Bezpečně na Internetu

Ondřej Šrámek

1. 2. 2020

Aktuální hrozby

Z novinových titulků

Benešovská nemocnice, kterou napadl hacker, je po téměř třech týdnech v plném provozu
ceskatelevize.cz/ct24 · před 5 dny

OKD ochromil hackerský útok, společnost zastavila těžbu uhlí
E15.cz · Poslední měsíc

- Počítače OKD napadli hackeři. Společnost přerušila těžbu ve všech dolech na Karvinsku
  iRozhlas.cz · Poslední měsíc

Vše o tomto tématu

OKD přerušila těžbu ve všech dolech, čelí útoku hackerů
IDNES.cz · Poslední měsíc

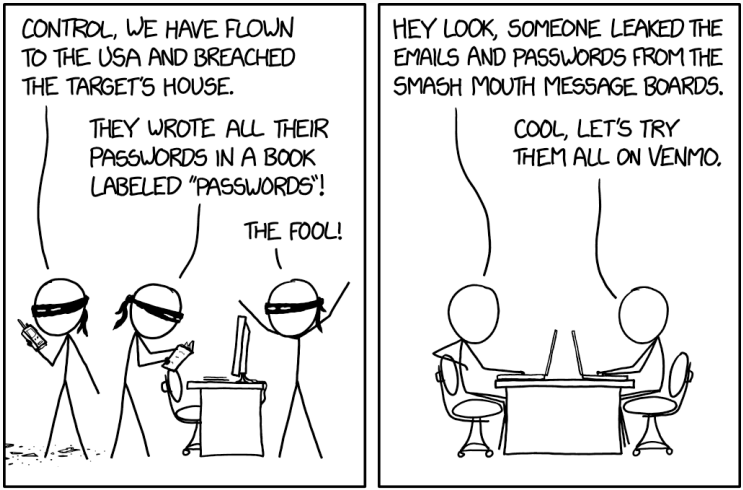
Hackeři neútočili na českou nemocnici poprvé. Podařilo se jim i získat výkupné
Sport IDNES.cz · Poslední měsíc · Satira

Kyberzločinci útočí nejen v Česku, cílem hackerů se stala také ECB
Reklen24 · Poslední měsíc

Hackeři ochromili benešovskou nemocnici. Nelze spouštět přístroje, ruší se operace
ceskatelevize.cz/ct24 · Poslední měsíc

Hackerským útokům čelilo MZV, volební web i nemocnice
Novinky.cz · Poslední měsíc

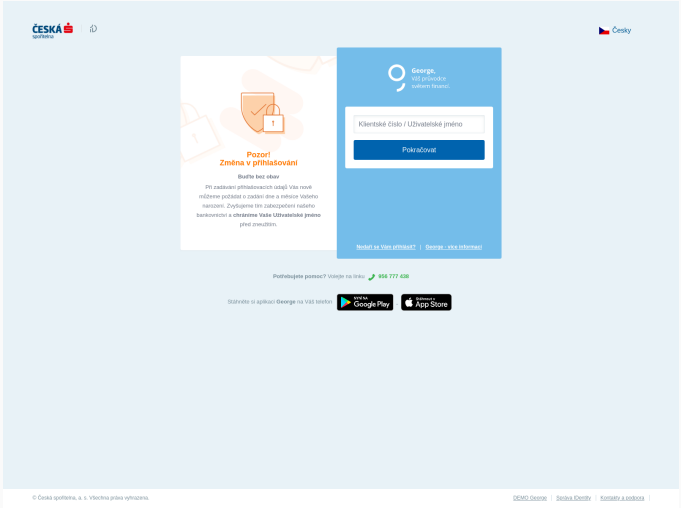
Co si lidé myslí a jak je to doopravdy



Jakým hrozbám uživatelé čelí?

