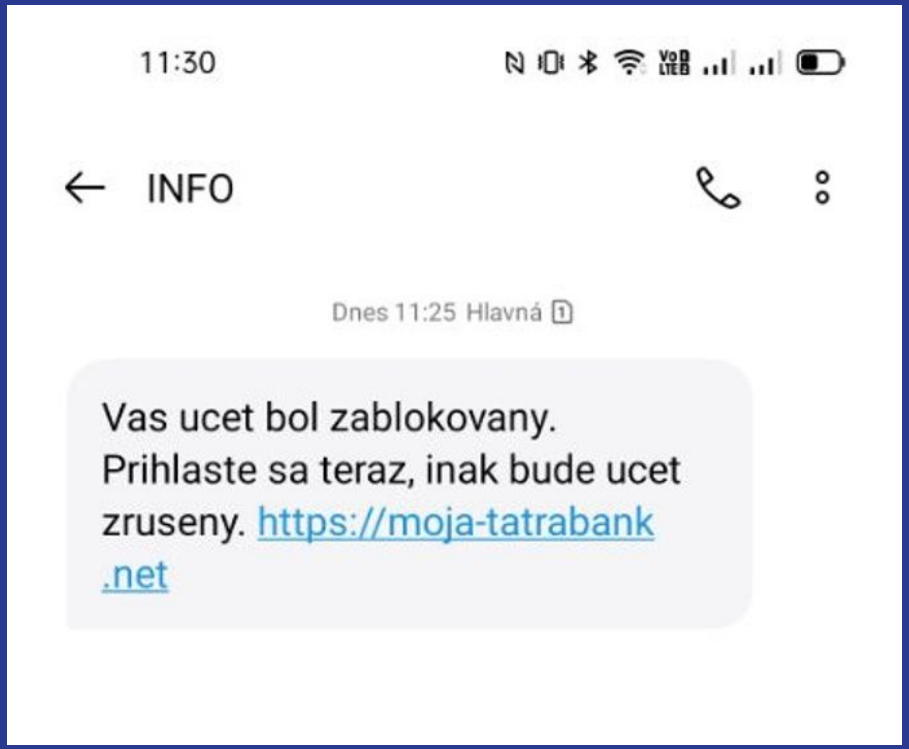
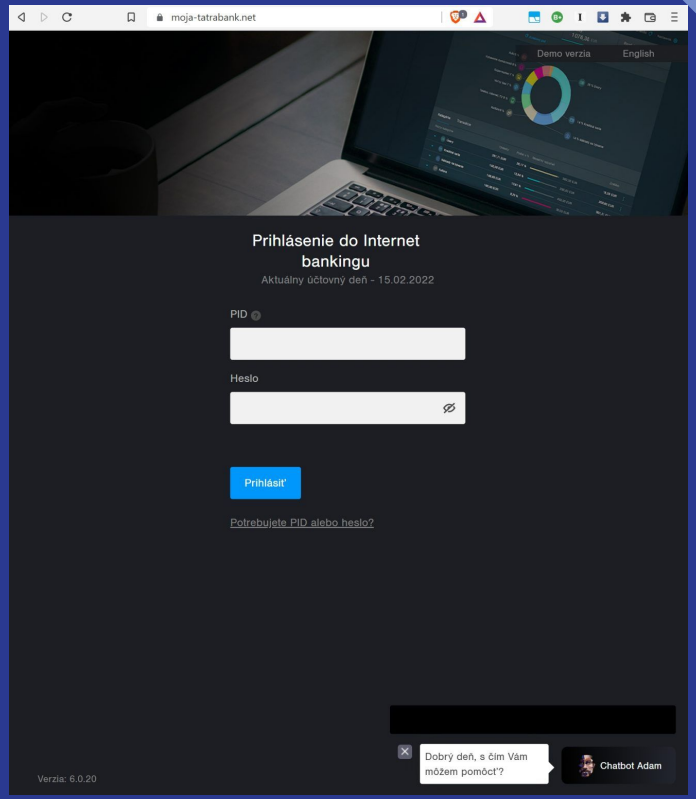
Podvodné správy

Podvodná správa

- Najčastejšie e-mail
- Skúša napodobniť overený zdroj/službu
- Písaná tak, aby vedela ovplyvniť
- Ciele: peniaze, informácie (napr. heslá, účty), ovládnutie zariadenia

