

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/c124 · 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

Rozhlas.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

Raklen24 · Poslední měsíc



Hackeři ochromili benešovskou nemocnici. Nelze spouštět přístroje, ruší se operace

ceskatelevize.cz/c124 · Poslední měsíc



Hackerským útokům čelilo MZV, volební web i nemocnice

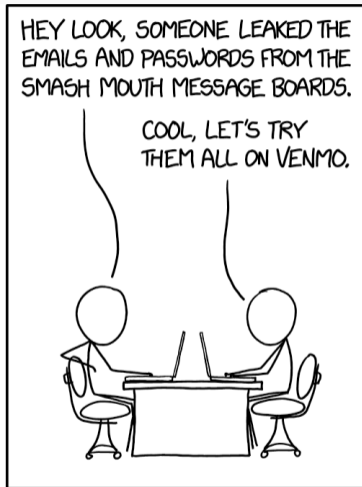
Novinky.cz · Poslední měsíc



Co si lidé myslí a jak je to doopravdy



HOW PEOPLE THINK HACKING WORKS



HOW IT ACTUALLY WORKS

Jakým hrozbám uživatelé čelí?

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

Phishing – Příklad

ČESKA spořitelna

Česky

Pozor! Změna v přihlašování

Buďte bez obav

Při zadávání přihlašovacích údajů Vám nově můžeme požádat o zadání dne a měsíce Vašeho narození. Zvýšíme tím zabezpečení našeho bankovního účtu a chráníme Vaše Uživatelské jméno před zneužitím.

George,
Váš průvodčí našim finančním

Klientské číslo / Uživatelské jméno

Pokračovat

Neboť se Vás přihlásit? | George... info@george

Potřebujete pomoc? Volajte na číslo 956 777 438

Stáhněte si aplikaci George na Váš telefon

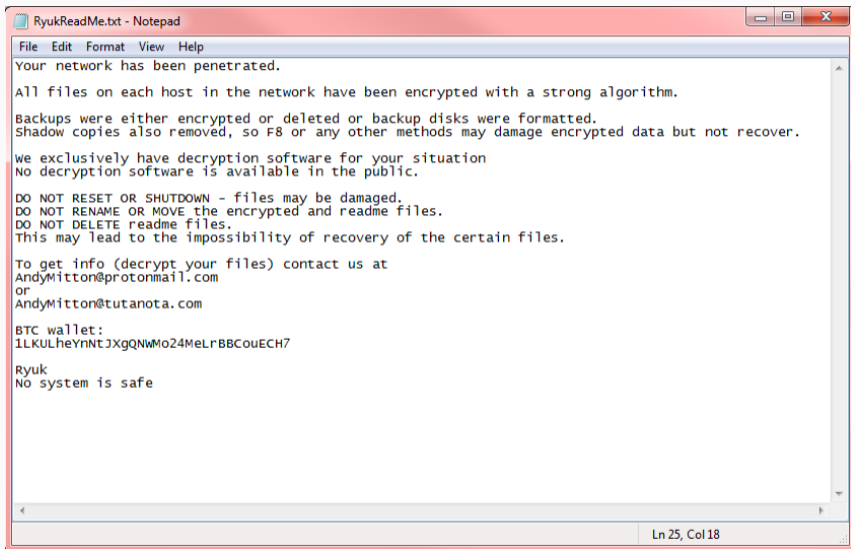
Google Play | App Store

© Česká spořitelna, a. s. Všechna práva vyhrazena.

DCMO George | Ochrana Identit | Statistiky a podpora

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

Ransomware – Příklad



RyukReadMe.txt - Notepad

File Edit Format View Help

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

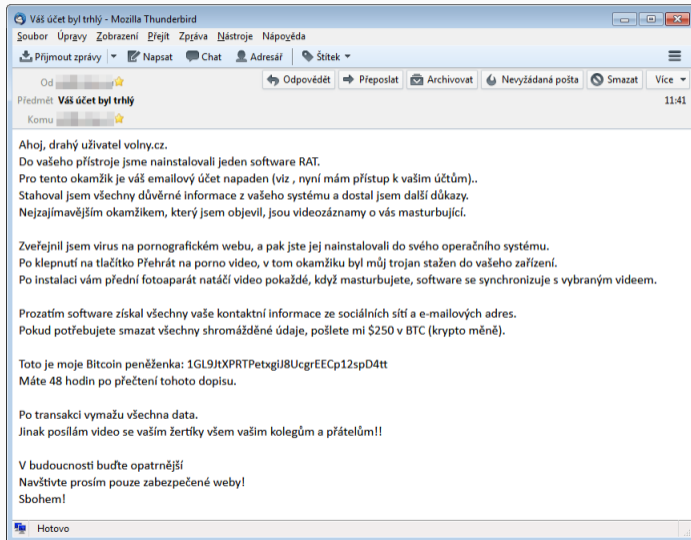
To get info (decrypt your files) contact us at
AndyMitton@protonmail.com
or
AndyMitton@tutanota.com

