TACTICAL TECH

“The Mindset”

Fundamental approaches to technology and digital safety for investigations

Topics Covered

- Risk Assessment
- Security Basics
- How to choose tools
- Internet Tools
- How the Internet Works
- VPNs

Why bother?

"If you gaze for long into an abyss, **the abyss gazes also into you**."

- Nietzsche

"Whoever fights monsters should see to it that in the process **he does not become a monster**."

- Nietzsche

"Whoever investigates to uncover, should see to it that in the process **they do not get uncovered**."

- Me

Risk Assessment

Your Digital Safety

- is about the function you perform and the context in which the function is performed
- cannot be approached in isolation from overall safety
- cannot be approached in isolation from that of other people you communicate with

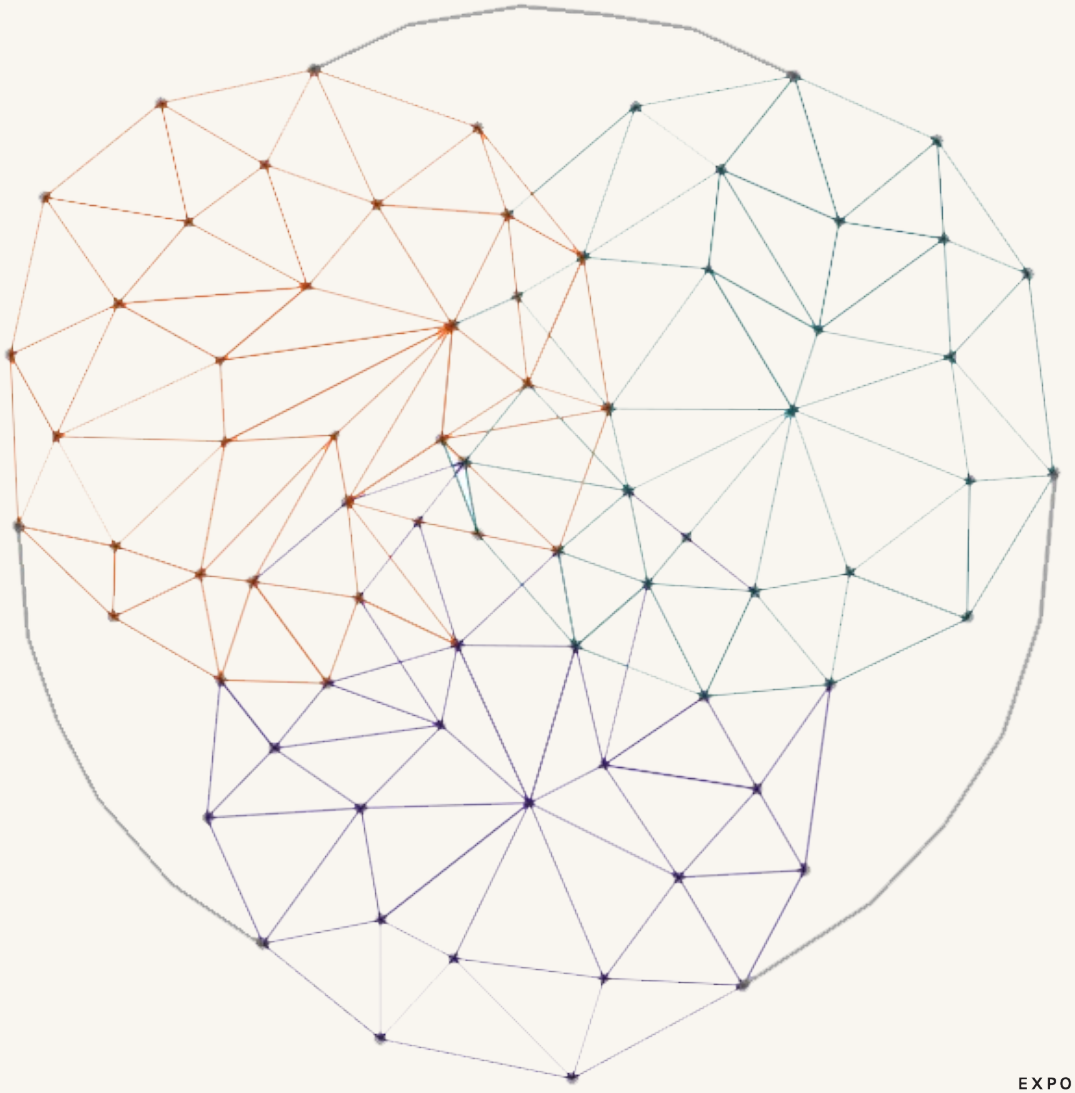
Holistic Security

△ **Physical Security**
Threats to our physical integrity. Threats to our homes, buildings, vehicles.

△ **Psycho-social Security**
Threats to our psychological wellbeing.

△ **Digital Security**
Threats to our information, comunication and equipment.

— Holistic security analysis, strategies and tactics.



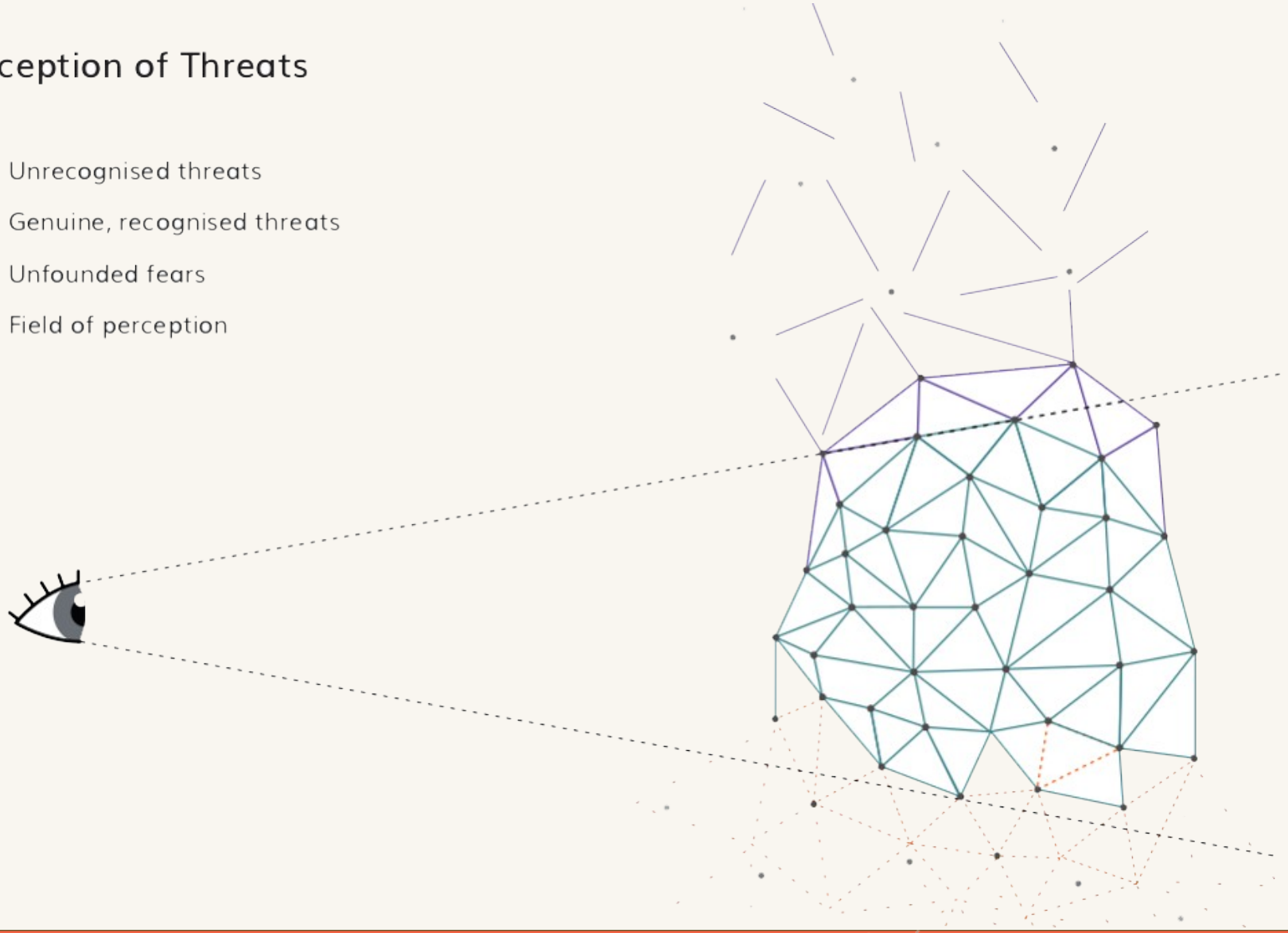
Risk

- What can happen?
- How likely is it?
- What will the consequences be?

Risk = **Likelihood x Consequence**

Perception of Threats

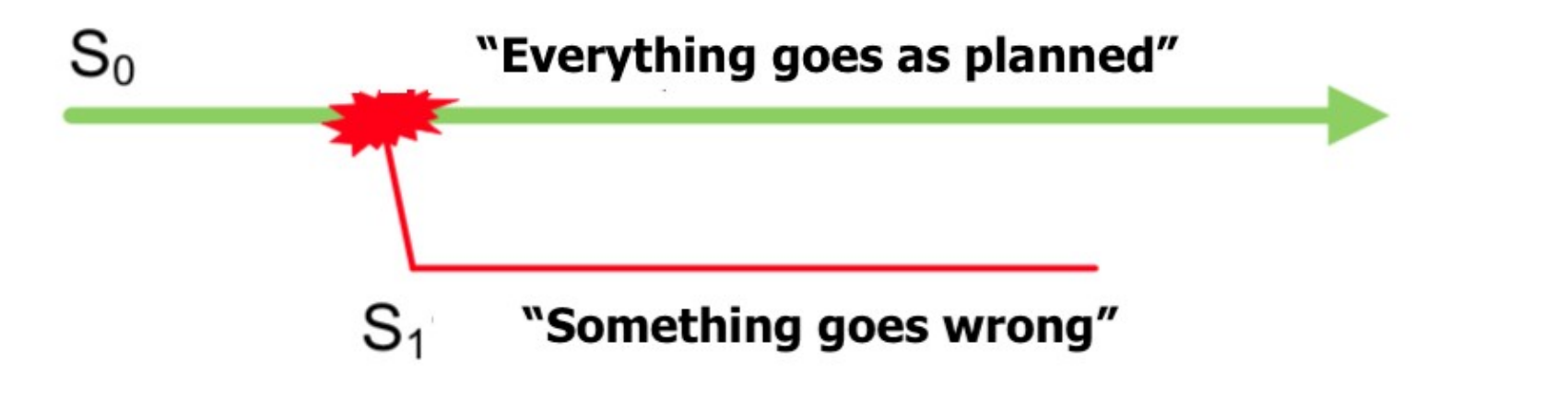
- Unrecognised threats
- Genuine, recognised threats
- Unfounded fears
- Field of perception