Príklady podvodnej správy





Zdroj: https://touchit.sk/tatrabank-podvod/399734

Neexistuje 100% bezpečnosť

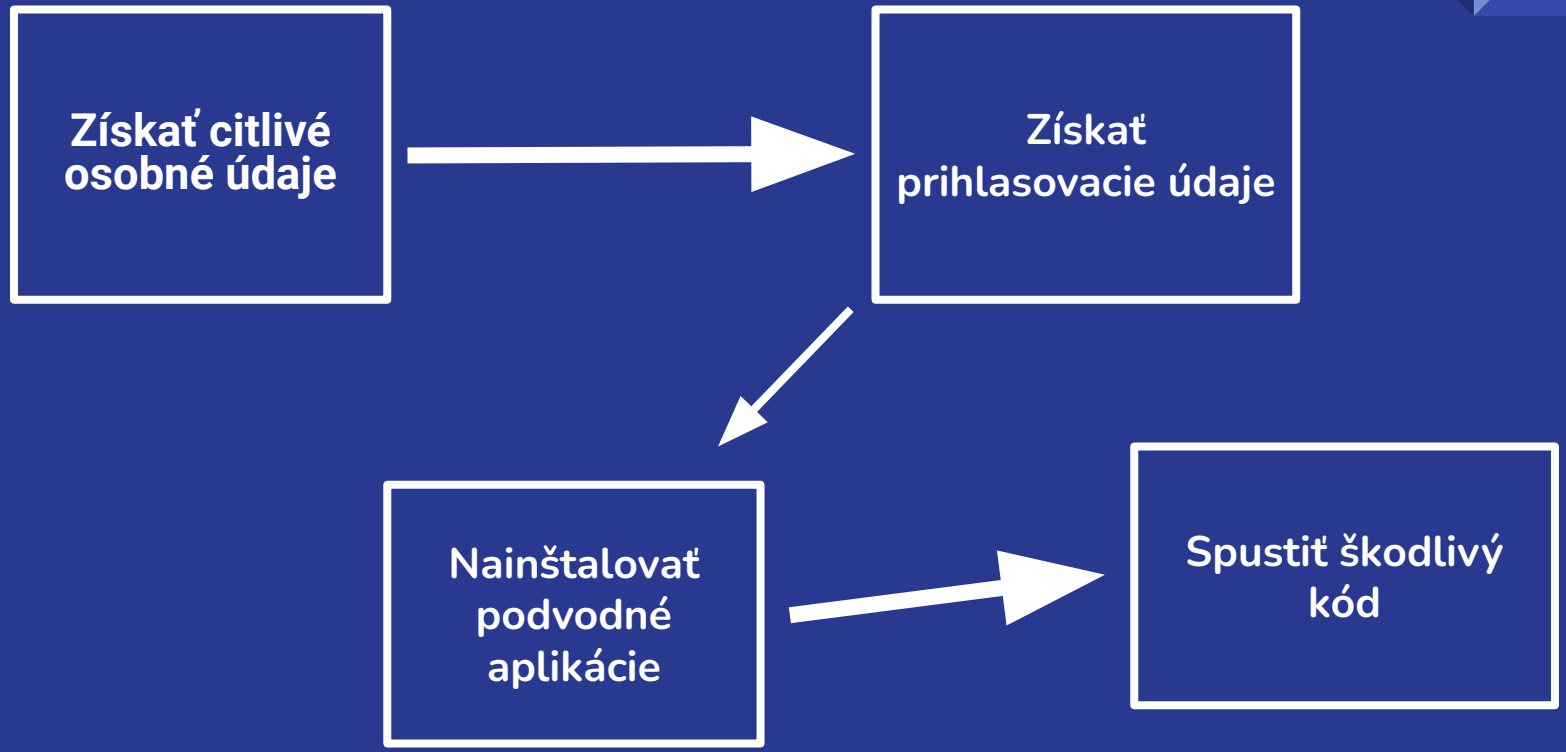
- Útočníci sú vždy popredu
- Vždy existuje riziko

Sociálne inžinierstvo

- Umenie manipulácie ľudí a schopnosť oklamať ich s použitím technológii alebo bez nich

- sociálne inžinierstvo – ”náhodná alebo vypočítavá manipulácia ľudí s cieľom ovplyvniť ich, aby robili veci, ktoré by bežne nerobili. A presviedčať ich bez toho, aby to vyvolalo čo i len náznak podozrenia.“ - Kevin Mitnick

