15. Riziká informačných technológií – (Informačná spoločnosť)

Riziká informačných technológií

Informačná spoločnosť je spoločnosť, kde práca s informáciami a údajmi je každodennou záležitosťou. Na prácu s informáciami používame rôzne ***informačné a komunikačné technológie (IKT)***. Okrem nesporného kladného vplyvu IKT nastupujú aj riziká, ktoré prináša nasadenie týchto technológií. Tieto riziká môžeme rozdeliť do dvoch skupín:

1. **Sociálne riziká**
   a) Strata súkromia na webe.
   b) Reklama na webových stránkach.
   c) Jednoduchý prístup k nevhodným informáciám,
   d) Dôveryhodnosť, pravdivosť informácií na webe, Anonymita na webe.
   e) Kyberšikanovanie.
   f) Hry a gambling.
   g) Nevyžiadané e-maily – spamy, poplašné správy (hoax).

2. **Technologické riziká**
   a) Škodlivý softvér – malware (vírusy, trójske kone, počítačové červy, spyware, adware).
   b) Počítačová kriminalita - prienik do počítačového systému, počítačové bankové krádeže (phishing, pharming, spoofing), dialery.
   c) Počítačová bezpečnosť (prevencia, detekcia, náprava) - zabezpečenie a spôsoby ochrany (heslá, šifrovanie, prístupové práva), elektronický podpis (súkromný a verejný kľúč), firewall.

1. Sociálne riziká

Pod pojmom **sociálne riziká informačných technológií** chápeme negatívne vplyvy, ktoré nepriaznivo vplývajú na sociálny vývoj jednotlivca, na formovanie vzťahov jednotlivca k spoločnosti a vzťahy medzi jednotlivcami navzájom.

Do tejto kategórie môžeme zaradiť:

a) Strata súkromia na webe. Využívanie Internetu umožňuje jednotlivcom komunikovať s rôznymi ľuďmi, ktorých osobne ani nepoznáme, no mnohokrát ich dôveryhodné správanie znižuje našu mieru pozornosti, čo následne vedie k zverejňovaniu rôznych osobných, dôverných informácií o sebe. Tieto informácie však môžu byť ďalej šírené už bez nášho súhlasu a možnosti ovplyvniť ich publikovanie, čím prichádzame postupne o svoje súkromie. Mnoho severov (napr. servery sociálnych sietí) nás priamo vyzýva na zadanie osobných informácií o sebe, zverejňovania informácií o našej činnosti, dáva možnosť zdieľať obsah aj dôverného charakteru (fotografie, videá...), podmieňuje to možnosťou využívania ich služieb. Všetky tieto informácie sa dostavajú do veľkého informačného priestoru a hrozí

riziko ich zneužitia a my postupne prichádzame o svoje súkromie, ktoré sa stáva pre iných ľahko dostupným.

b) **Reklama na webových stránkach.** Reklama môže byť rovnako pravdivá ako aj nepravdivá, no ľudia majú sklony uveriť obsahu reklám, čo v prípade nepravdivých, či zavádzajúcich reklám môže spôsobiť narušenie sociálneho správania sa jednotlivcov (prehnaná dôvera v obsah, zmenu vlastného hodnotového rebríčka, ...).

c) **Jednoduchý prístup k nevhodným informáciám**. Internet využívame hlavne na získavanie informácií, čo umožňuje pomerne ľahko získať aj informácie nevhodného charakteru, ktoré môžu negatívne vplývať na vývoj detí a mládeže.
Za nevhodný obsah pre deti sa považuje:
   - nahota a sexualita, (pornografia),
   - násilie, (násilné scény a videá, , sebapoškodzovanie, samovraždy, asistované samovraždy),
   - verbálna agresivita a vulgárne vyjadrovanie,
   - prezentácia netolerancie, (rasizmus, nacionalizmus, xenofóbia, extrémizmus, náboženský fanatizmus, sekty,...),
   - extrémnych spôsobov správania, (propagácia anorexie, bulímie),
   - užívania návykových látok, (drogy, lieky, steroidy),
   - používania zbraní, ako aj rôznych obsahov, ktoré u nich môžu vyvolať strach, úzkosť, depresiu alebo pocit ohrozenia.

d) **Dôveryhodnosť, pravdivosť informácií na webe. Anonymita na webe.** Internet nám poskytuje falošný pocit dôveryhodného prostredia. Preto máme sklony uveriť všetkým informáciám, na ňom uverejneným, čo môže negatívne ovplyvňovať naše rozhodnutia.

