(NE)bezpečný Internet

LUKÁŠ JELÍNEK

Policie České rebubliky
Krajské ředitelství policie Moravskoslezského kraje
Preventivně informační skupina Karviná

www.policie.cz

Obsah

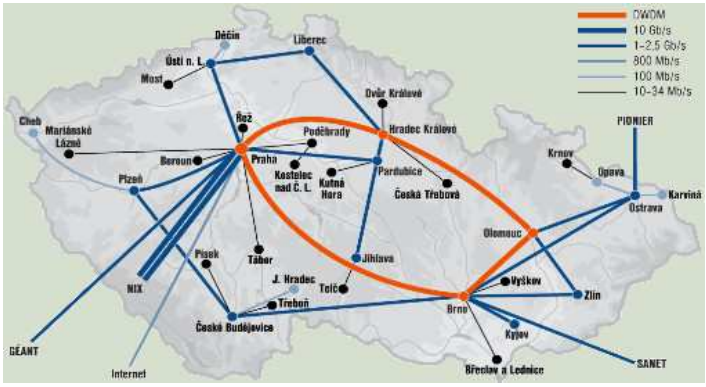
Předmluva

Tato publikace je určena především rodičům, pedagogům, preventistům a vůbec všem, kteří se chtějí ve virtuálním prostředí Internetu chovat co nejbezpečněji – stejně jako to dělají v běžném životě. Je to jakási sonda do této problematiky s cílem seznámit čtenáře s aktuálním stavem v této oblasti, poukázat na největší rizika a hrozby. Jen člověk s dostatkem informací má šanci nestát se obětí rizik, souvisejících s používáním Internetu a navíc poskytnout radu či pomoc ostatním, zejména pak dětem. Ty jsou nepochybně nejohroženější skupinou.

Vznik a vývoj Internetu

Internet je celosvětová počítačová síť vytvořena z jednotlivých podsítí.

Internetová síť nemá žádné centrum a je tvořena jednotlivými uzly, které jsou vzájemně propojeny. Z toho vyplývá fakt, že neexistuje žádná světová organizace či instituce, která by Internet řídila a shromažďovala jeho data. Existují však organizace, které po technické stránce Internet regulují nebo nějak ovlivňují.



Znázornění hlavních datových cest v ČR podle rychlosti.

V roce 1969 vznikla v USA malá decentralizovaná počítačová síť Arpanet, která měla čtyři uzly a byla využívána pro vědecké účely. Vyvinuta byla na armádní zakázku, s požadavkem na flexibilitu, adaptabilitu a neexistenci žádného centra nezbytného pro chod sítě. Postupem času se tato síť vyvinula a rozšířila až do dnešní podoby a změnila název na Internet. Dnes je Internet celosvětově rozšířen. V České republice je poměrně finančně dostupný a tudíž i velmi rozšířený nejen ve firmách a institucích, ale i v domácnostech. Rychlost připojení se pohybuje v průměru 10 – 25 Mbit/s, což umožňuje široké využití Internetu, včetně multimédií.

Do budoucna se tato rychlost bude jistě zvyšovat, Internet bude pronikat do stále většího počtu nejrůznějších zařízení a spotřebičů a bude tak stoupat jeho rozšiřitelnost a využitelnost.

S rozvojem těchto nových komunikačních technologií se bohužel zvyšuje i riziko jejich zneužití.

Nejpoužívanější komunikační technologie a aplikace Internetu

Služby, které Internet poskytuje, jsou orientovány především na komunikaci. Existuje celá řada komunikačních nástrojů, aplikací a programů, které tuto komunikaci v nejrůznějších formách umožňují. Pojďme si popsat ty nejpoužívanější z nich.

E-mail

E-mail je internetová služba umožňující posílání textových zpráv s přílohou. Přílohou může být soubor jakéhokoli typu, např. obrázek, video, zvuk, textový dokument, spustitelný program, atd. Velikost e-mailové zprávy je omezena. U většiny „free mailových" služeb je maximální velikost zprávy v řádu několika MB.

