Security Awareness Workshop

Null NEU + NEU Blockchain

- *Sooraj Sathyanarayanan*

FORTIFYING YOUR DIGITAL ASSETS

JOIN US TO DISCOVER ESSENTIAL STRATEGIES FOR SAFEGUARDING YOUR DIGITAL WALLETS

FRIDAY
9/27/2024

START AT
06:00 PM EDT

104, WEST VILLAGE G
NORTHEASTERN UNIVERSITY

Sooraj S
Security & Privacy Researcher

YOU'LL TAKE SECURITY AWARENESS TRAINING SERIOUSLY
memegenerator.net

Disclaimer

Not Financial or Legal Advice

The workshop is not sponsored by any company.

Accuracy and Completeness

Information in the field of cybersecurity may change rapidly.

Attendance implies acknowledgment of the disclaimer.

$ whoami – Sooraj Sathyanarayanan

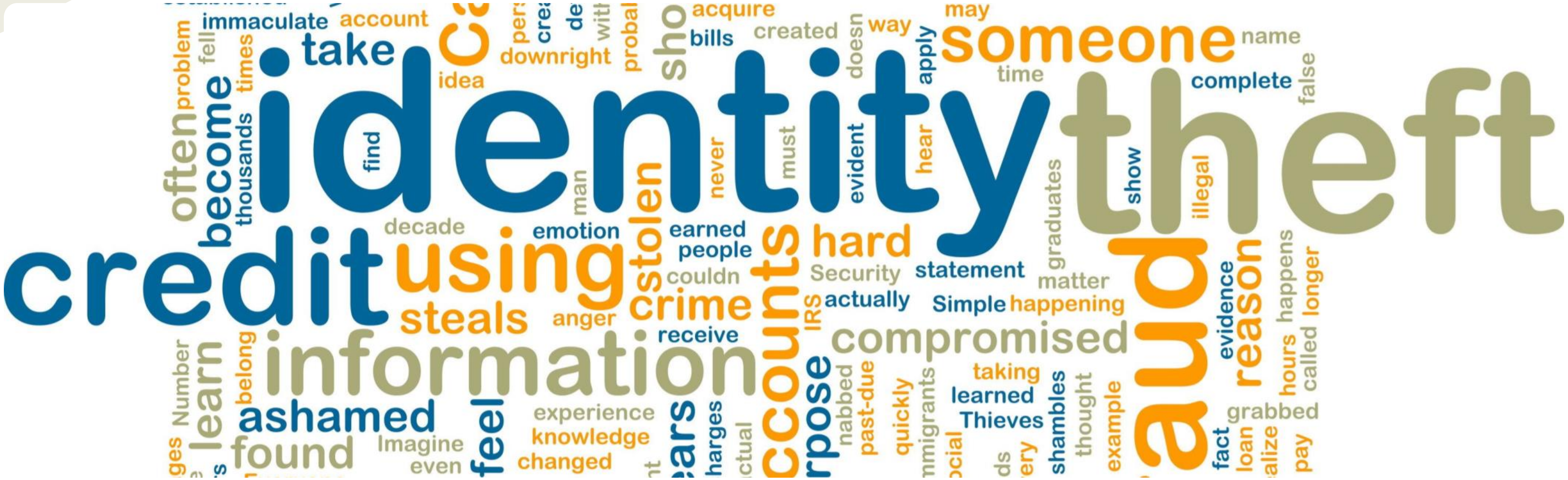
Education: Pursuing MS in Cybersecurity at Northeastern University

Professional Experience: IT Audit Analyst at Fidelity Investments, worked in Digital Forensics, Threat Research & Penetration Testing with over three years at a global Fortune 100 and cybersecurity consultancy.

Community Leadership: Chapter Lead at null NEU, nurturing a learning community with workshops and security awareness initiatives. Research Lead at NEU Blockchain Club (Decentralized Identity)

Vision & Advocacy: Passionate Opensource Enthusiast dedicated to data privacy and digital rights. Committed to lifelong learning and making impactful contributions in cybersecurity.

Connect Further: Explore more about my professional journey, projects, and insights on my personal website. (Include QR code for direct access)



Why even care?

Avoids financial losses (wallet / bank hack)

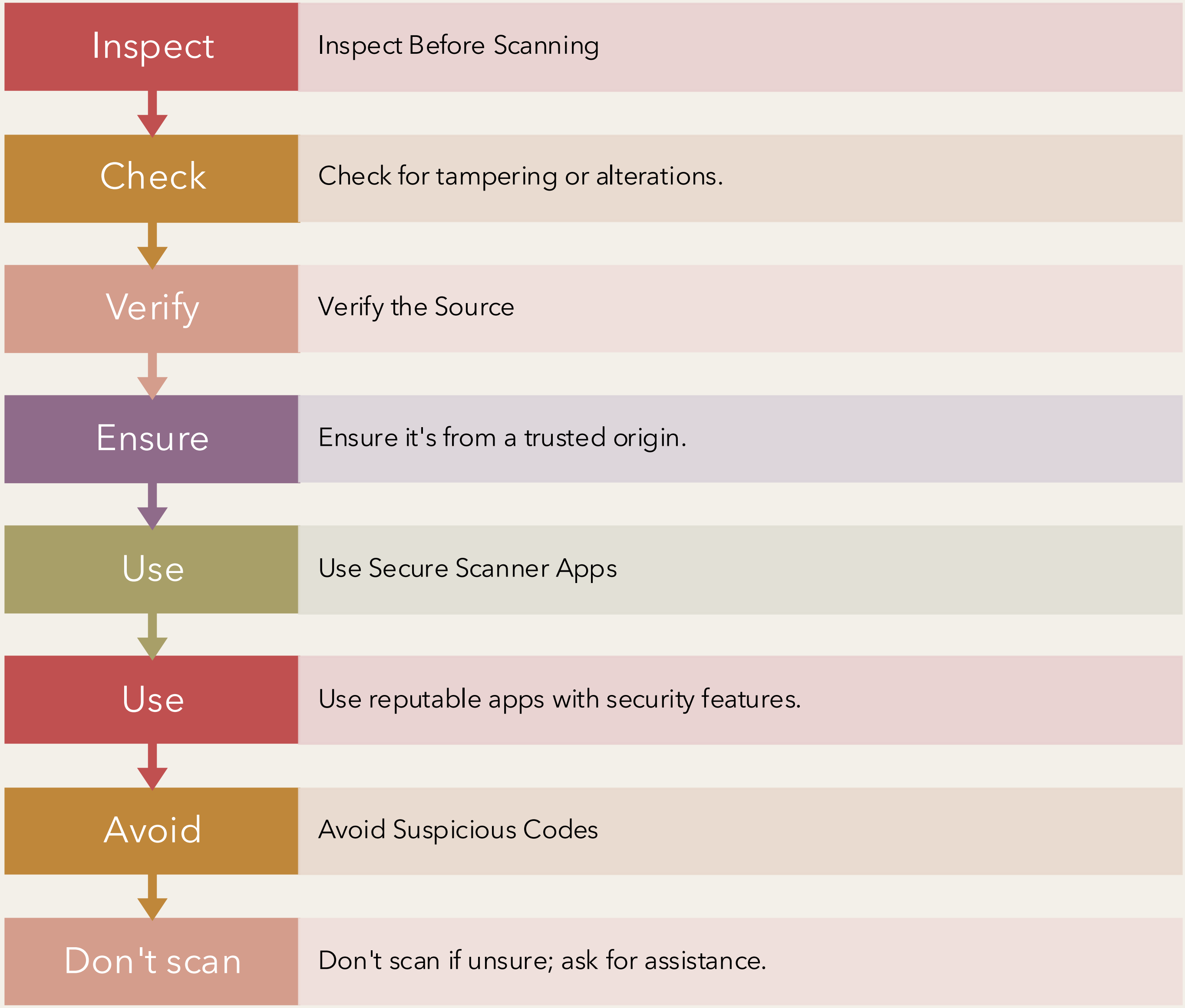
Protects reputation (street cred from crypto bros)

Reduces the risk of malware on devices (nothing is unhackable)

Prevent cyberbullying or harassment

Prevent identity theft

QR Code Safety Tips



Inspect — Inspect Before Scanning

Check — Check for tampering or alterations.

Verify — Verify the Source

Ensure — Ensure it's from a trusted origin.

Use — Use Secure Scanner Apps

Use — Use reputable apps with security features.

Avoid — Avoid Suspicious Codes

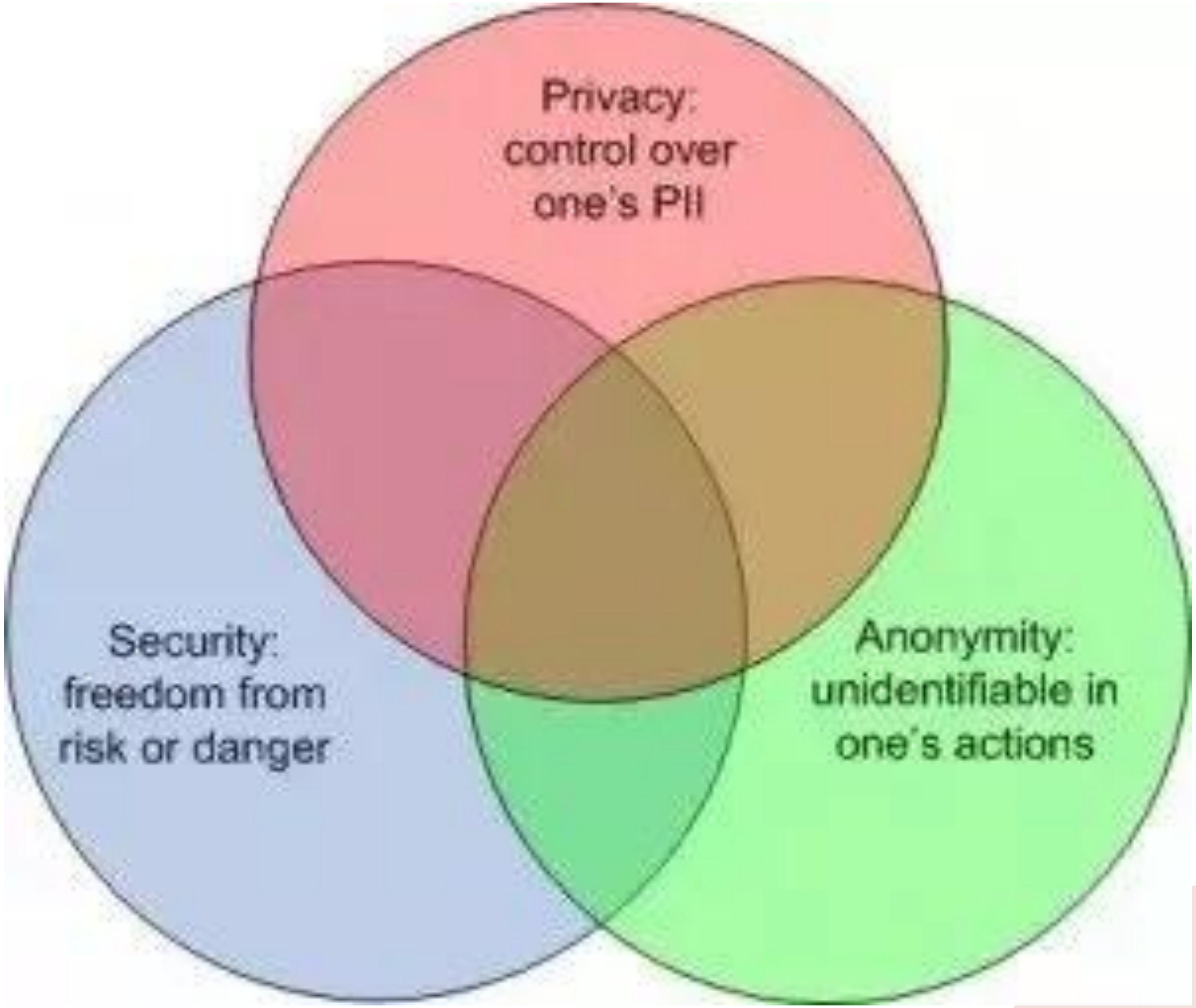
Don't scan — Don't scan if unsure; ask for assistance.

