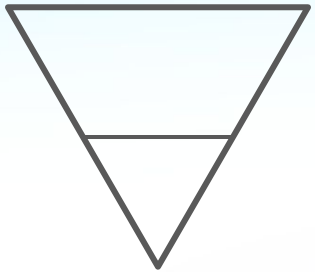


“The enemy is not just ‘men’ or their individual male chauvinism... Institutional sexism is sustained by a class system which supports male power.”

- Witches Midwives & Nurses, A History of Women Healers

Digital Privacy & Security:

Hide Your Footprints

Privacy = the default right to keep things secret. The ability to control how, when, where, and with whom your data is shared.

Security = Your safety, wellbeing and kept privacy by the software you use. It behaving as intended, and ability to withstand compromise.

Privacy = the default right to keep things secret. The ability to control how, when, where, and with whom your data is shared.

Security = Your safety, wellbeing and kept privacy by the software you use. It behaving as intended, and ability to withstand compromise.

OPSEC = What you do to maintain privacy and security, especially while doing something sensitive.

Compartmentalization = A way of approaching OPSEC that's about having clear thoughtful boundaries of what you use, how you use it, and containing its data.

Non-Technical Tips

Things you can do to minimize your data footprint and up your OPSEC game without needing to know much about how computers work

(but still using them to get your work done)

Non-Technical Tips

Threat Modeling

Non-Technical Tips

Threat Modeling

A process of figuring out what is worth protecting, assessing potential risks, and figuring out the capabilities of your adversaries.

Think through different scenarios, consider the tradeoff between likelihood and impact.

- Who are the threats?
- How might they impact your privacy and security?
- How likely will that happen?
- How would they do it?

Non-Technical Tips

Threat Modeling

Setting OPSEC standards with your community

Non-Technical Tips

Threat Modeling

Coming together to set rules, boundaries, approved procedures, technologies, and plans of action in case of incidents.

Setting OPSEC standards with your community

- Push a culture of consent when it comes to sharing data
- Make rules for yourself about what data you can't share with the group
- Think of it like social firewalls - AKA a system of deny/allow lists

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

Setting OPSEC standards with your community

Non-Technical Tips

Threat Modeling

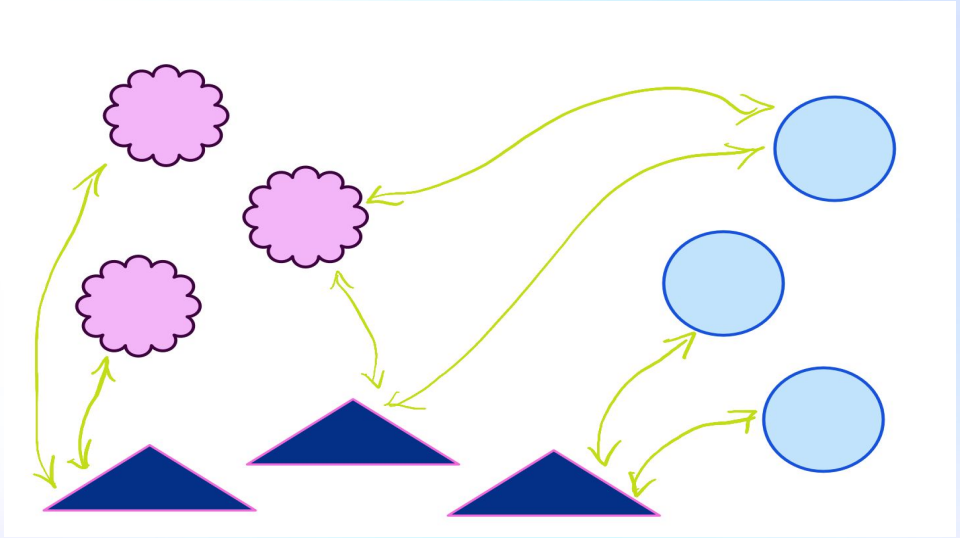
Setting OPSEC standards with your community

