech osobní údaje
- neposílejte své nahé fotografie – nikdy nikomu – dají se vždy snadno zneužít

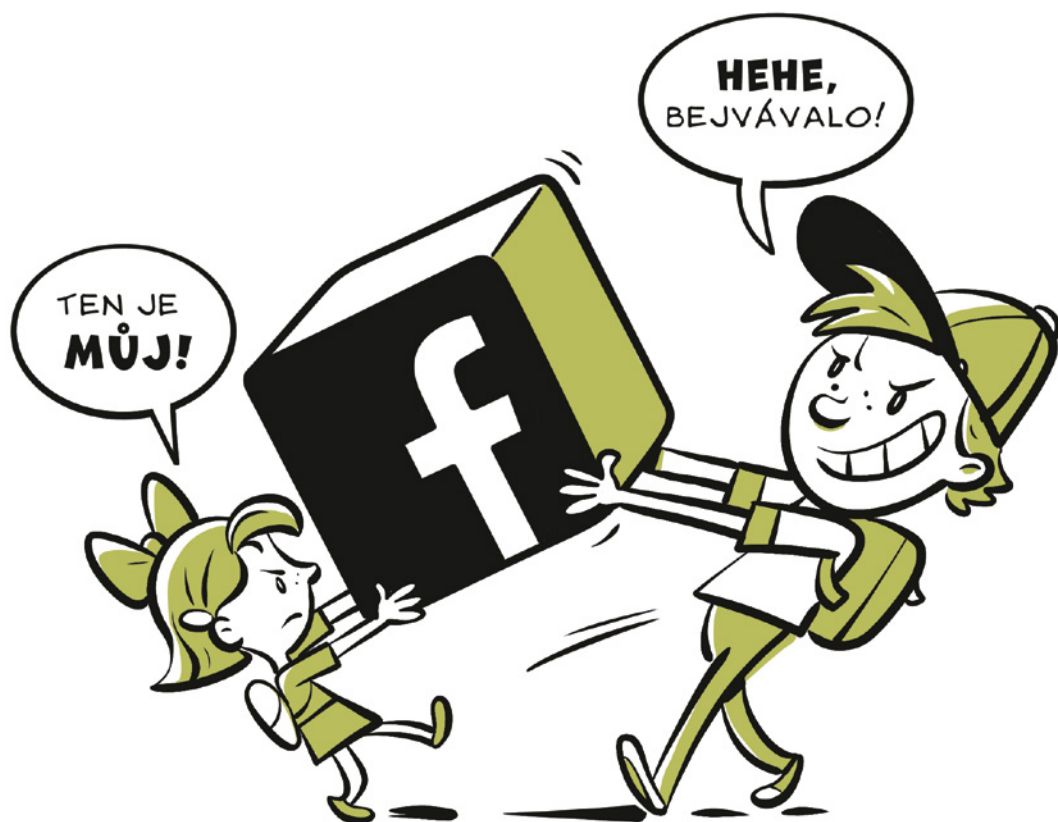
Dr. Netík říká:

Na sociálních sítích o sobě nezveřejňujte nic, co byste nevyvěsili na sloup na ulici.



10

MĚJTE SVŮJ PROFIL NA SOCIÁLNÍ SÍTI POD KONTROLOU



Používejte dvoufázové ověření

Dvoufázové přihlášení je běžné hlavně u bankovních ústavů. Kromě jména a hesla v něm musíte zadat ještě jeden další údaj, který nelze získat bez držení vašeho telefonu. Jde buď o kód ze SMS, nebo mobilní aplikace.

Na Facebooku si nastavte zasilání výstrah při přihlášení

Nastavte si Facebook tak, abyste měli pod kontrolou, co se o vás šíří. Díky tomu si odsouhlasíte i příspěvky, na kterých jste označeni.

Nenechte si napadnout svůj účet

Možná už jste o tom slyšeli. Ti méně šťastní to už zažili. Váš profil na Facebooku byl zneužit a začal si žít vlastním životem.