   Pocit anonymity vyvoláva sklony k negatívnemu, nevhodnému správaniu sa, ktoré by sme v reálnom živote normálne nevykonali.

e) **Kyberšikanovanie** (elektronické šikanovanie, cyberbullying, cybermobbing) – forma šikanovania, pri ktorej sa používajú nové technológie, ako je počítač, internet, mobilný telefón. Prebieha vo virtuálnom priestore s využitím rôznych služieb a nástrojov ako sú email, IM (instant messeneger - napr. Skype, ICQ), čet, diskusné fóra, sociálne siete, stránky na zverejňovanie fotografií a videí, blogy, SMS správy, telefonáty. **(**Šikanovanie – opakované a zámerné správanie, ktorého cieľom je vysmievať sa, ubližovať niekomu, ponižovať ho. Agresor zneužíva svoju moc nad obeťou.)

   Kyberšikanovanie je jedným z najčastejších negatívnych javov na internete. Nie je to niečo nové, je to len prejav, ktorý sa objavuje v inom priestore. S rozšírením moderných technológií sa aj výrazná časť šikanovania presunula do virtuálneho prostredia. Pre agresorov je ľahšie ubližovať niekomu, komu sa nemusia pozerať priamo do očí, menej vnímajú emócie a zranenie obete, menej si uvedomujú závažnosť svojho konania a zodpovednosť zaň. Takéto šikanovanie im môže

pripadať iba ako druh neškodnej zábavy. Agresora zároveň ich anonymita chráni pred odhalením. Pre obeť je virtuálne šikanovanie ešte závažnejšie – nemôže pred ním uniknúť nikam, ani do bezpečia domova. Ak používa mobilný telefón alebo internet, agresori sa k nej dostanú v ktorúkoľvek dobu a na ktoromkoľvek mieste.

Formy kyberšikanovania: urážanie a nadávanie, obťažovanie, zastrašovanie, vyhrážanie a vydieranie, zverejnenie trápnych, intímnych alebo upravených fotografií alebo videí, šírenie osobných informácií alebo klebiet , vylúčenie zo skupiny, kybernetické prenasledovanie.

f) Hry a gambling. Gaming – pojem označujúci hranie elektronických hier na rôznych zariadeniach. Ak sa pri hraní používa aj pripojenie na internet, hovorí sa o online gamingu. Pre označenie hráča sa používa anglický výraz gamer.

Hra je prirodzenou súčasťou ľudského života, a detského obzvlášť, je prostriedkom pre osvojovanie si nových zručností a získavanie nových skúseností. Je relaxom, zábavou i spoločenskou aktivitou. V posledných rokoch si čoraz väčší priestor získava hranie hier na počítačoch, mobiloch a hracích konzolách.

Okrem pozitív majú **počítačové hry** aj svoje **riziká**:

- jednostranné zameranie aktivít dieťaťa,
- riziko vzniku závislosti,
- nevhodné správanie a násilie v hrách,
- zdravotné riziká,
- únik do virtuálneho priestoru – od reálneho sveta,
- strata sociálneho cítenia.

g) Nevyžiadané e-maily – spamy, poplašné správy (hoax) - Okrem dôležitých a užitočných informácií sa cez internet a email šíri aj veľa zbytočného balastu. Prichádza množstvo reklamných správ a výhodných ponúk, preposlaných vtipných emailov a varovaní pred rôznymi nebezpečenstvami, ale aj vírusy a iný škodlivý softvér. Pri pozeraní webstránok vyskakujú blikajúce reklamné okná. To všetko je otravné, obťažuje nás pri práci, zbytočne pri čítaní strácame čas. Okrem toho hrozí, že naletíme na rôzne podvody alebo si nevedomky nainštalujeme vírus, ktorý poškodí počítač.