BTC wallet:
1LKULheYnNTjXgQNWmo24MeLrBBCouECH7

Ryuk
No system is safe

Ln 25, Col 18

Blackmailing – Příklad



Cryptomining – Příklad

The screenshot illustrates a cryptomining attack on a music website. The browser shows the search results for "Chris Rea - Road to Hell" on musicas.cc. The developer tools reveal a script tag from coinhive.com, which is used for cryptomining. The Windows Task Manager shows the system's resource usage, indicating that the mining process is consuming significant CPU and memory resources.

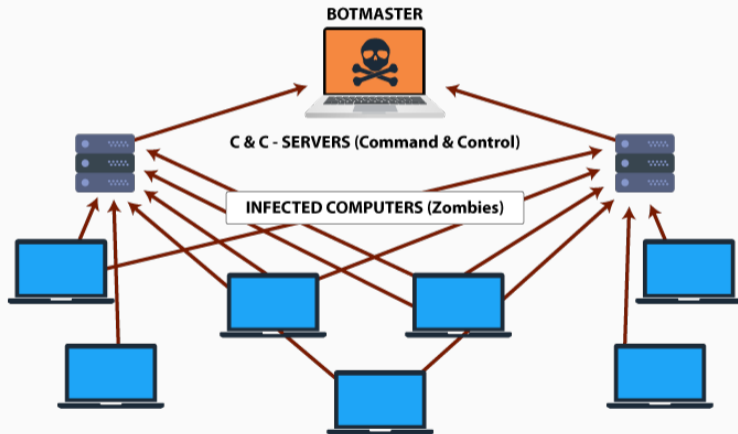
```
<script data-rocketsrc="https://coinhive.com/lib/coinhive.min.js" type="text/javascript"></script>
```

| CPU Usage | | CPU Usage History | |
|-----------|--|-------------------|--|
| 100 % | | | |

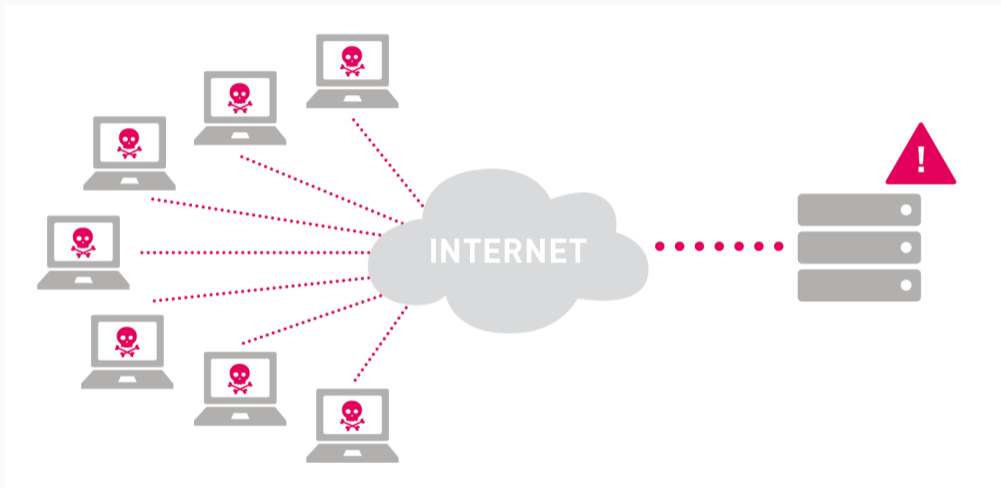
| Memory | | Physical Memory Usage History | |
|---------|--|-------------------------------|--|
| 2.43 GB | | | |

| Physical Memory (MB) | | System | |
|----------------------|------|---------|-------|
| Total | 4095 | Handles | 14682 |
| Cached | 329 | Threads | 563 |

The Structure of a Botnet



(D)DoS – Příklad



Státní aktéři – Příklady

- Informace (APT28, MZV ČR)
- Hybridní válka (Ukrajina)
- Peníze (WannaCry, KLDLDR)
- 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

