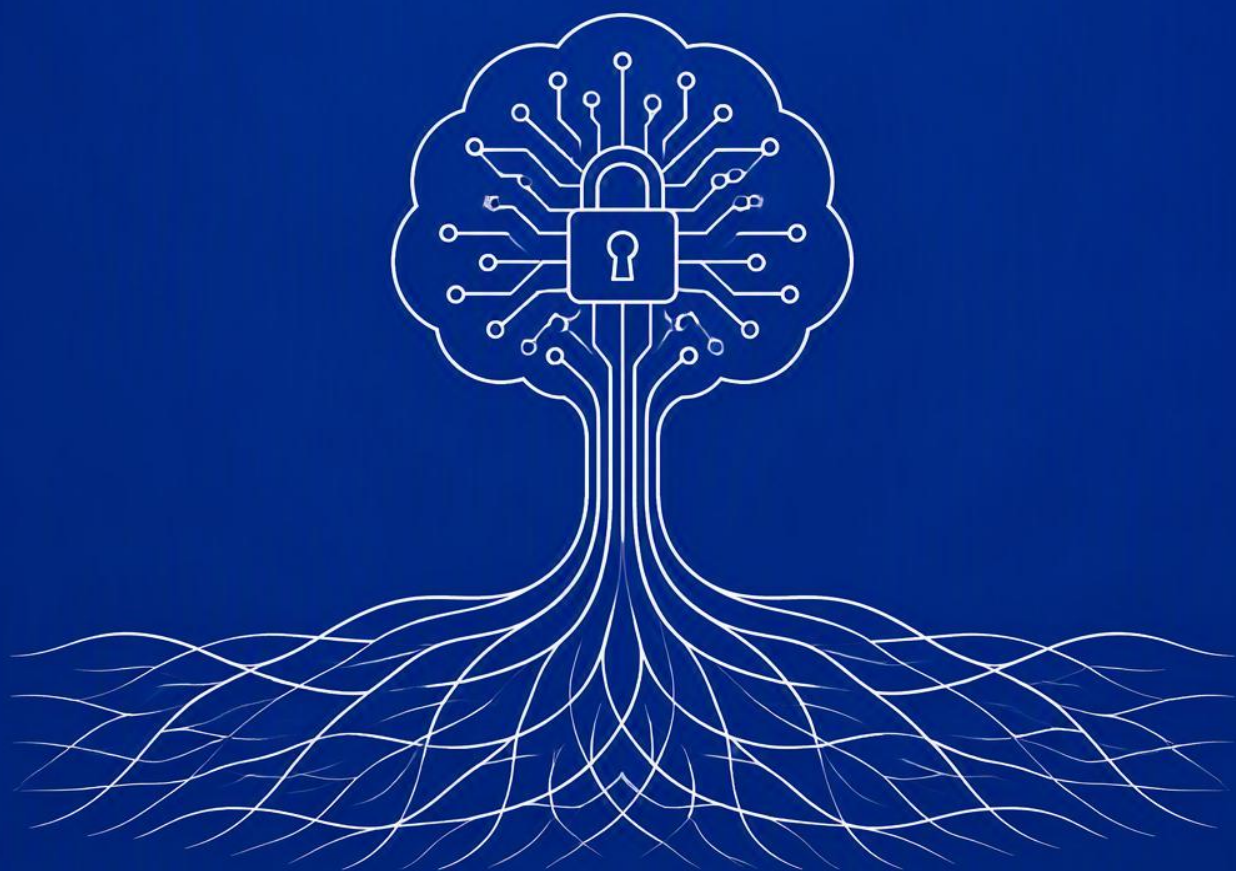




**Co-funded by
the European Union**

Digitálna bezpečnosť pre MVO:

Praktický sprievodca



Sprievodca digitálnou bezpečnosťou pre mimovládne organizácie (MVO) bol vypracovaný v rámci projektu „Fostering CSOs' Resilience to Shrinking Spaces and Strengthening their Capacities through Individual Mentoring and Value Mainstreaming in Hungary and Slovakia“ (FOREST), ktorý spoločne realizovali Alternative Communities Association (ACA), Partners for Democratic Change Slovakia (PDCS) a Transatlantic Foundation (TF).

Autor: Lukáš Zorád

Uverejnené: 31. augusta 2026



**Co-funded by
the European Union**

Projekt FOREST spolufinancovaný Európskou úniou. Uvedené názory a stanoviská sú však výlučne názormi autora (autorov) a nemusia sa zhodovať s názormi Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani poskytovateľ grantu EACEA nenesú za ne žiadnu zodpovednosť.

Obsah

1	Ako používať tento sprievodcu	4
2	Základné princípy online bezpečnosti:	4
3	Úniky dát.....	5
4	Heslá	5
5	Šifrovanie dát	7
5.1	Šifrovacie zariadenia.....	7
5.1.1	Pre Androidy:	8
5.1.2	Pre Windows:	8
5.1.3	Pre Mac OS X:	9
6	Malvér	9
6.1	Ako sa ku vám malvér môže dostať?	10
6.2	Ako sa môžeme voči malvéru chrániť?	11
6.3	Ako sa vyhnúť phishingu a ako ho vôbec rozoznať?.....	11
6.4	Sociálne inžinierstvo	12
6.5	Typy Malvéru.....	13
7	IP adresa a VPN	13
7.1	Spôsoby akými sa niekto môže zmocniť tvojej IP adresy	13
7.2	VPN.....	14
8	Bezpečnosť na sociálnych sieťach a nastavenia súkromia	16
9	Zdroje	17
10	Príloha 1: Cvičenie - Čo sme ochotní nahráť na sociálne médiá a prečo?.....	19
11	Príloha 2: Bezpečnostný plán - vzor	20

1 Ako používať tento sprievodcu

V jednotlivých kapitolách sú prehľadne spísané tipy a konkrétne kroky k lepšej digitálnej bezpečnosti mimovládnych organizácií. Nie je nutné si prečítať celého sprievodcu naraz, ale pri jednotlivých krokoch implementácie stačí zvoliť príslušnú kapitolu. Napríklad, ak si chcem nainštalovať VPN, kvôli ochrane osobných údajov a hackerským útokom, pozriem si kapitolu VPN.

2 Základné princípy online bezpečnosti:

Na to, aby sme boli v online priestore vo väčšom bezpečí, si môžeme zapamätať tieto 4 princípy, ktoré nám pomáhajú pochopiť, čo sa práve deje, aký to bude mať dopad a aké kroky musíme podniknúť k tomu, aby sme ostali v bezpečí, respektíve znížili potenciálne škody.

1. Čokoľvek, čo dáte na internet, zostáva na internete a nie je anonymné

Informácie zverejnené na internete sa dajú veľmi ťažko úplne odstrániť. Fotografie, komentáre, príspevky či dokumenty môžu byť skopírované, archivované alebo uložené inými ľuďmi bez vášho vedomia. Aj keď používate prezývku alebo anonymný účet, kombinácia rôznych údajov často umožňuje identifikovať konkrétnu osobu. Preto je dobré pred zverejnením zvážiť, či by vám daná informácia nemohla v budúcnosti spôsobiť problémy.