Privacy vs. Security vs. Anonymity

Privacy - being free from observation.

Security - being free from danger

Anonymity - being free from identification.



Privacy: control over one's PII
Security: freedom from risk or danger
Anonymity: unidentifiable in one's actions

Threat Model

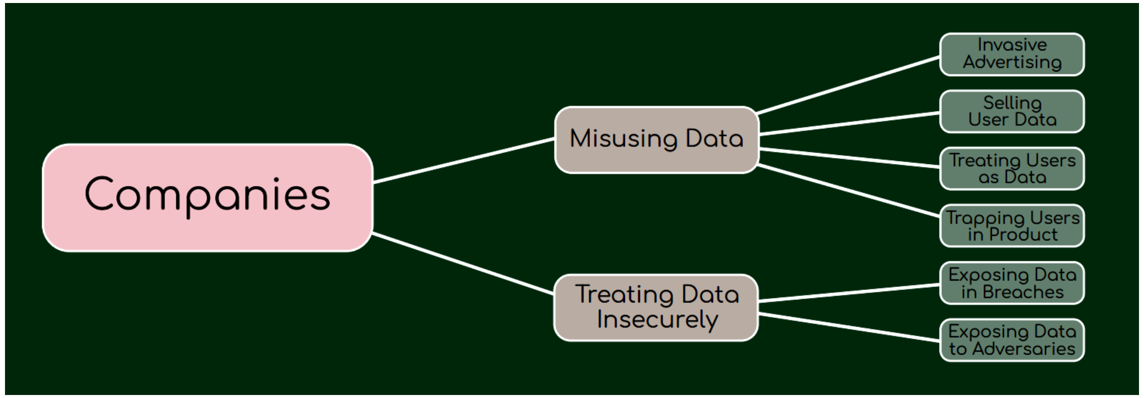
What to Protect

Who to Protect From

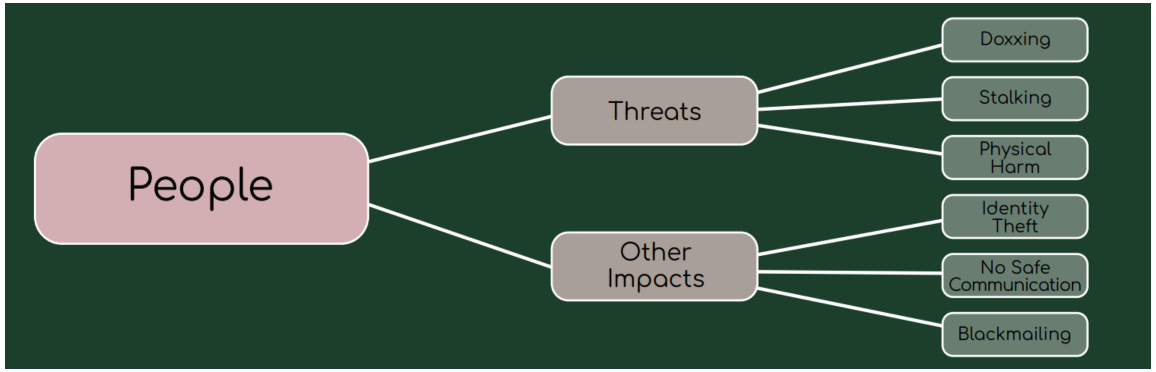
Consequences of Failure

Likelihood of Threats

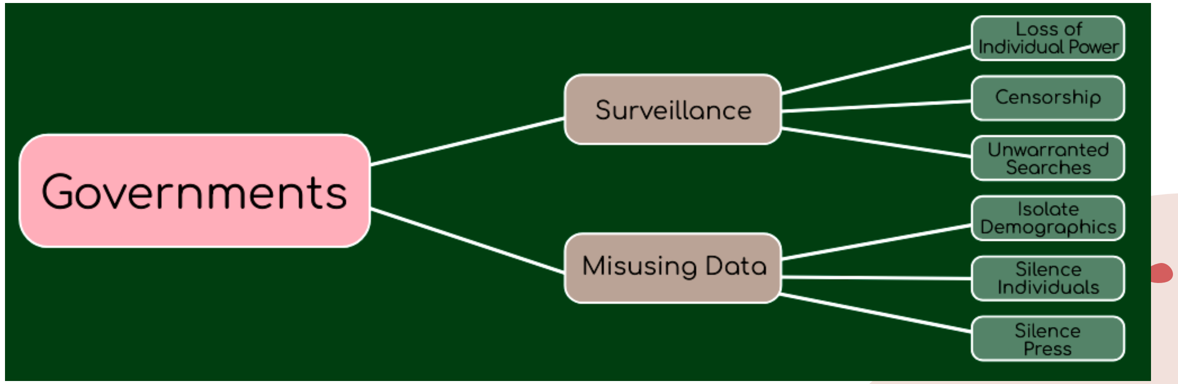
Cost-Benefit Analysis



Companies
Misusing Data
Invasive Advertising
Selling User Data
Treating Users as Data
Trapping Users in Product
Treating Data Insecurely
Exposing Data in Breaches
Exposing Data to Adversaries



People
Threats
Doxxing
Stalking
Physical Harm
Other Impacts
Identity Theft
No Safe Communication
Blackmailing



Governments
Surveillance
Loss of Individual Power
Censorship
Unwarranted Searches
Misusing Data
Isolate Demographics
Silence Individuals
Silence Press

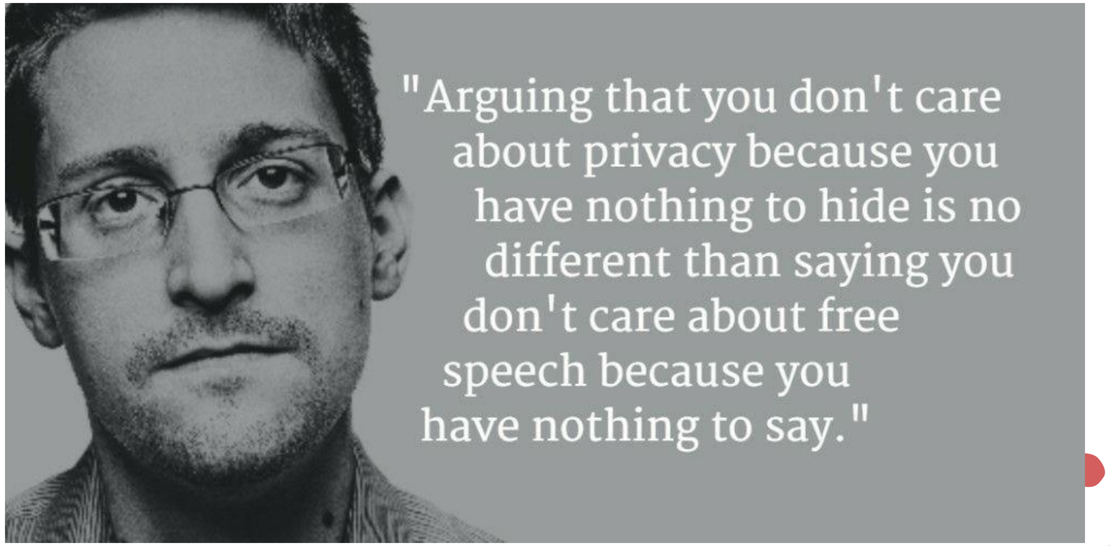
Why privacy matters?

Fundamental Right: Privacy is a fundamental human right that should be protected.

Control Over Life: It gives individuals control over their lives and the freedom to make choices without undue surveillance.

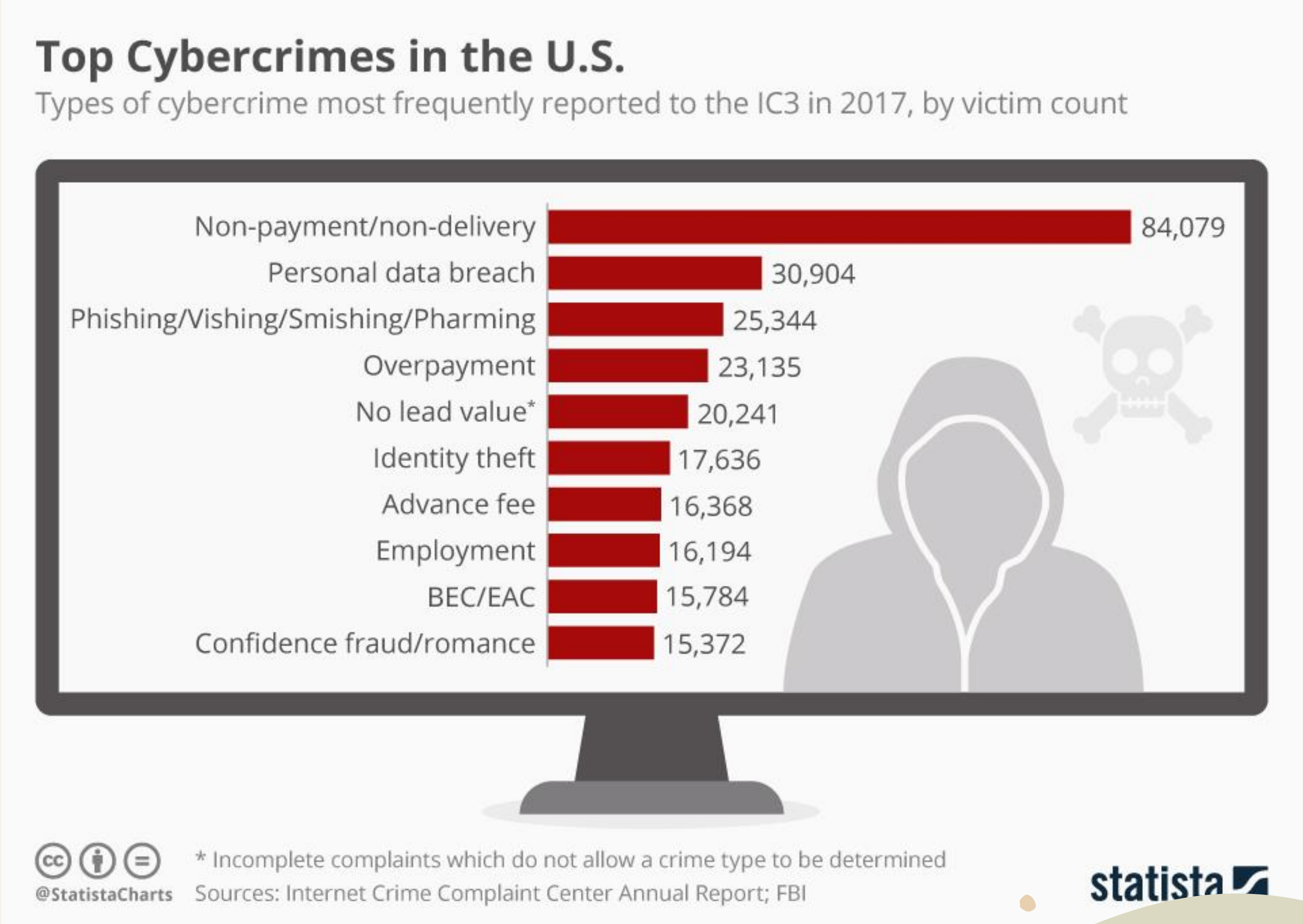
Security: Privacy is essential for personal security, including physical safety.