Z hlediska bezpečnosti jsou problematické přílohy, které mohou obsahovat viry a jiný škodlivý software. Často jsou obsaženy ve spamu, což je nevyžádaná pošta. Ta přichází od odesilatelů, které neznáte, většinou je v cizím jazyce (angličtině, ruštině, atd.) a obsahem bývá obchodní nabídka (Viagra, levná kreditní karta, software renomovaných výrobců za neuvěřitelně nízké ceny, atd.) nebo erotika (erotické zboží nebo služby).

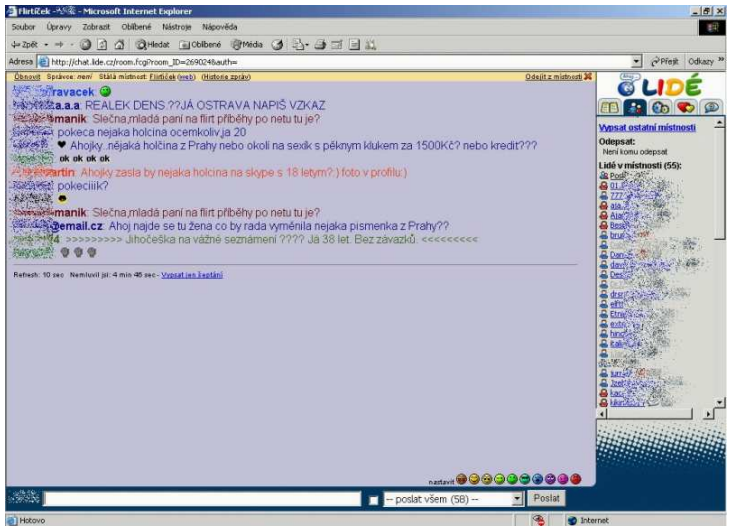
V textu se také mohou objevit odkazy vedoucí na podvodné stránky, jejichž hlavním cílem je vylákat od neopatrných uživatelů přihlašovací údaje – nejčastěji do internetového bankovnictví, platebních systémů či jiných aplikací, jejichž zneužití vede k majetkovému prospěchu pachatelů těchto podvodů. Jedná se o tzv. phishing.

V poslední době se bohužel objevují i podvodné e-maily, které jsou v češtině a odesílatel i obsah sdělení působí důvěryhodně. Ono totiž odesílatele e-mailové zprávy lze snadno podvrhnout. Proto vždy zvažujte, zda emailovou přílohu otevřít a zda věřit odkazům v textu.

Velkou pomocí v boji proti těmto jevům je antivirový program a antispamový filtr. Pro domácí použití existuje celá řada verzí, které jsou zdarma.

Chat

Chat je systém, který umožňuje uživatelům společnou komunikaci v „místnostech", které jsou tematicky rozděleny. Lidé v nich vystupují pod přezdívkami a další informace o své osobě jsou nepovinné. Určitým nebezpečím může být ona anonymita. Lidé, kteří jsou za ní schovaní, mají většinou tendenci se idealizovat a



chovat se mnohem odvážněji, často také vydávat se za opačné pohlaví.

V posledních letech jsou chaty na ústupu, už nemají tolik aktivních uživatelů. Důvodem je značná popularita sociálních sítí, ke kterým přešla většina mladých lidí.

Chat bývá součástí nebo doplňkem různých serverů, jako Lide, Seznam, Libimseti, Xteen, Xchat, atd.

Instant messiging

Zde se jedná o služby a aplikace na straně uživatele, které umožňují online komunikaci s dalšími lidmi. Nejznámějším a nejpoužívanějším programem je ICQ, dále pak třeba QIP, Jabber, Miranda, atd. Všechny tyto programy poskytují veskrze stejnou funkčnost, liší se především množstvím funkcí a licenčním ujednáním, které může být v některých případech pro uživatele nevýhodné.