Spam. Pod označením spam sa skrýva hromadne rozosielaná nevyžiadaná pošta. Najčastejšie sa šíri prostredníctvom emailov, ale aj cez SMS a MMS správy v mobiloch, na četoch alebo v online diskusiách. Veľkú časť spamu tvoria reklamné správy, výhodné ponuky nákupov, ponuky na účasť v súťažiach a lotériách, ako aj ponuky erotických telefonických liniek a pornografických stránok, zázračných liekov a liečebných postupov, nelegálneho softvéru a pod.

Ochrana pred spamom: ochrana osobných a kontaktných údajov, zamaskovanie emailovej adresy, ochrana počítača, nahlasovanie spamu, ochrana pred zasielaním reklamných správ

Hoax Pojmom hoax označujeme poplašné - podvodné správy, ktoré upozorňujú na neexistujúce nebezpečenstvá alebo sľubujú rýchle zbohatnutie. Patria medzi ne aj falošné alebo neaktuálne prosby o pomoc, reťazové listy šťastia a rôzne petície. Takéto správy kolujú po internete roky – postupne sú preložené do rôznych jazykov a aj keď sú v nich úplné absurdnosti, stále sa nájde niekto, kto im uverí a pošle ich ďalej. Tým sa hoax líši od spamu – väčšinou ho preposielajú dôverčiví užívatelia, ktorí si myslia, že ide o dôležitú správu, chcú pomôcť alebo sa podeliť o možnosť výhodného Hoax zdôrazňuje naliehavosť nebezpečenstva a dramaticky opisuje riziká. Autor sa snaží vzbudiť zdanie dôveryhodnosti, opiera sa o vymyslené vyjadrenia známych osobností, odborníkov, spoločností alebo o fiktívny zážitok blízkych ľudí (napr. „Microsoft varuje“ alebo „kamarátka mi rozprávala svoju skúsenosť“). Ďalším znakom je prosba o okamžité rozoslanie hoaxu všetkým známym a priateľom.

2. Technologické riziká

a) **Škodlivý softvér – malware** (vírusy, trójske kone, počítačové červy, spyware, adware).

Malware je **škodlivý/zhubný program,** všeobecné označenie škodlivého softvéru. Patria sem napríklad vírusy, trójske kone, spyware a adware.

Na pomenovanie celej skupiny škodlivého softvéru možno použiť výraz „vírusy“. Je to asi najrozšírenejšie pomenovanie, aj keď nie je celkom presné. Vírusy sú len jedno z mála nebezpečenstiev, ktoré ohrozujú náš počítač a naše osobné údaje uložené v počítači, resp. na sieti. Vírusy sú podskupinou tzv. malware – „malicious software“, čo v preklade znamená škodlivý softvér. Malware sa do počítača dostáva zvyčajne cez internet, hlavne pri prezeraní stránok s nie dobre zabezpečeným systémom (najčastejšie stránok s crackmi alebo stránok s erotickým obsahom).

Vírus - je programový kód, ktorý sa bez vedomia užívateľa replikuje (teda množí a rozširuje). Tento kód je pre užívateľa obvykle skrytý. Hlavnou vlastnosťou vírusov je ich vlastná replikácia, ktorá nemusí vždy škodiť. Podstatné je, že to prebieha samovoľne, inak by sme mohli nazvať vírusom aj operačný systém, ktorý sa pri inštalácii sám skopíruje na pevný disk.“ **Počítačový vírus je program.**“

- **Klasické počítačové vírusy**
  - súborové vírusy,
  - boot vírusy,
  - multipartitné vírusy,
  - stealth,
  - polymorfné.

Súborové vírusy sú škodlivé programy, ktoré sa nedokážu rozmnožovať samé. Pre svoje rozširovanie potrebujú, podobne ako biologický vírus, hostiteľa, teda iný program najčastejšie s koncovkou .exe, .com, .sys, .dll, prípadne dokumenty balíka MS Office.

