

Cítíte se v bezpečí?

Soukromí a bezpečí v kyberprostoru

Život v kyberprostoru

27. 11. 2019

Témata

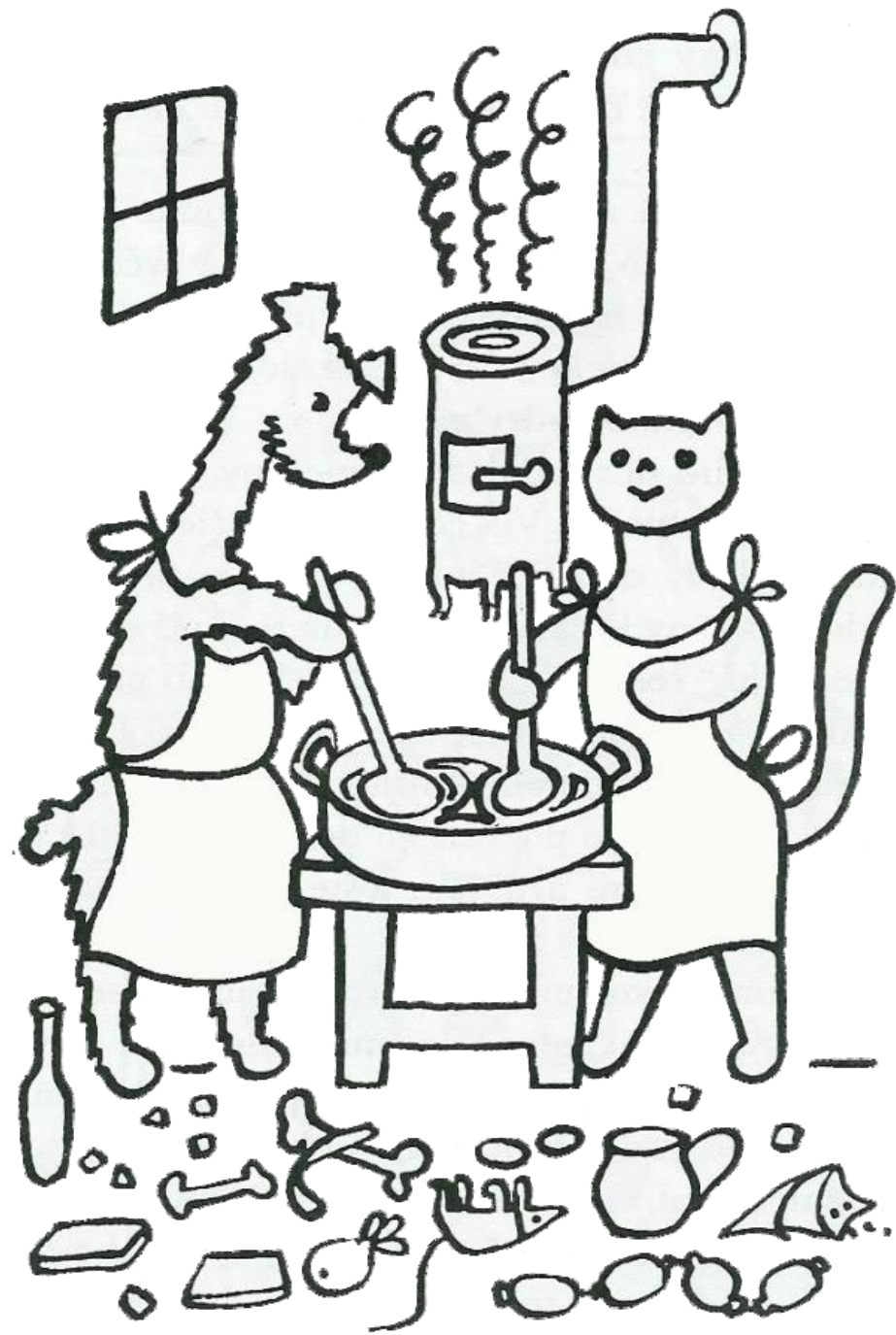
Anonymita na webu

Ochrana vlastních dat a šifrování

Hesla a zabezpečení účtů

Bezpečnost dalšího HW

Bezpečnostní hrozby



Je pro vás
soukromí důležité?

