## *****Škodlivý softvér (MALWARE)*****

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

1. ***Klasické počítačové vírusy***
2. ***Internetové červy***
3. ***Emailové červy***
4. ***Trójske kone***
5. ***Dialery***
6. ***Spyware***
7. ***Adware***
8. ***Spam***
9. ***PopUp a Hijackery***
10. ***Hoax***
11. ***Phishing***
12. ***Pharming***
13. ***Spoofing***

####

## Počítačové vírusy

* **Počítačový vírus je počítačový program, ktorý môže infikovať iný počítačový program takým spôsobom, že do neho skopíruje svoje telo, čím sa infikovaný program stáva prostriedkom pre ďalšiu aktiváciu víru.**
* **Súborové vírusy - pre svoje rozširovanie potrebujú, podobne ako biologický vírus, hostiteľa, teda iný program najčastejšie s koncovkou .exe, .com, .sys, .dll.**
* **Boot vírusy - bývajú uložené v boot sektore pevného disku. Tieto vírusy sa spúšťajú pri každom spustení operačného systému v infikovanom počítači.**
* **Neviditeľné vírusy (stealth) - majú schopnosť skryť sa pred užívateľom, preto ich niektoré antivírusové programy nie sú schopné zaregistrovať.**
* **Polymorfné vírusy - 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*****

* **Dokáže sa 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 zlého zabezpečenia PC.**
* **Na tomto počítači sa červ aktivuje a znovu sa skúša šíriť do ďalších počítačov.**
* **Počet nakazených počítačov stúpa exponenciálne.**



####

## *****E-mailové červy*****

* **Dali by sa zaradiť medzi červy, pretože sa šíria cez internet, ale i medzi klasické vírusy a trójske kone.**
* **Aktivujú sa otvorením spustiteľného programu v prílohe e-mailu.**
* **Po aktivovaní takéhoto vírusu sa tento dokáže napríklad rozposlať na emailové adresy ktoré sú v zozname napr. MS Outlook.**



####

## *****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.**
* **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 vrátka). Cez tieto zadné vrátka sa vie útočník, autor trójskeho koňa, dostať do systému bez toho, aby poznal prístupové meno a heslo.**
* **Druhy trójskych koňov:**

1. **Droppery** - v pravidelných intervaloch vpúšťajú do systému najrôznejší malware. Môžu obsahovať klasické vírusy, červy ale i spyware.
2. **Rootkits** - trójske kone ktoré sa dokážu v systéme zamaskovať tak, že to navonok vyzerá, že je všetko v poriadku.



####

## *****Dialery*****

* **Programy, ktoré menia telefonické pripojenie počítača.**
* **Spôsobujú presmerovanie na linky s vyššou tarifikáciou, hlavne na audiotextové a zahraničné čísla.**



####

## *****Spyware*****

* **Je softvér skrývajúci sa vo vašom počítači bez vášho vedomia.**
* **Využíva sa na zbieranie informácii o počítači (hardvéri, softvéri), o vašich surfovacích návykoch, heslách, emailových adresách a samozrejme aj o vašich osobných údajoch - mene, veku, a pod.**



####

## *****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.**



####

## *****Spam*****

* **Je to 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.**

#### https://informatikaedu.webnode.sk/_files/200000098-40ae541a85/Obr%C3%A1zok8.png

####

## *****PopUp*****

* **Do uvedenej kategórie patria programy vložené do webových stránok, ktoré otvárajú neželané okná s reklamou.**



####

## *****Hijackery*****

* **Hijackers, v preklade únoscovia spôsobujú „samovoľné“ otváranie okien prehliadača i v čase, keď používateľ žiadne webové stránky neotvára.**

## *****Hoax*****

* **Falošná správa/poplašná správa/podvod, ktorý varuje napríklad pred neexistujúcim nebezpečným vírusom.**

## *****Spoofing*****

* **Podvodná metóda, ktorú používajú útočníci na zmenu totožnosti odosielaných správ.**
* **Najviac nebezpečnou je však metóda nazývaná man-in-the-middle. 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 komunikácií.**



####

## *****Phishing*****

* **Týmto slovom sa označujú podvodné emaily, ktoré sú rozosielané na veľký počet adries.**
* **Príjemca je pod nátlakom hrozby nútený vyplniť osobné údaje (čísla účtu, kódy k internetovému bankovníctvu, pin pre platbu). Tieto údaje sú potom zneužívané.**

****

## *****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**.



####

## *****Prevencia*****

* **Zálohujte všetky svoje údaje a dáta.**
* **Zabezpečte svoj počítač proti neoprávnenému vniknutiu.**
* **Zabezpečte svoje bezdrôtové WiFi siete.**
* **Nenavštevujte nezabezpečené stránky.**
* **Nezverejňujte svoju emailovú adresu.**
* **Neotvárajte neznáme prílohy v e-maily.**
* **Udržujte všetky súčasti systému aktuálne, používajte najnovšiu verziu prehliadača a poštového klienta.**
* **Zvážte, ktoré priečinky budete zdieľať v sieti.**
* **Chráňte vstup do počítača heslom.**
* **Chráňte svoj počítač aktuálnym antivírusovým systémom.**

## *****Antivírusový software*****

* **Antivírusový softvér je počítačový program, ktorého cieľom je identifikovať a eliminovať počítačové vírusy.**
* **Typy antivírusových programov:**

1. ***Jednoúčelové antivírusy*** - Sú to antivírusové programy, ktoré sa zameriavajú na detekciu, príp. aj dezinfekciu jedného konkrétneho vírusu. Nedajú sa použiť ako plnohodnotná antivírusová ochrana.
2. ***On-demand skenery*** - Táto kategória antivírusových programov sa uplatní pri dezinfekcii počítačov, na ktorých nefunguje napr. MS Windows. Zaraďujú sa sem aj internetové on-line skenery.
3. ***Antivírusové systémy*** - Skladá sa z častí, ktoré sledujú všetky najpodstatnejšie vstupné miesta, ktorými by sa prípadná infiltrácia mohla do počítačového systému dostať (e-mail, www, disketa, CD-ROM, DVD, Flash, ...).
4. ***Komplexné antivírusové riešenia*** - Obvykle sú to balenia niekoľkých produktov od rovnakého výrobcu, obsahujú: antivírus, antispam, firewall, antispyware.

## *****Najznámejšie antivírusy*****

* **ESET Smart Security**
* **Kaspersky Internet Security**
* **Symantec Norton Security**
* **Avast Antivirus**
* **Microsoft Security Essentials**
* **Avira AntiVir**
* **Panda Antivirus**
* **McAfee AntiVirus**
* **G DATA AntiVirus**
* **Trustport Antivirus**
* **AVG Anti-Virus**

****

Viac tu: [https://informatikaedu.webnode.sk/pocitacove-virusy/](https://informatikaedu.webnode.sk/pocitacove-virusy/?utm_source=copy&utm_medium=paste&utm_campaign=copypaste&utm_content=https%3A%2F%2Finformatikaedu.webnode.sk%2Fpocitacove-virusy%2F)