## Učebnica INFORMATIKA pre stredné školy (Kalaš a kol.)

**Autorský zákon** určuje práva a povinnosti autora počítačového programu (diela). Právom autora je rozhodnúť o tom, ako sa bude jeho dielo používať alebo šíriť.
**Licenčná zmluva** stanovuje podmienky, za akých môžeme počítačový program používať. Ak tieto podmienky dodržiavame, hovoríme, že máme **legálny softvér**. licenčná zmluva sa v našich podmienkach podobá kúpno-predajnej zmluve, ktorá určuje práva a povinnosti predávajúceho aj kupujúceho. Licenčná zmluva programu nás zvyčajne:

- **upozorňuje**, že program môžeme inštalovať len vtedy, ak súhlasíme so všetkými podmienkami zmluvy. V úvode inštalácie programu sa zobrazí dialógové okno s textom zmluvy. Inštalácia pokračuje až vtedy, ak potvrdíme súhlas (inak sa inštalácia ukončí);
- **určuje**, do koľkých počítačov môžeme program nainštalovať;
- **určuje**, za akých podmienok (a či vôbec) môžeme program šíriť;
- **určuje**, čo nesmieme s programom robiť (napríklad ho meniť);
- **upozorňuje**, za čo preberá a za čo nepreberá zodpovednosť tvorca programu. (Obvykle nepreberá zodpovednosť za žiadne škody, ktoré vzniknú jeho používaním – ak takúto možnosť pripúšťajú zákony krajiny, v ktorej sa program šíri.)

Licenčná zmluva zvyčajne stanovuje, že zakúpený program nemôžeme používať súčasne na viacerých počítačoch. Možnosť legálne používať softvér na viacerých počítačoch sa nazýva **multilicencia**. Počet počítačov, na ktorých smieme legálne používať určitý program s multilicenciou, býva určený buď konkrétnym číslom (napríklad 10 počítačov) alebo miestom (napríklad v škole). **Školské** alebo **študentské licencie** bývajú lacnejšie, ale zakazujú používanie príslušného programu na komerčné účely (pomocou programu s takouto licenciou nemôžeme vytvoriť produkt, ktorý by sa potom predával). Shareware a freeware programy sa väčšinou šíria pomocou internetu. Za používanie **freeware** programov sa nevyžaduje platba, ak ich používame v súlade s licenčnou zmluvou. **Shareware** programy môžeme zvyčajne používať počas určenej doby bezplatne. Po tejto skúšobnej dobe sa však musíme rozhodnúť, či program prestaneme používať, alebo zaň zaplatíme.

## Prevzaté zo ZODPOVEDNE.SK

http://zodpovedne.sk

**BETA VERZIA:** *testovacia verzia komerčného programu*, šírená zadarmo za účelom testovania a reklamy, pritom sa užívateľ naučí pracovať s programom, keď je spokojný, je ochotný zaplatiť za ostrú verziu programu. Ostrá verzia vzniká vlastne spoluprácou užívateľa a programátora "vychytaním" múch pri používaní beta verzie. Môže mať časovo obmedzenú platnosť.
**DEMOVERZIA:** *verzia softvéru, ktorá funguje neobmedzene dlhý čas, ale nie sú funkčné všetky možnosti daného programu*, napr. nefunguje ukladanie zmien urobených pomocou tohto programu. Väčšinou sa jedná o hry alebo rôzne aplikácie. V podstate je to druh reklamy, ktorá umožňuje užívateľovi zoznámiť sa so základnou funkciou programu a rozhodnúť sa, či si ostrú verziu programu kúpi.
**FREEWARE:** *„slobodný softvér“*, *verzia softvéru zadarmo*, ktorej “sloboda“ sa určuje na viacerých úrovniach: je použiteľná na rôzne účely, je voľne šíriteľná, ale nie za poplatok, so súhlasom autora môže byť aj upravovateľná, a po jej vylepšení je možné poskytnúť ju širokej verejnosti, pričom autorské práva musia byt zachované. Rôzne freeware programy môžu byť obmedzené v niektorej z týchto úrovní.
**LICENCIA:** *súpis pravidiel, práv a obmedzení*, s ktorými musí užívateľ súhlasiť, pokiaľ chce produkt legálne používať.
**OPEN SOURCE:** *„voľný zdroj“*, vo všeobecnosti *akákoľvek informácia alebo zdrojový kód programov voľne a bezplatne dostupný verejnosti*. Programy, ktoré sú open source, je možné upravovať podľa vlastných predstáv, šíriť ďalej, či dokonca predávať. Takéto programy sú buď bez autorských práv, čiže *public domain*, alebo majú tzv. *GPL licenciu*, kde je meno pôvodného autora stále uvedené.
**SHAREWARE:** *verzia softvéru*, ktorá umožňuje program bezplatne vyskúšať alebo používať obmedzený čas alebo obmedzený počet spustení. Po uplynutí stanovenej doby alebo po určitom počte spustení sa program zablokuje celý alebo aspoň kľúčové funkcie. Za jeho ďalšie používanie je potrebné zaplatiť. V porovnaní s komerčnými programami je tento softvér lacnejší.
**TRIAL VERZIA:** *verzia komerčného software* na skúšku na určité obdobie, po vypršaní platnosti sa program zablokuje.

