STUDIJNÍ TEXT K PROJEKTU

MODERNÍ TRENDY VE VZDĚLÁVÁNÍ V PREGRADUÁLNÍ PŘÍPRAVĚ BUDOUCÍCH PEDAGOGICKÝCH PRACOVNÍKŮ NA UNIVERZITĚ PALACKÉHO V OLOMOUCI

E bezpečí

Jiří Novotný

Struktura sítě Internet

Internet je celosvětový systém počítačových sítí, které jsou vzájemně propojeny pomocí síťových uzlů. Pravidla komunikace mezi jednotlivými zařízeními v rámci celé sítě jsou stanovena rodinou protokolů TCP/IP. Připojení koncových uživatelů zprostředkovávají specializované firmy – poskytovatelé internetového připojení (ISP – Internet Service Provider), jež mají přístup do tzv. peeringových uzlů (IXP – Internet Exchange Point). Českým peeringovým uzlem je NIX.CZ.

Díky své struktuře je Internet systémem, který je decentralizovaný a jako celek nemá žádného majitele. Z toho důvodu je tedy velmi nepravděpodobné, že by někdy došlo k okamžitému ukončení jeho fungování, stejně jako pro potencionálního útočníka je nesmírně komplikované vyřadit Internet celkově z provozu. Dalším důsledkem hierarchie Internetu je nemožnost regulovat, příp. cenzurovat jeho obsah na celosvětové úrovni.

Každé zařízení v síti musí mít nějakou jednoznačnou identifikaci a ta je realizována IP adresou, která je v daný moment – s mírným zjednodušením - jednoznačná. V současnosti se používají dvě verze, starší IPv4 (např. 158.194.7.16) a novější IPv6 (např. 1001:718:1c01:16:214:22ff:fec9:ca5), ta se ovšem prosazuje jen velmi pozvolna.

Pro běžného uživatele je ale označování pomocí IP velmi nekomfortní kvůli její obtížné zapamatovatelnosti. Z toho důvodu se pro označování velké části počítačů používá systém DNS, který funguje na stejném principu jako seznam kontaktů v mobilním telefonu, kde ke konkrétnímu jménu osoby je přiřazeno odpovídající telefonní číslo. Systém DNS přiřazuje tzv. doménové jméno konkrétní IP adrese.

Tvorba doménových jmen podléhá přesně stanoveným pravidlům, kdy části domény jsou rozděleny do jednotlivých úrovní a jsou odděleny tečkou. Každá část domény musí být v dané struktuře jedinečná.

Příklad obvyklého tvaru domén, s nimiž přijde uživatel do styku: *portal.upol.cz*

- Poslední část v tomto názvu je doména první úrovně (TLD – Top Level Domain) a může být typu
    - národní TLD – dvoupísmenná, dá se z ní určit stát (.cz, .sk, .jp, .de),

  - generická TLD – víceznaková, obecné označení např. pro určitý typ zaměření, dat apod. (.com, .net, .biz, . aero., .museum, .bike, .beer),
  - infrastrukturní TLD – pro vnitřní potřeby Internetu (.arpa).
- Prostřední část je doména druhé úrovně a z jejího tvaru lze často odhadnout, kdo je majitelem dané domény nebo jaké informace daný server nabízí.
- Třetí část je doména třetí úrovně a její nejpoužívanější tvar je *www*, což označuje server nabízející stejnojmennou službu. Obecně na místě domény třetí úrovně ale může být jakýkoliv řetězec splňující pravidla pro tvar domény.
- Mohou existovat i domény vyšších úrovní, v praxi se však příliš často nevyskytují.

Porovnejme dvě domény velmi podobného tvaru - PUJCKY.CSOB.CZ a CSOB.PUJCKY.CZ. U té první se dá odhadnout, že spadá pod banku ČSOB a pravděpodobně se týká oblasti půjček u tohoto finančního ústavu. Doména druhá pod ČSOB zřejmě nespadá, možná pod nějakou firmu zabývající se finančním poradenstvím a tvar domény může být volen úmyslně tak, aby nezkušeného uživatele zmátl.

Pozn. Majitele domény druhé úrovně lze zjistit pomocí služby WHOIS. A konkrétně doména *pujcky.cz* patří firmě Elephant Orchestra, která se na vlastních webových stránkách prezentuje takto: *„Naše hlavní činnost je online lead generation. Jedná se o formu výkonnostního marketingu, kdy společnost jako Elephant Orchestra generuje pro své partnery kvalifikované kontakty (leady) na potenciální zákazníky. Jelikož naši partneři platí pouze za kontakty s jasně definovanými parametry, jedná se o jednu z nejefektivnějších a nejlépe měřitelných forem akvizice nových zákazníků.“* (www.elephant-orchestra.com/o-nas)

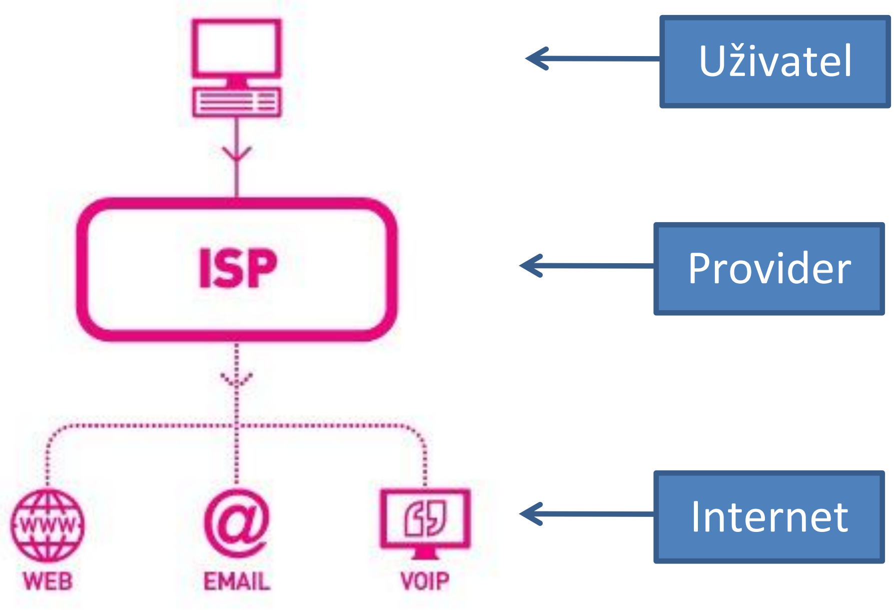
Anonymita uživatele na Internetu

Každé zařízení připojené v síti Internet je v dané chvíli jednoznačně označeno svou IP adresou a uživatel si svou IP adresu může zjistit např. na odkazu www.mojeip.cz. Ze znalosti IP adresy lze pak zjistit spoustu dalších souvisejících informací.

Nejpoužívanější službou dnešního Internetu je služba WWW, tedy procházení webových stránek. Při návštěvě každé webové stránky zanechá uživatel na dotyčném serveru určité informace, které jsou jeho správci/majiteli volně přístupné. Jedná se o:

1. IP adresa,
2. hostname,
3. stát,
4. operační systém zařízení, ze kterého si stránku prohlížím,
5. webový prohlížeč, kterým si stránku prohlížím,
6. nastavení monitoru (počet barev, rozlišení),
7. adresa předchozí navštívené stránky,
8. ISP – poskytovatel připojení k Internetu,
9. stav vypnutí/zapnutí javascriptu a cookies.