Inou skupinou sú tzv. ***boot*** vírusy, ktoré bývajú uložené v boot sektore, čo je prvý sektor diskety alebo pevného disku, kde sa nachádza spúšťacia časť operačného systému. Tieto vírusy sa spúšťajú pri každom čítaní z infikovanej diskety a tak isto pri každom spustení operačného systému v infikovanom počítači. Existujú aj kombinované vírusy nachádzajúce sa naraz v súboroch i v boot sektoroch, označujú sa tiež ako ***multipartitné vírusy*.**

Okrem samotnej reprodukcie sa vírus môže navonok prejavovať nejakou formou, napríklad môže vypisovať rôzne nečakané hlásenia, vytvárať na obrazovke grafické efekty alebo aj zvukovo sa prejaviť. Vírusy mávajú často deštruktívnu formu prejavu - napádajú systémové súbory operačného systému, kvôli čomu dochádza k „mrznutiu“ alebo celkovému znefunkčneniu daného systému, mažú súbory alebo adresáre, menia obsah súborov, šifrovanie dát, prípadne poškodzujú hardvér (prepísaním BIOSu na základnej doske). Vírusy majú zväčša väzbu na čas, alebo dátum, spúšťajú sa a pôsobia v určitých hodinách, dňoch (typickým príkladom bol v minulosti vírus Černobyľ).

Medzi ďalšie druhy vírusov patria tzv. neviditeľné vírusy označované ako ***stealth*.** Majú schopnosť skryť sa pred užívateľom, preto ich niektoré antivírusové programy nie sú schopné zaregistrovať. Takisto dokáže odvíriť vlastné súbory pri požiadavke o otvorenie súboru a po dokončení procesu ich znova infikovať.

Ďalším druhom vírusov sú vírusy ***polymorfné***, ktoré samé dokážu meniť časť svojho kódu, a preto žiadna kópia tela vírusu nie je totožná s inou kópiou. Detekcia takýchto vírusov je oveľa ťažšia.

- **Internetové červy**

V pôvodnom význame je červ tá časť vírusu, ktorá je zodpovedná za jeho šírenie. Kým klasickým súborovým vírusom trvalo mesiace až roky, kým sa rozšírili, internetovým červom na to stačí niekoľko dní, niekedy dokonca niekoľko minút. Kým súborový vírus vyžaduje zásah užívateľa, aby sa dostal z jedného počítača na druhý pomocou média (stiahnutím z internetu, CD, DVD alebo iný nosič), internetový červ sa dokáže rozšíriť sám pomocou počítačovej siete. Funguje tak, že sa pokúša pripojiť na každý možný počítač v počítačovej sieti a na svoj prenos využiť slabé miesto zle zabezpečeného počítača (predovšetkým vďaka chybám v operačnom systéme, či chybám v iných programoch poskytujúcich sieťové služby). Na tomto počítači sa červ aktivuje a znovu sa skúša šíriť do ďalších počítačov. Počet nakazených počítačov teda stúpa exponenciálne. Šíreniu červov sa dá zabrániť dobrým zabezpečením počítačovej siete, pretože napadnutiu vnútornej siete z internetu dnes už dokážeme ľahko zabrániť.

- **E-mailové červy**

Rozdelenie vírusov do spomínaných kategórií (klasické, červy a trójske kone) nie je úplne jednoznačné. Typickým príkladom sú e-mailové vírusy, ktoré by sa dali zaradiť medzi červy, pretože sa šíria cez internet, ale i medzi klasické vírusy a trójske kone, pretože sa aktivujú otvorením spustiteľného programu v prílohe emailu. Po aktivovaní takéhoto vírusu sa tento dokáže napríklad rozposlať na všetky emailové adresy zaznamenané v programe MS

Outlook a MS Outlook Express a tým pôsobiť ako mail poslaný od priateľa resp. známej osoby. Takže ak užívateľ poľaví v ostražitosti, jedným kliknutím môže rozšíriť tento vírus ďalším užívateľom.

- **Trójske kone**

Trójsky kôň je škodlivý kód pribalený k zdanlivo neškodnému, užitočnému softvéru. Od vírusov a červov sa líši tým, že sa nereprodukuje a v infikovanom počítači sa nachádza len v jednej kópii. Trójske kone môžu mať najrôznejšie účinky. Veľakrát môžu i priamo ohroziť počítač podobne ako vírusy vykonaním škodlivej akcie - formátovanie pevného disku, prepisovanie dát, a pod.