## Prevzaté z Wikipédie

http://sk.wikipedia.org/wiki/

Termínom **počítačová kriminalita** sa označujú trestné činy a priestupky zamerané proti počítačom ako aj trestné činy páchané pomocou počítača. Ide o nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu. Počítače v podstate neumožňujú páchať nový typ trestnej činnosti, iba poskytujú novú technológiu a nové spôsoby na páchanie už známych trestných činov ako je sabotáž, krádež, zneužitie, neoprávnené užívanie cudzej veci, vydieranie alebo špionáž.
Najvýraznejšími prejavmi počítačovej kriminality sú:

1. ***útok na počítač, program, údaje, komunikačné zariadenie:*** fyzické útoky na zariadenie výpočtovej techniky, magnetické médiá, vedenie počítačovej siete alebo elektrického rozvodu a pod., vymazanie alebo pozmenenie dát, formátovanie pamäťových médií nesúcich dáta, pôsobenie počítačových infiltrácií, nelegálna tvorba a rozširovanie kópií programov, získanie kópie hospodárskych dát, databáz zákazníkov, v štátnych orgánoch únik informácií o občanoch a pod. Z hľadiska rozsahu najväčších škôd pravdepodobne najväčší podiel patrí nelegálnej tvorbe a predaju autorsky chráneného programového vybavenia v počítačovom slangu označovaná ako Warez.
2. ***neoprávnené užívanie počítača alebo komunikačného zariadenia:*** využívanie počítačovej techniky, faxov, prostriedkov počítačových sietí, databáz a programov zamestnancami firiem a organizácií na vlastnú zárobkovú činnosť.
3. ***neoprávnený prístup k údajom, získanie utajovaných informácií (počítačová špionáž) alebo iných informácií o osobách, činnosti a pod.:*** prenikanie do bankových systémov, systémov národnej obrany, do počítačových sietí dôležitých inštitúcií a pod. Niekedy táto činnosť spôsobuje priame škody veľkého rozsahu, napr. nelegálne bankové operácie, ako aj nepriame škody spôsobené únikom informácií. V súvislosti s týmto trestným činom môže byť aj súbežný trestný čin ako napr. vydieranie, nekalá súťaž, ohrozenie hospodárskeho tajomstva, vyzvedačstvo, ohrozenie štátneho tajomstva.
4. ***krádež počítača, programu, údajov, komunikačného zariadenia***
5. ***zmena v programoch a údajoch (okrajovo i v technickom zapojení počítača resp. komunikačného zariadenia):*** zmena programov a údajov inými programami alebo priamymi zásahmi programátora, úprava v zapojení alebo inom atribúte technického vybavenia počítača.
6. ***zneužívanie počítačových prostriedkov k páchaniu inej trestnej činnosti:*** manipulácia s údajmi ako napr. zostavy v skladoch, tržby, nemocenské poistenie, stavy pracovníkov, stav účtov a pod., patria sem aj krádeže motorových vozidiel, falšovanie technickej dokumentácie, priekupníctvo, daňové podvody, falšovanie a pozmeňovanie cenín, úradných listín a dokladov, dokonca aj peňazí.
7. ***podvody páchané v súvislosti s výpočtovou technikou:*** využitie niečieho omylu vo svoj prospech (hry s vkladom finančnej čiastky a rozosielaním listov "následníkom" so sľubom zaručeného zisku). Tento druh trestnej činnosti možno vykonávať aj bez použitia výpočtovej techniky, ale s jej použitím je táto činnosť efektívnejšia.
8. ***šírenie poplašných správ:*** vytvorenie poplašnej správy upozorňujúcej na fiktívne nebezpečenstvo. Najčastejším motívom páchateľov tejto trestnej činnosti je pobaviť sa na nevedomosti ostatných, no môže ísť i o správy spojené s páchaním inej trestnej činnosti. Tieto správy sú v počítačovom slangu označovaná ako HOAX.

