

Slovník pojmů online bezpečnosti

Kyberprostor

- kyberprostor = virtuální svět vytvářený moderními technologiemi (počítači, Internetem, mobilními telefony apod.), oproti světu „reálnému“
- digitální domorodci/přistěhovalci = termínem „digitální domorodci“ se dnes zpravidla označují mladí uživatelé online technologií, kteří jsou připojeni takřka nonstop, s technologiemi běžně pracují a využívají je k řešení každodenních problémů a vzájemné komunikaci. Zpravidla bývají vybaveni nejmodernější technikou. „Digitálními přistěhovalci“ se zpravidla označují uživatelé, kteří se s moderními technologiemi učí pracovat a vyžívat je k činnostem, které dříve realizovali standardními metodami. Často mají z využívání technologií větší obavy, přechod do světa online pro ně není tak snadný a v jeho prostředí se zdaleka nepohybují s takovou jistotou, jako digitální domorodci.
- botnet = internetový robot, často tak označována síť infikovaných počítačů řízených z jednoho centra a využívaná internetovými škůdci k útokům na webové stránky, označovaným DOS
- troll = účastník internetové diskuze, jehož cílem je vyvolat hádku; reaguje kontroverzně, napadá ostatní účastníky diskuze
- počítačová kriminalita, kybernetická kriminalita, kybernalita = zneužití informačních technologií k činnostem v rozporu se zákonem; šíření dětské pornografie, šíření a prodej nelegálních kopií komerčních programů, filmů a hudby, cílené útoky zaměřené na krádeže databází, odcizení přístupových hesel k elektronickému bankovníctví za účelem odčerpání peněz z účtů poškozených uživatelů, útoky vedoucí k odstavení webových stránek, šíření extrémistického a hanobícího obsahu apod.
- facebook = nejrozšířenější sociální síť, určená ke vzájemnému propojování uživatelů a jejich komunikaci, odhaduje se, že v červnu 2013 mělo v jejím prostředí profil 3 900 000 českých uživatelů
- twitter = sociální síť, určená je sdílení krátkých informací, pocitů, zkušeností, zážitků, často s odkazem na jiné internetové zdroje. Zpráva v prostředí Twitteru, tzv. tweet., je omezena svou délkou.
- sociální síť = internetová aplikace, sdružující uživatele za účelem vzájemné komunikace. Nejznámějšími příklady sociálních sítí jsou Facebook, Google+, Lidé.cz nebo např. Spolužáci.cz.
- komunikátor = program určený pro online komunikaci

- instant messenger = program určený k okamžité a rychlé online komunikaci, např. ICQ, Skype, Microsoft live messenger
- závislost na internetu = stav psychické závislosti, vedoucí k nutkavému používání internetu. Závislý jedinec musí být neustále online, neustále kontroluje stav svých profilů na sociálních sítích, komunikaci prostřednictvím komunikátorů nebo instant messengerů, obsah e-mailové schránky apod. Zpravidla si nedokáže představit stav, kdy by byl offline a nacházel se v prostředí/situaci bez možnosti připojení k internetu. V takové situaci je nervózní, nedokáže se soustředit a vykonávat jiné činnosti.

Kyberšikana

- kyberšikana = chování, jehož záměrem je ublížit, ohrozit nebo zastrašovat žáka, případně skupinu žáků prostřednictvím elektronických prostředků
- kyberstalking = pronásledování prostřednictvím online a mobilních technologií
- bullycide (bullying - depression - suicide)
<http://www.youtube.com/watch?v=rn4w8kgIX1g&feature=g-vrec&context=G2d31748RVAAAAAAAAAAw>
- happy slapping = náhlý nečekaný útok na nic netušící oběť, zpravidla útočníky natočený a umístěný na internet
- falešný profil = profil obsahující nepravdivé údaje o svém uživateli (zpravidla věk a pohlaví)
- krádež účtu = ovládnutí účtu jiným uživatelem zpravidla za účelem škodlivé a nelegální činnosti (pomluvy, hanobení, cílené útoky na jiné uživatele apod.)

Kybergrooming

- kybergrooming = cílená snaha některých uživatelů internetu (tzv. kybergroomerů) kontaktovat zpravidla v prostředí sociálních sítí mladé uživatele a děti a manipulovat jimi komunikativními metodami za účelem jejich vylákání na schůzku v reálném světě a jejich potenciálnímu zneužití. Kybergrooming je jedním z velmi nebezpečných projevů škodlivého chování v prostředí online, vedoucí k fatálním následkům.
- pedofilie ve vztahu ke kybergroomingu = jednou z nejvíce nebezpečných skupin kybergroomerů jsou deviantní pedofilové, jejichž cílem s využitím prostředků groomingu vylákat na schůzku v reálném světě děti a poté je zneužít. Groomeři bývají často velmi inteligentní lidé s vypracovanými metodami, které jsou pro ostatní uživatele s menšími sociálními zkušenostmi snadno uvěřitelné.

