IT kriminalita

Celé téma volně ke stažení: IT kriminalita.pdf

Rozšiřování informačních a komunikačních technologií mezi širokou veřejnost s sebou přináší nové druhy kriminality. Se zvyšujícím se počtem uživatelů internetu a sociálních sítí zároveň narůstá počet hrozeb, které jsou stále sofistikovanější. Tomuto stavu napomáhá i skutečnost, že jsou uživatelé vystaveni obrovskému množství informací, aniž by měli schopnosti a dovednosti informace kriticky přehodnotit a zpracovat.

S využíváním informačních a komunikačních technologií jsou přímo spojeny hrozby počítačových podvodů, úniku a následného zneužití osobních dat, pomluv, pronásledování, vyhrožování, sexuálního nátlaku a mnoho dalších negativních aktivit. Z těchto důvodu je nutné být obezřetný a uvědomovat si všechny možná rizika, která s využívání moderních technologií souvisí.

Přehled kapitol:

Problematika sociálních sítí

Jakým způsobem využívat sociální sítě a na co si dát pozor z hlediska možného zneužití vašich osobních údajů? Na tyto otázky naleznete odpovědi v této kapitole.

NEJČASTĚJI POUŽÍVANÉ SOCIÁLNÍ SÍTĚ

V ČR je stále nejpoužívanější sociální sítí Facebook, dále s odstupem Twitter, Google +, Ask.fm, Tumblr, Instagram, Snapchat atd. Sociální sítě jsou atraktivní i tím, že často slouží jako první zdroj aktuálních informací, v mnohém nám komunikaci usnadňují (rychlá komunikace, možnost komunikovat kdykoli, snadná dostupnost), nesou s sebou však i některá negativa (ztráta soukromí, nepravdivé informace, rychlé šíření, anonymita, obtížná kontrola, vložený materiál zůstává na internetu napořád).

NEJVĚTŠÍ RIZIKA SOCIÁLNÍCH SÍTÍ

Nejzásadnějším rizikem při používání sociálních sítí je fakt, že cokoli na internet vložíte, zůstává tam v podstatě napořád a může být kdykoli zneužito. Tento důsledek si bohužel mnozí uživatelé vůbec neuvědomují.

Dalšími riziky jsou:

- zveřejňování osobních údajů,
- zveřejňování velkého množství obecných informací,
- komunikace s cizí osobou,
- osobní schůzka s cizí osobou.

Největším problémem na sociálních sítích je rizikové chování samotných uživatelů. Mnoho lidí o sobě zveřejňuje na sociálních sítích velké množství citlivých informací, komentářů, plánů, které by v reálném světě při rozhovoru s cizí osobou určitě nesdělili.

STALO SE: *Dvě studentky gymnázia si založily falešný profil na sociální síti a pod lživou záminkou vylákaly ze spolužačky intimní fotografie. Získaný materiál poté rozeslaly spolužákům a vyvěsily na internet. Všemu předcházela hádka mezi děvčaty.*

Nedostatečné zabezpečení profilu na sociální síti může vést k tomu, že se tam lehce dostane jiný uživatel a získané informace z profilu zneužije. Z profilu se o vás může zjistit téměř vše, včetně získání fotografií.

Z neopatrné komunikace může potenciální pachatel zjistit, kde budete na dovolené, kdy chodíte domů, kdy je dům prázdný a mnoho dalších informací, které zneužije pro svůj protizákonný záměr.

Falešný profil je další hrozba, která na internetu číhá. Mnoho uživatelů se skrývá pod falešnou identitou k páchání trestné činnosti. Vydávají se za někoho jiného z důvodu vylákání intimních fotografií, údajů k účtu nebo peněz samotných. Falešná identita často slouží i k navázání komunikace, získání důvěry a následnému vylákání na osobní schůzku.

JAK SE CHRÁNIT NA SOCIÁLNÍCH SÍTÍCH

Být či nebýt na sociálních sítích? Na tuto otázku si musí odpovědět každý sám. Pokud se rozhodnete založit si profil, myslete v první řadě na dostatečně kvalitní heslo, dále se důkladně seznamte s možnostmi nastavení a zabezpečení vašeho profilu, nepodceňujte obchodní a licenční podmínky služby a seznamte se s nimi.

Pečlivě hlídejte své soukromí (zvažujte výběr přátel a materiálu vkládaného na internet). Nesdělujte nikomu svá osobní data a citlivé údaje (rodné číslo, různá hesla, PIN kódy, údaje o svém zdravotním stavu apod.) ani v případě, že vás k tomu protější strana opakovaně vyzve. Vždy je nutné přemýšlet nad tím, s kým danou informaci sdílíte, jestli pouze se svými přáteli nebo jestli se k této informaci může dostat každý návštěvník vašeho profilu.

