



OSINT

- **Co je OSINT? Open Source Intelligence** = získávání informací z veřejně dostupných zdrojů.
- **Příklady použití:**
 - Investigativní žurnalistika (např. Bellingcat)
 - Státní aktéři - bezpečnostní a ozbrojené složky (policie, armáda)
 - Soukromý sektor - pracovní i osobní informace (firmy si googlí kandidáty)
- *Otázka:* Zkoušeli jste někdy někoho vygooglit? Co jste našli?
- **!! Osobní informace jsou velmi cenné a poměrně snadno dostupné!!**

- OSINT představuje revoluci ve sběru informací

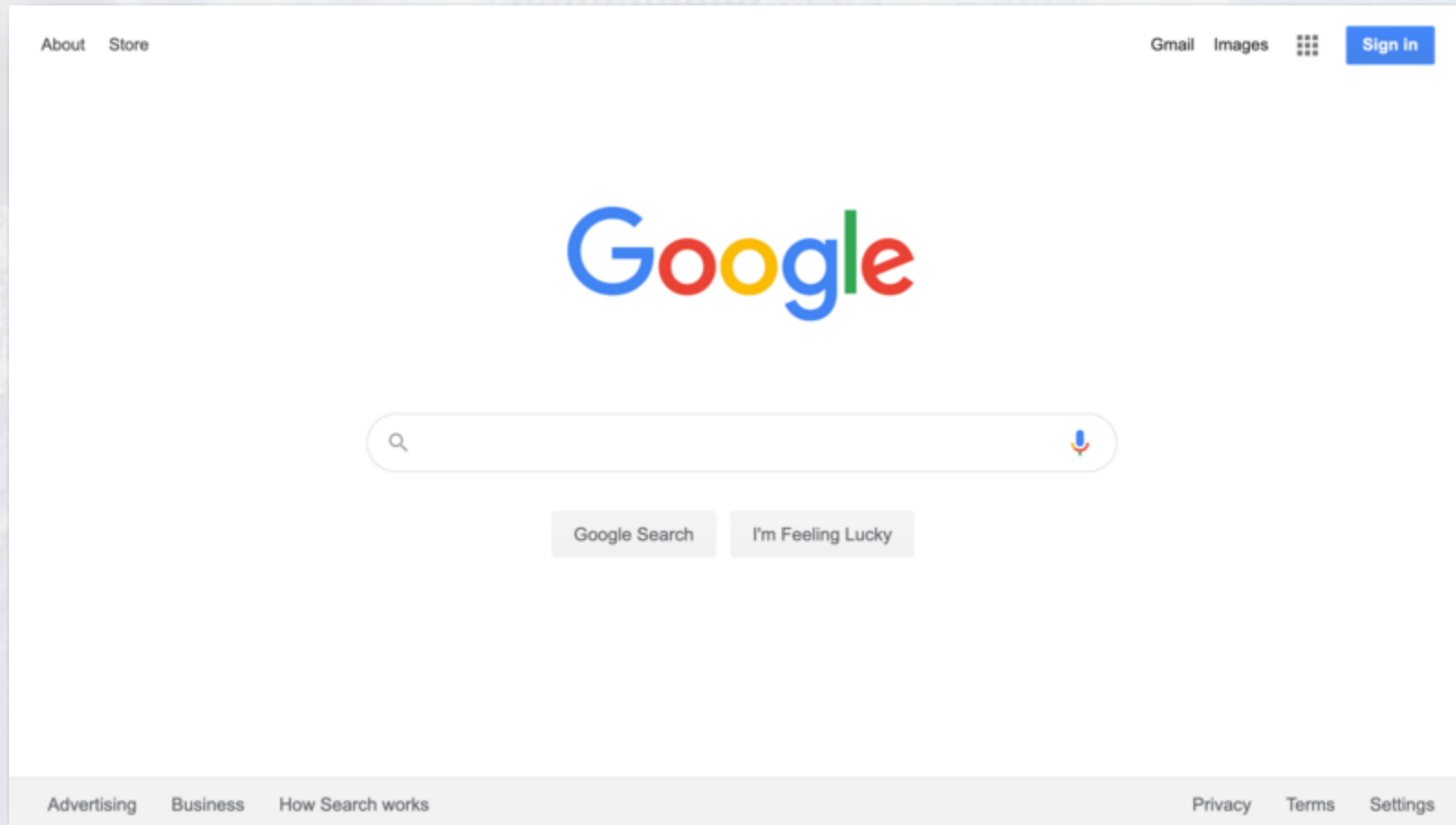




Kde začínáme?



