



Security Awareness Workshop

null NEU + Google DSC

At Northeastern University

Disclaimer



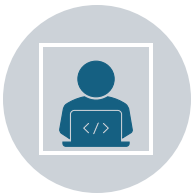
The information presented is for educational purposes only.



No endorsement of specific products or services is implied.



The workshop is not sponsored by any company.



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 two 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.
- **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)



QR Code - Best Practices



Inspect the QR Code: Before scanning, visually inspect the QR code for any signs of tampering or alterations. If it looks suspicious or out of place, exercise caution.



Verify the Source: Ensure that the QR code comes from a trusted and legitimate source. Be cautious when scanning QR codes from unknown or unverified locations.



Avoid Unknown or Suspicious QR Codes: Do not scan QR codes from sources that you do not trust or that appear suspicious. When in doubt, refrain from scanning.



Use a Dedicated QR Code Scanner: Consider using a reputable and dedicated QR code scanning app with built-in security features. These apps may provide additional protection and analysis of QR code content.



Ask for Clarification: In public places like restaurants or retail stores, if you encounter a QR code that seems unusual, consider asking staff for clarification or guidance.

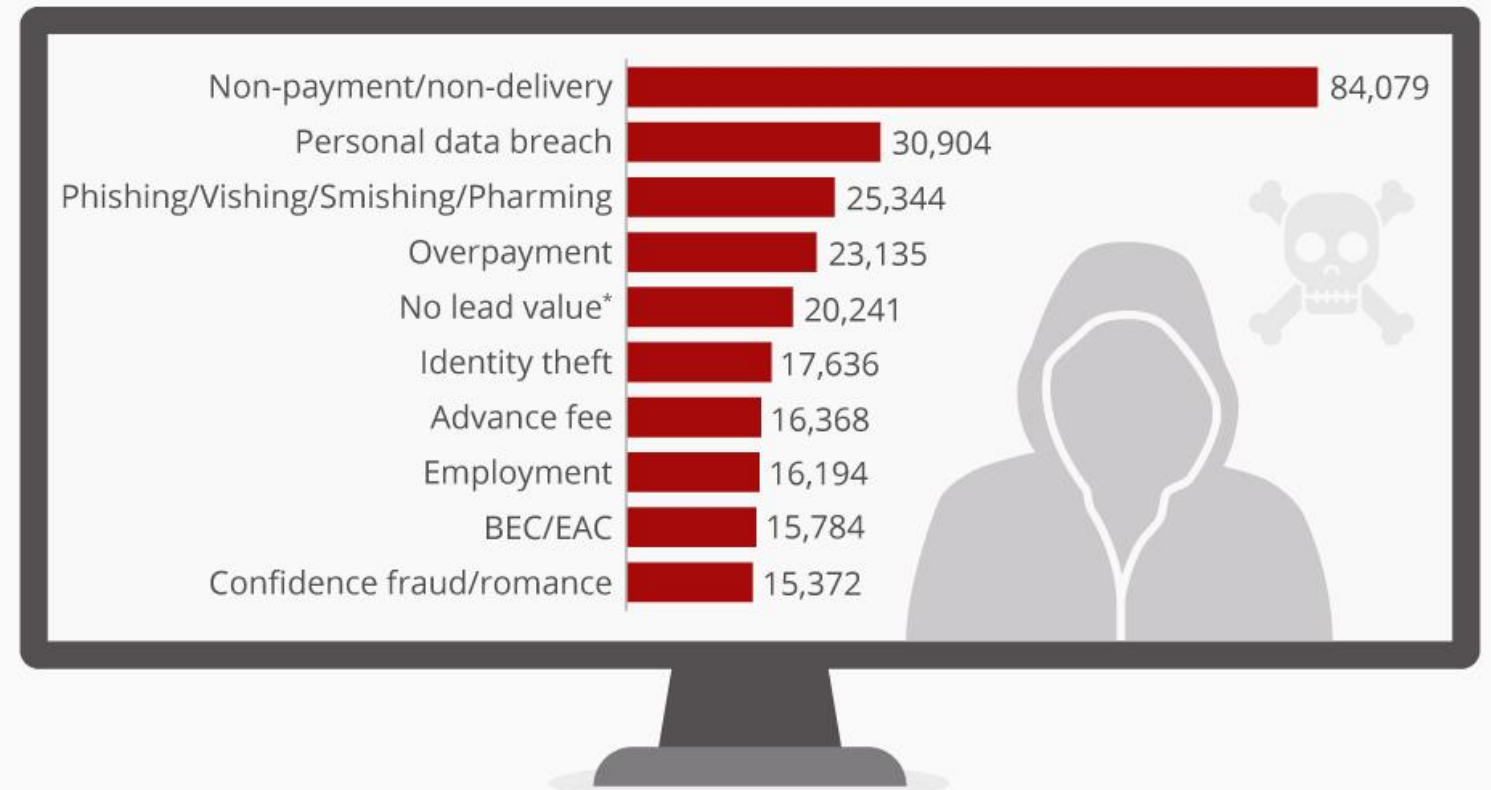


- Avoids financial losses
- Maintains business continuity
- Protects reputation
- Reduces the risk of malware on devices
- Prevent cyberbullying or harassment
- Prevent identity theft

Top Cybercrimes in the US

Top Cybercrimes in the U.S.