Proč to řešit?

- *„Když nemáš co skrývat...“*
- *„Soukromí už není sociální norma...“*
- [Glenn Greenwald](#)
- NSA PRISM
- Cambridge Analytica
- [technologie není apolitická](#)
- dohledový kapitalismus

- https://www.youtube.com/watch?v=V9_PjdU3Mpo

**THE AGE OF
SURVEILLANCE
CAPITALISM**

—
**THE FIGHT FOR A
HUMAN FUTURE
AT THE NEW
FRONTIER OF POWER**
—

**SHOSHANA
ZUBOFF**

**THE AGE OF
SURVEILLANCE**

THE FIGHT FOR
HUMAN FUTURE
AT THE NEW
FRONTIER OF
POWER

SHOSHANA
ZUBOFF



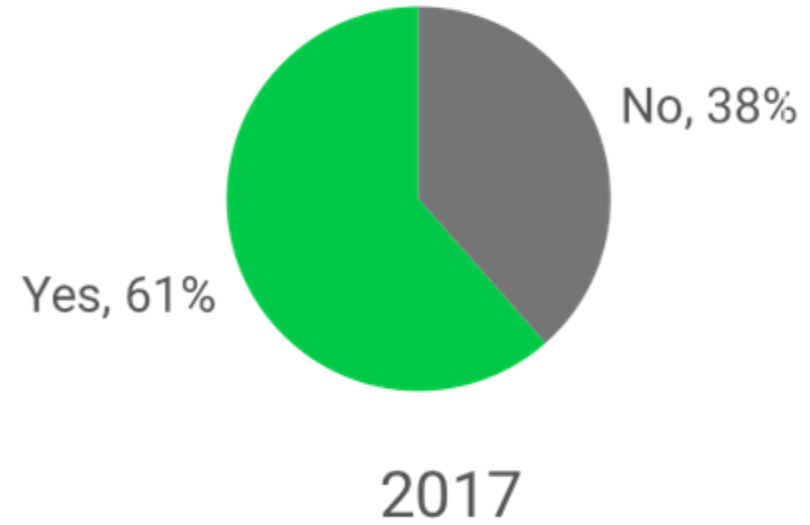
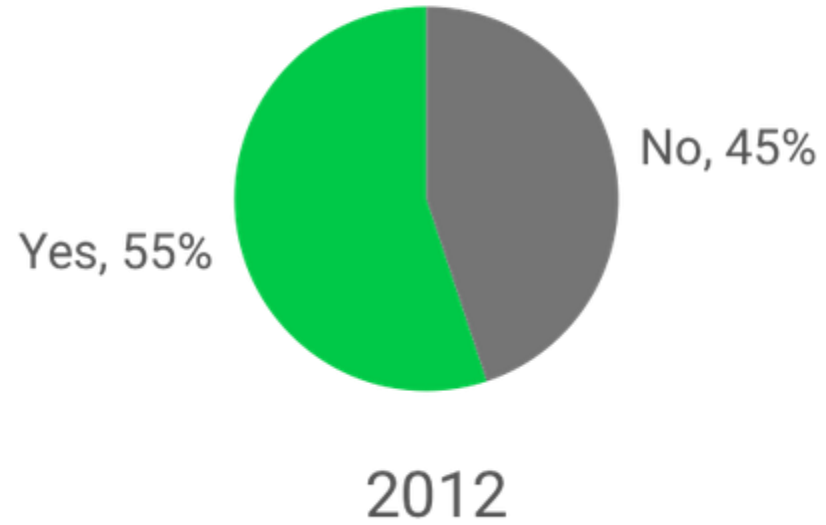
Co je to anonymita?