Nezákonný obsah

- pornografie = neumělecké znázornění lidského těla nebo sexuálního chování za účelem podněcování sexuálního pudu
 - dětská pornografie = pornografické materiály, jejichž objekty jsou děti
 - extremismus = jednání, ideologie či skupiny mimo hlavní (střední) proud společnosti, kterým je připisováno porušování či neuznávání základních etických, právních a jiných důležitých společenských standardů, zejména ve spojení s verbální nebo fyzickou agresivitou, násilím nebo hrozbou násilí
 - proana weby = webové stránky, nabádající k anorexii, která ve svém důsledku může vést k sebepoškození
 - promia weby = webové stránky nabádající k sebepoškození, především bulimii

Ochrana osobních údajů a osobnosti v online komunikaci

- IP adresa = číslo, které identifikuje počítač zapojený v počítačové síti. Zkratka IP znamená internetový protokol, což je forma komunikace zařízení zapojených do internetového prostředí
- MAC adresa = jde o jedinečný identifikátor síťového zařízení, MAC adresa je přidělena výrobcem a celosvětově jedinečná
- bot = program vykonávající automaticky různé jednoduché operace. Může jít např. o profil na sociální síti řízený počítačem, který se vydává za reálnou osobu s cílem získat o uživateli co nejvíce informací, nebo třeba o program rozesílající z e-mailové adresy uživatele bez jeho vědomí spam
- Server = v podstatě počítač poskytující nějaké služby. Může jít o služby lokální (např. obsluha tiskárny) nebo v prostředí sítě (na internetu či v rámci lokální sítě, např. školní): např. správa webových stránek nebo emailů.
- Pharming = využití špatně „přeložené“ IP adresy. Při zadání webové adresy je uživatel nasměrován na podvodný web vydávající se za pravý (např. vstupní stránka k internetovému bankovníctví).
- Phishing = snaha získat dále zneužitelné údaje o oběti (heslo, číslo kreditní karty atp.), nejčastěji formou e-mailu z „důvěryhodného“ zdroje. Např. jakoby žádost banky o zadání hesla k elektronickému bankovníctví kvůli údajnému restartování systému. Vzhledem k velkému počtu oslovených uživatelů se obvykle někdo „chytí“ a údaje zadá

- Spyware = program, který z počítače samotného uživatele monitoruje jeho činnost (vč. např. zadání hesla) a odesílá o ní zprávy. Mnohdy nevědomě nainstalován samotným uživatelem jako skrytá součást jiného programu
- Nigerijské dopisy = podvodné e-maily obvykle přislubující velkou finanční částku výměnou za malou zálohu ze strany adresáta (nebo třeba za poskytnutí jeho čísla účtu)

Autorská práva a internet

- peer to peer síť = typ počítačových sítí, kdy spolu komunikují přímo jednotliví klienti (uživatelé), někdy bývá také označována jako klient-klient. Nejčastějším obsahem, vyměňovaným přes tento typ sítí, bývají audio nahrávky, filmy a počítačové programy
- softwarový pirát = uživatel, který využívá nelegální kopie komerčních programů, šíří je,
- warez = v počítačovém slangu jde o autorská díla, se kterými se nakládá nelegálně, především jde o počítačové programy, hry a filmy. Nejčastějším prostředím pro šíření warezu je internet.
- cracky/záplaty = crack je malý program, který slouží k odstraňování ochranných prvků jiných programů za účelem jejich nelegálního používání či šíření. Jde o činnost ve většině zemí nezákonnou. Záplatou je zpravidla označováno softwarové vylepšení, které by mělo odstraňovat chyby předchozí verze softwaru. Často se hovoří o bezpečnostních záplatách, které odstraňují chyby operačního systému Windows anebo internetových prohlížečů.

Technické nástroje online bezpečnosti

- blacklist = v informatice jde o seznam obsahující zakázané položky, zpravidla adresy odesílatelů, od kterých nechceme přijímat zprávy, uživatelů, se kterými nechceme komunikovat prostřednictvím instant messagingu, internetových stránek, které by neměl prohlížeč zobrazovat atd.
- whitelist = seznam položek, které mají zvláštní privilegia, např. doporučené služby, internetové stránky, seznam odesílatelů e-mailů, od kterých nikdy nepříjde nevyžádaná pošta atd.
- rodičovská kontrola = jde o službu filtrace počítačového/internetového prostředí a monitoring jeho provozu při využívání dětmi. Prostřednictvím nástrojů rodičovské kontroly lze např. nastavit blacklist (seznam blokových) internetových stránek, na které děti nemají přístup, filtraci webových stránek, které obsahují klíčová slova (např. sex, porno atd.), sledování aktivit dětí v internetovém prostředí (seznam navštívených webů, délku pobytu na jednotlivých stránkách apod.).