2. Najslabším článkom kybernetickej bezpečnosti je človek

Väčšina úspešných kybernetických útokov nezačína prelomením technológií, ale oklamaním ľudí. Útočníci využívajú nepozornosť, zvedavosť, časový tlak alebo dôveru, aby získali heslá, citlivé údaje či prístup do systémov. Aj najlepšie technické zabezpečenie môže zlyhať, ak používateľ klikne na podvodný odkaz alebo poskytne informácie neoprávnenej osobe. Bezpečné správanie ľudí je preto rovnako dôležité ako kvalitný softvér.

3. Pripravte sa na to, že hackeri vás napadnú – už sa to určite stalo a aj sa to stane

Úplná ochrana pred útokmi neexistuje. Každý používateľ, organizácia či firma je potenciálnym cieľom automatizovaných alebo cielených útokov. Dôležité preto nie je len snažiť sa útokom predchádzať, ale aj pripraviť sa na situáciu, keď k nim dôjde. Pravidelné aktualizácie, zálohy, silné heslá a viacfaktorové overovanie výrazne znižujú škody, ktoré môže útok spôsobiť.

4. Systémovo zabezpečené súkromie je istejšie ako sľubované súkromie

Pri ochrane súkromia je lepšie spoliehať sa na technické riešenia než na deklarácie poskytovateľov služieb. Ak je komunikácia šifrovaná, údaje sú minimalizované a bezpečnostné opatrenia sú zabudované priamo do

systemu, ochrana nezávisí iba od dobrej vôle prevádzkovateľa. Sľuby o ochrane súkromia sa môžu časom meniť, technické zabezpečenie však poskytuje konkrétnu a overiteľnú úroveň ochrany.

3 Úniky dát

Môžete si skontrolovať, či máte účet, ktorý bol napadnutý v dôsledku porušenia ochrany údajov, na stránke <https://haveibeenpwned.com/>, ktorá je dnes už integrovaná priamo do webového prehliadača Firefox, kde si môžete nastaviť bezpečnostné upozornenia pre prípad, že dôjde k úniku vášho hesla, alebo vašich dát. Stačí zadať svoju e-mailovú adresu alebo používateľské meno, aby ste zistili, či je vaše heslo nezabezpečené¹.

Ak zistíte, že dáta z vašich účtov unikli (zobrazia sa na červeno a v texte sa dozviete presne ktoré vaše dáta unikli na dark web), postupujte podľa navrhovaných krokov. Vo väčšine prípadov postačí zmeniť heslo, odhlásiť účet zo všetkých zariadení a pokiaľ je účet dôležitý, zabezpečiť ho dvojfaktorovou autentifikáciou.

<https://monitor.firefox.com/>

<https://haveibeenpwned.com/>

<https://haveibeenpwned.com/Passwords>

4 Heslá

Heslá sú dôležitou súčasťou zabezpečenia toľkých vecí, ktoré používame - od našich sociálnych médií cez náš e-mail až po naše bankovníctvo.

Často sú prvou a jedinou bariérou medzi vašimi informáciami a každým, kto by si ich mohol prečítať, použiť alebo zničiť bez vášho súhlasu.

Môžete použiť najpokročilejšie bezpečnostné nástroje, ale ak je vaše heslo slabé alebo ak mu dovoľíte, aby sa dostalo do nesprávnych rúk, neurobí vám to dobre.

Použili ste napríklad niekedy niektoré z týchto hesiel?

- 1 - 123456 (Najbežnejšie heslo od roku 2018)
- 2 - 123456789
- 3 - qwerty
- 4 - password (Zostup o dve priečky nižšie, dlhodobo bolo na druhom mieste)
- 5 - 1234567
- 6 - 12345678
- 7 - 12345
- 8 - iloveyou

¹ Doplnkové čítanie v angličtine <https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/>

- 9 - 111111
- 10 - 123123
- 11 - abc123
- 12 - qwerty123
- 13 - 1q2w3e4r
- 14 - admin
- 15 - qwertyuiop
- 16 - 654321
- 17 - 555555
- 18 - lovely
- 19 - 7777777
- 20 - welcome

Kompletný rebríček najbežnejších hesiel aj ich vývoj v čase si môžete pozrieť tu:

https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Ak používate ktorékoľvek z týchto hesiel, musíte ich zmeniť.

Prečo?

Pretože protivníci používajú na získanie prístupu do vášho účtu zoznamy najbežnejších hesiel.

Ďalším rizikom je opätovné použitie hesiel. Služby sú niekedy hacknuté a heslá sú odcudzené.

To znamená, že ak ste použili rovnaké heslo v dvoch službách a dôjde k napadnutiu prvej služby, protivník sa pokúsi použiť toto heslo v druhej službe.

Ak ste heslo znova použili, môžu získať prístup k vašim účtom.

Ako vytvoriť silné heslá?

Skontrolujte, ako ľahko je možné do vášho hesla zahrnúť heslo: <https://howsecureismypassword.net/>

Rady/Pravidlá na vytvorenie silného hesla

- **Dĺžka hesla je dôležitejšia ako použitie znakov/čísel/veľkých malých písmen** (Napríklad heslo Lukas38! je slabé heslo, na rozkódovanie stačí 8 hodín)
- **Použite frázu, resp celú vetu v slovenčine:** „moja obľúbená kultová kniha je o čiernom zadku“ (2 trigintillion years)
- **Nikde neopakujte rovnaké heslá,**
- **Neprihlasujte sa cez iné aplikácie** (Facebook, Gmail), aj keď je to pohodlné
- **Zapnite si dvojfaktorovú autentifikáciu pri skutočne dôležitých kontách** (banky to vyžadujú, emaily, Facebook)

Ďalšie dobré rady: <https://www.eset.com/sk/blog/domaca-it-bezpecnost/ako-vytvorit-nepriestrelne-heslo/>

Password manager ako riešenie na nezabúdanie hesiel:

Môžete tiež použiť <https://www.KeepassX.org/>,

Bitwarden <https://bitwarden.com/> alebo platený

1password <https://1password.com/haveibeenpwned/ohno/>

a vždy použiť dvojfaktorovú autentifikáciu.

5 Šifrovanie dát

Šifrovanie je spôsob, ako zvýšiť bezpečnosť správy alebo súboru zakódovaním obsahu tak, aby ho mohol prečítať iba ten, kto má správny šifrovací kľúč alebo heslo na jeho dešifrovanie.

Čo robí šifrovanie?

Chráni vaše dáta pred prístupom alebo manipuláciou ktokoľvek, kto ich nechce vidieť.

V prípade komunikácie šifrovanie tiež pomáha zabezpečiť, aby sme hovorili so správnou osobou, a nie s podvodníkom.

Ako môžem zašifrovať údaje?

Veracrypt je dobrý, bezplatný nástroj na šifrovanie otvoreného zdroja. Rovnako ako trezor, VeraCrypt vytvorí v počítači alebo na pevnom disku šifrovaný kontajner, do ktorého môžete vložiť toľko súborov, koľko chcete.

Pamätajte:

- Šifrovaný kontajner musíte vždy zavrieť, aby fungoval.
- Protivníci, ktorí nedokážu prelomiť vaše šifrovanie, sa vám môžu pokúsiť ukradnúť heslo a získať prístup týmto spôsobom.
- Uistite sa, že používate veľmi silné heslá a tiež postupujte podľa pokynov v kurze škodlivého softvéru.

