Personal OSINT

OSINT for Ordinary People

Nadine Whitfield

SeaGL 2019

- About Me
- About OSINT
- Demo
- Good Practices & Countermeasures
- Closing Thoughts
- Q & A

About Me

- Certified Ethical Hacker. FullStack developer. Security & privacy advocate.
- Currently working at ThoughtWorks software consultancy.
- Enjoy photography, music and motorcycles.

Today’s presentation is to share some of my learnings on this topic and (hopefully) inspire you to learn more.

What is OSINT?

Open Source INTelligence is drawn from publicly available material, including:

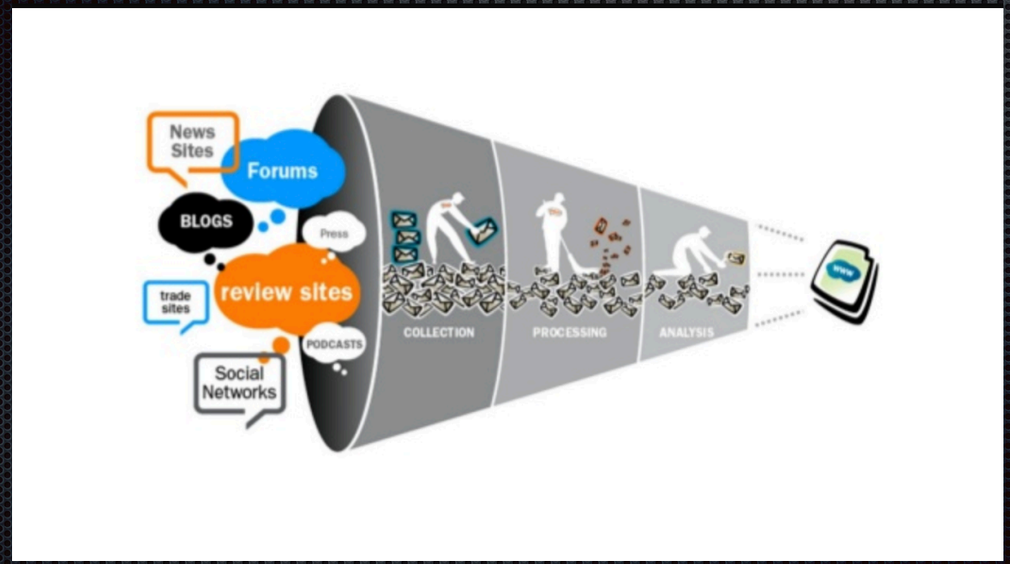
- Internet
- Offline media (e.g. television, radio, newspapers, magazines)
- Specialized journals, conference proceedings, and think tank studies
- Photos
- Geospatial information (e.g. maps and commercial imagery products)

- from cia.gov

Who does OSINT? Why do it?

- Hackers, Penetration testers, Business Researchers, Law enforcement, Journalists, Intelligence agencies, Stalkers, Criminals, Terrorists and…..You
- Depending on perspective any one of these could be an Investigator or Attacker
- Regardless, the Primary goal = identify actions and targets with *lowest* risk and highest chance of success

How?



Loop Arrows are missing!

Collection, Processing, Analysis

- Largely aided and abetted by Open Source Software
- Emerging technologies such as cloud computing and artificial intelligence have accelerated these efforts
- Starting with small bits of data, find relationships, analyze and pivot. Rinse and repeat.

Search engines are just the gateway

- In reality, most data on the internet is in databases or accessed through APIs. This is known as the "*deep web*" (not dark web). Much of this data can be extracted using enhanced queries (aka "google dorks") or tools with custom programming
- Anything connected to the internet or in public view is fair game for OSINT
- OSINT is the first part of any professional social engineering, penetration testing or cybersecurity attack, and is often used by low-tech criminals as well

We are swimming in a sea of data. *Some* is under your control

- Any device you *log into* or *wear* is a potential data source
- Social Media - Often called the '8th layer' of the OSI model by privacy researchers
- Online surfing and shopping habits. Big data insights often discover relationships that humans don't see

