Own Your OSINT

How to Minimize Your Digital Footprint

by RealAsira

Introduction

- **Open-source intelligence (or OSINT) is exactly what is sounds like ... intelligence or information that is open-source or publicly available. OSINT techniques and tools are therefore used to create a profile of who someone is.**

- **OSINT Profiles may include data as simple as social media accounts/posts or damning as a personal addresses, familial ties, birthdate, phone numbers, etc...**

- **Last month, redacted brilliantly demonstrated some of the OSINT tools that are available to help profile someone. During that demonstration he voluntarily doxxed information about himself and another participant. I then volunteered to have him produce a profile on me. Turns out, I'm pretty well hidden so I was invited to teach a follow-up on how to practice privacy and security. So welcome to the workshop, "Own Your Open Source Intelligence: How To Minimize Your Digital Footprint".**

Agenda

- A brief review of OSINT tools/techniques
- Practical steps you can start taking today to enhance your privacy
- Techniques you can use to reduce your digital footprint
- How to protect against OSINT-based targeting (and therefore minimize your doxxability)
- How to audit your own information that you've unwittingly open-sourced
- Best practices for security regarding you and your data

Disclaimer

- **It’s important to note that OSINT should always be conducted ethically and legally. The techniques demonstrated will focus on using publicly available information without infringing on privacy or breaking any laws.**

- **OSINT can be incredibly invasive if misused. Always ensure that your activities comply with legal standards and respect individual privacy. Targeting people without their consent is unethical and often can be illegal.**

- **Participating in this event does not imply endorsement of any unethical or illegal activities. The goal is to educate and inform about the capabilities and applications of OSINT, and how to protect yourself against bad actors, in a responsible manner.**

- **Furthermore, I offer no legal advice here. To the best of my knowledge and understanding, I'm only offering information that is entirely legal but it is up to you to validate that.**

What OSINT Exposes

- Full Name
- Birthdate
- Location
- Employment
- Family, Friends
- Public Records (Legal)
- Social Media
- Financial (Sometimes)
- Metadata
- Domain Information
- Email
- Phone Numbers
- and
- more

Recap on OSINT Techniques

- **Utilize online tools such as such a everyday search engines, specialized search engines, social media, and public records to find and link information to an individual or individuals.**
- **Safety: Use a VM (Linux-based preferred), privacy browser, VPN, and password manager for OSINT services (NOT related to regular password manager and 2FA).**

Get Hooked

- **Story of my online friend ... he asked me to doxx him using just a little information to start. I had his gamertag, DNS Provider, and some nearby stores he shops at.**
- **I found: his name, birthdate, several addresses, employment history, friends & family (didn't dig into), marriage record, domain information, phone numbers, email addresses, private websites and Github accounts.**

What is Privacy? Security?

- Privacy – The right and ability to control information about yourself.
- Security – The protection of systems, information, and assets.
- That is, mechanisms of security are used to ensure privacy. Privacy and security go hand in hand.

Don’t Sprint, Jog

- **Privacy and security are a marathon, not a sprint. About a decade ago I became curious to see what information I could discover about myself online. At the time I was a minor but still found my full name, my birthdate, home address, and links connecting “anonymous” profiles back to me.**
- **I promise it won’t take you a decade to get to a point of achieving security and privacy that aligns with your threat model, so long as you keep at it.**
- **Remember, you don’t need to do everything I’m about to teach or that are in the resources; your threat model is going to be different than mine. You may tolerate more or fewer privacy “holes” than I do.**

Threat Model

- What are you protecting? (Data, yourself)
- From whom?
- Risk likelihood?
- What are the consequences of failing?
- How much trouble are you willing to go through?