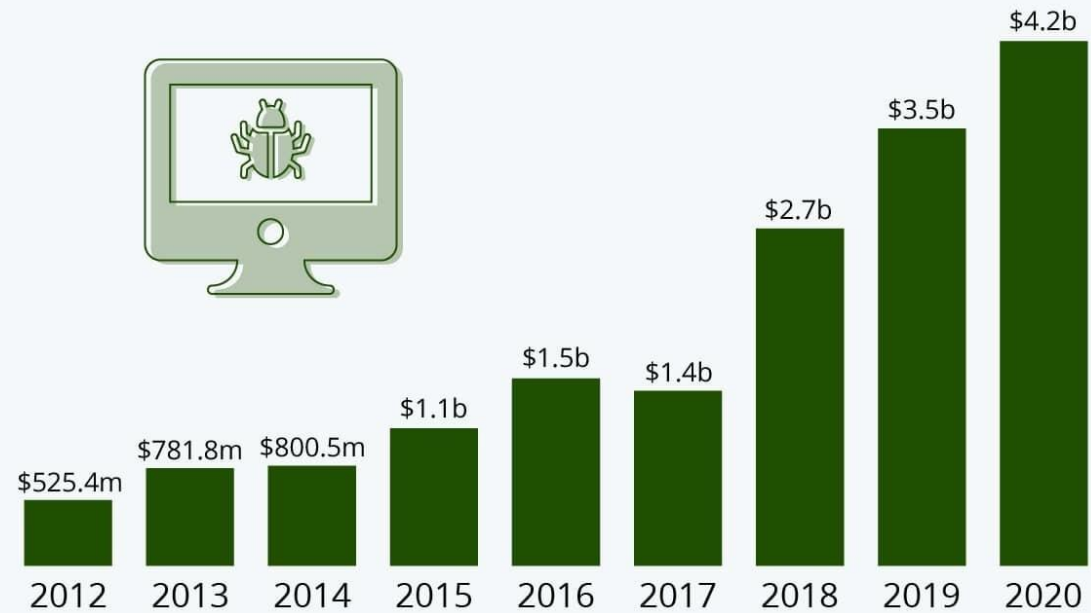
Types of cybercrime most frequently reported to the IC3 in 2017, by victim count



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

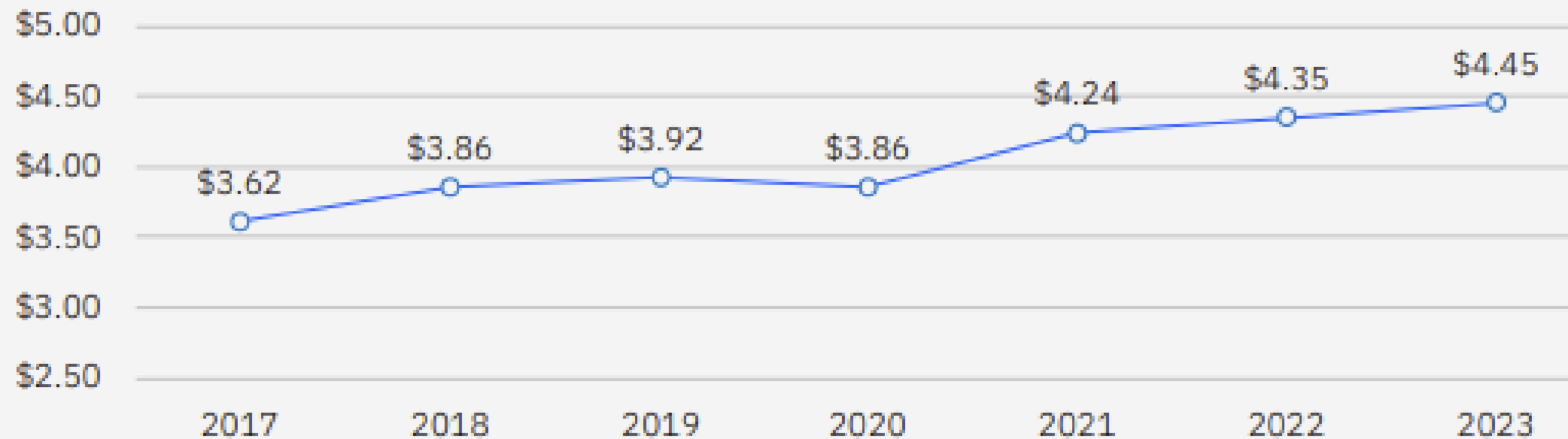


Source: FBI's Internet Crime Complaint Center



Average cost of a data breach in the United States from 2006 to 2023(in million U.S. dollars)