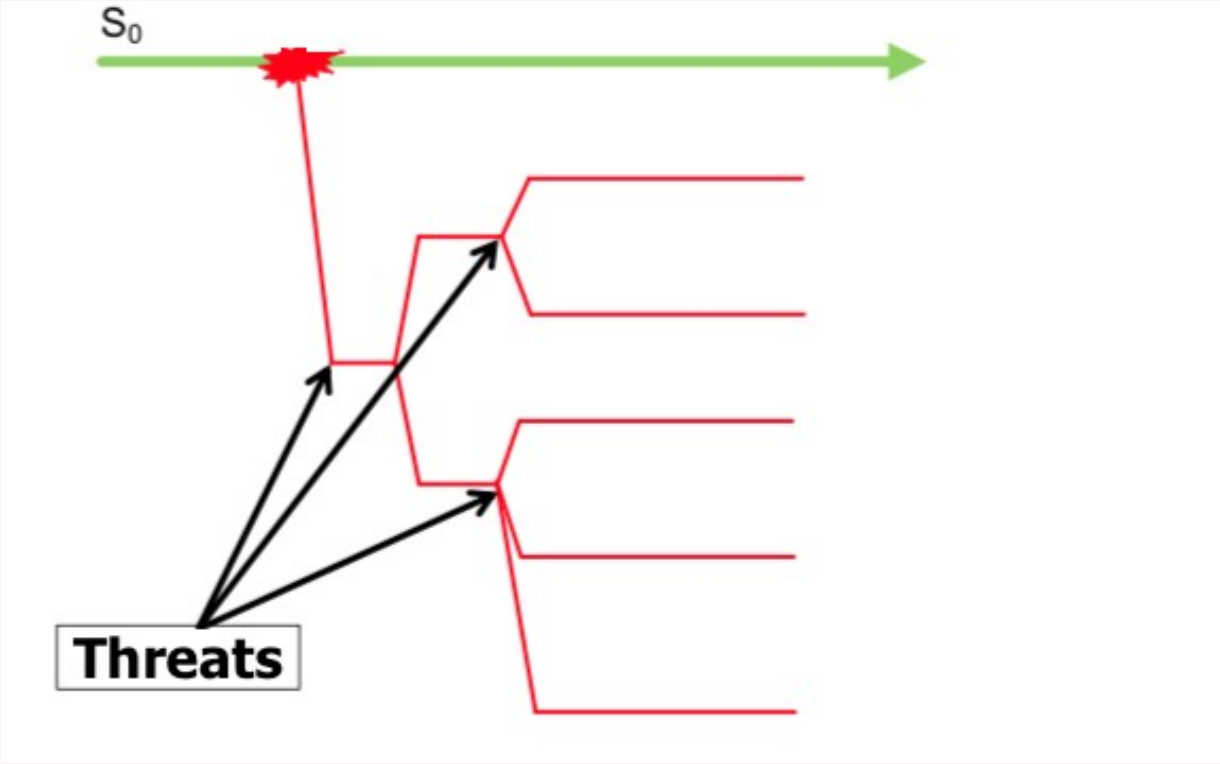
Risk Assessment

- Functions you perform
- Methods and tools you use to perform the functions
- Data you collect/ safeguard/ communicate
- Where do you have vulnerabilities? (software/ people/ data storage/ data transfer)
- Context(s) where you perform those functions
  - Adversaries
  - Capabilities of adversaries
  - Consequences

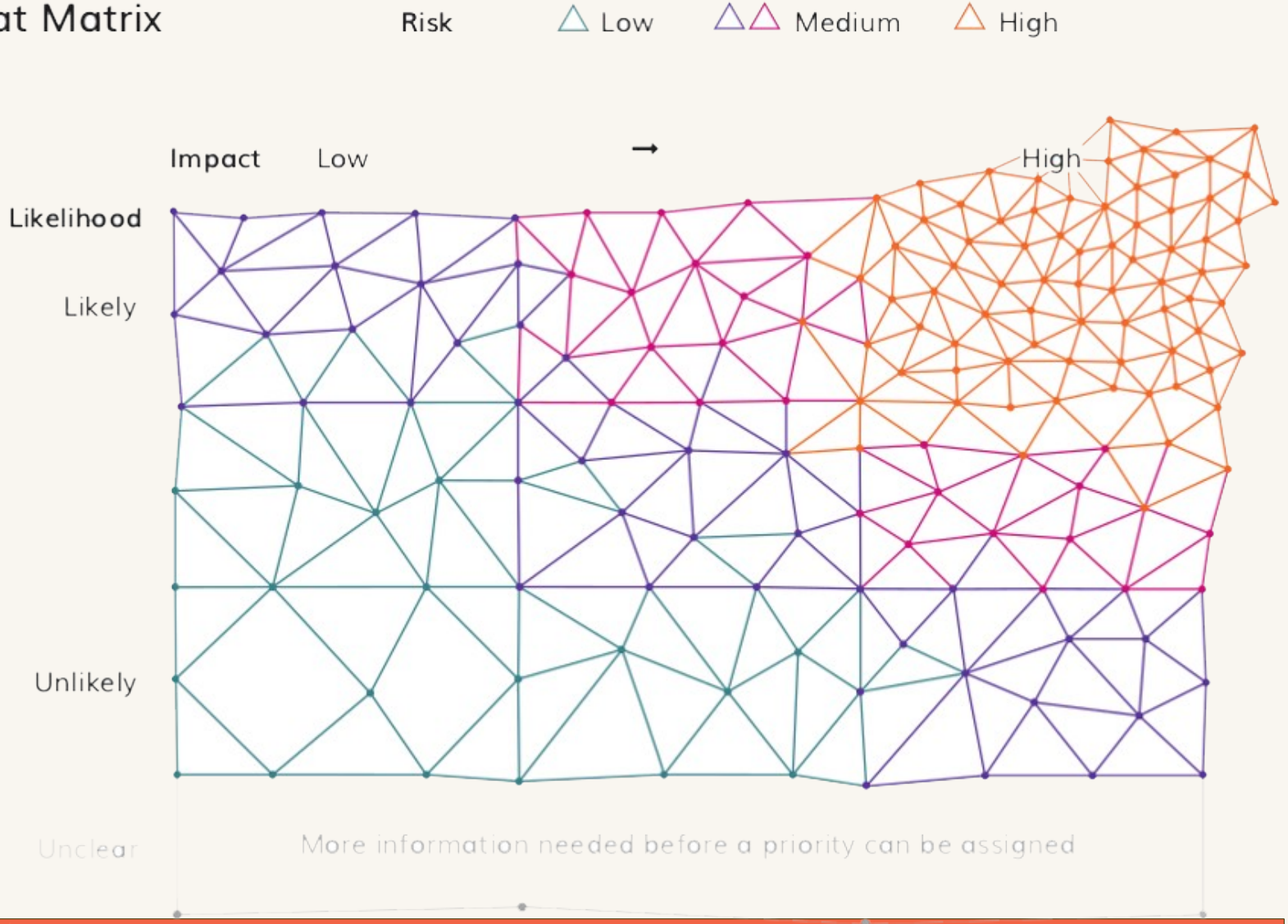
Something always goes wrong



Plan or improvise?



Threat Matrix



LIKELIHOOD	IMPACT				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	Moderate (5)	High (10)	High (15)	Catastrophic (20)	Catastrophic (25)
Likely (4)	Moderate (4)	Moderate (8)	High (12)	Catastrophic (16)	Catastrophic (20)
Possible (3)	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
Unlikely (2)	Low (2)	Moderate (4)	Moderate (6)	Moderate (8)	High (10)
Rare (1)	Low (1)	Low (2)	Low (3)	Moderate (4)	Moderate (5)

Action Mechanisms:

Low (1-3)	Accept Risk
Moderate (4-9)	Continuous Risk Monitoring
High (10-15)	Mitigation Measures
Catastrophic (16-25)	Mitigation Measures and immediate corrective action plans

Security Basics

What devices do you carry / use for research?

Mobile phones

Tablets

Laptops

E-readers

Wearables

External storage

...

What's in a device? .

- Personal photos / Work related photos
- Personal correspondence / Work correspondence
- Legal / Bank / Medical documents
- Personal preferences
- Online profiles
- Search history
- Travel history
- Location history
- Contacts, relationships
- ....

Most common actions:

- Online research (desk-top research)
- Offline research
- Communication: mail, phone, online, offline
- Storing information and data on devices
- Transferring information and data, remote collaboration
- Travel: locally and across borders
- Dealing with sources, vulnerable subjects

Digital Safety Tools Help Protect...

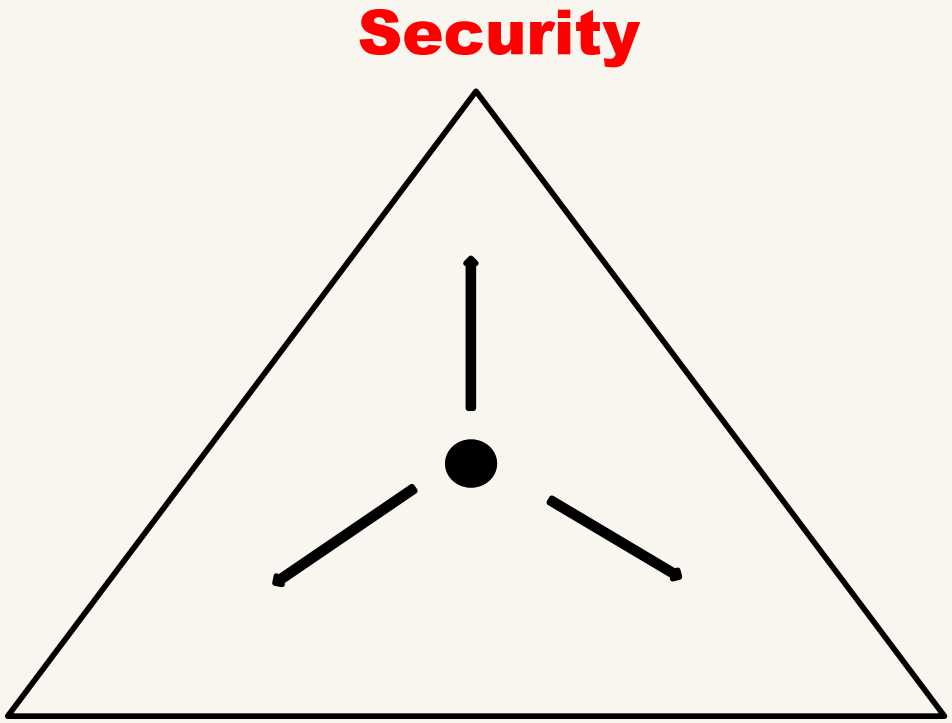
- Device and Data
- Communications
- Network Connections
- Online Accounts

But safety is not just **tools** ...

