

Slovníček pojmů

**Přiblížte se virtuálnímu světu a
proniknete do IT terminologie**



KRAJSKÉ ŘEDITELSTVÍ POLICIE
Jižní Moravského kraje

A

Adware - druh škodlivého software či viru, který obtěžuje uživatele reklamním sdělením, ať už ve formě banneru, pop-up (vyskakovacího) okna, vkládáním inzerátů do webových stránek či nedovolenou změnou domovské stránky v prohlížeči.

Anonymizér - software nebo webová stránka (také proxy server), umožňující změnit IP adresu počítače na výstupu a vydávat se tak za někoho jiného.

Anonymní email - anonymní "fake" email je emailová zpráva, které byla poměněna hlavička, takže se tváří, že odesílatel je někdo jiný. Tyto emaily stačí jen otevřít a mohou spustit škodlivý kód.

Antivirus - program, který slouží k zabezpečení počítače proti virovým hrozbám, k odhalení, eliminaci a k odstranění počítačových virů.

B

Blacklist (černá listina) – soupis těch, kterým byl z nějakého důvodu odmítnut přístup, nebo byla odmítnuta nějaká služba.

Baiting - může být považován za trojského koně v reálném světě.

Při tomto způsobu útoku útočník nechá infikované CD, flashdisk nebo jiné paměťové médium na místě. Poté již nechá pracovat zvědavost, se kterou oběť dříve či později vloží toto médium do svého počítače. Tím dojde k instalaci viru, za pomoci kterého získá útočník přístup k počítači nebo celé firemní počítačové síti.

Blog – webová aplikace obsahující příspěvky jednoho editora na jedné webové stránce. Autor se nazývá bloger.

Botnet - nepozorované napadení počítače a jeho zapojení do sítě tisíců počítačů ovládaných na dálku. Botnet pomocí jednoho příkazu ovládá všechny tyto počítače najednou. Nejčastěji jsou tyto roboty využívány k rozesílání spamu, získávání hesel a pinů, apod.

C

Cracking - činnost, při které cracker modifikuje aplikaci tak, aby obešel její omezení nebo zabezpečení. Jedná se VŽDY o ilegální aktivitu.

Cracker – osoba snažící se o neautorizovaný a nezákonný vstup do počítače a jeho následné ovládnutí, nebo o zcizení uložených informací.

Crackovat, cracknout – nezákonně se vloupat do počítače, obvykle za účelem zcizení či zničení dat, případně zamezení přístupu k systému ostatním uživatelům.

Cyberbullying - viz kyberšikana

Cyber grooming - viz kybegrooming

Cyber stalking - zneužití ICT k pronásledování oběti. Od 1. ledna 2010 je v ČR trestným činem. Jde o opakované a intenzivní obtěžování různým způsobem (sms, e-maily, kontaktování přes soc. sítě atd.).

Č

Četnout, četovat – komunikovat prostřednictvím chatu.

Čekovat – sledovat někoho ve virtuálním světě.

D

DDoS (distribuované odmítnutí služby) - útok na webovou stránku nebo jiný síťový zdroj, při kterém velké seskupení počítačů vyřadí stránku z provozu tím, že ji přetíží zbytečnými žádostmi.

Dox - "Doxovat" znamená zjišťovat něčí osobní údaje, jako jsou například skutečné jméno, telefonní číslo nebo adresa domů, a to obvykle pomocí sociálního inženýrství nebo vyhledávání na Googlu. Získané informace pak představují "dox" dané osoby.

F

Facebook - sociální síť sloužící k virtuální komunikaci mezi uživateli, sdílení dat.

Firewall – síťový prvek sloužící k řízení a filtrování komunikace mezi sítěmi a ke kontrole jejich důvěryhodnosti. Umožňuje filtrování probíhající komunikace a blokování nežádoucích přístupů.