Total cost of a data breach





**YOU'LL TAKE SECURITY AWARENESS
TRAINING SERIOUSLY**

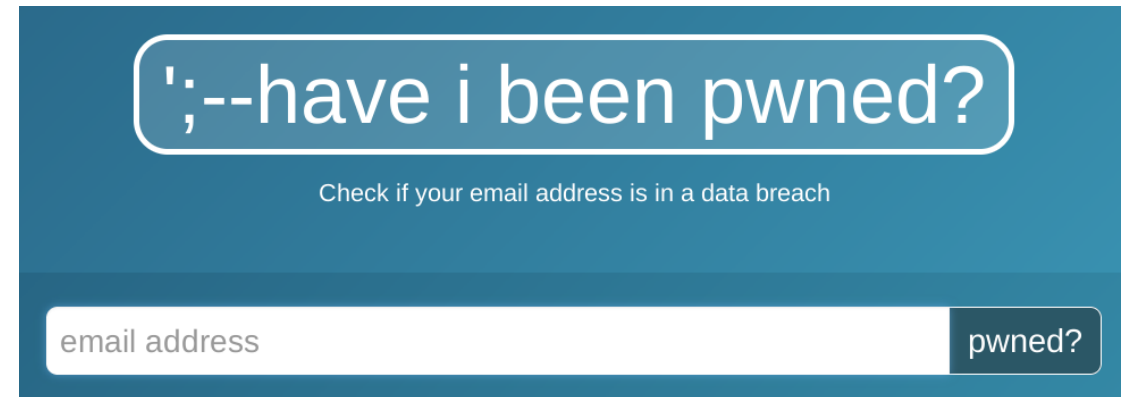


You are the final safeguard
against cyber threats. Take
action:

Be	Proactive Vigilance: Always be alert and cautious in your digital interactions.
Understand	Personal Responsibility: Understand that your actions have a direct impact on your digital safety.
Stay	Continuous Learning: Stay informed about evolving cyber threats and best practices.
Prioritize	Security-First Mindset: Prioritize security in all online activities, even if it means sacrificing convenience.
Share	Collaborative Approach: 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.

The image shows a screenshot of the 'have i been pwned?' website. The header is a dark blue rounded rectangle with the text 'have i been pwned?' in white. Below the header, the text 'Check if your email address is in a data breach' is displayed. At the bottom, there is a white input field with the placeholder text 'email address' and a dark blue button with the text 'pwned?' in white.

';--have i been pwned?

Check if your email address is in a data breach

email address pwned?

