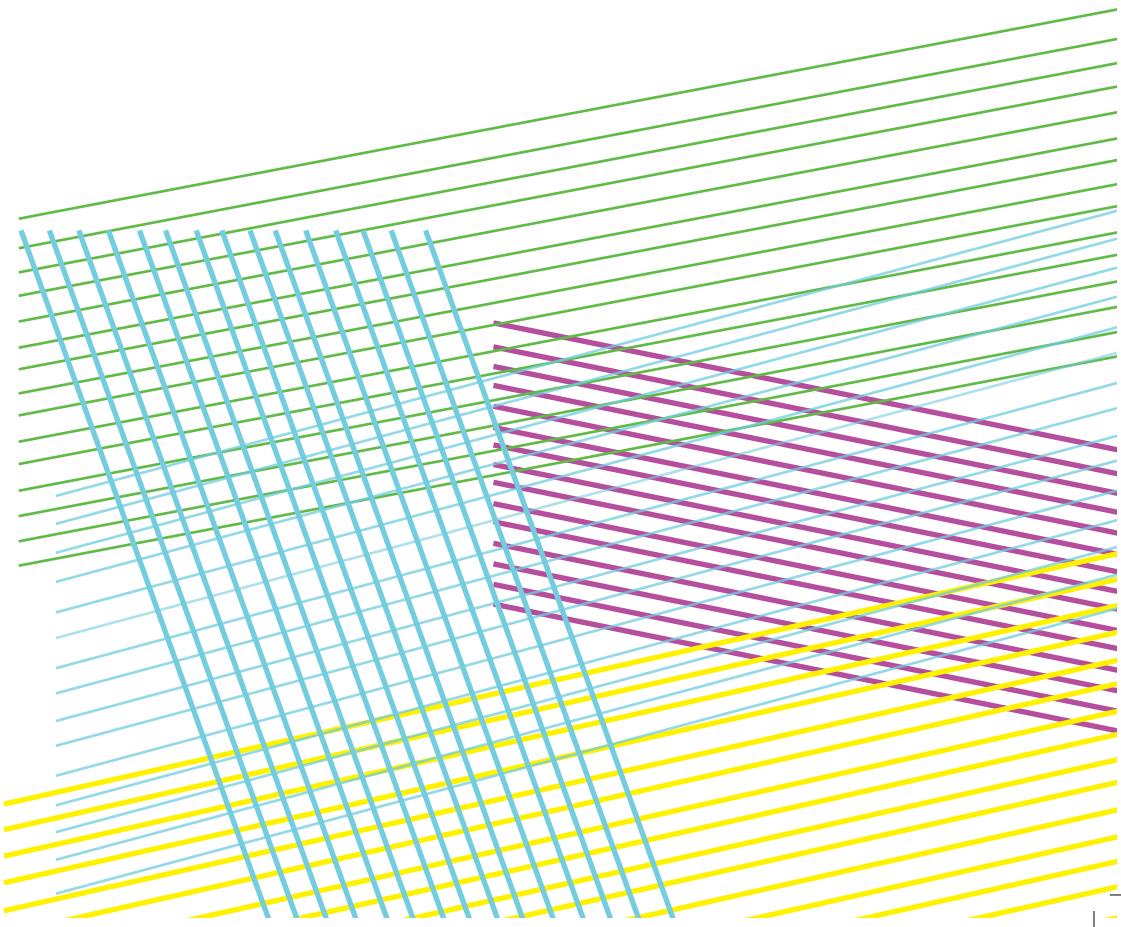
Bezpečnost v online prostředí

Roman Kohout / Mgr. Radek Karchňák

Biblio Karlovy Vary, z. s.

Bezpečnost v online prostředí

Roman Kohout / Mgr. Radek Karchňák



ISBN 978-80-260-9543-9

Autoři publikace

Roman Kohout (narozen v r. 1982)

studoval na Střední průmyslové škole v Ostrově, obor slaboproudá elektrotechnika. Od roku 2002 je příslušníkem Policie ČR, kde se specializuje na vyšetřování kybernetické trestné činnosti. Od roku 2013 se věnuje preventivní činnosti na základních a středních školách v Karlovarském kraji. V roce 2015 se stal lektorem nově vzniklého Světa záchranářů v Karlových Varech (www.svetzachranaru.cz), který vybudovala Asociace Záchranný kruh (www.zachranny-kruh.cz). Zde se podílel na vzniku preventivních programů pro veřejnost, které v tomto centru vyučuje především formou zážitkové pedagogiky. V rámci projektů dalších subjektů seznamuje děti i dospělé s riziky, které vznikají v kybernetickém prostředí.

Mgr. Radek Karchňák (narozen v r. 1969)

vystudoval na Filozofické fakultě Univerzity Karlovy obor pedagogika se zaměřením na sociální rozvoj a poradenství (1997). Na téže vysoké škole také studoval a státní závěrečnou zkouškou zakončil studia v oboru klinická psychologie (2002). V roce 2009 získal odbornou způsobilost pro klinickou psychologii. V témže roce ukončil pětiletý Rogersovský psychoterapeutický výcvik (person-centered therapy). Poté šestnáct let pracoval s mládeží jako psycholog v Pedagogicko-psychologické poradně v Karlových Varech. V roce 2015 začal provozovat privátní ambulanci klinické psychologie v Chebu, kde poskytuje poradenské služby osobám s psychosomatickým onemocněním, závislostmi na drogách a alkoholu. Spolupracuje s dalšími institucemi, realizuje přednáškovou činnost z oblasti klinické psychologie. Zabývá se řešením šikany ve školách v Karlovarském kraji.

Obsah

Vážení čtenáři,

do rukou se vám dostává brožura, jejímž úkolem je popsat a vysvětlit některá nebezpečí, s nimiž se kdokoli z nás může v online prostředí setkat. Mohl bych místo online prostředí užít slovo internet, to ale nevystihuje veškerý virtuální prostor, kde může ke kybernetické kriminalitě docházet.

Online prostředí však není jen internet a služby na něm provozované (Facebook, denní tisk, e-mail apod.). Kybernetický útok je totiž možné provést na moderní automobil, chytrý televizor, chytrou lednici, chytré hodinky, chytrý termostat ve vaší topné soustavě a další periferie, které budou zanedlouho propojeny tzv. Internetem věcí (IoT – Internet of Things). Na všechna zmíněná zařízení byl již úspěšný kybernetický útok proveden.

Nerad bych vás svými předchozími slovy vystrašil, či odradil od užívání moderních technologií. Naopak, člověk je tvor zvídavý, rád objevuje nové věci a právě touha po poznání společnost žene kupředu. Při každé cestě je ale třeba jistá míra obezřetnosti. Platí to rovněž při užívání si dobrodružství v online prostředí. I zde je třeba dodržovat několik zásad bezpečného chování a vypěstovat si do jisté míry schopnost vypozorovat možná nebezpečí a vyvarovat se jich.

Chtěl bych poděkovat panu Mgr. Radku Karchňákovi za jeho příspěvek na téma Psychické dopady kyberšikany, dále za rozbor tématu, který řeší a popisuje závislost na internetu, tzv. netholismus.

Snad vám tento vzdělávací materiál alespoň částečně pomůže blíže poznat online prostředí a pochopit význam bezpečného chování v něm. A také, že vám pomůže vyvarovat se možných rizik, se kterými se zde můžete setkat, či případně řešit již vzniklé problémy v kybernetickém světě.

Roman Kohout

Základní pravidla užívání počítače připojeného na internet

Základní pravidla užívání počítače připojeného na internet

Abychom mohli úspěšně čelit mnohým nástrahám v online prostředí, je třeba dodržovat několik hlavních zásad zabezpečení svého zařízení:

- **Aktualizovaný operační systém**
- **Aktualizovaný software**
- **Antivirový program**
- **Firewall**
- **Zabezpečený router**
- **Zálohování dat**

Operační systém

Každé zařízení (počítač, smartphone, smartwatch aj.) je vybaveno operačním systémem. Jde o základní program, který uživateli umožňuje zařízení ovládat, a to včetně dalších periferií k němu připojených. Jedná se o velice složitý software – program, který v sobě obsahuje nejen ovladače přidružených zařízení, ale dále například rozděluje systémové prostředky (výpočetní výkon procesoru, operační paměť apod.) mezi programy, které jsou spuštěny.

Mezi nejznámější operační systémy patří Windows, Mac OS, Linux, Android, iOS, Windows Mobile atd.

Útočníci (hackeři) často využívají chyb v operačním systému jakéhokoliv zařízení, proto je nutné operační systém udržovat aktualizovaný. Každý výrobce operačního systému pravidelně vydává aktualizace obsahující tzv. záplaty na zjištěné „díry“ – tedy opravy programového kódu operačního systému.

Software

Každý z nás užívá mnoho různorodých programů (softwaru), většinou specifických pro danou oblast práce. Internetové prohlížeče pro procházení webových stránek, grafické editory pro kreslení, kancelářské balíky apod. Každý z těchto programů se jako operační systém skládá ze statisíců řádků programového kódu (operační systém atakuje hranici několika miliónu řádků), v němž je rovněž veliký prostor pro případnou chybu.

Zejména internetové prohlížeče (Internet Explorer, Firefox, Chrome, Opera apod.), které mají nejblíže k útoku z prostředí internetu (podvržené webové stránky, webové aplikace spuštěné pomocí softwaru třetích stran atd.) je vysloveně nutné udržovat aktualizované jako operační systém. Výhodou je dokonalé ovládání používaného internetového prohlížeče. Můžeme tak často sami vypozorovat možný útok z prostředí internetu (například pharming, phishing apod.), a tím se mu včas vyhnout.

Antivirový program

V dnešní době je naprosto nemyslitelné užívat zařízení připojené na internet bez antivirového programu. Antivirový program je software sloužící k ochraně zařízení před viry a dalším malwarem, jejich detekováním, eliminaci jejich činností a úplným odstraněním ze zařízení. Antivirové programy škodlivé kódy detekují na základě svých databází a způsobu „chování“ programů nainstalovaných v zařízení. V dnešní době to antivirové programy nemají jednoduché, za účelem kvalitní ochrany zařízení vykonávají mnoho činností najednou - rezidentní štít, ochrana počítače proti počítačovým virům, virová truhla, kontrola e-mailů, rychlá ochrana proti virovým epidemiím, automatické aktualizace virových databází atd., a to vše s co možná nejnižšími systémovými nároky. Potřebujeme tedy ochranu na mnoha bojových frontách, nicméně nechceme, aby antivirový program jakkoliv „brzdil“ námi užívané zařízení.