Flaming (flame = hořet) - termín, označující nepřátelské chování uživatelů na Internetu, které obvykle doprovází urážky, nadávky, vyhrožování apod. Snaha vyprovokovat hádku.

Flaming se projevuje tak, že flamer = útočník opakovaně umísťuje urážlivé vzkazy do diskusních fór a následně stupňuje své útoky, přičemž ohnivě hájí své názory. Flamer útočí na toho, s jehož názory nesouhlasí, nepoužívá však propracovanou argumentaci, ale jednoduše nadává, uráží, vyhrožuje.

Flickr – komunitní web, díky kterému může uživatel zveřejňovat a sdílet fotografie.

FoMO syndrom – z anglického „fear of missing out“, tedy strach z toho, že něco zmeškáme,

propásneme ve virtuálním světě. Neustále chceme mít přehled o dění v prostředí sociálních sítí.

Freeware – software, kteří autoři bezplatně zpřístupnili uživatelům.

H

Hacker – někdo, kdo napadá počítačové systémy, nelegálně kopíruje data, píše viry, zneužívá chyby nebo neznalosti ostatních.

Hackovat, hackování – původně tento pojem znamenal rychlé napsání počítačového programu k určitému omezenému účelu, avšak jeho význam se postupem času vyvíjel. Pod tímto pojmem se stále častěji označuje vloupávání se do počítačových systémů s nekalými úmysly – této

činnosti lépe odpovídají pojmy CRACKOVAT, CRACKOVÁNÍ.

Happy Slapping - „spokojené fackování“. Nečekané fyzické napadení je nahráváno agresory na mobilní telefon nebo kameru. Ataky se vyznačují nebývalou zákeřností, která je hnána touhou získat co nejvíce šokující agresivní a „obdivuhodné“ video. Obětí bývá nahodilý i známý člověk, avšak útok je iniciován zcela záměrně a nečekaně, nejčastěji zezadu a ve skupině. Získanou nahrávku umístí na web jako další dobrý úlovek.

Hate Site – webová stránka, která podněcuje nenávist, většinou vůči určité rase, sexuální orientaci či náboženství.

Hoax – šíření poplašných, nebezpečných a zbytečných řetězových zpráv. Jako hoax můžeme také označit šířenou zprávu, která obsahuje nepřesné, zkreslující informace, účelově upravené polopravdy nebo směsku polopravd a lží.

V praxi můžeme použít následující pravidlo:

Jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to podezřelé a s největší pravděpodobností jde o HOAX. Pokud podobnou zprávu obdržíte a nemáte jistotu, můžete si prohlédnout některý ze seznamů HOAXů a potvrdit si skutečnost, že jde o hoax (www.hoax.cz).

CH

Chat – je komunikace nebo rozhovor dvou nebo více lidí prostřednictvím komunikační sítě. Uskutečňuje se vždy v reálném čase.

I

ICQ (I seek you [aj sík jů]) - neboli Hledám tě. Jde o jeden z nejužívanějších programů IM. Funkce

programu ICQ zahrnují posílání textových zpráv, offline posílání zpráv, skupinové chatování, odesílání SMS zpráv, odesílání souborů a hry pro více hráčů provozované pomocí technologie Flash.

ICT – informační a komunikační technologie, zahrnují veškeré informační technologie používané pro komunikaci a práci s informacemi. ICT ovšem nejsou jen hardwarové prvky (počítače, servery...), ale také softwarové vybavení (operační systémy, síťové protokoly, internetové vyhledávače...).

IM – zkratka Instant Messaging. Jedná se o internetovou službu, díky níž můžeme sledovat, který z našich přátel a známých je zrovna on-line. Služba umožňuje v reálném čase zasílat zprávy a soubory, většina programů IM poskytuje i možnost (video)hovorů. Programy IM jsou velmi špatně zabezpečeny, proto byste skrze ně neměli posílat citlivé informace, např. hesla, čísla platebních karet, PINy apod.