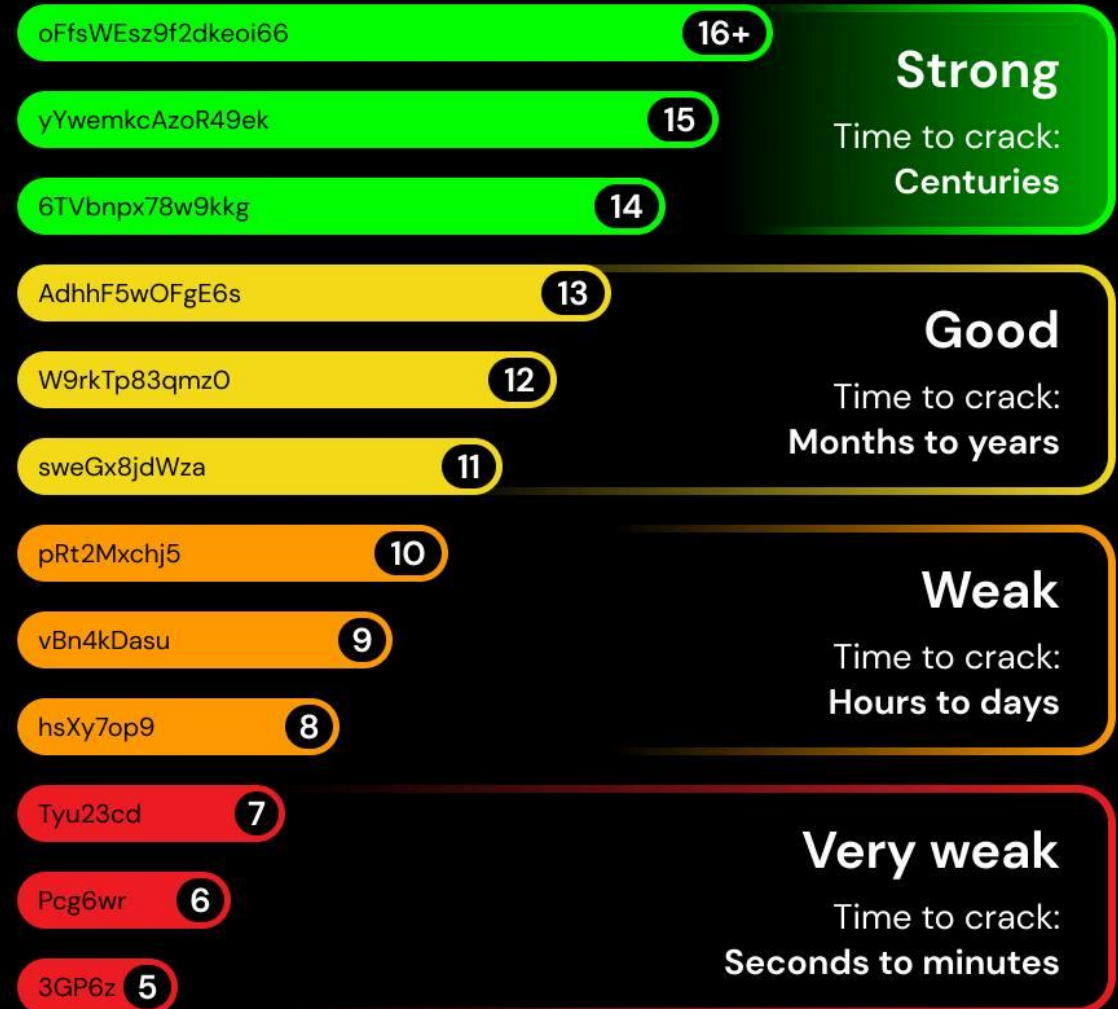
Passwords/Passphrases Don'ts

- **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

Password strength test chart



Number of characters

Minimum Criteria for Password Managers

- **Opensource for Transparency:** Password managers should be open source to ensure transparency and allow for community scrutiny.
- **Strong End-to-End Encryption (E2EE):** Passwords and sensitive data must be protected with robust end-to-end encryption to prevent unauthorized access.
- **Well-Documented Security Practices:** The password manager should have clear and well-documented security practices to ensure the safety of user data.
- **Audited by Reputed 3rd-Party:** Regular security audits by reputable third-party organizations should be conducted to verify the effectiveness of security measures.
- **Optional Telemetry:** Telemetry data collection should be optional, respecting user privacy preferences.
- **Minimal PII Collection for Billing:** If collecting personally identifiable information (PII) is necessary for billing purposes, it should be kept to a minimum to reduce privacy risks.
- **Tools:** Bitwarden, Proton Pass, KeePassXC



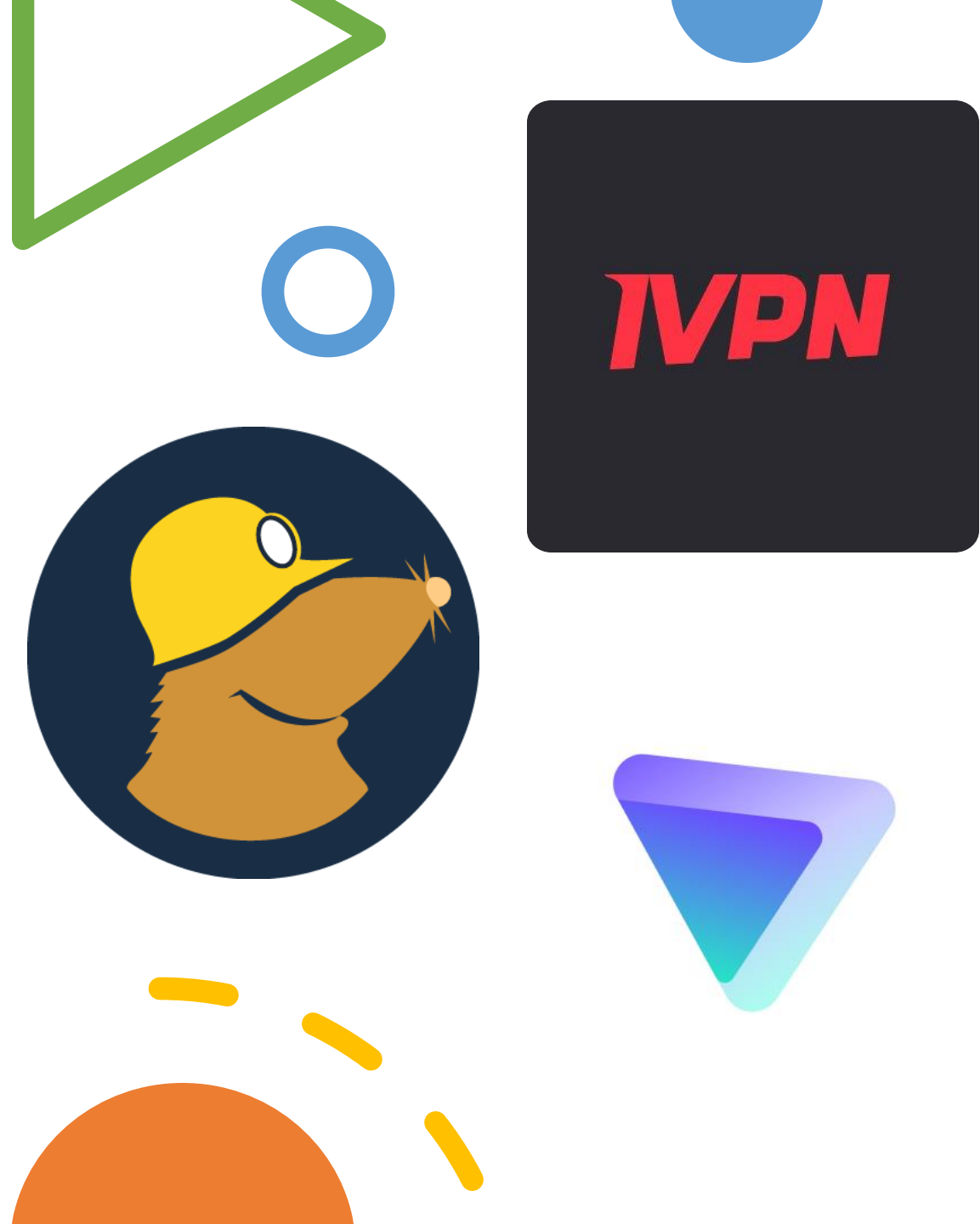
Social Media Safety Tips

- **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



Essential App Permission Tips for Android & iOS



Key Permissions:

Location, Camera, Microphone:
Grant judiciously.

Notifications:

Review visibility settings for
sensitive content.



Against Malware:

Android: Use Google Play Protect.
iOS: Rely on App Store's security
reviews.



Quick Tips:

Periodically audit permissions.
Update apps and OS regularly.
Remove suspicious apps
promptly.