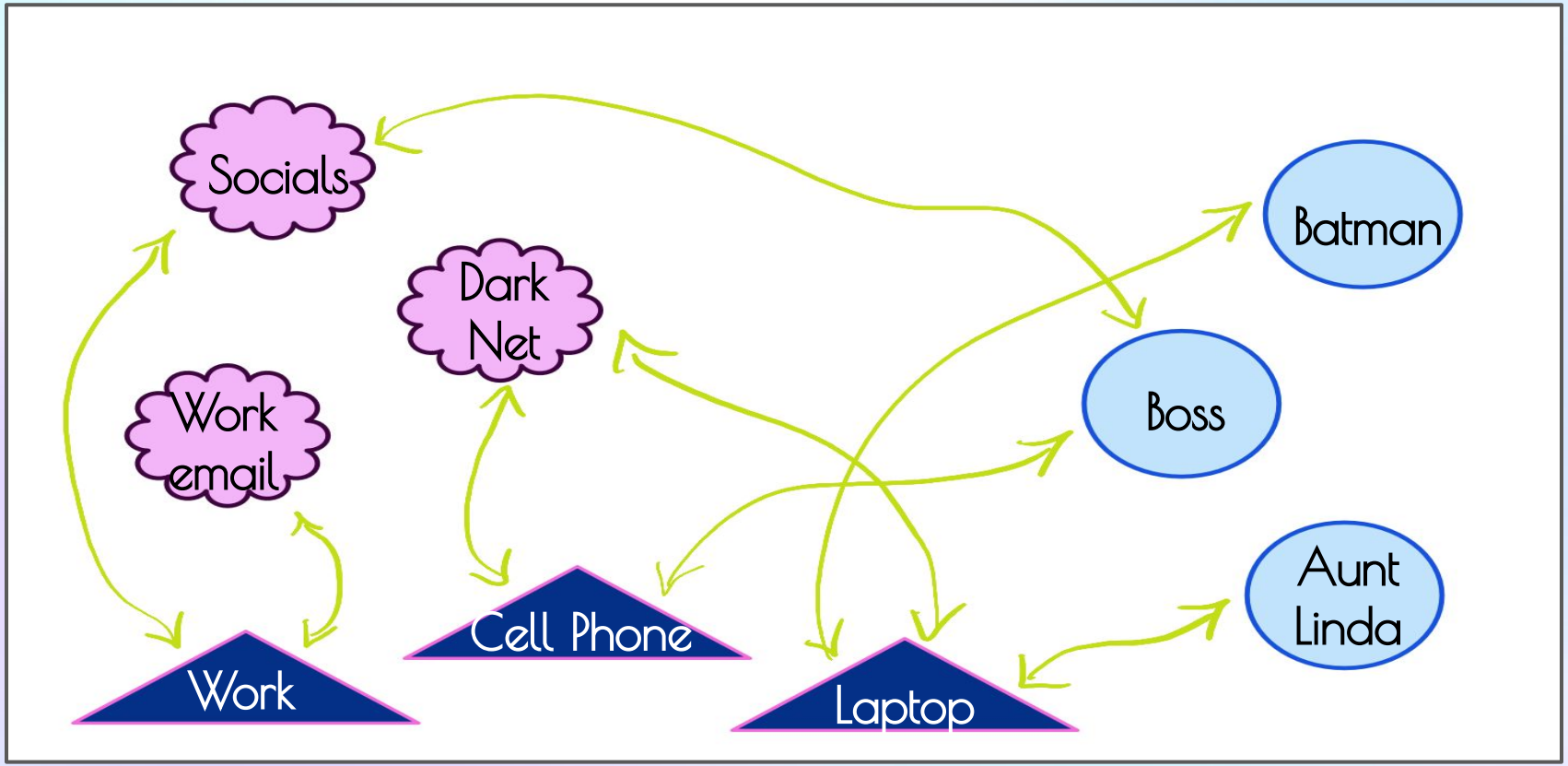
Mapping Your Digital Footprint

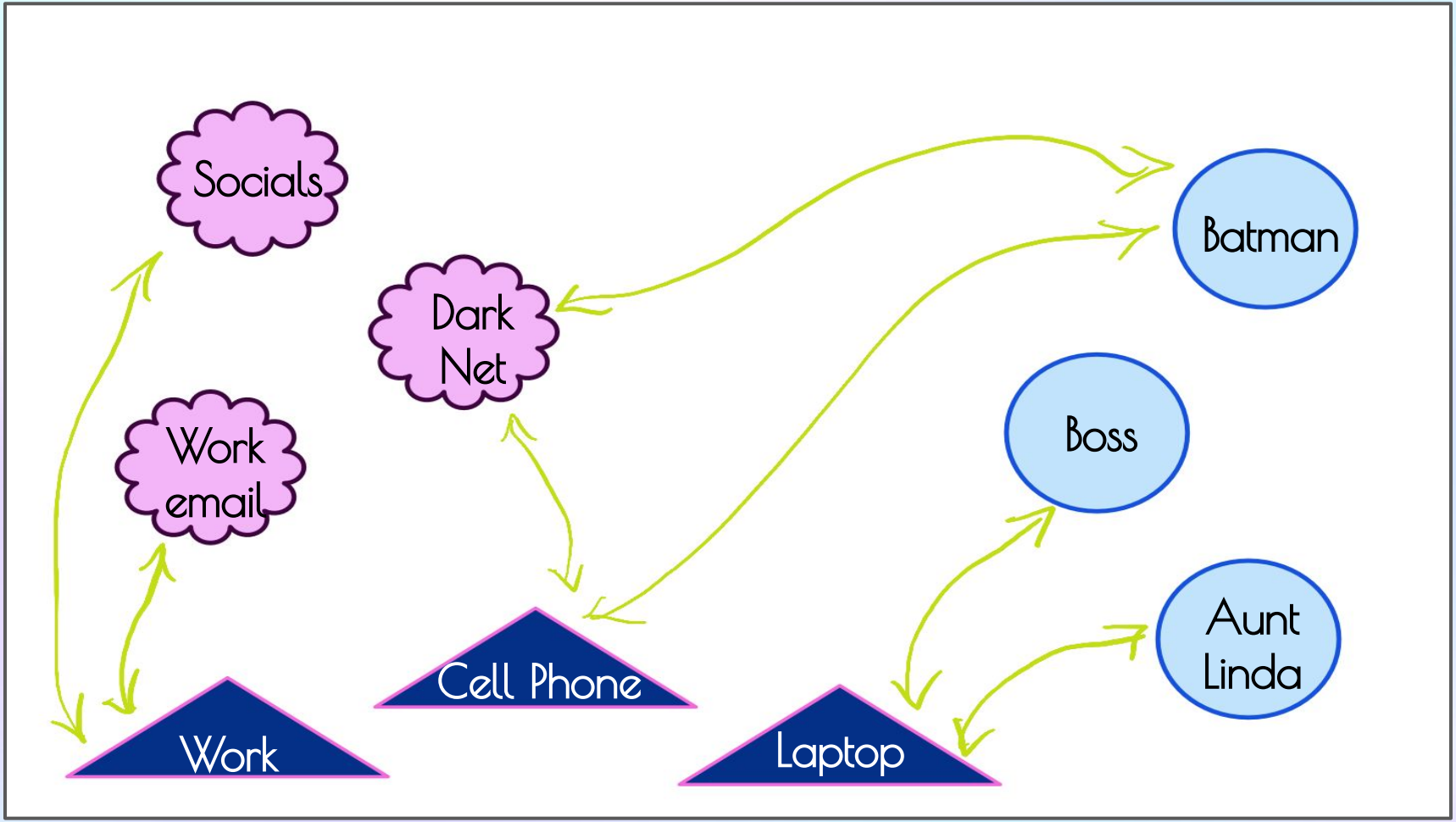
A way to visualize the ways in which your data is made and distributed.

It's done by drawing a map of the typical accounts and apps you use, the computers and devices you use to access them, and the groups of people you interact with.

Mapping Your Digital Footprint




Socials
Dark Net
Work email
Work
Cell Phone
Laptop
Batman
Boss
Aunt Linda


Socials
Dark Net
Work email
Batman
Boss
Aunt Linda
Cell Phone
Work
Laptop

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

Setting OPSEC standards with your community

Steganography

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

Setting OPSEC standards with your community

Steganography

AKA hiding information in plain sight.