IP adresa - unikátní číslo přiřazené každému zařízení, které se připojí k počítačové síti nebo internetu. Každá IP adresa sestává ze čtyř čísel (až třicetiferných) oddělených tečkami. IP je zkratka pro "internetový protokol".

IRC (Internet Relay Chat) – dílčí síť internetu, na níž může velký počet účastníků vést v reálném čase rozhovory v onlinových „chatovacích místnostech“ rozdělených podle zájmových činností.

IVR - telefonní phishing. Tato technika využívá falešného hlasového automatu (IVR) s podobnou strukturou jako má originální bankovní automat ("Pro změnu hesla stiskněte 1, pro spojení s bankovním poradcem stiskněte 2"). Oběť je většinou vyzvána emailem k zavolání do banky za účelem ověření informace. Zde je pak požadováno přihlášení za pomoci PINu nebo hesla. Některé automaty následně přenesou oběť do kontaktu s útočníkem vystupujícího v roli telefonního

bankovního poradce, což mu umožňuje další možnosti otázek.

K

Krádež identity - nedovolené shromažďování a používání osobních údajů, obvykle za účelem kriminální činnosti. Útočníci mohou využít například vaše uživatelské jméno, heslo, datum narození apod.

Kybergrooming – agresor se vydává za někoho jiného s cílem získat důvěru dítěte a následně jej pozve pod záminkou na osobní schůzku, kde může dojít k násilné trestné činnosti.

Kyberšikana (Cyber bullying) – je druh klasické šikany, která se děje prostřednictvím elektronických prostředků. Nejčastěji se projevuje posíláním urážlivých a zastrašujících e-mailů nebo sms zpráv, vytvářením internetových stránek

(blogů), které nějakým způsobem ubližují ostatním, nebo nahráváním a publikováním ponižujících videí. Právě poslední příklad bývá nejnebezpečnější, protože je v současné době velmi populární, a jde často ruku v ruce s klasickou šikanou. Účinek této formy šikany je navíc umocněn obrovskou velikostí internetu, takže oběť můžou vidět i desetitisíce (ne-li statisíce) lidí.

Kybersex – on-line komunikace za účelem sexuálního vzrušení. Často se za kybesex považuje i vzájemné posílání zpráv se sexuálním obsahem.

L

Lama – uživatel s hloupým jednáním.

Loudnout – nahrát.

M

Malware - škodlivý software, který napadá počítač a často je chybně označován jako vir.

Mem - průpovídka nebo obrázek, které se díky virální povaze internetu dostalo neočekávané popularity a jejíž význam nezasvěceným uživatelům internetu zpravidla uniká.

MMS – zkratka z anglického Multimedia Messaging Service. Multimediální zprávy, hovorově ememesky, obsahují kromě psaného textu také obrázky, zvuk či video. Posílat je můžeme mezi mobilními telefony, z mobilu na e-mail, popř. z internetu na mobil.

Mobbing – představuje šikanu, psychický teror nejen mezi dětmi, ale i mezi dospělými, například v zaměstnání.

MUD (Multiuser Domain, Multiuser Dimension nebo Multiuser Dungeons) – dílčí síť IRS, jejíž

účastníci hrají v reálném čase hry nebo provádějí simulované činnosti.

MySpace – komunitní server, kde uživatelé mohou mezi sebou komunikovat.

N

Netolismus – chorobná závislost na internetu.

Nigerijské dopisy - nebezpečná forma sociálního inženýrství, kde pachatelé (většinou z Nigérie a jižních zemí) komunikují s uživatelem, který např. něco prodává pomocí inzerátu. Pachatelé z něj podvodně získají peníze a přestanou komunikovat.

Nomofobie – chorobná závislost na mobilním telefonu

O

OP - zkratka pro „original poster“, volně přeloženo jako "zakladatel diskuse". Jde o osobu, která na internetovém fóru zahájila určitou diskusi.