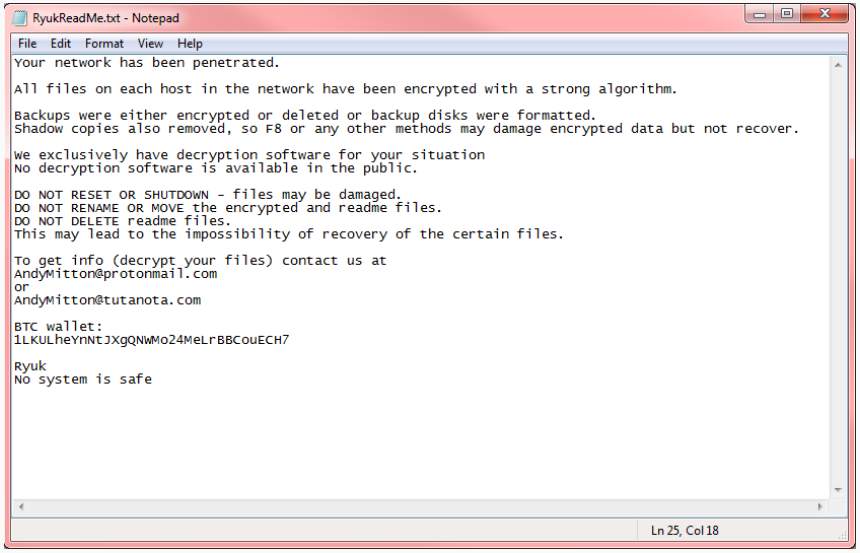
- (Spear)Phishing
- Ransomware
- Blackmailing
- Cryptomining
- D(DoS)
- Botnet
- Státem sponzorovaní aktéři, státní aktéři