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

Setting OPSEC standards with your community

Steganography

- An easy example is "asking for a friend." Gets your information across while dodging culpability
- Consciously make coded language with your allies. Avoid thinking of it as slang, but more inconspicuous code words
- (there is also a branch of technologies that do this by hiding text in images, in metadata, etc)

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

OPSEC Checklist

Setting OPSEC standards with your community

Steganography

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

OPSEC Checklist

A special list of things to do, in order, when you need extra privacy and security.

Setting OPSEC standards with your community

Steganography

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

Setting OPSEC standards with your community

OPSEC Checklist

1. Turn on VPN
2. Start virtual machine
3. Go online with Tor
4. Log into secure accounts
5. Do business & download data onto external disk
6. Log out and shut down each in order

Steganography

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

OPSEC Checklist

Setting OPSEC standards with your community

Turn it off/Leave it at home

Steganography

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

OPSEC Checklist

Setting OPSEC standards with your community

A network, social ones included, is only as strong as any connected node, and how they relate to each other.

Steganography

Improving your own privacy and security makes it easier for others to think about theirs, and vice versa. It improves the overall privacy and security of a community.

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

OPSEC Checklist

Setting OPSEC standards with your community

Turn it off/Leave it at home

Steganography

Non-Technical Tips

Threat Modeling

Mapping Your Digital Footprint

OPSEC Checklist

Setting OPSEC standards with your community

Turn it off/Leave it at home

Steganography

“When a woman thinks alone, she thinks evil.”

- Seneca, quoted in Malleus Maleficarum

Technical Tips

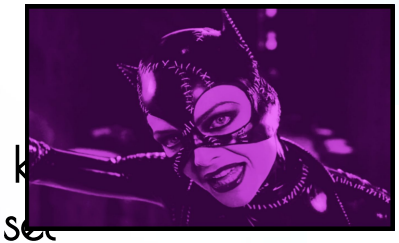
Passwords

Always make them long, unique, random, and difficult to guess.

Use a password manager to keep track of them. You can even set one up for an organization to share "vaults", generate passwords for you, sync across devices, and more

Passwords

Always make them long, unique, random, and difficult to guess.



Use a password manager to k
track of them. You can even se
one up for an organization to
share "vaults", generate passwords
for you, sync across devices, and
more

bitwarden

1Password

LastPass •••|

Registering Sensitive Accounts

- Unique, random login credentials
- Follow your OPSEC checklist
- Use throwaway or especially private email services
- Use separate phone numbers
- Connect to service while on VPN or on public network

Registering Sensitive Accounts

Disposable Email Services:

Registering Sensitive Accounts

Disposable Email Services:

GUERRILLAMAIL.COM
Guerrilla Mail - Disposable Temporary E-Mail Address

10 MINUTE mail

Secondary Phone Numbers:

Hushed

Burner

Google Voice

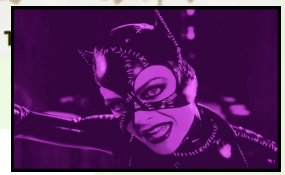
twilio

Registering Sensitive Accounts

Disposable Email Services:

GUERRILLAMAIL.COM

Guerrilla Mail - Disposable T



10MINUTE mail

Secondary Phone Numbers:

Hushed

Burner

Google Voice

twilio

A Bit About Mobile Privacy & Security

Hardening Basic Phone		Burner Phone	
Pros	Cons	Pros	Cons
Free / low $	High chance of data pollution across digital "selves"	Best method of compartmentalization	More $
Easy device management	IEMI (device address) always pinpoints back to you	Easiest method to mentally deal with	Requires strict OPSEC
No concern over cross device data pollution	Law enforcement seizure would mean they get everything	Plausible deniability if stopped by LE	Tech skills needed
Ease of use, lower technical proficiency required	Difficulty keeping digital selves separate on just one device	Best OPSEC possible without compromising social life	May invite suspicion