Outing – zasílání materiálů o oběti, které obsahují její citlivé, osobní nebo zostuzující informace. Patří sem i přeposílání soukromých zpráv a fotek (např. veřejné oznámení něčí homosexuální orientace bez souhlasu nebo proti vůli této osoby).

P

Pager – rozměry velmi malé telekomunikační zařízení, které umožňuje přijímat krátké textové nebo číselné zprávy. Funguje jednosměrně, zprávy můžete na pager pouze přijímat, nikoli odesílat.

V České republice nejsou pagery mezi širokou populací moc rozšířené.

Paket – malý řetězec digitalizovaných dat. Veškeré informace přenášené přes internet – e-maily, text, hudby, obrázky, grafika, zvuky – se rozdělují do paketů, které se u příjemce následně skládají do použitelného stavu.

Packet – sniffer – program zavedený do počítačového SMĚŘOVAČE, SERVERU nebo koncového počítače za účelem přesměrování PAKETŮ do počítače třetí strany, obvykle s cílem nezákonně číst uživatelské vzkazy nebo zjišťovat přístupové kódy a další informace.

Pejdžina – webová stránka

Pharming - je podobně jako phishing podvodná aktivita, která se snaží vylákat z lidí přístupová jména a hesla, je však mnohem zákeřnější. Pharming se nejčastěji zaměřuje na internetová bankovníctví. Útočníci vytvoří stránky, které se

tváří jako reálné stránky banky, ale ve skutečnosti se jedná o jejich kopii sloužící pouze ke sklizení přihlašovacích údajů, jejichž pomocí se pak mohou přihlásit a převést z napadených útočníků neomezené finanční částky. Technicky to vypadá tak, že útočníci napadnou špatně zabezpečený DNS sever, změní IP adresu URL odkazu internetové banky, přesměrují jej na falešné stránky a nebezpečí je na světě.

Phishing a Pharming - krádež citlivých osobních údajů. Phishing a pharming představují nástroje internetových pirátů, kteří se s jejich pomocí mohou dostat k přístupovým heslům internetového bankovníctví nebo k PIN kódům vašich platebních karet.

Slovem phishing označujeme podvodné e-mailové zprávy, které mají vzbudit dojem, že byly odeslány z e-mailové adresy vaší banky. Zpráva může být psána špatnou češtinou nebo je v angličtině, obsahuje link, tedy propojení na údajné stránky

banky a vyzývá k potvrzení osobních bankovních údajů. Cílem podvodného e-mailu může být získání přihlašovacích údajů k internetovému bankovníctví, PIN kódů platebních karet nebo dalších bezpečnostních údajů a jejich následné zneužití. Podobně se mohou podvodníci snažit získat přístupové údaje k elektronickým peněženkám pro obchodování na internetu (PayPal, eBay, Paysec).

Phreak – osoba provádějící PHREAKOVÁNÍ.

Phreakování – vloupávání se do telefonních systémů, převážně za účelem vedení bezplatných rozhovorů, odposlouchávání nebo narušování telefonních služeb.

Počítačový červ - program, který se dokáže sám šířit a pomocí počítačových sítí zasílá kopie sebe sama do dalších uzlů. K procesu šíření většinou nepotřebuje uživatele, stačí mu využít bezpečnostní chyby v programu, kterou poté zneužije k vniknutí do cizího počítače. Počítačový

červ funguje jako samostatná jednotka a samostatný proces, čímž se liší od viru. Červ díky svojí povaze přenosu často způsobuje zahlcení a neprůchodnost sítě.

Pornografie - vizuální materiály (knihy, časopisy, videa apod.), které jsou vytvořeny za účelem sexuálního vzrušení. V určitých případech se v této souvislosti jedná o protiprávní jednání (Šíření pornografie, Výroba a jiné nakládání s dětskou pornografií, Zneužití dítěte k výrobě pornografie).