Stane se to třeba takto:

Pracujete na počítači a najednou na vás vyskočí chatovací okno Messengeru. Je to zpráva od přítele, přesněji řečeno odkaz... Asi nějaká vtipná stránka? Zajímavost? Kliknete na to, protože přeci: Proč ne? A mají vás! Váš profil už není jen váš profil. Trojský kůň jej ovládl a z vaší adresy teď neuvěřitelnou rychlostí odcházejí zprávy všem vašim přátelům se stejně závadným obsahem. Nebo jim dáváte na jejich zed' odkaz na porno. Děje se to přímo před vašimi očima. Dřív, než se vzpamatujete ze šoku, vás někdo nahlásí a váš účet je zablokován. Možná jednou provždy. Jakmile je uvnitř systému, umožňuje kybernetickým padouchům nabourat se do vašeho facebookového účtu a šířit se z něj dál.

Jak tomu předejít?

1

Nikdy neotvírejte odkazy, které vám přijdou přes Messenger bez výslovného komentáře, a to ani od přátel

2

I pokud takový odkaz dostanete, zamyslete se, zda je pravý

3

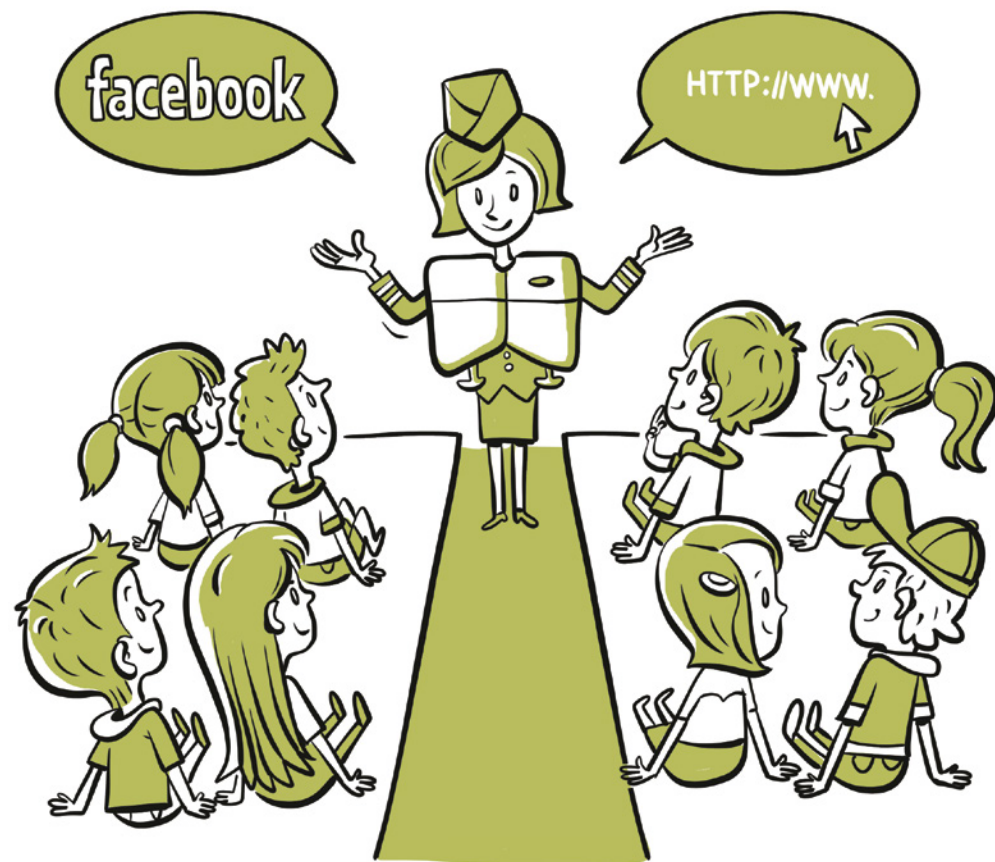
Pokud si nejste jisti, napište odesílateli a zeptejte se ho

4

V žádném případě neklikejte na odkazy od lidí, které neznáte nebo kteří teprve žádají o vaše přátelství

11

JAK INTERNET PŘEDSTAVIT SVÝM DĚTEM



Nejdůležitější je důvěra. Ve všech velkých příbězích se předávají zkušenosti z generace na generaci, ale z čeho má člověk vycházet, když v době našeho dětství žádný internet nebyl? Vždy se vyplatí spolehnout na instinkt a dělat to tak, jak byste chtěli, aby někdo učil vás.

1

Internetová výchova

2

Jděte dětem příkladem

Děti napodobují vaše chování. To, co budete v jejich přítomnosti dělat vy, budou dělat i ony. Totéž platí i v chování na internetu a používání připojených zařízení.