- What you choose to share
- How you communicate
- What you click (phishing)
- What services you choose

Humans are the weakest link

Digital Safety Trade-off



Should I always go for most secure tool?

Should I always go for most secure tool?

NO

Should I always go for most secure tool?

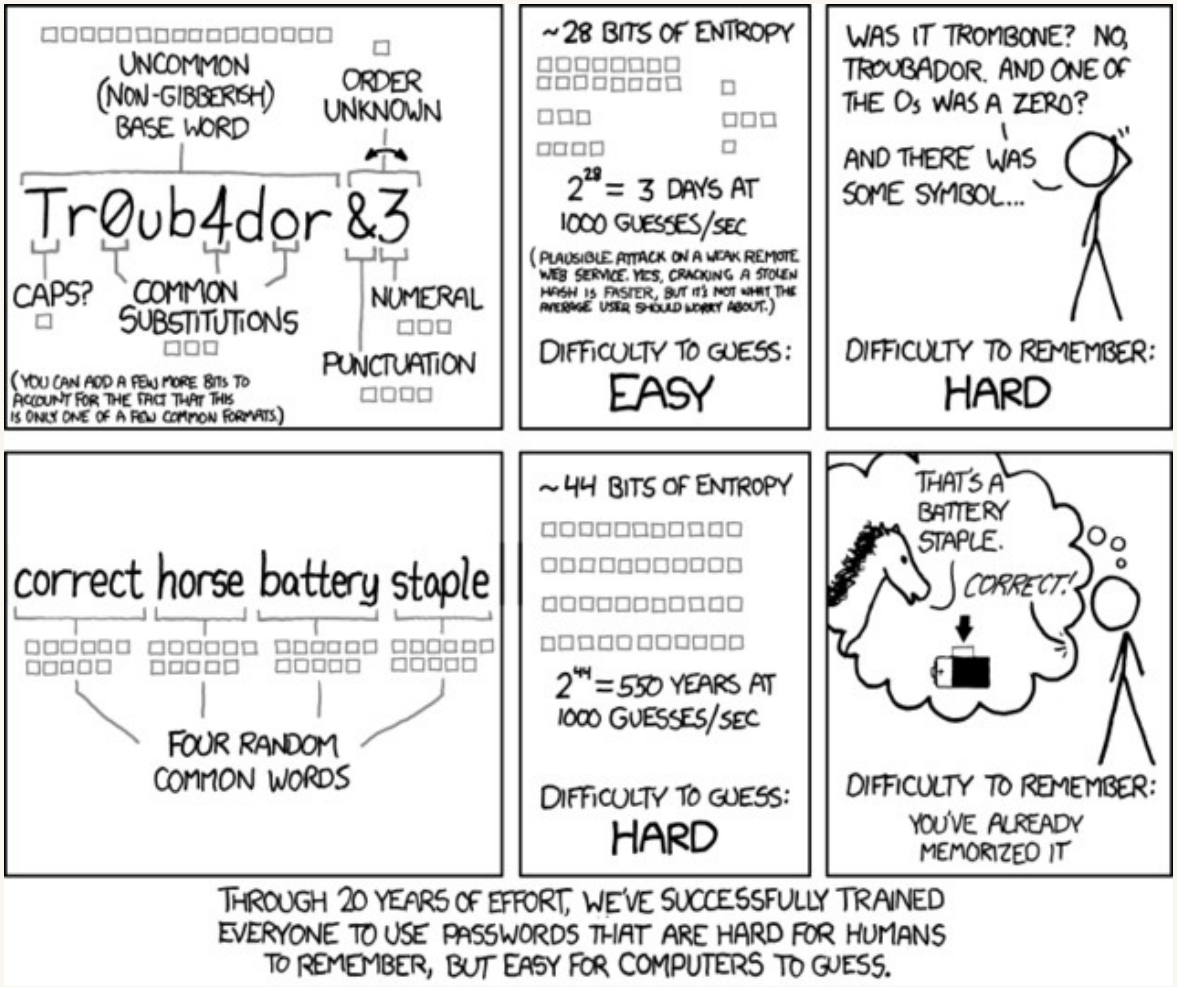
NO

- Secure tools don’t mean security
- Some security tools draw more attention (depending on country)
- Harder to adopt with no added value depending on context

Security Basics

- Long passwords(phrases) / 2FA
- Safeguarding passwords
- Backup data
- Encrypt data
- End to end encryption is important
- Be aware of who has access to your data
- Assess tools you use
- Your practices can cause more risks than the tools you use

Passphrase vs. Password



https://howsecureismypassword.net

do NOT enter your real passwords!

Creating and maintaining secure passphrases

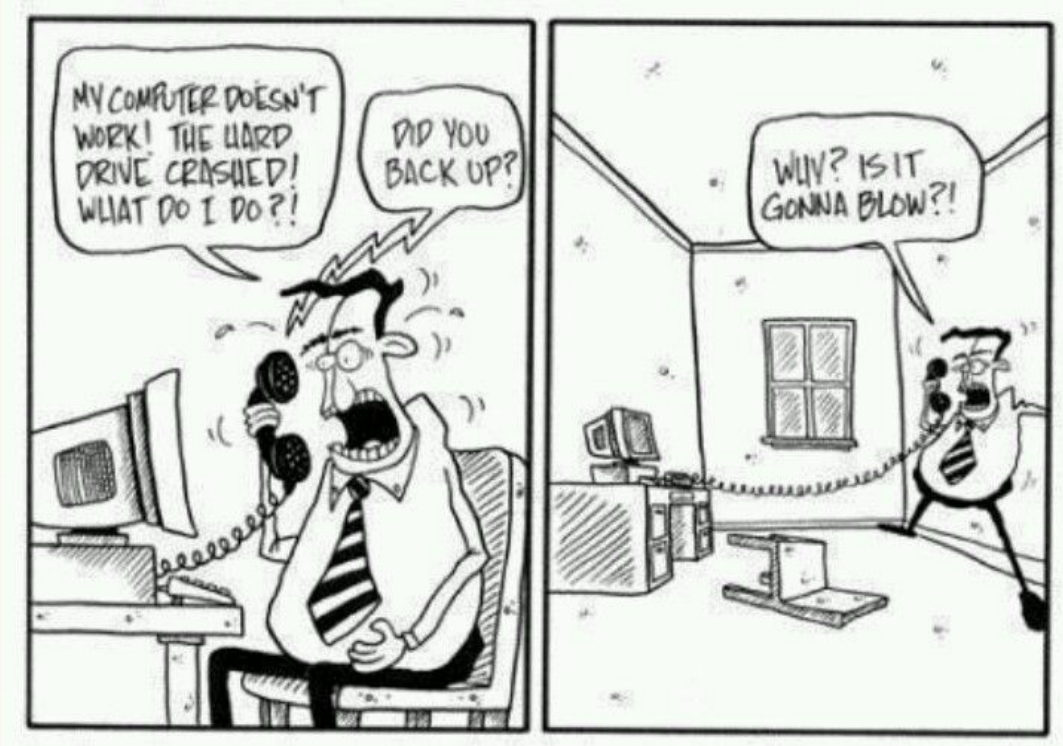
- Make it **long** and random – passphrase (hellohowareyou vs. Druggedroseriotingabsolutelycakes)
- **Not personally** identifiable (so no birth date, address, names of your puppies/kids/lovers/haters ..)
- Keep it **secret**
- Make it **practical** to remember
- **Unique** – to avoid major damage if it gets exposed
- **Keep it fresh** – change it every now and then

Password Management

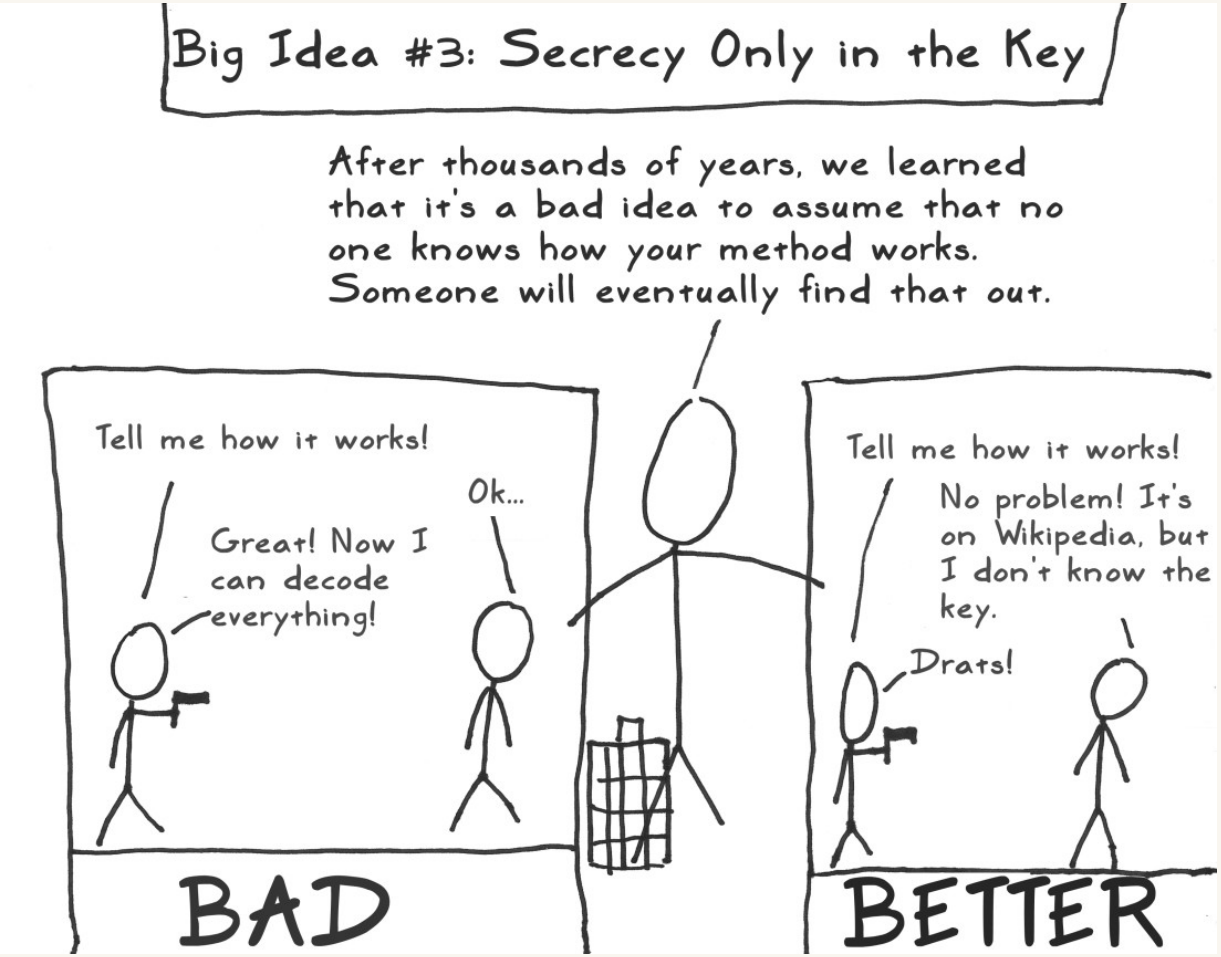
- Strong passwords
- Don’t repeat the same password for different sites and emails or devices
- Don’t forget the master password
- KeepassXC (offline), Firefox Lockwise (online)