Phishing – Příklad

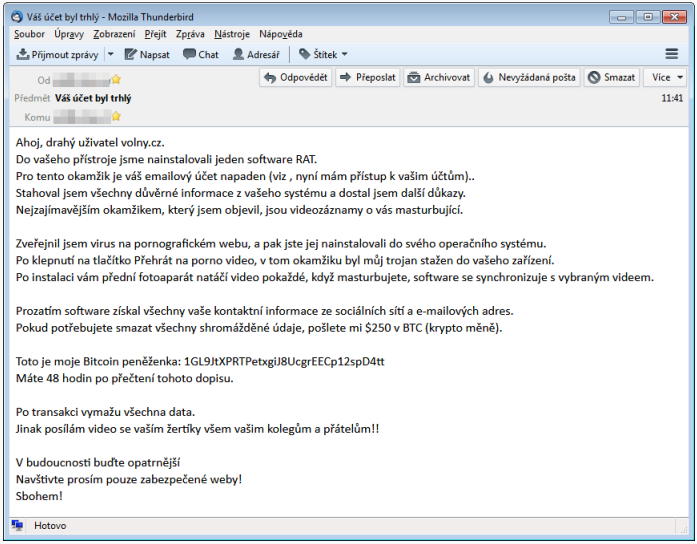


http://www.georgecsas.g6.cz/

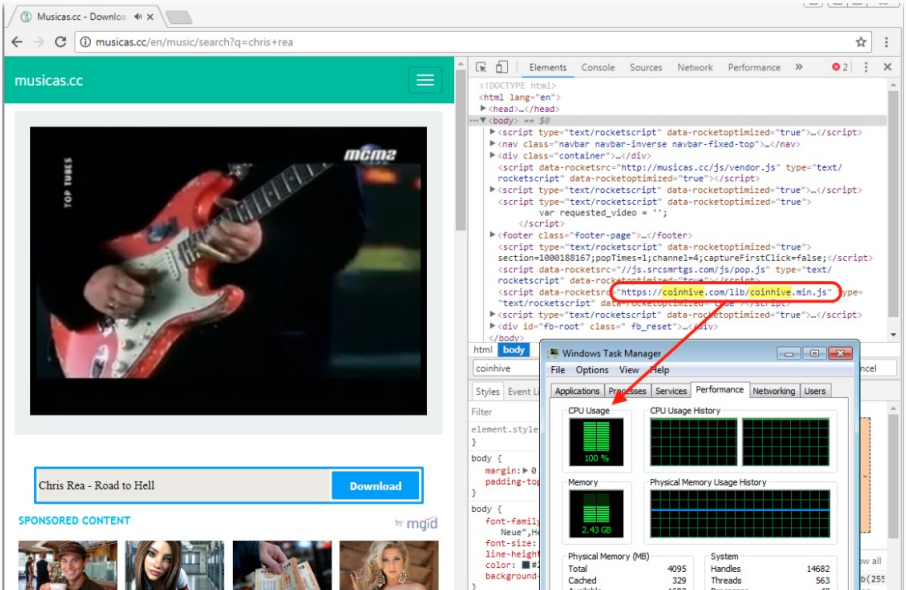
Ransomware – Příklad



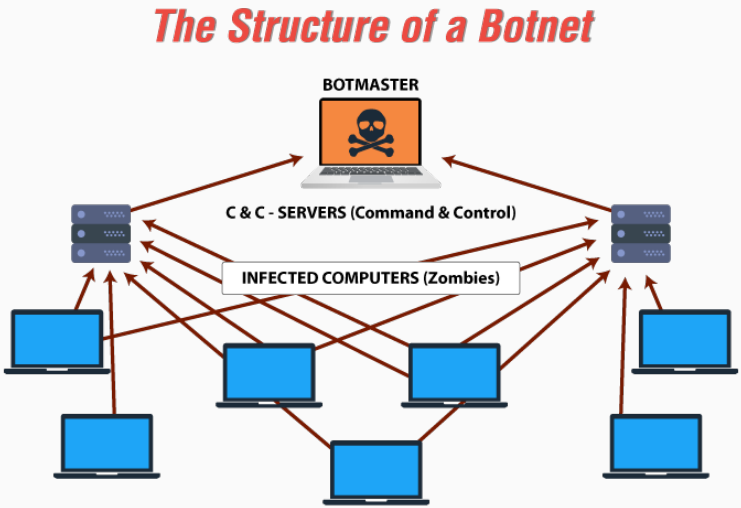
Blackmailing – Příklad



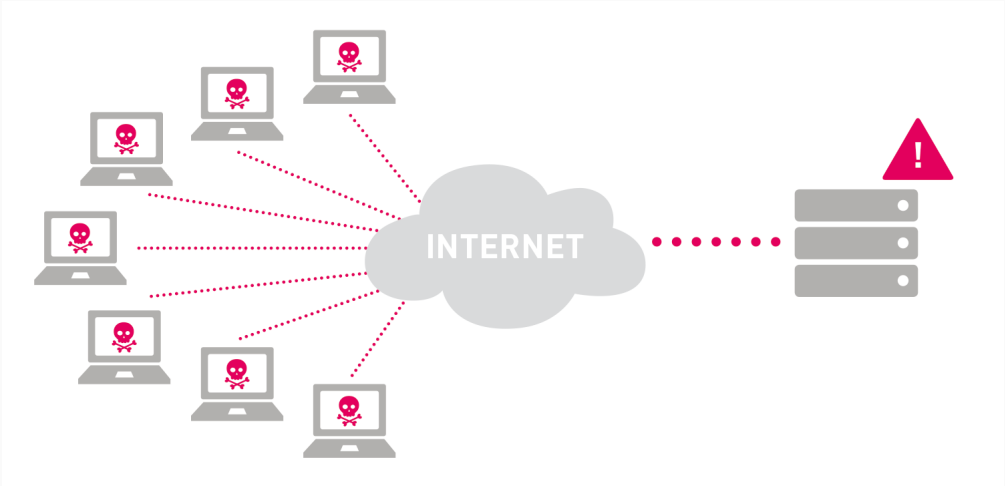
Cryptomining – Příklad



Botnet – Příklad



(D)DoS – Příklad



Státní aktéři – Příklady

- Informace (APT28, MZV ČR)
- Hybridní válka (Ukrajina)
- Peníze (WannaCry, KLDR)
- Strategická výhoda (Stuxnet, Irán)