Přitom podle statistik každý den vznikne více jak deset nových virů nebo jiného škodlivého kódu, na které je ze strany antivirového programu třeba reagovat. Z toho je více než jasné, že užívání neaktualizovaného antivirového programu je zcela bezpředmětné. **Nejznámější antivirové programy jsou** Avast, AVG, ESET NOD32 Antivirus, Norton Antivirus, McAfeeAntivirus, Kaspersky Antivirus atd..

Firewall

Firewall je program, který „dohlíží“ na datový tok mezi užívaným zařízením a vnější počítačovou sítí. Tento datový tok dokáže nejen kontrolovat, ale i regulovat, nebo dokonce závadový datový tok zastavit. Uživateli dává možnost kontroly tohoto datového toku a možnost regulovat jakýkoliv datový tok zvenčí.

V současné době je do nejrozšířenějšího operačního systému Microsoft Windows firewall integrován a mnoho uživatelů jej považuje za dostatečnou ochranu. Požaduje-li však některý uživatel podrobnější kontrolu, je třeba užít specializovaného firewallu. **Nejznámějšími firewally jsou** Comodo Firewall, ZoneAlarm, Privatefirewall apod. **Firewall je často s antivirovým programem součást balíku komplexní ochrany** od společností zabývající se bezpečnostními řešeními – ESET Smart Security, AVG Internet Security, Norton Internet Security, KasperskyLab apod.

Router

Router je zařízení, které propojuje dvě různé počítačové sítě a routuje (směruje) mezi nimi datový tok. Většina všech domácností je k internetu připojena právě skrze router. Proč ho ale zmiňuji? Právě nezabezpečený router je často prostředkem k neoprávněnému průniku do počítačové sítě (domácnosti, podniku) a následnému páchání trestné činnosti v dané počítačové síti, nebo je využit jako brána pro páchání trestné činnosti na internetu. Běžný uživatel zná router jako krabičku s anténkou, která mu doma vytvoří domácí WiFi síť, k níž vymyslí určitě neuhodnutelné heslo. Málokdo však tuto krabičku (router) otočí, aby zjistil, že přístup do administrace (nastavování) routeru je často opatřen heslem stejným jako uživatelským jménem – a to slovíčkem „admin“, jak je uvedeno na obrázku č. 1. Pro útočníka (hackera) není poté složité převzít kontrolu nad takovým routerem. Řešení je více než jednoduché: postačí ihned po zakoupení a zprovoznění nového routeru změnit heslo do jeho administrace.

Obrázek č. 1 – štítek nalepený na routeru s přihlašovacími údaji do administrace *(Zdroj: ee.co.uk)*

Zálohování dat

Zálohování dat je jednou z nejspolehlivějších metod ochrany důležitých dat před jejich ztrátou.

V době digitální fotografie, hudby, filmů a elektronických dokumentů je jejich ztráta citelná. O data nemusíme přijít pouze sofistikovaným kybernetickým útokem nebo virovou nákazou, ale lze o ně přijít triviálnějšími způsoby – postačí pouhé neúmyslné smazání nebo poškození harddisku počítače.

Zálohu můžeme provádět několika způsoby:

Na optická média (CD, DVD, Blu-ray)

Tento způsob je domácnostmi stále asi nejpoužívanější, avšak je třeba pamatovat na to, že i tato optická média se mohou po delším časovém úseku stát pro optické mechaniky nečitelná a v pravidelných intervalech je nutné pro následnou zálohu užívat vždy nový disk.

Externí pevné disky

Externí pevné disky nabízejí skvělý poměr kapacita/cena a jedná se o jednu z nejméně technicky náročných operací. Jako nevýhodu nutno podotknout možné mechanické poškození pevného disku nebo jeho konektivitu (způsob zapojení) v rámci delšího časového úseku do novějších počítačů.

NAS zařízení

Jedná se o síťové uložiště dat – externí pevný disk zapojený do domácí sítě – konektorem LAN nebo přes WiFi. Jeho správným nastavením lze zálohu dat nastavit v pravidelných intervalech automaticky. Další výhodou NAS zařízení je dostupnost pro další zařízení zapojené do domácí počítačové sítě – smart TV, tablety, mobilní telefony aj.

Cloudové uložiště

V poslední době se velkým hitem stala cloudová úložiště. Jedná se o datový prostor na serveru provozovatele cloudu, který je dostupný prakticky odkudkoliv a prakticky z kteréhokoliv zařízení (PC, tablet, mobilní telefon). Výhodou je okamžitá synchronizace dat mezi všemi připojenými zařízeními a možnost sdílení dat s dalšími uživateli. Nevýhodou je závislost na rychlosti připojení a také skutečnost, že uživatel svá data svěřuje ke správě „cizí“ společnosti. Nejznámější cloudová uložiště jsou Dropbox, OneDrive, Google Drive atd.

„Každý den vznikne více jak deset nových virů“…

Heslo

Heslo

Heslo je pro uživatele informačních a komunikačních technologií **prvotní a základní ochrannou hradbou** proti případným útočníkům, a proto je třeba heslu věnovat nemalou pozornost.

Vzhledem k tomu, že v dnešní době je na uživatele vytvářen tlak mít ke každé aplikaci a webové službě heslo, není pak prakticky v lidských silách zapamatovat si do každé takové služby jiné heslo. Často se pak stává, že uživatel rezignuje a u většiny webových **služeb užívá stejné heslo. Toto je však jedna z nejhrubších chyb**, které se uživatel může dopustit. Jednou ze zavedených praxí útočníků je prolomit a zjistit heslo u méně zabezpečených služeb a toto následně užít u těch lépe zabezpečených, např. zjistit heslo u diskusního fóra, kam se uživatel přihlásil a toto poté použít např. u sociální sítě Facebook. Má–li uživatel u obou služeb stejné heslo, je zřejmé, jaké to může mít následky. Vzhledem k tomu, že volba hesla je často podceňována, věnujeme heslu celou jednu kapitolu, ve které ukážeme **několik elegantních způsobů tvorby silného a lehce zapamatovatelného hesla**.

Co je to heslo?

Heslo je řetězec nesnadno zjistitelných a uhodnutelných znaků, který se užívá jako identifikační a ověřovací prvek.

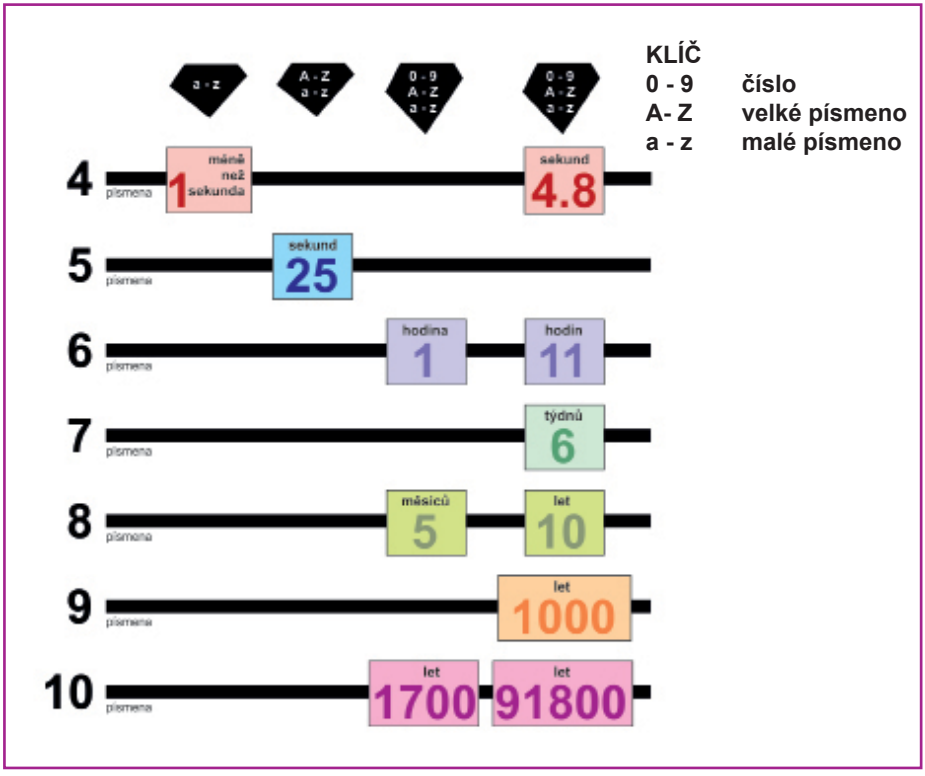
Společně s uživatelským jménem často tvoří základní ochranu k různým aplikacím, webovým službám, přístupu k počítačovým systémům, sítím apod.

Délka a vlastnosti hesla

Odborníci tvrdí, že bezpečné heslo by mělo mít minimálně 8 znaků, avšak v poslední době je trend doporučit heslo o délce **12 až 14 znaků**. K tomu odborníci dále doporučují minimálně kombinaci číslic, malých a velkých písmen. Dále je doporučeno doplnit heslo i o speciální znak. Je třeba se vyhnout snadno uhodnutelným heslům – běžná slova, jména blízkých osob, jména domácího mazlíčka, datum narození, běžným posloupnostem čísel (123456, 11111111 apod.) a očekávaným náhradám znaků – např. A → 4, O → 0, S → $, I → 1 apod.

Síla hesla

Pojem síly hesla si představíme na obrázku č. 2. V něm lze vyčíst časový údaj, za který se počítači se speciálním programem podaří takové heslo prolomit. Existuje mnoho programů specializovaných na prolomení hesla (passwordcrackery) užívajících různých metod prolomení – povětšinou kombinací těchto metod: slovníkový útok, brute-force, hybrid útoky, rainbow tabulky apod. Je třeba brát na zřetel, že výkon počítačů neustále stoupá a časy uvedené v tabulce se tím budou zkracovat. Rovněž i užití více počítačů použitých paralelně k prolomení hesla tuto dobu značně zkrátí.



Obrázek č. 2 – doba prolomení hesla v závislosti na počtu znaků a symbolů v heslu užitých. *(Zdroj: autor)*

Vytvoření hesla

Vytvořit tedy velmi silné heslo, ale lehce zapamatovatelné pro člověka, jsou naprosto protichůdné požadavky, avšak správným kompromisem lze bezesporu i toto splnit. Ukážeme si několik příkladů:

K tvorbě hesla si vymyslíme lehce zapamatovatelnou větu.