Initial Privacy Audit

- Use the “Privacy Audit worksheet.”
- Use OSINT tools to dig up as much public info as you can
- Record on the Privacy Audit worksheet

Basics of Personal Security

- **Password Manager**
- **2FA & Hardware Keys**
- **VPN & Internet Safety**
- **Biometrics?**
- **Carrying “Risky” Data**

Basics of Personal Privacy

- Delete your social media ... or make it entirely anonymous if you must have it
- Privacy-oriented web-browser
- Privacy-oriented search engine
- When you give data, it's "public" forever

Audit Your Digital Services

- **Determine EVERY digital service you've EVER used. Record the username, password, and email into your password manager.**
- **Don't change them yet.**
- **Decide what each services offers you. Is it worth keeping? Can you find an alternative for privacy? De-FAANG.**

Eliminate Services by Finding Alternatives

- ***Using Cloud Storage as an example***
- **Virtually every online service has alternatives. Consider:**
- **Use an offline option**
- **Consider self-hosting (NextCloud/FileBrowser)**
- **Privacy-oriented (Proton)**
- **Not linked to anything else, anonymous information (Anonymous Google)**

Eliminate Services by Deleting Your Data

- **Delete whatever information you can**
- **Replace remaining information with false info**
- **Request account deletion (delete button, from privacy page, send an email)**
- **Delete legally protected info after retention frame ends**

Better Password Management, 2FA

- **Change all your usernames to be entirely unique and anonymous … in way tied to you.**
- **Change all your passwords to be entirely unique. Use a random password generator with mixed-case, numbers, and symbols.**
- **Use 2FA absolutely everywhere … NO passkeys (biometrics)**
- **Consider a second 2FA**

Obfuscate Your Data

- **For whatever online services you have opted into, obfuscate your data.**
- **If they don’t need real data legally … don’t give it to them. Give them something made up.**
- **Word of warning: This can make online shopping MUCH more difficult, so carefully balance privacy with ability to shop online if needed. Consider shopping offline only.**

Domains for Email

- One for IT Hosting
- One for anonymous professional usage
- Make sure the registration information is hidden
- SSL and HTTPS only
- Cloudflare

Cloudflare Domains, SSL, HTTPS

- **Origin Server – Configure SSL behind firewall**
- **DNS Settings – Set to Proxy**
- **SSL (TLS) – Full Strict**
- **Page Rules – HTTP→HTTPS reroute**

Recommended Email Aliases

- Use private-provider like Proton or Tuta
- “Root” email (sign in only)
- Private email (friends and family)
- Professional anonymous (contact@example.com)
- Professional real name (name@example.com)
- A variety of anonymous emails for online services

Determine Which Services for Which Email

- Take your list of used services + apps.
- Determine which services “belong” to which emails
- Detach single-sign on such as Google Sign-In.
- Update sign-in email to new one
- Use “Tracker Tag” (name+service@example.com)
- Consider forwarding service like passfwd.com or simplelogin.io

Private Phone Number (VOIPs)

- **Find a provider such as voip.ms**
- **Avoid using your cell-service provided number**

Recommended Phone Aliases

- One “root” number … cell-service provider … never give
- One for friends a family
- One for employers
- One for shopping
- One for other online services
- 619.364.0003

Purchase Privacy

- **Use cash**
- **Use each credit card you have at only one location**
- **Use services such as privacy.com to create “burner cards”**

Private Address

- **Three Options – PO Box, CMRA, PMB**
- **All require a certain level of identity validation**
- **Your mail is sent to these companies … all can hold mail and PMB’s can forward**

PO vs CMRA vs PMB

- **PO Box – Requires current physical address and ID card. PO Box is linked to your address**
- **CMRA (such as UPS) – requires ID (passport) and utility bill (no address validation)**
- **Local CMRA – Other local CMRA's can be a better option than UPS as they are less stringent**
- **PMB – alternative to CMRA but I'm skeptical about their security.**

Public Alias

- If you aren’t required to legally identify yourself … don’t!
- Memorize alternate birthdate, VOIP number, address, and name.
- Consider carrying an alias “identity” card (e.g. idcreator.com) – never make it appear official, government issued, or to be legally identifying.
- Public-facing website to “authenticate” alias.