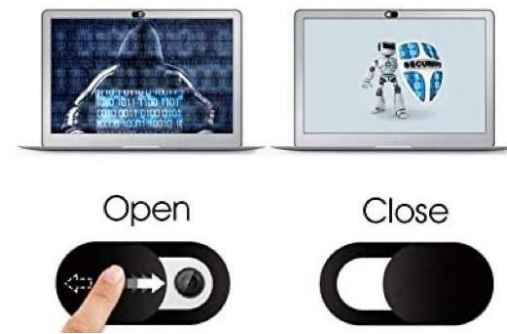
SquareX + GMail - Demo

- **Enhanced Privacy Mode:** Read emails without senders knowing.
- **Block Trackers:** Prevents email trackers from detecting when you open an email.
- **Simple Activation:**
 - **Install Extension:** Add SquareX to the Browser from sqr.x.com.
 - **Create Account:** Sign up for free.
 - **Enable Integration:** Activate 'Smart Integrations' in SquareX settings.
 - **Private Viewing:** Right-click emails and choose 'Preview in Enhanced Privacy Mode'.
- **Benefits:**
 - **Discreet Email Reading:** Open emails in a cloud-based Disposable File Viewer.
 - **Tracker-Free:** No sender alerts or tracking notifications.

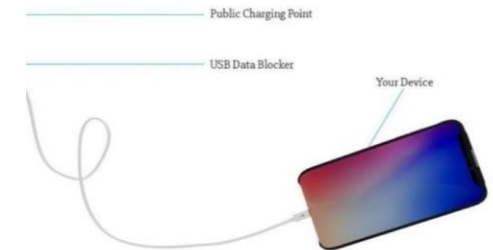
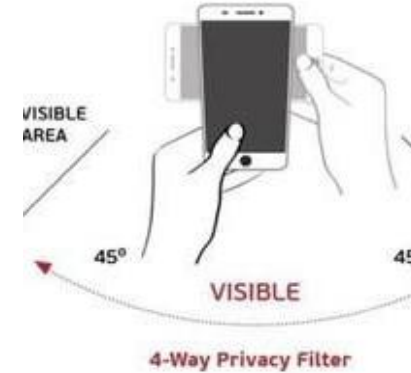


Securing Your Smart Home: IoT Device Safety

- **Manage Risks:**
 - Change default settings.
 - Regularly update device software.
- **Strengthen Defenses:**
 - Secure Wi-Fi with strong passwords.
 - Isolate IoT devices on a separate network.
- **Stay Vigilant:**
 - Monitor for strange device behavior.
 - Use two-factor authentication where possible.
- **Smart Choices:**
 - Select IoT products from reputable brands committed to security.



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

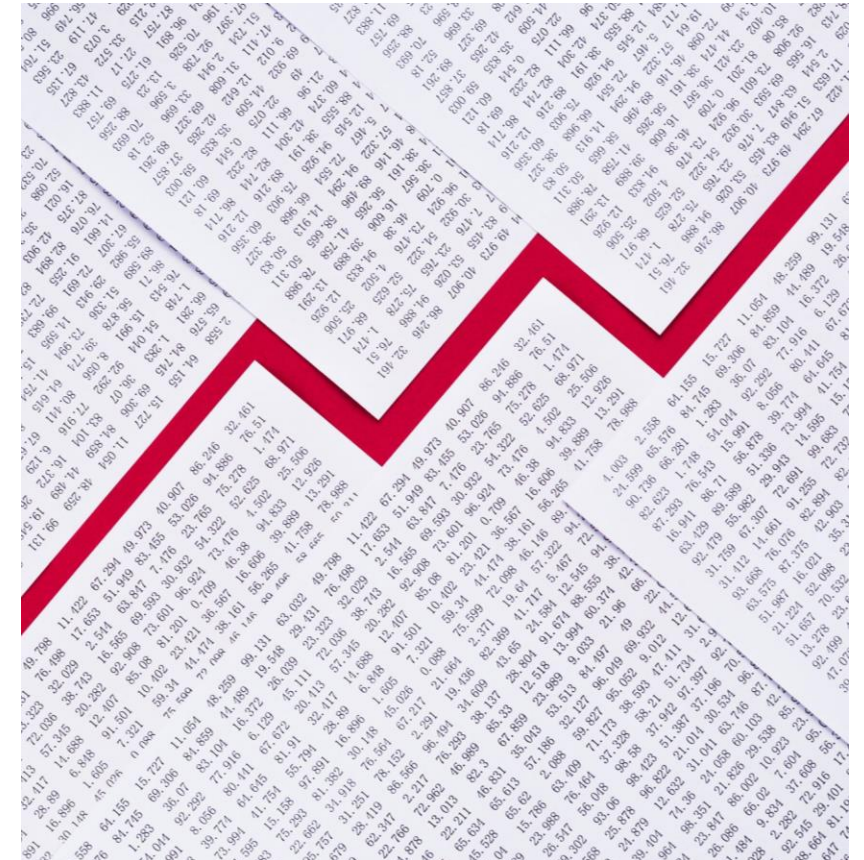


Miscellaneous

- 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.

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**
 - Hang up on suspicious calls.
 - Confirm via official contacts.
 - Block and report spam numbers.





Can You Spot a Phish? Take Google's Challenge!