Pretexting - utváření a využívání vymyšleného scénáře s cílem přesvědčit oběť k učinění potřebné akce nebo k získání potřebné informace. Jedná se o skloubení lži s kouskem pravdivé informace získané dříve. Může se jednat například o datum narození, rodné číslo, velikost posledního účtu, jméno nadřízeného atd. Cílem je přesvědčit oběť o legitimnosti akce, která je po ní požadována.

Profil – v současné době je tento výraz nejčastěji používán v souvislosti s profily na sociálních sítích. Každý člověk si může založit na sociálních sítích svůj účet, nahrát si do něj své fotografie a videa, napsat o sobě prakticky cokoli – své koníčky, zájmy, kontaktní údaje, názory na svět, s kým kamarádí apod.

S

Server – velký a výkonný počítač na určité síti, na němž jsou uložena data, webové stránky i soubory a k němuž mají uživatelé přístup.

Sexting - termínem sextingu (česky ekvivalent by zněl sextování) označujeme elektronické rozesílání zpráv, obrázků a videí se sexuálním obsahem. Nejčastěji tyto materiály vznikají v rámci partnerských vztahů, jejich pořízení nás uvádí do nebezpečí, že budou zveřejněny a šířeny bez

našeho vědomí internetem či pomocí mobilních telefonů. Podle jediného českého serveru sexting.cz, který se zabývá výhradně problematikou sextingu, skýtá tento nový fenomén několik druhů rizikového chování.

Shareware – software propůjčený tvůrcem za jednorázový poplatek nebo k omezenému použití.

Shell - softwarové rozhraní, které čte a vykonává příkazy. U špatně zabezpečených webových stránek se hacker může skrze administrační ovládací panel dostat až k shellu serveru, na němž jsou stránky hostovány, a jeho prostřednictvím pak server ovládat.

Skimming - činnost, jejímž výsledkem jsou padělané platební a kreditní karty. Pachatelé kopírují údaje z magnetického proužku platební karty a na základě získaných dat vytvářejí jejich

plagiáty. Kopírování probíhá ve vybraných napadených bankomatech.

Skript (software) – relativně jednoduchý počítačový program. Skripty se často používají k automatizaci různých úkonů.

Skype – komunikační program oblíbený především pro možnost telefonování z počítače na počítač zdarma. Můžete však volat i na pevné linky nebo mobilní telefony (služba SkypeOut) a naopak (služba SkypeIn). Nelze se však dovolat na linky tísňového volání. Skype dále umožňuje služby IM, tedy přenos zpráv a souborů v reálném čase.

SMS – zkratka z anglického Short Message Service. Krátká textová zpráva, hovorově též textovka či esemeska. SMS se nejčastěji posílají mezi dvěma mobilními telefony, lze je ale zaslat i na moderní přístroje pevné linky, posílat se mohou i z internetu.

SMS Spoofing - falešné SMS, odeslané z jiného telefonního čísla. Využívá krátkých textových zpráv (SMS), je k dispozici na většině mobilních telefonů a osobních digitálních asistentů. Spoofing má dvě použití: 1) legitimní: nastavení názvu firmy, ze které je zpráva zaslána, nastavení vlastního čísla, nebo název produktu a 2) nelegitimní: např. vydávání se za jinou osobu, firmu, produkt.

Sociální inženýrství - je strategie, která využívá lidského faktoru jako nejslabšího článku v informačních technologiích. Pomocí sociálního inženýrství se získávají důležité informace od uživatelů, aniž by o tom věděli.

Sociální síť – v původním významu jakákoli společenská síť, komunita lidí, kde se tvoří vztahy přátelské, sousedské, pracovní apod. V dnešní době jsou tímto pojmem označovány především internetové sociální sítě, které tvoří nový a čím dál více populární druh komunikačního kanálu. Mezi

nejznámější patří Facebook, YouTube, Instagram, Snapchat, MySpace, Twitter apod.

Spam - nevyžádané sdělení (nejčastěji reklamní) masově šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging.