SMS brány

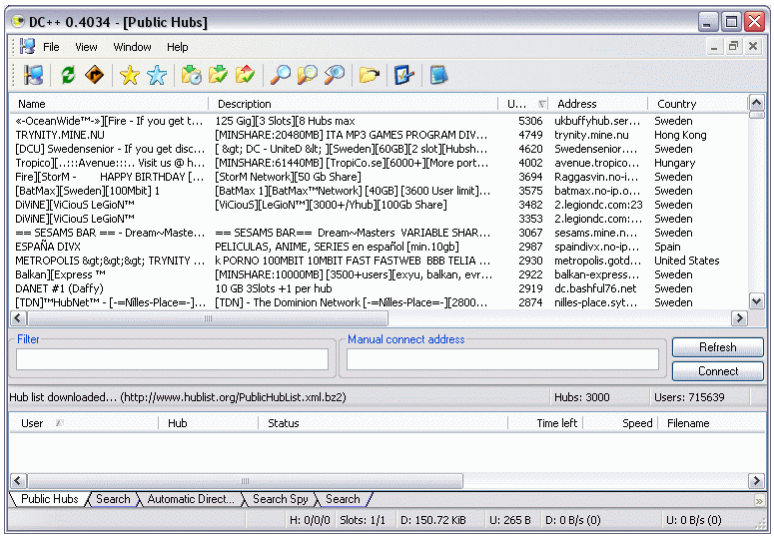
Pomocí této služby mobilních operátorů se dají posílat SMSky z Internetu, a to zdarma. Odesílatel tak vloží tel. číslo příjemce, textovou zprávu a odešle ji. Takto lze anonymně odeslat několik zpráv, což může být snadno zneužitelné. Dokonce existuje program, který dokáže odeslat SMS zprávu s podvrhnutým číslem odesílatele. Falšovat číslo odesílatele SMS není žádná věda, dokonce k tomu nejsou potřeba ani vědomosti, ani velký kapitál. Jednu falešnou SMS lze pořídit za pouhé dvě koruny, a to prostřednictvím lokalizované služby nikoliv undergroundové, nýbrž nadnárodní společnosti. Co takhle si poslat SMS z čísla prezidenta republiky?

Sociální sítě

Fenoménem poslední doby jsou sociální sítě, v České republice konkrétně americká síť Facebook. Obecně je sociální síť prostředí, ve kterém se sdružují lidé, kteří mají něco společného a vytváří tak virtuální sociální skupiny. Takovéto prostředí je především pro mladé uživatele velice atraktivní, mohou zde nacházet nové přátele, komunikovat s nimi, sdílet mezi sebou informace, fotky, videa, hrát hry, atd.

Na druhé straně je to prostředí, ve kterém si lidé mohou vytvářet falešnou identitu, lhát, podvádět, útočit, zneužívat, atd. K tomuto faktu bychom neměli být lhostejní a aktivně a vytrvale udržovat svoji bezpečnost. Ta spočívá především v ochraně svého soukromí a své identity. Neměli bychom sdělovat světu zbytečně moc informací o nás samotných, ani o našich blízkých a pečlivě zvážit zveřejnění soukromých videí či fotografií. Tyto informace a data se mohou stát vítanou pomocí pro potencionálního útočníka. Nelze slepě spoléhat na nějaké technické zabezpečení těchto sítí, nastavení stupně zabezpečení a podobně. Čas od času se stane, že i tato zabezpečení selžou. Mnohem častěji se ale stává to, že zapůsobí lidský faktor a útočník uživatele jednoduše obelstí. Vystupuje pod falešnou identitou, má nejrůznější výmluvy a scénáře, chová se podbízivě, atd. Rizikovou skupinou jsou zejména děti, které jsou důvěřivé a často takové nebezpečí nerozpoznají. Proto je zde důležitá informovanost jak jejich, tak rodičů.

