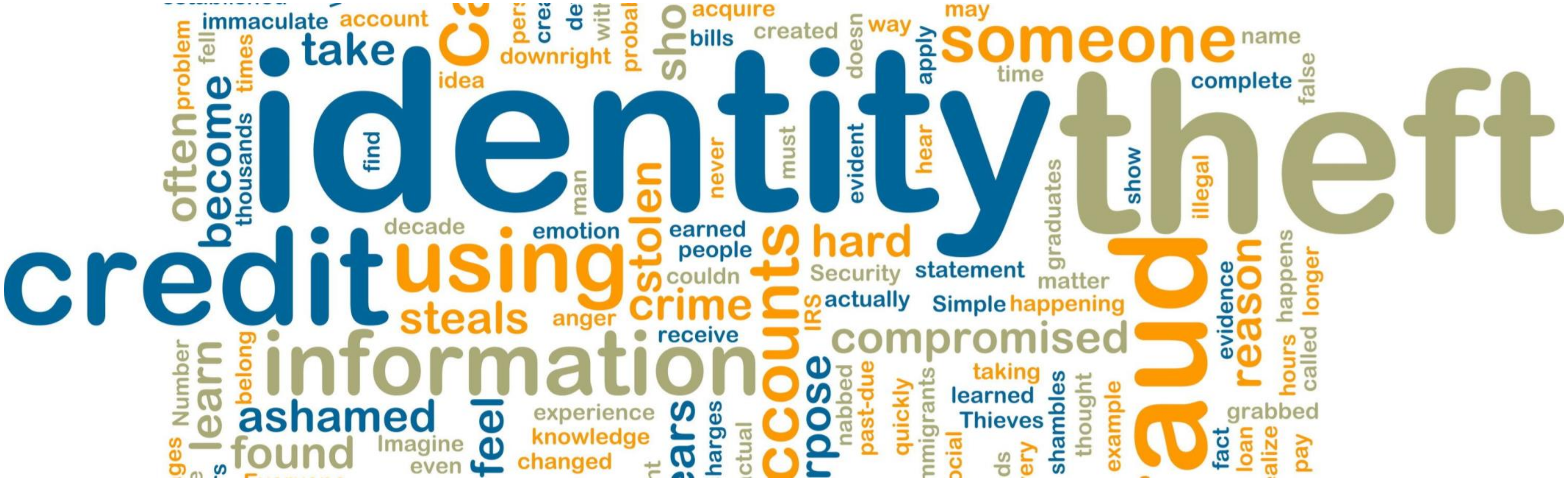
Cybersecurity Awareness Training by null NEU