Znalost těchto dat umožňuje např. lépe cílit reklamu (podle státu lze navolit reklamu pro danou oblast), zjišťovat četnost a opakovanost návštěv dané IP, podle rozlišení monitoru lze optimalizovat zobrazení stránky pro dané zařízení, … Dle českého právního řádu má ISP povinnost archivovat po určitou dobu metadata (údaje o komunikaci, nikoliv o jejím vlastním obsahu) a na žádost pověřených orgánů jim je vydat. Důsledkem tohoto je stav, že činnost uživatele na Internetu je zpětně dohledatelná.



Když uživatel navštíví nějakou webovou stránku, její správce sice netuší, který konkrétní počítač to byl (zná jen jeho IP adresu), ale ví, přes kterého ISP se uživatel na zmíněnou stránku díval, tedy v obrázku výše zná jen zpětnou cestu Internet -> Provider. Navíc má k dispozici i přesný čas, kdy ke komunikaci se stránkou došlo.

Protože ISP monitoruje provoz ve své síti, naprosto přesně ví, že v daný čas konkrétní IP adresa byla přiřazena ke konkrétnímu uživateli, v obrázku výše zná zpětnou část Provider -> Uživatel. Tudíž pokud se obě dvě informace zmíněné výše spojí, je možné zpětně vysledovat činnost uživatele na Internetu. Nehledě na to, že tuto kompletní informaci má i samotný ISP.

Příklad. Ze stolního počítače s IP adresou 158.194.48.212 na některé učebně FTK bude student ve 13:00 komunikovat se serverem zajišťující internetové bankovnictví banky XYZ. Správce tohoto serveru má pak k dispozici informaci, jaký byl tvar IP adresy v daný čas a že daný počítač patří do sítě Univerzity Palackého. Pokud má podezření, že během této komunikace došlo k trestnému činu (např. pokus o hacknutí serveru), může kontaktovat Policii ČR, která si následně u správce univerzitní sítě vyžádá informace o dotyčné IP adrese a tak se určí naprosto přesně, o jaký počítač se fyzicky jednalo.

Z výše zmíněného zcela jasně vyplývá, že anonymita na Internetu jako taková vlastně neexistuje a pokud chce uživatel být více či méně anonymní, musí k tomu používat některé nástroje. Důvodem k maskování se nemusí být jen páchání trestné činnosti, ale i zcela legitimní důvody – zachování soukromí, obejití cenzury, ochrana před politickým pronásledováním v totalitních režimech, …

Mezi nástroje, které pomáhají k anonymnějšímu používání sítě Internet, například patří:

- správné zacházení s cookies,
- proxy server,
- web anonymizer,
- specializované aplikace, které běží na počítači uživatele (SafeIP, Pencil2D, program typu proxy switcher),
- aplikace JonDo,
- VPN – Virtual Privat Network,
- síť TOR a TOR Browser.

Digitální stopa

Na data, která zanecháváme po své činnosti na síti Internet, je nutno pohlížet jako na jednu velkou informační databázi. Protože když kupř. uživatel zveřejní na inzertním webu nějaký inzerát včetně své emailové adresy, pomocí stejné emailové adresy se registruje na e-shopu a tutéž adresu používá na svém FB profilu, je naprosto jasné, že se jedná stále o téhož člověka, byť zmíněné tři servery nemají společné vůbec nic.

Mezi obvyklé lidské vlastnosti patří i to, že spoustu věcí časem zapomeneme, ale databáze tuto vlastnost nemají a pokud informace v nich někdo nesmaže, přetrvávají v nich napořád. Nehledě na to, že bez nadsázky se dá říct, že data, která se jednou ocitnou na Internetu, už žijí svým vlastním životem a jejich původní autor už nemá nad nimi žádnou moc. Pokud zveřejníme na svém facebookovém profilu svoji fotografii a třeba hned druhý den ji smažeme, nemáme jistotu, zda v mezičase si někdo tuto fotku neuložil na svůj počítač, neposílá ji mailem dalším lidem, …

Digitální stopou se obecně míní data, která vznikají:

- jako výsledek činnosti při používání Internetu,
- jako součást souborů, které editujeme,
- používáním přístrojů z oblasti IT,
- vytvářením profilů na sociálních sítích a interakcemi na nich,
- zveřejněním svých osobních dat, fotografií apod.,
- vytvářením databází, registrů s veřejným přístupem.

Sledování digitální stopy standardního internetového uživatele není zrovna obtížným úkolem i pro víceméně laika a tato stopa může o sledované osobě vypovědět více, než možná sám tuší. Na stránkách archive.org lze třeba nalézt jednoduchý vyhledávač, který umí zobrazit konkrétní webovou stránku s obsahem ve vybraný den.

Z těchto důvodů je vhodné zvážit, jaká data o sobě na Internetu zanecháme a zda je opravdu nutné uveřejňovat na Facebooku kdejaký detail ze svého života včetně fotografií. Zaměstnavatelé dnes zcela běžně prověřují uchazeče o zaměstnání i pomocí sociálních sítí a porovnávají údaje na nich s daty uváděnými v našem životopise.

Používání webového prohlížeče v tzv. anonymním režimu napomáhá omezit digitální stopu, stejně jako pravidelné mazání cookies.

Sociální sítě

Sociální síť je služba internetu, která dovoluje svým uživatelům komunikovat mezi sebou, přičemž drtivá většina komunikace probíhá zveřejňováním/sdílením textů, fotografií či videosekvencí. Dovoluje také propojovat jednotlivé uživatele do různých subkomunit, např. podle jejich zájmů, typu zaměstnání, politických názorů… Sociálním sítě jsou naprostým fenoménem dnešní doby, odhaduje se, že je používá takřka polovina světové populace.

Mezi nejpopulárnější a tedy i nejrozšířenější sociální sítě dnes patří:

- Facebook,
- Instagram,
- Twitter,
- Google+,
- YouTube,
- Flicker,
- Pinterest,
- WhatsApp.

Prvním rizikem spojeným s touto internetovou službou je nutnost vytvořit si vlastní profil, v němž uživatel zadává některé své osobní údaje. Zde více než kde jinde platí pravidlo, že jakoukoliv informaci, kterou o sobě člověk na Internetu prozradí, už většinou nelze vzít zpět.

Dále pak je obsah sociálních sítí prohledáván různými podvodníky, kteří se díky posbíraným datům mohou snadněji vydávat za někoho zcela jiného, různé „roztomilé“ fotografie malých dětí hrajících si na pláži, které zveřejní jejich pyšní rodiče, mohou být vyhledávány pedofily, případného zloděje může inspirovat k návštěvě dočasně opuštěného domu svými majiteli jejich aktuální fotografie z dovolené v Egyptě umístěná na Instagramu.

Třetí skupinou negativ sociálních sítí je šíření polopravdivých či vyloženě lživých informací, tzv. hoaxů. Velká část uživatelů bezmyšlenkovitě sdílí tato data, aniž by si na nějakém dalším nezávislém zdroji ověřila, zda jsou vůbec pravdivá.

S nekritickým přebíráním určitého typu zpráv souvisí termín „sociální bublina“. Jedná se o jev, kdy člověk se díky svým názorům či postojům může zařadit do skupiny podobně smýšlejících lidí, a protože většina jeho komunikace probíhá výlučně s těmito lidmi, utvrzuje se ve falešném přesvědčení, že pouze tyto názory jsou správné.

Sociální sítě mohou být využívány také ke kyberšikaně, vydírání, zakládání falešných profilů, kde je uveřejňován takový typ informací, které skutečnou osobu poškozují (kyberšikana).