3

Vysvětlete jim analogii se skutečným světem

Virtuální svět je odrazem toho skutečného. I v něm nám hrozí určitá rizika. Ukažte dětem, že stejně jako se musí připoutat v autě nebo si dávat pozor při chůzi ze schodů, nemohou se ani na internetu chovat neopatrně a cokoli bezhlavě sdílet.

4

Budte u toho s nimi

Podobně jako spolu s dětmi sdílíte radost z jejich objevování světa her, můžete to být právě vy, kdo je provede prvními kroky na internetu. Není důvod to odkládat – děti jsou zvědavé a budou chtít vědět, co se děje na displeji, ze kterého si denně něco čtete.

5

Odhadněte správný čas

Všechno má svůj čas. I na vás je seznamovat děti s odpovědností na internetu krok za krokem. Jakmile dítěti pořídíte první telefon, měli byste stanovit i základní pravidla pro jeho užívání. Spolu se založením účtu na sociálních sítích si promluvte o etiketě a bezpečném sdílení.

Nechte je, ať vás něco naučí

Nebudeme si nic nalhávat. V mnoha ohledech jsou na tom děti dál než my. Anebo brzy budou. Děti své rodiče rády poučují, a pokud jim v tom dáte sami prostor, nejenže se dozvíte něco nového, ale posílíte vzájemnou důvěru.

ZÁKLADNÍ KAMENY PRO SPRÁVNOU VÝCHOVU

12

ANO

Tyhle kroky už prověřily desetitisíce rodičů. Promluvte si o nich otevřeně s dětmi a diskutujte, jestli se na nich shodnete společně.

NE

Vzdělávejte se

Když budete v obraze, děti za vámi samy přijdou pro radu.

Budte otevření

Když něco nevíte, s největší pravděpodobností to budou vědět vaše děti. Zeptejte se jich! Nejenže vám to třeba řeknou, ale opět posílíte vzájemnou důvěru.

Staňte se jejich virtuálním přítelem

Budete mít přehled, co dělají a s kým se stýkají na sociálních sítích.

Naučte je kritickému myšlení

Ne všechno, co je na internetu, je pravda. Sledujte společně, co je zajímavé, a mluvte o tom.

Vedte je k ochraně soukromí

Předejdete únikům věcí, které může třetí strana zneužít.

Řekněte jim, ať vás upozorní, když se s nimi bude chtít někdo setkat

Protože ne každý je tím, za koho se na netu vydává.

Sledujte změny v jejich chování

Můžou být varovným signálem, že se vaše dítě stalo obětí kyberšikany nebo že ho někdo vydírá.

Naučte je, ať se vám svěřují s tím, co našly na netu

Tak to přece dobře funguje i v běžném životě.

Nezakazujte jim něco bez vysvětlení

Jen tak budou vaši autoritu skutečně akceptovat.

Nezakazujte jim pohyb po internetu, ale sledujte ho

Neshazujte jejich chuť brouzdat po síti, bavte se o jejich zájmech.

Neříkejte, že vy jste jako děti přežili bez Facebooku

Stejně tomu tím nezabráníte.

Nedávejte nikdy nikam jejich nahé fotografie

Nikdy nevíte, kde a hlavně u koho můžou jednou skončit.

13

TO SE ŘEKNE
MÍT DÍTĚ POD
DOHLEDEM,
ALE JAK NA TO?



Když si s ním jdete hrát ven, také
jej nenecháte bez dozoru.
Tady chodíme po tenkém ledě,
řeknete si. Není snad neetické
sledovat, co někdo jiný dělá ve svém
soukromí - byť je to „jen“ děcko?
Stále je to však dítě, které může
některá rizika podcenit.

Kdo vám pohlídá děti?

Přehled nejen o tom, kde zrovna vaše děti běhají nebo jestli už jsou doma ze školy, ale i o stránkách, které na internetu navštěvují, a co si stahují, získáte díky řadě programů a nástrojů. Zkuste využít tipy z nabídky T-Mobile.