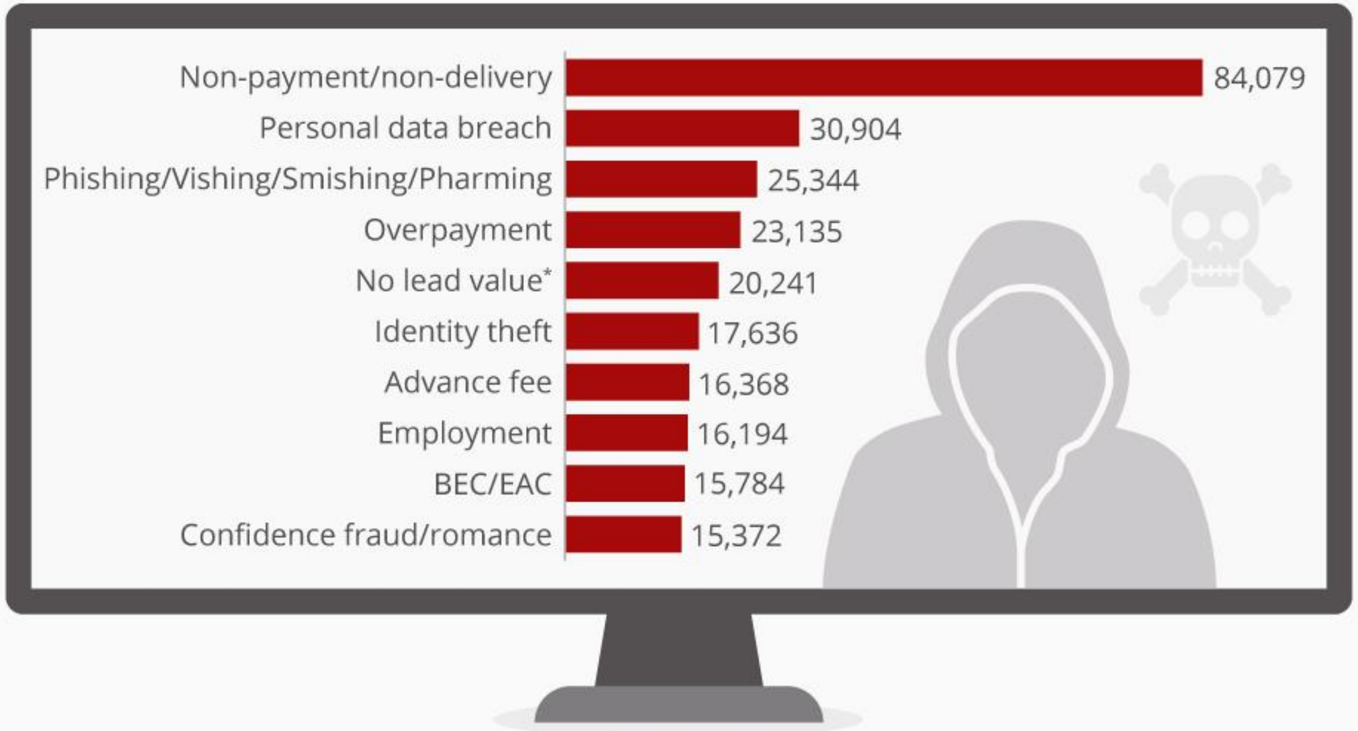
From Awareness to Action: Your Complete Guide to Cybersecurity



Importance of Security Awareness