Democracy and Civil Liberties: It is vital for upholding democracy and protecting civil liberties within a country.



"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Top Cybercrimes in the US



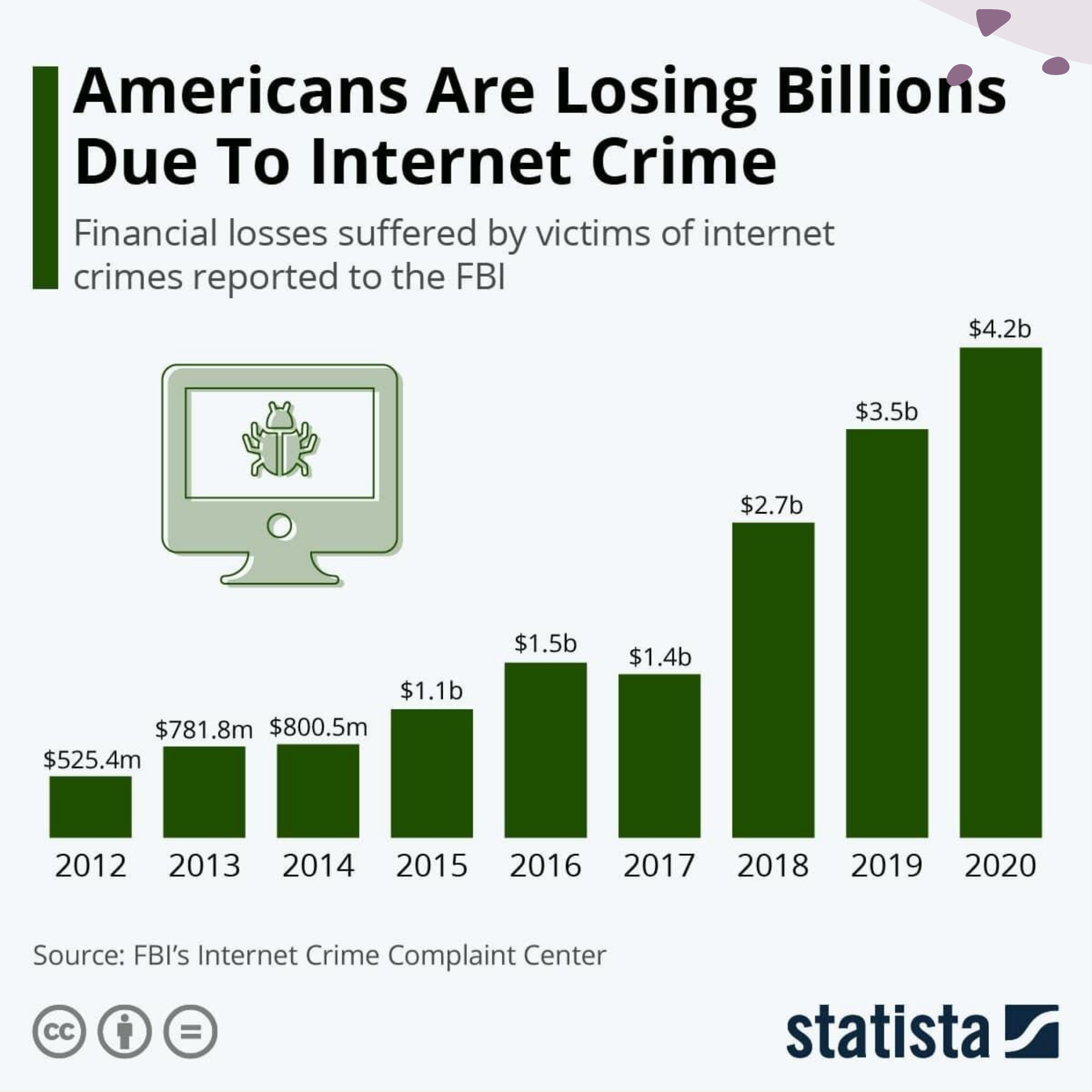
Top Cybercrimes in the U.S.

Types of cybercrime most frequently reported to the IC3 in 2017, by victim count

* Incomplete complaints which do not allow a crime type to be determined

Sources: Internet Crime Complaint Center Annual Report; FBI

How much does cybercrime cost the US?



Americans Are Losing Billions Due To Internet Crime

Financial losses suffered by victims of internet crimes reported to the FBI

Source: FBI's Internet Crime Complaint Center

statista

Developing a Security Mindset

Be	Proactive: Always be alert and cautious in your digital interactions.
Understand	your actions have a direct impact on **your safety**.
Stay	informed about evolving cyber threats and best practices.
Prioritize	security in all online activities, even if it means sacrificing convenience.
Share	**knowledge** and best practices with others to enhance collective security.

Check Your Exposure: Have I Been Pwned?

What Is It? A tool to check if your email or phone is in a data breach.

Importance: Identifies your exposure in breaches to enhance security.

How to Use:

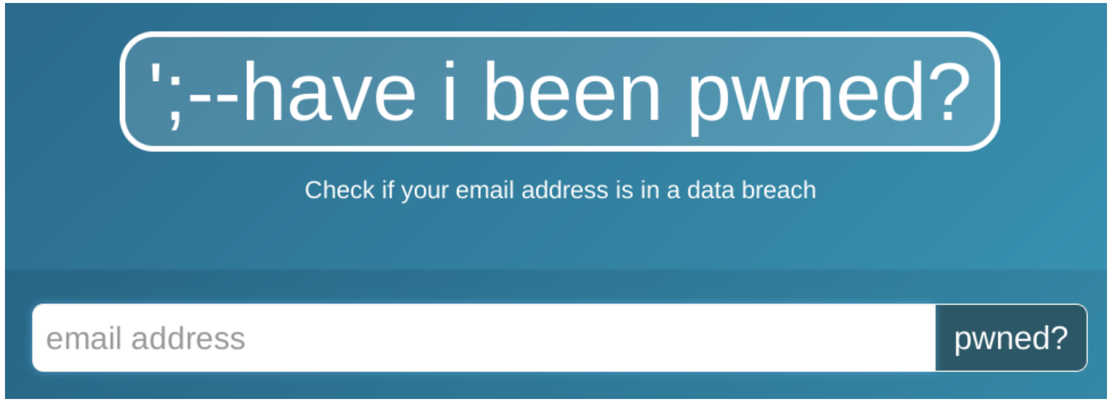
- Visit Have I Been Pwned website.
- Enter your email or phone number.
- Discover if you've been compromised.

If Pwned:

- Change Passwords immediately.
- Enable 2FA for added security.
- Monitor Accounts for unusual activity.

Prevention:

- Regular checks on Have I Been Pwned.
- Use complex passwords and a password manager.
- Stay cautious with personal info online.



';--have i been pwned?

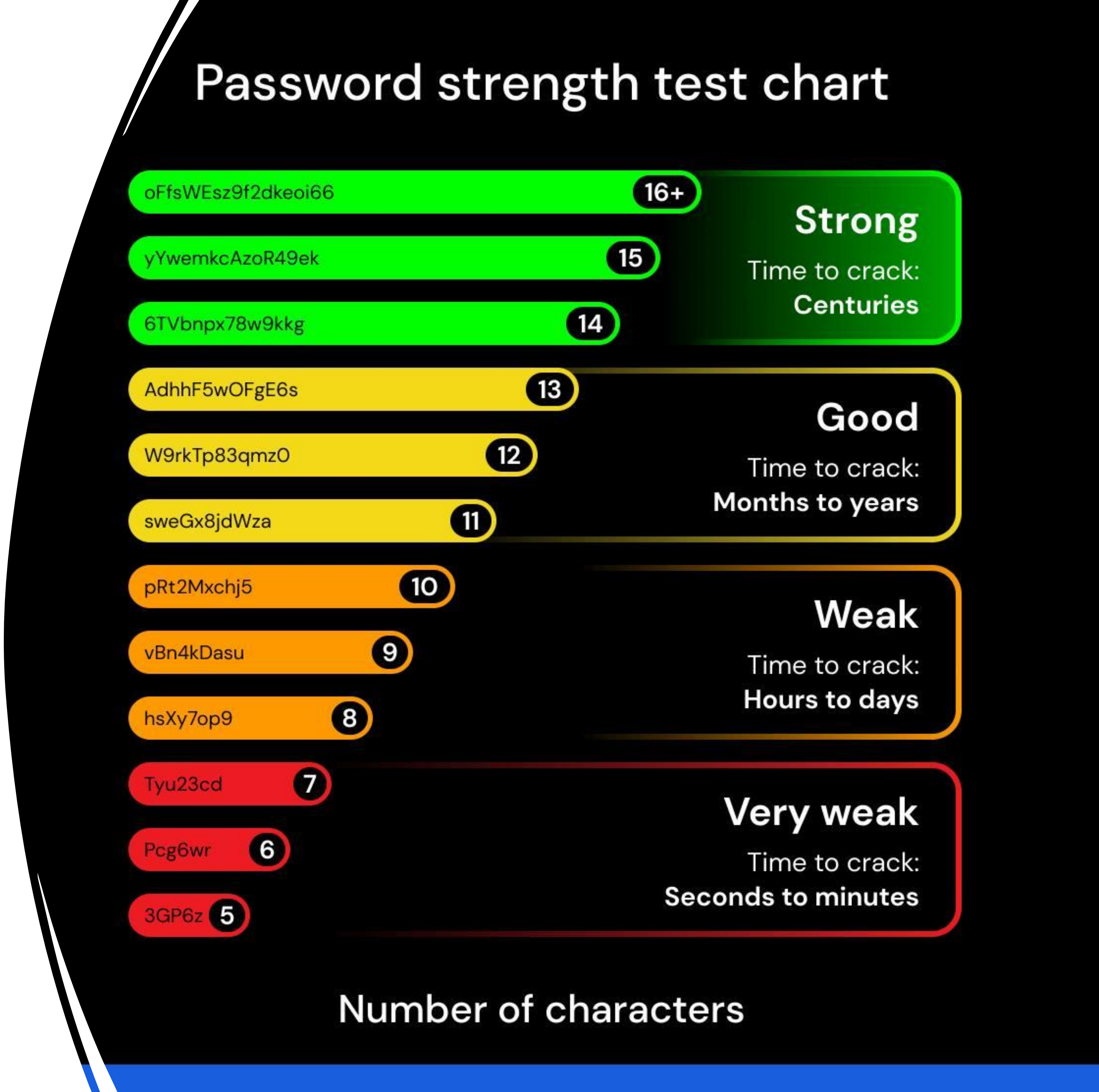
Check if your email address is in a data breach