T-Mobile Školák

Tato služba je pro všechny zodpovědné rodiče. Díky ní uvidíte, kde se vaše děti nacházejí a jaké mají výdaje. Velkou výhodou je, že se vám dovolají i bez kreditu. S aplikací Surfie se dozvíte, že vaše dítě dorazilo bezpečně domů. Vedle toho sleduje jeho aktivity na internetu, monitoruje navštěvované stránky, stahované aplikace a čas strávený na netu. Službu T-Mobile Školák získáte ke svému tarifu za 99 korun měsíčně.

www.t-mobile.cz/skolak

Dětský zámek

Chrání děti a mladistvé před nevhodným obsahem v mobilu. Díky němu se nemusíte obávat, co vaše děti na mobilu vyvedou. Zámek jim zabrání v přístupu ke službám, které pro ně nejsou vhodné. Služba je poskytována všem rodičům zdarma.

www.t-mobile.cz/detsky-zamek

Rodičovská kontrola Kaspersky

Firemní zákazníci, kteří si aktivovali nový tarif pro podnikatele obsahující produkt Kaspersky Internet Security, mohou využít jeho funkci Rodičovská kontrola. Ta umožňuje nastavit omezení přístupu k webovým prostředkům a aplikacím pro různé uživatele podle jejich věku a zobrazení statistických zpráv o činnostech kontrolovaných uživatelů.

Bezpečný obsah

Na této stránce najdete seznam bezpečných aplikací a spoustu další zábavy nejen pro vaše děti.

www.aplikace.cz/skolak

**ŠIKANA BOLÍ
I NA NETU. JAK SE
MŮŽEME BRÁNIT?
A CO VAŠE DÍTĚ?**

14



Šikana na internetu = kyberšikana.
Ať už se stane cokoli, málokdy je
to tak zlé, aby se to nedalo řešit.
Největší chybou je nedělat nic.
Oběť se zpravidla cítí bezmocně
a osamoceně. Stydí se a neví, na
koho se obrátit, protože se bojí, že
si tak třeba ještě přitíží.

Co je kyberšikana?

- rozesílání urážlivých a zastrašujících zpráv nebo pomluv
- pořizování audio a video záznamů nebo fotografií a jejich zveřejnění s cílem poškodit oběť
- vytvoření webové (facebookové) stránky, která uráží, pomlouvá nebo ponižuje oběť
- krádež identity (prolomení zabezpečení e-mailové schránky nebo profilu na sociální síti) a následné vystupování útočníka pod identitou oběti
- provokování a napadání uživatelů v diskuzních fórech
- odhalování cizích tajemství
- vydírání, obtěžování a pronásledování pomocí informačních a komunikačních technologií

Dr. Netík říká:

Podle výzkumné zprávy Univerzity
Palackého v Olomouci se s kyberšikanou
setkalo 51 % dětí. 8 % českých dětí se
stalo obětí vydírání.



Kdy už končí legrace

Někdy už to není jenom o pocitech ponížení, ale o reálném vydírání. Dětem začíná hrozit riziko od deseti let věku, kdy se naučí samostatně komunikovat a navazují nové vztahy po síti a přidávají si přátele lehkomyšlně jako pokémony. Nový přítel skrývající se pod falešnou identitou z nich pak může vymámit (třeba i nahé) fotografie nebo osobní údaje. Tím získá nástroj pro další vydírání.

V horším případě může dojít k tomu, že někdo dítě zmanipuluje a vyláká ho na osobní schůzku, kde ho místo očekávaného kamaráda bude čekat dospělý člověk s nekalými úmysly. K tragickým případům nebo reálnému zneužití, které začaly zdánlivě nevinnou internetovou komunikací, došlo nejen v zahraničí, ale i u nás.

Děti byste měli poučit, že když po nich chce někdo něco, co jim není příjemné, měly by vám to oznámit. Současně lze takového člověka nahlásit. Pokud cítíte, že může jít o jednání směřující k trestné činnosti, nepodceňujte to. Nic ze sítě nemažte, protože historie komunikace může sloužit jako důkazní prostředek v dalším řízení.

Jak to řešit a na koho se obrátit

Nahlaste kyberšikanu. Je to snadné, protože to lze učinit **u každého příspěvku na Facebooku**.

Při podezření, že může jít o trestný čin, kontaktujte **Policii ČR: 158**

Když si děti nevědí rady, můžou kdykoli anonymně volat **Linku bezpečí: 116 111**

Dospělí se mohou poradit na **Rodičovské lince: 840 111 234 a 606 021 021**

Dr. Netík říká:

Podle výzkumné zprávy Univerzity Palackého v Olomouci pozvání na schůzku sjednanou přes internet potvrdilo skoro 32 % dětí a téměř 21 % na schůzku skutečně dorazilo.