- 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

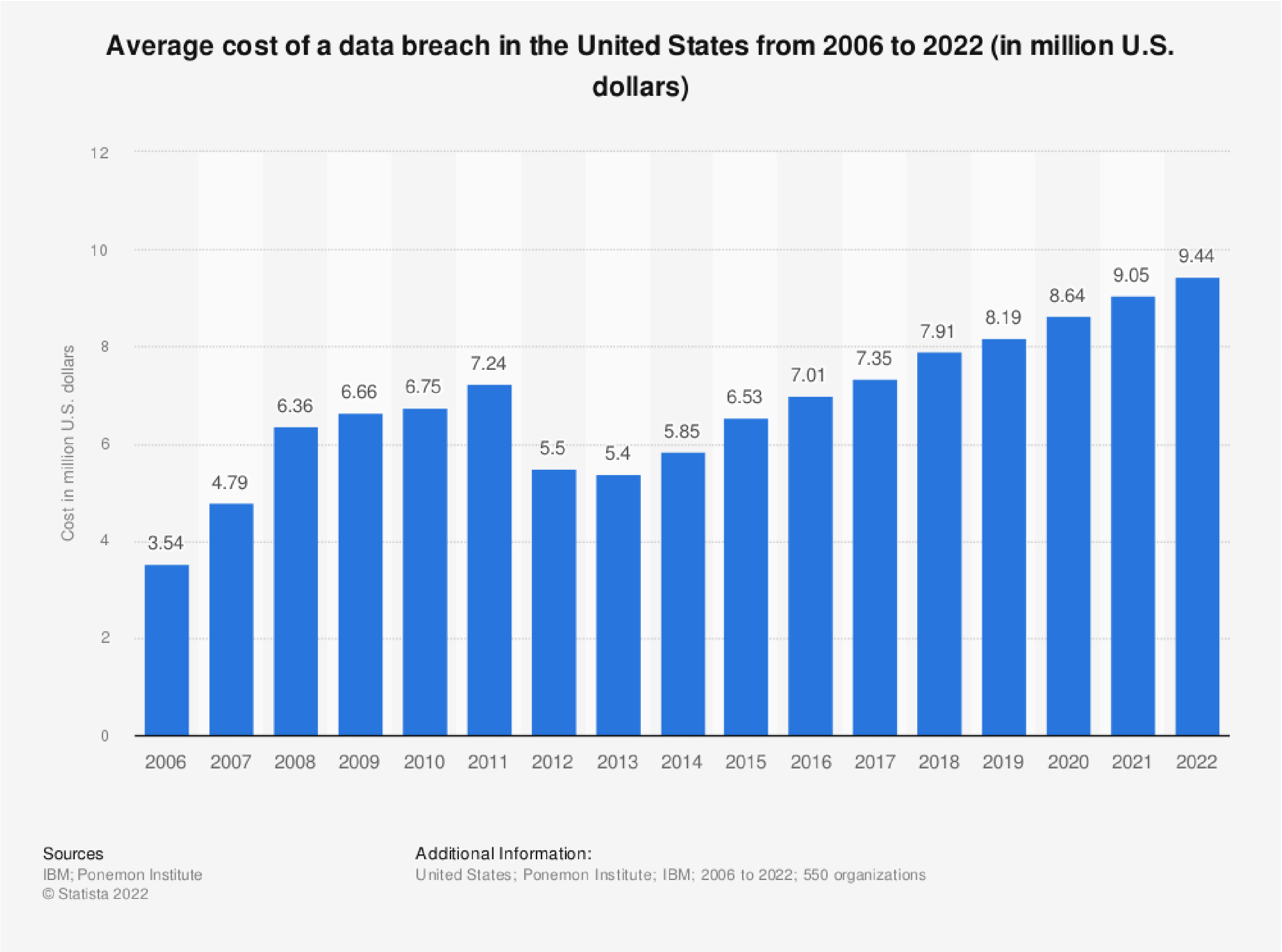
* Incomplete complaints which do not allow a crime type to be determined