Passwords/Passphrases Don'ts

- Don't use **personal** information: Avoid using your name, birthdate, or address as part of your password
- Don't reuse **passwords**: Use unique passwords for each account or service you use
- Don't share **your** password: Keep your password confidential and avoid sharing it with anyone, even family and friends
- Don't write **it** down: Avoid writing your password down or storing it in an easily accessible location
- Don't use **common** passwords: Avoid using easily guessed passwords such as "password" or "123456"

How secure is your password ?

Use a good password manager example:
Bitwarden/Proton Pass



Multi-Factor Authentication (MFA)

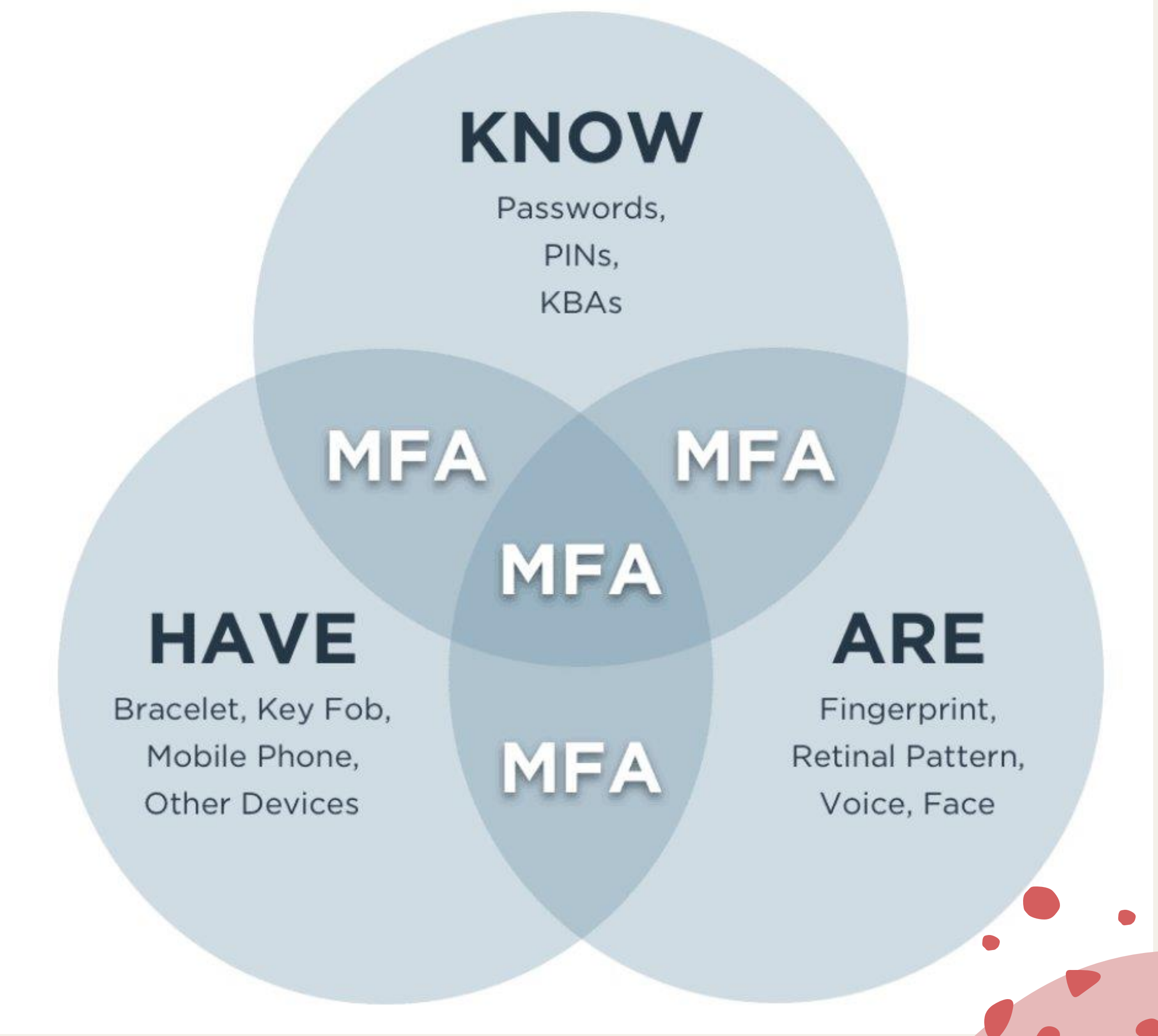
- **What is MFA?**
  - Security measure requiring two or more verification factors
  - Examples: Password **and** fingerprint
- **Why Use MFA?**
  - Adds an extra layer of security
  - Prevents unauthorized access to accounts
- **Effectiveness:**
  - Prevents over **95%** of bulk phishing attempts
  - Stops over **75%** of targeted attacks

Types of MFA (aka Multi-Factor Authentication)

Something you know: password, PIN, security question

Something you have: phone, smart card, token

Something you are: fingerprint, facial recognition, iris scan



Multi-Factor Authentication - TOTP

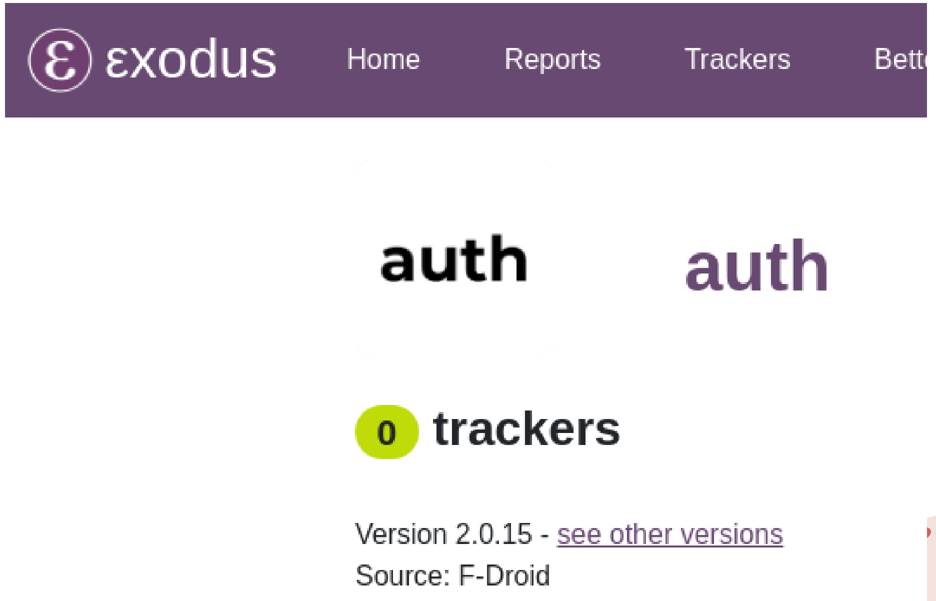
Spotlight on **ente auth** – for most folks

Why?

- Opensource
- End-to-End Encrypted Backups
- Multi-Device Support
- Offline Mode
- Cross-Platform

Comparison: https://ente.io/compare/ente-auth-vs-others

Special Mention: Bitwarden Authenticator



0 trackers

Version 2.0.15 - see other versions
Source: F-Droid

Upgrade MFA?

Anti-Phishing: Bound to the website's URL, hardware keys offer robust protection against phishing.

No Shared Secrets: Eliminate the risk of code interception – keys don't rely on shared secrets.

Portability & Speed: A convenient solution across devices, often faster than SMS or app-based 2FA.

Impenetrable Physical Security: No physical key equals no access, securing your accounts even if your device is compromised.

Recommended Tools: Yubico Yubikeys, Google Titan Keys

Phishing Scams & Secure Email Services

Phishing scams are designed to trick you into giving away your personal information. Tips to help you protect yourself:

Verify the email source by checking the email headers

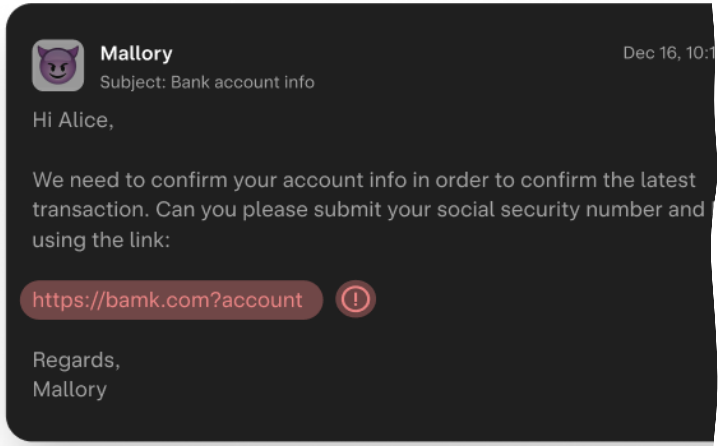
Use secure email services to block trackers and remote content.

Report suspicious emails to the relevant authorities.

Protect your email by using aliasing services.