Nebezpečnou akciou, ktorú môžu trójske kone vykonávať, je otvorenie tzv. ***backdoor*** (v preklade zadné dvierka). Cez tieto zadné dvierka sa vie útočník, autor trójskeho koňa, dostať do systému bez toho, aby poznal prístupové meno a heslo.

Adware

je softvér, ktorý automaticky zobrazuje, prehráva alebo sťahuje reklamný materiál do počítača po svojej inštalácii alebo pri používaní tohto softvéru. Často ho používajú firmy, ktoré poskytujú služby typu zarábaj cez internet. Vtedy používateľ "prenajme" časť monitora, kde sa budú zobrazovať reklamné bannery.

Spyware

je softvér skrývajúci sa v počítači bez vedomia majiteľa. Zbiera informácie o počítači, o surfovacích návykoch, heslách, emailových adresách a ďalšie osobné údaje

Detekovanie vírusov (škodlivých programov)

Antivírusový softvér je program, ktorého cieľom je identifikovať a eliminovať počítačové vírusy.

Typy anivírusových programov:

- **Jednoúčelové antivírusy** - sú to antivírusové programy, ktoré sa zameriavajú na detekciu, príp. aj dezinfekciu jedného konkrétneho vírusu. Nedajú sa použiť ako plnohodnotná antivírusová ochrana. Používajú sa len ak vieme, že máme v počítači konkrétny vírus. Na rozdiel od plnohodnotného antivírusového systému ponúkajú dôkladnejšiu dezinfekciu a ďaleko väčšiu rýchlosť. Väčšinou vznikajú len na detekciu/dezinfekciu hojne sa vyskytujúcich vírusov.
- **Balík jednoúčelových antivírusov** - ide o podobnú záležitosť ako v predošlom prípade, s tým rozdielom, že tento druh antivírusu dokáže nájsť a odstrániť väčšie množstvo obvykle hojne sa vyskytujúcich vírusov.

- **Komplexné antivírusové systémy** - najčastejšia forma antivírusových programov. Skladá sa z častí, ktoré sledujú všetky najpodstatnejšie vstupné miesta, ktorými by sa prípadná infiltrácia mohla do počítačového systému dostať (e-mail, www, média(disketa, CD-ROM, DVD, Flash...)). Samozrejmosťou býva aj aktualizácia prostredníctvom internetu.

Všeobecné antivírusové techniky

a) **Porovnávací test.** Antivírusový program si po inštalácii vytvorí databázu informácií o súboroch uložených na diskoch počítača. Potom porovnáva napríklad veľkosť spustiteľného súboru s údajom naposledy zapísaným do databázy. Pri zmene veľkosti spustiteľného súboru antivírový program upozorní na možnosť vírusovej nákazy. Možno totiž predpokladať, že veľkosť spustiteľného súboru sa nemení. Táto metóda detekcie vírusov nevyvoláva toľko planých poplachov ako napríklad metóda heuristickej analýzy. Na druhej strane autor nového vírusu môže obísť problém databázy informácií o súboroch priamo úpravou zápisu v tejto databáze.