Sources: Internet Crime Complaint Center Annual Report; FBI

@StatistaCharts

statista

Average cost of a data breach in the United States from 2006 to 2022

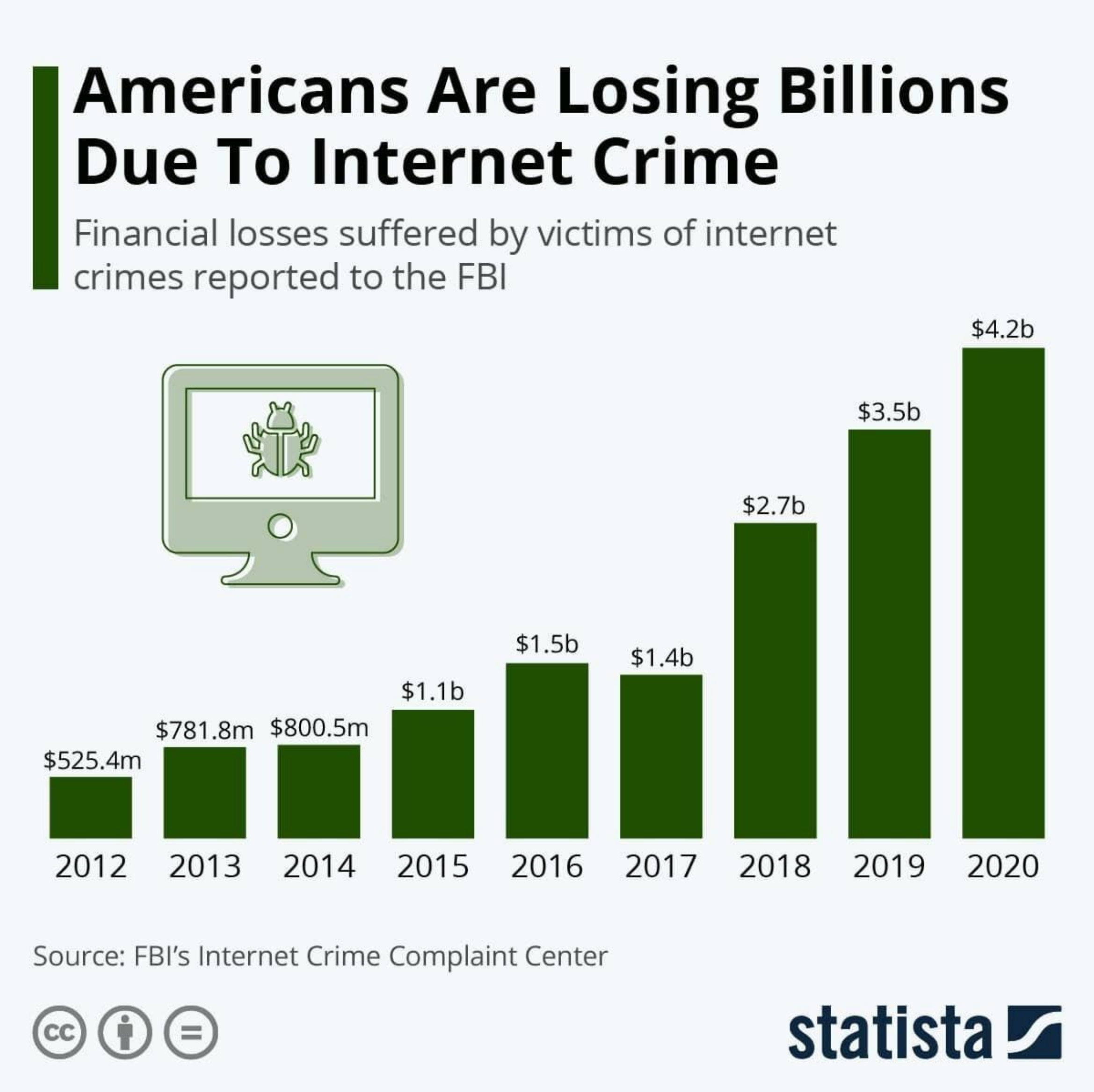


Average cost of a data breach in the United States from 2006 to 2022 (in million U.S. dollars)

