eset | bezpečne na nete

Malvér

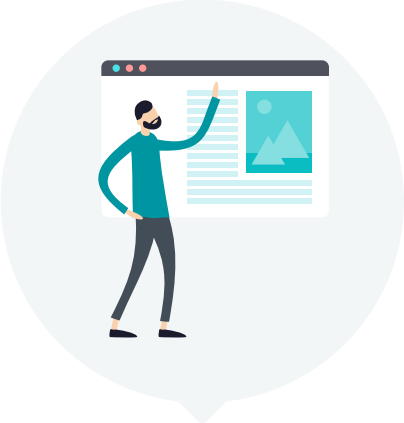
Malvér (škodlivý softvér, škodlivý kód, pôvod slova - malicious software)

Spoločný výraz pre všetky formy škodlivého kódu. Úlohou malvéru je napadnúť zariadenie a vykonať v ňom neželané zmeny. Šíri sa prostredníctvom bezpečnostných zraniteľností v systémoch, na ktorých neboli nainštalované potrebné záplaty či aktualizácie.

Potenciálne ohrozené zariadenia

Počítač
Tablet
Smartfón
Smart TV
Smart hodinky
Internet vecí

Najbežnejšie spôsoby šírenia malvéru:



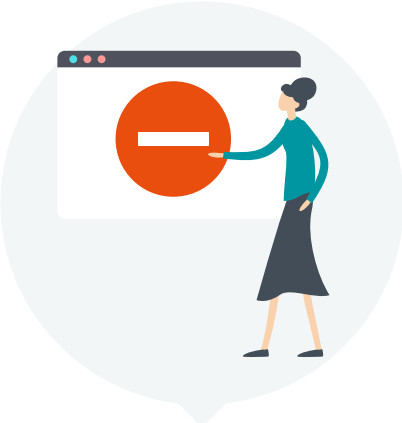
Webový prehliadač

E-mail

Vyskakovacie okná

Četovacie služby

Sociálne siete



Skompromitované webové stránky

Znaky upozorňujúce na prítomnosť malvéru:

- spomalený výkon operačného systému,
- zaplnená e-mailová schránka správami bez odosielateľa alebo predmetu,
- problém s prístupom na internet,
- webové stránky s množstvom reklám a kontextových okien,
- upozornenia bezpečnostného softvéru na prípadnú zachytenú hrozbu.

Malvér, advér, ransomvér – nie je vér, ako vér

S týmito názvami sa už stretol asi každý, ale viete, čo znamenajú a aký je medzi nimi rozdiel?

Malvér

Zastrešuje všetky formy škodlivého kódu bez ohľadu na spôsob, akým postihuje obete, ako sa správa alebo aké škody spôsobuje.

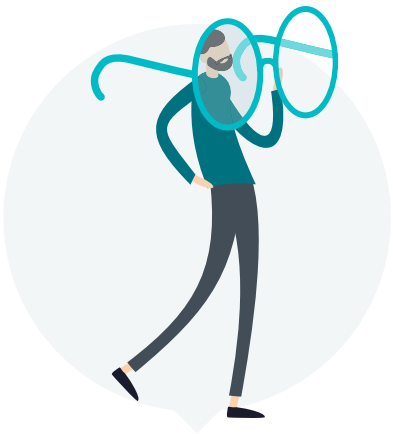
Najbežnejšie druhy malvéru:

Ransomvér

Malvér, ktorý po infiltrácii počítača uzamkne súbory používateľa. Používateľovi zabráni vo využívaní zariadenia a pýta za odomknutie súborov „ransom“, teda výkupné (zvyčajne v kryptomene).

Trójsky kôň

Známy aj ako trojan, sa používa na pomenovanie škodlivého softvéru na rôzne falošné účely, často deštruktívme alebo na účely krádeže dát. Trojan neobsahuje nič okrem svojho vlastného kódu. Preto je jediným riešením ho vymazať.



Spyvér

Sledovací škodlivý softvér, ktorého primárnou funkciou je zhromažďovanie osobných informácií uložených vo vašom počítači či monitorovanie webových stránok, ktoré navštevujete alebo položiek, ktoré si zakúpite online.

Keylogger

Druh malvéru, ktorý zaznamenáva čo píšete na klávesnici vášho zariadenia. Takto dokáže zachytávať správanie obete a ukradnúť aj dáta, ktoré obeť nemá nikde uložené a len ich príležitostne zadáva do niektorej služby či programu.

Password Stealer

Malvér, ktorý sa môže pokúsiť ukradnúť uložené užívateľské mená či heslá. Je podobný spyvéru či bankovému malvéru, no zameriava sa výhradne na súbory či programy, ktoré by mohli obsahovať heslá.

Bankový malvér

Tento druh malvéru sa zameriava na krádež finančných informácií obete, ako sú čísla kreditných kariet, prístupy do bankových účtov, kryptopeňaženiek či iných služieb spojených s peniazmi alebo kryptomenami.

Advér

Advér je škodlivý softvér s účelom šírením reklamy. Zobrazuje vyskakovacie okná počas surfovania po internete, nastavuje rôzne internetové stránky ako domovské stránky alebo otvára špeciálne okno programového rozhrania. Advér býva často nainštalovaný spolu s voľne stiahnuteľnými programami.

Červ

Malvér, ktorý má schopnosť replikovať sa z počítača na počítač bez potreby akéhokoľvek zásahu zo strany človeka. Ak máte nakazený počítač, nepošle ďalej len jedného červa. Pokúsi sa nakaziť množstvo ďalších počítačov tým, že rozpošle tisíce jeho kópií, ktoré sa následne replikujú.

Ako sa ochrániť pred malvérom?

Krok 1.