..googlením



Používání uvozovek: "jméno příjmení"

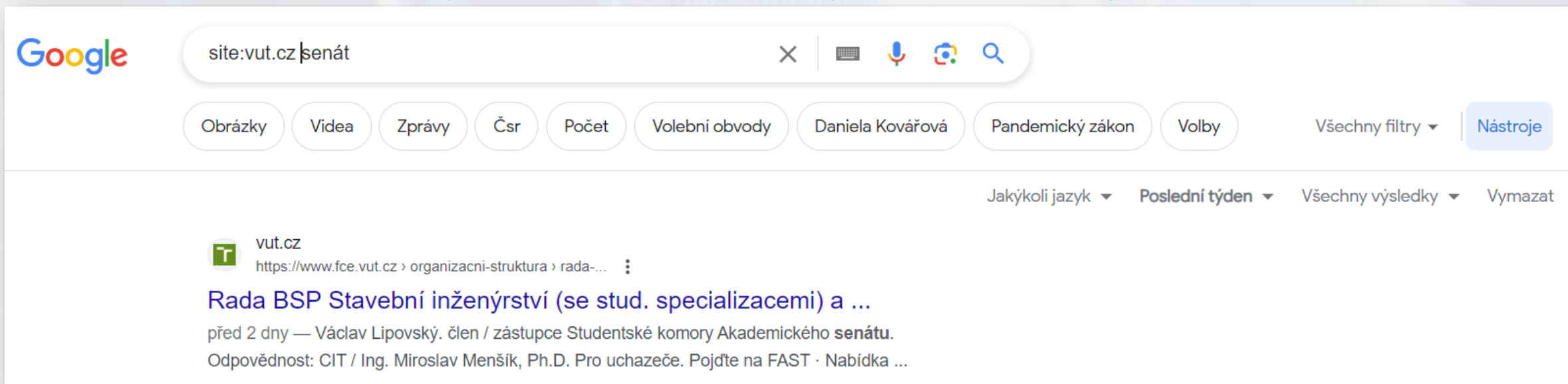
Hledání na konkrétním webu: site:instagram.com

Pokročilé triky: filetype:pdf, intitle:, -slovo

Obrázky a reverzní vyhledávání:

Ukázka nástroje: Google obrázky / Yandex / TinEye

.. Než se přesuneme k více specifickému vyhledávání



Google site:vut.cz senát

Obrázky Videá Zprávy Čsr Počet Volební obvody Daniela Kovářová Pandemický zákon Volby Všechny filtry Nástroje

Jakýkoli jazyk Poslední týden Všechny výsledky Vymazat

vut.cz
https://www.fce.vut.cz › organizacni-struktura › rada-...

Rada BSP Stavební inženýrství (se stud. specializacemi) a ...
před 2 dny — Václav Lipovský. člen / zástupce Studentské komory Akademického senátu.
Odpovědnost: CIT / Ing. Miroslav Menšík, Ph.D. Pro uchazeče. Pojdte na FAST · Nabídka ...

filetype:pdf europol list

filetype:pdf lenka auermullerová



Městská část Brno-Líšeň

https://www.brno-lisen.cz › kst2-14

z jednání stavební komise při MČ Brno - Líšeň, konané dne ...

Lenka Auermüllerová. Lubomil Oral. Jaromír Hladký. Ing. Hana Krafková. Ing. Vladimír Moravec CSc. za OÚRV ÚMČ Brno-Líšeň. May lecher. Аши. Grady. Жал plo ...