The screenshot shows the Windows Update settings window. On the left is a navigation pane with the following items: Domů, Najít nastavení (search bar), Aktualizace a zabezpečení (expanded), Windows Update (selected), Optimalizace doručení, Zabezpečení Windows, Zálohování, Odstranit potíže, Obnovení, Aktivace, Najít moje zařízení, Pro vývojáře, and Program Windows Insider. The main content area is titled 'Windows Update' and features a 'Vyhledávají se aktualizace...' (Searching for updates...) status with a refresh icon. Below this are five settings: 'Dočasně pozastavit aktualizace na dobu 7 dní' (temporarily paused for 7 days), 'Změnit dobu aktivního používání' (change active time, currently 8:00 to 17:00), 'Zobrazit historii aktualizací' (show update history), and 'Upřesnit možnosti' (refine options). On the right side, there are three sections: 'Seznámení s novinkami' (learn more about new features), 'Hledáte informace o nejnovějších aktualizacích?' (looking for the latest updates?), and 'Pomozte zdokonalit systém Windows' (help improve Windows). Each section includes a link to learn more.

Nastavení

Domů

Najít nastavení

Aktualizace a zabezpečení

- Windows Update
- Optimalizace doručení
- Zabezpečení Windows
- Zálohování
- Odstranit potíže
- Obnovení
- Aktivace
- Najít moje zařízení
- Pro vývojáře
- Program Windows Insider

Windows Update

Vyhledávají se aktualizace...

- Dočasně pozastavit aktualizace na dobu 7 dní
Pokud chcete změnit dobu pozastavení, navštivte stránku [Upřesnit možnosti](#).
- Změnit dobu aktivního používání
Aktuálně 8:00 do 17:00
- Zobrazit historii aktualizací
Zobrazit aktualizace nainstalované v zařízení
- Upřesnit možnosti
Další ovládací prvky a nastavení aktualizací

Seznámení s novinkami

Vaše zařízení nedávno získalo nejnovější aktualizaci s novými funkcemi a důležitými vylepšeními zabezpečení.

[Prozkoumat nové funkce](#)

Hledáte informace o nejnovějších aktualizacích?

[Další informace](#)

Související propojení

[Zkontrolovat úložné místo](#)

[Informace o buildu operačního systému](#)

Pomozte zdokonalit systém Windows

[Sdělte nám svůj názor](#)

2. Antivir

Ochrana zařízení před **škodlivým** kódem

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

2. Antivir – Příklad

The screenshot displays the ESET Smart Security Premium user interface. At the top left, the ESET logo and 'SMART SECURITY PREMIUM' are visible. A navigation menu on the left includes 'Home', 'Computer scan', 'Update', 'Tools', 'Setup', and 'Help and support'. A central green banner with a white checkmark reads 'You are protected'. On the right, there is a 3D rendering of a futuristic robot. Below the banner, three blue feature tiles are shown: 'Password Manager' (store secure passwords), 'Secure Data' (encrypt data on computer and USB drives), and 'Connected Home Monitor' (check network security). At the bottom, a status bar indicates 'Last update: 32 minutes ago'.