Sources
IBM; Ponemon Institute
© Statista 2022

Additional Information:
United States; Ponemon Institute; IBM; 2006 to 2022; 550 organizations

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

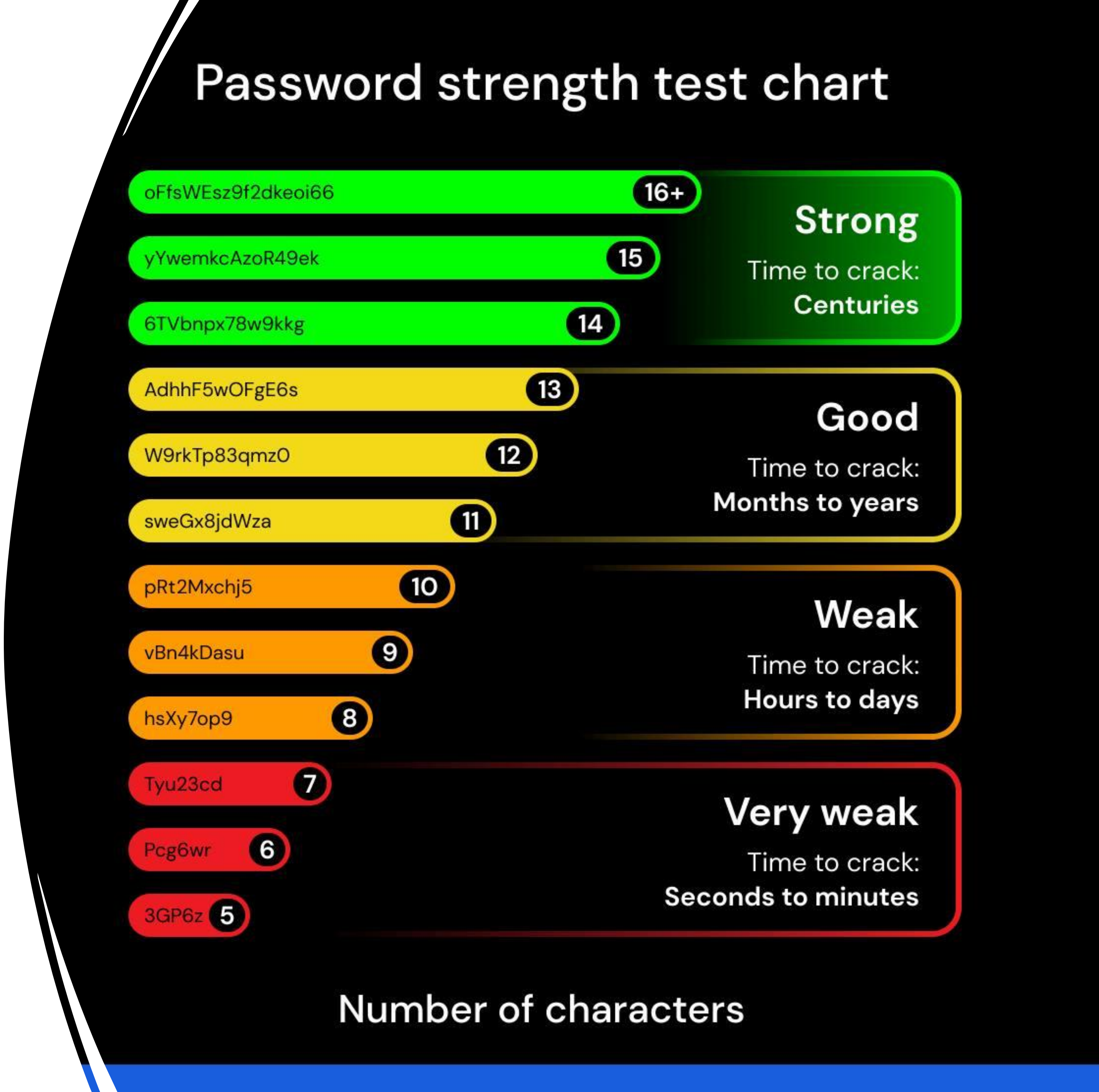
Source: FBI's Internet Crime Complaint Center