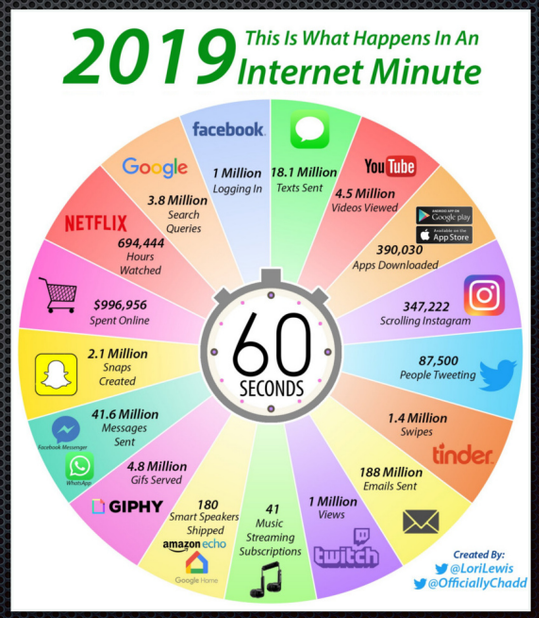
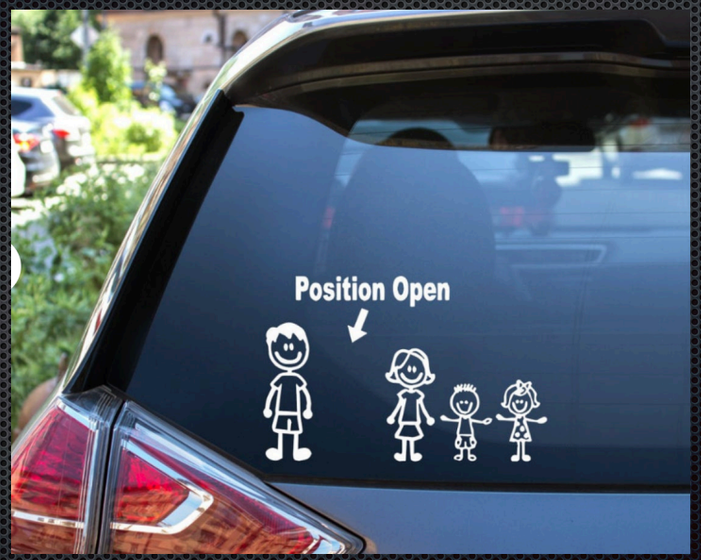


Image credit —
https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/

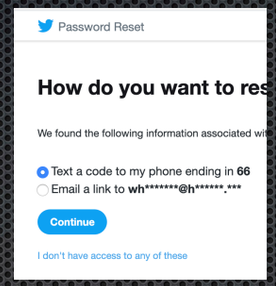
Data under your control

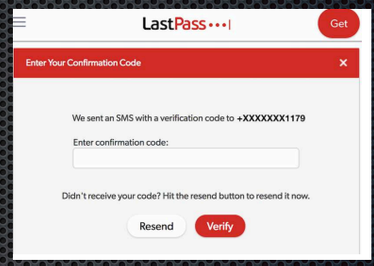


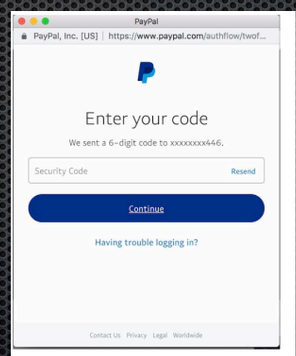
Family structure. Marital status.

Careful with that phone number!

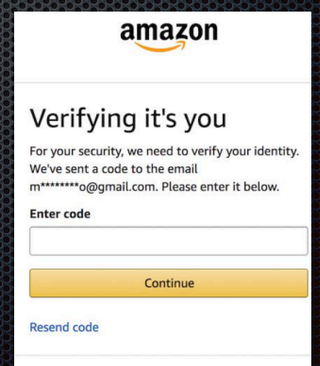
- Mobile Phone numbers often link directly to credit history, social security number and other sensitive data
- Please do NOT use text messages for Multi-factor Authentication!