Nerozesílejte svým přátelům fotografie, mohou se dostat i k osobám, kterým byste je nikdy neposlali. Uvědomte si, že přehnaná informovanost o vašich aktivitách může být zneužita - každý ví, kdy a kde se právě nacházíte a co děláte. O bezpečném chování na sociálních sítích a možných rizicích poučte i své děti.

Pokud zjistíte, že vaše údaje byly zneužity, kontaktujte jak administrátora stránek (smazání informací), tak i policii (jako důkaz si zkopírujte a uložte závadný materiál).

***TIP:** K nahlášení problémového obsahu webových stránek lze využít i formulář pro hlášení závadového obsahu a aktivit v internetové síti (např.: http://aplikace.policie.cz/hotline/).*

Zpět na přehled kapitol

Rizika informačních technologií

Jak se vyznat v pojmech týkajících se počítačové kriminality a jak se bránit pokusům o podvod nebo zneužití vašich dat? Na tyto otázky naleznete odpovědi v této kapitole.

POJMY

Existuje mnoho pojmů, které souvisejí s počítačovou kriminalitou, příp. vyjadřují nežádoucí aktivity spojené s užíváním internetu:

- **spam** - zasílání nevyžádané elektronické pošty (často reklam) je jedním z nejčastějších obtěžujících aktivit, které kromě zahlcení vaší e-mailové schránky mohou skrývat úmyslně i neúmyslně také viry (např. v přílohách),
- **hoax** - poplašné nebo řetězové zprávy, vyzývající k rozesílání dalším adresátům, často mají senzační obsah nebo jsou na ně navázány petice proti nějakému jevu (zde hrozí snadné získání vaší e-mailové adresy k dalšímu rozesílání spamů),
- **phishing** a **pharming** - cílená snaha získat citlivé osobní údaje, např. přístup k vašemu internetovému bankovnictví pomocí odkazů na falešný web vaší banky (existuje i telefonická forma **voice phishing** - získávání údajů po telefonu),
- **malware** - počítačový program, který slouží ke vniknutí do počítačového systému nebo jeho poškození, představuje počítačové viry, trojské koně, spyware,
- **spyware** - ilegální software, který se automaticky nainstaluje do počítače uživatele a monitoruje jeho aktivitu, často s cílem odposlechu hesel,
- **SMS spoofing** - falešné SMS, které se tváří, že jsou odeslané z konkrétního telefonního čísla,
- **sociální inženýrství** - představuje prostředek k získání informací prostřednictvím vystupování pod falešnou identitou,
- **flaming** - úmyslné umisťování provokujících či urážlivých vzkazů nebo informací na internet s cílem někoho vyprovokovat k hádce.

JAK CHRÁNIT SEBE A SVŮJ POČÍTAČ

Stolní počítač, notebook, tablet i chytrý telefon mají přístup na internet a jsou tedy z hlediska počítačové kriminality zranitelné. I to nejlepší technické zabezpečení vašeho přístroje však musí být doplněno také zodpovědným chováním uživatele.

Základem ochrany je legální software v kombinaci s kvalitním antivirovým programem. Nezapomínejte na chytré telefony, i ty mohou být napadeny jako počítač a únik dat hrozí úplně stejně. Proto antivirový program použijte i na svůj chytrý telefon. Vždy také prověřujte externí zařízení, která k počítači připojujete přes USB (flash disk, externí disk apod.). Pokud obdržíte nečekanou poštu od neznámého odesílatele (často ze zahraničí), nereagujte na nabídky, neotvírejte přílohy, neklikejte na odkazy a nevolejte na uvedená telefonní čísla (možné viry, několikanásobně zvýšené poplatky za hovory). Podvodné maily mohou mít podobu žádosti o finanční pomoc, pomoc při převodu peněz, informace o neexistující exekuci, informace o vyzvednutí balíku na poště. Takový e-mail okamžitě odstraňte. Podezřelé e-maily poznáte často i podle toho, že je zde špatná čeština.

Řetězové (přeposílací) e-maily neposílejte dál přátelům, kromě zbytečného zahlcování e-mailové schránky jim můžete poslat nevědomky i virus a také předáváte ohromné množství e-mailových adres dále k dispozici. Informace v těchto typech e-mailů se nezakládají na pravdě, většinou mají ohromující ráz nebo se snaží dotknout citové oblasti (úžasné, opravdu to funguje, týrané zvířátko, nemocné dítě). Jedná se o hoax a jejich výčet můžete nalézt na www.hoax.cz. Pokud posíláte e-mail více různým příjemcům, využívejte funkci skrytého zobrazení adresátů („undisclosed recipients“), aby se dál zbytečně nešířily e-mailové adresy vašich známých.