**Warez** je termín počítačového slangu označujúci autorské diela, s ktorými je nakladané v rozpore s autorským právom. Slovo bolo vytvorené odvodením z množného čísla anglického slova ***software*** nahradením písmena "s" za písmeno "z" - wares --> warez. Najčastejším spôsobom šírenia warezu je dnes internet. Ľudia, zaobchádzajúci s warezom, bývajú označovaní ako softvéroví piráti.
Podľa druhu býva warez rozdeľovaný na:

- **appz** – aplikácie: vo všeobecnosti maloobchodné verzie softvérových balíkov
- **crackz** – cracky: záplaty určené na pozmenenie skúšobnej verzie programov na plné alebo na obídenie protipirátskej ochrany
- **keyz/key generatorz** - inštalačné a registračné kľúče: kľúče k inštalačným programom alebo ich generátory, ktoré umožňujú nelegálne nainštalovať program alebo odstránia obmedzenia skúšobnej verzie programu
- **gamez** – počítačové hry: počítačové hry a hry pre hracie konzoly
- **moviez** – filmy: pirátske filmy
- **musicz/mp3z** – hudba: pirátske albumy, single alebo iné hudobné formáty distribuované vo forme hudobného formátu MP3
- **E-Bookz/Tutorialz** – knihy: do tejto kategórie spadajú pirátske eknihy, naskenované knihy a návody k programom.

**Typický priebeh šírenia warez-u:**

1. Je vydaná nejaká očakávaná verzia komerčného softvéru
2. Warezová skupina využije svoje kontakty k tomu, aby získala kópiu ešte pred vydaním (alebo odcudzí CD z továrne, kde sa vyrába)
3. Softvér je odovzdaný skúsenému programátorovi (crackerovi), ktorý zo softvéru odstráni ochranu proti kopírovaniu

4. Takto nahrá na hlavné servery tzv. Topsites
5. Potom ho rozdistribuujú tzv. kuriéri na mnoho FTP serverov po celom svete.

Výsledkom je, že nelegálne kópie programu sa bežne objavia v rovnaký deň ako oficiálne vydanie (tzv. *deň 0*, *0-day*), niekedy dokonca ešte skôr.

**Prienik do systému**

Ďalšou rozšírenou trestnou činnosťou je neoprávnené vniknutie do systému. Človek zaoberajúci sa touto činnosťou sa v počítačovom slangu nazýva hacker. Najčastejšie metódy na prienik do systému sú tieto:

- **Útok hrubou silou**
  Útok hrubou silou je metóda, ktorá spočíva vo vyskúšaní všetkých možných kombinácií znakov. Útočník zostrojí program, ktorý sa pokúša postupným vyskúšaním všetkých možností uhádnuť Vaše heslo. Rozlúšteniu takéhoto hesla zabránite použitím dostatočne dlhého hesla (pri súčasnom výkone počítačov sa odporúča minimálne 8 znakov). Dôležité je použiť čo najširší možný okruh znakov – malé i veľké písmená, čísla a ďalšie symboly. Toto heslo je potrebné tiež často meniť. Samozrejme to záleží na dôležitosti príslušného hesla. Je nanajvýš nevhodné ukladať hesla na verejne dostupných počítačoch.
- **Slovníkový útok**
  Tento útok spočíva v skúšaní všetkých slov daného jazyka. Takémuto útoku sa dá predísť tak, že použijete heslo, ktoré nie je slovom žiadneho jazyka. Bezpečné heslo si môžete odvodiť napríklad takto: Vezmime si prvé písmená vety, ktorú si ľahko zapamätáme: A predsa sa točí. Galileo Galilei. Dostaneme Aprsto-GaGa. Toto heslo môžeme ešte vylepšiť napríklad takto Apr100-2*Ga.
- **Odpočúvanie sieťovej komunikácie**
  Vaše heslo sa dá veľmi jednoducho získať odpočúvaním nezabezpečených komunikačných liniek ako sú http:// a ftp://. Preto nikdy nezadávajte svoje údaje do stránky, ktorá nie je zabezpečená šifrovanou komunikáciou https:// alebo ftps:// (poprípade inou).
- **Využitie neukončeného spojenia**
  Útočník môže využiť, že sa zabudnete odhlásiť zo systému. Využije otvorené spojenie, ktoré zneužije vo svoj prospech. Niektoré stránky sa proti takýmto útokom chránia automatickým ukončením spojenia pri nečinnosti (preto sa nedá odoslať mail, ktorý píšete dlhšie ako 15 minút).
- **Zadné vrátka**
  Útočník zostrojí program nazývaný Backdoor (zadné vrátka), ktorý mu umožní pripojiť sa do systému bez nutnosti poznať správne používateľské meno a heslo. Tento program rozšíri pomocou počítačového červa alebo trójskeho koňa.
- **Odchytenie hesla**
  Útočník zostrojí program nazývaný Key-logger, ktorý zaznamenáva stlačené klávesy a takto získané údaje mu odosiela prostredníctvom Internetu. Tento program rozšíri pomocou počítačového červa alebo trójskeho koňa.
- ***Počítačové* bankové *krádeže***
  Bankové krádeže uskutočnené pomocou počítača sú zatiaľ u nás zriedkavé no vo svete sa začínajú čoraz viac vyskytovať. Známe sú nasledujúce tri typy krádeží:
- **Phishing**
  Správy, ktoré Vás pod určitou zámienkou nabádajú ku zmene osobných údajov sa odborne nazývajú Phishing (v preklade rybárčenie). V takomto emaile je umiestnený odkaz , na ktorom si heslo máte zmeniť. Odkaz však nesmeruje na stránku banky, ale na jej dokonalú napodobeninu. 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**
  Najzákernejší spôsob, ktorým Vás hacker môže pripraviť o vaše úspory, je Pharming (farmárčenie). Táto metóda spočíva v presmerovaní názvu www stránky na inú adresu. Každej mennej adrese napríklad ib.vub.sk prislúcha číselná adresa napríklad 215.5.214.144. Pomerne jednoduchým spôsobom sa dá toto nastavenie zmeniť. Ak zadáte mennú adresu do Vášho prehliadača, miesto stránky banky sa zobrazí jej dokonalá napodobenina. Vy teda ani nezbadáte, že ste na inej stránke. Po zadaní údajov, ich získa neoprávnená osoba, ktorá takúto falošnú stránku vytvorila. Proti takejto hrozbe sa môžete brániť rôznym spôsobom. Najjednoduchším spôsob je zistiť si číselný kód stránky internetbankingu. Stačí otvoriť príkazový riadok a zadať príkaz ping adresa (napr. ping ib.vub.sk). Potom miesto mennej adresy do prehliadača zadáte číselnú adresu (napríklad https:// 215.5.214.144). Ďalšou možnosťou je overovanie platnosti certifikátu a upozornenie pri prechode zo zabezpečenej stránky na nezabezpečenú. Tieto funkcie sa dajú nastaviť v internetovom prehliadači. Niektoré banky sa proti takémuto spôsobu elektronického podvodu bránia tak, že Vám ihneď po prihlásení do systému pošlú SMS s kódom, ktorý musíte zadať alebo Vás aspoň upozornia, že sa niekto prihlásil k Vášmu účtu.

- **Spoofing**
  Do kategórie Spoofing patria všetky metódy, ktoré používajú hackeri na zmenu totožnosti odosielaných správ. Jednou z týchto metód je i náhrada emailovej adresy pri phishingu, ktorá zabezpečí, aby správa vyzerala tak, že ju odoslala banka. Ďalšou metódou je podvrh IP adresy na stránky, ktoré takýmto spôsobom overujú totožnosť prihlasujúceho. Najviac nebezpečnou je však metóda nazývaná MITM (man-in-the-middle v preklade „muž v strede“). Táto metóda spočíva v narušení komunikácie medzi klientom a bankou, pri ktorej útočník naruší šifrovací systém verejného a súkromného kľúča, ktorý sa používa pri komunikácii. Použiť metódu MITM však nie je jednoduché, pretože na narušenie komunikácie je potrebné získanie kľúča (niekedy tiež označovaný ako certifikát) banky, ktorý sa často mení. Je preto dôležité nastaviť Váš internetový prehliadač tak, aby overoval, či je certifikát ešte platný.