Further reading: https://ssd.eff.org/en/module/creating-strong-passwords

Data Security – Backup and Encryption



Encrypt



Kerckhoffs's Principle

- A system should be secure even if everything about the system, except the key, is public knowledge
- Assume "the enemy knows the system"

Devices and Data

- Use Full Disk Encryption
- Use tools like Bitlocker (Windows), FileVault (Mac), dm-crypt (Linux)
- Use VeraCrypt, Cryptomater file containers for data
- Backup your data in case of loss of devices (Duplicati, Clonezilla, Spider Oak, NextCloud, Tresorit, Google*...and hard drives)

Cryptomator

VeraCrypt

Sending Data

- **Send.Tresorit** – End to end file sharing service
- **OnionShare** – Peer to peer sharing using Tor

The Best Kept Secret

How to Choose Tools

Presumption of Guilt

Instead of looking for signs of something **wrong** with software, search for **what's right with software.**

How secure is a tool?

- Open source
- End to end encrypted
- Does not store data unnecessarily
- Does not leak data
- Does not share data

Open Source

Q: Doesn't hiding source code automatically make software more secure?

No. Indeed, vulnerability databases such as CVE make it clear that merely hiding source code does not counter attacks:

Hiding source code *does* inhibit the ability of third parties to respond to vulnerabilities (because changing software is more difficult without the source code), but this is obviously *not* a security advantage. In general, "Security by Obscurity" is widely denigrated.

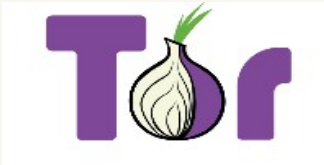
https://dodcio.defense.gov/Open-Source-Software-FAQ/

How we choose tools

1. Open source
2. Trusted (audited)
3. Mature (stable, active user community and responsive developer community)
4. User-friendly
5. Multi-language with localisation support (you can find your own language or localise it)
6. Multi-platform (Mac, Windows, Linux, Android)
7. Have available documentation

Internet Tools

Network



- Tor
- VPN
- Trusted Apps

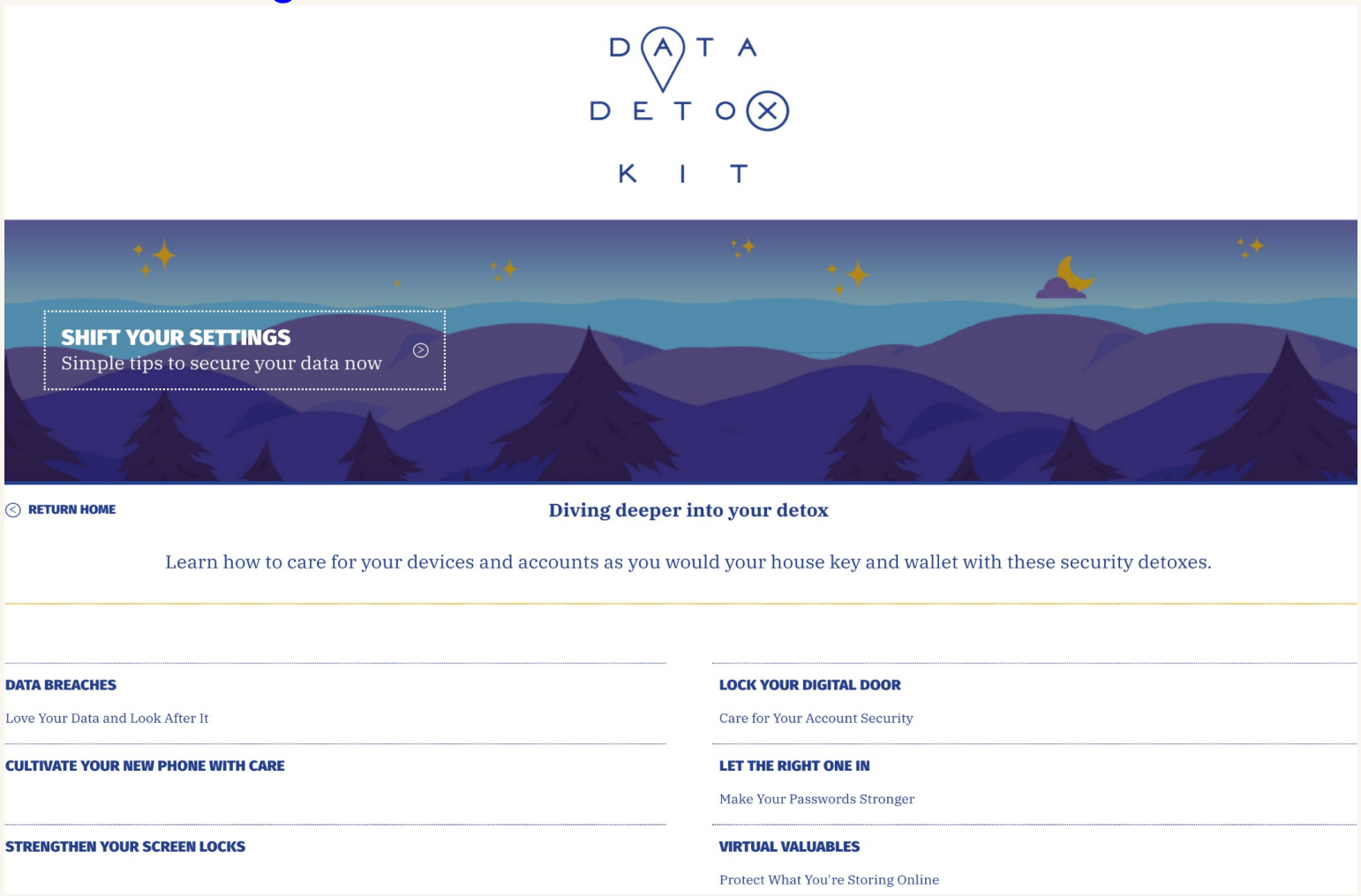
Communication

- Trusted Apps
- Encrypted messaging apps (Signal)
- PGP
- VPN/Tor

Online Accounts

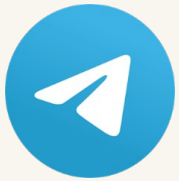
- Secure your credentials
- Password Manager
- Not sharing extra information
- Two Factor Authentication
- Protect your data from online platforms
- Incognito mode, clear browser history
- Privacy Badger, HTTPS

Simple steps to clean up your devices and online behavior:
https://datadetoxkit.org/



Communication metadata

- Trusted Apps
- Encrypted messaging apps (Wire, Signal, WhatsApp)
- PGP



! Encrypted communication vs. legal requirements

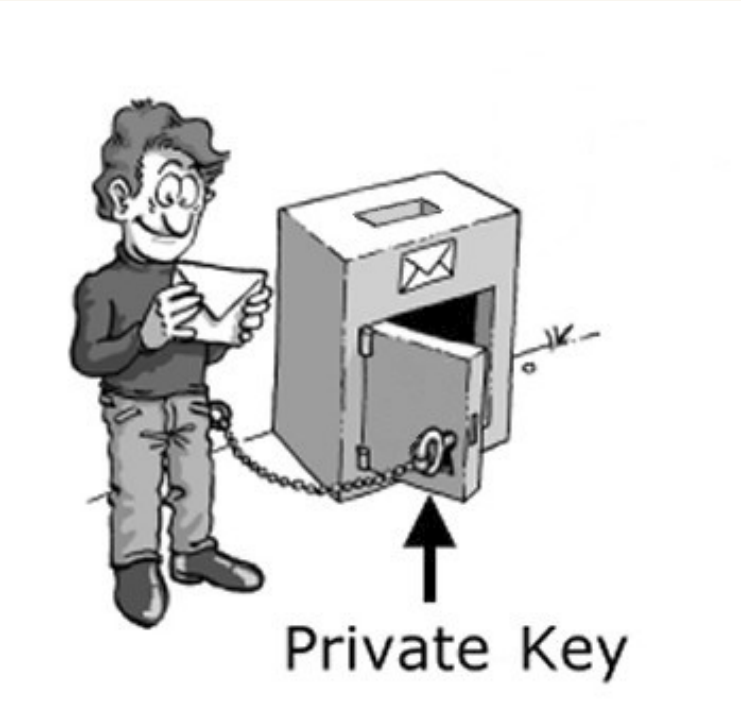
How to use PGP?