- Interactive Phishing Quiz: Dive into real-life examples.
 - Test Your Skills: Can you tell a legit email from a phish?
 - Learn as You Play: Instant feedback with tips and tricks.
 - Boost Your Cyber Smarts: Elevate your defenses against cyber cons.
 - Action Step:
 - Try it now! [Google's Phishing Quiz](#)
-

Enhancing Google Account Security- Check Google Hardening Guide

Strong Passwords

- Use 12+ characters with a mix of symbols, numbers, and cases.
- Employ password managers for security.

Two-Factor Authentication

- Activate 2SV for added login security.
- Consider using physical security keys.

Phishing Protection

- Identify and report suspicious emails.

Regular Account Reviews

- Check for unknown activities.
- Update recovery options and app permissions.

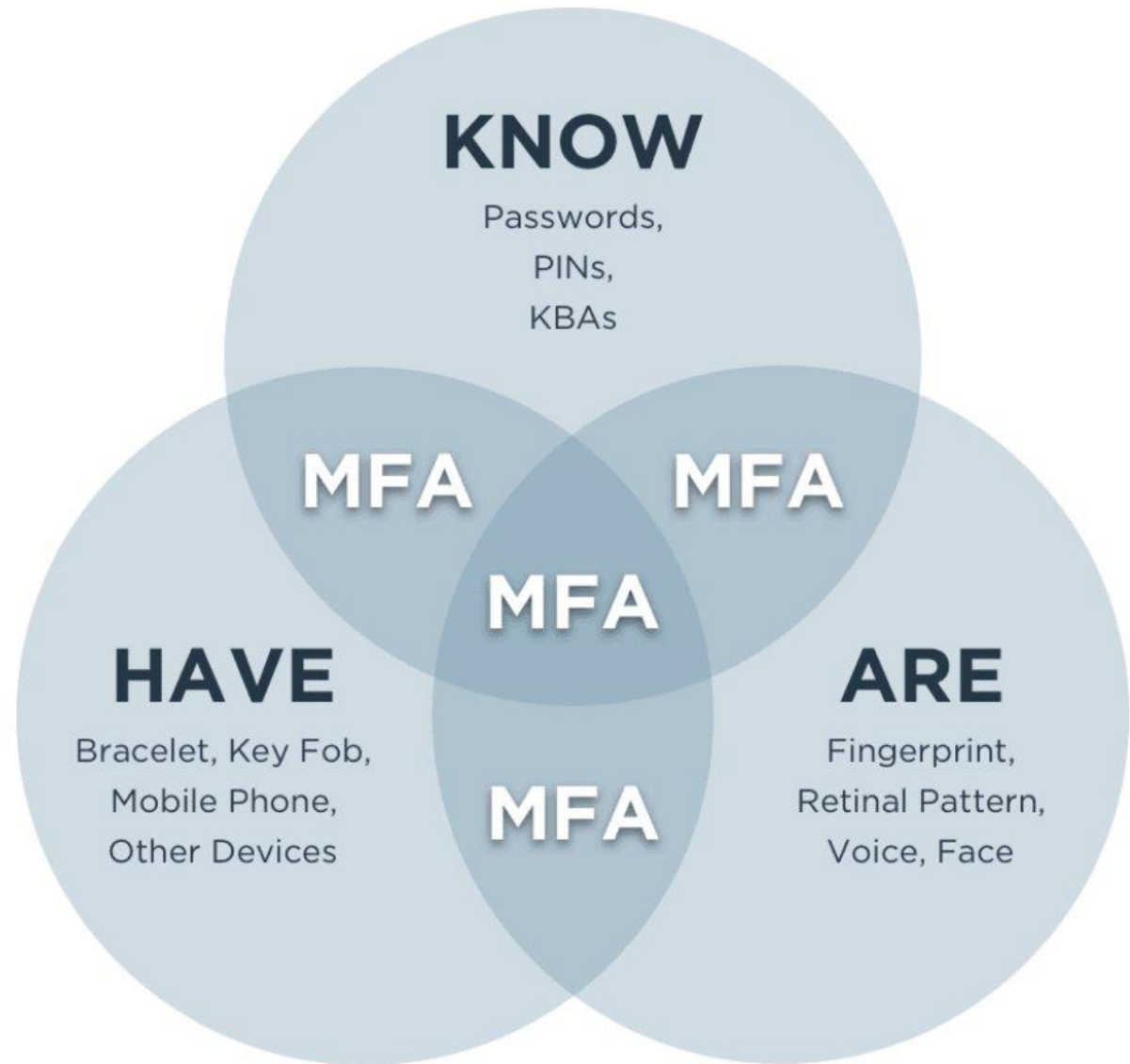
Multi-Factor Authentication (MFA)

- MFA is a security measure that requires users to verify their identity using two or more factors, such as a password and a fingerprint, before gaining access to an account.
- Provides an additional layer of security to prevent unauthorized access.
- Prevent over 95% of bulk phishing attempts and over 75% of targeted attacks. Example: NEU Cisco Duo