## Vírusový slovník ESET

http://www.eset.sk/virus-info/slovnik?inc=12751

**Adware**
Adware je akýkoľvek softvér, ktorý spôsobuje automatické sťahovanie, zobrazovanie alebo prehrávanie reklamných a propagačných materiálov v počítači užívateľa bez jeho vedomia, či za čiastočnej asistencie. Príznakmi sú napríklad vyskakujúce pop-up okná, vnucovanie stránok (nastavenie ako domovskej stránky bez vedomia užívateľa) a pod. Existujú aj programy, ktoré vstupujú do počítača so súhlasom užívateľa, pretože podmienkou ich bezplatného používania je práve prítomnosť reklamných materiálov.

**Backdoor**
Backdoor je aplikácia typu klient - server, ktorá umožní autorovi vzdialený prístup na počítač. Na rozdiel od bežných legálnych aplikácii s podobnou funkciou prebieha jeho inštalácia bez vedomia klienta.

**Boot sektor vírusy**
Boot sektor vírusy napádajú zavádzací sektor pevného disku počítača, čím zabezpečia svoje spustenie pri štartovaní počítača. Ide o pomerne staršiu skupinu vírusov.

**Dialer**
Dialer je program, ktorý presmeruje telefonické pripojenie, prostredníctvom ktorého sa užívateľ pripája na internet, na určité platené číslo. Tieto programy možno využívať legálne pri platení za internetové služby, avšak často sa zneužívajú na podvody pri presmerovaní bez vedomia používateľa.

**Červ**
Červ je samostatný program, ktorý rozširuje svoje kópie pomocou internetu, alebo lokálnej siete. Klasický vírus je pasívny a na rozšírenie potrebuje kopírovanie nakazeného súboru. Červ sa rozširuje aktívne, rozosielaním kópií po lokálnej sieti alebo internete využívajúc e-mailovú komunikáciu, prípadne na nižšej úrovni bezpečnostné diery operačného systému. Červ môže so sebou niesť aj ďalší škodlivý program, ktorý môže vykonať rozličné činnosti ako napr. inštalovať tzv. backdoor. Aj bez takéhoto "nákladu" môže červ spôsobiť veľké škody vplyvom zahltenia komunikačných kanálov. Dôsledkom rozšírenosti internetu je červ schopný rozdistribuovať sa po celom svete v priebehu niekoľkých hodín. Vedľajším efektom môže byť kompletné zahltenie siete, nevnímajúc podnikové LAN.

**HLL vírusy**
HLL (High Level Languages) vírusy boli vytvorené vo vyšších programovacích jazykoch ako Pascal, C, C++, Delphi, Basic alebo Visual Basic. Na rozdiel od bežných vírusov, vytvorených v jazyku Assembler, sú HLL vírusy mohutnejšie a ich analýza je komplikovanejšia. Takmer nemožná je detekcia heuristickou analýzou.

**Hoax (fáma)**
Hoax (fáma) je poplašná správa posielaná e-mailom, ktorá na svoje šírenie využíva dôverčivosť ľudí. Šíri sa výhradne ľudským pričinením a preto jediným spôsobom, ako sa pred takouto správou dá brániť, je opatrnosť. Fáma sa vo väčšine prípadov odvoláva na dôveryhodnú firmu ("Microsoft varuje...", "CNN oznámila", a pod.), často informuje o katastrofálnych dôsledkoch, napr. epidémie počítačového vírusu. Spoločným menovateľom týchto správ je výzva na okamžité postúpenie ďalšiemu užívateľovi. Týmto spôsobom sa fáma šíri k ďalším užívateľom internetu.

**Makrovírusy**
Makrovírusy sú makrá, ktoré sú schopné kopírovať sa z jedného dokumentu do druhého. Tzv. makrá sú bežnou súčasťou aplikácií v kancelárskych balíkoch a môžu pozitívne rozšíriť ich funkcionalitu. Sú však programovateľné v bežných jazykoch a teda zneužiteľné. Ak je to zámer autora, môžu teda manipulovať s dátami aplikácie, či modifikovať ostatné dáta v počítači. Vírusy napísané špeciálne pre konkrétnu aplikáciu sa môžu šíriť v zásade len na tejto konkrétnej aplikácii. Autori škodlivého kódu teda hľadajú aplikácie, ktoré sú všeobecne rozšírené. Ich podmienky dnes spĺňajú najmä programy z balíka Microsoft Office, ako napríklad Word či Excel.