Častým typem nevyžádaných e-mailů jsou komerční nabídky firem, u kterých jste např. v minulosti nakupovali přes e-shop. Solidní firmy vždy dávají možnost deaktivovat zasílání nevyžádaných e-mailů. Pokud to není možné automaticky, oslovte je přímo s žádostí o ukončení zasílání nevyžádané pošty. V případě, že i

nadále vám chodí takovéto nevyžádané e-maily, nastavte si ve svém emailovém klientovi filtraci zpráv, tak ať emaily z těchto adres rovnou padají do složky s nevyžádanou poštou.

***TIP:** Pokud vás často obtěžuje množství nevyžádané elektronické pošty, je možné si nechat nainstalovat specializovaný program k filtraci e-mailů.*

Buďte velmi opatrní při využívání elektronického bankovnictví. Nikdy do něj nevstupujte přes odkazy v mailu. Vždy jděte přes oficiální webové stránky vaší banky. V případě jakéhokoliv podezření se ujistěte u vaší banky, že je systém v pořádku a funkční. Pokud vás banka informuje např. e-mailem, že v určitou dobu bude elektronické bankovnictví nefunkční, ověřte si to na jejich webových stránkách. Pravidelně kontrolujte stav vašeho účtu a provedené platby, v případě neoprávněných manipulací ihned kontaktujte banku a policii.

Zpět na přehled kapitol

Kyberšikana

Co vše může být považováno za kyberšikanu a jak se proti ní bránit? Na tyto otázky naleznete odpovědi v této kapitole.

Kyberšikana je druh šikany, která využívá elektronické prostředky, jako jsou počítače, mobilní telefony, e-maily, internet apod. Její nejobvyklejší projevy představuje zasílání obtěžujících, urážejících či útočným e-mailů, SMS, průnik na účet, krádež identity, obtěžování prozváněním, publikování nejrůznějších fotografií, vydírání atd.

Formy kyberšikany:

- **cyberstalking** - opakované intenzivní obtěžování nebo zastrašování (prozvánění, telefonáty, e-maily),
- **cyber grooming** - chování, které v adresátovi vyvolá falešnou důvěru, následné pozvání na schůzku a zneužití,
- **sexting** - obtěžující rozesílání fotografií, videí a SMS se sexuálním obsahem,
- **happy slapping** - tzv. fackování pro zábavu je napadením nic netušící osoby se současným nahráváním a umístěním nahrávky na internet.

JAK PŘEDCHÁZET KYBERŠIKANĚ

Základní radou je obezřetnost při sdílení informací, zejména na sociálních sítích. Nepublikujte nic, co by mohlo být v budoucnu zneužitelné (např. choulostivé fotografie, osobní údaje, urážlivé komentáře apod.). Pečlivě si vybírejte své přátele, se kterými se o své zážitky a fotografie dělíte. Nebuďte přehnaně důvěřiví. Máte-li podezření na kyberšikanu vůči své osobě, projděte za pomoci nejběžnějších vyhledávačů údaje, které jsou o vás na internetu k dispozici.

JAK SE ZACHOVAT V PŘÍPADĚ KYBERŠIKANY

Pokud se stanete svědkem nebo obětí kyberšikany, je třeba okamžitě jednat. Když se nezačnete bránit, útočník bude s největší pravděpodobností své negativní chování vůči vám nebo vašim blízkým stupňovat.

Pokud pachatele neznáte, pokuste se co nejdříve ukončit s ním komunikaci (např. i za cenu zrušení telefonního čísla nebo profilu na sociálních sítích). Jde-li o nebezpečné chování, např. vydírání, vše si zdokumentujte a obraťte se na policii. Policie má možnosti odhalit pachatele pomocí „elektronických stop“ při používání e-mailu, telefonu nebo profilu na sociální síti. Je možné, že nejste sami a podobných postižených jedním pachatelem je více. V případě potřeby také můžete přes provozovatele nechat zablokovat účet na sociálních sítích nebo si vytvořit jako svou ochranu jinou virtuální identitu.

***TIP:** Jednou z možností, jak upozornit na nevhodný obsah na internetu, zejména týkajícího se zneužívání dětí (dětská kyberšikana a pornografie) je **Horká linka** (www.horkalinkaczi.cz), na kterou můžete anonymně nahlásit svůj nález.*

Pokud pachatele znáte, opět si zdokumentujte jeho činnost a upozorněte ho na to, že máte důkazy, které můžete předat policii, v případě dětí i rodičům nebo učitelům ve škole. V každém případě se útočníkovi vyhýbejte. Není-li to účinné, oznamte to policii.

Poté, co kyberšikana skončí, zkontrolujte si např. přes reverzní vyhledávače fotografií (např. prostřednictví vyhledavače Google), že na internetu nezůstalo nic, co by vás mohlo dále poškodit.

Zpět na přehled kapitol