P2P sítě



Takovéto sítě jsou určené ke sdílení dat. V drtivé většině jsou tyto sítě využívány k šíření nelegálního obsahu (hudba, filmy, hry, programy, atd.). Jedním ze zástupců těchto sítí je např. Direct Connect nebo BitTorrent.

Spousta uživatelů těchto sítí si ani neuvědomuje společenskou nebezpečnost, právní odpovědnost a důsledky svého jednání. Problémem je, že v naší společnosti je pohled na tento druh trestné činnosti velmi mírný, přestože finanční ztráty společností jsou obrovské a tresty vysoké.

Podstata nebezpečí internetové komunikace

V internetové komunikaci je nejrizikovějším faktorem anonymita uživatelů. Ti si mohou svou identitu skrýt nebo vytvořit jinou, falešnou. Takto skryti se většinou chovají jinak, než ve skutečnosti. Jistě znáte případy, kdy člověk vystupující pod nějakou přezdívkou píše komentáře, třeba na nějakých zpravodajských serverech, ve kterých je hrubý, útočný a vulgární, ačkoliv se tak v běžném životě nechová. Právě ona anonymita dodává takovýmto lidem pocit velikosti a odvahu k věcem, které by jinak neudělali.

Na Internetu působí spousta „špatných“ lidí, útočníků, kteří se snaží někoho zneužít. Motivem jejich jednání jsou peníze, pomsta, závist, touha po sexu, různé deviace a podobně. Využívají k tomu lsti, psychologické metody nátlaku i technické prostředky. V nebezpečí jsme

v podstatě všichni, protože obětí se může stát prakticky kdokoli. Ovšem nejrizikovější skupinou jsou děti, které na Internetu tráví spoustu času a často bez dozoru rodičů.

Základní obranou je důsledná ochrana soukromí a přiměřená nedůvěra k lidem, které osobně neznám.

- *Nevěřte slepě cizím lidem z Internetu.*
- *Chraňte si svou identitu a pokud možno, zůstávejte v anonymitě.*

Hesla

Nejpoužívanější formou identifikace uživatele v prostředí Internetu je v dnešní době kombinace uživatelského jména a hesla. Tato metoda je založená na nějaké znalosti uživatele, v našem případě hesla. Existují i další metody, které jsou bezpečnější, jako biometrie (otisk prstu, obraz sítnice oka, atd.) či ověřování pomocí hardwarového klíče (čipové karty, USB tokeny, atd.). Tyto metody jsou však využívány spíše v komerčním sektoru a tam, kde je nutná velmi vysoka míra zabezpečení. V současné době je nejbezpečnější kombinace všech tří zmiňovaných metod identifikace.

Vraťme se nyní k heslům. Heslo bychom měli volit uvážlivě, jelikož na něm záleží naše zabezpečení. Heslo by mělo být dostatečně „silné“ a neměli bychom používat jen jedno pro vstup do všech systémů a služeb. Ideální stav je mít pro každou službu jiné heslo. Do těch zvlášť rizikových, jakým je kupříkladu internetové bankovnictví, je dobré zvolit si unikátní heslo. Heslo je tím silnější, čím je menší pravděpodobnost jeho uhodnutí. Tu můžeme snížit několika způsoby:

- volit heslo delší, než šest znaků, ideálně osm znaků a víc
- použít znaky malé a velké abecedy, speciální znaky a čísla (jejich kombinace zvyšuje míru složitosti)
- nevolit jako heslo veřejně známé údaje (datum narození, jméno, příjmení, atd.)
- nevolit jako heslo slovo nějakého významu. Důvodem je prevence před „slovníkovým útokem“, jehož podstatou je automatizované zkoušení slov ze slovníku daného jazyka.

Příkladem silného hesla by mohlo být toto: „A7f8§3_o“. Z praktických důvodů není dobré používat znaky „Y“ a „Z“ a znaky s diakritikou. Důvodem jsou různé klávesnice na různých počítačích. Hesla bychom měli chránit a pravidelně obměňovat. Jedině tak dosáhneme uspokojivé míry zabezpečení.