Alias Disclaimer

- **To reel it back in: DO NOT use an alias identity if you are legally required to provide your legal information. This is especially true for law enforcement, financial institutions, medical institutions, age dependent establishments such as bars, etc... In fact, you should print "not for legal identification" or some other disqualifier on said card. Further, it is absolutely illegal to put anything that my look like a legal identity, includes anything that might indicate government, etc...**

When Legal ID is Required

- **When you are required to give legal ID, avoid giving them your driver's license. Shockingly, your passport is actually a lot more private and secure than you driver's license and it is technically more "validated by the government". This is great for employment, age-regulated establishments, financial and medical institutions, etc.**

Estate Planning

- **Prepare a will**
- **Prepare funeral plans**
- **Review them regularly**
- **Get an estate-planning attorney**

Device Privacy and Security

- Devices are not friendly by default
- They want to steal and sell your info
- Start owning your devices ... don’t let them own you!

- Properly configured firewall & VPN
- Disable startup apps
- Remove unnecessary apps

Switch to Linux!

- **Linux is simply the best option when it comes to privacy**
- **Find a flavor/fork you like and go from there**
- **There are privacy-hardened flavors such as Fedora, Qubes, Tails,UPR, Alpine, and Kali. Really any version of Linux is better than the alternatives tho, so find one you enjoy.**

Don’t Switch to Linux!?

- **Linux is becoming more and more compatible every day but it isn’t 100% there yet.**
- **Use a registry editor like O&O Shutup 10 to lock down telemetry on your device. Regularly re-check the settings.**

Mac Users are Screwed

- **Just ... anything is better for your privacy than Apple. Literally anything.**

Mobile Forensics Recap

- **Your phone stores everything on it and in cloud backups**
- **EVEN DELETED DATA**
- **View the Intro to Mobile Forensics Lab Worksheet**

GrapheneOS for Mobile

- **Android is better for privacy but Google DOES have telemetry baked in.**
- **Consider using GrapheneOS instead.**
- **The only thing I haven’t gotten to work on GrapheneOS is tap-to-pay; However, it WILL take work to get it set up and find alternatives to your apps in some cases.**

IOS Users are SCREWED

- **Again ... anything is better for your privacy than Apple. Literally anything.**

To Smart Phone or Dumb Phone?

- **I would actually recommend having a smart phone because you can use it for 2FA, VOIP, password management, and communication. You could use a physical hardware key (or keys) instead of mobile-2FA, have a dumb-phone with multiple SIMs, and keep password management exclusively on your laptop/desktop ... but that is extreme, unnecessary, and impractical for most people.**

Privacy Audit Round 2 & 3 & 4 & etc

- Regularly audit your information (1-2 times/annum)
- Look for leaks
- Patch holes
- Replace information
- Delete accounts
- Etc

How to Maintain Your Privacy

- **Do you need this new services you're considering?**
- **Is there an alternative?**
- **Is it worth giving up your info to be sold?**
- **How about obfuscated information?**
- **If you want to delete that account/info ... what does the process look like?**
- **Regular audits! Patch leaks immediately ... don't ever reuse compromised data.**

Additional OSINT and Privacy Resources

- **https://inteltechniques.com/ is my favorite spot to launch an OSINT profile. It also has links to the OSINT Techniques and Extreme Privacy books for purchase. The OSINT Techniques book provides in depth information on profiling publicly available information. Extreme Privacy details how to protect yourself from it. It also has tools for starting an OSINT profile.**
- **https://osintframework.com/ is another really good spot to start and OSINT profile and provides quite a variety of tools to do so.**
- **https://dnsdumpster.com/ and https://lookup.icann.org/en are my go-to's for investigating information publically contained in website registration records.**
- **https://www.iplocation.net/ is great for approximately geo-location an IP address (possibly gained from DNS records).**
- **https://github.com/krishpranav/maigret/ is an open-source tool for automagically creating a digital profile from usernames.**
- **https://usersearch.org/ is a great tool to quickly lookup everywhere a username has been used.**

Other Thoughts

- **It is possible to further hide addresses, phone numbers, and income information. But they are more advanced and beyond the scope of this presentation.**
- **Extreme Privacy book – private homes, lodging, vehicles, driver's license, data brokers, disinformation, death & disaster planning. These are beyond the scope of likely almost everyone here and I'm not familiar enough with some of these advanced concepts to feel comfortable teaching them.**

Thank you for attending my Ted Talk

- **Yes really, thank you. I would be very sad if I came and presented to an empty room.**