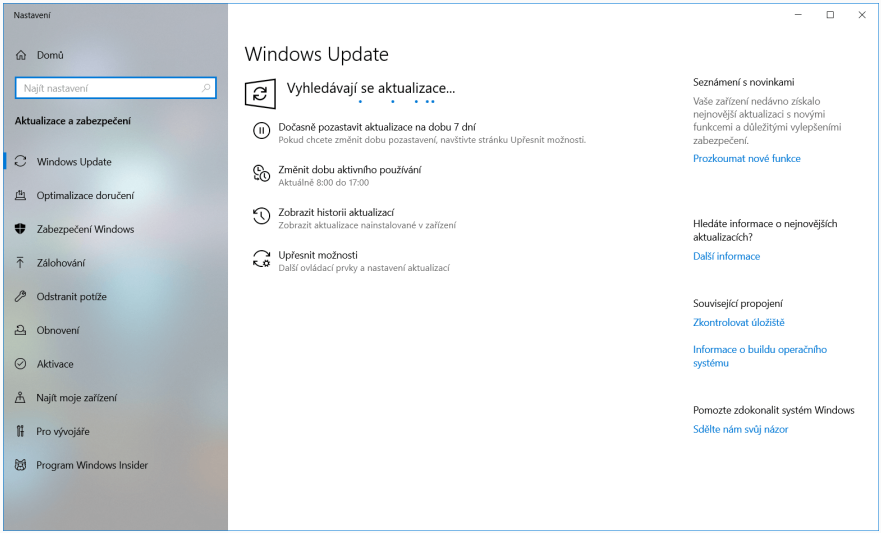
Desatero

1. Aktualizace

Udržují systém **aktuální** – přidávají nové funkce, opravují chyby a zranitelnosti

- Aktualizace vychází zpravidla každý měsíc (Microsoft, Google,...)
- V nepravidelných intervalech (čtvrtletně, půlročně, ročně) dochází k vylepšením celého systému (iOS, macOS, Windows,. . .)
- Vhodné instalovat bez prodlení, minimálně ty bezpečnostní
- Aplikace, operační systém (počítače, telefony, tablety) ale i modem, router, televize, set-top-box,. . .

1. Aktualizace – Příklad

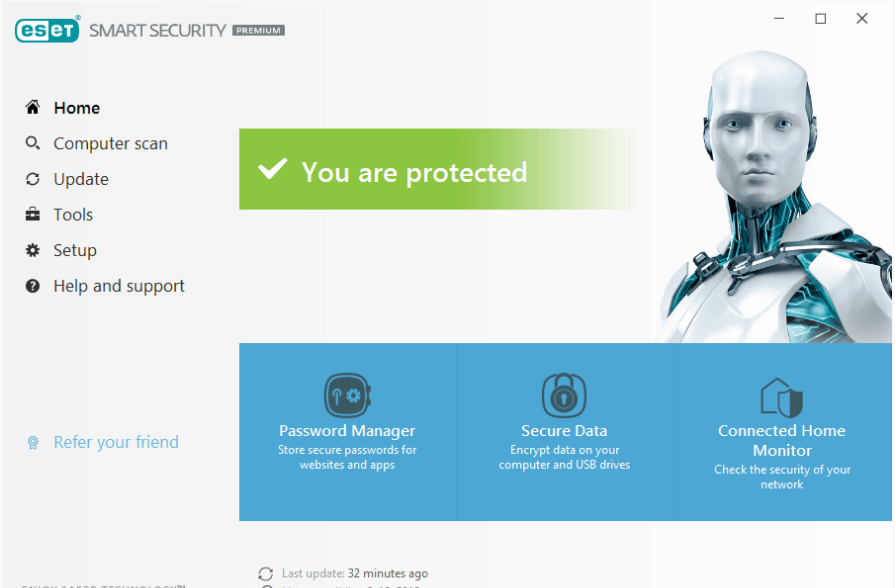


2. Antivir

Ochrana zařízení před **škodlivým** kódem

- **Součást** systému (Windows)
- Často obsahuje *další* funkce (firewall, rodičovská kontrola,...)