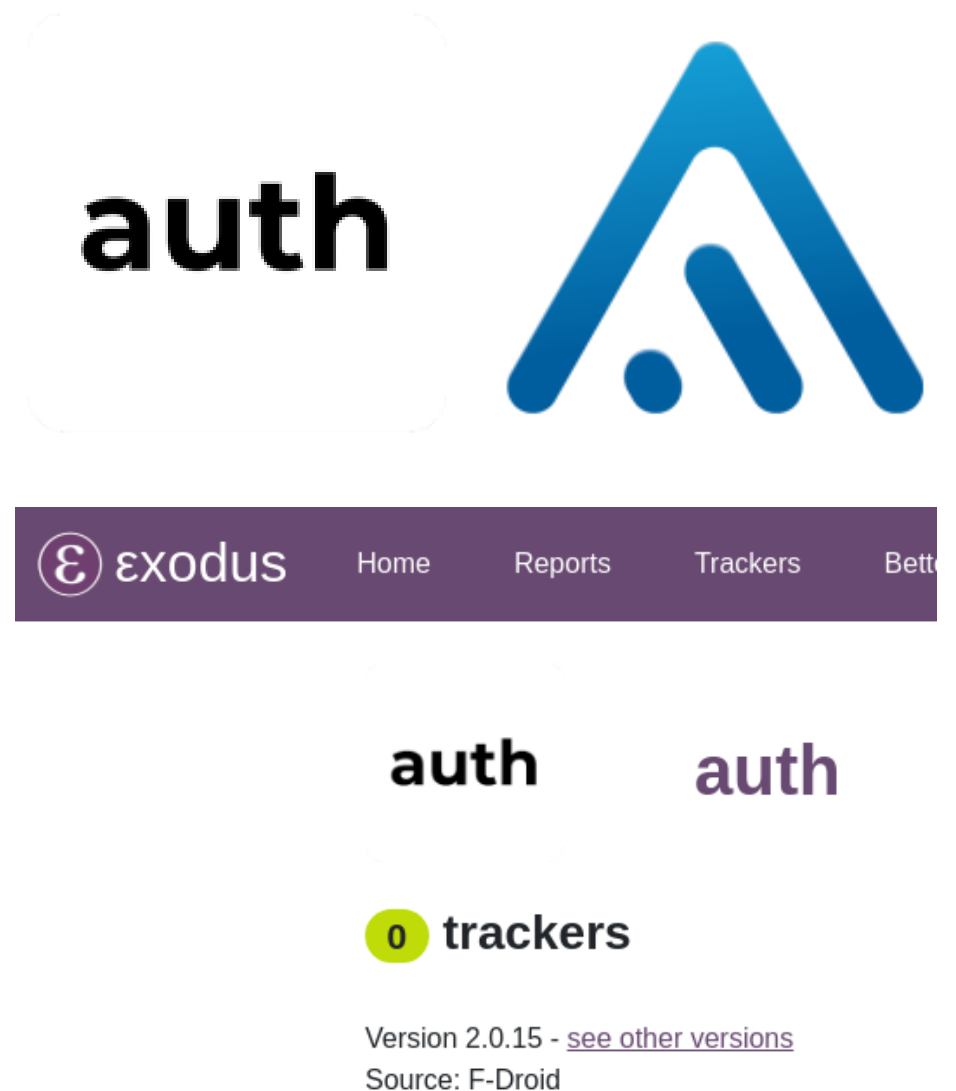
Types of MFA (aka Multi-Factor Authentication)

- 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
 - Check their code here - <https://github.com/ente-io/auth>
 - End-to-End Encrypted Backups
 - Multi-Device Support
 - Offline Mode
 - Cross-Platform
- Special Mention: Aegis Authenticator (Android)



Upgrade MFA?