- Úniky dat a narušení bezpečnosti
- Hactivismus a data jako komodita

533 million Facebook users' phone numbers and personal data have been leaked online

Aaron Holmes Apr 3, 2021, 4:41 PM SELČ



Boeing assessing Lockbit hacking gang threat of sensitive data leak

Air Guardsman charged over US classified document leak



CYBER
SECURITY HUB

INCIDENT OF THE WEEK



Incident Of The Week: Garmin Pays \$10 Million To Ransomware Hackers Who Rendered Systems Useless

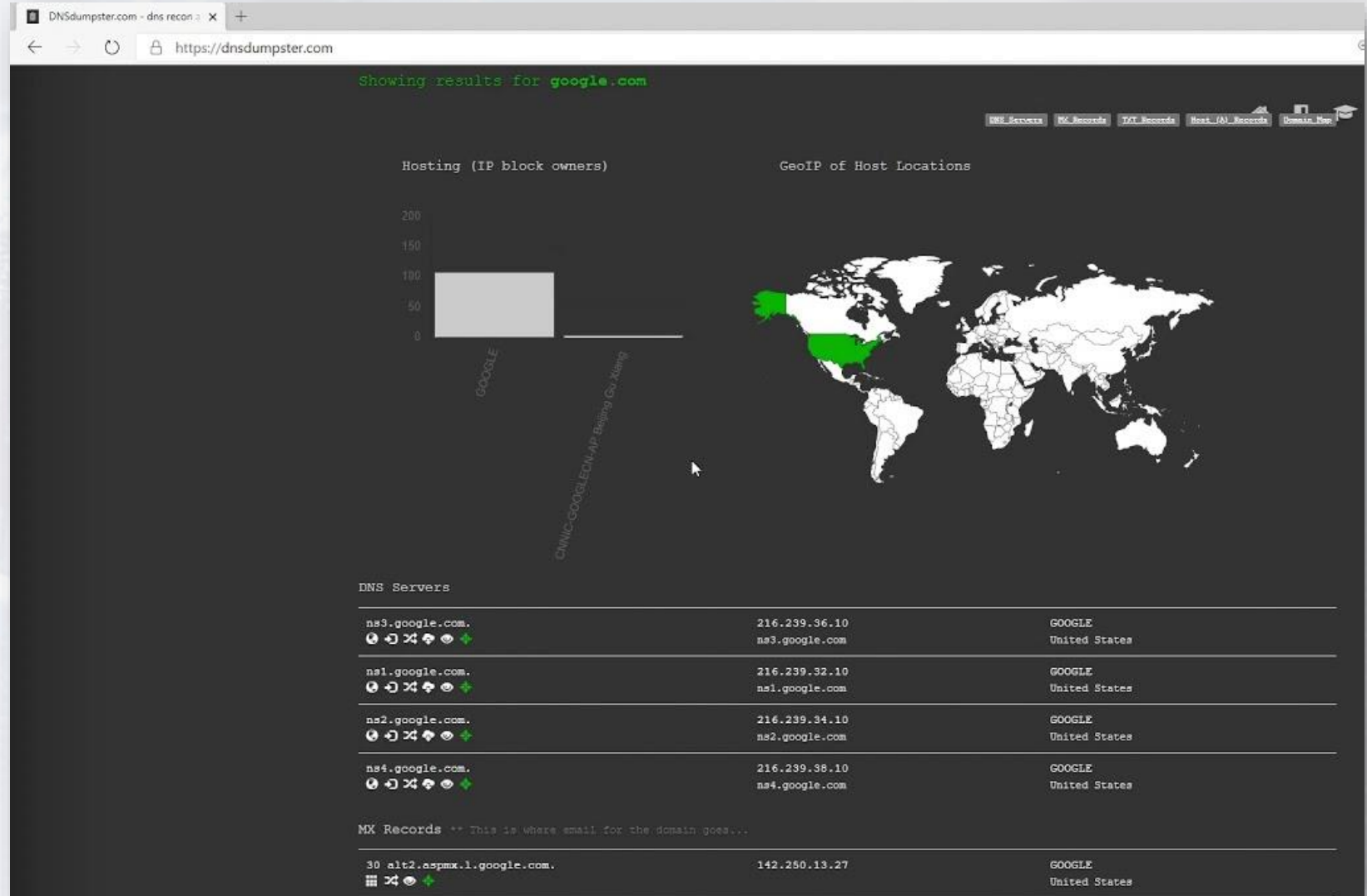
It is believed that Garmin paid the \$10 million ransom.