- Mailvelope
- Thunderbird
- Kleopatra
- GPG

GnuPG

PGP

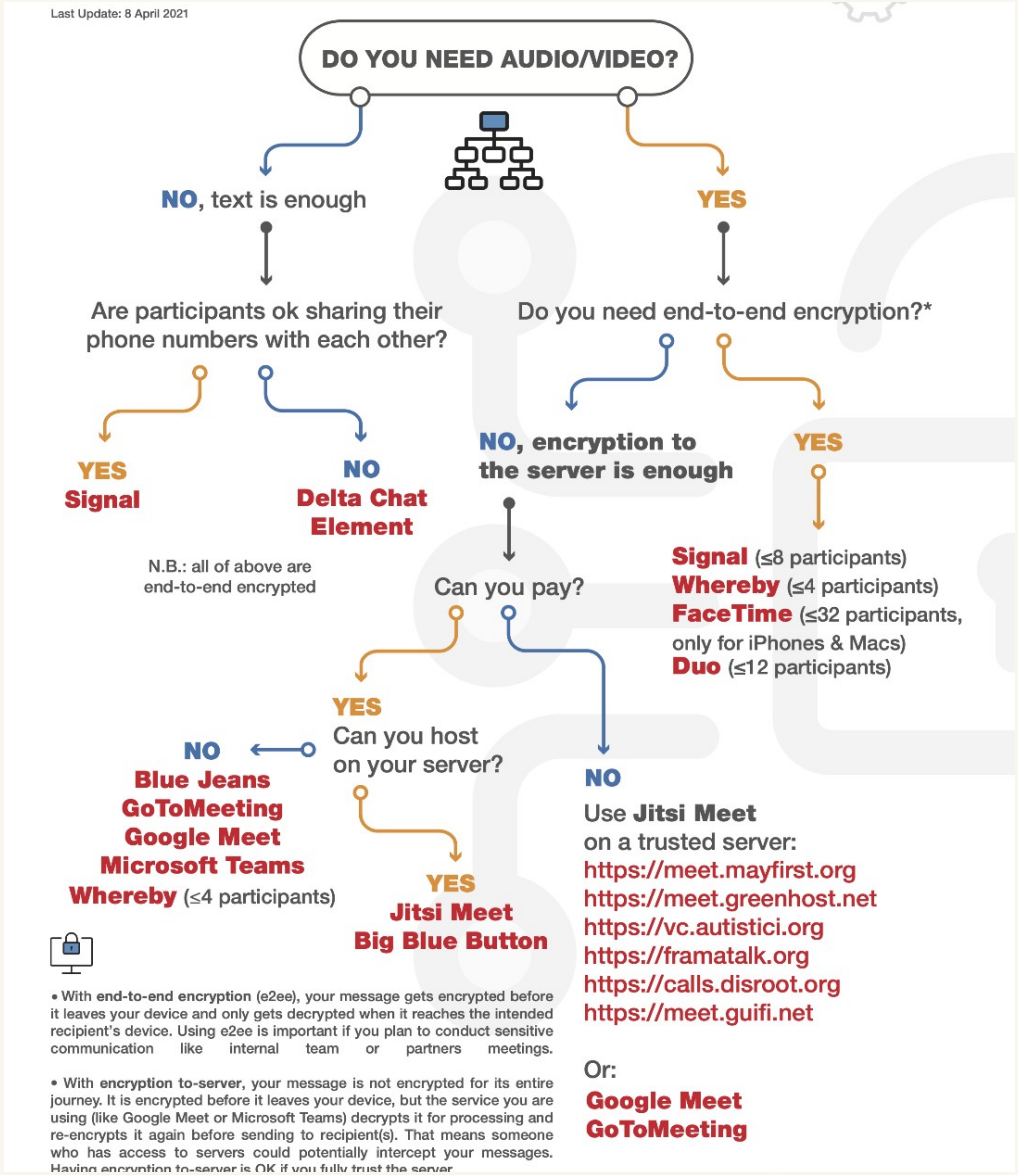
Public Key – Private Key



https://myshadow.org/resources/the-key-concept

https://vimeo.com/134932244

SECURE GROUP CHAT AND CONFERENCING TOOLS



Source and details:
https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools

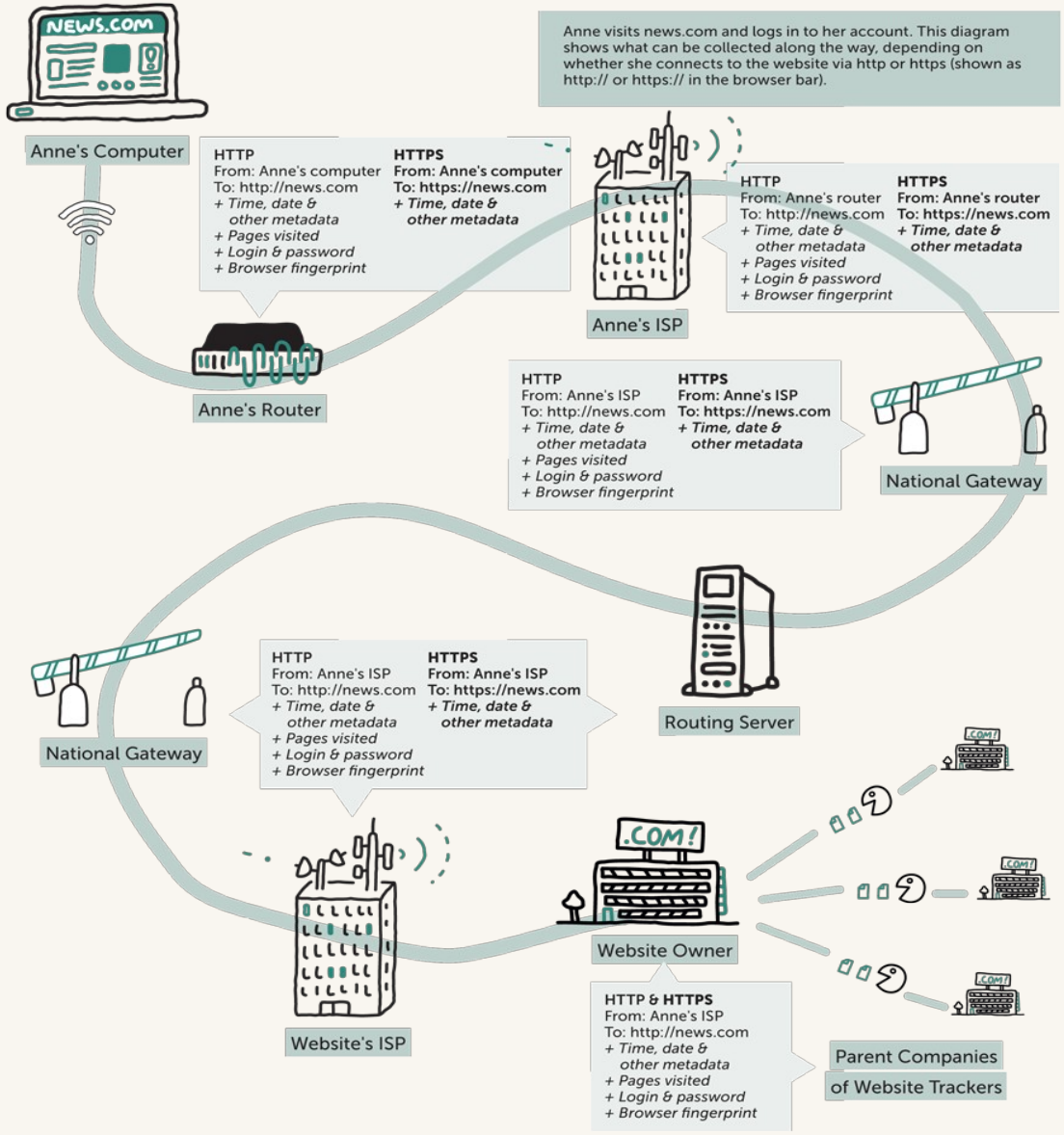
PROTECT ONE EMPOWER A THOUSAND

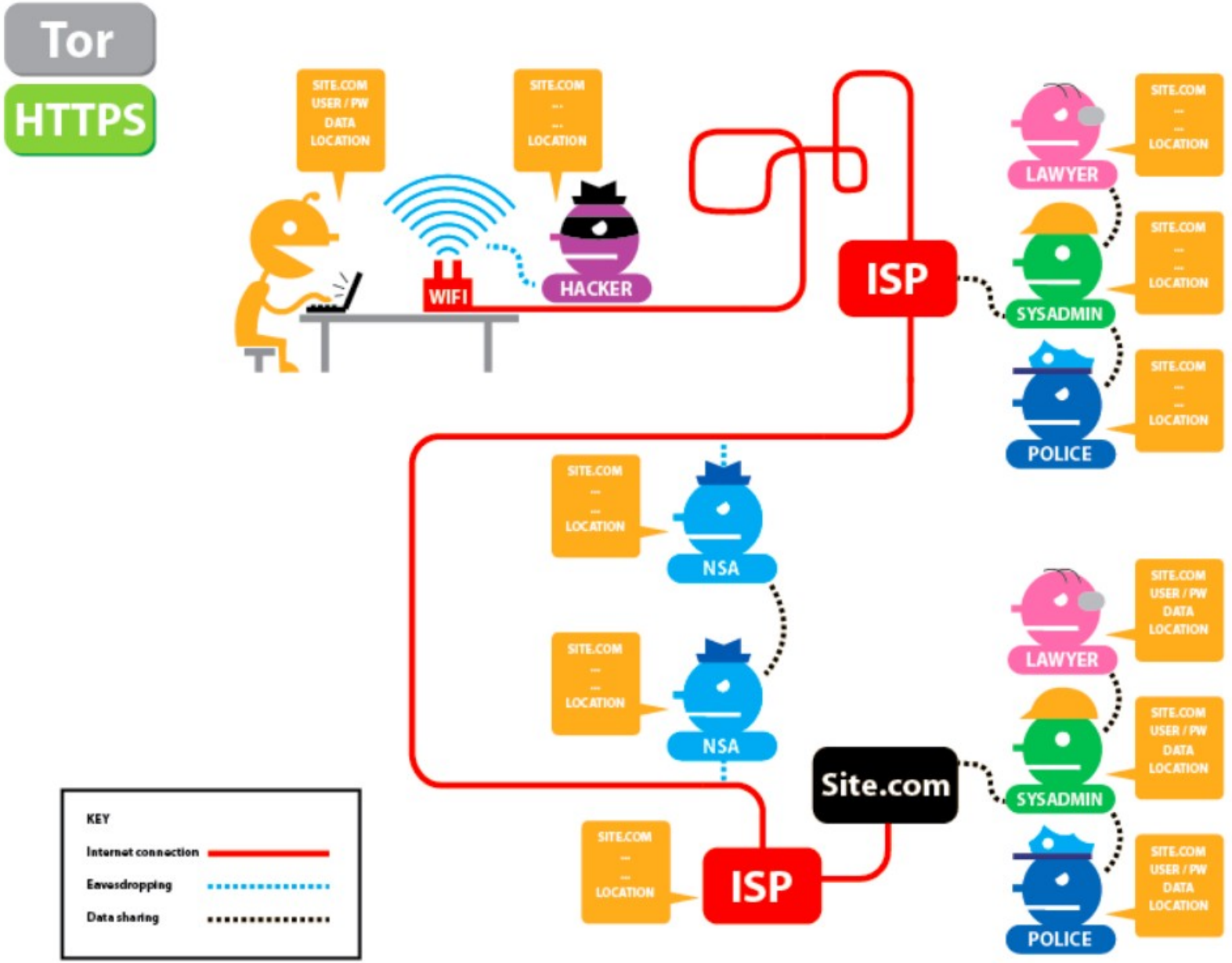
FRONT LINE DEFENDERS
www.frontlinedefenders.org