2. Antivir – Příklad

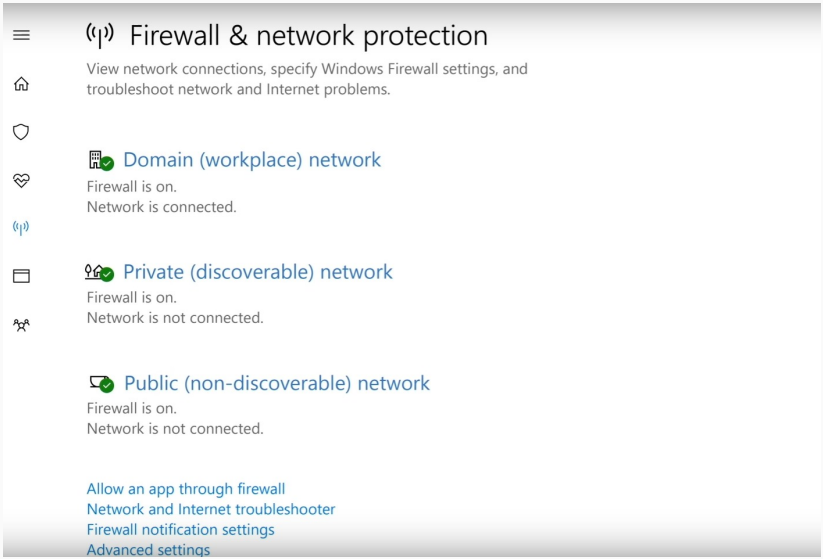


3. Firewall

Chrání zařízení před **nežádoucím** připojením (příchozím i odchozím)

- **Součást** systému (Windows, macOS)
- Často jako součást *antivirového* řešení

3. Firewall – Příklad



4. 2FA – Druhý faktor autentizace

Další stupeň ověření při přihlašování

- SMS
- Speciální aplikace (**Authy**, **Duo**)
- Speciální token (**YubiKey**, vydaný bankou nebo poskytnutý zaměstnavatelem)
- Internetové bankovnictví, platby na Internetu
- Google, Microsoft, Facebook, Instagram, mojeiD, twitter, Dropbox,...

4. 2FA – Příklady

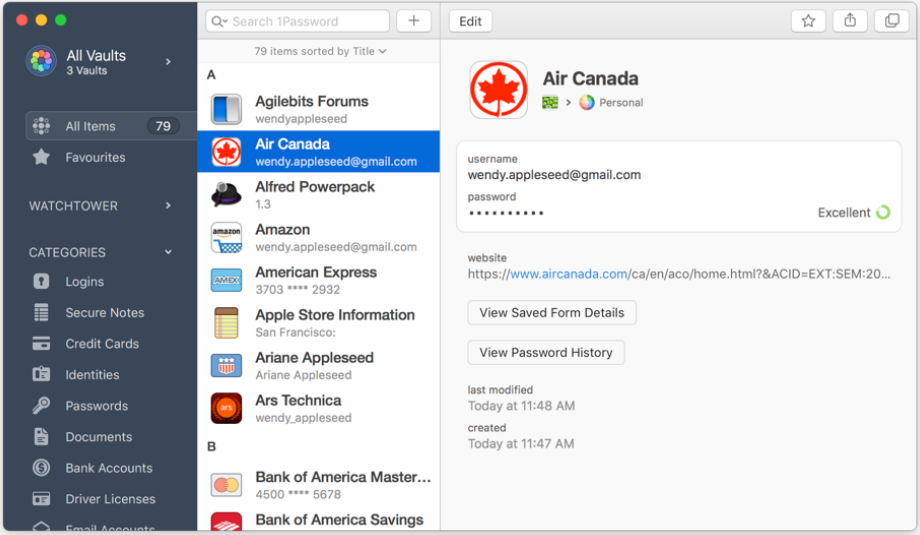
5. Správce hesel

Pamatuje si za vás všechna vaše hesla

- Generuje *náhodná* hesla
- Pamatuje si jejich *historii*
- Kontroluje výskyt vašich hesel mezi *uniklými*

- Deník na hesla (pod máte počítač jen doma)
- **KeePass** (pokud používáte jen počítač s Windows, na jednom místě)
- **Bitwarden**, **1Password** (pokud používáte více zařízení – telefon, notebook)

5. Správce hesel – Příklad



6. Unikátní heslo

Co služba/přístup, to jiné heslo

- Zajistí správce hesel : (**LdbC4c4JzWs2QHj3@!io7**)
- Více slov (4+), s pomlčkou : (**hračka-rvačka-mačka-kačka**)

Podstatná je délka (12+)