eset SMART SECURITY PREMIUM

- Home
- Computer scan
- Update
- Tools
- Setup
- Help and support

✓ You are protected

Refer your friend

Password Manager
Store secure passwords for websites and apps

Secure Data
Encrypt data on your computer and USB drives

Connected Home Monitor
Check the security of your network

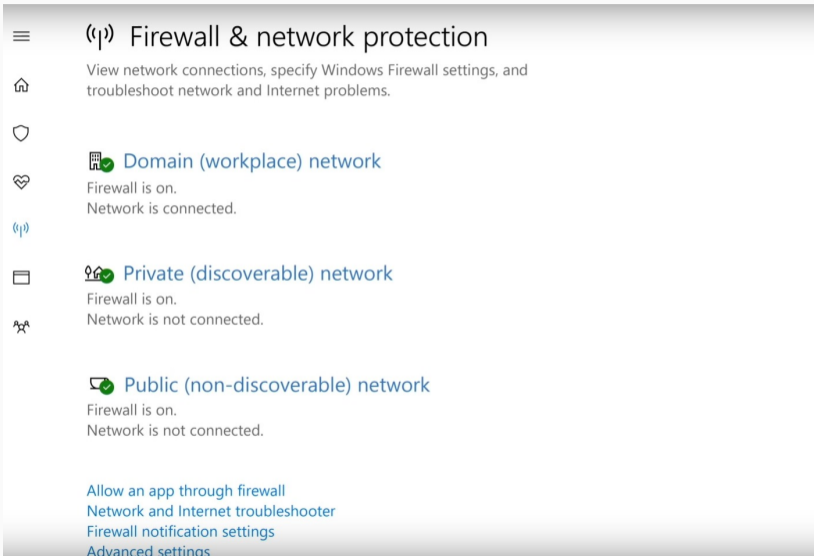
Last update: 32 minutes ago

3. Firewall

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

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

3. Firewall – Příklad



The screenshot shows the Windows Settings application for Firewall & network protection. It features a left-hand navigation pane with icons for a menu, home, shield, heart, network, folder, and people. The main content area is titled "Firewall & network protection" and includes a descriptive paragraph: "View network connections, specify Windows Firewall settings, and troubleshoot network and Internet problems." Below this, three network profiles are listed: "Domain (workplace) network" (firewall on, network connected), "Private (discoverable) network" (firewall on, network not connected), and "Public (non-discoverable) network" (firewall on, network not connected). At the bottom, there are four links: "Allow an app through firewall", "Network and Internet troubleshooter", "Firewall notification settings", and "Advanced settings".

☰ Firewall & network protection

View network connections, specify Windows Firewall settings, and troubleshoot network and Internet problems.

🏠

🛡️

❤️

📶

📁

👥

🏢 **Domain (workplace) network**
Firewall is on.
Network is connected.

🏠 **Private (discoverable) network**
Firewall is on.
Network is not connected.

🌐 **Public (non-discoverable) network**
Firewall is on.
Network is not connected.

[Allow an app through firewall](#)
[Network and Internet troubleshooter](#)
[Firewall notification settings](#)
[Advanced settings](#)

4. 2FA – Druhý faktor autentizace

Další stupeň ověření při přihlašování

- SMS
- Speciální aplikace (**Authy**, **Duo**)
- Speciální token (**YubiKey**, vydaný bankou nebo poskytnutý zaměstnavatelem)
- Internetové bankovníctví, 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

The screenshot displays the 1Password application interface. On the left is a dark sidebar with navigation options: All Vaults (3 Vaults), All Items (79), Favourites, WATCHTOWER, and CATEGORIES (Logins, Secure Notes, Credit Cards, Identities, Passwords, Documents, Bank Accounts, Driver Licenses, Email Accounts). The main window shows a search bar for '1Password' and a list of 79 items sorted by title. The 'Air Canada' entry is selected and highlighted in blue. The right pane shows the details for this entry, including the Air Canada logo, the username 'wendy.appleseed@gmail.com', a masked password, and a green 'Excellent' status indicator. Below the password field are buttons for 'View Saved Form Details' and 'View Password History'. At the bottom, it shows the last modified time as 'Today at 11:48 AM' and the creation time as 'Today at 11:47 AM'.

Search 1Password + Edit ☆ 📄

79 items sorted by Title ▾

A

- Agilebits Forums
wendyappleseed
- Air Canada**
wendy.appleseed@gmail.com
- Alfred Powerpack
1.3
- Amazon
wendy.appleseed@gmail.com
- American Express
3703 **** 2932
- Apple Store Information
San Francisco:
- Ariane Appleseed
Ariane Appleseed
- Ars Technica
wendy_appleseed

B

- Bank of America Master...
- Bank of America Savings

Air Canada
Personal

username
wendy.appleseed@gmail.com

password
..... Excellent 🟢

website
<https://www.aircanada.com/ca/en/aco/home.html?&ACID=EXT:SEM:20...>

View Saved Form Details

View Password History

last modified
Today at 11:48 AM

created
Today at 11:47 AM

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

The screenshot shows the official website of Valašské Meziříčí. At the top, there is a navigation bar with a crown logo, the text "Valašské Meziříčí OFICIÁLNÍ INTERNETOVÉ STRÁNKY", and language options (UK, DE, other). A search bar is also present. Below the navigation is a large photograph of a street scene with colorful buildings. On the left side of the page, there are social media icons for Facebook, Twitter, YouTube, and Instagram. On the right side, there is a vertical list of numbers 1 through 5, with the number 2 highlighted in red. At the bottom of the page, there are three red navigation buttons with icons and text: "POTŘEBUJI SI VYŘÍDIT" (with a document icon), "MĚSTO VALAŠSKÉ MEZIŘÍČÍ" (with a crown icon), and "ŽIVOT VE MĚSTĚ" (with a heart icon). Each button has a corresponding list of links below it.