b) **Heuristická analýza.** Je spôsob podrobnej analýzy obsahov súborov na pevnom disku spojenej s vyhľadávaním rôznych podozrivých častí kódu (priame zápisy na disk, prevzatie kontroly nad operačným systémom). Heuristická analýza je všeobecne fungujúca metóda, ktorá nie je závislá na vírusovej databáze. Automaticky sa pri tejto metóde vykonáva test aj na známe vírusy. Ak je niektorý súbor označený ako napadnutý, prehľadáva sa v databáze vírusov a meno vírusu je vypísané, v opačnom prípade je vírus označený ako neznámy. Ak antivírusový program obsahuje tzv. plnú heuristickú analýzu (heuristická analýza s emuláciou kódu), vtedy sa antivírový program priamo pokúša emulovať (emulovať – schopnosť napodobniť jeden systém iným) činnosť počítača pri spustení programu. Touto metódou môže antivírový program nájsť a odhaliť úplne nový, neznámy vírus, ktorý nie je obsiahnutý v databáze antivírového programu, ktorý prehľadáva súbory metódou skenovania. Táto metóda odhaľovania vírusov môže označiť za nakazené neznámym vírusom aj tie súbory, ktoré sú v poriadku. Stačí, keď vnútorná štruktúra kódovania bude podobná kódovaniu vírusov alebo ich správaniu.
c) **Skenovanie.** Je metóda založená na porovnávaní reťazcov kódov vírusov obsiahnutých v internej databáze antivírového programu s reťazcami v skenovaných súboroch. Ak narazí antivírový program na súbor, ktorý obsahuje kód vírusu zhodný s kódom v internej databáze, ohlási nájdenie vírusu a pomenuje ho menom priradeným kódu v databáze. Takýto spôsob ochrany je veľmi spoľahlivý, na druhej strane úroveň ochrany závisí na aktuálnosti vírusovej databázy. Ak ju užívateľ nebude pravidelne a často aktualizovať, program proti novým vírusom nemá najmenšiu šancu. Najväčšou výhodou tejto metódy je jej rýchlosť, táto metóda sa preto používa pre pravidelné kontrolovanie pevného disku.
d) **Rezidentné sledovanie (Rezidentný štít).** Pri štarte počítača sa do operačnej pamäte automaticky zavedie rezidentný antivírus, ktorý monitoruje činnosť počítača. V prípade neobvyklých operácií (zápis do systémových oblastí diskov, modifikácie spustiteľných súborov apod.) antivírový program ihneď upozorní na túto neobvyklú činnosť a čaká na reakciu užívateľa. Táto metóda je využívaná od doby, keď sú počítače dostatočne výkonné a majú dostatočnú operačnú pamäť, takže rezidentný antivírus systém prakticky nezaťažuje.

Príklady antivírusových systémov

- ESET Smart Security
- avast!
- AVG
- Norton AntiVirus
- Kaspersky AntiVirus
- NOD32
- McAfee Viruscan
- Panda AntiVirus
- Ad-Aware
- Dr.Web CureIT!
- Avira

b) Počítačová kriminalita

Počítačová kriminalita je relatívne novým druhom závažnej trestnej činnosti. Od klasickej kriminality sa odlišuje celým radom osobitných charakteristík a zvláštností. Trestný čin môže byť spáchaný v anonymite na diaľku, sprostredkovane a to všetko v priebehu niekoľkých sekúnd bez toho, aby poškodený zaregistroval spáchanie takéhoto trestného činu a niekedy sa o tom vôbec dozvedel. Internet, anonymita a nedostatočná legislatíva, robia z počítačovej kriminality mocný nástroj na páchanie domácich a medzinárodných trestných činov veľakrát závažného charakteru s priamym dopadom na ekonomiku krajiny a jej bezpečnosť.

Druhy kriminality:

- útok na počítač, program, údaje, komunikačné zariadenie,
- neoprávnené užívanie počítača alebo komunikačného zariadenia,
- krádež počítača, programu, údajov, komunikačného zariadenia
- zmena v programoch a údajoch,
- podvody páchané v súvislosti s výpočtovou technikou.

Prienik do počítačového systému

je druh počítačovej kriminality a znamená útok na počítačový systém. Človek zaoberajúci sa touto činnosťou sa v počítačovom slangu nazýva **hacker.**

Hacker - počítačový expert, dobrý programátor, hľadajúci bezpečnostné diery v systémoch, za účelom zlepšenia ich bezpečnosti. O nájdených chybách a nedostatkoch informuje autorov programov, správcov systému aj verejnosť.

Cracker - má technické schopnosti ako hacker, ktoré ale používa vo svoj prospech, väčšinou ilegálne. Patria sem aj takzvaní softvéroví, filmoví a hudobní piráti, lovci čísiel kreditných kariet a iní. Najčastejším motívom je pre nich uznanie v komunite a peniaze. Jedná sa o plánovanú a premyslenú činnosť.