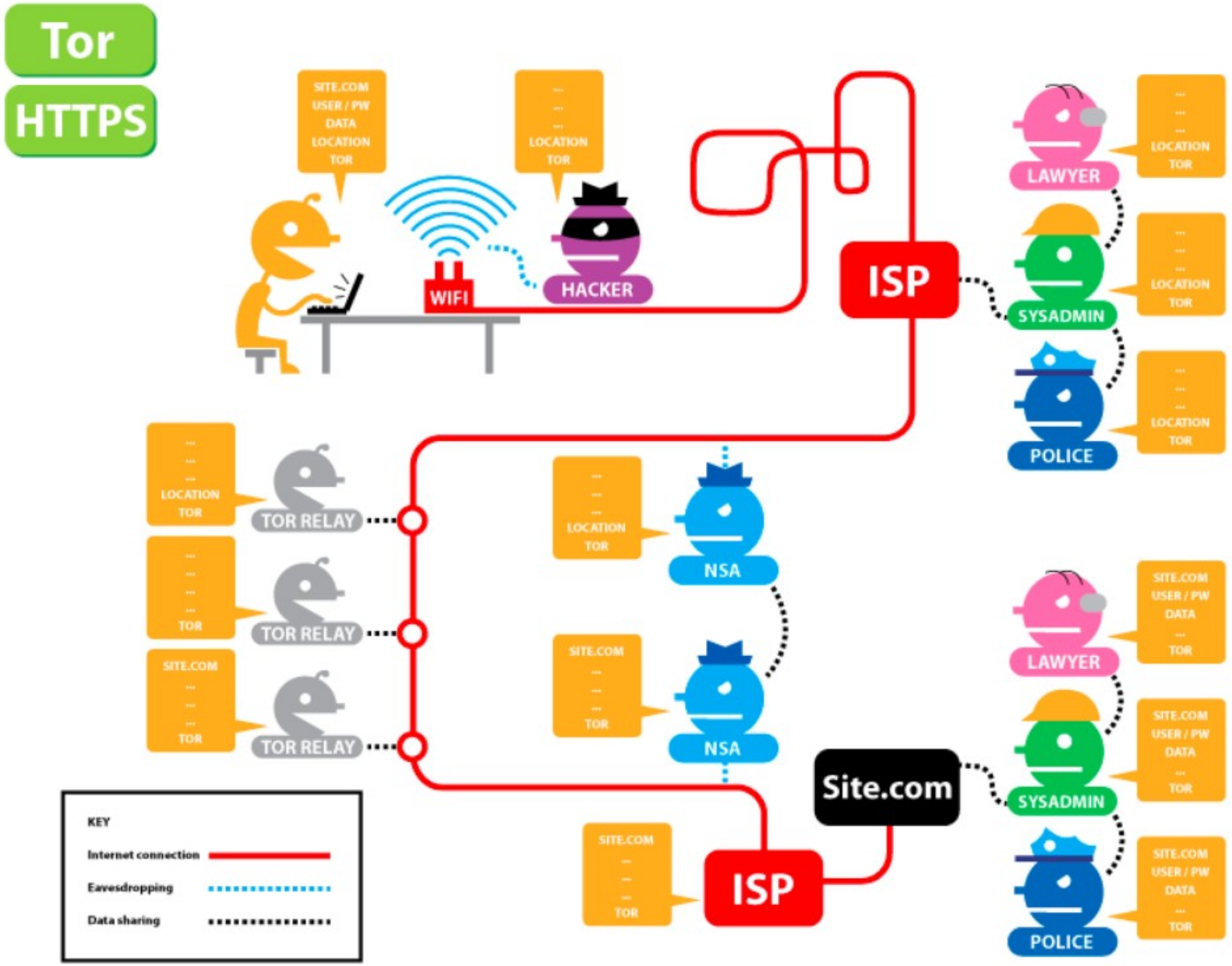
How the Internet Works

How the Internet works: exercise and discussion

See More at: https://myshadow.org/materials
And: https://www.eff.org/pages/tor-and-https


Anne visits news.com and logs in to her account. This diagram shows what can be collected along the way, depending on whether she connects to the website via http or https (shown as http:// or https:// in the browser bar).
NEWS.COM
Anne's Computer
HTTP
From: Anne's computer
To: http://news.com
+ Time, date & other metadata
+ Pages visited
+ Login & password
+ Browser fingerprint
HTTPS
From: Anne's computer
To: https://news.com
+ Time, date & other metadata
Anne's Router
Anne's ISP
HTTP
From: Anne's router
To: http://news.com
+ Time, date & other metadata
+ Pages visited
+ Login & password
+ Browser fingerprint
HTTPS
From: Anne's router
To: https://news.com
+ Time, date & other metadata
HTTP
From: Anne's ISP
To: http://news.com
+ Time, date & other metadata
+ Pages visited
+ Login & password
+ Browser fingerprint
HTTPS
From: Anne's ISP
To: https://news.com
+ Time, date & other metadata
National Gateway
Routing Server
National Gateway
HTTP
From: Anne's ISP
To: http://news.com
+ Time, date & other metadata
+ Pages visited
+ Login & password
+ Browser fingerprint
HTTPS
From: Anne's ISP
To: https://news.com
+ Time, date & other metadata
Website's ISP
.COM!
Website Owner
HTTP & HTTPS
From: Anne's ISP
To: http://news.com
+ Time, date & other metadata
+ Pages visited
+ Login & password
+ Browser fingerprint
Parent Companies of Website Trackers

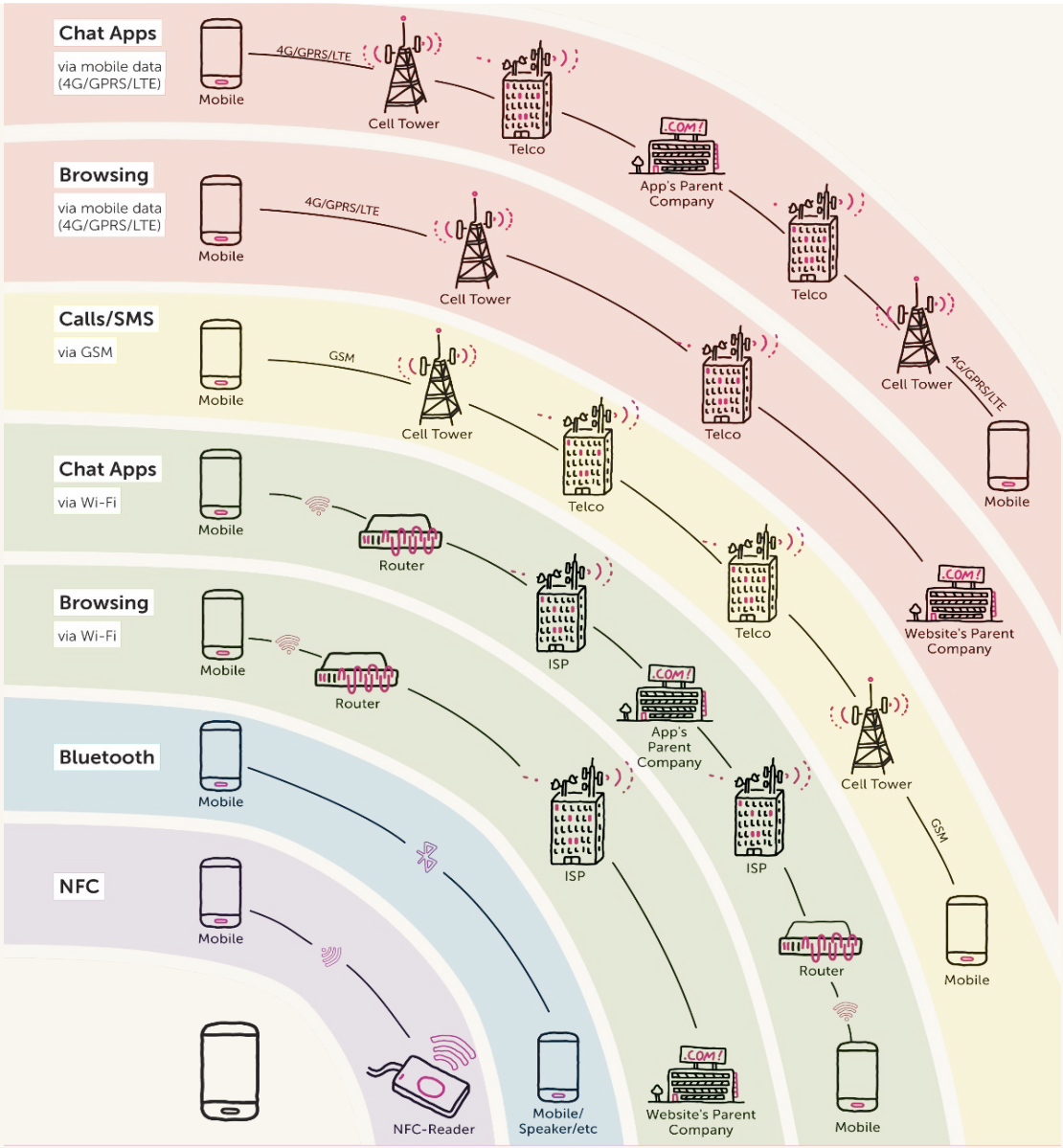

Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
...
...
LOCATION
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing



EXPOSING THE INVISIBLE

THE KIT

Surveillance

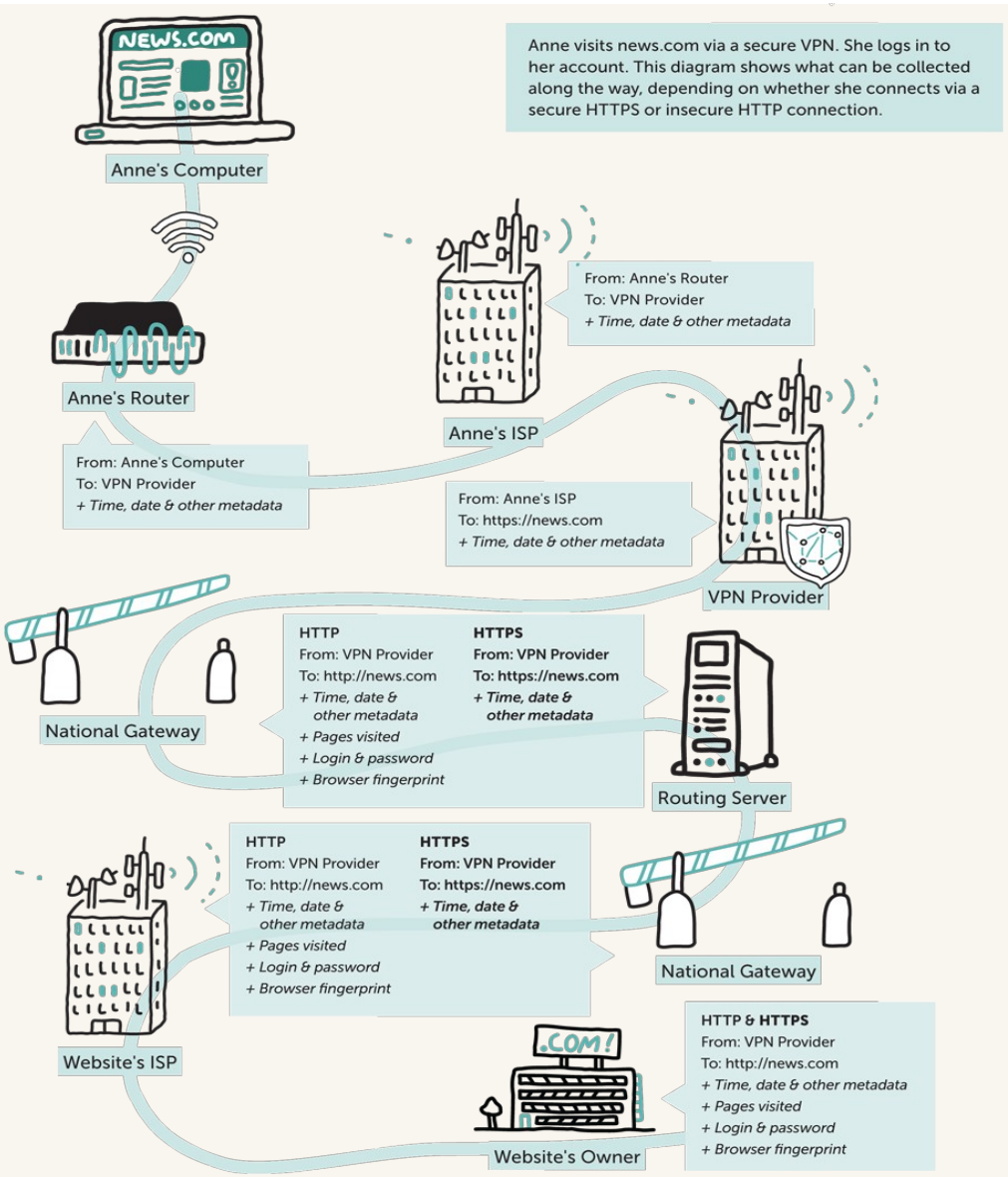


VPNs

How VPNs Work: exercise and discussion

See More at: https://myshadow.org/materials
And: https://www.eff.org/pages/tor-and-https

VPN


Anne visits news.com via a secure VPN. She logs in to her account. This diagram shows what can be collected along the way, depending on whether she connects via a secure HTTPS or insecure HTTP connection.
NEWS.COM
Anne's Computer
Anne's Router
From: Anne's Computer
To: VPN Provider
+ Time, date & other metadata
Anne's ISP
From: Anne's Router
To: VPN Provider
+ Time, date & other metadata
From: Anne's ISP
To: https://news.com
+ Time, date & other metadata
VPN Provider
National Gateway
HTTP
From: VPN Provider
To: http://news.com
+ Time, date & other metadata
+ Pages visited
+ Login & password
+ Browser fingerprint
HTTPS
From: VPN Provider
To: https://news.com
+ Time, date & other metadata
Routing Server
Website's ISP
HTTP
From: VPN Provider
To: http://news.com
+ Time, date & other metadata
+ Pages visited
+ Login & password
+ Browser fingerprint
HTTPS
From: VPN Provider
To: https://news.com
+ Time, date & other metadata
National Gateway
.COM!
Website's Owner
HTTP & HTTPS
From: VPN Provider
To: http://news.com
+ Time, date & other metadata
+ Pages visited
+ Login & password
+ Browser fingerprint

VPNs (Virtual Private Networks)

- Claims
- Business model
- Reputation
- Data collection
- Location and laws
- Encryption

VPNs

It is recommended you choose a **VPN** company that claims that they do not record logs of your traffic.

THAT ONE PRIVACY SITE

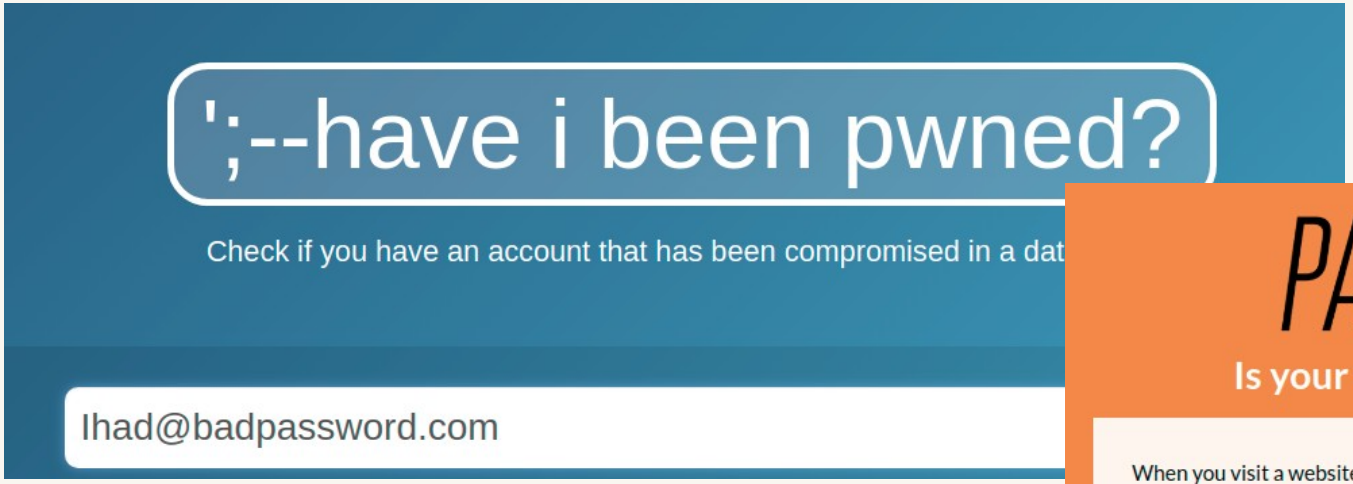
https://thatoneprivacysite.net/

Most free **VPN**s should be avoided because they are often funding their operation by selling their log data.

Reputable exceptions are:

- Riseup VPN
- PsIPhon
- Lantern
- ProtonVPN

Know your weaknesses



https://haveibeenpwned.com/

https://panopticlick.eff.org/

Where to next?

- https://kit.exposingtheinvisible.org/
- https://datadetoxkit.org/en/home
- https://xyz.informationactivism.org/en/
- https://holistic-security.tacticaltech.org/
- https://securityinabox.org/en/
- https://ourdataourselves.tacticaltech.org
- https://myshadow.org/

TACTICAL TECH
Making sense of the digital

Behind the Data: Metadata Explorations

Techniques, tips and safety considerations

Session topics:

1. What is metadata and why it matters.
2. Metadata we disclose.
3. Metadata we want to safeguard
4. Q & A

? - Which of these elements is not metadata?

A. The date when a photo was taken.

B. The objects you see in an image.

C. The location from where a Twitter message was posted.

D. The type of device used to record an interview.

What is metadata and why it matters.

Implications for research and safety

Digital Objects and what they can tell us

- Data
- Metadata
- Metadata
- Metadata
- Metadata
- Metadata

The

- **WHO**
- **WHAT**
- **WHEN**
- **WHERE**
- **HOW**

of any data

```
GPS Latitude Ref                : North
GPS Longitude Ref               : East
GPS Altitude Ref                : Above Sea Level
GPS Time Stamp                  : 11:07:47
GPS Img Direction Ref           : True North
GPS Img Direction               : 82.12307692
GPS Date Stamp                  : 2011:09:04
XMP Toolkit                     : XMP Core 5.1.2
Creator Tool                    : 4.3.5
Date Created                    : 2011:09:04 12:51:11
Image Width                     : 1024
Image Height                    : 765
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 2.8
GPS Altitude                    : 0 m Above Sea Level
GPS Date/Time                   : 2011:09:04 11:07:47Z
GPS Latitude                    : 38 deg 54' 35.40" N
GPS Longitude                   : 1 deg 26' 19.20" E
GPS Position                    : 38 deg 54' 35.40" N, 1 deg 26' 19.20" E
Image Size                      : 1024x765
Megapixels                      : 0.783
Shutter Speed                   : 1/3016
Focal Length                    : 3.9 mm
Light Value                     : 14.9
```

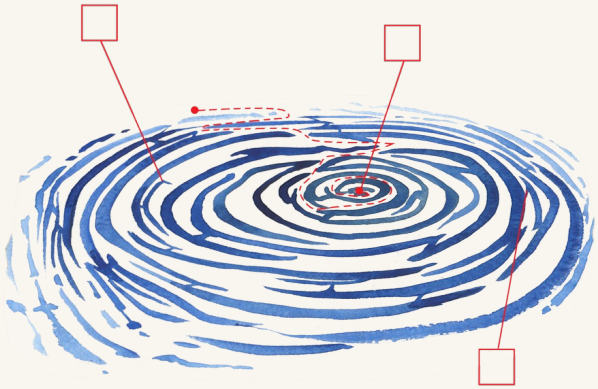
Information about information

Helps to:

- search, index, understand the information you gather
- identify source
- verify context
- preserve evidence
- prove

A checklist for 'good' evidence

- is first-hand
- is timely
- is documented and preserved to prove how it was obtained
- **includes metadata**
- has an unbroken chain of custody
- can be verified by others
- connects other pieces of information together
- doesn’t expose human sources to risk
- may contradict you
- speaks for itself.