Hardening Basic Phone		Burner Phone	
Pros	Cons	Pros	Cons
Free / low $	High chance of data pollution across digital "selves"	Best method of compartmentalization	More $
Easy device management	IEMI (device address) always pinpoints back to you	Easiest method to mentally deal with	Requires strict OPSEC
No concern over cross device data pollution	Law enforcement seizure would mean they get everything	Plausible deniability if stopped by LE	Tech skills needed
Ease of use, lower technical proficiency required	Difficulty keeping digital selves separate on just one device	Best OPSEC possible without compromising social life	May invite suspicion

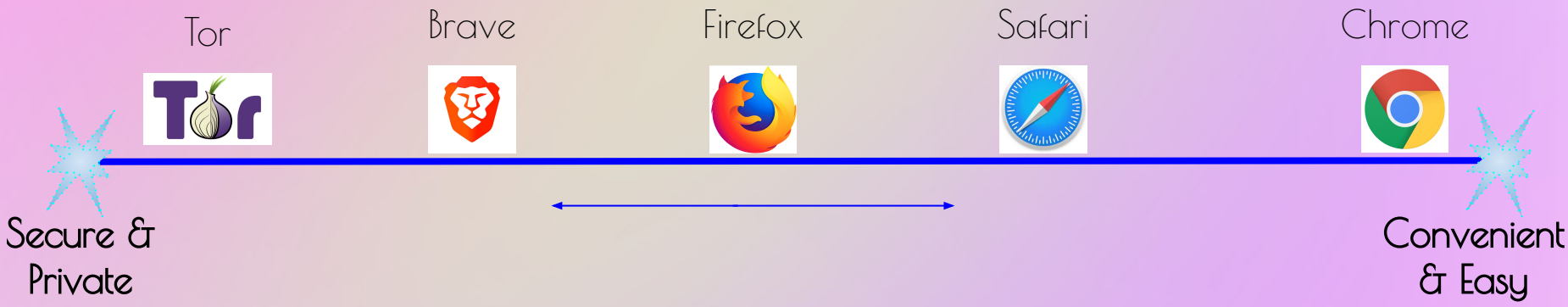
Hardening Basic Phone

- Turn Ad-ID off
  - Android: Settings > Privacy > Ads: "Delete Ad ID"
  - iOS: Settings > Privacy > Tracking: "Allow Apps to Request to Track"
- Enable long, difficult to guess PIN to unlock
  - Turn off biometric unlocking for at least when traveling to/from sensitive locations/activities
- Install app for secondary phone number
  - Google Voice = free. Burner = $ but good service. Hushed = $.
  - Do not mistake these services for private E2EE messagers
- Install private E2EE messaging app.
  - Signal, Keybase
- Carefully review apps permissions
  - Especially location services. "Allow while using" at bare minimum.

Burner Phone

- Get device
  - Buy new or used, in cash, mask on
  - Do not connect to home network, do not have on when with regular phone
  - Do not give name or any PII while purchasing. You never need to!
  - Pixel models 3-6 are most supported for privacy ROMs
  - Buy prepaid SIM card either same time or somewhere else, also in cash
- Install Graphene OS or CalyxOS
  - Both relatively easy to install
  - Graphene = most secure. Calyx = more usable for day to day use.
- Create accounts for needed services for this device only
  - Best OPSEC while doing so
- Never connect to home wifi, avoid networks & locations you commonly associate your other device with
- Enable PIN scrambling

Choosing Browsers (for mobile & desktop)



Browsers are free. Why not use multiple?

Whatever you choose, look into its privacy settings and raise the bar on them from their "out of box" state

Choosing Browsers (for mobile & desktop)

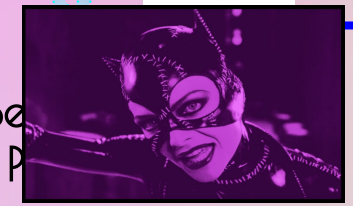
Tor

Brave

Firefox

Safari

Chrome



Se
P

Convenient
& Easy

Browsers are free. Why not use multiple?