Not Secure — valasskemezirici.cz

Valašské Meziříčí
OFICIÁLNÍ INTERNETOVÉ STRÁNKY

other Vypnout grafiku | Mapa stránek | RSS | KONTAKTY

Google Vlastní vyhledávání

1
2
3
4
5

POTŘEBUJI SI VYŘÍDIT

Potřebuji si vyřídit | Formuláře ke stažení | Organizační struktura | Kontakty | Objednání online, Eslužby | ... další

MĚSTO VALAŠSKÉ MEZIŘÍČÍ

O našem městě | Vedení města | Rada a zastupitelstvo města | Městská policie | Organizace města | ... další

ŽIVOT VE MĚSTĚ

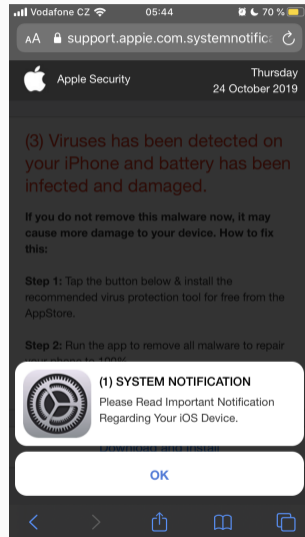
Fotogalerie | Výstrahy ČHMÍ | Kultura | Sport | Zpravodaj ke stažení | ... další

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

The screenshot shows the Windows File History settings window. The title bar reads "Historie souborů". The navigation pane on the left includes "Hlavní ovládací panel", "Obnovit osobní soubory", "Vybrat jednotku", "Vyloučit složky", and "Upřesnit nastavení". The main content area has the heading "Uchovávejte historii svých souborů." followed by the text "Služba Historie souborů ukládá kopie vašich souborů, takže je můžete získat zpět v případě jejich ztráty nebo poškození." Below this, a message states "Služba Historie souborů je vypnutá." and lists the source and destination: "Zdroj kopírovaných souborů: Knihovny, plocha, kontakty a oblíbené položky" and "Cíl kopírování souborů: ZALOHA-4TB (F:) 1,67 TB volných z 3,63 TB". A red box highlights the "Zapnout" button at the bottom right of the message box. At the bottom left, there are links for "Viz také", "Obnovení", and "Záloha bitové kopie systému".

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

Nástroj BitLocker Drive Encryption

← → ↕ ↗ 🗨️ << Systém a zabez... > Nástroj BitLocker Drive Encryption 🔍 ↻ 🔍 Prohledat Ovládací panely

Hlavní ovládací panel

Nástroj BitLocker Drive Encryption

Pokud u svých jednotek použijete nástroj BitLocker, lépe ochráníte své soubory a složky před neautorizovaným přístupem.

Jednotka operačního systému

C: Nástroj BitLocker provádí šifrování.

Nástroj BitLocker Drive Encryption

Šifrování...

Jednotka C: – dokončeno 54.2 %

Zavřít

[Spravovat nástroj BitLocker](#)

- Zálohovat obnovovací klíč
- Změnit heslo
- Odebrat heslo
- Vypnout nástroj BitLocker

Viz také

- Správa čipu TPM
- Správa disků

Prohlášení o zásadě osobních údajů

10. Šifrování – Příklad

BitLocker

K odemknutí této jednotky zadejte heslo.

Chcete-li při psaní zobrazovat heslo, stiskněte klávesu Insert.

Pokračujte stisknutím klávesy Enter.

Nástroj BitLocker obnovíte stisknutím klávesy Esc.

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

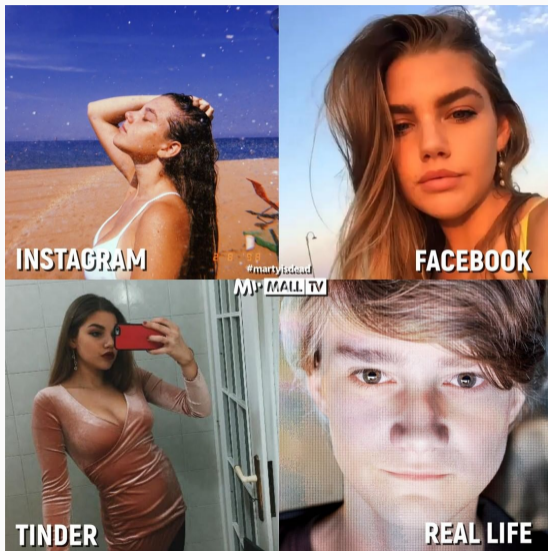


Nikdy nevíte, kdo je na druhé straně. . .

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

- 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>