Můj pes má čtyři nohy a jeden ocas – MpM4Na1o

M	Můj
p	pes
M	Má
4	čtyři
N	Nohy
a	a
1	jeden
o	ocas

Jak se z lesa volá, tak se z lesa ozývá – Jszlv;Tszlo!

J	Jak
s	se
z	z
l	lesa
v	volá
;	čárku nahradíme středníkem
T	Tak
s	se
z	z
l	lesa
o	ozývá
!	doplníme za heslo navíc

Takto vytvořená hesla doplňme o zkratky služeb, ke kterým se přihlašujeme a získáme lehce zapamatovatelné heslo pro každou aplikaci nebo službu, ke které se přihlašujeme.

Tuto kapitolu jsem si dvakrát přečetl – Tkjs2xp

Tkjs2xp!Pc – přihlášení do počítače

Tkjs2xp!Fc– Facebook

Tkjs2xp!Ml – e-mailová schránka

Tkjs2xp!nakup – přihlášení do internetového obchodu

Původní heslo doplníme námi vymyšlenou zkratkou služby, ke které se přihlašujeme a toto oddělíme speciálním znakem, v tomto případě vykřičníkem.

Ochrana hesla

Své pracně vytvořené heslo je třeba dále ochraňovat – zejména tím, že jej nebudeme psát na papírek ležící u klávesnice, do poznámek v telefonu a hlavně jej nebudeme nikomu sdělovat.

V rámci ochrany svého hesla musíme také zvažovat, na jakém zařízení a při jakém připojení k internetu jej budeme k přihlášení zadávat. Měli bychom pamatovat na to, že pokud se takto budeme připojovat např. v internetové kavárně, mohou zde být počítače vybaveny monitorovacím programem – např. keyloggerem (program zaznamenávající každou stisknutou klávesu) – provozovatel takové internetové kavárny může získat obsah veškeré komunikace - tedy včetně hesla. Stejně tak může být vybaveno monitorovacím programem veřejné připojení k internetu, např. v nákupním centru (WiFi).

Program pro správu hesel

Pokud by pro někoho i výše uvedené sestavování hesel bylo příliš náročné, nebo užívá skutečně mnoho různých hesel, může užívat správce hesel. Jedná se o program s jednoduchým systémem. Uživatel si pamatuje pouze heslo do programu, všechna ostatní hesla jsou poté uložena ve správci hesel. Takto si uživatel může uložit ke každé službě jiné heslo a nemůžou tedy hrozit komplikace, pokud útočník prolomí jedno z uložených hesel. Správci hesel často obsahují generátor bezpečných hesel, hesla tedy nemusíme pracně vymýšlet.

Vygenerované heslo vypadá asi takto:

FjqPqaNEESfo.EWY2K1h7NFqV.R@bL

Mezi nejznámější správce hesel patří programy Keepass, 1Password, StickyPassword atd.

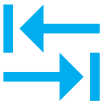
Nejhorší hesla

Nakonec si představme seznam nejhorších hesel pro rok 2015 dle společnosti SplashData (*www.splashdata.com*).

12456	master
password	**monkey**
12345678	letmein
qwerty	**login**
12345	princess
123456789	**qwertyuiop**
football	solo
1234	**batman**
1234567	**baseball**
welcome	**dragon**
123456890	1qaz2wsx
abc123	**111111**

Můj pes má čtyři nohy a jeden ocas – MpM4Na1o

Obecná nebezpečí na internetu



Spam

Co je spam?

Spam nebo také spamming lze nejjednodušeji vysvětlit jako zasílání nevyžádané elektronické pošty. Jedná se o masové rozesílání e-mailů s převážně reklamním sdělením, avšak s příchodem diskusních fór a různých messengerů spamming přechází i na tyto kanály. Nejedná se o cílené zasílání reklamního sdělení, ale o masové, dostane jej kdokoli.

Pokud není zařízení dostatečně chráněno, po napadení virem může i ono dále rozesílat spam bez uživatelova vědomí.

Značná část spamových e-mailů obsahuje malware – škodlivý kód, který může z počítače např. „krást“ osobní data.

Jak se chránit?

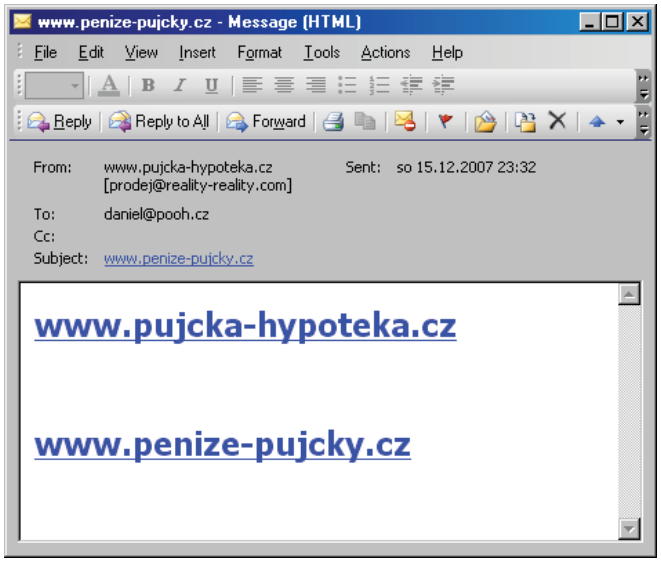
Zbytečně na internetu nezveřejňujte svou e-mailovou adresu. Pokud ji uvést musíte, uveďte ji v tomto formátu: jmeno(zavinac)domena.cz – **znak zavináče nahradíte slovem**. Program - robot, který po internetu sbírá e-mailové adresy za účelem rozesílat spam, takto napsanou adresu nevyhodnotí správně a přeskočí ji.

Nežli potvrdíte registraci v jakékoliv internetové službě, objednávku v internetovém obchodě nebo např. odsouhlasíte podmínky své věrnostní karty v kamenném obchodě, ujistěte se, že tím rovněž neodsouhlasíte zasílání reklamního sdělení. Po odsouhlasení by se o spam nejednalo.

Spamové zprávy neotevírejte. Pokud je možnost, nahlaste je a smažte. V žádném případě v takové zprávě nikdy neklikejte na žádný odkaz nebo tlačítko!

Pokud jste v minulosti např. nedopatřením odsouhlasili zasílání reklamního sdělení, na konci těchto zpráv bývá tlačítko „odhlásit“.

Příklad spamu



Obrázek č. 3 – příklad spamu *(Zdroj: www.pooh.cz)*

Čísla

V roce 2014 tvořil spam ze všech e-mailových zpráv poslaných po celém světě 66,76 %. Podíl spamu tedy pomalu klesá, jeho vrchol byl v roce 2009, a to 85,2 %.

Hoax

Co je to hoax?

Název hoax pochází ze stejného anglického slova, což v překladu znamená falešná zpráva, mystifikace, novinářská kachna, poplašná zpráva, výmysl, kanadský žert.

V elektronické komunikaci se význam tohoto slova nikterak nemění. Jedná se o poplašnou zprávu, která např. varuje před neexistujícím nebezpečím, před počítačovým virem, prosí o pomoc, anebo chce pouze pobavit. Často je ve zprávě kladen důraz na další přeposlání zprávy přátelům – řetězová zpráva. Většinou právě podle této žádosti o přeposlání lze hoax identifikovat.

Jaký je účel hoaxu?

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

Příklady hoaxu

„1. *Jakmile se ocitnete v situaci, že musíte pod nátlakem vybrat peníze z bankovního automatu na přinucení násilníkem, zadejte svůj PIN opačně. Automat vám peníze přesto vydá, ale též současně přivolá policii, která vám přijede na pomoc.*

2. Dávejte si pozor na své děti! Upozorňuji na případ, který se stal nedávno mé známé při nakupování v obch. domě IKEA. Rodiče šli nakupovat se svou desetiletou dcerou do obch. domu IKEA. Najednou zjistili, že dcera s nimi není. Chvíli čekali, jestli se neobjeví. Pak se rozhodli nechat ji vyhlásit. Obchodní dům hned uzavřel všechny východy a začal ji hledat. Holčička byla objevena na toaletě, ostříhaná a převlečená do jiných šatů. Asi to nebyl první případ, co se tam stal. Proto pozor při předvánočních nákupech!

3. Dobrý den, mohu vám říci, že Facebook oznámil, že od zítra se bude platit 12 eur za měsíc, musí se rozozaslať tato zpráva minimálně 15 svým kontaktům a stát vás označí přezdívkou „Gold", takže nemusíte platit. Pokud nevěříte, zkuste to sami. Zkopírovat a vložit, i když jsou spojené … to je vážné, informace pochází … od spolehlivého a důvěryhodného zdroje.

4. Malá holčička na obrázku má rakovinu mozku. Společnost AOL za každý odeslaný e-mail daruje 5 centů na její operaci. Prosím, pomozte."

Jak se hoaxu bránit? Je to jednoduché, jakmile usoudíme, že jde o hoax, zprávě nevěnujeme pozornost, ihned ji smažeme nebo v e-mailové schránce označíme jako spam. Hoax dále nepřeposíláme a případné přílohy neotevíráme.

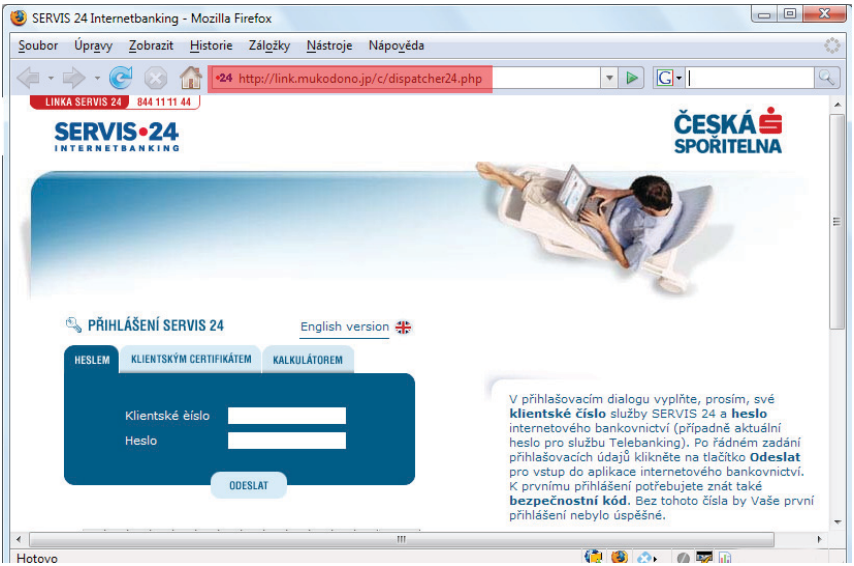
Podrobnosti i nejrozšířenější hoaxy najdete na www.hoax.cz.