Není žádným tajemstvím, že provozovatelé sociálních sítí mají k dispozici obrovské množství informací. Ty jim na sebe prozradí buď uživatelé přímo nebo zprostředkovaně díky sdílení určitých typů dat, lajkováním typických příspěvků, příslušností k určité skupině, … Je evidentní, že když uživatel XY bude členem několika facebookových skupin, které se obsahově týkají fotbalu, dá se odhadnout, že jej tento sport patrně zajímá. A pokud tatáž osoba bude hojně lajkovat příspěvky na oficiální FB profilu fakulty tělesné kultury UP či rovnou psát nějaké komentáře, opět se dá odhadnout, že uživatel XY na stejné fakultě i studuje a možná je i aktivním fotbalistou.

A k čemu se dá takové kvantum dat využít? Cílená reklama!

Poslední nebezpečí, které provází používání sociálních sítí, je instalace aplikací třetích stran, které jsou na nich k dispozici. Zde je vždy dobré vědět, jaká povolení pro přístup do vašich dat daná aplikace vyžaduje či jaké jsou podmínky pro používání služby s ohledem na zpracování osobních dat.

Sociální inženýrství

Sociální inženýrství je cílená manipulace s lidmi pomocí zkreslených či nepravdivých informací za účelem provedení určité akce nebo získání nějaké informace, které se ve svém konečném důsledku obrátí proti zmanipulované osobě.

Důvod úspěšnosti sociotechniků vystihuje citát připisovaný Albertu Einsteinovi: *„Pouze dvě věci na světě jsou nekonečné, Vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist“*.

Útočníci používající sociální inženýrství spoléhají na chybu lidského faktoru, na hloupost lidí, na jejich neinformovanost, naivitu či důvěřivost. Proč pracně zjišťovat přístupové heslo do informačního systému tím, že útočník bude hledat případnou chybu v příslušném software, když mnohem jednodušší je šikovným trikem hesla z uživatelů vylákat přímo?

Příklad takového pokusného útoku byl před časem popsán na serveru latrine.cz (https://www.latrine.cz/jak-zjistit-heslo-na-seznam-e-mail):

Jak zjistit heslo na Seznam E-mail

Tento fígl jsem objevil náhodou, když jsem sledoval při práci admina ze Seznamu. Je to prosté: na server zašle požadavek (speciální e-mail), ten jej vyhodnotí a pošle zpět odpověď. Administrátoři Seznamu to používají při práci „v terénu“. Teď prozradím přesný tvar e-mailu, kterým lze získat heslo k jakékoliv schránce na Seznam E-mail.

E-mail je třeba odeslat na adresu *get.password@seznam.cz*. Jako předmět se musí uvést *L4_Tr1N3*. Zpráva musí být přesně v tomto formátu:

$src:adresa@seznam.cz (tedy adresa, k níž chcete znát heslo)

auth:vase_adresa@seznam.cz (vaše adresa, na ni bude zasláno heslo)

##auth:vase_heslo (a heslo pro ověření vaší totožnosti)

Pozor, je nutné mít schránku na Seznamu, aby server mohl ověřit přihlašovací údaje!

Tedy pokud chcete zjistit heslo ke schránce *petr.nozicka@seznam.cz* a sami máte e-mail *franta@seznam.cz* s heslem *12345*, pak odešlete zprávu ve znění

$src:petr.nozicka@seznam.cz

auth:franta@seznam.cz

##auth:12345

Nezapomeňte na předmět ve správném tvaru. Obratem přijde zpět e-mail s heslem ke schránce.

Na první pohled se zdá, že máme k dispozici jednoduchý návod, jak zjišťovat hesla těch, kteří si zřídili emailovou schránku na Seznamu. Ve skutečnosti – pokud bychom podle tohoto návodu postupovali – jsme prozradili svoje přihlašovací údaje (řádek *auth* a řádek *##auth*) někomu, kdo si zřídil email ve tvaru get.password@seznam.cz. A onou osobou může být kdokoliv, třeba soused v lavici, stačí jen, aby výše zmíněný tvar emailu byl volný.

Masové komunikační prostředky sice nejsou nezbytnou podmínkou pro úspěšně vedený útok sociotechnika, ale s jejich pomocí je mnohokrát vytvoření falešné iluze snadnější a dokonalejší. V reálném světě se lze jen velmi těžko vydávat za prezidenta naší republiky, pomocí mailu nebo telefonu je úspěšnost dobře provedeného útoku mnohem pravděpodobnější.

Vlastnosti, které se v sociálním inženýrství využívají:

- Autorita – tendence podřídit se osobě s vyšší funkcí/mocí.
- Sympatie – člověk snáz uvěří někomu, kdo je nám sympatický.
- Důslednost – lidé mají tendenci se podřídit, pokud veřejně vyjádřili podporu.
- Společenský souhlas – např. „Ten dotazník už všichni ve firmě vyplnili“.
- Využití vzácné příležitosti – „Prvních sto zaregistrovaných má slevu“, „Pokud podepíšete smlouvu na místě, nemusíte platit administrativní poplatky“.

Metody:

- Stres, vyvolání pocitu nebezpečí – vytvoření nátlaku na oběť, aby si nemohla v klidu promyslet či prokonzultovat daný problém.
- Důvěryhodná činnost – útočník se na rozdíl od předchozího snaží oběť naopak ukonejšit a koná tak, aby si nebyla vědoma nějakého ohrožení.
- Lákavá činnost – útok je veden tak, že oběť se domnívá, že se k ní dostanou nějaká zajímavá data.
- Vydávání se za někoho známého – zvlášť v kybernetickém světě relativně snadné.

Nejrozšířenější konkrétní metody sociálního inženýrství ve spojitosti s IT jsou:

- **Trashing** – procházení domovního odpadu a hledání cenných informací v něm (bankovní výpisy, výpisy telefonních účtů).
- **Phishing** – přesměrování na falešné webové stránky, které jsou vizuálně velmi podobně těm originálním. Přesměrování se děje nejčastěji pomocí podvrženého odkazu v těle mailu, který vypadá, že byl odeslán např. z banky. U odkazu se sice na první pohled zdá, že vede na stránku organizace, která mail jakoby zaslala, ve skutečnosti ale směřuje na počítač, který má ve své správě útočník. Pokud případná oběť zde zadá přihlašovací údaje, prozradí je tím pádem útočníkovi.

- **Pharming** – podobný jako phishing, ale mnohem nebezpečnější a zákeřnější. Opět se jedná o přesměrování na podvodné stránky, a pokud na nich uživatel zadá přihlašovací údaje, zná je pak i útočník. Přesměrování se v tomto případě děje tak, že ke správnému doménovému jménu je přiřazená nesprávná IP adresa, která ovšem označuje počítač útočníka. Přepsání IP adresy je uskutečněno buď napadením DNS (dosti komplikované) nebo útokem na konkrétní počítač, telefon.
- **Tabnabbing** – přepsání webové stránky poté, co byla ponechána nějakou dobu bez povšimnutí, často se využívá záložek prohlížeče.
- **Evil Twin** – vytvoření falešné bezdrátové sítě, která vypadá jako nějaká veřejná síť, např. svým pojmenováním. Útočník se pak snaží zachytit důvěrné informace.
- **Smishing** – princip podobný jako u phishingu, oběť je oklamána pomocí falešné SMS s telefonním číslem, které sice vypadá, že patří např. bance, ale ve skutečnosti jej používá útočník.
- **SCAM 419 (Nigerijské dopisy)** – typ podvodu, kdy je oběti přislíbeno, že se může dostat k vysoké finanční částce, k lukrativnímu zaměstnání nebo třeba vyhrát v loterii. Ke slibované transakci však nikdy nedojde, ba naopak oběť je z různých vymyšlených důvodů neustále žádána a zaplacení dalších a dalších relativně nízkých poplatků. Navíc autor podvodu je zpětně jen velmi těžko dohledatelný, takže i při oznámení podvodu na policii je jen velmi malá pravděpodobnost, že se oběť se svými penězmi někdy shledá. Varianty jsou:
    - převod peněz z bankovního konta po zemřelém bohatém člověku,
    - podvody se zaměstnáním,
    - podvody se zvířecími mazlíčky,
    - loterijní podvody,
    - online aukce a prodeje,
    - láska před internet.