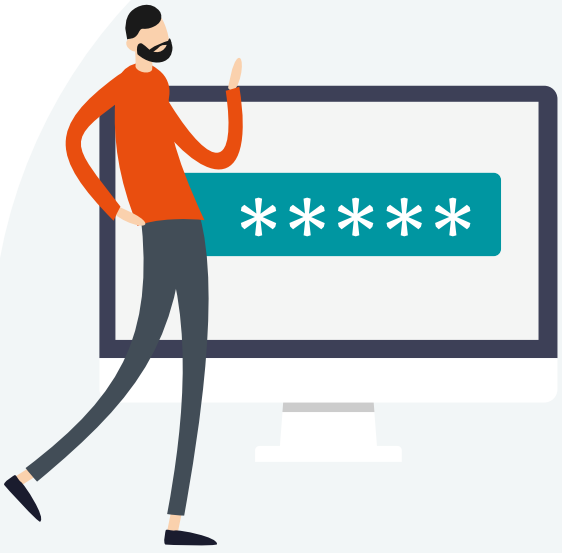
Udržujte operačný systém a bezpečnostný softvér v aktuálnom stave.

Krok 2.

Ak si vaše dáta ceníte, nezanedbávajte zálohu. Zálohovať vaše dáta môžete rôznymi spôsobmi:

Externé disky

Cloudová služba



Krok 3.

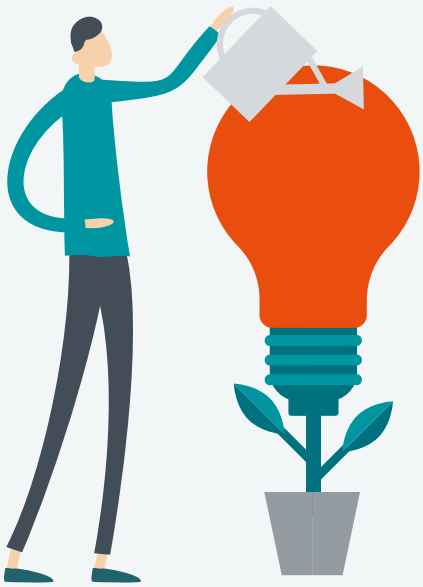
Používajte silné prihlasovacie údaje a zvoľte frázové heslo. Fráza by mala mať pre vás nejaký význam, a pritom sa vám ľahko pamätá. Používajte unikátne heslo pre každú službu.

Dobrý tip

Majte aktívnu dvojfaktorovú autentifikáciu pri online službách, ktoré pracujú s vašimi citlivými údajmi, ako napríklad Gmail, Facebook či Instagram.

Krok 4.

Majte zapnutú bránu Firewall, ktorá chráni siete a počítače pred neoprávnenými zásahmi zo strany hackerov, ako aj pred útokmi, prostredníctvom ktorých by mohli prevziať kontrolu nad zariadeniami a zneužiť ich na nekalé účely.



Krok 5.

Na internete sa správajte zodpovedne a kliknutie si dvakrát rozmyslite:

- Ak nepoznáte odosielateľa e-mailu, nesťahujte prílohu v e-maile bez kontroly.
- Minimalizujte počet sťahovaní rôznych dokumentov na neoverených weboch.
- Nenavštevujte weby s nelegálnym obsahom.
- Majte zapnuté blokovanie automatického otvárania okien.
- Nezdieľajte vaše osobné údaje s hocikým alebo verejne.

Ransomvér, čo sa skrýva za týmto zlovestne znejúcim názvom?

Malvér, ktorý dokáže uzamknúť zariadenie alebo zašifrovať jeho obsah s cieľom vymôcť od majiteľa daného zariadenia peniaze. Na oplátku autori škodlivého kódu sľubujú, samozrejme bez akýchkoľvek záruk, obnovenie prístupu k zablokovanému zariadeniu alebo dátam.

Najčastejšie používané techniky:

1.

Diskcoder ransomvér

Zašifruje celý disk a zamedzí používateľovi prístup k operačnému systému.

2.

Screen locker

Zablokuje prístup k obrazovke zariadenia.

3.

Crypto-ransomvér

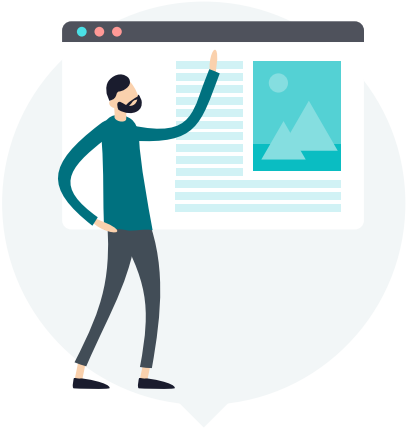
Zašifruje dáta uložené na disku obete.

4.

PIN locker

Zameriava sa na zariadenia so systémom Android a mení prístupové kódy s cieľom „vymknúť“ používateľov z ich zariadení.

Spôsoby infikovania:



Škodlivé webové stránky

E-mailové prílohy

Skrátené odkazy v e-mailoch

Nástroje, ktoré slúžia na sťahovanie rôzneho obsahu

Príspevky na sociálnych sieťach a četovacie služby

Máte podozrenie, že sa váš počítač nainfikoval ransomvérom?

- okamžite odpojte zariadenie z domácej siete, vypnite pripojenie WiFi (alebo mobilné dáta) a hibernujte počítač,
- ak hibernácia nie je možná, počítač vypnite a vyhľadajte odborníka alebo dodávateľa svojho bezpečnostného softvéru,
- po vyčistení počítača nasaďte zálohu (pokiaľ si sami netrúfate, obráťte sa na profesionála),
- v prípade, ak bolo vaše zariadenie napadnuté ransomvérom s podmienkou zaplatenia výkupneho, určite nič neplaťte.