Ciele sociálneho inžinierstva



Typy útokov

Phishing

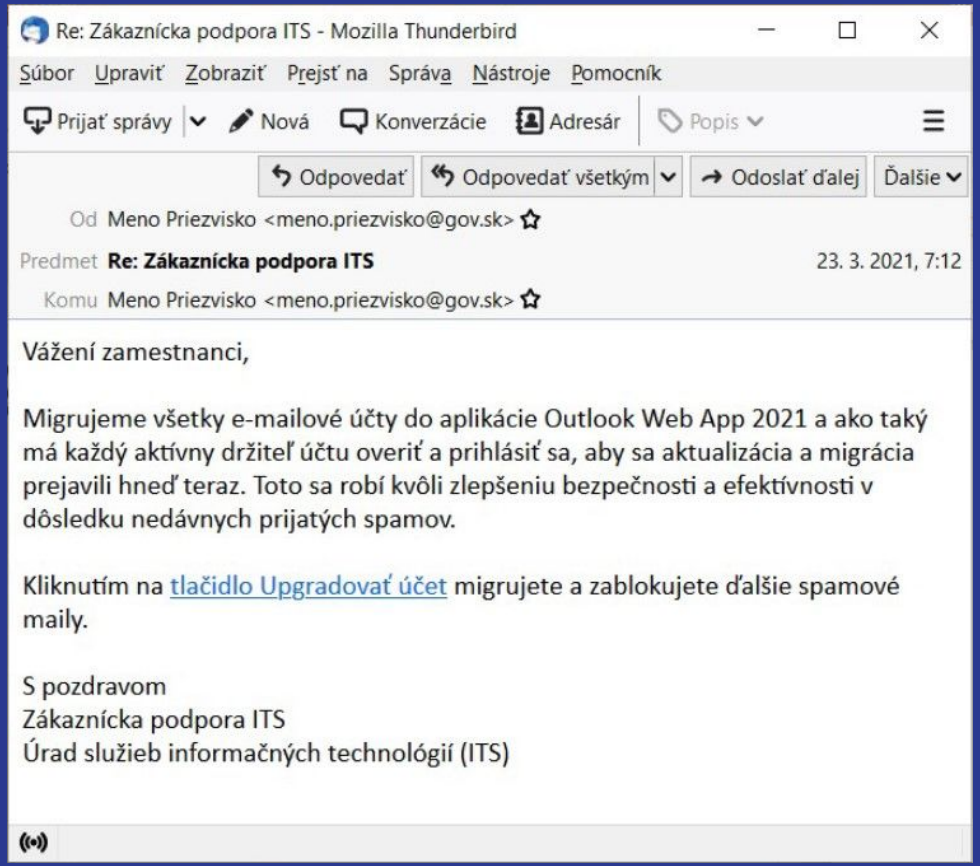
Spear phishing

Vishing

Phishing (I.)

- Veľká väčšina útokov začína Phishingom
- Jeden z najčastejších spôsobov pre získavanie osobných údajov
- Email, ktorý vyzerá dôveryhodne využíva rôzne dôvody, ako napríklad:
  - Získanie peňazí
  - Oznámenie o ukončení platnosti účtu alebo zablokovaní účtu
  - Žiadosť o overenie totožností a iných údajov (napr. číslo karty)

Phishing (II.)


Re: Zákaznícka podpora ITS - Mozilla Thunderbird
Súbor Upraviť Zobraziť Prejsť na Správa Nástroje Pomocník
Prijať správy
Nová
Konverzácie
Adresár
Popis
Odpovedať
Odpovedať všetkým
Odoslať ďalej
Ďalšie
Od Meno Priezvisko <meno.priezvisko@gov.sk>
Predmet Re: Zákaznícka podpora ITS
23. 3. 2021, 7:12
Komu Meno Priezvisko <meno.priezvisko@gov.sk>
Vážení zamestnanci,
Migrujeme všetky e-mailové účty do aplikácie Outlook Web App 2021 a ako taký má každý aktívny držiteľ účtu overiť a prihlásiť sa, aby sa aktualizácia a migrácia prejavili hneď teraz. Toto sa robí kvôli zlepšeniu bezpečnosti a efektívnosti v dôsledku nedávnych prijatých spamov.
Kliknutím na tlačidlo Upgradovať účet migrujete a zablokujete ďalšie spamové maily.
S pozdravom
Zákaznícka podpora ITS
Úrad služieb informačných technológií (ITS)