Příklad podvodu SCAM 419 (http://www.policie.cz/clanek/chtela-byt-fiktivni-dedickou-a-prisla-o-617-571-korun.aspx):

Mladá žena z Jindřichova Hradce chtěla rychle zbohatnout bez jakékoliv vynaloženého úsilí a práce. Místo „ zaručeného dědictví“ však přišla prostřednictvím internetu o celoživotní úspory. Fiktivní zpráva, kterou emailem obdržela zněla velmi lákavě.

V měsíci květnu roku 2009 odeslal dosud neznámý pachatel ze svého e-mailového účtu patchanprivacy004@yahoo.com pošk. zprávu, ve které se představil jako Patrik Chan a uvedl, že je zaměstnancem banky v Hongkongu, měl bohatého klienta Musa Omara Numana, který před šesti lety zemřel v Iráku při výbuchu bomby a na jeho účtu, vedeném právě u banky v Hongkongu, u které je Patrik Chan zaměstnán po něm zůstala finanční částka 22.500.000,-USD. Vzhledem k tomu, že se bance nepodařilo zjistit žádnou osobu v příbuzenském vztahu k zemřelému Musa Omarovi Numarovi, požádal Patrik Chan poškozenou , zda by se nevydávala za jeho příbuznou, Patrik Chan by vyřídil veškeré formality s tím spojené včetně dědického řízení, zajistil by převedení výše uvedených finančních prostředků na účet a ona mu následně zašle 70 % z této částky. Poté odkázal poškozenou na osobu Pietera Rodolfa, který dle jeho tvrzení pracuje v bankovním ústavu v Nizozemí a tento jí zajistí založení účtu u této banky , který je nutný pro převod peněz.

Mladá žena zřejmě pod vidinou „ závratného zisku“ ztratila racionální uvažování a kontaktovala prostřednictvím e-mailu Pietera Rodolfa, který jí následně založil fiktivní účet u neexistující banky v Nizozemí a prostřednictvím za tímto účelem úmyslně založených webových stránek navodil v poškozené dojem, že má skutečně zřízen účet u banky v Nizozemí a prostřednictvím webové aplikace internet banking komunikuje s tímto účtem on-line.

Dále pod různými záminkami jako zřízení účtu v Nizozemí , jeho změna pro přijetí tak vysoké částky a podobně vylákal celkem na ziskuchtivé poškozené celkem 3.900 USD. A rozehrání šachové partie neznámého pachatele pokračovalo. E-mailem se ozval Patrik Chan, který mladé ženě sdělil, že zahájil převod výše uvedené částky 22.500.000 USD z banky v Hongkongu na tento její nově zřízený účet v Nizozemí. Poškozená si poté ověřila na tomto svém fiktivním účtu, že na něj byla částka skutečně připsána a P. Rodolf, který vystupoval jako zaměstnanec Post Bank jí následně sdělil, že pro převod takto vysoké částky do jiné banky, musí poškozená uhradit tzv. osvobození od daně ve výši 29.250 USD, což žena učinila a peníze dne 31. července 2009 odeslala na účet uvedený P. Rodolfem. Zhruba za tři týdny jí přišla od P. Rodolfa zpráva, že peníze byly v pořádku připsány na účet a byl jí zaslán číselný kód, který měla poškozená zadat do svého účtu u banky v Nizozemí a poté měla dát příkaz k převodu výše uvedené částky na její účet v České republice. To učinila, zadala číselný kód do svého fiktivního účtu, avšak následně byla webovou aplikací vyzvána k zadání dalšího číselného kódu. Poškozená se tedy obrátila opět na P. Rodolfa, který jí sdělil, že si musí zaplatit tzv. antiteroristický kód, neboť tento je nutný pro převod tak velké finanční částky do jiné banky. Za tento kód požadoval po poškozené finanční částku ve výši 49.550.60 USD, avšak tyto peníze již neodeslala.
Celkem tak žena z Jindřichova Hradce přišla o 617. 571 korun.

Ochrana proti sociálnímu inženýrství:

- ZDRAVÝ ROZUM, informovanost, opatrnost.
- Zabezpečený počítač proti napadení (antivir, antispyware, firewall).
- Pro běžnou práci používat počítač v neadministrátorském režimu.

- Při instalaci software na chytrý telefon si zkontrolovat, do jakých částí systému vyžaduje aplikace povolení k přístupu.
- S institucemi komunikovat jen přes oficiální kontakty.
- Nenavštěvovat podezřelé webové stránky.
- Instalovat jen legální software pořízený z legálních zdrojů.

Hesla

Heslem se v oblasti IT rozumí obvykle řetězec několika znaků, kterým se ověřuje identita uživatele. Podobnou funkci jako heslo může zastávat např. domluvený signál, gesto, sken oční sítnice nebo analýza hlasu.

Základní pravidla pro nakládání s hesly:

- Nikomu neprozrazovat. V případě, že se vyskytnula ojedinělá situace, kdy uživatel heslo úmyslně sdělil jiné osobě, je nutné jej při nejbližší příležitosti změnit.
- Nikam nezapisovat, protože hrozí nebezpečí snadného prozrazení (nalezení papíru s hesly, při opisování někdo uvidí poznamenané řetězce). Ukládání papírku s napsaným PINem do peněženky hned vedle bankovní karty je taktéž velmi rizikové.
- Při zadávání hesla na veřejných místech je dobrý být obezřetný a sledovat okolí. Může se stát, že nedaleko stojící osoba bude sledovat naši činnost a může vidět, které klávesy stiskneme. Navíc v dnešní době, kdy jsou kamery takřka na každém kroku, se může lehce stát, že někdo nasnímá pohyb prstů nad klávesnicí.
- Po určité době heslo změnit. Čím cennější data heslo chrání, tím by časový úsek pro změnu heslu měl být kratší. U internetového bankovnictví je vhodné měnit heslo aspoň dvakrát ročně, naopak u emailu, který má uživatel například jen pro registraci při instalaci software, vystačí stále stejné heslo třeba i pět roků.
- Nepoužívat stejné heslo pro různé systémy. Mít stejné heslo na Facebooku, do emailu (zvláště pokud tento email na FB uvádím) a do internetového bankovnictví je velmi neopatrné. Hesla pro přístup k citlivým a důležitým datům musí být unikátní.

Slabá – a tedy nevhodná – hesla jsou:

- Příliš krátký řetězec.
- Slovo, které je nějak spojeno s uživatelem (jméno, přezdívka, jméno přítele/přítelkyně/manžela/tchýně, bydliště, datum narození, jméno domácího mazlíčka, …).
- Logické sekvence znaků (12345, abcd, qwert).
- Slova psaná pozpátku.
- Jakékoliv slovo v libovolném jazyce (angličtina nejhorší volba, finština či maďarština je sice lepší, ale stále špatný nápad).