Etický hacking

- Network scanning
- Hledání slabín

who.is

WHOIS Search, Domain Name, Website, and IP Tools



';--have i been pwned?

Check if your email address is in a data breach

pwned?

Oh no — pwned!

Pwned in 18 [data breaches](#) and found 3 [pastes](#) ([subscribe](#) to search sensitive breaches)



Heroes of Newerth: In December 2012, the multiplayer online battle arena game known as [Heroes of Newerth](#) was [hacked](#) and over 8 million accounts extracted from the system. The compromised data included usernames, email addresses and passwords.

Compromised data: Email addresses, Passwords, Usernames



LinkedIn: In May 2016, [LinkedIn](#) had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords



4chan



reddit

STRAVATM

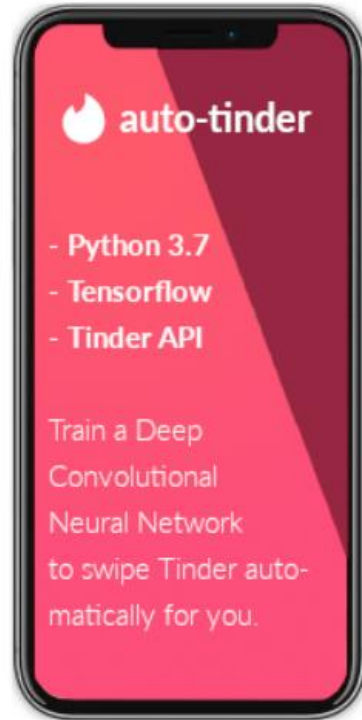


Rizika sdílení informací na sociálních sítích



- **Příklad:** Najdeme něčí Instagram/TikTok a ukážeme, co všechno o sobě (nechtěně) prozradil:
 - Kde bydlí
 - Kam chodí do školy
 - S kým se stýká
 - Kdy není doma
- **Reálné případy:**
 - Krádeže kvůli postům z dovolené
 - Kyberšikana a doxxing
 - Fake profily a catfishing
- "Zkuste o sobě zjistit, co je veřejně viditelné. Překvapilo vás něco?"

Rizika sdílení informací na sociálních sítích



```
(kali@Iris)-[~]  
$ python Uscrapper.py -u z0m31en7.github.io
```

USCRAPPER (v1)

A Webpage scrapper for OSINT.
-By: Pranjal Goel (z0m31en7)

[+] Email Addresses:
pranjalgoel@protonmail.com

[+] Social Media Links:
<https://instagram.com/z0m31en7>
<https://github.com/z0m31en7>

[+] Author Names:
sage

-----Non-Hyperlinked Details-----

[+] Email Addresses:
pranjalgoel@protonmail.com

[+] Phone Numbers:
+917415122415

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE

Python + - [] [X]

```
ocal/Programs/Python/Python39/python.exe "c:/Users/USER/Desktop/Person  
al Assistant/pro1.py"  
<Profile cristiano (173560420)>  
Username: cristiano  
User ID: 173560420  
Number of Posts: 3147  
Followers: 346382334  
Followees: 483  
Bio: http://www.cristianoronaldo.com/
```

Jak to funguje v armádě??

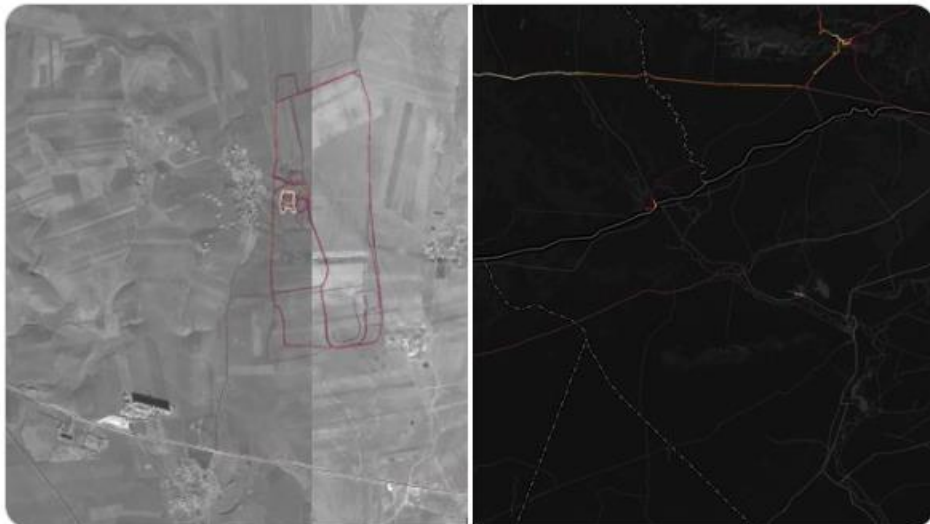
- OPSEC = „operational security“
- Opatření na ochranu potenciálně významných informací o vlastním subjektu
- Porušením OPSEC může být příspěvek na sociálních sítích, telefonát
- K porušení OPSEC může dojít ze strany jednotlivců, ale také například z oficiálních kanálů a třetích stran