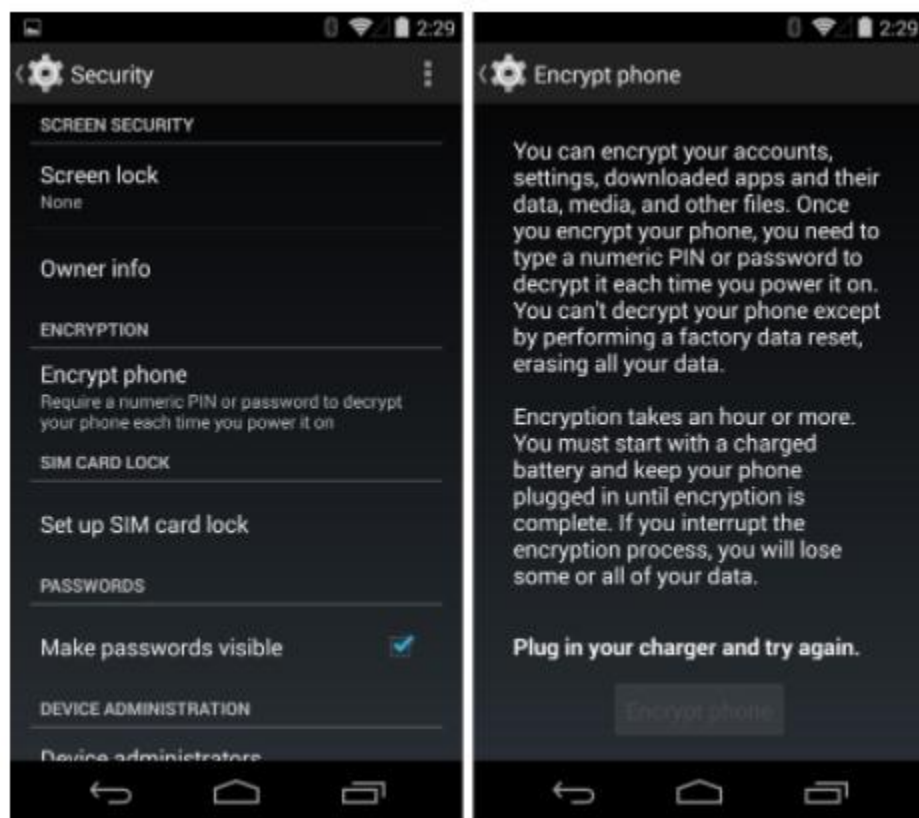
5.1 Šifrovacie zariadenia

Šifrovanie vašich zariadení, napríklad počítača a telefónu, je dôležité. Bez neho môže ktokoľvek, kto získa fyzický prístup k vášmu zariadeniu, ľahko získať prístup ku všetkým vašim informáciám. Mnoho zariadení má v súčasnosti zabudované šifrovanie „celého zariadenia“, ktoré môžete zapnúť, aby ste tomu zabránili.

Ukážeme si, ako zapnúť šifrovanie v telefónoch so systémom Windows, Mac OS X a Android.

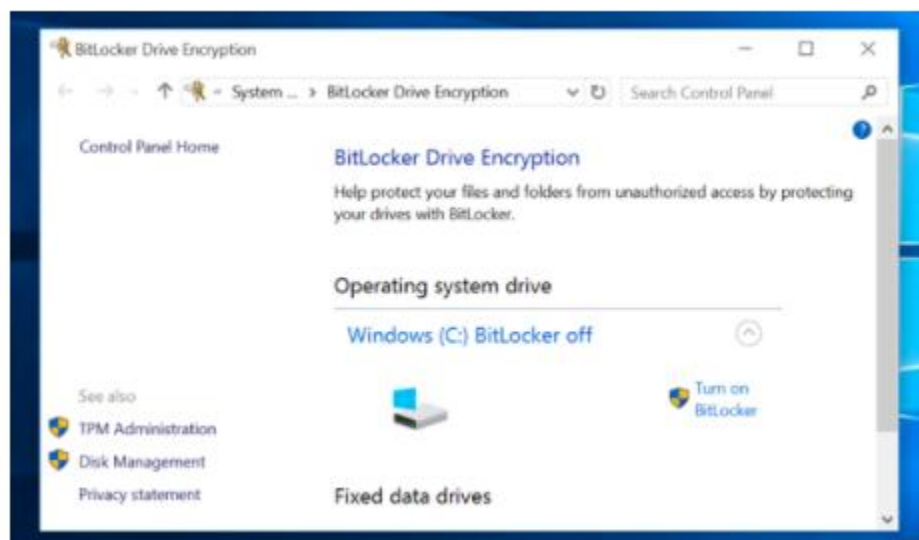
Všetky Apple iPhone aktualizované na najnovšiu verziu softvéru majú automaticky zapnuté šifrovanie.

5.1.1 Pre Androidy:



1. Chodíte do nastavení (Settings)
2. Choďte do bezpečnosti (Security)
3. Zvoľte Šifrovať telefón (Encrypt Phone)

5.1.2 Pre Windows:



Digitálna bezpečnosť pre MVO

1. Chodíte do Ovládacieho panelu (Control Panel)
2. Bitlocker
3. Zvoľte “Šifrovat” (Encrypt)

5.1.3 Pre Mac OS X:



1. Chodíte do Systémové preferencie (System Preferences)
2. Bezpečnosť a súkromie (Security & Privacy)
3. Zvoľte FileVault

Pamätajte:

- Aby šifrovanie fungovalo, musíte vždy vypnúť počítač alebo zamknúť telefón.
- Vaša bezpečnosť je rovnako silná ako vaše heslo.
- Uistite sa, že používate veľmi silné heslá.
- Postupujte tiež podľa pokynov v kurze škodlivého softvéru.

6 Malvér

Malvér je všeobecný zastrešujúci pojem pre viacero druhov škodlivého softvéru, ktorý sa potenciálny útočník môže snažiť dostať do vášho zariadenia (mobil, tablet, laptop, PC).

Určite ste už počuli výrazy ako počítačový vírus, červ, trójsky kôň, spyware, ransomware.. Všetko sú to typy malvéru (z anglického malware, Malicious software /škodlivý softvér), ktorých cieľom je dostať sa do vášho zariadenia a ukradnúť z neho informácie, prípadne zamedziť váš prístup k vašim informáciám za účelom

vydierania. Malvér umožňuje útočníkom kontrolovať vaše zariadenie na diaľku. Môže sa dostať k vašim citlivým údajom, platobným kartám, môže vo vašom mene rozosielať emaily a správy a tak šíriť citlivý kód ďalej a podobne. Tu je zopár príkladov toho, čo môže útočník robiť:

1. Nainštaluje si u vás v zariadení tzv. keylogger.

Všetko, čo píšete v zariadení, zaznamenáva. Takto si môže prečítať napríklad vaše heslá (aj preto bývajú heslá väčšinou skryté pod symbolmi ako bodky, alebo hviezdičky)

2. Screenshots.

To znamená, že si spraví fotografiu vašej obrazovky každých pár sekúnd, čiže dokáže potom zrekonštruovať, čo presne ste robili a navždy uchovať napríklad vaše osobné konverzácie, či fotografie o ktorých si myslíte, že ich vidíte iba vy.