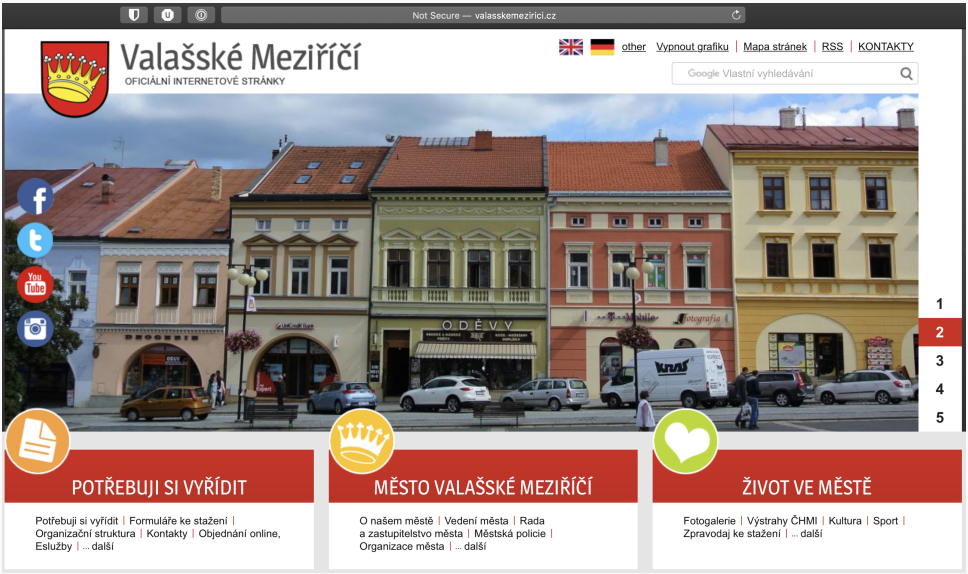
- Čím delší heslo, tím obtížněji se na něj útočí
- Přidáte-li navíc i velké písmeno, bude to ještě lepší

7. HTTPS

Zabezpečený přístup

- Zámeček, před adresou webové stránky
- Nutnost, když uživatel zadává citlivá data (jméno, heslo, rodné číslo, telefon a jiné údaje)
- Nemusí jít jen o přihlašování, ale i o registrační formuláře
- Důvěryhodný obsah – úřední deska, formuláře ke stažení,...
- V případě, že vidíte **nezabezpečeno** – nepřihlašujte se!

7. HTTPs – Příklad



8. Obezřetnost

Přemýšlím než kliknu

- Odkaz v e-mailu (váš e-mail byl zablokován)
- „Výhodné“ nabídky – iPhone za korunu apod.

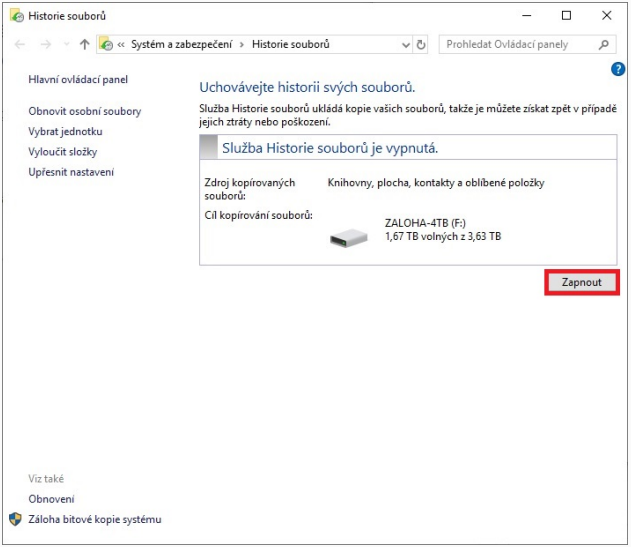
8. Obezřetnost – Příklad

9. Zálohování

V případě nenadálé ztráty dat (odcizení zařízení, poruchy nebo jiných problémů) jsou data stále k dispozici

- Součást systému (Windows, iOS, macOS, Linux, Android)
- Záloha vybraných dat vs. záloha celého systému
- Doporučeno v pravidelném intervalu (denně, týdně, měsíčně) v závislosti na povaze dat
- Lokální (externí disk) vs. vzdálená (cloud)