Spyware - obdobně jako počítačový červ využívá ke své instalaci bezpečnostní díru počítače. Úkolem tohoto ilegálního softwaru je monitorování aktivit uživatele a poté odeslání informací svému autorovi. Informace o uživateli jsou využívány k cílení reklamy na uživatele nebo k odposlechu hesel.

SQL injekce - tento termín, někdy též zkracován na SQLi, značí metodu útoku, při které hacker získá přístup do databáze zranitelných stránek tím, že jí podsuně podvodný příkaz. Tento příkaz se často dá poslat přes běžný webový formulář dostupný

i normálním uživatelům. Pomocí tohoto postupu může hacker získat i informace, jež měly řadovým uživatelům zůstat skryty.

T

Trashing - prohledávání se odpadky s cílem nalezení dokumentů s citlivými údaji, které je možné zneužít pro finanční nebo jiný zisk podvodníka.

Trojský kůň - škodlivý program, který po nainstalování umožňuje vzdálený přístup do napadeného počítače. Není snadné ho odhalit, protože se dokáže tvářit užitečně, například jako spořič obrazovky. Do počítače se dostane například jako příloha v e-mailu. Od počítačového viru se liší tím, že nedokáže sám sebe množit a infikovat tak další počítače.

Troll - člověk, snažící se vyvolat konflikt, rozvrátit diskusi apod. Troll často do diskuse zavádí témata, která nesouvisí s řešeným problémem. Například vulgarity, politická sdělení apod.

Twitter – mikrobloginovací systém sloužící k vyjádření názorů nebo sdílení prostřednictvím krátkých zpráv.

V

Vishing - podvodná technologie zneužívající Voice over Internet Protocol (VoIP) k získání citlivých osobních a finančních údajů za účelem zisku. Typický postup je takový, že podvodník nakonfiguruje vytáčení čísel, uživatel přijme hovor, ve kterém ho automatický záznamník upozorní například na podezřelou aktivitu s jeho účtem a odkáže ho na bezplatné telefonní číslo, asociované s telefonními čísly banky, za kterou se podvodník vydává. Na telefonním čísle se poté ozve počítačem generovaný hlas, který po uživateli

žádá číslo platební karty, PIN kódy a podobně. Tyto údaje pak podvodník samozřejmě neváhá použít ve svůj prospěch.

Video blog, zkráceně nazývaný **vlog**, je blog, při kterém se dotyčná osoba nevyjadřuje písemně, ale ústně, a zároveň při tom může točit sebe nebo své okolí. Natáčení vlogů je populární na platformě YouTube. Člověk, který při svém vyjadřování používá formu video blogu, je video blogger či vloger. Točit vlogy je pro lidi některé jednodušší než psát dlouhé odstavce; pro diváka bývá požitek z videa zase zábavnější. Mezi vlogy se můžou řadit různá instruktážní videa, humorná videa nebo pravidelné shrnutí novinek. Vlogy můžeme také nazývat dle pravidelnosti (například „denní vlog“).

VPN (virtuální soukromá síť) - síťová technologie, která přes internet poskytuje vzdálený a bezpečný přístup k síti prostřednictvím procesu zvaného "tunelování". Spousta organizací používá VPN k tomu, aby jejich zaměstnanci mohli pracovat

z domova a zároveň se bezpečně připojovat k centrální firemní síti.

W

Warez – nezákonně okopírovaný komerční software.

Whitelist – seznam povolených aktivit či adresátů. Lze vytvořit např. whitelist webových stránek, které mohou uživatelé internetu otevřít, nebo whitelist e-mailových adres (tedy seznam e-mailů, ze kterých nechodí spam).

Worm (červ) – program sloužící k infikování počítače a následně vykonání předem naprogramované činnosti.

Y

YouTube – internetový portál (www.youtube.com) s video obsahem, na který může každý člověk nahrát svá videa a sdílet je s lidmi na celém světě. Pod videi je možnost diskuze, do které může svůj názor na natočené video sdělit každý z nás.