Silné (= vhodné) heslo je takový řetězec, který nesplňuje ani jednu z podmínek v seznamu výše, a:

- Je dostatečně a adekvátně dlouhý.
- Obsahuje alfanumerické i speciální znaky (zkrátka vše, co lze z klávesnice napsat).
- Vyskytují se v něm malá i VELKÁ písmena.

- Znaky národních abeced heslo zesilují, ale může se vyskytnout problém, že z počítače, který daný jazyk nepodporuje, nepůjde některý znak jednoduše napsat.

Příkladem silného hesla může být řetězec *uj2%Bt5dX.* Ale i u hesla tohoto typu je zde jeden zádrhel. Uvedený řetězec sice splňuje požadavky na silné heslo, jako celek je však jen velmi obtížně zapamatovatelný.

Jak si tedy vytvořit silné, ale zapamatovatelné heslo?

Dobrou variantou je zvolit nějakou mnemotechnickou pomůcku, která pomůže heslo vytvořit a zapamatovat. Mějme třeba větu *V roce 2018 jsem začal studovat na fakultě tělesné kultury v Olomouci*. Vezměme první písmenka z každého slova a máme vytvořené silné a současně zapamatovatelné heslo *Vr2018jzsnftkvO*.

Zbývá ještě dořešit problém, jak se vypořádat se zapamatovatelností většího počtu silných hesel, protože už víme, že používat jedno jediné heslo pro přístup do mnoha účtů je riziková činnost.

První možností je mít více mnemotechnických pomůcek. Pro heslo *„12345ctJcts?“*, které chrání přístup do emailu na Seznamu, máme mnemotechnickou pomůcku *„Jedna, dvě, tři, čtyři, pět, cos to, Janku, cos to snědl?“*, heslo do portálu UP, které má tvar *„mB4jaDj2“*, použijeme pomůcku *„měla Babka čtyři jabka a Dědoušek jen dvě“* a pro heslo do internetového bankovnictví výše zmíněnou větu o počátečním roku studia na FTK.

Drobným problémem tohoto přístupu je, že časem se nám mohou použité mnemotechnické pomůcky začít plést.

Druhou možností je zvolit postup, kdy si vytvoříme základ hesla a už tento výchozí řetězec bude silným heslem. Následně budeme tento základ modifikovat přidáním dalších znaků podle toho, kam se upraveným heslem budeme přihlašovat. Že by takovou úpravou vzniklo heslo slabé se bát nemusíme, protože když k heslu dobrému přidáme ještě další znaky, jeho síla naopak dále vzroste.

Vysvětleme si to na zjednodušeném příkladu. Jako základ hesla mějme „babku s dědouškem“, tedy *„mB4jaDj2“*, a tento základ doplníme o některé znaky na základě toho, jak se jmenuje server/služba, kam se přihlašujeme:

- portál UP - *LmB4jaDj2P*
- mail na seznam - *MmB4jaDj2S*
- profil na Facebooku - *KmB4jaDj2F*

Heslo pro Portál UP vzniklo tak, že na konec se přidalo písmeno *P* a na začátek písmeno *L,* tedy první a počáteční písmenko z názvu *„portál“*. Heslo na Seznam bylo stejným postupem obohaceno o první a poslední písmenko z názvu *„seznam“* a tentýž mechanismus zafungoval u hesla pro Facebook.

Při tomto postupu si na rozdíl od první varianty nemusíme pamatovat větší množství mnemotechnických pomůcek, ale stačí jen jedna pro základ hesla. Jako druhou věc si pak musíme zapamatovat algoritmus, kterým základ hesla modifikujeme pro konkrétní servery.

Pro práci s vytvářením hesel, s testováním síly a s udržováním jejich databáze lze použít velké množství různých programů. Zde doporučuji používat pouze prověřené programy a získané/stažené jen z legálních zdrojů. V opačném případě hrozí napadení počítače například viry či spywarem, které mohou naše hesla odesílat autorům takových to programů.

Pozn. Na adrese https://haveibeenpwned.com lze otestovat, zda heslo k zadané e-mailové adrese nebylo prolomeno a nenabízí se například někde na Internetu.

Malware

Termínem malware se označuje počítačový kód, který nepozorovaně infikuje systém za účelem poškození či odcizení dat, ovládnutí celého systému, sledování uživatele apod. Jedná se tedy o software, o nějž uživatel rozhodně nestojí a který mu svou činností škodí. Slovo vzniklo jako složenina z anglických slov *maliciouos* a *software*, tj. škodlivý, zákeřný software.

Tento typ nechtěného software se dělí podle různých hledisek do mnoha kategorií s většími či menšími rozdíly.

Nejčastější typy malware jsou:

- backdoor,
- rootkit,
- trojský kůň,
- červ,
- virus,
- spyware.

BACKDOOR (neboli zadní vrátka)

Tímto termínem se označuje chyba (ať už úmyslná či zanechaná omylem), které může útočník využít k další činnosti na napadeném zařízení. Dochází k obcházení standardních autentizačních postupů, takže nabízí skrytou metodu vstupu do programu či celého zařízení. Backdoor může být obsažen v software i v hardware. Např. backdoor v rooteru by mohl dovolit sledovat síťovou komunikaci za účelem získávání citlivých dat.

ROOTKIT

Software, který je navržen tak, že dokáže skrýt svou přítomnost a činnost před bezpečnostními programy, například antivirovým systémem, a dovoluje vzdáleně ovládat počítač bez vědomí jeho uživatele.

Úkolem většiny rootkitů dneška je zpřístupnit počítač pro další malware.

Jakmile se rootkit dostane do zařízení, jeho detekce je velmi obtížná. Antivirový systém a firewall nehlásí žádné nebezpečí, právě z toho důvodu, že rootkit upravil jejich činnost. Takže jeho přítomnost odhalí běžný uživatel většinou jen zcela výjimečně a náhodně na základě zpozorování nějaké neobvyklé aktivity. Odstranění tohoto typu malwaru je velmi náročné, mnohdy nezbyde nic jiného, než přeinstalovat operačním systém.

TROJSKÝ KŮŇ

Tento typ malware sice vykonává pro uživatele nějakou užitečnou činnost, zároveň však na pozadí běží skrytý škodlivý kód, o němž již uživatel není informován.

Příklady činnosti:

- ovládání vzdáleného systému,
- získávání hesel,
- destrukce souborů,
- procházení registru Windows,
- zneužití počítač k DDoS útokům,
- rozesílání spamu,
- stahování dat bez vědomí uživatele.

Trojský kůň (zkráceně trojan) se nejčastěji šíří pomocí příloh v emailech nebo bývá ukrytý v bezplatných aplikacích či filmech. Relativně dobrou zprávou je fakt, že se na napadeném zařízení nedokáže sám množit.

Nejlepší ochranou proti trojanům je preventivní opatrnost uživatele spolu s používáním software, který dokáže trojské koně detekovat a odstranit. Což znamená:

- Neotvírat emaily z neznámých adres zvlášť obsahují-li přílohu.
- Nneklikat na odkazy na www stránky uvedené v emailech z neznámých kontaktů.
- Nnestahovat data z pochybných zdrojů.
- Vyhýbat se používání tzv. torrentů.
- Aktualizovat operační systém.
- Používat firewall.
- Používat antivirovým systém v jeho nejnovější verzi.