9. Zálohování – Příklad

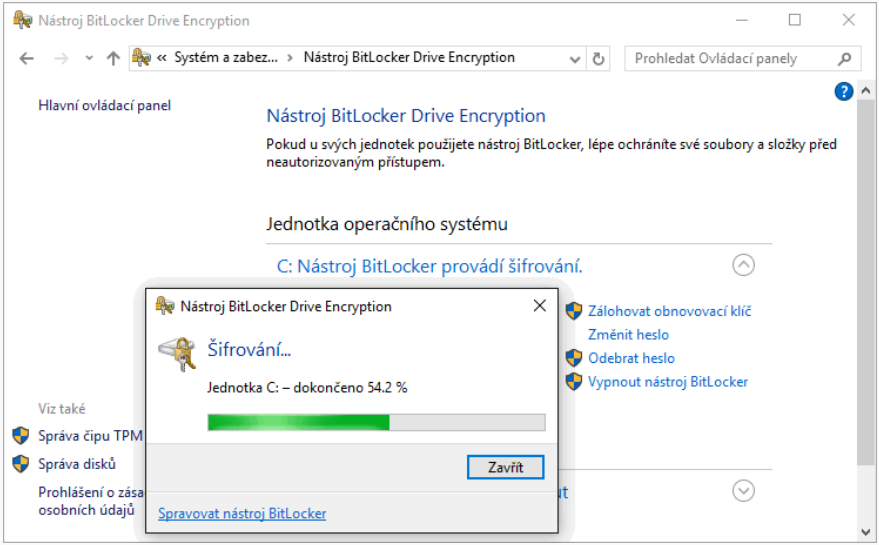


10. Šifrování

V případě ztráty/pokusu o neautorizovaný přístup k zařízení jsou data v bezpečí

- Součást systémů (Windows, iOS, macOS, Linux, Android)
- Nutnost u firemních zařízení (nejen přenosných)

10. Šifrování – Příklad



10. Šifrování – Příklad

Co dělat když...

. . . vám nadávají nebo vyhrožují (na sociálních sítích)

- Neodpovídat
- Udělejte záznam (screenshot)
- Konverzaci nemazat!
- Ignorace
- Nahlášení provozovateli/policii
- Informování přátel/rodiny
- Svěřte se

. . . potřebujete pomoc.

- Policie ČR
- CSIRT.CZ (veřejnost), GovCERT.CZ (státní správa, KII/VIS)
- Banka (v případě zneužití karty/účtu)
- Linka Bezpečí
- Nahlášení závadného obsahu, `https://www.stoponline.cz/stoponline/`

Sociální sítě

Než něco někam nahraji...

Nezveřejňujte více než musíte...

- Fotky letenek, platebních karet, klíčů nebo bříšek prstů
- Příspěvky o tom, že se chystáte na dovolenou,...
- Fotky dětí

Příklad: Letenky

Příklad: Karty, klíče

Nikdy nevíte, kdo je na druhé straně...

Vydávat se za někoho jiného, je snazší než si myslíte...

- Falešné profily podporující politiky
- Falešné profily za účelem sledování
- (Sexuální) predátoři

Falešný profil: Příklad profilové fotky

Co si z dneška odnést

Shrnutí

- Aktivujte si 2FA (e-mail, sociální sítě, cloud, banka,...)
- Používejte správce hesel
- Mějte všechna hesla jiná
- Hesla měňte až je to potřeba
- Sledujte aktivitu účtů (e-mail, sociální sítě, cloud,...)
- Neposílejte nikomu žádné kódy z SMS/aplikací
- Nezveřejňujte fotky kódů, letenek, vstupenek apod.
- Zálohujte

Díky za pozornost!

Otázky?

Ondřej Šrámek

https://ondrejsramek.cz/cs/blog/bezpecne-online

Další vzdělání

Více se tomuto tématu věnujeme na jednodenním kurzu *Úvod do (online) bezpečnosti*

9.2.2020, Praha
30.5.2020, Zlín
13.6.2020, Brno

`https://www.czechitas.cz/cs/co-delame/jsem-online-bezpecne`

Více informací

Zkuste si

- Je vaše heslo mezi uniklými?
  `https://haveibeenpwned.com/`
- Zkuste si phishing kvíz
  `https://phishingquiz.withgoogle.com/`

Další zdroje

- Podcast ČRo o internetové bezpečnosti
  `https://www.irozhlas.cz/cookies`
- Databáze podvodných zpráv
  `https://hoax.cz/`
- Přehledně o dezinformacích a poplašných zprávách.
  `https://manipulatori.cz/`
- Milionářem snadno a rychle? Spíš ne...
  `https://www.investigace.cz/vyzkouseli-jsme-za-vas-milionarem-snadno-a-rychle/`
- Seriál #martyisdead
  `https://www.mall.tv/martyisdead`