**Parazitné vírusy**
Parazitné vírusy sa pripájajú k spustiteľnému súboru ako k hostiteľovi bez toho, aby samotný súbor akýmkoľvek spôsobom poškodili. Pri infekcii je pôvodný súbor upravený tak, aby po jeho následnej aktivácii došlo aj k aktivácii vírusu.

**Phishing**
Phishing je formou nežiaducej aktivity, ktorá využíva prvky tzv. sociálneho inžinierstva. Postup je charakteristický pokusmi podvodne získať citlivé informácie ako napr. heslo, či detaily platobnej karty maskovaním sa za dôveryhodnú

osobu alebo spoločnosť. Najčastejšie má podobu falošného oficiálneho e-mailu, prostredníctvom ktorého podvodník žiada údaje od užívateľa. Účelom je zneužiť tieto citlivé informácie v neprospech poškodeného.

**Prepisujúce vírusy**

Prepisujúce vírusy sú najjednoduchšou formou infekcie. Dochádza pri nej k vymazaniu pôvodného kódu a nahradeniu novým, škodlivým kódom. Spustením infikovaného súboru dochádza v skutočnosti k aktivácii samotného vírusu, ktorý sa môže snažiť o ďalšiu replikáciu.

**Retrovírusy**

Retrovírusy sú škodlivé aplikácie, ktoré sa snažia o zneškodnenie, vymazanie alebo deaktivovanie antivírusových systémov.

**Riskware**

Riskware ako pojem zahŕňa všetky aplikácie, ktoré používateľovi prinášajú pri spustení určité bezpečnostné riziko. Podobne ako pri inštalácii spyware alebo adware môže byť ich inštalácia odsúhlasená v licenčnej dohode, pri inštalácii programu. Príkladom takéhoto programu sú napríklad tzv. dialery.

**Rootkit**

Rootkit je špeciálny typ infiltrácie, ktorý má schopnosť skryť svoju prítomnosť v napadnutom systéme a tak uniknúť detekcii. Zväčša ide o balík škodlivého kódu, ktorý umožňuje útočníkovi zneužiť zraniteľné miesta v systéme a získať tak plnú kontrolu nad napadnutým počítačom. Pri rootkitoch najdôležitejšia prevencia, čiže schopnosť proaktívne zastaviť infiltráciu už pri pokuse preniknúť do systému a skôr, ako sa stihne aktivizovať. Rootkit sa dokáže v systéme po svojej aktivácii „zneviditeľniť“ a napadnutý užívateľ tak môže získať falošný pocit bezpečia.

**Sociálne inžinierstvo**

Sociálne inžinierstvo je spôsob získavania dôverných informácií pomocou manipulácie. Metóda bežne používa telefóny alebo internet, pričom zneužíva dôverčivosť ľudí vydávaním sa za známe a existujúce spoločnosti či inštitúcie.

**Spyware**

Spyware je program, ktorý využíva internet na posielanie rozličných údajov o používateľovi bez jeho vedomia. Podobne ako pri adware, súhlas s inštaláciou podmienkou licenčnej dohody môže byť súčasťou voľne šíriteľného programu. Spyware aplikácie zväčša odosielajú štatistické údaje, ako napr. informácie o nainštalovaných programoch, navštívených stránkach a podobne. Získané informácie bývajú v zásade zneužité na cielenú reklamu.

**Súborové vírusy**

Súborové vírusy využívajú ako hostiteľa jednotlivé súbory. V zásade ide vždy o spustiteľné súbory, pretože cieľom škodlivého kódu je jeho kopírovanie. Najčastejšie ide o vírusy s príponou „.COM“, „:EXE“, „.BAT“ alebo „.SYS“.