2FA shows 3 digits



azon password reset using phone number

Data NOT under your control

- Data breaches, Sites that share or sell it*
- Government & real estate sites
- Photo tagging, facial recognition, chatty friends on social media

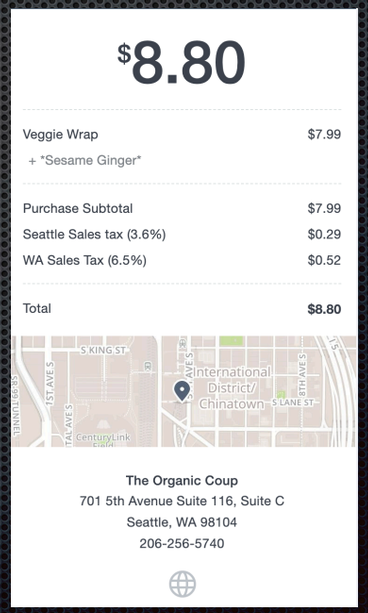
- FB has the largest repository of facial images in the world w/location attached

- Newsletters often publicize life events
- ex. Google dork -> church|temple|synagogue|mosque newsletter filetype:pdf -sample. These are usually archived over time.

- interior shots, floor plans, video walkthroughs, etc

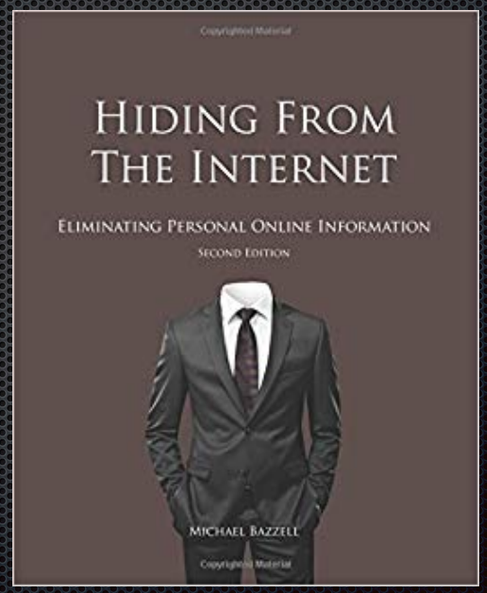
Data sharing between merchants and websites

- If you sign up to get an email receipt at one merchant who uses the *Square* device for checkouts, the system defaults to automatically email you receipts from any other merchants you visit in the future who also use Square
- This is totally separate from data mining sites who freely share , sell and re-sell data



Good Practices & Countermeasures

1. Do OSINT on yourself. Learn what is out there. A tool like the Lockfale OSINT framework provides a useful guide with links to appropriate tools.
2. Visit the 'Data Detox' kit online, It offers concrete steps you can take for mobile devices as well as for your online profile.
3. Change passwords today (no reuse!). Best to get a password manager to help with this.



Lockfale OSINT framework -
https://osintframework.com

Data Detox Kit -
https://datadetoxkit.org/en/home

Password Managers (openSource and commercial) -
https://www.ign.com/articles/the-best-password-managers-2019

Image — Michael Bazzel is a great source of info about privacy —https://inteltechniques.com/

More…

- Strict separation of personal and professional accounts
- Consider spreading a little partially true information about yourself to create noise
- Discuss your data sharing wishes with those who might share data about you (children, colleagues, friends, family, relatives)

Closing Thoughts

- Every online service and activity requires a trade-off regarding privacy. You need to decide— Is it worth this?
- If you know students (high school or younger), here is a great lesson to raise awareness — http://digitalfootprintimu.weebly.com/

Resources file has info about “opting out” of mailing lists, but this is not very practical. There are too many sites that share & sell data to others

http://localhost:57575/session/0a3b387c-d8e0-4fa2-810b-c65f34aad45c

Want to learn more?

- Check out my GitHub repo.
- If you find another great resource, please fork my repo and submit a pull request.
- Url — https://github.com/infomaven/personal-osint


DEMO

THANK YOU

PS - check the calculator