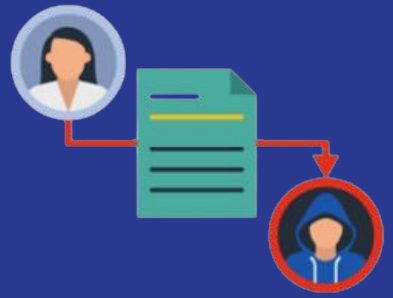
Spear phishing

Spear phishing - je narozdiel od phishingu priamo cielený na konkrétnu osobu alebo organizáciu

- Útočník si určí o aké dáta mu ide a identifikuje osobu, ktorá tieto dáta má

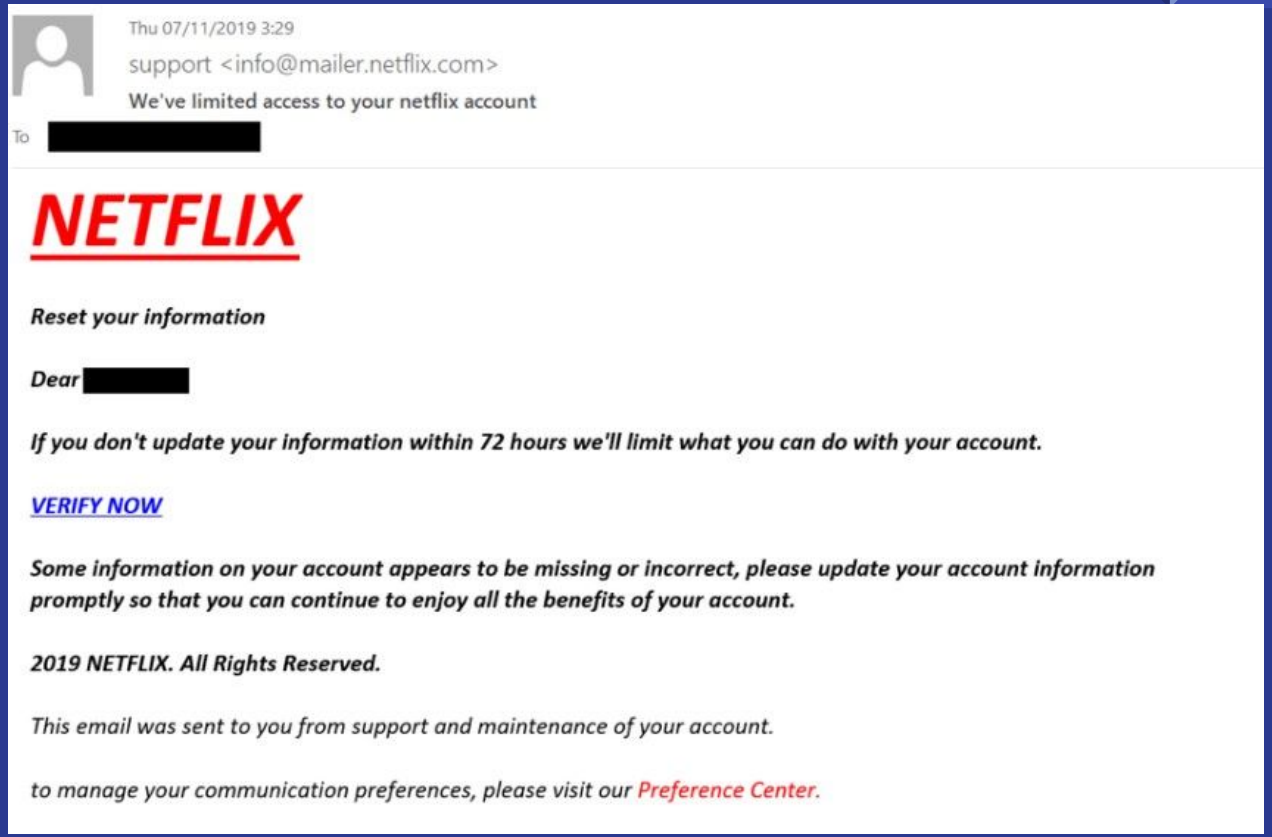
- Útočník kontaktuje danú osobu alebo organizáciu a predstiera, že je dôveryhodná osoba

- Útočník presvedčí danú osobu, aby mu požadované dáta poskytne alebo vykoná škodlivú aktivitu v napadnutom zariadení



Zdroj: https://us.norton.com/internetsecurity-malware-what-spear-phishing.html

Spear phishing (II.)



Thu 07/11/2019 3:29

support <info@mailer.netflix.com>

We've limited access to your netflix account

To [redacted]

NETFLIX

Reset your information

Dear [redacted]

If you don't update your information within 72 hours we'll limit what you can do with your account.