- *Používejte silná hesla.*
- *Nepoužívejte jen jedno heslo do všech systémů.*
- *Svá hesla chraňte a pravidelně obměňujte.*

Kyberšikana

Šikana je opakované a dlouhodobé psychické či fyzické ubližování člověku (nebo skupině lidí). Útočníkem může být jednotlivec nebo skupina. Obětí je většinou ten, kdo se nějakým způsobem odlišuje od ostatních členů skupiny. Ve školní třídě slabší žák, obézní spolužačka, v pracovním týmu nevýkonný pracovník, atd. Zkušený pedagog šikanu pozná a v nejbližším okolí se o ní ví, problémem je však nezájem kolektivu situaci řešit. Nic neodradí útočníka víc, než naprosté odsouzení jeho jednání ze strany kolektivu. Pro útočníka je totiž jeho zájem a obdiv jednou z hlavních motivací k šikaně.

Kyberšikana vychází z běžné šikany, jen je použito Internetu či mobilního telefonu. Většinou je kyberšikana spojena s klasickou šikanou, ale nemusí tomu tak vždy být. Pro útočníka má totiž ta virtuální mnoho výhod:

1. Útočníkem může být kdokoliv. Nezáleží na věku, pohlaví, síle ani společenském postavení.
2. Útočník může být anonymní, a to jak pro své okolí, tak pro svou oběť.
3. Útočit lze kdykoliv a odkudkoliv, kde je připojení k Internetu nebo GSM signál.
4. Útočník se může chovat mnohem agresivněji, než by si to dovolil ve skutečnosti.
5. Obětí může být kdokoli. Opět nezáleží na věku, pohlaví, síle ani společenském postavení. Není výjimkou, že např. žák školy šikanuje na Internetu svého učitele. Reálně by si to jen stěží dovolil, avšak jako anonymnímu útočníkovi mu to nečiní problémy.
6. Oběť se jen těžko brání.

Jak je vidět, kyberšikana je velice nebezpečný jev, který může oběť velice silně psychicky zasáhnout a společensky poškodit.

Dokladem může být případ, kdy oběť jako řešení této situace zvolila sebevraždu. Pět spolužáků podrobilo Annu před celou třídou sexuální šikaně (strhali z ní šaty a předstírali, že ji znásilňují). Celou scénu nahráli na mobil a vyhrožovali dívce, že nahrávku zveřejní na internetu. To také později udělali, video umístili na stránku YouTube. Pro Annu to měla být pomsta za to, že s jedním z chlapců nechtěla chodit. Důsledek: Anna spáchala sebevraždu.

- *Kyberšikana je nebezpečný jev, který může vést k psychické újmě. Nepodceňujte ji!*
- *Účinnou obranou bývá pomoc kolektivu v podobě pasivity či odsouzení jednání útočníka.*
- *Útočníkem i obětí se může stát kdokoliv.*

Kybergrooming

Jev, který spočívá ve vylákání oběti na osobní schůzku. Nejedná se však o běžnou schůzku, ale o skutečně nebezpečné jednání s cílem ublížit či zneužít oběť. Útočníci často používají lsti, psychického nátlaku, falešné identity, vlídného až podbízivého chování, uplácení, atd. s cílem se s obětí osobně setkat.

Proto by se člověk neměl setkávat s cizími lidmi z Internetu. A pokud ano, tak na veřejném místě v rozumnou denní dobu. Minimalizovat tak riziko fyzického napadení. Nenechávat si nic jen pro sebe. Svěřit se někomu s tím, že mám schůzku a kde. Zde jsou nejrizikovější skupinou mladé dívky.