Secure email services examples: **Proton Mail, Tutanota**

Examples of Phishing Scams



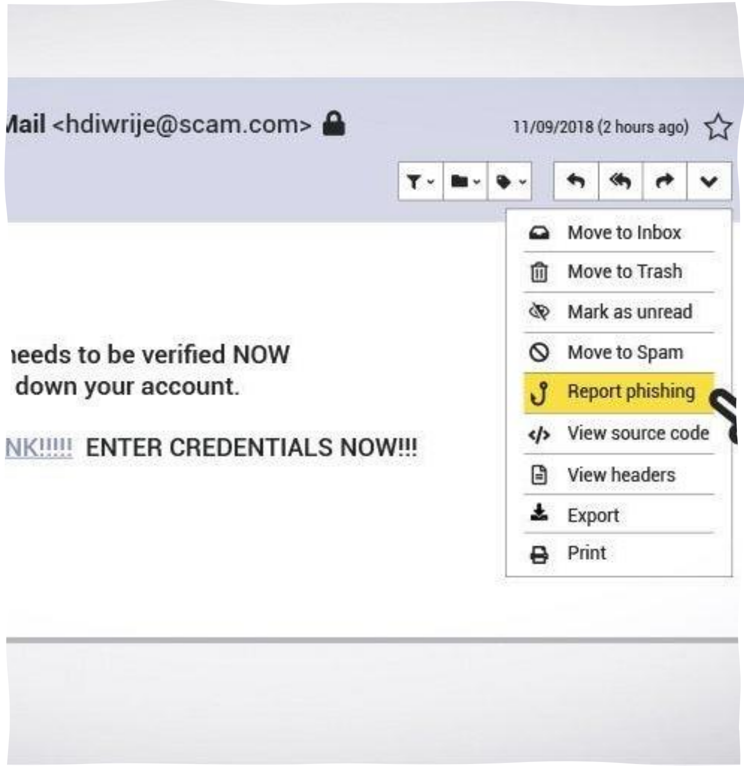
Mallory
Dec 16, 10:1
Subject: Bank account info

Hi Alice,

We need to confirm your account info in order to confirm the latest transaction. Can you please submit your social security number and using the link:

https://bamk.com?account

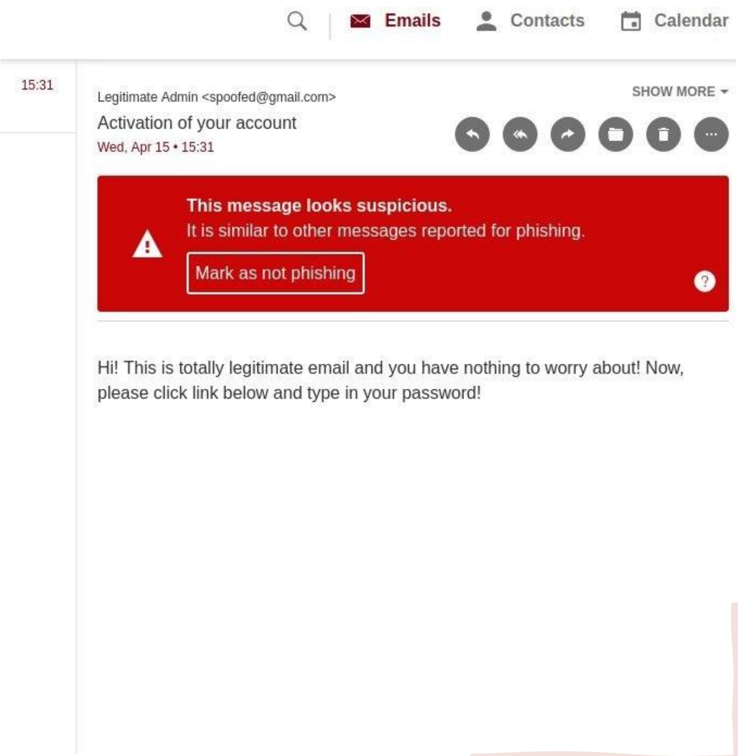
Regards,
Mallory



Mail <hdiwrije@scam.com>
11/09/2018 (2 hours ago)

ieeds to be verified NOW
down your account.

NK!!!!! ENTER CREDENTIALS NOW!!!



Legitimate Admin <spoofed@gmail.com>
Activation of your account
Wed, Apr 15 • 15:31

This message looks suspicious.
It is similar to other messages reported for phishing.

Hi! This is totally legitimate email and you have nothing to worry about! Now, please click link below and type in your password!

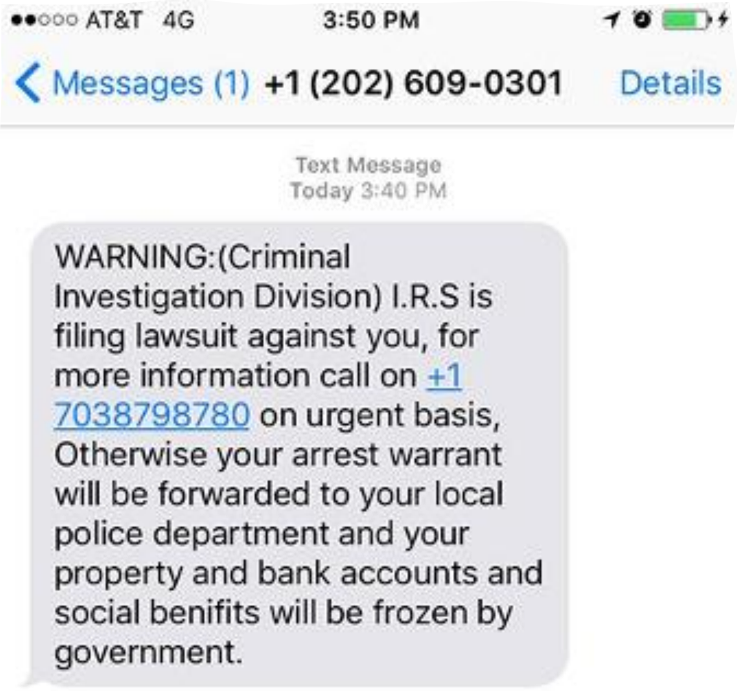
SMS Scams aka Smishing

Avoid tapping links in unsolicited text messages.

Don’t respond to any unknown or unwarranted text messages.

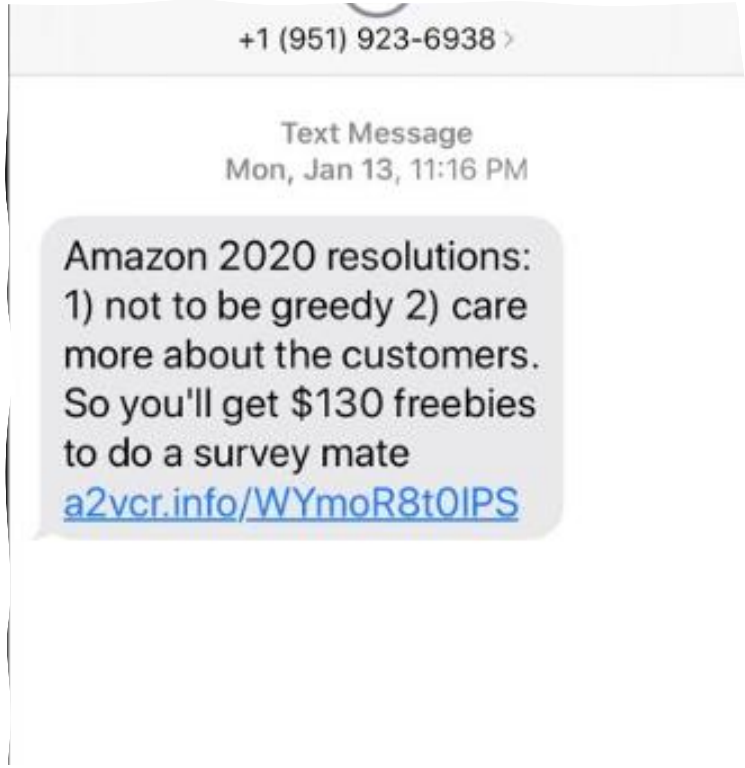
Some common signs of a smishing scam include urgent requests, offers that seem too good to be true, and messages that ask for personal information

Examples of Smishing



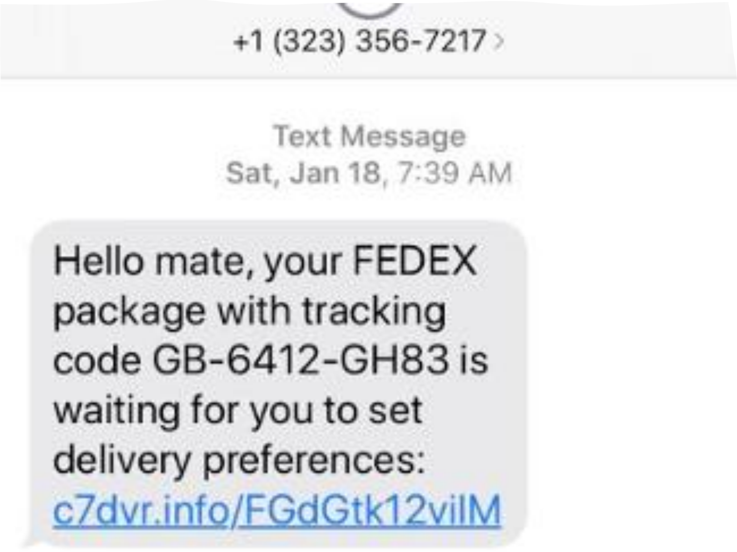
Text Message
Today 3:40 PM

WARNING:(Criminal Investigation Division) I.R.S is filing lawsuit against you, for more information call on +1 7038798780 on urgent basis, Otherwise your arrest warrant will be forwarded to your local police department and your property and bank accounts and social benifits will be frozen by government.



Text Message
Mon, Jan 13, 11:16 PM

Amazon 2020 resolutions: 1) not to be greedy 2) care more about the customers. So you'll get $130 freebies to do a survey mate a2vcr.info/WYmoR8t0IPS



Text Message
Sat, Jan 18, 7:39 AM

Hello mate, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: c7dvr.info/FGdGtk12vilM

Combating Spam Calls and Scams

Spotting Spam:

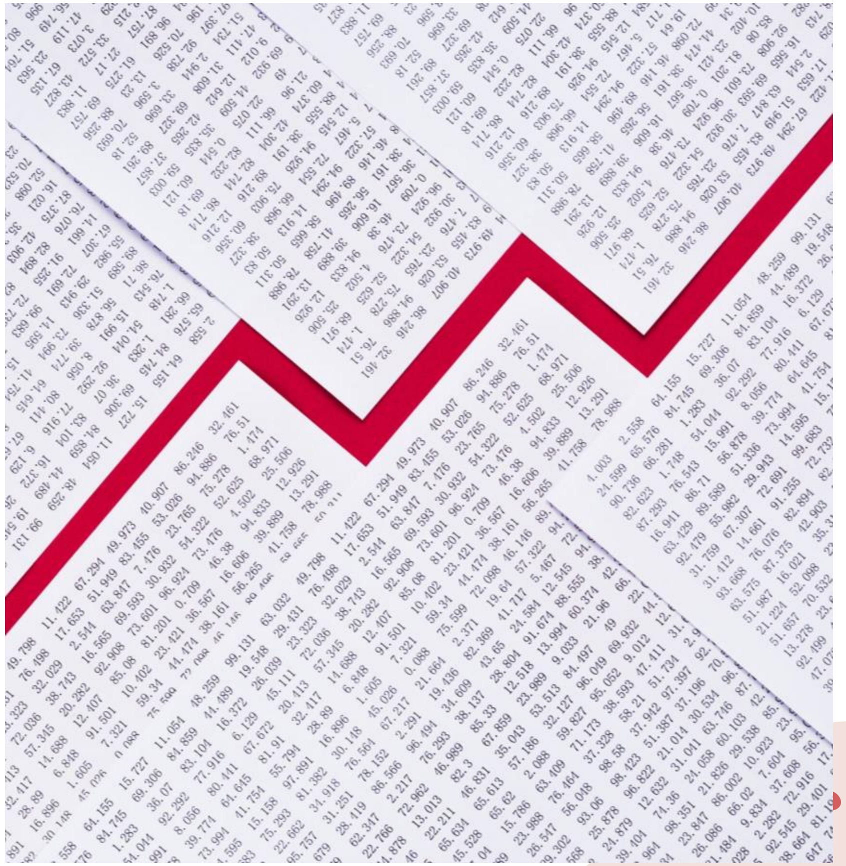
- Offers or threats from unknown numbers.