**Nathan Ruser**

@Nrg8000 · Follow



Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). [medium.com/strava-enginee...](https://medium.com/strava-engineering) ... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable



7:24 PM · Jan 27, 2018

**B B C**[Home](#) [News](#) [Sport](#) [Business](#) [Innovation](#) [Culture](#) [Travel](#) [Earth](#) [Video](#) [Live](#)

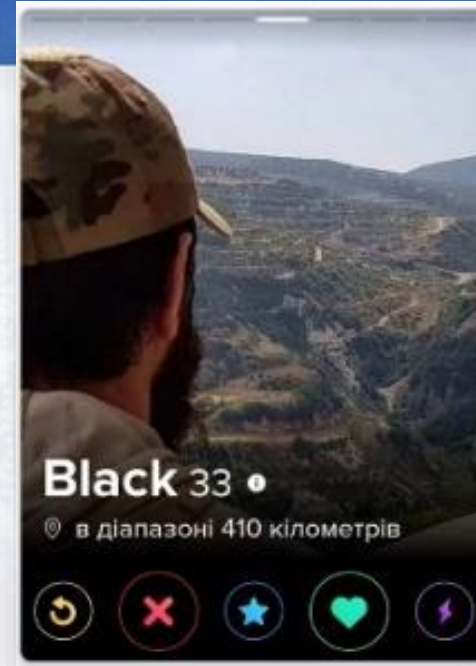
Ukraine war: Russian ex-navy commander shot dead while jogging in Krasnodar

11 July 2023

Share

George Wright
BBC News

OSINT, OPSEC v armádě



Dasha: "Where are you? Are you in Kharkiv?"

Andrei: "Of course I am not in Kharkiv but I am close – 80km."

Dasha: "Do you have any plans to visit us?"



July 2012

New photo

June 2014

July 2014



Zlaté pravidlo: "Sdílej jen to, co bys ukázal učiteli nebo babičce."

1. Ochrana účtů:

- Dvoufázové ověření
- Silná a odlišná hesla
- Pozor na phishing

2. Pozor na to, co posíláte

- Sexting = nebezpečí (i právní důsledky)
- Nevěřit lidem jen podle profilovky

3. Digitální stopa

- Co na internet dáš, to tam zůstane

1. Soukromý a pracovní (služební) život nelze v online době oddělit!
2. Emoce jsou vždy silnější než rozum člověka!
3. Lež se sociálními sítěmi šíří rychleji než „nezajímavá“ pravda!
4. Pokud si chceme posílit argumentaci hledáním na internetu – vždy si najdeme dostatek důkazů o své pravdě (konfirmační zkreslení)!
5. I když si myslím, že já nejsem pro nikoho (útočníka, hackera) zajímavý – jsem zajímavý!
6. Na mě si s phishingem nepřijdou – ale přijdou, pokud nebudu opatrný!
7. Já tomu rozumím, četl jsem to na netu! – nemusí to být pravda – pravidlo 4!
8. Digitální stopu nevymažeš!
9. Pokud neplatíš za produkt, ty jsi ten produkt!
10. Lidská hloupost nezná hranic!



- ✓ Wi-Fi a Bluetooth používat jen výjimečně,
- ✓ chytré hodinky, bezdrátová sluchátka atd. – potenciální přístupová cesta do mobilního telefonu.



Dotazy?

Děkuji za Vaši pozornost