3. Môže prehľadávať vaše dokumenty.

4. Môže získať prístup ku vašej web kamere a mikrofónu, čím môže vyhotovovať nahrávky z vašej domácnosti/pracovne atď.

5. Môže vám zmazať dokumenty.

6. Môže vám zašifrovať dokumenty a donútiť vás zaplatiť výkupné, ak sa k nim chcete ešte niekedy dostať.

7. Môže získať prístup k vašim systémovým zariadeniam a svojvoľne ich meniť

6.1 Ako sa ku vám malvér môže dostať?

- Cez infikovaný hardvér, ako napríklad USB kľúč. Poznáme prípady z rôznych konferencií, kedy účastníci konferencie dostali medzi reklamnými materiálmi infikované USB kľúče².
- Kliknutím na neznámy škodlivý link, cez ktorý sa k vám vírus stiahne (napríklad cez falošný reklamný banner).
- Stiahnutím prílohy emailu.
- Z tzv. “Drive-by downloads”, malvér, ktorý sa automaticky začne sťahovať, keď navštívite nejakú nastraženú webstránku.
- Cez softvér, ktorý nemá licenciu, tzv. “cracked” softvér. Tu väčšinou útočníci zneužívajú fakt, že ľudia si chcú vyskúšať nový softvér zadarmo a stiahnuť si ho bez zaplatenia oficiálnemu distribútorovi, alebo jednoducho nemajú dosť peňazí (častým príkladom je Windows). Napriek tomu, že nie všetok zadarmo

² Winners of security award rewarded by infected USB sticks

<https://www.welivesecurity.com/2018/01/12/taiwan-rewards-winners-malware-usb-sticks/>

softvér na internete je škodný, jeho stiahnutím sa vystavujete vyššiemu riziku, že si stiahnete infikovaný softvér.

6.2 Ako sa môžeme voči malvéru chrániť?

Spôsob akým sa ku nám dostáva malvér nám zároveň ponúka odpovede na to, ako sa chrániť.

- Nainštalujte si antivírus s dobrou reputáciou, existujú aj bezplatné verzie antivírusov: Antivírusové firmy dnes zachytávajú až 300.000 nových a dovtedy neznámych škodlivých kódov denne a pômôžu vám zachytiť najzákladnejšie škodlivé kódy ešte pred tým, ako sin a nich kliknete. Dôležité sú pravidelné updaty antivíru (ideálne si nechať automatické nastavenie pravidelného update).
- Používajte softvér s licenciou a povoľte pravidelné updaty. Každý softvér má potenciálne bezpečnostné diery, ktoré čakajú na ich objavenie. Solídne firmy preto pravidelne vydávajú tzv. Záplaty, ktoré váš softvér ochránia pred zneužitím odhalených bezpečnostných dier.
- Dávajte si veľký pozor na tzv. Phishing: Pozor na túto formu útoku, pretože útočníci sa často môžu vydávať za niekoho, koho poznáte a komu dôverujete, a z adresy, ktorá je podobná adrese vášho kamaráta vám pošlú malvér, či už vo forme linku, alebo prílohy v emaily. Keďže ide o najčastejší prípad útoku, rozoberieme si ho podrobnejšie.
- Pozor na sociálne inžinierstvo: psychologická manipulácia ľudí k tomu, aby nám poskytli dôverné informácie. Sociálne inžinierstvo môže byť aj dobré, ale aj zlé, viac detailov nižšie.

6.3 Ako sa vyhnúť phishingu a ako ho vôbec rozoznať?

Dostanete email, alebo osobnú správu na sociálnych sieťach. Pokiaľ je to od niekoho, koho nepoznáte, alebo od koho správu neočakávate, ihneď si overte, či ide o legitímny kontakt, alebo nie. Omnoho horšie je, keď dostanete škodlivú prílohu, alebo link od niekoho, koho poznáte, alebo komu dôverujete. To totiž znamená, že útočník sa nabúral do konta tohto človeka a rozosiela emaily, alebo správy v jeho mene, no i tu sa dá pracovať s pravdepodobnosťou toho, či takú správu od toho človeka očakávate, alebo nie. Napríklad, keď dostanete od svojho šéfa, alebo od svojej mamy čudnú prílohu, alebo čudný link, bez nejakých konkrétnych vysvetlení a viete, že takýto štýl emailu nezvyknete od nich dostávať, automaticky treba byť podozrievavý. Sofistikovanejšie útoky už dnes kopírujú dokonca aj štýl a spôsob komunikácie na aký sme zvyknutí a tu už je rozoznanie phishingu naozaj ťažké.

Dobrá správa je, že na to, aby malvér, ktorý je vám zaslaný prostredníctvom phishingu, fungoval, musí sa dostať do vášho zariadenia a tomu vieme predísť.

Ďalší spôsob phishingu je získať váš login a heslo cez stránky, ktoré pravidelne navštevujete, napríklad cez gmails, Facebook, alebo online noviny, ktoré čítate. Väčšinou dostanete falošný email tváriaci sa ako správa od poskytovateľa služby s okamžitou požiadavkou o zmenu hesla a linkom, kde tak môžete urobiť. Ako to v panike a v rýchlosti urobíte, poskytnete svoje heslo útočníkom. Tí vás potom môžu úplne vyblokovat' z vašej služby a samozrejme, dostať sa k vašim údajom. Tu vás môže zachrániť najmä dvojfaktorová autentifikácia.

Odporúčanie: Spravte si krátky kvíz o malvéri a pishingu a všimajte si detaily. Pokojne si kvíz spravte aj 2-3 krát po sebe, pretože takýmto tréningom zvýšite vlastnú citlivosť na podvodné emaily a získate prax a návyk v detailoch, ktoré si treba všímať.

1) v anglickom jazyku <https://phishingquiz.withgoogle.com>

2) v Slovenskom jazyku: <https://safelab.sk/phishingovy-test/start> alebo [6-kapitola-phishing-a-socialne-inzinierstvo | ResilienceLab.online](#)

6.4 Sociálne inžinierstvo

Sociálnym inžinierstvom nazývame psychologickú manipuláciu ľudí k tomu, aby nám poskytlí dôverné informácie. Môže sa to udiať online (napríklad cez telefón), alebo offline (napríklad v kancelárii, na vrátnici a pod.). Napríklad niekto sa vydáva za poštára, donáškovú službu, opravára – skrátka niekoho kto nevzbudzuje podozrenie. Keď sa dostane k nejakému vášmu zariadeniu fyzicky, je preňho jednoduchšie dostať sa do vašich zariadení a obísť vaše bezpečnostné nastavenia (aj preto je potrebné mať na všetkých zariadeniach aktivované rôzne vrstvy ochrany, ako heslo, PIN a pod.). V žiadnom prípade nikdy nedovoľte cudziemu človeku, nech už pôsobí akokoľvek dôveryhodne, aby robil čokoľvek na vašom zariadení (napríklad vás môže poprosiť, či si od vás môže poslať email, alebo zatelefonovať).

Špeciálny pozor si treba dávať na neznáme USB, ktoré si akože niekto niekde zabudol. Naša zvedavosť môže zapríčiniť, že sa budeme chcieť pozrieť, čo na USB je a nevedome si spustíme v našom zariadení malware a umožníme prístup hackerom.

6.5 Typy Malvéru

Stalkerware, alebo spyware

Ide o aplikáciu, ktorá umožňuje útočníkovi špionáž vášho zariadenia, alebo sledovanie vašej polohy a ďalších údajov, bez vášho súhlasu (tu treba podotknúť, že mnohé legálne aplikácie ako gmail, Facebook, chatovacie služby atď, tieto informácie o vás automaticky zbierajú, pokiaľ ich ručne nedeaktivujete). Niektoré takéto aplikácie môžu byť u vás nainštalované aj bez ikonky, takže ich ľahko prehliadnete a vaše zariadenie tak môže byť monitorované na diaľku.

