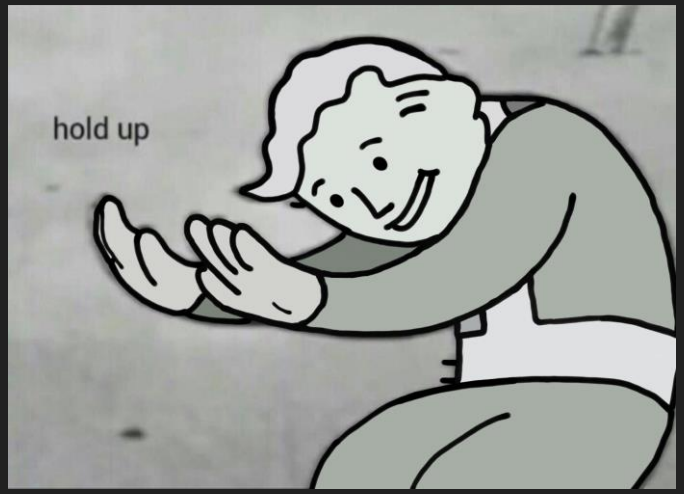
OSINT

and a tiny bit of social engineering

By Aaron

Disclaimer

I'm not a lawyer, don’t take my word for it. Don’t do something stupid. I’m not responsible for your actions.



But wait, isn't that illegal?

OSINT: *“Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context.” (in other words, looking at someone’s public digital footprint)*

Social Engineering: Morally wrong.

OSINT is NOT doxing.

Doxing = stalking (harassment) (don’t do this)

Mindset to have

Be ethical.

Don't abuse it.

Proportionality is important (Don’t break your friends)

What is OSINT?

- InfoSec
- Open Source Intelligence
- Useful Life skill
- Good foundation to any pen-test

- Passive reconnaissance (only open public information)
- Active reconnaissance (physically engage. Information behind portals) (This is where it becomes illegal)

Uses?

- Paid to find out information about a company or someone? OSINT!
- Want to know what people to talk to at an event? OSINT!

- Seen the show *Hunted UK* before? (I recommend)
- That entire thing, is OSINT.
- Your basically a spy.
- Have fun

How bad is the UK?

- Surely no one will look into me?/want to get my data
- THEY WILL

- UK is Part of the most watched nation
- All data online is usually tracked or logged. Sometimes we have access (if you have a tin-foil hat, please put it on now)
- (https://en.wikipedia.org/wiki/UKUSA_Agreement)

Tools to use

- Google
- Facebook (Lookup numbers, social networks, marketplace postcodes etc)
- Twitter (lookup numbers)
- LinkedIn (Become a company, you can get there email)
- Whatsapp (type in there number, get a photo and name :))
- https://github.com/Greenwolf/social_mapper
- t2a.io
- Maltego!
- Namechk
- Haveibeenpwened
- Wayback machine
- Electoral-role
- Companies house
- Brain (Think outside the box)

Google Dork

Site: www.yoursite.com

Inurl: “/admin.php”?

Intitle: “Index Of”

-site:facebook.com +site:facebook.*

(site:facebook.com | site:twitter.com) & intext:"login"

Filetype:docx

Cheatsheet: https://gist.github.com/sundowndev/283efaddbcf896ab405488330d1bbc06

Facebook

- Search for numbers
- Search for emails
- Extract friend list/close friends
- See location (Through marketplace)

Whatsapp

- Add number in your contacts
- Whatsapp will suggest there name along with their profile picture

Linkedin

- get someones email, contacts, CV(?), and more!

Wayback Machine

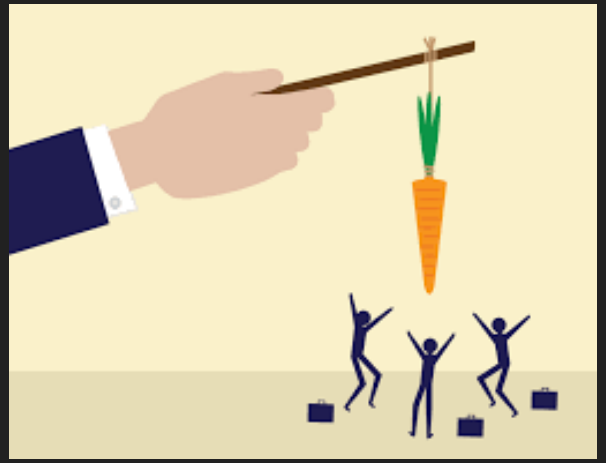
- Crawls the internet making copies of EVERYTHING!
- https://web.archive.org/

The “tiny bit of social engineering”

- Social Engineering, the art of being 1 step ahead
- Behaviour models
- People's mindset (Changing, get sub-conscious attention, Inject information)
- Neurotypical - Neuroatypical
- Subliminal - Superliminal
- Neuro-linguistic programming (NLP) (words effect message)

- People have alerts/triggers. (suspicious? Shutdown.)

Cognitive Biases



- Shortcuts

- Humans love patterns. Everyone follows patterns. EVERYONE
- If you say your exhemt, your not…
- Walking, Mirroring.

Cognitive Biases

- CVE’s of humans
- Anchoring BIAS:
- Confirmation BIAS: needs conformation of things they do
- Attentional BIAS: Ignores other factors when making decisions
- Ostrich BIAS: The tendency to ignore DANGEROUS factors when doing something
- Clustering BIAS: seeing patterns in random events

- Cool infomation: https://www.verywellmind.com/cognitive-biases-distort-thinking-2794763

Challenge:

Find out information about this person:

https://twitter.com/owoodflint

- Email
- Password
- Address
- Wifi SSID

- References: tryhackme.com