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**

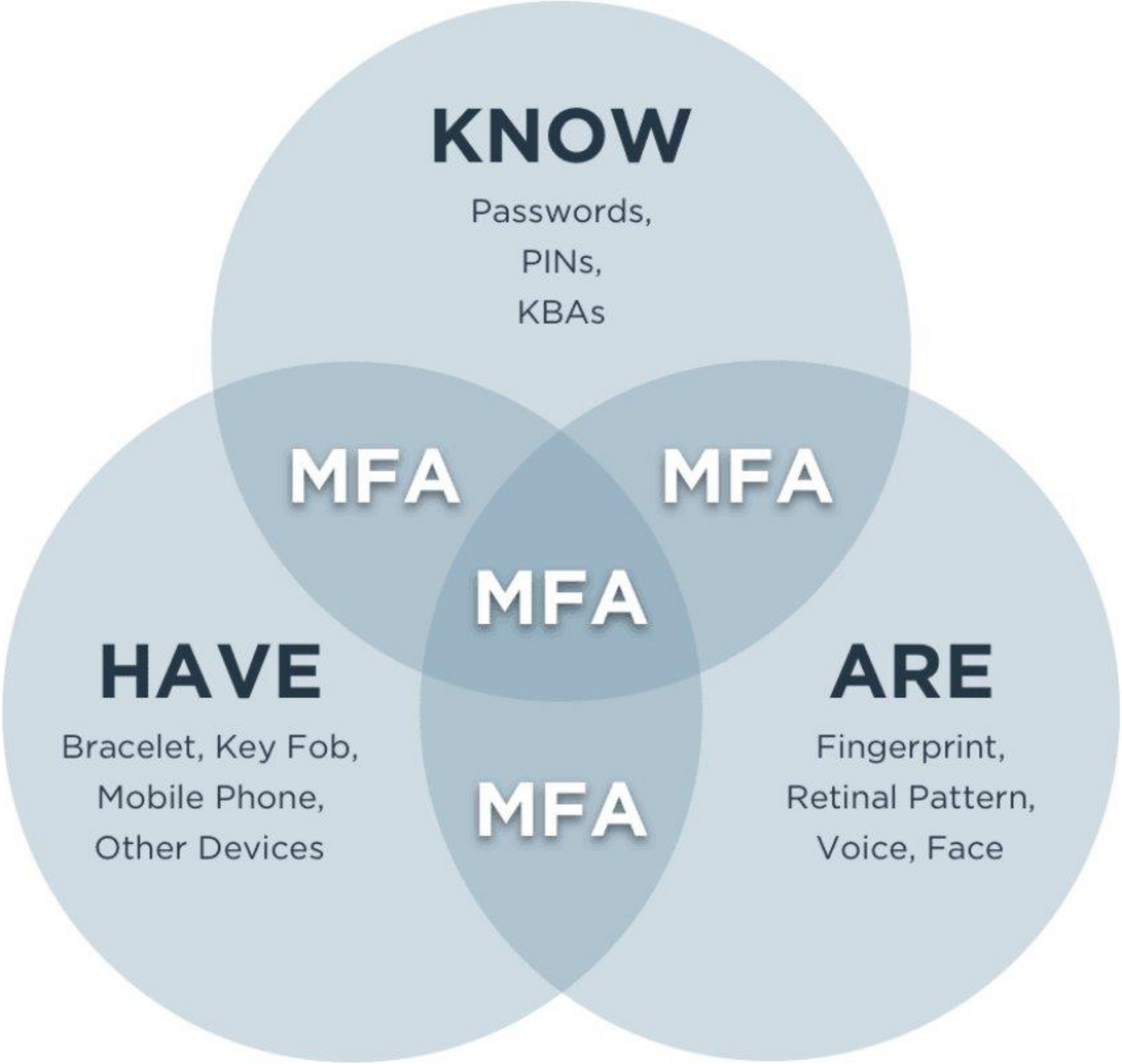


Multi-Factor Authentication (MFA)

- 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.