- *digitální stopa*
- jméno osoby
- lokace
- pseudonym spojitelný s reálným jménem nebo lokací
- pseudonym prozrazující jiné informace
- odhalující vzorce chování
- členství v některé sociální skupině
- předmět či dovednost naznačující osobní charakteristiky

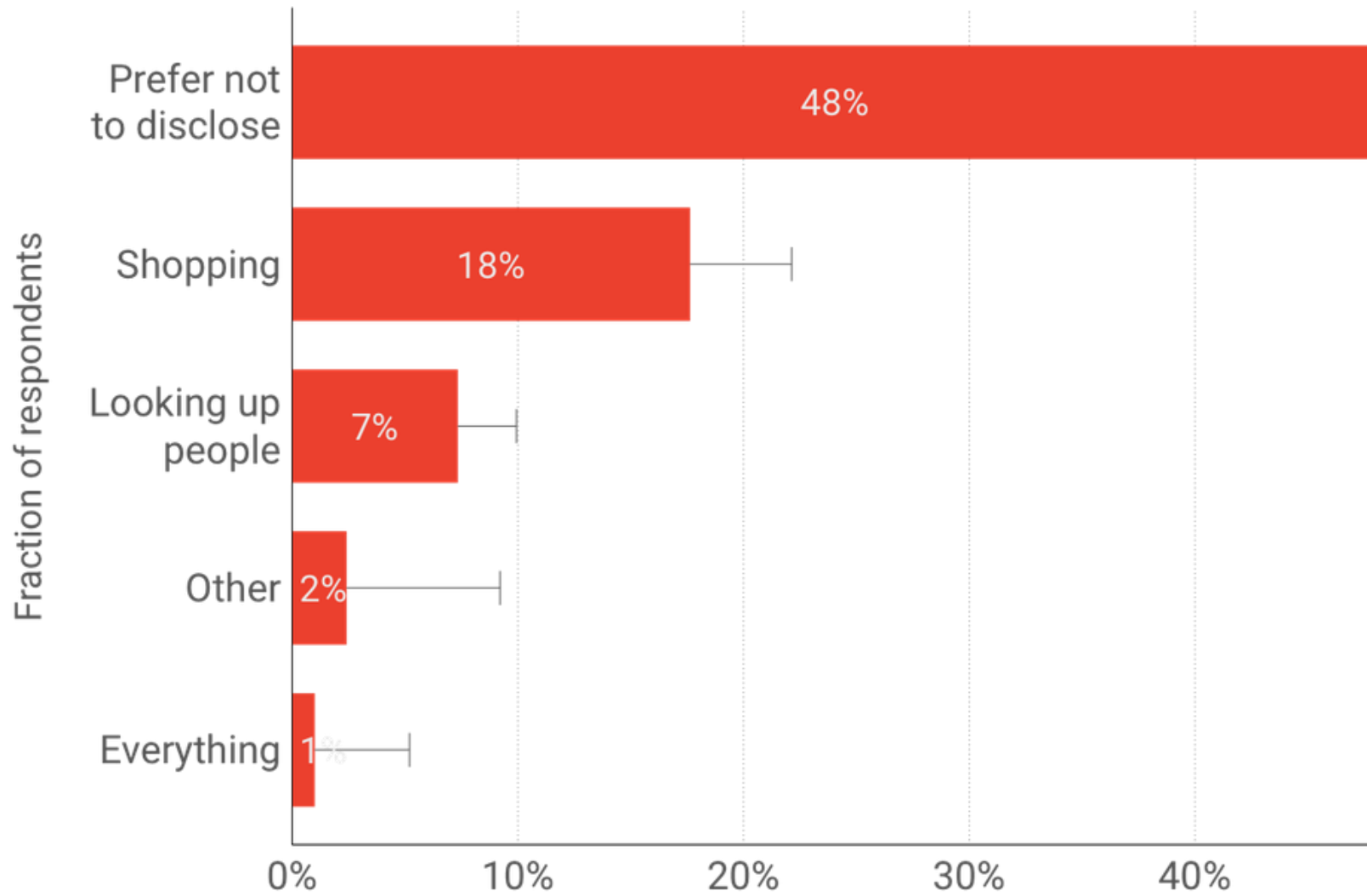


You've gone incognito

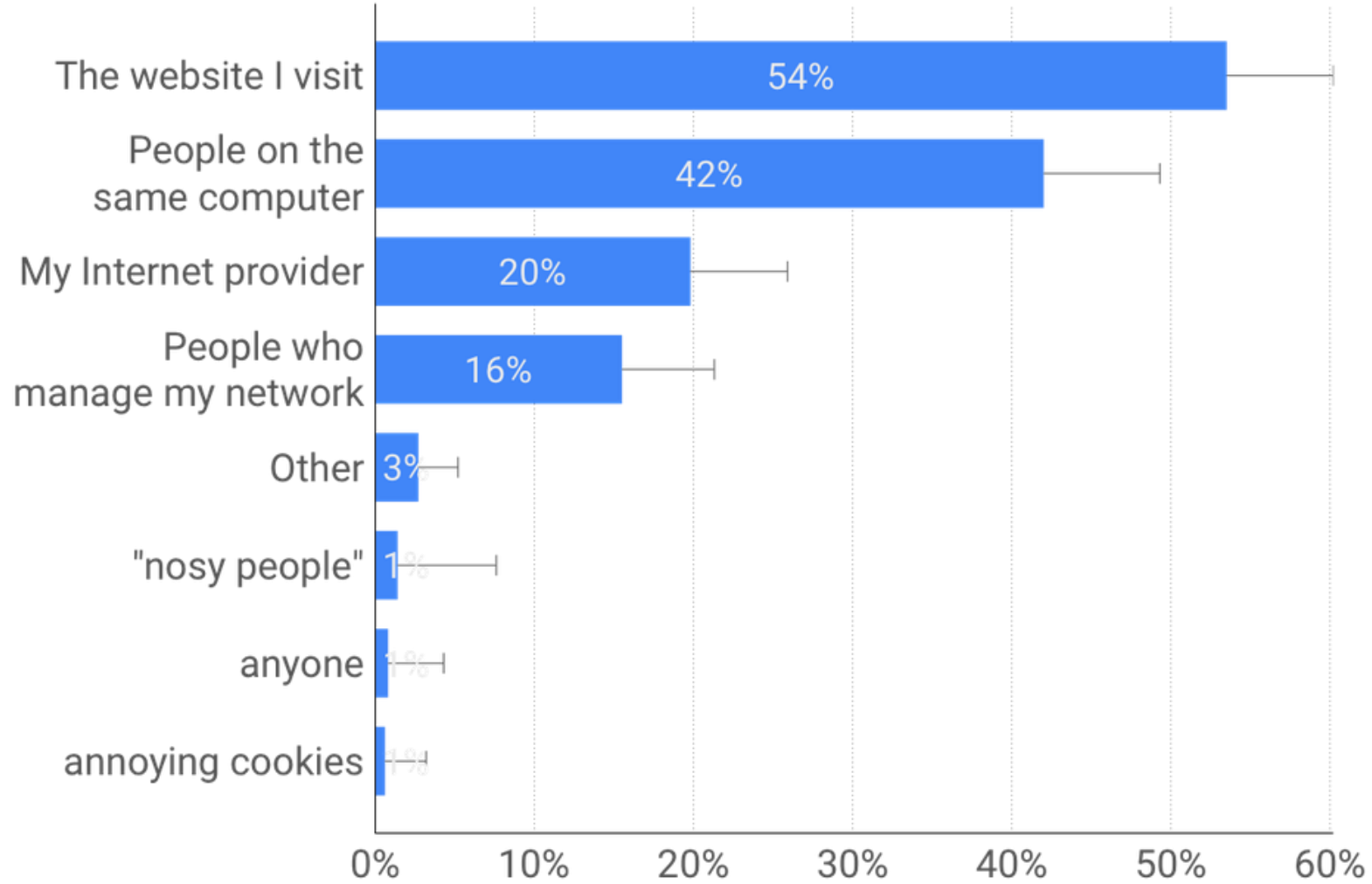
Do you know what private browsing is?