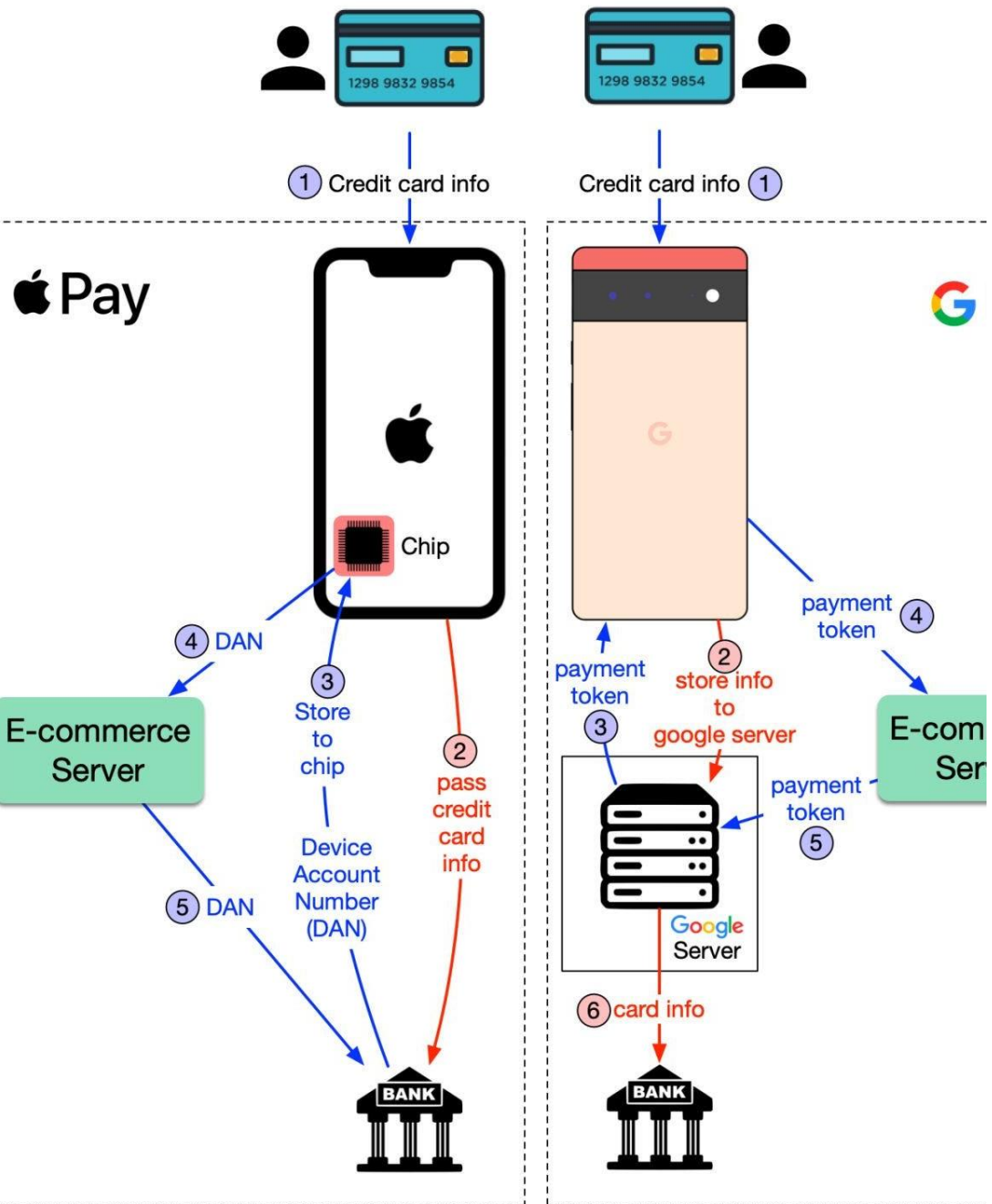
- Anti-Phishing: Bound to the website's URL, hardware keys offer robust protection against phishing.
 - No Shared Secrets: Eliminate the risk of code interception – keys don't rely on shared secrets.
 - Portability & Speed: A convenient solution across devices, often faster than SMS or app-based 2FA.
 - Impenetrable Physical Security: No physical key equals no access, securing your accounts even if your device is compromised.
-
- Recommended Tools: Yubikey, Nitrokey



Why Opt for Google Pay Over Traditional Cards?

- **Enhanced Security:**
 - Tokenization hides real card info.
 - Biometric verification for transactions.
- **Physical Risk Reduction:**
 - No risk of losing physical cards.
 - Contactless payments deter skimming.
- **Privacy and Control:**
 - Merchants get tokens, not card numbers.
- **Ease of Use:**
 - Instantly lockable if devices are lost.
 - Accepted widely for contactless payments.





Apple Pay vs. Google Pay

- **Tokenization:** Both use unique codes for transactions, keeping card details secure.
- **Storage & Privacy:**
 - Apple Pay: Stores token in-device on a secure chip.
 - Google Pay: Stores card info on servers; uses token for payments.
- **Authentication:**
 - Apple Pay: Requires biometric/passcode for all transactions.
 - Google Pay: Offers PIN bypass for quick payments.
- **Data Association:**
 - Apple Pay: No link to Apple ID.
 - Google Pay: Payment methods tied to Google account.

Pixel. The only phone engineered by Google.



New

Pixel 8 Pro



New

Pixel 8



Pixel 7a



Pixel Fold



Pixel 7 Pro



Pixel 7



Pixel 6a



Compare phones



New

Pixel cases

Why Choose Google Pixel Phones for Enhanced Mobile Security?

- Pixel's Security Edge:
 - Titan Chip: Dedicated security for unbeatable protection.
 - Verified Boot: Ensures only trusted software runs at startup.
- Longevity Benefits:
 - Extended Updates: 7+ years of security updates from Pixel 8 onwards.
 - Buy New: Longer support means better security over the device's life.
- Verdict: Google Pixel delivers superior hardware security and the longest update support in the Android ecosystem, making it the top recommendation for security-conscious consumers.

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

••••• AT&T 4G 3:50 PM 100%
< Messages (1) +1 (202) 609-0301 Details

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](tel:+17038798780) 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.

+1 (951) 923-6938 >

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/WYmoR8tOIPS

+1 (323) 356-7217 >

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

Secure Browsing

- **Secure Connections:** Prefer sites with 'HTTPS' over 'HTTP'.
- Be cautious about pop-up ads and never click on them
- Avoid downloading files or software from untrusted websites
- Comprehensive Comparison of Browsers: privacytests.org
- Use a private & secure browser: Examples: Brave, Mullvad



How to prevent & respond to cyberbullying?



Block the bully & report the behavior to the appropriate authority or platform.



Don't respond or retaliate, as this can make the situation worse.



Talk to someone you trust about what's happening.



Encourage a positive and respectful online culture by not engaging in cyberbullying and reporting any instances you witness.

Recognizing and Responding to Device Compromise



Signs of Compromise:

Slow performance, crashes, or unknown apps.

Spike in data usage.

Strange account activities.



What to Do:

Disconnect: Immediately take your device offline.

Scan: Use trusted antivirus to identify malware.

Passwords: Change them for all online accounts.



Update: Install the latest software and app updates.



Expert Help: Consider professional cybersecurity assistance if needed.



Prevention:

Regular backups.

Update security software.

Exercise caution with downloads and attachments.

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



Super
Important
Resource