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



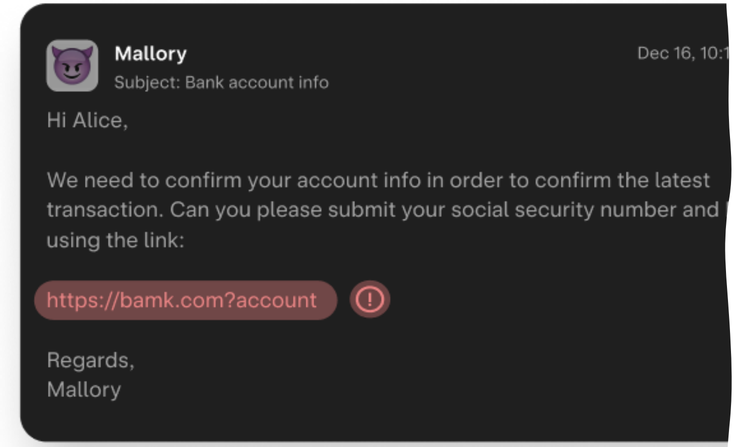
Phishing Scams & Secure Email Services

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, Skiff Mail**

Examples of Phishing Scams



Mallory

Subject: Bank account info

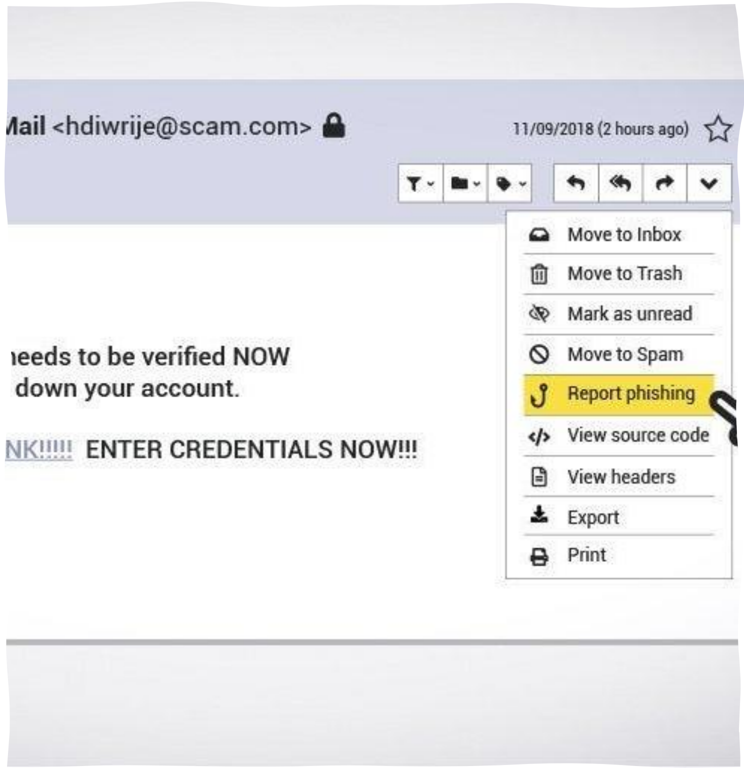
Dec 16, 10:1

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

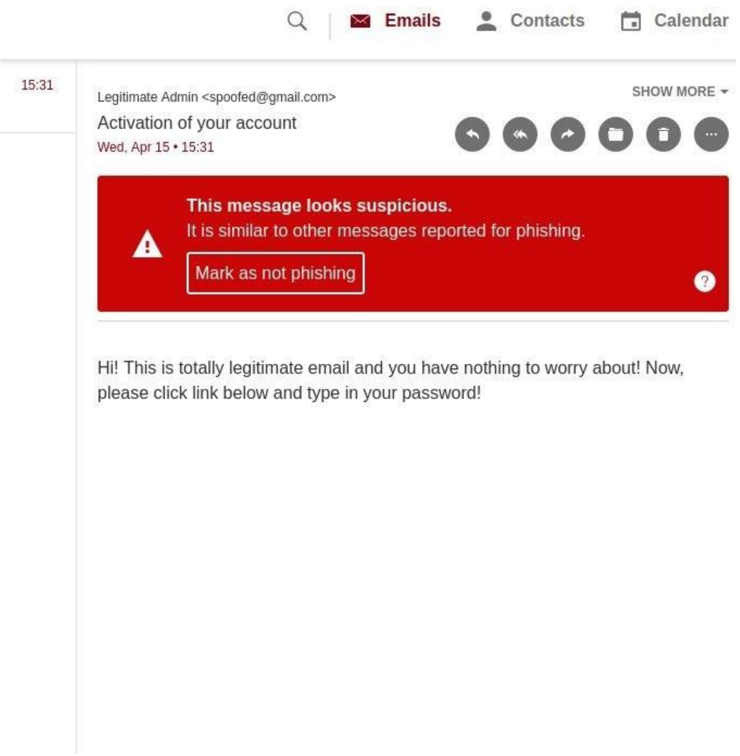


Mail <hdiwrije@scam.com>

11/09/2018 (2 hours ago)

needs 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.