What do you use private browsing for?



You use private browsing to hide from...



Trackování na webu

- *datoví paraziti*
- cookies
- sledovací skripty
- *retargeting*
- browser fingerprinting
- canvas fingerprinting



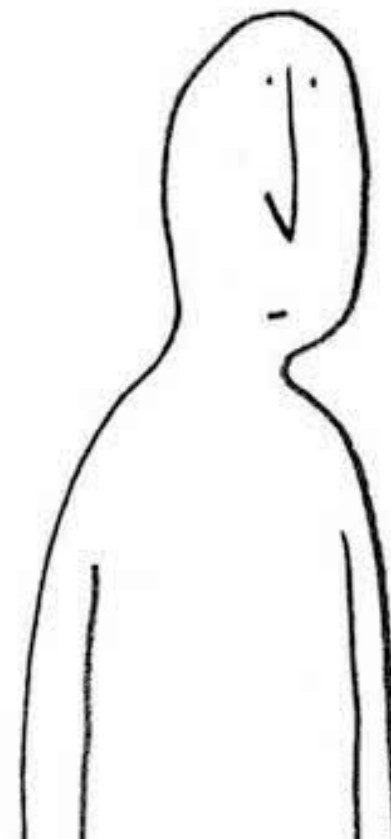
Pár doplňků a nástrojů

- [Panopticklick](#)
- [Am I Unique?](#)
- [Browser Leaks](#)

- [Privacy Badger](#)
- [Ghostery](#)

Jak to může vypadat v praxi

- Firefox – implementované nástroje
- uBlock Origin
- Privacy Badger
- [Firefox Containers](#)



HTTPS

- co je za potíže s HTTP?
- certifikace
- šifrované propojení
- <https://www.eff.org/https-everywhere>



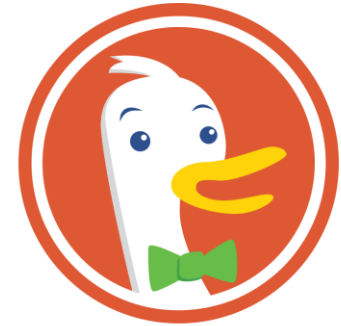
„Anonymní“ prohlížeče

- prohlížeče se striktním přístupem ke sledování
- většina blokací přímo zabudována
- <https://www.epicbrowser.com/>
- <https://brave.com/>



„Anonymní“ vyhledávání

- vyhledávače s odlišným modelem monetizace
- nesbírají data o uživatelích
- neprodávají reklamní prostor
- *za jakou cenu?*
- <https://duckduckgo.com/>
- <https://restoreprivacy.com/private-search-engine/>



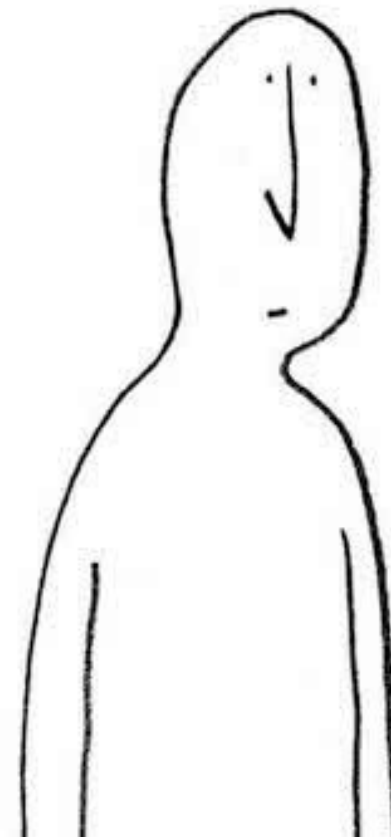
DuckDuckGo.