Z

Zdrojový kód – soubor písmen, číslic a typografických symbolů, který programátor využívá k psaní softwaru v jednom nebo několika programovacích jazycích. Zdrojový kód se následně konvertuje ve strojový kód, s nímž počítač skutečně pracuje. Zdrojový kód je obvykle tajný a jeho tvůrce nebo vlastník ho bedlivě střeží.

Použité zdroje:

www.kr-jihomoravsky.cz/kyber

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN isbn978-80-7387-545-9.

Zkratky používané dětmi při komunikaci na sociálních sítích

Akronym	Anglický význam	Český překlad
2U	To You	Tobě
4U	For You	Pro tebe
4YEO	For You Eyes Only	Tajné, soukromé, jen pro tvé oči
2L8	Too Late	Pozdě
AFAIK	As Far As I Know	Pokud vím
ASAP	As Soon As Possible	Jakmile to bude možné
AYOR	At Your Own Risk	Na vlastní riziko
BB	Bay Bay	Čau čau
BBL/S	Be Back	Vrátím se

	Later/Soon	později/brzy
BTW	By The Way	Mimochodem
CU,CUS	See You	Ahoj (uvidíme se)
CU2	See You Too	Taky ahoj
CUS	See You Soon	Brzy na viděnou
DND	Do Not Disturb	Nerušit
DIY	Do It Yourself	Udělej si sám
FE	For Example	Například
FCI	Free Cool In	Frikulín, osoba, co je free-cool-in, zpravidla hanlivé)
FYI	For Your Information	Pro tvou informaci
GR8	Great	Paráda

GL	Good Luck	Hodně zdaru
GNSD	Good Night, Sweet Dreams	Dobrou noc, sladké sny
GTB/GS	Go Too Bed/Go sleep	Jdu do postele, jdu spát
HF	Have Fun	Bav se
IC	I See	Aha, chápu
IDK	I Don't Know	Nevím
IDGI	I Don't Get It	Nechápu
JFGI	Just Fucking Google It	Vygoogluj si to
K, OKI	OK	Ok
KISS	Keep It Short and Simple	Udělej to stručně a jednoduše
LMAO	Laughing	Smíchy se asi

	My Ass Off	znečistím
LOL	Laughing Out Loud	Směji se, až se za břicho popadám
L4	Looking For	Hledám
L8R	Later	Později
M2	Me Too	Já také
NP	No Problem	Žádný problém
NRN	No Reply Necessary	Odpověď není nutná
NT	Nice Try	Dobrý pokus
NVM	Never Mind	Nevadí
OMG	Oh My Got	Panebože
PEBKAC	Problem Exists Between Keyboard and Chair	Problém se nachází mezi židlí a klávesnicí
PLS	Please	Prosím
ROFL	Rolling On Floor	Válím se smíchy po

	Laughing	zemi
RTFM	Reead The Fucking Manual	Přečti si sakra ten návod
SNAFU	Situation normal, All Is Fucked Up	Situace je normální, všechno je v pytli
SRY	Sorry	Promiň
TGIF	Thanks God, Its Friday	Díky Bohu, že je pátek
THX	Thanks	Díky
U2	You Too	Ty taky, tobě taky
W8	Wait	počkej
WTF	What The Fuck	Co to sakra...
MOS	Mom over Shoulder	Máma za zády

Důležité kontakty a odkazy:

- www.rodicovskalinka.cz (840 111 234,
606 021 021)
- www.linkabezpeci.cz (116 111)
- www.stoponline.cz
- <http://www.kr-jihomoravsky.cz/kyber/>
- www.e-bezpeci.cz
- www.saferinternet.cz
- www.bezpecnyinternet.cz
- www.seznamsebezpecne.cz
- www.internetembezpecne.cz



KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

jihomoravský kraj

B | R | N | O