ČERV

Počítačový červ je škodlivý program, který ke svému šíření využívá zejména počítačových sítí, dosti často ve formě přílohy emailů. Škodí už jenom samotným množením, které zatěžuje a tím pádem zpomaluje počítač i počítačovou síť.

Většina červů však s sebou nese i tzv. náklad, což je sekundární činnost červa na napadeném zařízení. Tato činnost může způsobit:

- modifikaci souborů,

- nestabilní chování programů nebo celého systému,
- zneprovoznění počítače,
- procházení dat za účelem získávání osobních údajů,
- vytváření backdoor,
- zahlcení počítačové sítě.

Obrana proti červům je podobná jako u trojských koňů, tedy kombinace preventivních opatření na straně uživatele a používání bezpečnostního software spolu s nastavením vyšší úroveň bezpečnosti v emailovém klientovi.

VIRUS

Základní charakteristikou počítačového viru je jeho rozmnožování pomocí napadených souborů, které se označují jako hostitelé. Nejčastěji se jedná o spustitelné soubory nebo dokumenty. Pokud se na počítač nějakým způsobem dostane nakažený soubor (např. stažením z Internetu, přenesením na flash disku) a dojde k jeho následnému použití, virus začne být aktivní, začne napadat další soubory a také vykonává konkrétní škodlivou činnost, na kterou byl naprogramován. Výsledky činnosti viru jsou totožné nebo podobné jako činnost trojských koňů nebo červů.

Významnou částí ochrany před zavirováním počítače je stejně jako u červů preventivní chování uživatele. Z hlediska software je důležité používat nějaký antivirový systém. V dnešní době je jich na výběr velká řada a dobrý antivirový systém má následující charakteristiky:

- jednoduchá instalace,
- automatická aktualizace,
- snadné používání,
- rezidentní štít,
- možnost nastavení pravidelných kontrol,
- kombinace různých technik k detekci virů,
- kontrola emailů,
- rychlá reakce výrobce při virových epidemiích.

Mezi kvalitní antivirové programy například patří:

- ESET,
- Norton Symantec,
- TrustPort,
- BitDefender,
- Avira,

- Kasperski,
- AVG,
- AVAST.

SPYWARE

Tento druh škodlivého software je velmi nebezpečný z toho důvodu, že většinou je navržen ke sledování uživatelů, pochopitelně bez jejich vědomí. Monitoruje práci uživatele na počítači, sleduje historii navštívených webových stránek, sbírá osobní údaje, hesla atp. Na počítač se dostane třeba prohlížením nakažených webových stránek nebo instalací programu, který v sobě spyware již obsahuje.

Mezi druhy činnosti spyware patří:

- Adware - násilné zobrazování pop-up oken s reklamou, což je velmi obtěžující.
- Keylogger - mapování stisknutých kláves na klávesnici, což může odhalit nejen zadávaná hesla, ale i celé obsahy editovaných dokumentů.
- Hijacker – změna domovské stránky v prohlížeči.
- Remote administration – vzdálená správa napadeného počítače.
- Sniffer – zjišťování a odesílání přihlašovacích údajů, hesel, čísel bankovních karet.
- Sledování historie navštívených stránek nebo seznamu spouštěných/nainstalovaných programů, což může vést ke snazšímu profilování uživatele a tedy následně k cílené reklamě.
- Odesílání celých dokumentů nebo procházení jejich obsahu a hledání osobních údajů.

Detekovat přítomnost spyware na počítači není pro uživatele jednoduchým úkolem, software je napsán tak, aby jeho činnost byla maximálně utajena. Přesto existuje několik příznaků, kdy by měl uživatel zpozornět. Patří mezi ně:

- Změněná domovská stránka prohlížeče.
- Pomalý start systému či webprohlížeče.
- Pomalé vypínání počítače.
- Nestabilní chování programů nebo i celého systému.
- Nové ikony v jakékoliv složce.
- Výskyt reklamních oken při práci s počítačem.

Prevence proti výskytu spyware je stejná jako prevence u trojských koňů uvedená výše. V oblasti software je vhodné používat tzv. anti-spyware, tedy programy, jež jsou schopné tyto hrozby detekovat a následně zneškodnit.

Spam, hoax

Společným znakem obou činností je hromadné rozesílání informací, nejčastěji pomocí emailu, ale stejným problémem mohou být postiženy různé diskuze či sociální sítě. V současné době se jedná o velký problém Internetu, protože se odhaduje, že 80-90% emailové komunikace jsou spamy. Je tedy evidentní, že existence spamu zatěžuje počítačové sítě, neboť snižuje jejich průchodnost zbytečnými daty.

SPAM

je hromadné rozesílání *nevyžádaných* informací převážně reklamního charakteru a neexistuje proti němu stoprocentní ochrana. Tato forma rozesílání se volí z toho důvodu, že je levná, rychlá a masivní. Navíc spammeři se mohou nabourat do cizích počítačů a nelegálně je tak využívat ke své činnosti.

Škodlivost spamu spočívá:

- Etický problém – obtěžování ostatních uživatelů informacemi, o které nestojí.
- Možnost poškození nějaké osoby či firmy.
- Obírá příjemce spamu a čas i peníze.
- V emailové schránce lze přehlédnout nebo smazat důležitý mail.
- Zabírá místo ve schránce, prodlužuje dobu stahování pošty.
- Zahlcuje počítačové sítě.
- Filtrace spamu může zpozdit poštu řádově i o hodiny.

Ochranu proti výskytu spamu ve vlastní emailové schránce lze rozdělit na dvě oblasti – prevence (spočívá v tom, že alespoň některou emailovou adresu má uživatel víceméně utajenou před spammery) a filtrace (došlé maily jsou vyhodnocovány a ty, jež jsou označeny jako spam, se přesunou do zvláštní složky). Nutno podotknout, že prevence je důležitější než samotná filtrace, protože když je uživatel spamem obtěžován v minimální míře, nemusí nějak komplikovaně řešit filtraci.

Základní myšlenkou prevence je nakládat s emailovou adresou tak, aby se nedostala do spammerských databází. Protože jakmile se v nich jednou ocitne, uživatel nemá žádný nástroj na její vyřazení. K preventivním zásadám patří:

- Není-li to nezbytně nutné, svou emailovou adresu nikam nezadávám.
- Vyžaduje-li např. webová stránka zadání emailu, přičemž zadané adresy se v budoucnu nebude ke komunikaci s uživatelem využívat, je dobré zadat falešný mail. V podstatě se jedná o to, zadat řetězec, který vypadá jako email, ale není platný. Např. *trhnisinohou@upol.cz*.

- Při zveřejnění adresy v psaném textu ji napsat nějakým „alternativním“ způsobem, př. *„Pro více informací pošlete mail na karel (zavináč) gmail.com*“, nebo *„Kontaktovat mě můžete na mailu martina98 a jsem na Seznamu*“.
- Zvážit, jaký tvar bude mít moje adresa před znakem zavináč (*„x16jirka*“ je lepší než jen samotné *„jirka*“) a na jakém serveru si email vytvořím (hodně známé servery jsou častějším terčem útočníků s cílem získat adresy, u neprověřených serverů zase uživatel neví, jak dobře jsou proti těmto útokům zabezpečeny).
- Zvážit, komu svoji emailovou adresu prozradím.
- U internetových služeb, kde se pro jejich činnost musí zadat email (např. Uschovna.cz), si rozmyslet, kterou svou adresu - a zda vůbec - ji zadám.
- Mít více emailových adres a používat je v přesně definovaných případech:
    - privátní – pouze pro komunikaci s lidmi, které osobně znám a jsou „prověření“ (pravděpodobnost prozrazení této adresy je nízká),
    - veřejná – pro komunikaci s ostatními lidmi,
    - registrační – pro nakupování na e-shopech, při registraci instalovaného software, pro vytváření profilů na sociálních sítích (zde se dá očekávat, že v databázích se objeví docela brzy).
- Pokud je mail vyhodnocen jako spam, je dobré jej bez čtení rovnou smazat. Rozhodně na něj NIKDY nereagujeme.