Rodiče by měli mít přehled, kde a s kým jejich dítě tráví volný čas. Útočník totiž často zjišťuje, zda má dítě oba rodiče, sourozence, zda je v pokoji samo, jestli má nějaké problémy, jestli je má s kým řešit a podobně. Tím se dostává do jeho přízně a zvyšuje pravděpodobnost osobního setkání.

Příkladem může být skutečný případ, v němž usvědčený deviant Pavel H. (vrátný v tiskárnách) využíval k seznamování se s oběťmi diskusní fóra, chat či inzeráty. Předstíral, že vybírá děti z dětských domovů do soutěže Dítě VIP apod. Osobní informace a fotografie, které od dětí získal, pak použil k vydírání. Kombinací vydírání a uplácení přiměl některé děti k osobní schůzce. Důsledek: Znásilňování a zneužívání 20 chlapců. Byl uvězněn na 8 let.

- *V případě žádosti o osobní schůzku dbejte zvýšené opatrnosti při komunikaci a pokud si nejste jisti, na schůzku nechoďte.*
- *Případnou schůzku uskutečněte v rozumnou denní dobu, na veřejném místě a někomu o ní řekněte.*
- *Mluvte s vašimi dětmi o jejich problémech a snažte se mít přehled kde a s kým tráví volný čas.*

Kyberstalking

Jedná se o nebezpečné pronásledování, špehování a obtěžování na Internetu nebo prostřednictvím mobilního telefonu. Útočník může, ale nemusí být anonymní. Jeho motivem je většinou touha až posedlost po své oběti. Zde jsou rizikovou skupinou ženy a slavné osobnosti. Pronásledovatel, kterého oběť ve skutečném světě odmítá, využívá Internetu či mobilu k tomu, aby ji byl blíž, kontaktoval se s ní, sbíral o ní informace, fotky a podobně. Takové jednání je obtěžující a často nahání strach.

Řešením je naprostá ignorace útočníka, změna návyků (obvyklá cesta do školy či práce, oblíbený obchod, profil na sociální síti, tel. číslo, e-mail, atd.) nebo se obrátit na policii.

- *Nereagujte na svého pronásledovatele, buďte vůči němu pasivní.*
- *Zkuste změnit své návyky (obvyklá cesta do školy či práce, oblíbený obchod, profil na sociální síti, atd.).*
- *Nebojte se situaci řešit a oznámit ji na polici.*

Sexting

Sexting je posílání zpráv a dat (fotky, videa) se sexuální tématikou, případně jejich vyžadování. Zde jsou rizikovou skupinou děti. Vzhledem k jejich věku si nedovedou dost dobře poradit s takovýmto jednáním. Útočník jedná se sexuálním motivem a nabízí oběti své erotické fotky či video, peníze nebo nějakou protislužbu. Požaduje vesměs erotické zprávy, fotky či video, společné focení či natáčení nebo sexuální kontakt.

- *Nikdy neposílejte nikomu cizímu své intimní fotografie či videa.*
- *Informujte své děti o nevhodnosti komunikace s cizími lidmi přes Internet na toto téma.*

Hoax

Tento nepříliš společensky nebezpečný jev spočívá v hromadném rozesílání poplašné zprávy. Děje se tak většinou pomocí e-mailu, jelikož oběť, která sdělení uvěří, ho okamžitě rozesílá dál všem lidem v adresáři.

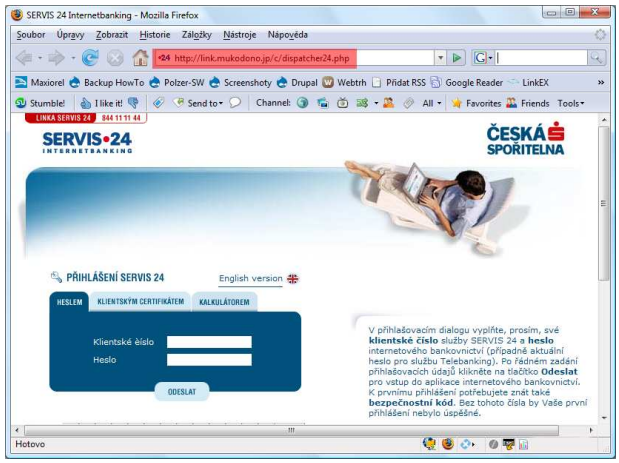
Hoax může mít podobu pomluvy, podvodu, lživé informace, nějakého apelu, atd. s cílem obelstít co nejvíce lidí. Jedinou obranou je zdravý rozum.