**Trójsky kôň**

Trójsky kôň (trójan) je škodlivý program, ktorý na rozdiel od vírusov alebo červovnemá schopnosť samostatne sa kopírovať a infikovať súbory. Najčastejšie sa vyskytuje vo forme spustiteľného súboru s príponou „.exe“, alebo „.com“. Súbor neobsahuje v zásade nič iné okrem samotného škodlivého kódu. Najúčinnejšia metodika jeho odstránenia je jednoduchá, zmazanie. Trójsky kôň sa môže tiež vydávať za užitočný program. Tento typ infiltrácie má rozličné funkcie, od zasielania stlačených kláves (keylogger) až po mazanie súborov (napr. sformátovaním disku). Zvláštnou funkciou je inštalovanie tzv. backdooru.

**Vírus**

Vírus je program, ktorý pripája svoje kópie k vykonávateľným súborom a zabezpečí ich aktiváciu. Jeho názov je odvodený od podobnosti s vírusmi v biológii. Vírus sa do vášho počítača môže dostať predovšetkým cez internet. Ďalšie možnosti jeho šírenia sú napríklad prenos v rámci lokálnej siete či kopírovanie z dátového média, ako disketa, CD, DVD a podobne. Exitujú súborové vírusy, čiže samostatné škodlivé programy, boot vírusy, ktoré napádajú zavádzací sektor disku a zabezpečia tak svoj štart už pri spustení počítača a makrovírusy, ktoré sú najčastejšie súčasťou dokumentov s príponou „.doc“ a „.xls“.

Ďalšie delenie vyplýva zo spôsobu vykonania škodlivej činnosti. Zatiaľ čo vírusy priamej akcie vykonajú svoju aktivitu v okamihu spustenia zavíreného objektu, rezidentné vírusy zostanú v pamäti počítača a vykonávajú škodlivú činnosť.

## Prevzaté zo ZODPOVEDNE.SK

http://zodpovedne.sk

**ADWARE:** *advertising-supported software, 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.
**CRACKER:** *človek, ktorý deaktivuje a obchádza softvérové ochrany*, robí teda úpravy v programoch, aby fungovali bez registrácie, a teda bezplatne; táto činnosť je protizákonná.
**CYBERBULLYING:** *„kyberšikana“*, je šikanovanie pomocou nových informačných a komunikačných technológií (t.j. najmä cez internet a mobilné telefóny). Príkladmi môžu byť anonymné vášnivé alebo nenávistné e-maily, obťažovanie prostredníctvom textových správ.