Scam Tactics:

- Callers pretending to be officials.
- Urgent demands for money or data.

Your Defense:

- Secret phrases for friends and family (helps against AI)
- Hang up on suspicious calls.
- Confirm via official contacts.
- Block and report spam numbers.



Safe Browsing

Use Private Search Engines

- *Example*: Brave Search

Browse with Secure Browsers

- *Example*: Brave Browser

Check for Secure Connections

- Look for the 🔒 padlock icon (HTTPS)

Avoid Pop-Up Ads

- Be cautious; never click on them

Download Wisely

- Avoid files from untrusted websites

Social Media Safety Tips

Be Mindful: Be aware and thoughtful about your online posts, both about yourself and others.

Protect Personal Information: Refrain from sharing sensitive details like your birthday, phone number, home address, or banking information online.

Geotagging Caution: Avoid geotagging your current location, especially when on vacation.

Location Privacy: Do not post photos that reveal your precise residential location.

Building Your Digital Footprint: Remember that everything you post online contributes to your digital footprint.

Secure your Network

Verify

Always verify the authenticity of the Wi-Fi network before connecting to it

Avoid

Avoid accessing sensitive information like bank accounts, credit card information, and other personal data while using open Wi-Fi networks.

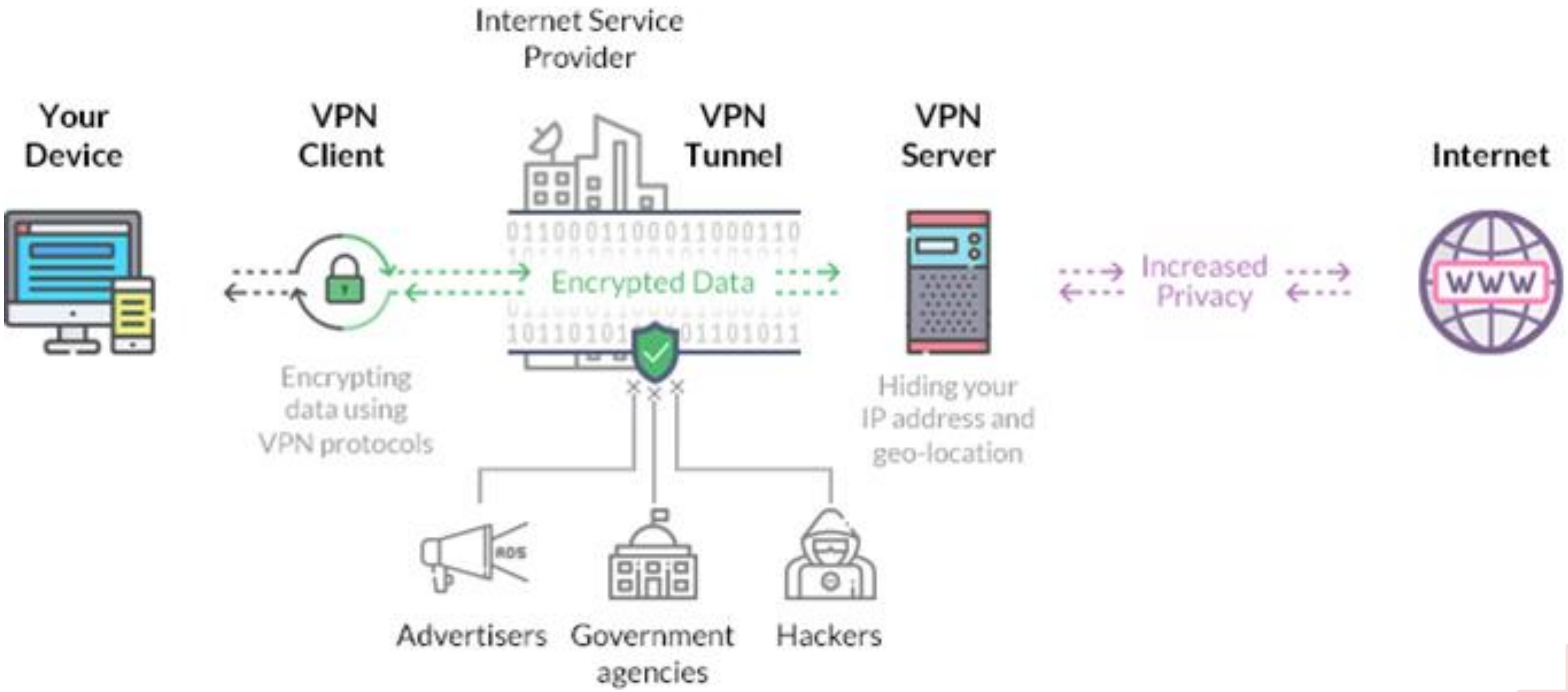
Disable

Disable the automatic Wi-Fi connection option on your device and manually connect to trusted networks only.

Use

Use a virtual private network (VPN) when accessing sensitive information or connecting to a network remotely.
Examples: Mullvad, Proton VPN, IVPN

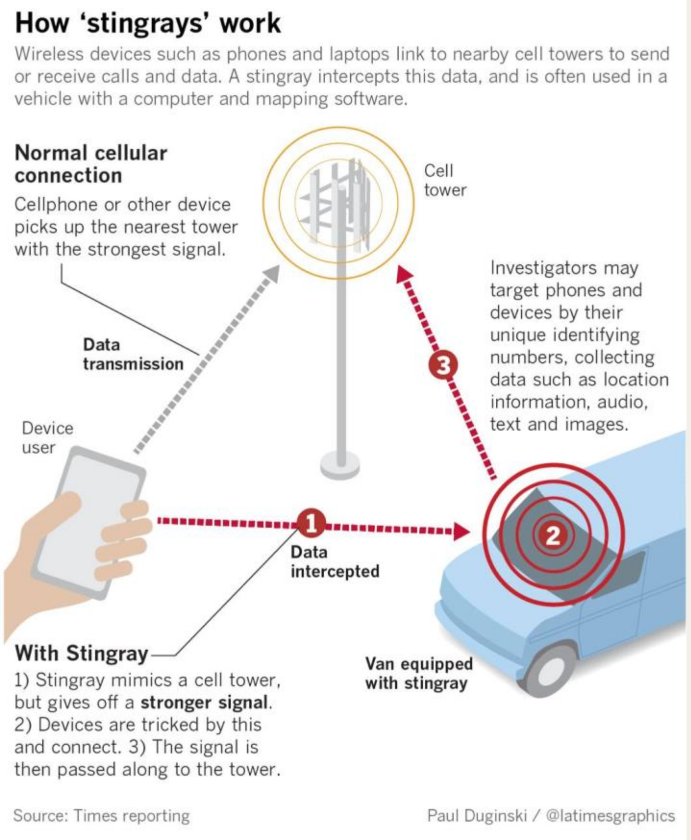
How a VPN secures your online activity?



Cell Phone Surveillance

Methods: There are various methods of cell phone surveillance, including:

- **GPS Tracking:** Tracking the device's physical location in real-time.
- **Call Interception:** Listening to or recording phone conversations.
- **Text Message Monitoring:** Accessing and reading text messages.



How 'stingrays' work

Wireless devices such as phones and laptops link to nearby cell towers to send or receive calls and data. A stingray intercepts this data, and is often used in a vehicle with a computer and mapping software.

Normal cellular connection

Cellphone or other device picks up the nearest tower with the strongest signal.

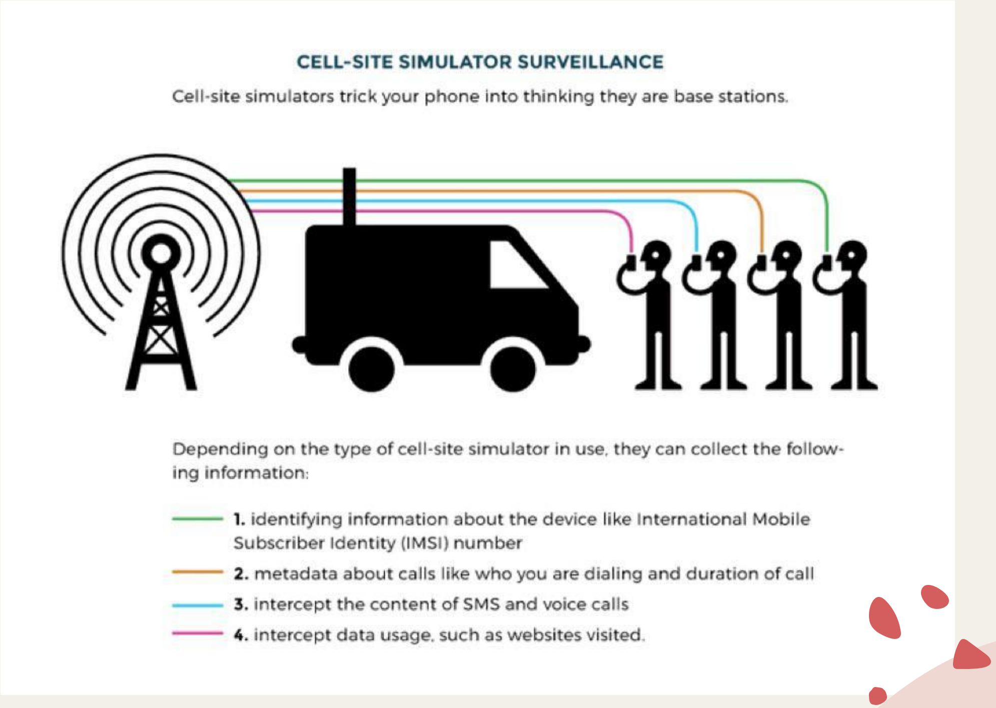
Investigators may target phones and devices by their unique identifying numbers, collecting data such as location information, audio, text and images.