Adware (skratka z anglického *advertising-supported software*) je softvér, ktorý do vášho zariadenia automaticky sťahuje a zobrazuje reklamy. Vývojárom generuje príjmy zakaždým, keď sa reklama zobrazí alebo keď na ňu kliknete. Často sa šíri ako "pribalený" bonus k bezplatným programom alebo aplikáciám.

Vírus: je škodlivý program (malware), ktorý sa sám kopíruje a vkladá svoj kód do iných súborov či programov, **Trójsky kôň** (alebo slangovo **trojan**) je typ škodlivého softvéru (malvéru), ktorý sa maskuje za neškodný alebo užitočný program, aby oklamal používateľa. Na rozdiel od klasických počítačových vírusov sa sám nerozmnožuje ani nenapáda ďalšie súbory, ale spolieha sa na to, že ho používateľ nevedomky sám stiahne a spustí.

Počítačový červ (worm) je typ škodlivého softvéru (malwaru), ktorý sa dokáže sám replikovať a šíriť cez počítačové siete bez toho, aby potreboval akýkoľvek zásah používateľa. Na rozdiel od klasického vírusu sa nepotrebuje „pripojiť“ k inému programu.

Ransomware (alebo ransomvér) je druh škodlivého softvéru (malvéru), ktorý sa nepozorovane dostane do vášho počítača alebo siete. Následne zablokuje prístup k zariadeniu alebo zašifruje vaše súbory a útočníci požadujú zaplatenie výkupného (najčastejšie v kryptomenách) za ich odblokovanie.

Rootkit je zákerný typ škodlivého softvéru, ktorý útočníkovi umožňuje získať kontrolu nad počítačom a zároveň maskuje svoju prítomnosť. Pred bežnými antivírusmi a správcami úloh sa schováva tak, že sa integruje hlboko do operačného systému alebo jeho jadra (kernela)

Keylogger (alebo klávesnicový záznamník) je softvérový program alebo fyzické hardvérové zariadenie, ktoré tajne zaznamenáva každé stlačenie klávesu na klávesnici. Jeho hlavným účelom je špehovanie a krádež citlivých dát, ako sú heslá, čísla kreditných kariet a súkromné správy.

7 IP adresa a VPN

7.1 Spôsoby akými sa niekto môže zmocniť tvojej IP adresy

1

Požičaním si tvojho zariadenia: Keď niekto pracuje na vašom zariadení, jednoducho navštívi stránku WhatIsMyIPaddress.com a je to.

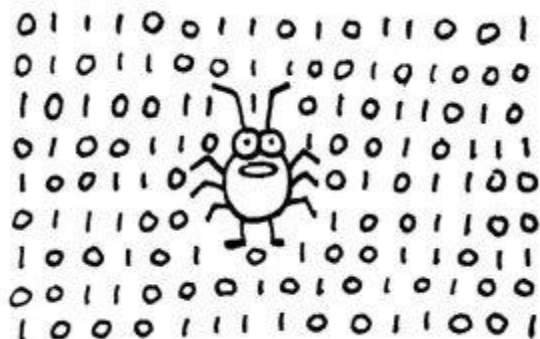
2

Nabúraním sa do tvojej WiFi siete. Ak necháte akéhokoľvek host'a používať vašu WiFi, vie si zistiť vašu IP adresu

3

Pozrie sa na tvoj email: Našťastie dnes už väčšina emailových služieb nezobrazuje vašu IP adresu, ale menší poskytovatelia občas môžu. Skúste si tento nástroj a zistíte, čo o vás vie zistiť ktokoľvek [trace email tool](#).

4



Cez HTML Bug Tento chrobáček nie je zlý, nie je vírusom. Je to kus kódu, ktorý je vložený napríklad do obrázku v emaily. Keď sa naň pozriete, už len tým, že otvoríte ten email, chrobáček povie odosielateľovi, že ste si email prečítali a prezradí mu aj vašu IP adresu. Existujú služby, ktoré napomáhajú ľuďom takýchto chrobáčikov nastaviť [WhoReadMe.com](#).

5

Web server logs. Zakaždým, keď navštívite nejakú webstránku, zanechávate tam vašu IP adresu. Je to niečo ako váš digitálny pas na online pripojenie. Webstránka môže (ak to jej admin tak nastaví) mať prehľad o všetkých IP adresách, ktoré ju navštívili. Pre webstránky to je užitočná informácia, pretože tak vedia zistiť, či ich nejaká IP adresa navštevuje pravidelne, koľko majú náhodných návštev, odkiaľ sú.

6

Internetové fóra a komentáre pod blogmi a článkami: Opäť platí, že pre adminov stránok je veľmi užitočné poznať vaše IP adresy, pretože ak porušujete pravidlá danej stránky, vedia vás zablokovat' (napríklad keď spamujete fórum pod rôznymi užívateľskými menami, ale admin vidí, že je to z jednej a tej istej IP adresy).

7

Cez sociálne siete (Facebook, Twitter, Instagram, Snapchat, etc.) síce neukazujú IP adresy medzi používateľmi, ale administrátori stránok vaše IP poznajú. Taktiež keď na sociálnych médiách kliknete na reklamu, zachytia vašu IP adresu.

9

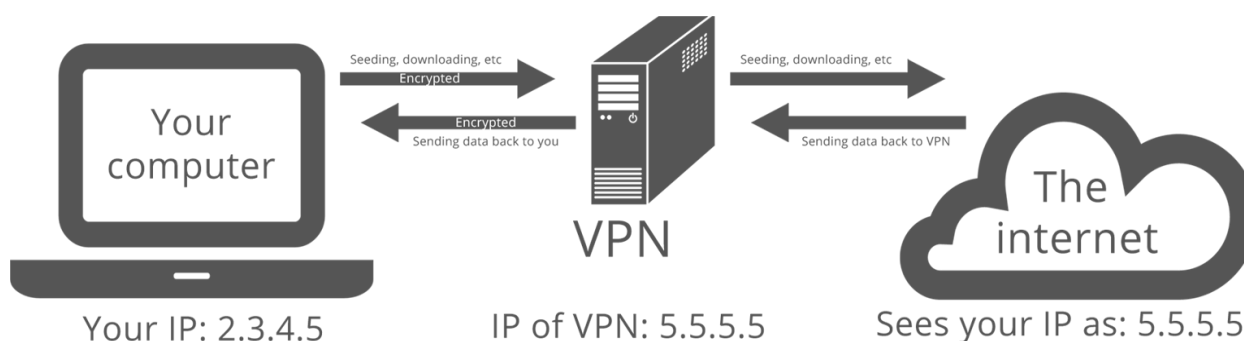
Cez chatovacie aplikácie ako WhatsApp, či Viber, keď kliknete na link v správe, dostávate sa na webovú stránku, ktorá zachytí vaše IP. Takéto sledovacie linky sa dajú vytvoriť napríklad na [grabify.link](#) alebo [iplogger.org](#).