Příklady hoaxu:

- „Smažte win.exe z instalace Windows, je to virus."
- „Od 1.1. 2012 bude ICQ placené. Pokud jej chcete dále využívat zdarma, pošlete tuto zprávu dalším 15 lidem z vašeho seznamu kontaktů do jedné hodiny od obdržení této zprávy."
- „Pošli 100 korun na 5 adres, které jsou uvedeny na začátku dopisu. Přepiš dopis, na první místo napiš sebe, poslední adresu vynech. Pošli svým 5 přátelům. Brzo obdržíš obálky, ve kterých bude (pokud nikdo řetěz nepřeruší) 500+2500+12500+62500+312500 = 390 500,- Kč. Proto nepřerušuj řetěz."

- *Nevěřte všem informacím, které vám někdo pošle.*
- *Pokud si nejste jisti, zkuste si danou zprávu ověřit na serveru Hoax.cz, kde jsou kromě užitečných rad a informací evidovány známé hoax zprávy.*
- *V případě obdržení hoaxu informujte odesílatele, případně své známé o této skutečnosti.*

Phishing



Phishing je přesměrování uživatele na podvodnou stránku. Technických metod jak toho docílit je několik. Všechny vedou k tomu, že by si uživatel vůbec neměl všimnout toho, že je ve skutečnosti na jiné stránce, než si myslí.

Příkladem může být falešná stránka internetového bankovnictví Servis24. Ta může vypadat velmi podobně, jako ta skutečná. Návštěvník těchto stránek pak vyplní přihlašovací, osobní či jiné údaje a ty jsou odeslány na cizí server patřící podvodníkům. Takto ukradená data mohou být snadno zneužita.

Nejčastěji jsou tímto způsobem zneužívány internetové obchody, banky, platební systémy a podobně. Motivem tvůrců těchto podvodných stránek je totiž jednoznačně finanční zisk.

- *Zvýšenou pozornost věnujte internetovým obchodům, platebním systémům a bankám.*
- *Všímejte si případných rozdílů na internetové stránce. Varovným signálem může být cizí slovo v textu, špatná gramatika, jiné grafické rozložení stránky, žádost o nestandardní osobní údaje, podivná adresa ve stavovém řádku či použití nezabezpečeného spojení.*

Viry, spam a jiná havěť

Virus je počítačový program, který je uživateli skryt a jeho cílem je nějakým způsobem škodit. Rovněž má schopnost se šířit, ať už pomocí paměťových médií (flash disk, externí harddisk, atd.) či počítačových sítí. Účinnou obranou je antivirový program.

Počítači připojenému k Internetu hrozí ještě další nebezpečí, jako hackerský útok, mallware, spyware, atd. Nemá smysl se v tomto textu detailně zabývat touto problematikou. Obecně však platí, že dostatečnou obranou je kombinace antivirového programu, aktivního firewallu a aktualizovaného operačního systému.

Speciálním nástrojem k obraně proti spamu je antispamový filtr. Ten je ve většině e-mailových služeb aktivní na straně serveru. Eliminuje tak počet spamu ve vaší schránce.