Phishing

Co je Phishing?

Phishing je podvodná technika využívající informační a komunikační technologie k získávání citlivých údajů (přihlašovací údaje k různým webovým službám a aplikacím) hesel, čísel kreditních karet apod..

Princip celého podvodu spočívá ve velmi věrohodném napodobení žádosti např. z banky nebo obdobné instituce, upozornění od provozovatele e-mailové schránky nebo sociální sítě tak, aby uživatel byl „nucen" zadat své přihlašovací údaje. Tyto zprávy a žádosti jsou šířeny převážně e-mailem. Ten rovněž obsahuje odkaz, na nějž je nutné kliknout k následnému přihlášení. Po odkliknutí odkazu se však uživatel neocitá na webových stránkách instituce, která je v e-mailu uváděna, ale na podvržených webových stránkách útočníka, jenž je vytvořil prakticky k nerozeznání od webových stránek instituce uvedených v e-mailu. Zadáním přihlašovacích údajů do formuláře na takto podvržených webových stránkách je uživatel „předává" útočníkovi k dispozici a ten je poté využije ku svému prospěchu – ať se jedná o přihlašovací údaje k internetovému bankovnictví, e-mailové schránce nebo profilu na sociální síti. V poslední době se zprávy s phishingovým odkazem šíří přes sociální sítě. Často i zkušený uživatel může mít problém tento druh podvodu odhalit.



Obrázek č. 4 – příklad podvržené webové stránky banky Česká spořitelna. Dle webové adresy je zřejmé, že se nejedná o oficiální webové stránky České spořitelny, ale webové stránky podvržené útočníkem.
(Zdroj: www.maxiorel.cz)

Jak se phishingu bránit?

Banka, ani žádná podobná instituce vás nebude žádat o přihlášení, obnovu certifikátu, ověření nebo změnu přihlašovacích údajů prostřednictvím e-mailu! Ověřujte odesílatele, na vložené odkazy neklikejte a e-mail rovnou smažte.

Pokud nainstalujete program nebo aplikaci, která bude požadovat přihlášení například k vašemu profilu na sociální síti, buďte obezřetní. Zdáním přihlašovacích údajů je vydáváte třetí straně – možnému útočníkovi!

Při komunikaci s institucemi jako je například banka prostřednictvím webového rozhraní buďte obezřetní. Sledujte, zda jste na správné webové adrese a zda jste připojeni přes zabezpečené spojení.

Phishingové útoky vedené ze zahraničí lze rozeznat např. špatnou češtinou v textu e-mailu.

Pharming

Pharming je sofistikovanější a mnohem nebezpečnější formou phishingu. Jedná se rovněž o podvodnou techniku k získávání citlivých údajů uživatele. Princip však spočívá v napadení DNS serveru a přepsání IP adresy. DNS server překládá doménové jméno na IP adresu – podobně jako v telefonním seznamu je uloženo telefonní číslo pod jménem (vybereme jméno volaného a telefonní přístroj vytáčí telefonní číslo), DNS server překládá po zadání www.seznam.cz na IP adresu 77.75.72.3, což je IP adresa českého vyhledávače.

Uživatel tedy správně zadává www.seznam.cz, napadený DNS server však nepřeloží na správnou IP adresu, ale na webové stránky s IP adresou útočníka – v principu na pohled k nerozeznání od originálu.

V tomto případě ani zkušení uživatelé nemusejí včas podvodnou techniku rozeznat.

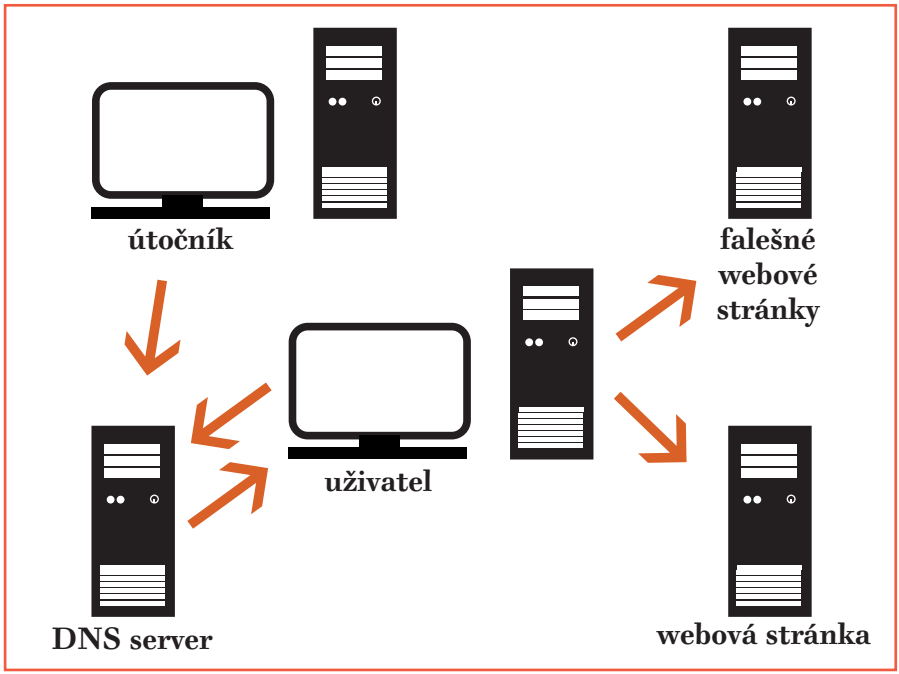
Druhá forma pharmingu je založena na útoku proti počítači uživatele. Počítače s operačním systémem Windows obsahují soubor Hosts. Ten funguje obdobně jako DNS servery – obsahuje doménová jména a k nim přiřazené IP adresy. Následný efekt je totožný jako u výše popsané formy.

Ochrana

Z výše uvedených informací je zřejmé, že pharming je mnohem nebezpečnější formou phishingu, protože dokáže oklamat i zkušenější uživatele. I zde ale existuje možnost bránit se.

U první popsané formy pharmingu nemá běžný uživatel mnoho prostředků k obraně, avšak DNS servery jsou jakousi „páteří internetu“ a jsou velice dobře zabezpečené. Zdolat ochranu nejlépe chráněných serverů internetu je velice obtížné i pro zkušeného útočníka a je velice nízká pravděpodobnost toho, že by došlo k útoku na DNS server, aniž by si toho správci všimli.

Z tohoto důvodu se útočníci uchylují spíše k druhé formě útoku. V tomto případě nelze doporučit nic jiného, než užívat kvalitní a pravidelně aktualizovaný antivirový program, firewall a internetový prohlížeč. Tato kombinace by měla ve většině případů jako ochrana proti pharmingu postačit.



Obrázek č. 5 – grafická ukázka pharmingu – napadení DNS serveru. *(Zdroj: autor)*

Malware

Slovo malware vzniklo složením anglických slov maliciousa software tedy škodlivý software. V češtině je někdy označováno jako počítačová havěť. Jedná se o počítačový program nebo jakýkoliv kus programového kódu vytvořeného za účelem napadení – vniknutí do systému (jeho infikování) za účelem jeho poškození, odcizení dat, sledování uživatele, apod.

Pod malware spadají počítačové viry, červi, trojské koně, spyware, adware, rootkity, keyloggery, dialery atd. Některé si blíže představíme.

Spyware

Je druh škodlivého kódu, který bez vědomí uživatele v systému, v němž je nainstalován, shromažďuje a odesílá data. V lepším případě shromažďuje data např. o navštívených webových stránkách za účelem lepšího cílení reklamy, v horším případě shromažďuje a odesílá třeba osobní data uživatele. Spyware sám sebe v drtivé většině případů nekopíruje, nepoškozuje uložená data, nepřesouvá, ani je nemaže.

Adware

Je škodlivý kód, který má během své činnosti za úkol zobrazovat reklamu v jakékoliv formě – vyskakující bannery, pop-up okna v internetovém prohlížeči nebo nepříjemnou a nežádoucí změnu domovské stránky v internetovém prohlížeči. Povětšinou není nikterak nebezpečný. Je spíše obtěžující a často je distribuován společně s jinými programy. Adware neshromažďuje informace a nikam je neodesílá. Se spywarem tak nemá prakticky nic společného, v některých případech může reklamu cílit na základě informací nashromážděných spywarem.

Rootkit

Rootkit je soubor nástrojů (programy a technologie), kterými lze maskovat činnost škodlivých kódů v systému. Maskování může probíhat skrýváním adresářů s malwarem, skrýváním klíčů v registrech, skrýváním běžících procesů, síťových spojení a dalších systémových služeb tak, že činnost škodlivého kódu je běžnými systémovými prostředky těžko odhalitelná.

Keylogger

Jedná se o škodlivý kód nainstalovaný v systému, jehož činnost je uživateli dokonale skryta a jeho úkolem je zaznamenat činnost uživatele zejména zaznamenáním každého stisku klávesy. Některé keyloggery jsou vybaveny funkcí „vyfocení“ aktuální pracovní plochy uživatele v daném časovém intervalu. Takto získané informace keylloger ukládá do předem nastaveného skrytého adresáře v uložišti systému nebo v nastaveném časovém intervalu (objemu zaznamenaných dat) odesílá útočníkovi.

Keyloggery se nejčastěji užívají za účelem odhalit hesla uživatelů, čísla platebních karet, čísla bankovních účtů, obsah korespondence a další citlivé údaje.

Někdy se keyloggery užívají jako legitimní monitorovací prostředek pro monitorování činnosti uživatele – např. kontrola dítěte rodiči.

Dialer

Dialer je škodlivý kód, jehož činnost spočívá v přesměrování standartní telefonní linky na linku s vysokým tarifem. Tento druh malwaru se užíval převážně v dobách tzv. vytáčeného internetu – v současné době, kdy roste tzv. trvalé připojení (ADSL, VDSK, WiFI, kabel apod.), je tento druh malwaru na ústupu.

Počítačový vir

Za počítačový vir je označován škodlivý program, který sám o sobě nemá schopnost šířit sám sebe bez vědomí uživatele systému. Tento škodlivý kód ke svému šíření využívá hostitele – jiné soubory, do kterých je vkládán (zkopírováním svého těla) a tyto využívá jako prostředek pro své další přenášení za účelem infikovat další systém. K tomuto šíření využívá zejména spustitelné soubory (EXE, COM, SYS atd.), různé dokumenty (DOC, XLS apod.) nebo funguje jako samospustitelná příloha e-mailové komunikace. V chování počítačového viru lze nalézt paralelu v chování viru biologického.