7.2 VPN

Odporúčaný spôsob, ako si môžeme chrániť našu IP adresu a tým pádom ďalšie detaily našej online prítomnosti, je používať tzv. VPN (Virtual Private Network), teda akýsi súkromný a šifrovaný tunel, cez ktorý prúdia naše informácie a online aktivity. Ako to funguje je znázornené na obrázku nižšie. Z vášho zariadenia sa za normálnych okolností pripojíte na internet (ISP – Internet Service Provider), kde bude svietiť vaša IP adresa. Ak sa však pripojíte cez VPN server, tento server zmení vašu IP adresu, aj vašu geografickú polohu a bude šifrovať

(zneviditeľní) vašu online aktivitu a tok dát a informácií. VPN zároveň šifruje stránky, ktoré navštevujete (DNS – Domain Name System), čiže stalker/cielená reklama, nebudú poznať vašu históriu browsovania.

Techsoup Europe odporúča používať Proton VPN, pretože ide z hľadiska bezpečnosti o jeden z najlepšie hodnotených VPN aj preto, že ich jadrový server je tiež pod kľúčom. To znamená, že keď sa aj útočník dostane k VPN server (hackne VPN server), tak na ňom nájde iba šifrované dáta. Samotný Proton VPN nemá prístup k vašim dátam. Sú samozrejme aj iné možnosti pre VPN softvér. Nižšie uvádzame základné rady na čo si dávať pozor pri výbere VPN.



Vyberám si VPN, na čo sa mám pozrieť?

Platené VPN samozrejme ponúkajú lepšie služby ako zadarmo verzie, no každá VPNka je iná. Pri jej výbere dbajte na tieto skutočnosti:

Hodnotenie profesionálnymi recenzentami, ktorí nepracujú pre žiadnu z týchto firiem. Vždy je dobré overiť si zdroje cez viaceré rebríčky a recenzie. Na internete je ich mnoho a takéto overovanie netrvá zas až tak dlho.

Zdieľané IP adresy: Vyberte si také VPN, ktoré ponúka zdieľané IP adresy, to znamená, že viacero zariadení od rôznych užívateľov, bude mať rovnakú IP. Čím viac takýchto anonymných užívateľov, tým súkromnejšie je vaše prehliadanie, pretože je pre útočníka nemožné rozoznať, kto je kto.

Servery: Čím viac serverov má firma k dispozícii, tým kvalitnejšie bude pripojenie.

Šifrovanie: Aktuálne je najbezpečnejšie šifrovanie AES-256 (Advanced Encryption Standard), ktoré je prakticky neprelomiteľné, pretože používa viacero šifrovacích kombinácií, ako existuje hviezd vo vesmíre (obrazne povedané).

Protokol: Vyhýbajte sa slabším protokolom ako je PPTP a radšej zvolte spoľahlivejšie Open VPN.

Záznamy dát: zvolte si takú VPNku, ktorá neuchováva vaše dáta (čiže nezaznamenáva vaše online aktivity). O tom, či tak robí, alebo nerobí sa dozviete v ich pravidlách.

Bezplatná skúšobná verzia – Je skvelé si niečo vyskúšať, kým to začneme používať.

8 Bezpečnosť na sociálnych sieťach a nastavenia súkromia

Sociálne siete do našich životov nepochybne prinášajú rôzne výhody ako napríklad jednoduchšiu koordináciu aktivít s priateľmi, rodinou, či kolegami, mnohé organizácie dlhodobo promujú svoje aktivity a obsah práve cez sociálne médiá, naše poslanstvo sa dostane k veľkému počtu ľudí, no používanie sociálnych sietí prináša aj rôzne riziká. V tejto kapitole sa pozrieme na tieto riziká a ukážeme si základné možnosti ako im predchádzať, alebo ich minimalizovať.

Väčšina sociálnych sietí je zadarmo. Pri tomto modeli zväčša platí, že keď je to zadarmo, produktom sa stávajú užívatelia sociálnych sietí a ich dáta. Dáta o ich správaní, súkromí, záujmoch a podobne. Keď pri prihlasovaní sa do sociálnej siete stlačíme tlačidlo „Akceptujem“, väčšinou súhlasíme s tým, že tieto firmy majú právo zhromažďovať naše osobné údaje ako protislužbu za ich služby. Tým pádom môžu sledovať našu aktivitu a mať prístup napríklad aj k stránkam našich organizácií, ktoré manažujeme.

Čo všetko sociálne siete vidia/vidia?

- S kým sa priateľíme
- S kým a o čom sme sa rozprávali
- Kedy sa s nimi rozprávame
- Kedy trávime na sociálnej sieti čas
- Kedy a kde sa nachádzame
- Aký tip informácií sledujeme, čo nás zaujíma
- Čo si nakupujeme a mnohé ďalšie

Metadáta zväčša slúžia na cielenejšiu reklamu a obsah, ktorý vám sociálne siete ponúkajú, čo nemusí byť nevyhnutne zlé, avšak metadáta majú aj svoje temné stránky. V rôznych krajinách ich využívajú vlády na sledovanie občianskych aktivistov, ale k týmto metadátam sa môžu dostať aj iní ľudia. Útočníci sa vám rôznym

spôsobom môžu nabúrať do vášho konta (hackerský útok, phishing a ovládnuť vaše konto. Môžu ho použiť rôznym spôsobom, napríklad na zdieľanie dezinformácií o vás a akoby od vás, môžu ho využiť na rozosielanie škodlivého kódu (malware), aby sa dostali k citlivým dátam ďalších ľudí, čo môžu využiť na vydieranie.

Aby sme zminimalizovali tieto riziká, môžeme si upraviť naše bezpečnostné nastavenia.

Princípy používanie sociálnych sietí a odporúčania nastavenia súkromia:

- Limitujte viditeľnosť svojich príspevkov (verejné vs. privátne)
- Majte založené separátne kontá, jedno pracovné a jedno súkromné
- Limitujte množstvo osobných a senzitívnych príspevkov
- Uzatvárajte skupiny a kontrolujte, koho do nich vpustíte
- Nezverejňujte detaily o stretnutiach aktivistov, určite nezverejňujte lokalitu stretnutia, ak to nie je nutné
- Vypnite si zdieľanie lokality (location settings)
- Nikdy nenechávajte sociálnu sieť pamätať si vaše bankové údaje,
- Keď niekoho nepoznáte, nikdy mu nepotvrdte priateľstvo
- Pozor na falošné účty, ktoré vyzerajú ako vaši priatelia. Ak dostanete žiadosť o priateľstvo od niekoho koho poznáte, overte si, či je to naozaj on/ona, ideálne telefonicky. Útočníci sa často vydávajú za vašich priateľov
- Zdieľať čo najmenej, nezdieľať osobné veci
- Byť si vedomý nastavení súkromia a bezpečnosti – limitovať
- Netagovať fotografie, aspoň nie verejné
- Mať vytvorené súkromné konto a pracovné konto na správu stránok
- Obidve kontá mať dobre zabezpečené, používať dvojfaktorovú autentifikáciu,
- Nepoužívať Facebook na prihlasovanie do iných aplikácií!!! Kvôli potenciálnemu úniku osobných údajov a dát,
- Mnohí experti na digitálnu bezpečnosť by povedali, nepoužívať sociálne siete vôbec a keď už tam ste, tak nič nelajkovať, nijako sa neprejavovať, byť anonymný atď (extrém)

Sociálne siete dnes pod tlakom verejnosti, či zákonov umožňujú lepšiu kontrolu vašich osobných dát. Skontrolujte si z času na čas, či sú vaše osobné nastavenia súkromia a bezpečnosti aktuálne, či tam nie je niečo nové.