Co se týče filtrace spamů, je dobré si uvědomit, že do cílové emailové schránky dorazí jen mizivá část původního množství. Je to dáno tím, že maily jsou během své cesty Internetem vícekrát filtrovány a většina spamu je zavčas detekována již díky tomuto postupu. Principy a algoritmy tohoto typu filtrace nemusejí koncového uživatele zajímat, protože jsou to záležitosti, které nemůže ovlivnit. Důležitou informací je naopak fakt, že na svůj počítač si může nainstalovat speciální typ software, tzv. antispam. Obecně se jedná o software, který spolupracuje s poštovním programem a detekuje a třídí nevyžádanou poštu podle zadaných kritérií.

Zařadit sem můžeme:

- SPAMfighter,
- Spamihilator,
- SpamBayes,
- MailWasher.

HOAX

je hromadné rozesílání zpráv s nepravdivým obsahem, ve formě poplašných zpráv, řetězcových emailů, … Na rozdíl od spamu, který je doručován z nám neznámých adres, hoax posílají obvykle lidé, se kterými jsme např. v mailovém kontaktu. Tyto osoby nám nechtějí primárně uškodit, hoaxy posílají ve víře, že napomáhají dobré věci.

K typickým druhům hoaxů patří:

- Varování před viry či jinými ohroženími počítače.
- Falešné prosby o pomoc (některé z nich však mohly být kdysi i skutečné).
- Různé „zaručené“ rady.
- Popisy nereálného nebezpečí.
- Petice.
- Řetězcové maily.
- Pyramidové hry.

Škodlivost hoaxů se shoduje se škodlivostí mailů, jakousi „přidanou hodnotou“ je tu ještě šíření nepravdivých zpráv, což může vést k poklesu důvěryhodnosti osoby/zdroje, která tyto zprávy opakovaně posílá.

Charakteristickými znaky, podle nichž lze usoudit, že zaslaná zpráva je hoaxem, jsou:

- Popis nebezpečí.
- Hromadná žádost o pomoc.
- Důvěryhodnost zprávy je podpořena nějakou významnou firmou, známou osobností, velkou organizací.
- Žádost o rozeslání dalším lidem.

Zvlášť poslední bod je velmi podstatný, jakmile jej zpráva obsahuje, můžeme si být takřka jisti, že se jedná o hoax.

V případě, že uživatel zjistí, že zaslaná zpráva spadá do této kategorie, měl by udělat dvě věci. V žádném případě nerozesílat zprávu dalším uživatelům a současně informovat původního odesílatele o tom, že rozesílá nesmysly. Případně mu také doporučit návštěvu webu www.hoax.cz, kde si o této problematice může přečíst více. Protože jak již bylo řečeno, hoaxy se šíří díky neznalosti lidí, jejich naivitě, neochotě ověřovat si informace apod.

Zneužívání osobních údajů

Osobní údaje jsou nedílnou součástí soukromí a jejich ochrana v posledních letech nabývá stále více na významu. S rozvojem informačních a komunikačních technologií roste počet situací, kam člověk svá osobní data zadává, ať už přímo nebo využíváním určitých služeb např. na Internetu. Díky tomu je také snadnější tato data vyhledávat, pátrat po souvisejících informacích a získávat tak detailnější obraz o konkrétní osobě, firmě nebo organizaci.

Zákonná definice říká: *„Osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu."*

Musíme si uvědomit, že při používání různých služeb Internetu, které jsou zdarma, platíme za tyto služby jinou formou. A sice svými osobními údaji. Takže přicházíme o soukromí, přičemž cizím subjektům dovolujeme získat informace o naší osobě, které se pak přes cílenou reklamu snaží zpeněžit.

Toto ale není principiálně nic špatného, pokud se to děje při dodržení zákonných podmínek. Je jen a jen na uživateli jaká svá data a komu poskytne. Když např. dobrovolně zadá svoji mailovou adresu a odsouhlasí pravidelné zasílání newsletteru na nějakém e-shopu, nemůže se divit, že mu chodí pravidelně maily s nabídkou zboží z tohoto obchodu.

Zcela jiným problémem ovšem je, pokud někdo získá naše osobní údaje a snaží se je zneužít v rozporu s morálkou či dokonce se zákonem. Zneužitím osobních údajů se v podstatě rozumí jakékoliv neoprávněné nakládání s nimi. Fyzická či právnická osoba, která nakládá s osobními údaji v rozporu se zákonem, se může dopustit přestupku případně trestného činu.

Krádež identity může znamenat, že na naše jméno si pachatel požádá o úvěr, nabízí prodej zboží našim jménem, uzavírá smlouvy, které jsou napsány na nás, …

Základní pravidla pro ochranu před zneužitím osobních dat:

- Nesvěřovat osobní doklady jiné (cizí) osobě mimo svůj dohled.
- Platební karty a peněženku nosit odděleně od osobních dokladů.
- Neumožnit cizí osobě udělat si kopie osobních dokladů.
- Zbytečně nezveřejňovat svá osobní data, příp. zvážit, která z nich poskytnu zcela neznámým lidem a která i svým přátelům. Typicky uplatnitelné v rámci sociálních sítí.
- Dávat si pozor na to, abych svá dat někomu nevědomky prozradil (viz sociální inženýrství).

Kybergrooming, kybešikana, kyberstalking, sexting

Všechny formy tohoto závadného chování na Internetu (nejčastěji na sociálních sítích) se nevyhýbají z pozice oběti žádné věkové kategorii, za nejvíce ohrožené se však dají považovat děti a teenageři. Je to dáno tím, že právě tyto věkové skupiny využívají možnosti kybernetické komunikace v maximální míře a bohužel si jen málo uvědomují rizika s tím spojená.

KYBERGROOMING

Termínem kybergrooming se označuje takové jednání, kdy pachatel si z veřejně přístupných zdrojů na Internetu vytipovává svoji oběť, poté se snaží získat její důvěru a navázat bližší vztah, aby ji přinutil k osobní schůzce. Důvodem k osobnímu setkání je následné sexuální zneužití oběti, její fyzické napadení, případně vydírání s cílem donutit oběť páchat trestnou činnost.

Obvykle se pachatel vydává za někoho mladšího a atraktivnějšího, pří svém jednání zneužívá dětské naivity, důvěřivosti, jeho touhy po něčem výjimečném, …

Agresor obvykle postupuje podle následujícího schématu:

1. Vytipování oběti.
2. Navázání kontaktu, snaha izolovat oběť od okolí.
3. Rozvíjení virtuální komunikace, budování důvěry oběti až její závislosti (i pomocí dárků).
4. Případné získání kompromitujících materiálů.
5. Další manipulativní jednání s cílem osobní schůzky.
6. Útok agresora (napadení, zneužití, …).

Základní myšlenkou obrany proti kybergroomingu je chránit si své citlivé údaje a v žádném případě nikomu cizímu neposkytovat materiály, které mohou být využity k vydírání. Rovněž pokud by mělo přeci jen dojít k prvnímu setkání s „virtuálním“ přítelem, dítě by mělo informovat rodiče nebo aspoň své kamarády.