**CYBERSTALKING:** *„online prenasledovanie“*, označuje sa tým zneužívanie online komunikácie k ponuke nepožadovaných služieb alebo vecí, virtuálne prenasledovanie, obťažovanie a zastrašovanie cez internet. Obete tohto chovania sú potom prenasledované a obťažované v četovacích miestnostiach, je im úmyselne ubližované napríklad zasielaním vírusov, atď.
**ČERV:** *worm*, je to škodlivá infiltrácia, ktorá sa šíri formou prílohy v e-mailoch alebo pri prezeraní internetových stránok. Na rozdiel od vírusu sa vie replikovať sama, bez toho aby bola súčasťou nejakého hostiteľského programu.
**FIREWALL:** *sieťové zariadenie alebo softvér*, kontroluje komunikáciu medzi nezabezpečenou (internet) a zabezpečenou (počítač) zónou. Slúži na ochranu pred nebezpečnou, nežiadanou komunikáciou zvonku; aktívna ochrana proti hackerom.
**HACKER:** *človek*, ktorý je schopný sa pomocou svojich znalostí a hackerských programových nástrojov nabúrať do cudzích systémov, serverov a e-mailov, ničiť ochrany a obchádzať zabezpečenie. Sú to ľudia, ktorý majú veľké znalosti v oblasti internetu a počítačov a dokážu ich často aj zneužiť, dostať sa do vášho e-mailu, získať práva k prepísaní vášho webu, zničiť dáta v databáze, získať prístupové práva k bankovým účtom.
**HACKING:** *činnosť*, pri ktorej sa hacker alebo skupina hackerov snaží vniknúť do cudzieho systému.
**HOAX:** *falošná správa/poplašná správa/podvod*, ktorý varuje napríklad pred neexistujúcim nebezpečným vírusom. Najčastejšie sa môžeme stretnúť s falošnými prosbami o pomoc, fámami o mobilných telefónoch, petíciami a výzvami, reťazovými listami šťastia, atď.
**KEYLOGGER:** *hardvérové zariadenie alebo softvér*, jeho hlavnou úlohou je zachytávať stlačenie klávesov na počítači a ukladať ich do súboru alebo posielať svojmu administrátorovi. Zneužívajú ho hackeri na odchytávanie vašich prístupových hesiel a podobne.
**MALWARE:** *škodlivý/ zhubný program*, všeobecné označenie škodlivého softvéru. Patria sem napríklad vírusy, trójske kone, spyware a adware.
**MAKRO:** *séria príkazov a pokynov zoskupených do jedného príkazu* na automatické vykonanie úlohy v balíku MS Office. Uľahčuje a urýchľuje prácu v programoch MS Word, Excel, PowerPoint.
**NETIQUETTE:** *„netiketa“, zásady slušného správania sa na internete*. Každý používateľ internetu by mal ovládať základy slušného a etického správania sa na internete, v e-mailovej korešpondencii atď.
**PHARMING:** *podvodné internetové stránky*, princíp týchto stránok spočíva v presmerovaní názvu www stránky na inú adresu, miesto pôvodnej stránky sa zobrazí jej dokonalá napodobenina. Zväčša sa jedná o podvodné web-stránky bánk, ktoré od vás žiadajú vyplnenie napr. kódov z viacerých pozícii GRID karty, heslá vašich účtov a pod.
**PHISHING:** týmto slovom sa označujú *podvodné e-maily*, ktoré sú rozosielané na veľký počet adries. Na prvý pohľad vyzerá táto pošta ako napríklad informácie z banky. Príjemca je pod nátlakom hrozby nútený vyplniť osobné údaje (čísla účtu, kódy k internetovému bankovníctvu, pin pre platbu). Tieto údaje sú potom zneužívané.
**ROOTKIT:** *sada softvérových nástrojov, ktorých účelom je zamaskovať bežiace procesy*, súbory alebo iné údaje pred užívateľom. Rootkity boli pôvodne určené na nedeštruktívne účely, ale v poslednom čase sú stále častejšie využívané rôznymi druhmi malware (zhubného programu), ktoré sa tak stávajú neviditeľné pre väčšinu antispyvérových programov.
**SPAM:** *nevyžiadaná pošta*, spočíva v rozosielaní jednej a tej istej správy viacerým prijímateľom súčasne, ktorí o ňu nestoja. Môže obsahovať lacné reklamy, elektronické letáky, vírusy, phishing - podvody, hoax - poplašné správy a iné ohrozenia z internetu.
**SPOOFING:** *podvodná metóda*, ktorú používajú útočníci na zmenu totožnosti odosielaných správ. Jednou z týchto metód je náhrada e-mailovej adresy pri *phishingu*. Ďalšia spočíva v podvrhu IP adresy pri *pharmingu*. Najviac nebezpečnou je však metóda nazývaná *man-in-the-middle*, čo znamená „muž v strede“. Táto metóda spočíva v narušení komunikácie medzi klientom a bankou, pri ktorej útočník naruší šifrovací systém verejného a súkromného kľúča, označovaný ako certifikát banky, ktorý sa používa pri bezpečnej komunikácií.
**SPYWARE:** *softvér skrývajúci sa vo vašom počítači bez vášho vedomia*. Využíva sa na zbieranie informácii o počítači (hardvéri, softvéri), o vašich surfovacích návykoch, heslách, e-mailových adresách a samozrejme aj o vašich osobných údajoch - mene, veku, a pod.
**TROJAN HORSE:** *„trójsky kôň“*, nevinne vyzerajúci *program, ktorý v sebe ukrýva škodlivý kód*. Nevie sa samostatne kopírovať ani infikovať ďalšie počítače. Väčšinou si ho aktivuje sám užívateľ svojou nevedomosťou.
**VÍRUS:** *program, ktorý spravidla vykonáva deštrukčnú činnosť*, bez vedomia a súhlasu užívateľa. Vírusy sú malé programy, ktoré boli stvorené tak, aby sa šírili a páchali škodu. Ich cieľom je rozšíriť sa na čo najviac počítačov a napáchať čo najväčšiu škodu.
**ZOMBIE PC:** *počítač infikovaný trójskym koňom typu backdoor, ovládateľný proti vôli užívateľa.* Váš počítač tak plní príkazy spamera alebo hackera, ktorý môže cez váš počítač robiť nezákonnú činnosť, čo navonok vyzerá, že ju prevádzate vy.