Počítačové bankové krádeže

Phishing

Phishing (rybárčenie) využíva metódy sociálneho inžinierstva a rozširuje sa v prvom rade e-mailom. Falšovaná správa, ktorá vás pod určitou zámienkou nabáda ku zmene

osobných údajov. Správa vyzýva užívateľa, aby zmenil resp. upravil svoje osobné údaje v bankových inštitúciách, alebo na web stránkach, kde sa držia finančné prostriedky, resp. záväzné objednávky. V takomto emaile je umiestnený odkaz, na ktorom si heslo máte zmeniť. Odkaz však nesmeruje na inú web stránku, ako je originálna web stránka spomenutej inštitúcie. Táto web stránka vyzerá a správa sa takmer úplne rovnako, užívateľ si to nevšimne. Prihlásením sa na tejto web stránke získa nepovolaná osoba prístupové údaje a možnosť okradnúť užívateľa o finančné prostriedky. Takéto správy sú väčšinou veľmi formálne napísané. Niektoré dokonca vyzerajú tak, že ich odosielateľom je samotná banka. Preto si vždy overte pravosť takejto správy a neotvárajte stránku cez odkaz v pošte.

Pharming

Pharming (farmárčenie) má rovnaký efekt ako phishing, ale pracuje na inej báze. V tomto prípade je napadnutý buď internetový poskytovateľ, alebo užívateľský počítač, kde sú zmenené tzv. DNS záznamy. Touto cestou adresy web stránok ukazujú na iné miesta, ako by mali, takže nastáva rovnaký efekt ako pri phishingu - užívateľ sa dostane na falošnú web stránku, kde prezradí dôležité tajné informácie ako napríklad meno a heslo k bankovým operáciám.

Dialery

Ďalším zákerným spôsobom ako od používateľa získať finančné prostriedky sú programy, ktoré menia telefonické pripojenie počítača tzv Dialery. Tieto programy používajú za účelom prístupu na platené služby v Internete bez použitia kreditnej karty.

c) Počítačová bezpečnosť

.Cieľom počítačovej bezpečnosti je zabezpečiť:

- ochranu pred neoprávneným manipulovaním so zariadeniami počítačového systému,
- ochranu pred neoprávnenou manipuláciou s dátami,
- ochranu pred nelegálnou tvorbou kópií dát,
- bezpečnú komunikáciu a prenos dát,
- bezpečné uloženie dát,
- integritu a nepodvrhnuteľnosť dát.

Zabezpečenie počítačových systémov je zložitá problematika. Spoločnosti vynakladajú nemalé finančné prostriedky na previerky bezpečnosti (bezpečnostný audit) - firmám, ktoré sa na takúto úlohu špecializujú. Cieľom takejto činnosti je vypracovanie bezpečnostného projektu firmy

Cieľom tohto projektu je docielenie takého stavu, aby úsilie, riziko odhalenia a finančné prostriedky potrebné na narušenie bezpečnostného systému boli adekvátne v porovnaní s hodnotou, ktorú chráni bezpečnostný systém.

Každý bezpečnostný projekt pozostáva z troch hlavných častí:

- prevencia - hovorí o predchádzaní bezpečnostných rizík,
- detekcia - hovorí o spôsobe odhaľovania narušenej bezpečnosti,
- náprava - hovorí o odstraňovaní škôd a zamedzení opakovania v prípade zistenia narušenia bezpečnosti.

Základné pravidlá prevencie:

- **Zálohujte všetky svoje údaje** na disky chránené proti zápisu. Zálohovaním dát sa vyhnete i strate dát následkom výpadku prúdu alebo tvrdého reštartu.
- **Zabezpečte svoj počítač proti neoprávnenému vniknutiu.** Tento krok môžete urobiť použitím tzv. firewall, ktorý vytvára ochrannú stenu medzi vaším počítačom a potenciálne škodlivým obsahom na internete.
- V prípade, že využívate pripojenie k internetu cez dial-up, **kontrolujte, aké číslo pri pripájaní počítač vytáča**, používajte programy, ktoré zabraňujú dialerom v zmene čísla a **v prípade, že máte pochybnosti o vytočenom čísle, odpojte sa od internetu**, preverte počítač antivírusovým programom, reštartujte ho a vyskúšajte sa pripojiť odznova.
- **Zabezpečte svoje bezdrôtové WiFi siete.**
- **Nenavštevujte nezabezpečené stránky.** Snažte sa vyhnúť stránkam s pornografiou, stránkam s mp3 hudbou, filmami, licenčnými kľúčmi a pod. Nesťahujte žiadne programy, ktorých činnosť by mohla byť v rozpore s autorskými zákonmi.
- **Pred stiahnutím každého freeware programu si pozorne prečítajte, či jeho súčasťou nie je niektorý z uvedených nebezpečných programov.** Pozorne si prečítajte podmienky používania programu a vyhnite sa všetkým programom, ktoré podmieňujú svoju inštaláciu nainštalovaním tzv. Third Party Components (komponenty od tretích strán) a tiež tým, ktoré sa v zmluve zbavujú zodpovednosti.
- **Nezverejňujte svoju emailovú adresu.** Vaša emailová adresa je váš osobný údaj. Veľmi dobre si rozmyslite, do akého formulára ju vyplníte. Používajte radšej niekoľko adries (jednu pre priateľov a druhú na vyplňovanie do formulárov).
- **Neotvárajte neznáme prílohy.** Ak neotvoríte spustiteľnú prílohu emailu, nemôžete dostať emailový vírus. Preto radšej všetky cudzojazyčné emaily vymazávajte. Vírus však môžete dostať i od rodiny či priateľov bez toho, aby vedeli, že vám taký email poslali. Pred otvorením podozrivej prílohy emailu si radšej overte, či vám ju dotyčný chcel poslať.
- **Nespúšťajte neoverené makrá v dokumentoch.** V súčasnosti sa i makrá podpisujú digitálnym podpisom. Preto si pred jeho spustením overte platnosť digitálneho podpisu a neaktivujte neznáme makro.
- **Udržujte všetky súčasti systému aktuálne, používajte najnovšiu verziu prehliadača a poštového klienta.** Aktualizovaním súčastí systému odstraňujete jeho nedostatky, ktoré by škodlivé programy mohli využiť.
- **Chráňte svoj počítač aktuálnym antivírusovým systémom.** Aby bola ochrana účinná, antivírusové systémy sa aktualizujú i niekoľkokrát za deň.

- **Chráňte svoj počítač anti-spyware programom.** Tieto programy sa aktualizujú rovnako ako antivírusové systémy.
- **Zvážte, ktoré priečinky budete zdieľať v sieti.** Nastavte na všetky zdieľané priečinky príslušné oprávnenia a chráňte k nim prístup heslom.
- **Vypnite automatické spúšťanie programu po vložení média (CD, DVD, USB DISK).**
- **Chráňte vstup do počítača heslom.** Nedovoľte neznámej osobe, aby sa dostala do vášho počítača.
- **Majte prehľad kto a ako využíva váš počítač.** Veľa užívateľov využívajúcich cudzí počítač prejavuje menšiu zodpovednosť ako pri vlastnom počítači, preto sa treba dohodnúť na konkrétnych pravidlách a určiť vopred aké súbory budú otvárané/používané a predtým ich skontrolovať pomocou antivírusového programu.
- **Zálohujte svoje dáta.** Zálohovaním predídete škodám, ktoré vzniknú pri chybe alebo poškodení hardvéru alebo softvéru.

Firewall softvér alebo hardvér, ktorý blokuje vstup hackerov alebo škodlivého softvéru z internetu do počítača. Tiež umožňuje zastaviť odosielanie škodlivého softvéru z počítača do ďalších počítačov.

Elektronický podpis

V súčasnosti je možné písomnosti (ako napríklad daňové priznanie, či ročné zúčtovanie pre zdravotné poisťovne, elektronické faktúry a podobne) posielať elektronickou formou. Aby bolo možné odoslaným dokumentom dôverovať, je potrebné zaručiť nepopierateľnosť a nepozmeniteľnosť dokumentov. Na tento účel slúži elektronický podpis,