- *Používejte antivirový program.*
- *Používejte legální operační systém a pravidelně ho aktualizujte.*
- *Vyhněte se pochybným a nebezpečným stránkám (porno, nelegální software, atd.)*

Trestně právní odpovědnost

Stejně jako v reálném světě, i na Internetu se lidé musí řídit určitými právními normami. Nelze se domnívat, že internetové prostředí je plně anonymní, nikdo o mě nemůže nic zjistit a já si tak mohu dělat, co chci. Policie ČR má dostatek technických prostředků k tomu, aby lokalizovala a monitorovala činnost jakéhokoli pachatele trestného činu. Mnohdy si pachatelé ani neuvědomují, že se trestného činu dopouštějí, ovšem jak je známo, neznalost zákona neomlouvá.

Lidé se tak mohou stát pachateli např. těchto trestných činů:

Vydírání - §175 zákona č. 40/2009 Sb.

1. Kdo jinému násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo peněžitým trestem.

Nebezpečné pronásledování - §354 zákona č. 40/2009 Sb.

1. Kdo jiného dlouhodobě pronásleduje tím, že
    a. vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým
    b. vyhledává jeho osobní blízkost nebo jej sleduje
    c. vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje
    d. omezuje jej v jeho obvyklém způsobu života
    e. zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu

    a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

Pomluva - §184 zákona č. 40/2009 Sb.

1. Kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán odnětím svobody až na jeden rok.
2. Odnětí svobody až na dvě léta nebo zákazem činnosti bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

Porušení tajemství dopravovaných zpráv - §182 zákona č. 40/2009 Sb.

1. Kdo úmyslně poruší tajemství
    b. datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo
    c. neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data

    bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti

Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí - §183 zákona č. 40/2009 Sb.

1. Kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Výroba a jiné nakládání s dětskou pornografií - §192 zákona č. 40/2009 Sb.

1. Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, bude potrestán odnětím svobody až na dva roky.
2. Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.
3. Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 2
    b. tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

Zneužití dítěte k výrobě pornografie - §193 zákona č. 40/2009 Sb.

1. Kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let.

Svádění k pohlavnímu styku

1. Kdo nabídne, slíbí nebo poskytne dítěti nebo jinému za pohlavní styk s dítětem, pohlavní sebeukájení dítěte, jeho obnažování nebo jiné srovnatelné chování za účelem pohlavního uspokojení úplatu, výhodu nebo prospěch, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem.
2. Odnětím svobody na šest měsíců až pět let bude pachatel potrestán
    a. spáchá-li čin uvedený v odstavci 1 na dítěti mladším patnácti let
    b. spáchá-li takový čin ze zvlášť zavrženíhodné pohnutky
    c. pokračuje-li v páchání takového činu po delší dobu, nebo
    d. spáchá-li takový čin opětovně.

Tento výčet trestných činů, platných k 1.3.2011, není samozřejmě úplný. Jedná se jen o ty nejčastější nebo nejzávažnější trestné činy, které se v elektronické komunikaci objevují.

Důležité je nebýt k těmto věcem lhostejní, účinně bránit sebe a své nejbližší a nebát se takové věci ohlásit na polici.

- *Pokud máte problém, svěřte se. Nebojte se spolupracovat s policí, pomůžete nejen sobě, ale i ostatním.*
- *Nebuďte lhostejní ke svému okolí a svým nejbližším.*

Jak zůstat na Internetu v bezpečí

Na závěr bych chtěl shrnout několik bezpečnostních rad a zásad, kterými když se uživatel Internetu bude řídit, bude relativně v bezpečí. Ona jedna věc je technické zabezpečení v podobě různých programů a nastavení, ale většinou tu hlavní roli v oblasti bezpečnosti hraje lidský faktor. To znamená mít dostatek informací o této problematice a zodpovědně přistupovat ke své bezpečnosti.

1. Chraňte si svou identitu a pokud možno buďte anonymní
2. Chraňte svá osobní data
3. Nevěřte cizím lidem na Internetu
4. Nesetkávejte se s nimi
5. Používejte „silná“ hesla
6. Udržujte svůj operační systém aktualizovaný
7. Používejte antivirový program
8. Nenavštěvujte stránky se závadným či pochybným obsahem (nelegální software, pornografie, atd.)