See more at “What makes an investigation”: https://kit.exposingtheinvisible.org/en/investigation-concepts.html

A treasure for investigators

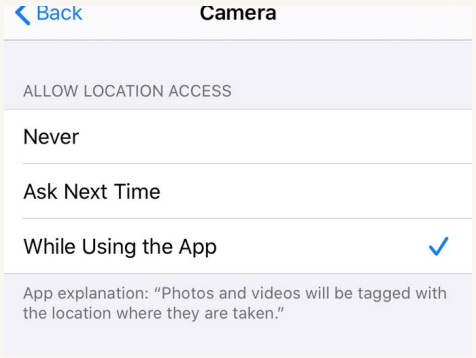
- used in OSINT investigations (e.g. https://www.bellingcat.com/)

Dmitry Peskov's $600,000 watch

Read more: https://www.bellingcat.com/resources/case-studies/2015/08/19/yachtspotting/

But then...

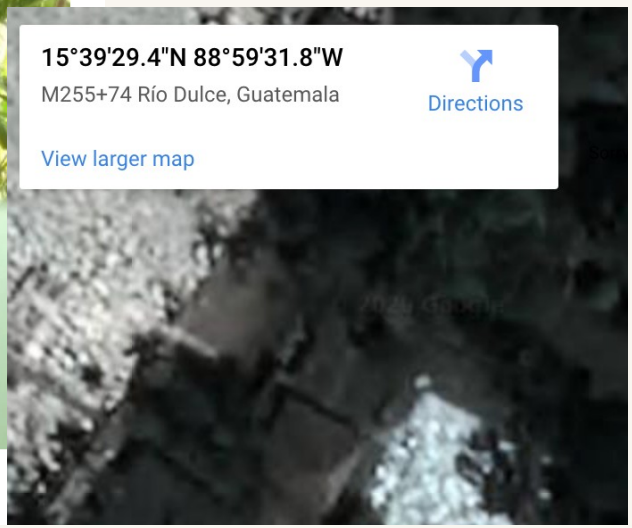

PLEASE BE CAREFUL WHEN
SHARING PHOTOS ON SOCIAL
MEDIA. THEY CAN LEAD POACHERS
TO OUR RHINO
TURN OFF GEOTAG FUNCTION
AND DO NOT DISCLOSE WHERE THE
PHOTO WAS TAKEN

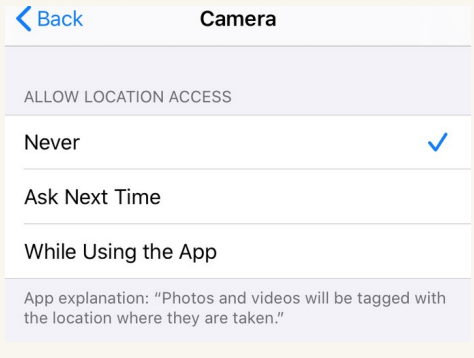


Vice piece:
https://www.vice.com/en/article/yv5kyv/we-are-with-john-mcafee-right-now-suckers

Oops! Did Vice Just Give Away John McAfee's Location With Photo Metadata?

John McAfee and Vice editor in chief Rocco Castoro. *Photo: Robert King/VICE*





Source: https://www.wired.com/2012/12/oops-did-vice-just-give-away-john-mcafees-location-with-this-photo/

Keep in mind

Metadata: best friend vs. worst enemy

- It can provide very useful proof to investigators, but it is also very vulnerable to manipulation.
- As evidence, it needs to be carefully preserved and safeguarded.
- Your metadata makes you and your sources/peers vulnerable, if exposed.

Generating and safeguarding metadata

Metadata we disclose

Safety First! - Common actions we do / Devices we use

- Desk & online research / documentation
- Field research / documentation
- Human interaction: finding and communicating with sources, witnesses, whistleblowers, ex-employees, etc...

- Mobile phones
- Tablets
- Laptops
- E-readers
- Wearables
- External storage

Task - see what you disclose to websites

In your current web browser, open a new tab and visit the online tool below to see what information you might be leaking to the websites you visit and the companies that own them:

https://coveryourtracks.eff.org/

Cover Your Trascks analyzes how well your browser and its add-ons protect you against online tracking techniques (it also works on TOR browser.) It may also generate related advice on how to improve your settings based on the 'diagnosis' it gives you.

Tools from EFF's Tech Team: https://www.eff.org/pages/tools

Other ways to see what you disclose to websites

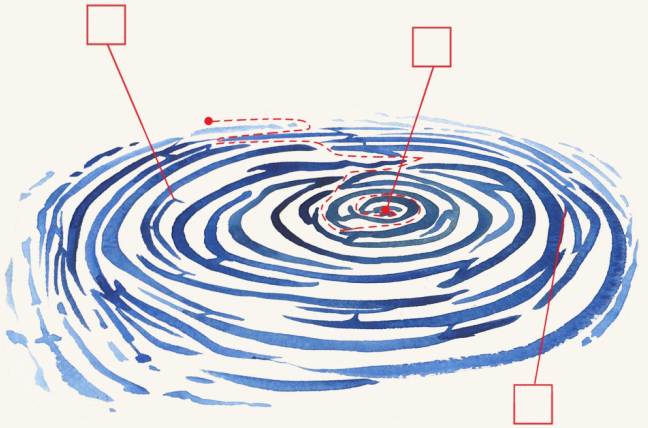
https://browserleaks.com/

A list of web-browser security-testing tools that tell you what personal data you may be leaking to others, without your knowledge or permission, when you search on the internet (also works on TOR browser.)

Your Metadata:

make a checklist of traces you might leave to evaluate risks

- on public wifi access/traces
- image metadata when sending/sharing/storing
- your calls/communication metadata
- mobile 'location on'
- cookies
- social media presence/apps (incl. what your connections post)
- document medatada
- wearable data/metadata
- personal apps data/metadata
- travel documents/online travel accounts



Communication metadata

- It depends on the type of communication used (i.e. email, mobile phone, smartphone, etc).

- In general it can reveal the following (if no tools to hide the metadata are used):
  - Ids of the sender and the receiver
  - Date and time of communication
  - Location
  - Mode of communication..etc

Communication metadata

- Trusted Apps
- Encrypted messaging apps (Signal)
- PGP

! Encrypted communication vs. legal requirements (e.g. Keybase)

Generating and safeguarding metadata

Metadata we want to safeguard

Chain of custody

Storage, transfer...

- Use *VeraCrypt, Cryptomator* file containers for data storage and safer transfer
- Backup your data in case of loss of devices (*Duplicati, Clonezilla, Spider Oak, NextCloud, Tresorit, Google**...and hard drives)
- Transfer files while preserving metadata: *Onionshare, Tresorit*

Metadata tools - photos

https://fotoforensics.com/

Jeffrey's Image Metadata Viewer

http://exif.regex.info/exif.cgi

ExifTool by Phil Harvey

Read, Write and Edit Meta Information!

https://exiftool.org/

Image Verification Assistant

helps you to analyse the veracity of online media

http://reveal-mklab.iti.gr/reveal/

Always use more tools to verify the same image

Videos

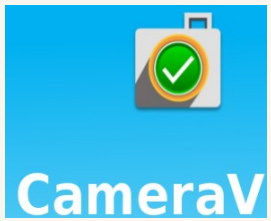
- Automatically generated metadata:
  - creation date,
  - size, format,
  - codecs,
  - duration,
  - location.

- Manually added metadata:
  - information about the footage,
  - text transcriptions,
  - tags,
  - further information and notes to editors..etc.

Videos

- Exact Upload Time
- Determine original video if several copies exist
- Useful to find older versions of the same video, by conducting a reverse image search

- Can be downloaded and installed on your computer
- You check and can alter image metadata



- Secure way to take and store photos and videos on mobile/tablet.
- Encrypts content and saves metadata for evidence.

- Store, preserve metadata, share mobile media while protecting your privacy.
- Safely stores media to archives (Internet Archive or your own)

Documents

- Metadata:
  - The names of all the different authors
  - Lines of text and comments that have been deleted in previous versions of the document
  - Creation and modification dates
  - **Can be removed, modified**

- PDF:
  - Windows and Mac can change metadata using Adobe Pro (Trial version or purchase)
  - Linux – PDF Mod but can't change device or creation date

- WordOffice document
  - File → Properties

Discussion: You took a video of an incident and you want to send it to a colleague as evidence for your investigation/case. How do you make sure you preserve the metadata? *tip: there is no right answer :)*

A) I send the video via Signal because it is encrypted.

B) I attach the video to an email to make it easier to keep track of communications.

C) I copy it to a USB and send it by post to avoid digital tracking of our communication.

D) I upload it to a shared folder in the cloud because it's faster for them to get it.

E) I share it on Facebook live to prove I was really there.

Safety First! - Remember Your Risk Assessment

- Goal of your research/investigation
- Functions you perform
- Methods and tools you use to perform the functions
- Data you collect/ safeguard/ communicate
- Context(s) where you perform those functions
  - Adversaries
  - Capabilities of adversaries
  - Consequences

More resources:

- ***Why Metadata Matters*** - an introduction from Surveillance Self Defense / EFF: https://ssd.eff.org/en/module/why-metadata-matters. See the entire digital list of safety modules: https://ssd.eff.org/

- ***Behind the Data: Investigating Metadata*** - a guide with methods, cases and tools for tracking and verifying metadata in different contexts and online platforms: https://exposingtheinvisible.org/guides/behind-the-data-metadata-investigations/

- ***How to See What's Behind a Website*** - An introductory guide with resources and tips on investigating website ownership data and website metadata (whois); from Tactical Tech's Exposing the Invisible - The Kit: https://kit.exposingtheinvisible.org/en/how/web.html

- ***Metadata or It Didn't Happen*** - an article/interview with Harlo Holmes from the Electronic Frontier Foundation (EFF) about CameraV (tool to capture, encrypt and share videos while preserving metadata) and the need to preserve metadata as evidence: https://exposingtheinvisible.org/resources/harlo-holmes

- ***Everything you wanted to know about media metadata, but were afraid to ask***: https://freedom.press/training/everything-you-wanted-know-about-media-metadata-were-afraid-ask/

Contact us:

Wael @ tacticaltech.org
Laura @ tacticaltech.org

Exposing the Invisible

https://exposingtheinvisible.org/
https://kit.exposingtheinvisible.org/

Tactical Tech

https://tacticaltech.org/