Patrně nejznámějším českým kybergroomerem byl Pavel Hovorka, který měl sexuálně zneužít více než dvacet chlapců. Své oběti vyhledával na seznamovacích serverech. Zpočátku si s nimi dopisoval a telefonoval, později je pozval k sobě do práce - pracoval jako ostraha v tiskárně. Tam je vydíral jejich nahými fotografiemi a donutil je tak k pohlavnímu styku.

KYBERŠIKANA

Jako kyberšikanu označujeme jednání, kdy oběť je vystavena ponižování a fyzickému i psychickému omezování za pomoci masové elektronické komunikace (email, mobilní telefony, sociální sítě).

Pachatel šikanuje tím, že např. posílá obtěžující nebo dokonce útočné zprávy nebo vytváří blogy či webové stránky, které svým vymyšleným obsahem oběť poškozují. Mezi další formy patří natáčení videí s úmyslným provokováním oběti nebo i jejím fyzickým napadením, tyto záznamy jsou pak posílány dalším lidem nebo jsou umísťovány třeba na sociální sítě.

Na rozdíl od klasické šikany spočívá zvýšené nebezpečí této formy útlaku v tom, že kyberšikana trvá mnohonásobně delší dobu, protože videozáznamy mohou na webových stránkách figurovat mnoho měsíců a ve virtuálním světě Internetu vlastně mohou zůstat navěky. Taktéž počet lidí, kteří se o kyberšikaně dozvědí, je mnohem větší a mnohdy se k ponižování oběti i přidají.

Domnělá anonymita Internetu, možnost vystupovat pod jakoukoliv identitou, která s realitou nemusí mít vůbec nic společného (fyzicky slabý jedinec si na síti může troufnout i na pořádného hromotluka), obecně vzrůstající apatie ve společnosti a použití technologií, které jsou dospělým přece jen trochu cizí, jsou důvody, proč kybešikana stále vzrůstá a objevují se její další nové formy.

Příkladem budiž tzv. Happy Slapping, kdy skupina útočníků napadá nic netušící a mnohdy náhodně vytipovanou osobu a pořizuje z toho napadení videozáznam. Přičemž jediným cílem tohoto jednání je „mít další cool video a zveřejnit ho“.

Kyberšikana je taktéž velkým nebezpečím pro samotné učitele. Např. na YouTube lze nalézt spoustu videí, kdy žáci záměrně provokují učitele s úmyslem vyvést jej z míry a cílem celého jednání je snaha vyučujícího zesměšnit. Toto je v kyberprostoru nesmírně jednoduché a o to víc lákavé.

V roce 2010 Facebook zrušil skupinu „Polovina třídy spí, druhá si maluje a učitelka si povídá s tabulí“, která nasbírala až 170 tisíc fanoušků a kde byly zveřejňovány hlavně zesměšňující fotografie a videa nejen žáků, ale i učitelů.

Nechvalně známým případem kyberšikany, který skončil sebevraždou oběti, je případ ze školy v polském Gdaňsku z roku 2006. Čtyři zhruba čtrnáctiletí chlapci povzbuzeni ostatními napadli stejně starou Annu Halmanovou, kterou napřed fyzicky týrali a následně provedli simulaci znásilnění. To vše „pochopitelně“ jeden ze čtveřice nahrával na telefon a za chvíli už nahrávka kolovala po Internetu. Napadená Anna utekla domů, kde ji matka druhý den ráno našla oběšenou na švihadle. Nepochopen celého fenoménu kyberšikany dokládá rozhodnutí vedení školy, které žáky nijak nepotrestalo. A rodiče hochů proti soudnímu rozsudku, který pachatele umístil do nápravných ústavů, protestovali s odůvodněním, že ke skutečnému znásilnění vůbec nedošlo a šlo jen o nevinnou dětskou hru.

Dobrými příklady, kam až může (kyber)šikana zajít je estonský film *Zkažená mládež* z roku 2007 nebo film *Zlo mezi námi*, švédský snímek z roku 2003.

KYBERSTALKING

Za kyberstalking se považuje činnost, při níž pachatel využívá komunikačních a informačních prostředků k dlouhodobému pronásledování oběti nevyžádanou či nechtěnou pozorností. Cílem tohoto jednání bývá většinou úmysl vyvolat u oběti pocit strachu o své bezpečí, soukromí, majetek nebo zdraví.

Jedná se hlavně o zasílání emailů, sms zpráv nebo vzkazů přes další komunikační kanály, vkládání příspěvků na profily sociálních sítí oběti nebo v extrémním případě i monitorování počítače speciálními programy. Nejčastějšími obětmi těchto aktivit mohou být politici, celebrity, ex-partneři nebo třeba lidé z konkurenčních firem.

Jak se dá kyberstalkingu předcházet:

- Chránit si svá osobní data a citlivé údaje.
- Mít zabezpečený počítač nebo telefon proti zavirování.
- Používat kvalitní a silná hesla.

SEXTING

Jak už samotný název napovídá, jedná se posílání textovým či multimediálních zpráv se sexuálním obsahem prostřednictvím komunikačních technologií. Tato činnost je provozována převážně mladistvými, ale nevyhýbá se ani dospělým osobám.

Rizika sextingu:

- Citlivý materiál, který někomu posíláme v dobré víře, může být zneužit proti nám.
- Tento materiál může být použit i za několik roků po svém vzniku (např. ex-partner jej z pomstychtivosti zveřejní na Internetu).
- Data mají svůj vlastní internetový život a mohou na něm kolovat mnoho a mnoho let.
- V případě sextingu u dětí se tak může pachatel stát šiřitelem dětské pornografie.
- Materiál zaslaný v rámci sextingu bývá často použit jako nástroj k vydírání u kybergroomingu.

Největší nebezpečí z následků takové „zábavy“ hrozí zejména u dětí a mladistvých, dle šetření Policie ČR se tato aktivita týká dokonce i dětí ve věkovém rozmezí 11 – 13 let.

Jediným skutečným fungujícím preventivním opatřením proti zveřejnění sextingového obsahu je nejen nikomu taková data neposílat, ale ani je nepořizovat. Případy z mobilních telefonů uniklých fotografií různých (pseudo)celebrit jsou dostatečně známé. I když nutno podotknout, že v mnoha kauzách byl „únik“ možná plánovaný ☺.

Příklad zneužití sextingu v ČR:

Sedmnáctiletý mladík se na sociální síti Omegle.com náhodně seznamoval s dívkami z České republiky. Po krátké konverzaci je požádal o poslání fotky jejich nahého těla a takřka každá desátá mu vyhověla, ať už ji zaslala emailem nebo třeba přes Snapchat. Mezi zaslanými fotografiemi byla i taková, na níž dvanáctiletá dívka pózovala se zeleninou ve svém přirození. Posléze byl onen mladík obviěn z trestných činů Výroba a jiné nakládání s dětskou pornografií a Zneužití dítěte k výrobě pornografie. Přestože dívky mu posílaly samy bez nějakého nátlaku či vydírání.

Zdroje:

www.jaknainternet.cz

cs.wikipedia.org

www.computerworld.cz

www.zive.cz

www.latrine.cz

www.policie.cz

www.internetembezpecne.cz

www.it-slovnik.cz

is.muni.cz

www.zakonyprolidi.cz

www.nebudobet.cz

www.e-bezpeci.cz

www.sexting.cz