Cílem počítačového viru je zpravidla poškodit uživatele samotného, kupříkladu smazáním souborů bez vědomí uživatele. Klasický počítačový vir je v dnešní době na ústupu, je vytlačován sofistikovanějšími formami útoku na systém, neboť si s ním dokáže poradit prakticky každý antivirový program.

Trojské koně

Trojským koněm (Trojan) je označován škodlivý kód, který je ukryt v počítačovém programu a který se může na první pohled tvářit užitečně. Jde třeba o drobnou hru, spořič obrazovky, anebo právě program na odstranění malwaru. Často využívá legitimitu důvěryhodného zdroje – e-mailová zpráva s přílohou (v níž je trojský kůň) vytvářející domnění, že pochází např. od společnosti vyvíjející antivirové programy. Paralelu v názvu nacházíme v řecké mytologii o dobytí bájné Tróji, kde byl dřevěný kůň zdánlivým darem, avšak ve svých útrobách nesl řecké vojáky, kteří se později města Tróji zmocnili.

Stejné poslání má i Trojský kůň v počítačovém světě, protože jeho účelem je často získat moc nad systémem, kam byl propašován. Jde o získávání hesel, manipulaci se soubory uživatele, ovládání běžících systémů (vzdálené ovládání systému) apod. Na rozdíl od počítačového viru se zpravidla nesnaží o své „samošíření“.

Počítačoví červi

Počítačový červ (worm) je zvláštním druhem počítačového viru – škodlivý kód, který se replikuje do počítačových systémů prostřednictvím počítačových sítí. Jejich cíl je stejný jako u počítačových virů, avšak liší se formou jakou se šíří – narozdíl od virů se červi mohou šířit sami. Ke svému šíření využívají programových chyb systémů a dalších programů, které mají k systému přístup nebo mohou ovlivnit běh systému.

Ransomware

Ransomware je druh škodlivého kódu (malware), který v infikovaném systému zpravidla zašifruje sadu vybraných souborů a uživatel je následně vydírán zaplacením výkupného – cryptovirální vydírání. Ransomware se šíří jako červ nebo trojský kůň. Často je uživateli zpřístupněn podrobný návod k nápravě po uhrazení „poplatku". Útočníci užívající ransomware k vydírání jsou často natolik „drzí", že zřídí i uživatelskou podporu pro méně počítačově zdatné uživatele. Po uhrazení „výpalného" bývá zašifrovaná sada souborů opět zpřístupněna, není to však pravidlem.

Za zmínku stojí, že koncem října 2015 se k ransomwaru vyjádřila americká FBI, která uvedla, že s případy užití ransomwaru toho FBI moc nezmůže a radí výpalné platit, případně své klíčové dokumenty a soubory řádně zálohovat. Tento postoj však nesdílí společnost KasperskyLab vyvíjející stejnojmenný antivirový program, která v rámci svého boje proti počítačovým záškodníkům uvolnila již přes 14.000 klíčů pro dešifrování dat, která byla zašifrovány několika malwary typu ransomware.

Ubránit se ransomware z pozice běžného uživatele prakticky stojí pouze na pozornosti k přijímané e-mailové komunikaci, neboť právě ta je hlavním prostředkem šíření tohoto druhu malware – neotevírat přílohy e-mailů od neznámých odesílatelů.

Obrázek č. 4 – příklad ransomware - druh Win locker. *(Zdroj: www.awinit.cz)*

...narozdíl od virů se červi mohou šířit sami...

Sociální sítě

Sociální sítě

Sociální síť v rámci počítačového pojetí můžeme definovat jako online službu, která na základě registrace umožní vytvořit profil uživatele, pod kterým lze tuto službu využívat zejména ke komunikaci, sdílení informací, fotografií, videa atd. s dalšími registrovanými uživateli.

Mezi nejznámější sociální sítě patří Facebook, Google+, Twitter, Youtube, LinkedIn, Vkontakte, Instagram, Ask.fm aj.

Mezi nejznámější české sociální sítě patří Spoluzaci.cz, Lide.cz, Libimseti.cz apod.

Sociální sítě jsou v současné době velice často diskutovaným tématem. Jejich užívání sebou nese rizika a uživatelé dle názoru mnoha sociologů s možnostmi dnešních sociálních sítí v oblasti své bezpečnosti ještě neumí nakládat. Uživatelé zpravidla nečtou podmínky užívání sociálních služeb a v rámci této nevědomosti si nejsou vědomi, že např. osobní údaje zadané při registraci mohou být předávány třetím stranám. Stejně tak zmíněné sdílení informací – názorů, fotografií apod. nese svá rizika, pokud není profil uživatele dobře zabezpečen a ochráněn proti zneužití. Veškeré osobní údaje jsou cenným artiklem, se kterým se v rámci virtuálního světa velice čile obchoduje. V lepším případě jsou osobní údaje užity pouze k marketingovým účelům, v horším případě mohou být zneužity k páchání trestné činnosti.

Dnes je již např. běžnou praxí personálních oddělení různých společností případné zájemce o pracovní pozici „lustrovat“ skrze sociální sítě a na základě zjištěných údajů rozhodnout o přijetí či nepřijetí. Evidují se i případy, kdy pojišťovna odmítla pojistné plnění v rámci úrazového pojištění, neboť pojistník uvedl, že úraz mu znemožňuje pohyb, zatímco na svém profilu zveřejnil video, ve kterém je v danou dobu zaznamenán, jak se aktivně věnuje své oblíbené sportovní činnosti.

Několik zásad bezpečného užívání sociální sítě:

1. Nepoužívejte stejná hesla k více internetovým službám najednou.

2. Před každým potvrzením si vždy přečtěte veškeré podmínky.

3. Na profilech sociálních sítí nikdy neuvádějte své telefonní číslo, rodné číslo nebo adresu.

6. Svým přátelům přiřaďte různá práva (např. pro spolupracovníky jiná než pro rodinu).

7. Nenechte se označovat jinými uživateli na fotografiích (v nastavení soukromí nastavte vyšší úroveň kontroly).

8. Ignorujte neslušné zprávy a neodpovídejte na ně.

9. Pokud s někým nechcete komunikovat, nekomunikujte.

10. Na schůzku domluvenou přes internet nechoďte, aniž byste o tom řekli další osobě.

11. Nesdílejte své intimní fotografie, mohou být dále rozesílány.

12. Nesdílejte věci, které někdo může použít proti vám (například v pracovní době vložit komentář, že váš šéf nepatří mezi nejbystřejší apod.)

13. Nespojujte jiné webové služby s uživatelským účtem na Facebooku - například přihlášení do internetového obchodu pomocí FB účtu - nepředávejte své přihlašovací údaje třetí osobě.

Zajímavost

V dnešní době je podle statistických čísel nejrozšířenější sociální sítí Facebook.

Počet aktivních uživatelů
(v milionech září 2015)

Facebook	1550
Instagram	400
Twitter	316
Vkontakte	100
LinkedIn	97

(Zdroj: www.statista.com)

Počet denně aktivních uživatelů Facebooku
(v milionech prosinec 2015)

Q4/2011	483
Q4/2012	618
Q4/2013	757
Q4/2014	890
Q3/2015	1007

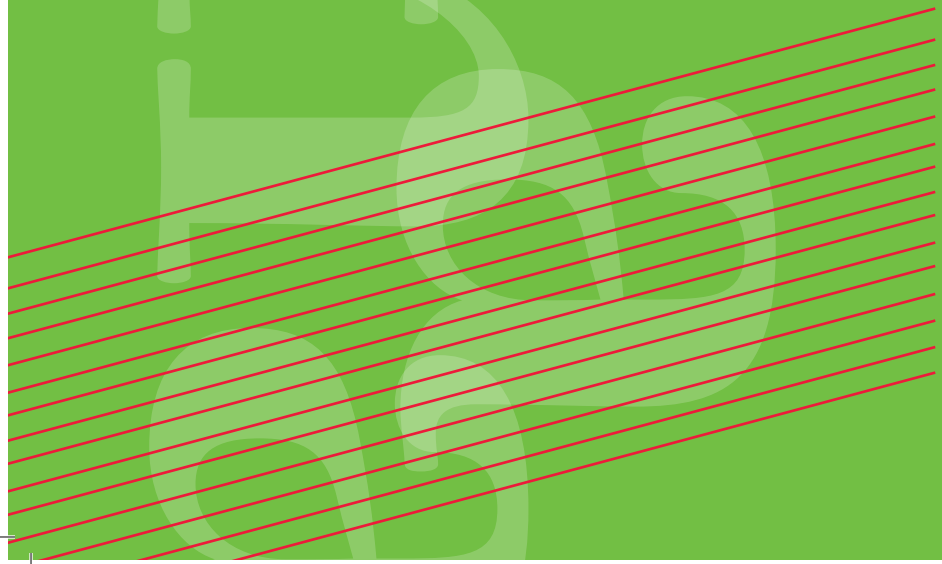
(Zdroj: www.statista.com)

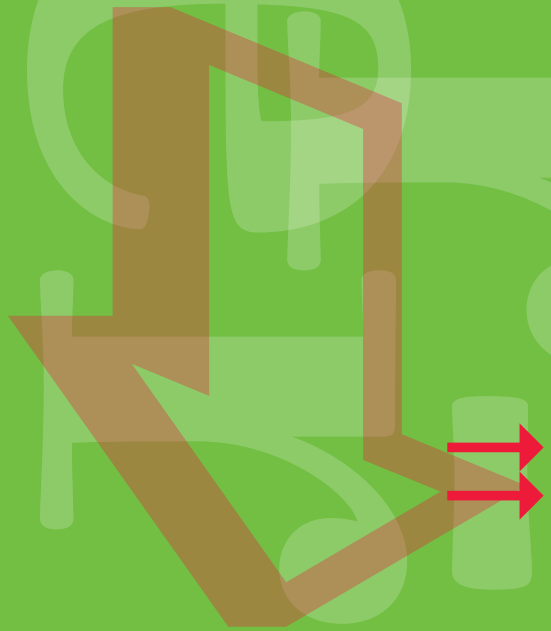
Čistý zisk společnosti Facebook za rok 2014 byl 2,94 miliardy amerických dolarů.