9 Zdroje

Bezplatné školenia a kvízy o digitálnej bezpečnosti: [ResilienceLab.online](https://resiliencelab.online/) – [Vzdelávacia platforma pre občiansku spoločnosť](#)

Odporúčaná literatúra k rizikám používania sociálnych sietí, ich bezpečnosti, súkromia, ale aj ďalších aspektov používania sociálnych sietí:

- SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company, 2015. ISBN 978-0-393-35217-7.
- SCHNEIER, Bruce. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. New York: W. W. Norton & Company, 2018. ISBN 978-0-393-60960-8.
- MITNICK, Kevin a Robert VAMOSI: *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data..* New York: Little, Brown and Company, 2017. ISBN 978-0-316-38050-8.

Použité zdroje:

- Ako si vybrať správnu VPN: <https://blog.avast.com/cs/jak-si-vybrat-tu-spravnou-vpn>)
- Kontrola IP adresy: <https://whatismyipaddress.com/get-ip> (skrátené)
- Bezpečne na nete, ESET: <https://bezpecnenanete.eset.com/sk/>
- Kyberbezpečnosť – slovník: <https://www.koop.cz/kyberbezpecnost-slovník>
- Kaspersky Resource Center: <https://www.kaspersky.com/resource-center>
- Vizualizácia najväčších únikov dát <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- Rootkity v Digitálnom Svete: Hrozby a Ako sa Chrániť, 9. marca 2026
- Keylogger. Čo to je a ako sa pred ním chrániť, 5 marca, 2025: <https://gdpr-slovensko.sk/keylogger-co-to-je-ako-funguje-a-ako-sa-pred-nim-chranit/>

10 Príloha 1: Cvičenie - Čo sme ochotní nahrat' na sociálne médiá a prečo?

Čo bežne zdieľam na sociálnych médiách? (Príklady)	+ aké výhody mi to prináša? Čo tým získavam?	Aké sú riziká/nevýhody?
<i>Fotky (aj osobné, napr. z dovolenky, rodinných osláv a podobne)</i>	<i>Pozornosť od kamarátov a známych/Nemusím každému zvlášť vysvetľovať, kde som bol a čo som tam robil</i>	<i>Závisť od druhých, Nieкто vie, že teraz nie som doma (zlodeji), veľa osobných informácií, ktoré sú zneužitelné (napr. kam deti chodia do školy),</i>
<i>Fotky detí</i>	<i>Zdieľanie s vzdialenou rodinou a priateľmi</i>	<i>Zneužitie fotografií, ich ukradnutie, identita detí je</i>
<i>Fotky z práce</i>	<i>Prestíž, meno, reklama, budovanie značky, ale aj šírenie povedomia</i>	<i>N/A</i>
<i>Rôzne osobné dilemy</i>	<i>Získam vzhľad od ľudí, s ktorými sa bežne nerozprávam, s ktorými by som sa nestretol,</i>	<i>Nemám kontrolu nad tým, kto si to číta a kedy to na mňa vytiahne</i>
<i>Keď niečo zháňam/potrebujem</i>	<i>Zožením to rýchlejšie, mám rôzne názory od ľudí, ktorým dôverujem</i>	<i>Každý vie, že čo potrebujem, že napr. robím prerábku bytu,</i>
<i>Politické názory / spoločenské názory</i>	<i>Širšie spektrum názorov</i>	

Čo nie sme ochotní nahrat' na sociálne médiá a prečo?

Čo by som nikdy nenahrál na sociálne médiá	Prečo?
<i>Intímne fotografie</i>	<i>Vydieranie, šikana,</i>

11 Príloha 2: Bezpečnostný plán - vzor

Bezpečnostný plán (Meno ORG)

Zoznam ľudí zapojených do implementácie bezpečnostného plánu

Osoby zapojené do navrhovania a realizácie opatrení kybernetickej bezpečnosti			
Meno	Rola	Tel.	E-mail

IT aktíva

Siete, úložiská, servery a zariadenia.

Dôležité údaje, ktoré uchováваме, či sú uložené na e-mailovom serveri, v cloude alebo v Salesforce

Citlivé údaje - čísla kreditných kariet a iné chránené údaje o cieľových skupinách.

Bezpečnostné vybavenie - firewall, antivírusový softvér, ochranné techniky (šifrovanie a zálohovanie údajov).

Zdieľané nástroje - napr. VPN, monitoring cloudu, správca hesiel.

Tabuľka na správu aktív

Typ informácie	Miesto (zariadenie / online služba)	Hodnota (vysoká, stredná, nízka)	Relevantné hrozby	Treba:
Heslá		vysoká	Pri neoprávnenom použití vymknutie z online služieb, strata aktuálnych (ešte nezálohovaných)	Nainštalovať/kúpiť bitwarden, zaškoliť ľudí ako to používať, vytvoriť databázu hesiel

Digitálna bezpečnosť pre MVO

			údajov, možnosť získania kontroly nad online aktivitami organizácie	
Zložky s citlivými údajmi (zmluvy, mzdové údaje, finančná správa)		Vysoká	Porušenie GDPR	
Zložky na zdieľanie v cloude		Stredná	Únik organizačných dát, obsahu	
Zložky		Vysoká	Vymknutie	
Mobily	Org/súkromné	Vysoká	Miešanie súkromných a organizačných záležitostí, únik citlivých informácií, kontrola nad komunikáciou	
USB kľúče		Nízka	Čiastočný únik dát, potenciálne porušenie GDPR	
Notebooky + iné zariadenia / tablety		Stredná		
Sociálne siete spravované cez súkromný účet		stredná	Únik hesiel a údajov, monitoring internej komunikácie, zdieľanie škodlivého obsahu pod naším menom, stalking, doxxing - poškodenie dobrého mena.	
Sociálne siete spravované cez organizačný účet		stredná	zdieľanie škodlivého obsahu pod naším menom	
Iné? Spoločný softvér (Salesforce, Miro, účtovníctvo....)		Stredná	Rôzne hrozby	

Opatrenia na detekciu hrozieb voči IT aktívam

Decentralizovaný antivírusový softvér.....

free verzia antivírusu? Každý sám? Spoločný platený antivírus?

Nastavenia spoločných kont na zasielanie upozornenia pri nezvyčajnom prihlásení (nezvyčajná lokalita, nezvyčajné zariadenie). Na akú adresu vám to chodí?

Minimálne požiadavky: zapnutá funkcia Defender v Microsoft Windows spolu s Firewall ochranou a priebežným skenovaním súborov.

Voliteľné nastavenia: zálohovanie na Microsoft Cloud.