VERIFY NOW

Some information on your account appears to be missing or incorrect, please update your account information promptly so that you can continue to enjoy all the benefits of your account.

2019 NETFLIX. All Rights Reserved.

This email was sent to you from support and maintenance of your account.

to manage your communication preferences, please visit our Preference Center.

Vishing

Ako prebieha?

- Podvodníci vám môžu priamo zavolať na telefón a predstierajú, že zástupcovia technickej spoločnosti
- Môžu sa vydávať za dôveryhodné číslo spoločnosti a oklamať tak obeť
- Môžu požadovať o inštaláciu aplikácie tretej strany do vášho zariadenia, aby k nemu mali vzdialený prístup

- Útočníci môžu taktiež nadviazať kontakt zobrazením falošných hlásení chýb na webstránke, ktorú navštívite
- Môžu vás tak nalákať na sfalšované číslo, ktoré má zobrazovať technickú podporu pre určitý problém

Tzv. falošná technická podpora

Ako sa chrániť ?

Phishing a Spear phishing

- Emaily ponúkajú niečo lákavé alebo vyvolávajú hrozbu
- Vždy keď ide o príliš dobrú ponuku, spozornite !
- Phishing sa riadi podľa aktuálnych trendov a snaží sa tým vzbudiť dôveru
- Mali by ste si všímať email odosielateľa, meno a doménu v emailovej adrese
- Všimnúť si, že ponúkajú obmedzený čas na rýchlu reakciu obete
- Dávať pozor na možné tlačidlo v emaile, ktoré smeruje na podvodnú stránku

Vishing

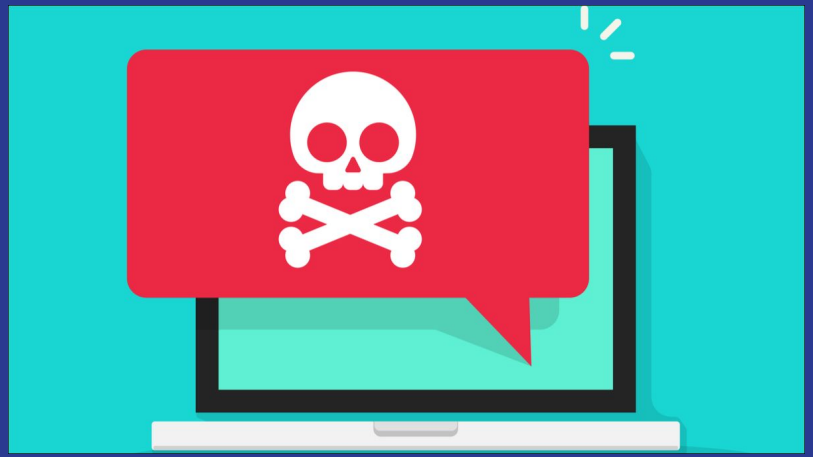
- Väčšina dôveryhodných spoločností neposiela nevyžiadané emailové správy a neuskutočňujú nevyžiadané hovory, aby od vás vyžiadali osobné či finančné informácie
- Ak sa na vašej obrazovke objavia malé vyskakovacie okná v ktorých môže byť spomenuté číslo na ktoré máte zavolať je dobré si ho predtým overiť alebo okno iba zatvoriť

Malware

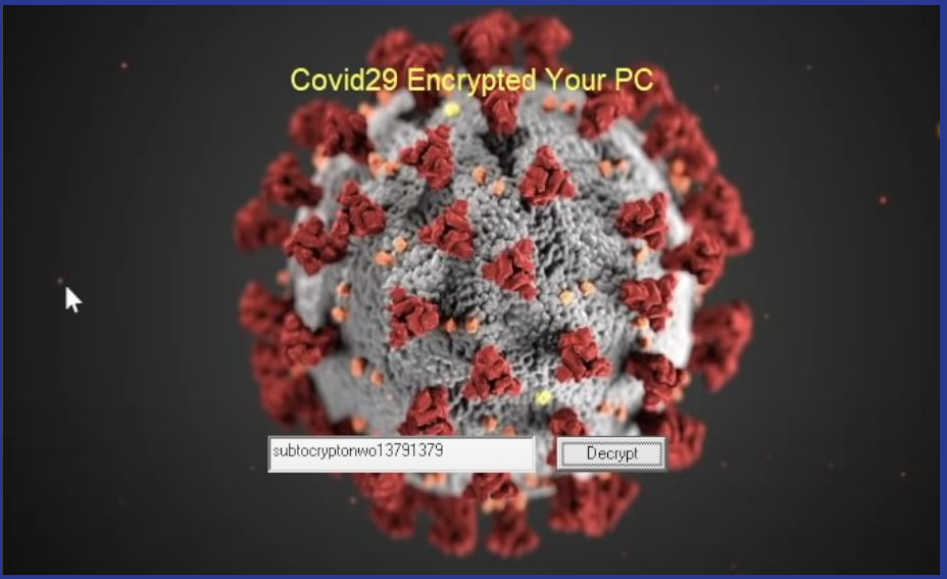
- Škodlivý kód
- Môže byť skrytý v podvodnej správe
- Zvyčajne napácha viac škôd ako predošlé 3 typy útokov