Dle odhadů v roce 2015 využívá sociální síť Facebook 4,2 milionu uživatelů v České republice. Vzhledem k aktuálnímu počtu obyvatel České republiky 10.546.120 (ČSÚ 30.9.2015) je to úctyhodné číslo. Pakliže lze z těchto hodnot usoudit vysokou oblíbenost tohoto virtuálního sociálního prostředí, je třeba mít na paměti, že tato čísla bohužel mohou rovněž vyjádřit velikost prostoru pro závadové, až trestné jednání některých osob užívajících toto virtuální prostředí.

Čistý zisk společnosti Facebook za rok 2014 byl 2,94 miliardy amerických dolarů.

Kyberšikana





Kyberšikana

Kyberšikana (kybernetická šikana, angl. cyberbullying) je druh šikany využívající informační a komunikační technologie (počítače, tablety, mobilní telefony, sociální sítě, e-maily apod.) k ublížení druhému (vydírání, ztrapňování, obtěžování, ohrožování, zastrašování apod.).

Cíl kyberšikany je tedy totožný jako u klasické šikany, avšak svými aspekty se liší několika rysy:

Anonymita

Útočník je často anonymní, vystupuje pod falešnými přezdívkami (nicky), vytváří jednoúčelové e-mailové schránky nebo falešné profily na sociálních sítích a díky tomuto pocitu anonymity je posílena jeho odvaha k použití agresivnější formy útoku. Z technologického hlediska je tato anonymita však pouze vzdušným zámkem, neboť odhalení takového útočníka dnes pro Policii ČR není velkým problémem. Problém nastává v hledisku právním, neboť kyberšikana není právně nijak vymezena a je-li právně kvalifikována jako přestupek, nemá za současného stavu policejní orgán příliš možností jak provozně lokalizační údaje vyžádat.

Profil útočníka

Ve virtuálním světě neplatí pravidla klasické šikany – nezáleží zde na věku, pohlaví, fyzické síle útočníka, sociálním postavení apod. Převládají převážně znalosti a dovednosti v užívání informačních a komunikačních technologií.

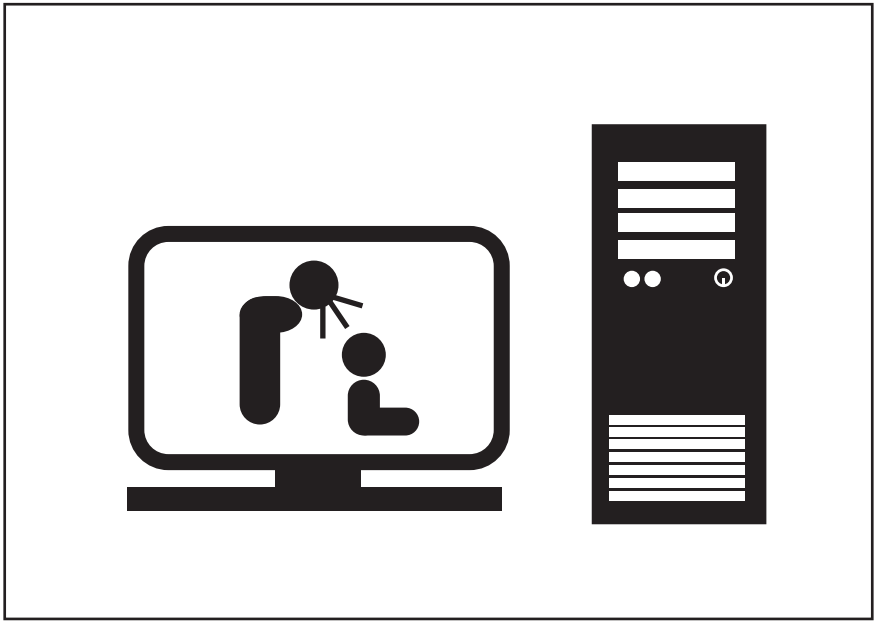
Místo a čas útoku nelze předpokládat – zatímco u klasické šikany lze předpokládat, kdy a kde k útoku dojde (o přestávce ve třídě, po vyučování před školou, v odpoledních hodinách na hřišti apod.), u kyberšikany útok může přijít kdykoliv a jakkoliv. Třeba o půlnoci prostřednictvím SMS, e-mailu, příspěvkem na sociální síti apod.

V šíření kyberšikany pomáhá útočníkovi „publikum“ – zejména možnost sdílení nebo následné přeposílání závadových příspěvků zvyšuje intenzitu vedeného útoku. Útočníkovi tedy postačí příspěvek publikovat pouze jednou, o jeho opakování a šíření se postará ono „publikum“. Jednání tohoto publika nepřímo, ale velice důrazně zvyšuje dopad na oběť.

Není snadné rozeznat dopad kyberšikany na oběť – vzhledem k tomu, že dopady kyberšikany jsou spíše v rovině psychické, je nesnadné je na oběti rozeznat nebo poznat oběť samotnou. Na rozdíl od klasické šikany u kyberšikany je o mnoho složitější vysledovat varovné signály – modřiny, potrhané a špinavé oblečení apod. Oběť se často uzavírá do sebe a přestává komunikovat s okolím, ať už ze strachu, že útočník zintenzivní své útoky, ze studu, nebo nepochopení problému rodiči nebo učiteli.

Kyberšikana může být způsobena i neúmyslně – zárodkem neúmyslné kyberšikany je povětšinou špatně odhadnutý dopad hloupého žertu.

Úmyslná kyberšikana je často spojena s klasickou šikanou.



Nejčastější projevy kyberšikany:

1. Rozesílání urážlivých a zastrašujících zpráv nebo pomluv (e-mail, SMS, instant messengery, Skype apod.).

2. Pořizování audio a video záznamů, fotografií, jejich následná úprava a zveřejnění s cílem poškodit oběť (předem připravený fyzický útok, natáčení spolužáka, učitele apod.).

3. Vytvoření webové stránky (facebookové stránky), která uráží, pomlouvá nebo ponižuje oběť.

4. Krádež identity (znamená prolomení zabezpečení e-mailové schránky nebo profilu na sociální síti vybrané osoby a následné vystupování útočníka pod identitou oběti.

5. Provokování a napadání uživatelů v diskuzních fórech (příp. trolling).

6. Odhalování cizích tajemství.

7. Vydírání pomocí informačních a komunikačních technologií.

8. Obtěžování a pronásledování pomocí informačních a komunikačních technologií.

Happy Slapping

Z anglického překladu „spokojené fackování". Jedná se o předem naplánované fyzické napadení nic netušící oběti, které je natáčeno na mobilní telefon nebo kameru. Záznam je poté zveřejněn na internetu, příp. dále šířen. Tento druh kyberšikany byl poprvé zaznamenán v jižní části Londýna v roce 2004. Název „Happy Slapping" byl poprvé užit v novinovém článku v roce 2005. Toto jednání bylo i ze strany společnosti chápáno jako nevhodný žert, útoky se však stávaly častějšími, jejich agresivita rostla a evidují se případy, kdy Happy Slapping skončil smrtí oběti. Aktéři útoku byli odsouzeni k několika letům vězení včetně komplice, který celou událost natáčel.

Happy Slapping se nevyhnul ani České republice. V roce 2005 Policie ČR pozatýkala členy gangu nazývaného Plameňák, kteří napadali náhodné osoby na ulicích, vše natáčeli a zveřejňovali na internetu.

Sexting

Slovo sexting je spojení slov sex a textování, a znamená posílání textového, fotografického, audio a video obsahu se sexuálním podtextem prostřednictvím informačních a komunikačních technologií.

Takový obsah, zasílaný převážně v rámci milostného vztahu, je zejména po jeho ukončení zneužit k poškození druhé strany jeho zveřejněním nebo k výhrůžce jeho zveřejnění.

Sexting, v němž figurují nezletilé a mladistvé osoby, může být z právního hlediska kvalifikován i jako trestný čin. Jedná se o velmi rizikové chování!

Rizika sextingu:

- Potencionální útočník obdrží citlivý materiál, který může v budoucnu zneužít.

- V případě zveřejnění citlivého materiálu na internetu je prakticky nemožné tento materiál „smazat“ – může být zneužit i po velice dlouhé době od zveřejnění.

- Trestní odpovědnost za šíření sextingu.

- Sexting se často stává prostředkem pro vydírání dětí v rámci tak zvaného kybergroomingu.

Kybergrooming

Kybergrooming je psychická manipulace prostřednictvím moderních komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít.

Kybergrooming se nejčastěji vyskytuje v rámci instant messengerů (Facebook messenger, ICQ, Skype), sociálních sítí (Facebook, Twitter, Badoo), internetových seznamek (libimseti.cz) a různých blogovacích stránek.

Obětí kybergroomingu se může stát prakticky kdokoliv, zpravidla se ale jedná o dívky ve věku 11-17 let, často užívající informační a komunikační technologie, trpící nedostatkem sebedůvěry, pocitem osamění. Jsou otevřené manipulaci a neznalé rizik internetové komunikace.

Kybergroomer je zpravidla sexuální útočník využívající informační a komunikační technologie k prosazení svého cíle. Často se vydávají za jinou osobu, než ve skutečnosti jsou, dle vybrané oběti. Pokud se snaží spřátelit se s 12 letou dívkou, vydává se za 15 letého chlapce. Významnou vlastností kybergroomera (není však pravidlem) je trpělivost – vydrží si s obětí i několik měsíců jen tak psát, aby získal pevně její důvěru.

Typický průběh kybergroomingu:

1. Vzbuzení důvěry a snaha izolovat oběť od okolí.
2. Podplácení dárky, penězi, budování přátelského vztahu.
3. Získání nebezpečných materiálů k vydírání.
4. Emocionální závislost na útočníkovi.
5. Osobní schůzka.
6. Sexuální obtěžování, zneužití.

Jak chránit své dítě v online prostředí?

Žijeme v době, kdy je užívání internetu dětmi prakticky nevyhnutelné a znalosti dětí v oblasti informačních a komunikačních technologií často převyšují znalosti jejich rodičů. Mnozí rodiče vzhledem k této skutečnosti na ochranu svých dětí v online prostředí prakticky rezignují. Nechají své děti v online prostředí bez dozoru. Naivita, důvěřivost, nekritické přejímaní informací a nedostatek životních zkušeností však mohou být důvodem, že se dítě stane obětí virtuálních predátorů. Z předchozích kapitol je více než zřejmé, že rizik v online prostředí je nepřeberné množství a že ochraně těch nejzranitelnějších je třeba věnovat mnohem více prostoru.

Jak se tedy stát zodpovědným rodičem?

Dítě ve svém rodiči spatřuje vzor, u rodiče hledá rady, pochopení, pomoc. Proto, aby se rodič dokázal stát silnou oporou pro své dítě, musí začít u sebe.