Whatever you choose, look into its privacy settings and raise the bar on them from their "out of box" state

Secure Messaging

Choose end-to-end encrypted options for messaging with other people. For further compartmentalization, register them with secondary phone numbers

Signal is a good option for phone use, for both 1 on 1 and group settings

TutaNota & Protonmail are easy to use good options for email

Browser Extensions

Tracker Blockers

Privacy Badger

uBlock Origin

DuckDuckGo

Password Managers

1Password

bitwarden

Other

NoScript

Click&Clean

https://www.hotcleaner.com

Browser Extensions

Tracker Blockers

Privacy Badger

uBlock Origin

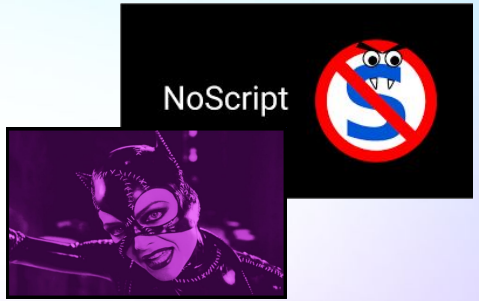
DuckDuckGo

Password Managers

1Password

bitwarden

Other



Click&Clean

https://www.hotcleaner.com

Payment Processing & Finances

- Use linguistic steganography when appropriate
  - Adds plausible deniability on more "surface" options
- Privacy.com credit card for compartmentalizing payments
  - Looks and behaves just like any credit/debit card
  - Allows "false" names
  - Does tie to bank accounts
- Monero cryptocurrency is extremely private and virtually untraceable
  - Means you have to engage with cryptocurrencies, ick
- Cash is almost always anonymous

VPNs

What they do: Routes your internet traffic through another computer. Hides your IP address and can make you appear somewhere else

What they don't do: Stop spies, scams, encrypt everything you do, or block internet trackers.

Be mindful that if you choose a commercial VPN option, you are entrusting that company with you internet traffic data.

You may look into setting up your own. It has the potential to be more private and secure than any commercial option, but requires the tech skill, time and money to do it.

NordVPN

MULLVAD

IVPN

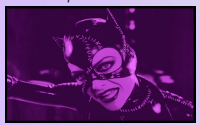
VPNs

What they do: Routes your internet traffic through another computer. Hides your IP address and can make you appear somewhere else

What they don't do: Stop spies, scams, encrypt everything you do, or block internet trackers.

Be mindful that if you choose a commercial VPN option, you are entrusting that company with you internet traffic data.

You may look into setting up your own. It has the potential to be more private and secure than any commercial option, but requires the tech skill, time and money to do it.



NordVPN

MULLVAD

IVPN

Virtual Machines

A way to "virtualize" a whole operating system on top of your current one.

Great for keeping a "sandboxed environment" with all your apps, settings, and sensitive things in one place, separate from your main system.

These machines are often highly volatile. Taking regular "snapshots" of their working states, and backing up data from them regularly is vital.

Virtual Machines

VirtualBox is a free option, but a bit more hands-on configuration

VMWare is a paid option for Windows.

Parallels is a paid option for MacOS

Choose an operating system that is lightweight and built for privacy and security in mind.

Linux distributions like Ubuntu and Mint are easy and more familiar to use out of the box.

Arch is highly configurable but requires tech savvy.

Operating Systems

If you have the means to own a separate device especially designated for Catwoman behaviors, these are two recommended operating systems to consider, especially designed for extremely good OPSEC.

The queen of compartmentalization! Difficult to learn, but worth the effort.

Inconvenient for persistent storage, but excellent for high sensitive operations that need privacy

Operating Systems

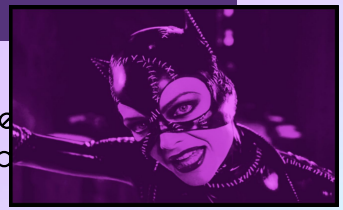
If you have the means to own a separate device especially designated for Catwoman behaviors, these are two recommended operating systems to consider, especially designed for extremely good OPSEC.

QUBES OS
A REASONABLY SECURE OPERATING SYSTEM

The queen of compartmentalization! Difficult to learn, but worth the effort.

Tails
theamnesicincognitolivesystem

Inconvenient for storage, but exce sensitive operatio privacy



“Human security is the idea of helping each person’s vital capacities to flourish, across all the dimensions of their existence.”

- The Security Principle, Frédéric Gros