With Stingray

1) Stingray mimics a cell tower, but gives off a **stronger signal**. 2) Devices are tricked by this and connect. 3) The signal is then passed along to the tower.

Source: Times reporting

Paul Duginski / @latimesgraphics



CELL-SITE SIMULATOR SURVEILLANCE

Cell-site simulators trick your phone into thinking they are base stations.

Depending on the type of cell-site simulator in use, they can collect the following information:

1. identifying information about the device like International Mobile Subscriber Identity (IMSI) number
2. metadata about calls like who you are dialing and duration of call
3. intercept the content of SMS and voice calls
4. intercept data usage, such as websites visited.

Secure Messaging – Why?
Example: Signal

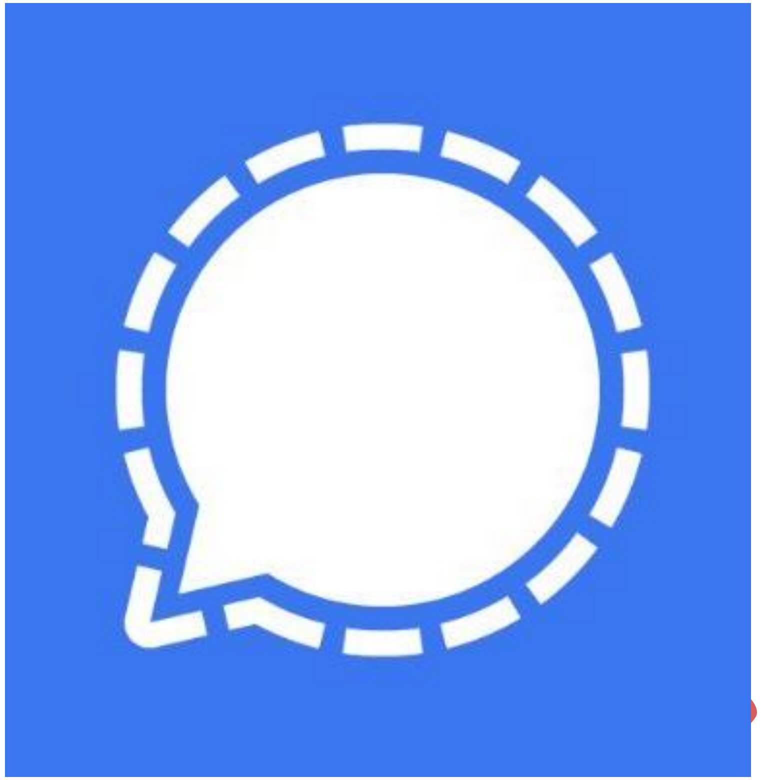
Encrypt your messages to protect your privacy

Prevent interception of your messages

Provide end-to-end encryption to ensure only the intended recipient can read your messages

Do not store your messages on their servers, making it less likely for them to be accessed by unauthorized parties

They offer additional security features such as self-destructing messages and two-factor authentication



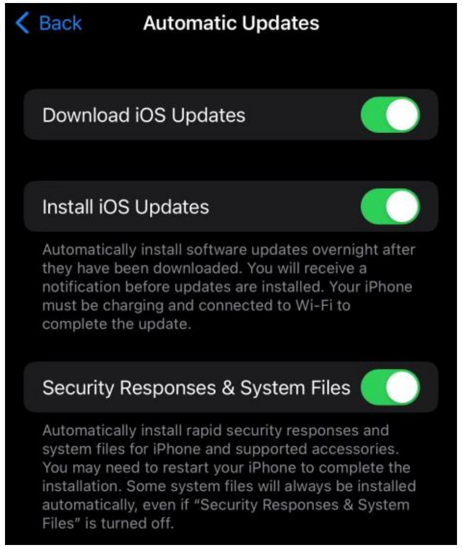
Keep Your OS and Apps Updated

Updating helps defend against known vulnerabilities

Enable automatic updates or check for updates frequently in the options menu

Install updates as soon as they become available

Staying up to date keeps your device secure and ahead of adversaries.



Automatic Updates

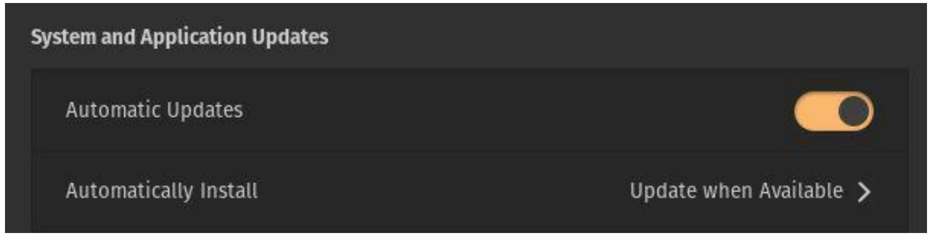
Download iOS Updates

Install iOS Updates

Automatically install software updates overnight after they have been downloaded. You will receive a notification before updates are installed. Your iPhone must be charging and connected to Wi-Fi to complete the update.

Security Responses & System Files

Automatically install rapid security responses and system files for iPhone and supported accessories. You may need to restart your iPhone to complete the installation. Some system files will always be installed automatically, even if "Security Responses & System Files" is turned off.



System and Application Updates

Automatic Updates

Automatically Install — Update when Available

Miscellaneous Tips

Beware of "Juice Jacking": a cyberattack that can occur when you charge your device in a public area. Stay safe by using a plug-to-outlet charger or a **data blocker** to prevent unauthorized access to your data.

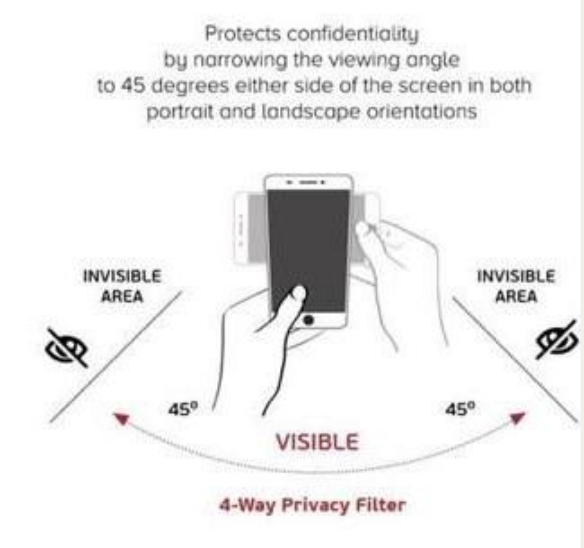
Use a **privacy screen** for your phone and laptop to protect your screen from prying eyes, especially in public spaces.

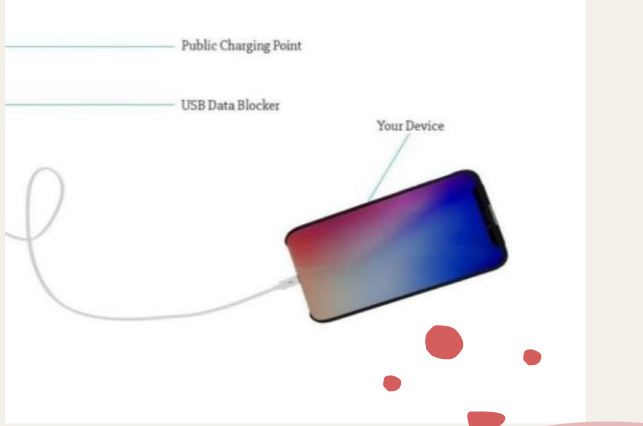
Protect your webcam: hackers can gain access without your knowledge. Use a **webcam cover** that you can easily open or close.

RFID Blocking: Use RFID-blocking wallets and bags to prevent skimmers from stealing your credit card or passport information.

Did you know that hackers could access your webcam without your permission?

The only way to protect your privacy is to cover the camera when you are not using it.

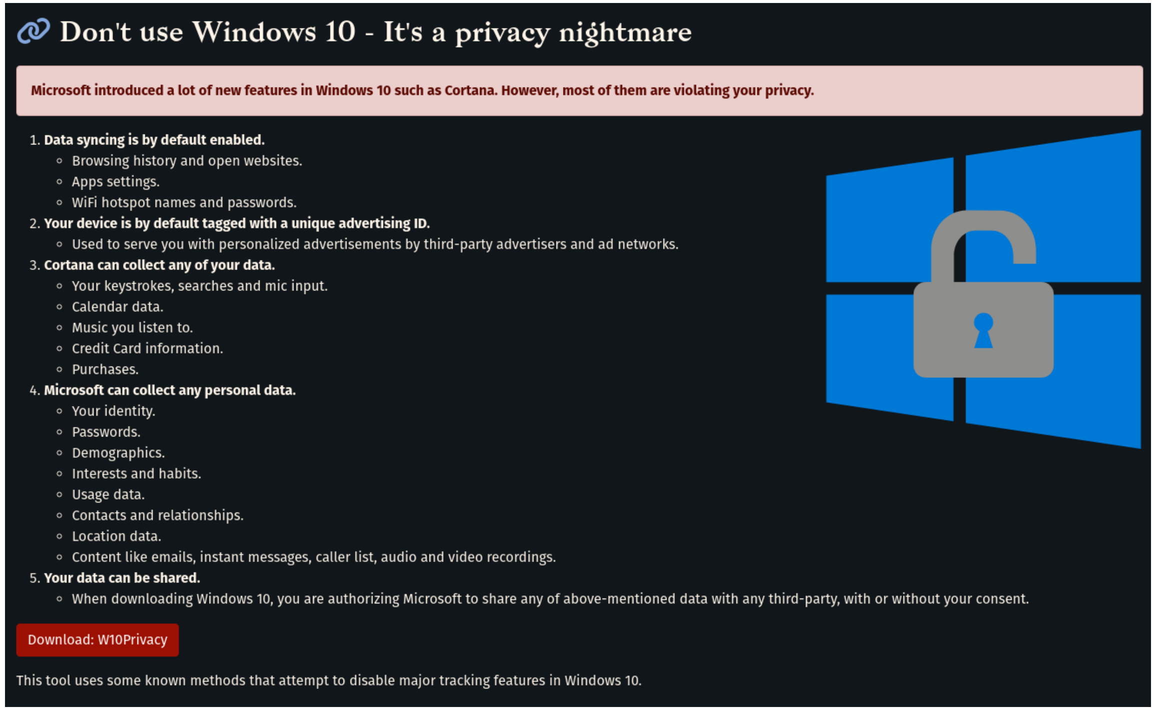

Protects confidentiality by narrowing the viewing angle to 45 degrees either side of the screen in both portrait and landscape orientations



Issues with Windows

Windows:

- **Mandatory Accounts**: Often requires a Microsoft online account for installation.
- **Invasive Telemetry**: Collects broad data including typing, browsing history, and more.
- **Limited Offline Installation**: Microsoft pushing for always-online installations.