Vzdělávejte se

Svět informačních a komunikačních technologií je velice dynamické prostředí a k jeho pochopení je třeba se neustále zajímat o nové online služby a technologické novinky, které online služby dovolí užívat. Sebevzdělávání v této oblasti přinese větší nadhled nad nebezpečími, která dětem mohou hrozit.

Komunikujte

Pakliže vás dítě svými znalostmi v oblasti informačních a komunikačních technologií převyšuje, umožněte mu vás vzdělávat – vneste ho do role učitele a ponechte si roli žáka. Tímto jednoduchým trikem lze získat více, než nové zkušenosti. Kromě aktivní komunikace s dítětem získáte přehled o tom, jak dítě tráví čas na internetu a o co na internetu jeví zájem. Diskutujte o tom, jaké služby na internetu využívá a proč. Ptejte se i na rizika s užívanými službami spojená, poznáte, zda si je jich dítě vědomo.

Buďte i „virtuálním“ přítelem

V opravdovém světě chce mít většina rodičů přehled o tom, s kým se jeho dítě stýká. To už je potřeba i ve světě virtuálním.

Staňte se přítelem svého dítěte na sociálních sítích, které užívá. Získáte tím nejen přehled o jeho „virtuálních“ přátelích, ale i další zdroj informací o zálibách nebo momentálních náladách dítěte. Vysvětlete dítěti, co je nevhodné zveřejňovat na sociálních sítích a proč tomu tak je.

Užívejte internet společně

Vzdělávejte se společně a naučte se hledat kvalitní zdroje informací. Naučte děti, že ne vše, co je na internetu psáno, musí být pravdou!

Učte dítě, že i na internetu je nutné dodržovat pravidla slušného chování.

Vysvětlete, že nevhodným chováním na internetu se může stát i pachatelem trestného činu (např. sdílení obsahu chráněného autorským zákonem).

Zkuste společně hledat případy, kdy se dítě stalo obětí virtuálních predátorů. Diskutujte na tato témata a ujistěte se, že dítě rozumí pojmům jako je kyberšikana, sexting nebo kybergrooming.

Buďte oporou – ne vychovatelem

Na základě vzájemné dohody upřesněte pravidla užívání internetu – zejména čas jeho užíváním strávený.

Reagujte na případné nevhodné chování dítěte na internetu přiměřeně, aby nemělo zábrany v budoucnu s vámi o případných problémech hovořit.

Nezakazujte dítěti po špatné zkušenosti další užívaní internetu nebo jeho služeb. Začne před vámi svou opravdovou činnost skrývat. Rozumně prodiskutujte vzniklý problém a vysvětlete rizika.

Vysvětlete, že pokud se stanou obětí virtuálních predátorů, není to jejich chyba a není ostuda se s tím někomu svěřit.

V případě potřeby sami vyhledejte pomoc institucí uvedených v kapitole „Kam se obrátit“.

Upozorněte dítě, aby nikde na internetu nesdělovalo své osobní údaje - zejména:

- adresu bydliště a školy / věk (hlavně u mladších dětí)
- příjmení / rodinnou, finanční a vztahovou situaci
- přístupová hesla / rodné číslo
- číslo mobilního telefonu / osobní e-mail
- intimní fotografie, videa a informace
- nepřítomnost rodiny doma (dovolená apod.)

Upozorněte dítě na nebezpečná setkání

Vysvětlete, že je nebezpečné setkávat se s přáteli z internetu, které osobně neznají.

Kontrolujte!

Pravidelně kontrolujte historii navštívených webových stránek. Kontrolujte komunikaci – najdete-li závadovou komunikaci, zálohujte ji jako případný důkaz. Jedná-li se o závažnou závadovou komunikaci, kontaktujte Policii ČR a zálohu ponechte odborníkům.

Staňte se přítelem svého dítěte na sociálních sítích, které užívá.


Psychi
Psychi
dopadl
dopadl
kyberš
kyberš

Psychické dopady kyberšikany

Psychické dopady kyberšikany

Dnes si neumíme představit, že by moderní informační a komunikační technologie nebyla součástí našeho života. Hovoří se o tom, že nové technologie jsou pro nás důležité a jejich důležitost je podmíněná být tzv. online. Opak této aktivity, tj. být offline, by znamenalo pro mladého člověka sociální vyloučení.

David – Ferdonová a Feldman – Hertzová (in. Černá a kol., Grada, 2013, str. 14) popisují výhody být online následovně:

„Umožňují lidem komunikovat s lidmi z celého světa.

Přinášejí snadnější a pravidelnější spojení s rodinou - zvyšuje se prvek bezpečí a soudržnosti s jejími členy.

Představuje kompenzační prvek, jakmile dospívající mají problémy komunikovat tváří v tvář.

Podstatně rychleji získávají informace, které využívají při studiu, podnikání, výchově dětí, krizové pomoci atd.“

(in. Černá a kolektiv, Grada, 2013, strana 14)

Dospívající jedinci mají několik potřeb, které jsou propojeny s přítomností ICT technologie. Na internetu je možné se prezentovat, každý se může zviditelnit a očekávat i zpětnou vazbu směrem k vlastnímu chování atd. Svůj sebeobraz si vytváříme na základě reakcí okolí. V době dospívání je tento fenomén výrazně vystupňován. V adolescenci potřebujeme také experimentovat a komunikovat. Hledání vlastní identity je závislé na experimentování.

Bohužel být online má také negativní stránky. Především se lidé stávají pro širokou oblast lidí známí, kdokoliv si může o komkoliv zjistit citlivé údaje. U vybraných jedinců se v takovém případě stupňují formy chování, které můžeme nazvat online disinhibice. Volně přeloženo by se mohlo jednat o ztrátu zábran v komunikaci a prezentování.

Za inspirativní považujeme pochopení, proč na internetu dochází k disinhibovanému chování:

„1. Možnost skrýt svou identitu, díky čemuž se lidé cítí být méně zranitelní.

2. Lidé získávají odvahu dělat věci, které by jinak nedělali, protože je skrývá a chrání jejich anonymita.

3. Komunikace přes internet neprobíhá bezprostředně, jedinec má možnost obsah sdělení řádně promyslet.

4. Na základě toho, jak se partner projevuje, si vytváříme o něm obrázek. Hodnocení osobnosti zúžíme na fakt, jak dokáže písemnou formou komunikovat, ostatní aspekty hodnocení osobnosti potlačíme.

5. Člověk se vzdaluje od běžného reálného světa a dostává se na půdu světa imaginárního či virtuálního. V takovém případě si člověk uvědomuje, že nemusí za své jednání nést následky.

6. Na internetu nevíme, jaký statut zaujímá komunikační protějšek. Mizí tak zábrany a předsudky.

7. Můžeme pozorovat i v jiných prostředích než jen na internetu – třeba ve společnosti neznámých lidí, o nichž víme, že se s nimi už znovu nesetkáme. Mnohdy jsme v takové společnosti otevřenější a ochotnější hovořit i o intimních záležitostech. Máme větší tendenci k sebeodhalování. Internet je v lecčem podobný – poskytuje určitou anonymitu, svobodu a tím i půdu pro otevření se a sdílení.“
(Suler, in. Černá a kol., Grada, 2013, str. 16)

Konkrétní psychické dopady kyberšikany

Psychické dopady nemusí být nutně pouze u oběti kyberšikany, nýbrž mohou být i na straně agresora a přihlížející většiny taktéž.

Psychické dopady u oběti kyberšikany:

- **Poškozený sebeobraz:** jedinci mají tendenci se srovnávat neboli hodnotit vlastní osobu a porovnávat ji s jinými lidmi. Ti, kdo se stávají obětí kyberšikany, ztrácejí na své sociální aktivitě. Nepřímo tak dochází k jejich vyloučení ze skupiny. Jedinci se sníženým sebehodnocením se často izolují, vyhýbají se kontaktu s dalšími lidmi.

- U jedince se mění jeho totožnost, přijímá obraz toho druhého, nebo se jím alespoň hlouběji zaobírá, což přináší riziko zvýšeného psychického napětí. Nesoulad mezi obrazem a sebeobrazem je spouštěčem pro úzkostné a depresivní ladění.

- Přítomnost akcentovaných emotivních stavů jako např. vztek na sebe sama a na okolí, pocit bezradnosti, strach z opakovaného napadení, stud z odhalení, poukázání na nějakou oblast, která se stala posměškem pro ostatní, smutek jako reakce na ztrátu.

- Objevují se komplexní problémy v emotivní rovině jako např. výbuchy zlosti, kolísavá nálada, únik z reality ústící do stavů zvané derealizace a depersonalizace. Často bývá přítomen i strach o vlastní osobu, o vlastní bezpečí. Jedinci v takovém případě vykazují známky vyhýbavého chování.

- V behaviorální rovině se u těchto osob objevuje tendence k podezíravosti, sklon ke lžím, napadání a znevažování záměru druhých.

- **Sebevražedné tendence:** u obětí kyberšikany stejně tak jako u klasické formy šikany existuje riziko sebevražedných tendencí. Vybraní jedinci jakmile pociťují, že situace je bezvýchodná, začínají propadat beznaději a vykazují ve větší či menší míře sebevražedné úmysly.

- **Dopady kyberšikany na oběť**: pakliže se oběť vystavuje kyberšikaně, naučí se reagovat na tyto podněty. Mění své způsoby chování, vytváří se maladaptivní vzorce reagování. Naučené vzorce chování jako např. nízké sebevědomí, strach z opakování situací, obavy z odmítnutí, patří mezi přímé dopady kyberšikany na oběť. Odcizují se kolektivu, ztrácejí zájem o sociální dění, ochuzují kontakty s vrstevníky. Tím se snadno stávají středem zájmu agresorů, neboť působí jako sociální outsideři

na okraji sociální skupiny a ti mají vysokou pravděpodobnost být opět kyberšikanovaní.

Psychické dopady kyberšikany na agresory

Mohlo by se zdát, že u agresorů nedochází k žádným osobnostním změnám. Oproti obětem kyberšikany se nachází u agresorů zvýšená pravděpodobnost výskytu poruch chování.