VPN

- důležitým identifikátorem je IP adresa
- *virtuální privátní síť*
- jak to funguje?
- jaké to má potíže?

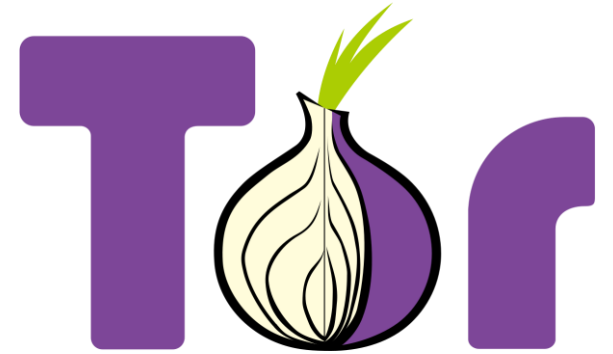
Jak to může vypadat v praxi

- ProtonVPN
- hostováno ve Švýcarsku
- no-log policy
- transparentnost
- *dvousečná zbraň*



Tor/Onion

- *onion routing*
- deepweb / darkweb
- Tor Browser / Orbot
- speciální struktura *.onion*
- opět: dvousečná zbraň



Categories

Drugs	18836
Fraud Related	2026
Guides & Tutorials	3702
Services	1431
Jewellery	54
Digital Goods	12425
Erotica	1396
Counterfeits	683
Electronics	33
Security & Hosting	90
Miscellaneous	312

Welcome to HANSA Market

The Darknet Market with the main focus on a trustless payment system, which makes it impossible for the vendors OR the site staff to run away with Bitcoins of the buyers.

Multisig escrow


Optional 2-of-3 multisig for buyers and 2-of-2 multisig as a fallback for buyers that do not want to bother with multi-signature. Money can never be accessed by the market staff. Theft is impossible.

No Bitcoin deposits

Every order has its unique Bitcoin address similar to BitPay's or Coinbase's payment system. Buyers have 15 minutes to pay the order and do not have to wait for deposits to arrive.

No Finalize Early

We do not support FE or partial escrow releases and we don't have to! The multisignature escrow makes it impossible for the site staff or vendors to steal any Bitcoins.

 Current Lottery Jackpot: ₿ 8.4545 USD 21,635.72 [Buy tickets](#)

Featured Listings



USD 11.36
₿ 0.0044

0.2G Sample - 80% Pure Bolivian Cocaine (Levamisole Free) (Free shipping) 10 €

AmsterdamSupply [+8|0]

Level 2 (9)



USD 199.00
₿ 0.0778

100 XTC Pill 230mg (MDMA) 84% ★ PINK DONALD TRUMP FACE ★ ONLY USA ★ SPECIAL DISCOUNT

DreamShop [+588|0]

★ Level 9 (800+)



USD 150.99
₿ 0.059

100 - Xanax Pfizer X2 Replicas 3mg Alprazolam - US2US - Tracked

StarkoftheNorth [+1|0]

★ Level 1 (1)

Decentralizovaný internet

- *běžný stav*: data na serveru
- *decentralizace*: každý kousek dat u sebe
- data nevlastní centrální bod
- v šifrované podobě
- <https://zeronet.io/>



Anonymní OS

- nejvyšší level
- všechno v jednom
- běží z CD nebo USB
- nezanechává stopu v PC
- <https://tails.boum.org/>
- *jaké to má potíže?*