Don't use Windows 10 - It's a privacy nightmare

Microsoft introduced a lot of new features in Windows 10 such as Cortana. However, most of them are violating your privacy.

1. **Data syncing is by default enabled.**
   - Browsing history and open websites.
   - Apps settings.
   - WiFi hotspot names and passwords.
2. **Your device is by default tagged with a unique advertising ID.**
   - Used to serve you with personalized advertisements by third-party advertisers and ad networks.
3. **Cortana can collect any of your data.**
   - Your keystrokes, searches and mic input.
   - Calendar data.
   - Music you listen to.
   - Credit Card information.
   - Purchases.
4. **Microsoft can collect any personal data.**
   - Your identity.
   - Passwords.
   - Demographics.
   - Interests and habits.
   - Usage data.
   - Contacts and relationships.
   - Location data.
   - Content like emails, instant messages, caller list, audio and video recordings.
5. **Your data can be shared.**
   - When downloading Windows 10, you are authorizing Microsoft to share any of above-mentioned data with any third-party, with or without your consent.

This tool uses some known methods that attempt to disable major tracking features in Windows 10.

Desktop - Linux

Privacy & Anonymity: No mandatory account for usage; minimal to no telemetry.

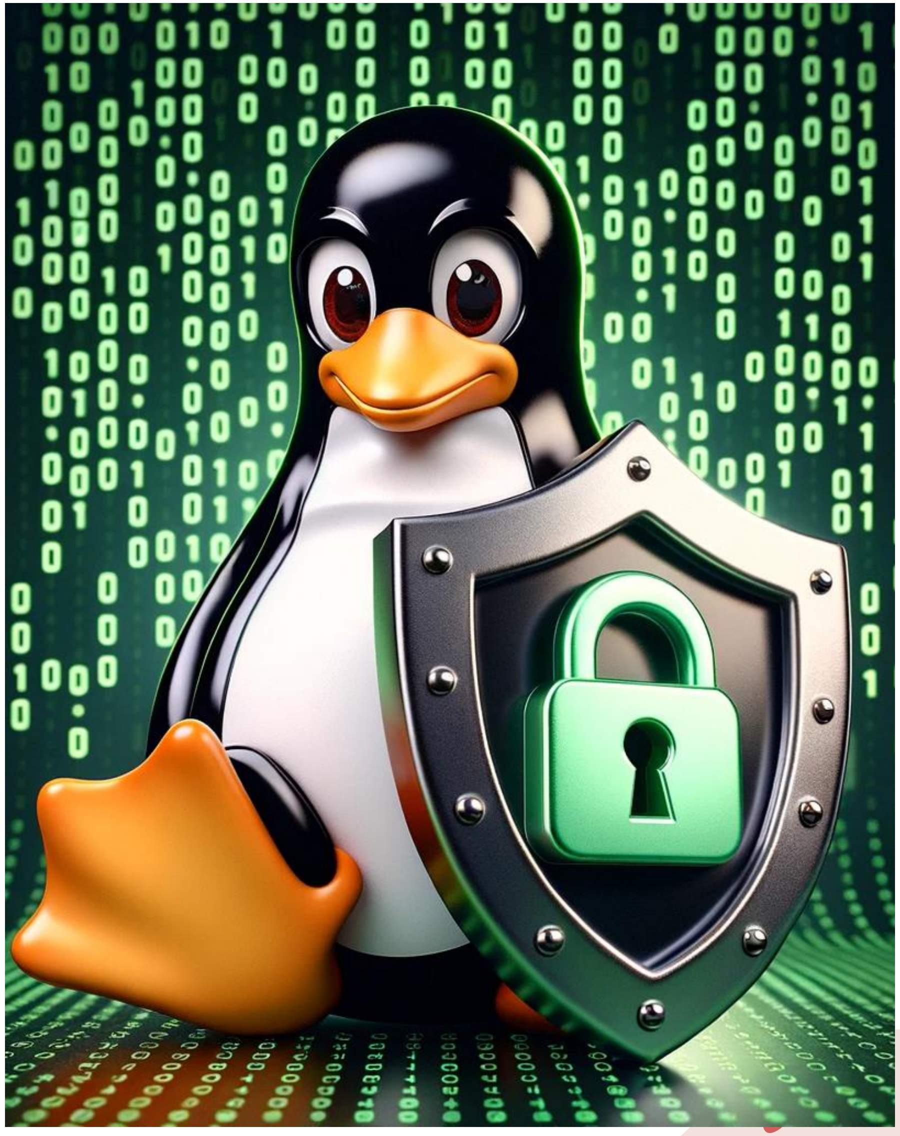
Security: Fewer threats than Windows; superior to macOS in terms of privacy.

Open Source: Transparent and auditable code; trusted by global communities.

Customizability: Full control over software; no forced default apps.

Efficiency: Lightweight OS, optimized for both new and legacy hardware.

Hardware Flexibility: Suitable for diverse hardware; easy component modifications.



GrapheneOS: Where Privacy Meets Practicality

Why Switch to GrapheneOS?

Top-Tier Security: Advanced protections beyond standard Android, including robust app sandboxing.

Memory Defense: Hardened memory allocator to thwart exploitation techniques.

Trustworthy Verification: Device integrity checks with the Auditor app.

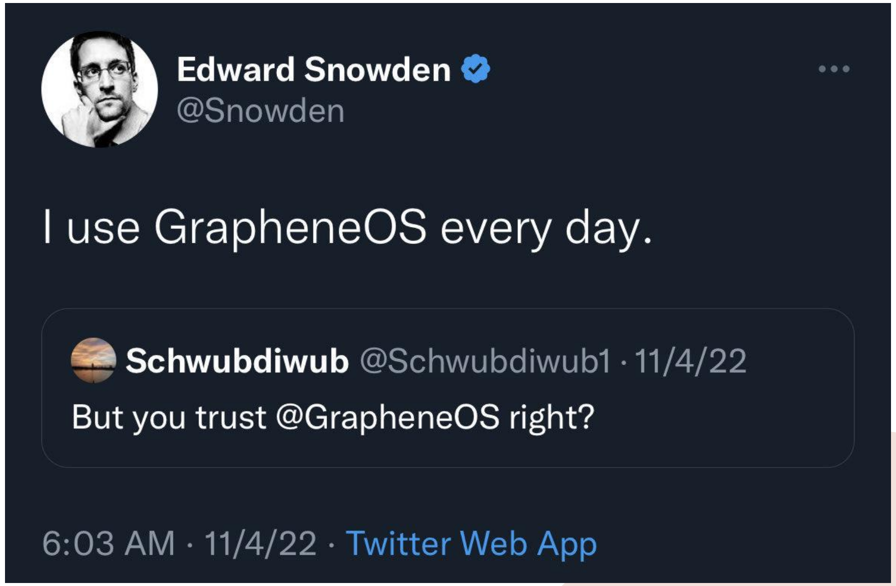
Sleek & Clean: No bloatware, ads, or unnecessary services. Minimal attack surface.

Physical Privacy: Enhanced controls over camera & microphone access.

Swift Updates: Stay protected with frequent security patches.

True Open Source: Transparent, peer-reviewed, and community-driven.

Android App Compatible: Security without sacrificing your favorite apps.



Edward Snowden
@Snowden

I use GrapheneOS every day.

Schwubdiwub @Schwubdiwub1 · 11/4/22
But you trust @GrapheneOS right?

6:03 AM · 11/4/22 · Twitter Web App

Private Payments

Cash: Traditional, private, but with reporting laws for large sums.

Prepaid & Gift Cards: Buy with cash; limitations based on merchant policies.

Online Marketplaces: Use cryptocurrency for gift cards; different account limits.

Virtual Cards: Mask banking info; not entirely anonymous.

Cryptocurrency: Digital, decentralized; public chains lack privacy.

Privacy Coins: Offer transaction anonymity; subject to scrutiny.

Wallet Custody: Choose noncustodial for greater control and privacy.

Acquisition Tips: Securely get privacy coins like Monero/Zcash

Safety Measures: Wear nondescript attire in-person; use Tor/VPNs online.

Digital Minimalism Checklist

o **Declutter Computers:** Remove bloatware and uninstall unused programs to streamline your computer's performance.

o **Effective Uninstall:** When removing programs, ensure you clean up any remnants to avoid clutter.

o**File Management:** Delete unnecessary files and move non-essential data to external drives for efficient storage.

o**Spyware:** Be cautious about spyware and unwanted software during installations.

o**Minimalist Approach:** Embrace digital minimalism to prioritize what truly matters in your digital life.

Secure Your Crypto Like a Pro

From wallet basics to advanced security techniques, all in one place.

Strategies to defend against phishing, malware, and social engineering attacks.

Step-by-step instructions to implement top security practices immediately.

Contribute to the guide, share your experiences, and learn from others.

Peace of Mind 🌟

Guide: https://github.com/iAnonymous3000/cryptocurrency-wallet-opsec

Aura >9000

Resources

- **VirusTotal:** Analyze suspicious files and URLs to detect types of malware.

https://www.virustotal.com/gui/home/url

- **Blacklight by The Markup:** A real-time website privacy inspector.

https://themarkup.org/series/blacklight

- **Exodus Privacy:** Understand the permissions, trackers behind apps.

https://exodus-privacy.eu.org/en/

- **Dangerzone:** Convert potentially dangerous PDFs or office documents into safe ones.

https://dangerzone.rocks/

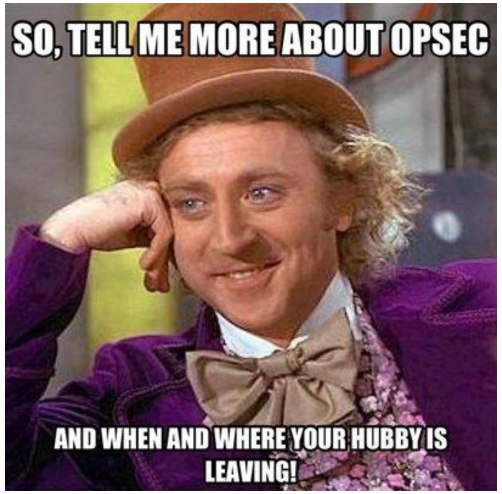
- **Device Info:** Detailed information about your device and its capabilities.

https://www.deviceinfo.me/

- **Terms of Service; Didn't Read (ToS;DR):** Get informed about the terms and conditions and privacy policies you're agreeing to.

https://tosdr.org/

Questions & Clarifica tions?


SO, TELL ME MORE ABOUT OPSEC
AND WHEN AND WHERE YOUR HUBBY IS LEAVING!

- **Your Input Matters:** We welcome your questions and doubts.

- **Thank You:** We appreciate your involvement and look forward to your questions.