„Jejich včasné neřešení může u řady agresorů vést k vystupňování obtíží vedoucí až k patologickému chování širšího pojetí např. zneužívání návykových látek, násilná trestná činnost.“
(Ybara, Mitchell, in. Černá a kol., Grada, 2013, str. 93)

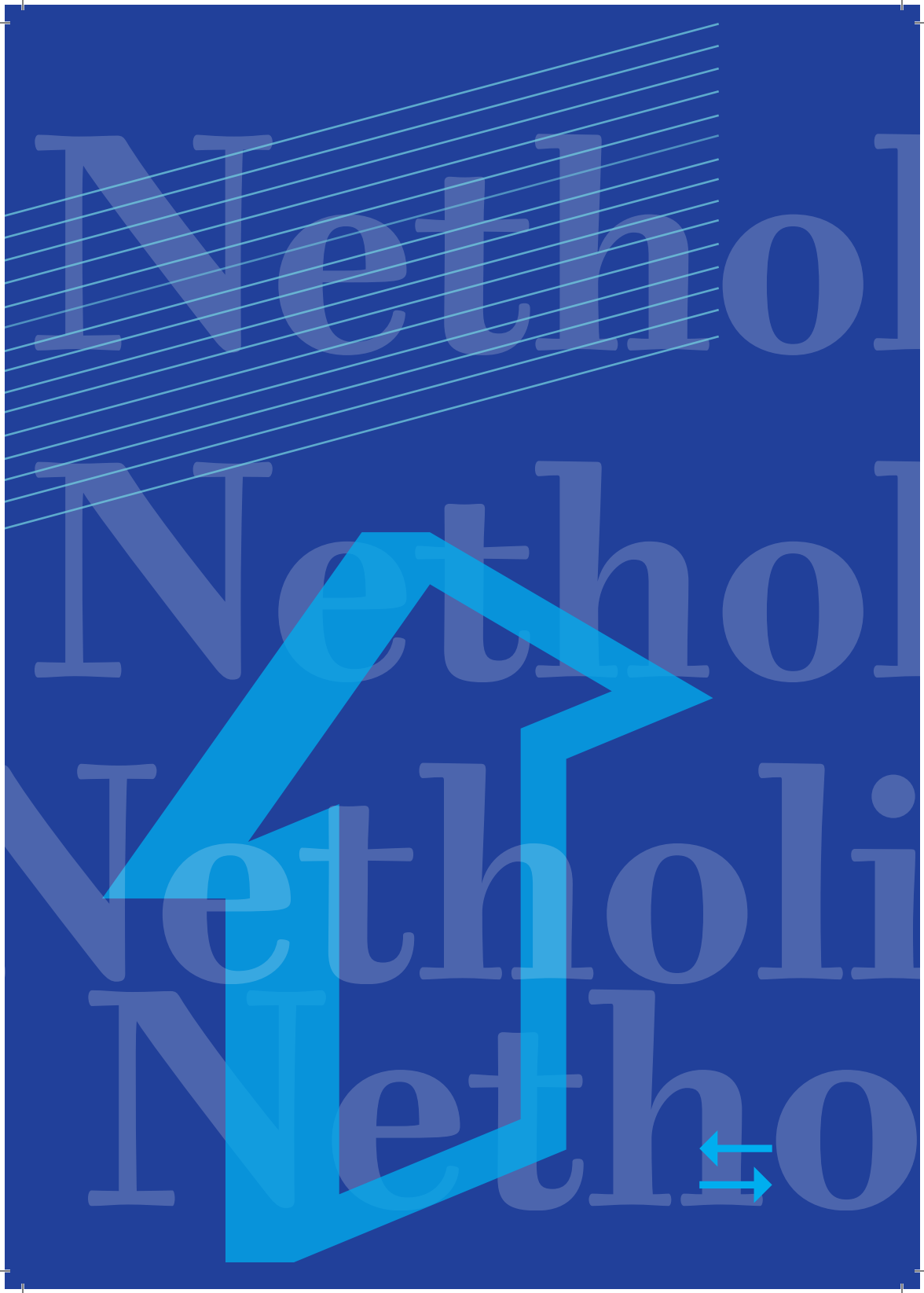
Dopady kyberšikany na skupinu přihlížejících

Sociální společnost po dobu kyberšikany oběti mlčí. Pouze přihlíží, co se v jejich okolí děje. Málokdo z nich si přizná svojí slabost a zároveň přání se současným stavem něco udělat. Převládne strach a obava ze zviditelnění a tím se vlastně i u nich objevují negativní formy prožívání jako je strach, emoční napětí, bezradnost. Jejich psychická reakce se velmi podobá reakcím obětí. Obětí kyberšikany se může stát každý ve skupině, proto tato hrozba padá na všechny zúčastněné.

Psychické dopady na přihlížející, kteří pomáhají agresorovi

V sociální skupině mohou být přítomny „nezdravé“ normy. V případě přihlížejících, kteří se rozhodnou pomoci agresorovi, to může znamenat posílení jejich pozice v sociální skupině a tudíž upevnění obrany proti případnému kyberšikanování sebe sama.

„Pro řadu přihlížejících se mohou přítomností ve skupině stát populární, více vyhledávané. Konečným důsledkem pak je jejich upevnění negativního chování.“
(Černá a kol., Grada 2013, str. 95)



Netholismus

Netholismus

Jedná se o moderní druh závislosti na virtuálních drogách. Co to může pro mladé lidi znamenat? Termínem netholismus označujeme závislost - závislostní chování (behaviorální závislost) či závislost na procesu na tzv. virtuálních drogách. Mezi ně patří zejména **počítačové hry, sociální sítě, internetové služby (různé formy chatu), televize** aj.

Znaky závislosti podle WHO:

1. Silná touha nebo pocit puzení užívat látku.

2. Potíže v kontrole užívání látky, a to pokud jde o začátek a ukončení nebo o množství látky.

3. Užívání látky k odstranění abstinenčních příznaků.

4. Průkazná tolerance (vyžadování vyšších dávek látky, aby se dosáhlo účinků původně vyvolaných nižšími dávkami).

5. Postupné zanedbávání jiných potěšení a zájmů ve prospěch užívané psychoaktivní látky a zvýšené množství času potřebného k získání nebo užívání látky.

6. Pokračování v užívní přes jasný důkaz zjevně škodlivých následků.

Nahradíme-li termín návyková látka termínem návykový proces (behaviorální závislost), můžeme snadno znaky závislosti vypozorovat i v samotném netholismu: Např. **silnou touhu zapnout počítač bez jasného cíle, zkontrolovat SMS, zkontrolovat statuty na sociální síti, neschopnost vymezit si začátek a konec aktivit na internetu, postupně zanedbávat další aktivity** atd.

Druhy netholismu:

- závislost na virtuální sexualitě
- závislost na virtuálních vztazích
- internetová kompulze (nutkání)
- závislost na PC
- přetížení informacemi

Mezi typické příznaky netholismu patří:

1. **Ztráta kontroly nad časem**
   Zvyšuje se tolerance, brzké vstávání či naopak ponocování z důvodu potřeby být online.

2. **Psychické projevy**
   Pocit prázdnoty, když člověk není u počítače či mobilu, rostoucí nervozita a neklid, když člověk nepoužívá počítač delší dobu, přemýšlení o počítači, když ho člověk zrovna nepoužívá, zatajování informací o závislosti, počítači/mobilu jako únik od osobních problémů atd…

3. **Psychosociální projevy**
   Narušení vztahů s rodinou, ztráta dřívějších přátel.

4. **Projevy spojené s prací**
   Méně vykonané práce, zanedbávání učení, zhoršující se prospěch.

(zdroj: www:Netolismus. cz)

Závislost na internetu lze léčit svépomocí, ale výsledek je často v nedohlednu. Účinnější formou je vyhledat odbornou pomoc, nejlépe tam, kde již mají zkušenost s léčbou závislosti na internetu.

⇉

...kam se obrátit...

Kontakty – kam se obrátit v případě potřeby

Policie České republiky - tel. 158, www.policie.cz

Poradna E-bezpečí - www.napisnam.cz

Národní centrum bezpečnějšího internetu - www.horkalinka.cz

Linka bezpečí - tel. 116 111

Rodičovská linka - tel. 840 111 234

Použitá literatura

Knihy:
ČERNÁ, Alena. Kyberšikana: průvodce novým fenoménem. Vyd. 1. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-210-6374-7.

Internetové zdroje:
Netolismus: průvodce online závislostmi [online]. Olomouc: Pedagogická fakulta Univerzity Palackého v Olomouci, c2015 [cit. 2016-03-01].

Dostupné z: https://www. netolismus.cz/

Policie České republiky [online]. c2015 [cit. 2016-03-01].

Dostupné z: https://www. policie.cz/

Wikipedia [online]. San Francisco: Wikimedia Foundation, Inc., c2016 [cit. 2016-03-01]. Dostupné z: https://www.wikipedia.org/

Securelist [online]. AO Kaspersky Lab., c2016 [cit. 2016-03-01]. Dostupné z: https://securelist.com/

Hoax [online]. Josef Džubák & HOAX.cz Code & design DIGITAL ACTION s.r.o., c2000-2016 [cit. 2016-03-01].

Dostupné z: https://www.hoax.cz/cze/

Viry [online]. Dvůr Králové nad Labem: Bc. Igor Hák, c2016 [cit. 2016-03-01].

Dostupné z: https://www.viry.cz/

Živě [online]. Praha: Mladá fronta a. s., c2007-2016 [cit. 2016-03-01].

Dostupné z: https://www.zive.cz/

Statista [online]. Hamburg: Statista GmbH, c2008-2016 [cit. 2016-03-01].

Dostupné z: https://www.statista.com/

Nebuď oběť! [online]. Ostrava: Rizika internetu a komunikačních technologií, z.s., c2010-2015 [cit. 2016-03-01].

Dostupné z: https://www.nebudobet.cz/

E-bezpečí [online]. Olomouc: Centrum PRVoK PdF, Univerzita Palackého v Olomouci, c2008-2015 [cit. 2016-03-01]. Dostupné z: https://www.e-bezpeci.cz/

Saferinternet.cz [online]. Praha: Národní centrum bezpečnějšího internetu, c2013 [cit. 2016-03-01]. Dostupné z: https://www.saferinternet.cz/

Brožura byla zpracována spolkem Biblio Karlovy Vary z. s. v rámci projektu s názvem Bezpečnost v online prostředí díky knihovnám (nejen) Karlovarského kraje.

Brožura byla vytvořena za podpory ČSOB Nadačního programu vzdělání.

Bezpečnost v online prostředí
Autoři: Roman Kohout, Mgr. Radek Karchňák
Vydal: Biblio Karlovy Vary z. s.
Tisk: Polypress
Grafická úprava: Mgr. Lucie Linhartová
Náklad 600 ks
Vydání: první
Karlovy Vary 2016, duben
ISBN 978-80-260-9543-9