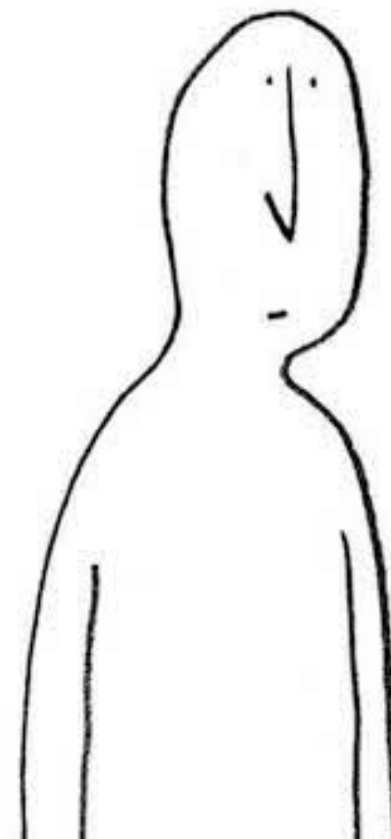
Váš obsah jinde

- *Gmail, Facebook,...*
- Přístup k vlastním datům
- Co to obnáší? – nastavení soukromí
- <https://haveibeenpwned.com/>

- [PRISM](#)
- [https://en.wikipedia.org/wiki/PRISM_\(surveillance_program\)](https://en.wikipedia.org/wiki/PRISM_(surveillance_program))

Jak to může vypadat v praxi

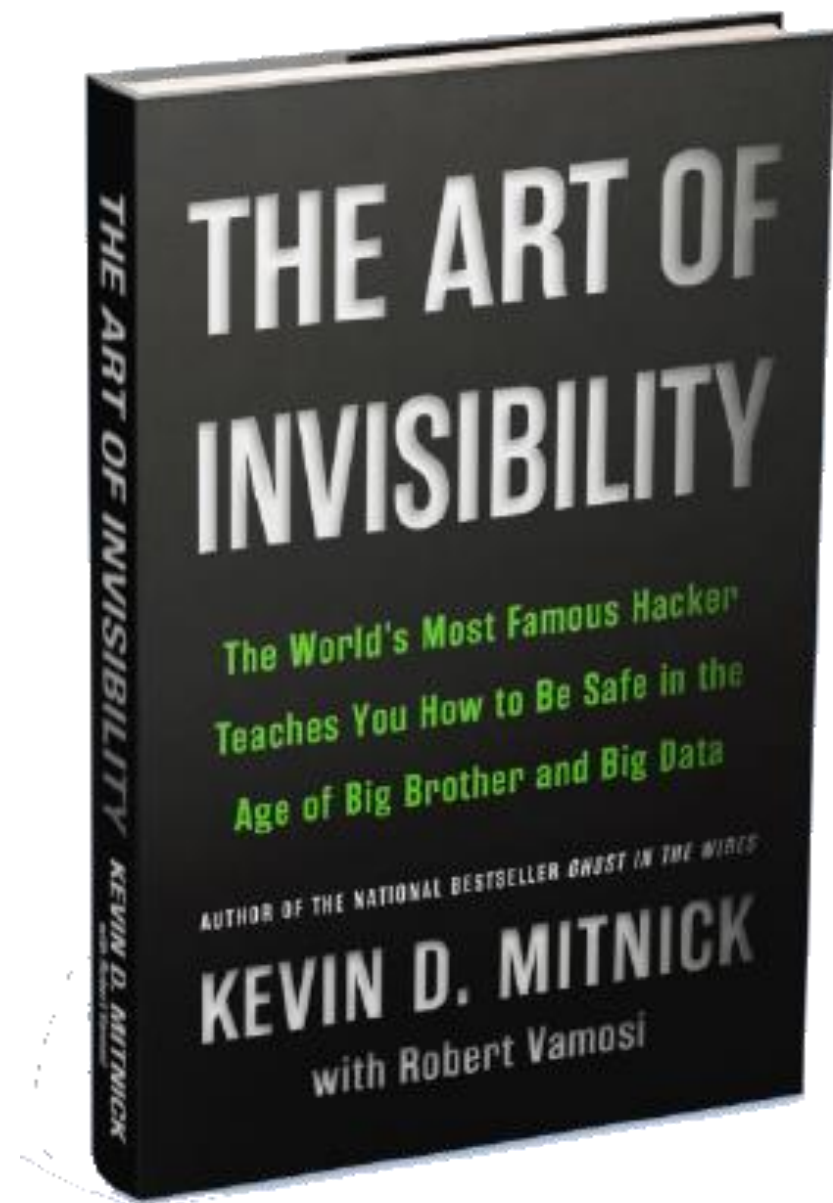
- Proklikat si všechna nastavení soukromí
- Zjistit si, co které znamená
- Nastaveny alerty na úniky dat
- Používat bezpečnější nástroje