Pokyny pre používateľov a štandardné postupy

Aj keď niektoré hrozby pochádzajú z prostredia mimo organizácie, mnohé z nich sú dôsledkom konania nášho tímu. Na zvýšenie ochrany je možné zaviesť nasledovné postupy:

Pokyny a štandardné postupy				
Oblasť	Cieľ/účel pokynu	Pokyn/postup	Komu je určený	Poznámka
VPN	Znížiť riziko pri pripájaní sa cez verejné wifi siete	Odporúčame nainštalovať Proton VPN	Kto sa pripája cez wifi sieť inde než v práci a doma	
Dvoj(viac)faktorová autentifikácia	Dôležité pre zníženie rizika úniku dát	Odporúčame zaviesť 2FA na najdôležitejšie kontá (email....)		
Zálohovanie	Zabrániť strate údajov pri strate zariadenia, zlyhaní disku alebo útoku ransomware		Každému, kto vytvára nové materiály a ukladá ich na individuálne alebo lokálne zariadenia, ktoré nie sú	

			pripojené na spoločnú sieť, ani nie sú synchronizované s Google Drive./ One Drive atc.	
Šifrovanie	Zabrániť úniku údajov pri strate zariadenia alebo útoku ransomware	Údaje, ktoré by mohli pri úniku spôsobiť porušenie GDPR alebo ohrozenie fungovania organizácie, je potrebné uchovávať pod heslom. Šifrovanie je možné pre individuálne súbory jednoduchým heslom, aj pre celé zložky.	Každému, kto má na ním/ňou používanom zariadení údaje, ktoré by mohli pri úniku spôsobiť porušenie GDPR alebo ohrozenie fungovania organizácie	
Aktualizácia (softvéru)	Zamedziť neoprávnenému prístupu cez (staršie) bezpečnostné diery	Aktualizovať operačný systém, antivírusový program, prehliadač a ďalšie programy pracujúce s údajmi vyžadujúcimi ochranu	Každému, kto používa údaje organizácie cez softvér s možným rizikom bezpečnostnej diery	

Postup na zvládnutie situácie skutočného napadnutia

Prevencia je len jednou stranou rovnice kybernetickej bezpečnosti.

Potrebujeme mať však aj pripravený postup, čo robiť v prípade zistenia narušenia bezpečnosti. Môže ísť o jednoduché kroky, ako napríklad zmeniť heslá, obnoviť dáta alebo môže ísť o zložitú analýzu údajov a vyhľadanie právnej pomoci.

V minimálnom variante potrebujeme izolovať bezpečnostný incident a rýchlo previesť dotknuté údaje do režimu offline.

Identifikácia hrozieb a príležitostí a zhodnotenie ich možného dopadu na organizáciu.

Ked' sa stane:	Čo treba urobiť:	Poznámka
Strata/krádež mobilu	Zablokovať SIM-kartu cez mobilného operátora a požiadať o vydanie náhradnej s rovnakým číslom. Zabezpečiť čím skôr náhradný mobil s rovnakým číslom kvôli dvojfaktorovej autentifikácii Ak je podozrenie, že niekto sa dostal k dátam na stratenom/ukradnutom mobile, tak zmeniť heslá k individuálne využívaným službám a tiež k spoločným kontám, ktoré mohli byť kompromitované (napr. zapamätané v prehliadači v mobile).	
Strata/krádež notebooku	Podľa miery zabezpečenia v počítači (vstupné heslo, biometrické odomykanie, šifrovanie dát apod.) treba posúdiť mieru rizika, že niekto sa dostal k dátam na stratenom/ukradnutom notebooku. Podľa toho následne zmeniť heslá k individuálne využívaným službám a tiež k spoločným kontám, ktoré mohli byť kompromitované (napr. zapamätané v prehliadači v notebooku), obnoviť dáta zo záloh, na novom notebooku nastaviť primeranú mieru ochrany	
Napadnutie počítača/notebooku vírusom	Nepripájať notebook/počítač k spoločnej sieti, neprihlasovať sa k online službám organizácie. Zálohovať dáta na prenosný USB disk (nie na internú sieť, nie na spoločný Google Drive/One Drive), skúsiť odstránenie vírusu, podľa výsledku prípadne preinštalovať celý počítač (manufacturer settings reset), preskenovať zálohované dáta antivírusovým softvérom, a následne	

	ich obnoviť. Potom zmeniť heslá k individuálne využívaným službám a tiež k spoločným kontám, ktoré mohli byť kompromitované (napr. zapamätané v prehliadači v notebooku) Antivírusom skontrolovať a prípadne vymazať USB kľúče, ktoré boli aspoň raz vložené do napadnutého počítača.	
Kompromitované heslo (wifi, online služba, heslo k prístupu do počítača apod.)	Bezodkladne zmeniť predmetné heslo. Overiť integritu dát, ku ktorým mohol byť neoprávnený prístup (čo chýba, čo bolo zmenené), antivírusová kontrola. Ak išlo o heslo, ktoré by umožnilo prístup k viacerým službám (napr. heslo na vstup do počítača alebo heslo na vstup do správcu hesiel), tak postupovať ako pri strate/krádeži notebooku.	
Útok ransomware	Odpojiť počítač/notebook úplne od siete. Informovať ostatných, ktorí by mohli byť tiež ohrození, aby vedeli svoje dáta včas zálohovať a ochrániť si počítač (počítače, ktoré boli napojené na rovnakú internú sieť ako váš, alebo do ktorých ste prenášali cez USB kľúč dáta v dobe, v ktorom mohlo dôjsť k vniknutiu ransomware vírusu). Poradiť sa s expertom, ako ďalej.	

Testovanie a audity kybernetickej bezpečnosti

Pravidelné opatrenia na zisťovanie nových slabých miest.

Audity kybernetickej bezpečnosti, ktoré nám umožnia vyhodnotiť, aká účinná je ochrana a či je bezpečnostný plán treba aktualizovať.

HaveIBeenPwned / Firefox monitor (skontrolujte adresy všetkých pracovníkov a v prípade úniku dát/hesiel, pošlite im informáciu o zmene hesla)

<https://haveibeenpwned.com/>

<https://monitor.mozilla.org/>

Dátum kontroly a pridania do Firefox monitoru	Pracovník	Akcia / poznámka

Pravidelná zmena hesiel (Aspoň 1x ročne na najdôležitejších účtoch)

Dátum zmeny	Ktoré kontá sme menili?	Kto menil?

Školenia kybernetickej bezpečnosti

Pripomenutie si štandardných postupov organizácie, zisťovania a nahlásovania podozrivého správania, e-mailov, telefónnych hovorov a webových stránok, oboznámenie sa s novými typmi hrozieb.

Školenie zamestnancov o kybernetickej bezpečnosti			
Téma školenia	Plánovaný dátum (deň alebo mesiac)	Zodpovedná osoba	Poznámka

Aktualizácia bezpečnostného plánu

Aktualizácia bezpečnostného plánu			
Verzia bezpečnostného plánu	Dátum (mesiac) aktualizácie	Osoba	Poznámka

Zoznam užitočných linkov:

1) Bezpečne na nete

<https://bezpecnenanete.eset.com/sk/>

2) National Cyber Security Centre UK

<https://www.ncsc.gov.uk/section/advice-guidance/all-topics>

3) Informácie o hackerských útokoch, The Hacker News

<https://thehackernews.com/>

4) Bezplatné školenia a kvízy o digitálnej bezpečnosti

[ResilienceLab.online – Vzdelávacia platforma pre občiansku spoločnosť](#)



**Co-funded by
the European Union**

Upozornenie: Názory vyjadrené v tejto publikácii sú výlučne názormi autora (autorov) a nemusia odrážať názory organizácií TF, GMF, PDCS, ACA a EACEA.

**G | M | F Transatlantic
Foundation**

<https://www.gmfus.org/transatlantic-foundation>



<https://www.pdcs.sk>



<https://altkozegy.hu>