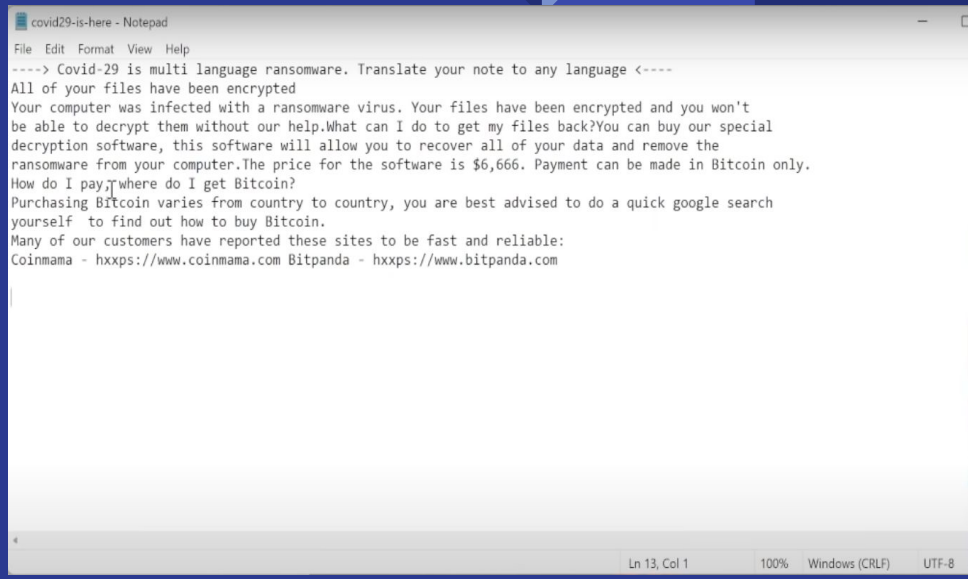
Čo môže spôsobiť ?

- prístup do zariadenia odkiaľkoľvek
- ťaženie krypta
- zasielanie údajov
- prístup do rôznych účtov obete
- šifrovanie dát a požadovanie výkupného
- stiahnutie ešte viac škodlivého kódu



Ukážka malvéru





Ako zistím, že môj počítač má malware?

- zariadenie je spomalené alebo nereaguje
- v počítači pribudli neznáme súbory
- váš internetový prehliadač je spomalený
- počítač sám od seba vykonáva určité akcie (reštart, vypnutie, zatváranie okien,...)
- časté vyskakovanie error správ
- nemôžete sa dostať do určitých oblastí zariadenia

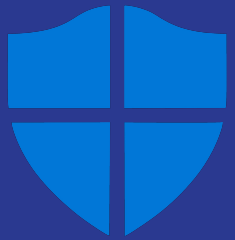
Ako sa chrániť pred malvérom?

- Antivírus
- Aktualizácia systému
- Nesťahovať a neotvárať neoverené súbory (najčastejšie cez torrent alebo zo stránok typu ulož.to)

Najlepšie antivírusové programy:

Sophos

ESET



Windows Defender

Overte si vaše E-maily a heslá!

Have I Been Pwned: https://haveibeenpwned.com/ --- Preverenie či ste neboli súčasťou úniku dát
Firefox Monitor: https://monitor.firefox.com/ --- Taktiež preverenie či ste neboli súčasťou úniku dát
Have I Been Sold: https://haveibeensold.app/ --- Preverenie či Váš E-mail nebol predaný
CSIRT UPJS: https://csirt.upjs.sk/phishing/ --- Otestujte sa či dokážete rozpoznať podvodný E-mail!

Otestuj sa!

Aké silné je vaše heslo?

Bol si súčasťou úniku dát?

Predali vašu E-mail adresu?

Rýchly Quiz

joinmyquiz.com

Ďakujeme za pozornosť!