E2E šifrování

- end-to-end
- WhatsApp, Signal, Threema
- *jaké to má potíže?*
- kritický počet uživatelů
- zadní vrátka
- [má to kontext](#)





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

AUTHOR OF THE NATIONAL BESTSELLER *OWST IN THE WOODS*

KEVIN D. MITNICK
with Robert Vamosi

THE ART OF INVISIBILITY KEVIN D. MITNICK

Šifrování dat

- šifrování dat na HDD
 - proč se to dělá?
 - implementováno do Windows
 - ochrana USB paměti
 - <https://a2larm.cz/2018/04/rozsifrovali-moji-radcove/>
-
- *mazání dat?*

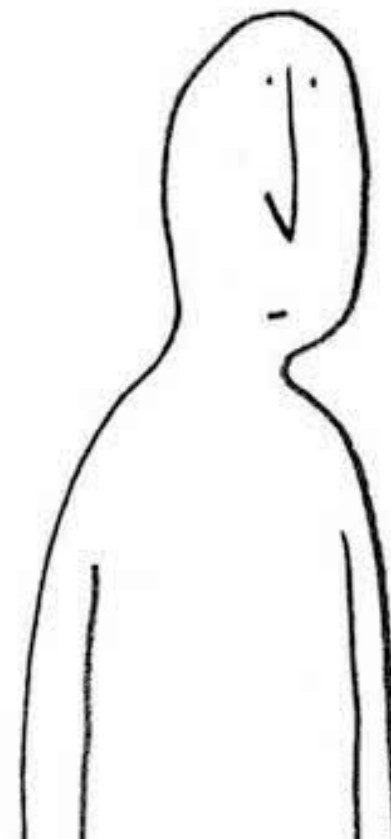
Heslo

- příběh ze života (HLP)
 - pevná hesla
 - správci hesel – jaké to má potíže?
 - 2FA
 - slovník / [brute force](#)
 - <https://haveibeenpwned.com/Passwords>
-
- pokud chcete lísteček, nastavte si jasná pravidla



Jak to může vypadat v praxi

- šifrování přes BitLocker
- LastPass jako správce hesel
- silné unikátní heslo
- některá hesla jen v hlavě
- 2FA skrze HW klíč



Není to jen o PC

- mobil jako vstupní brána do vašeho života
- anonymita? – *burner* – Kevin Mitnick
- IMSI CATCHER – Agáta
- geolokace

- IoT – internet věcí, chytrá zařízení (Aware Home)

- modemy
- <https://upc.michalspacek.cz/>

Není to jen o PC

- fotoaparáty
- EXIF informace
- <http://exif.regex.info/exif.cgi>
- geolokace
- webkamera

Myslete na soukromí

- Připusťte si roli soukromí v kyberprostoru
- Cílem není primárně schovat se před státem
- Cílem není schovat nelegální aktivity
- Mnoho stran dnes vidí, co děláte
- Vaše chování a data jsou pro korporáty zbožím
- Je na vás, jak si jich sami budete cenit
- Jednoduché akce razantně pomáhají