Mark as not phishing

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

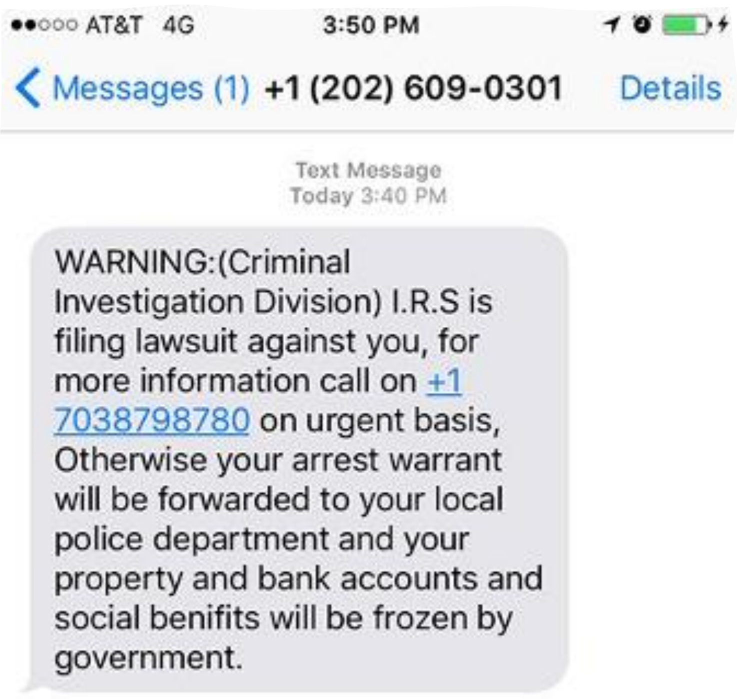
SMS Scams aka Smishing

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

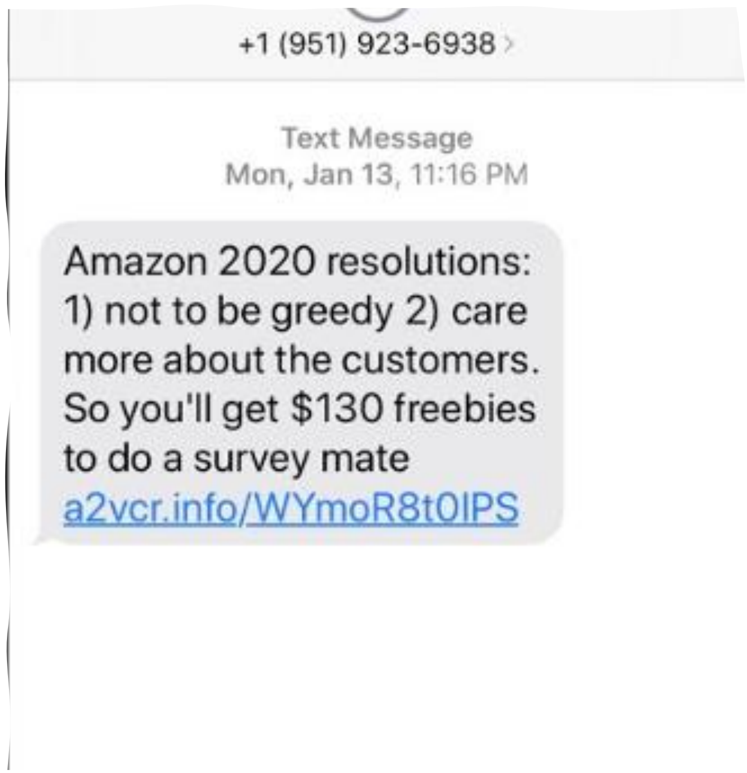
Examples of Smishing


●●○○○ AT&T 4G 3:50 PM

+1 (202) 609-0301

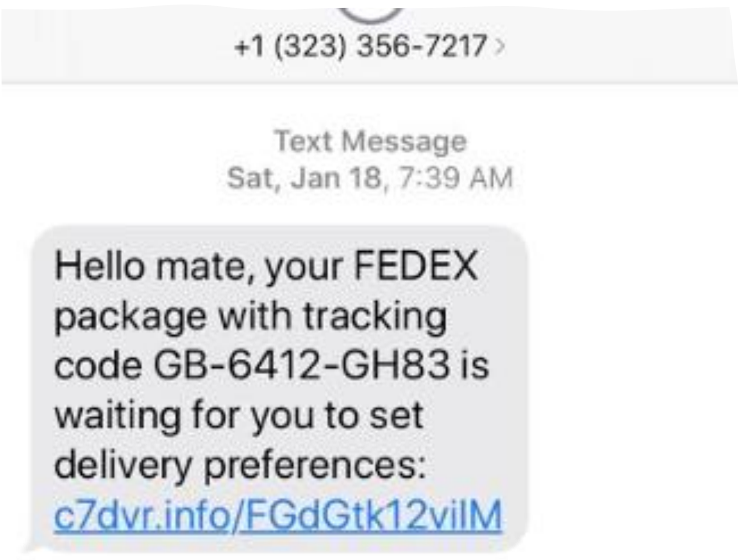
Text Message
Today 3:40 PM

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.


+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/WYmoR8t0IPS


+1 (323) 356-7217

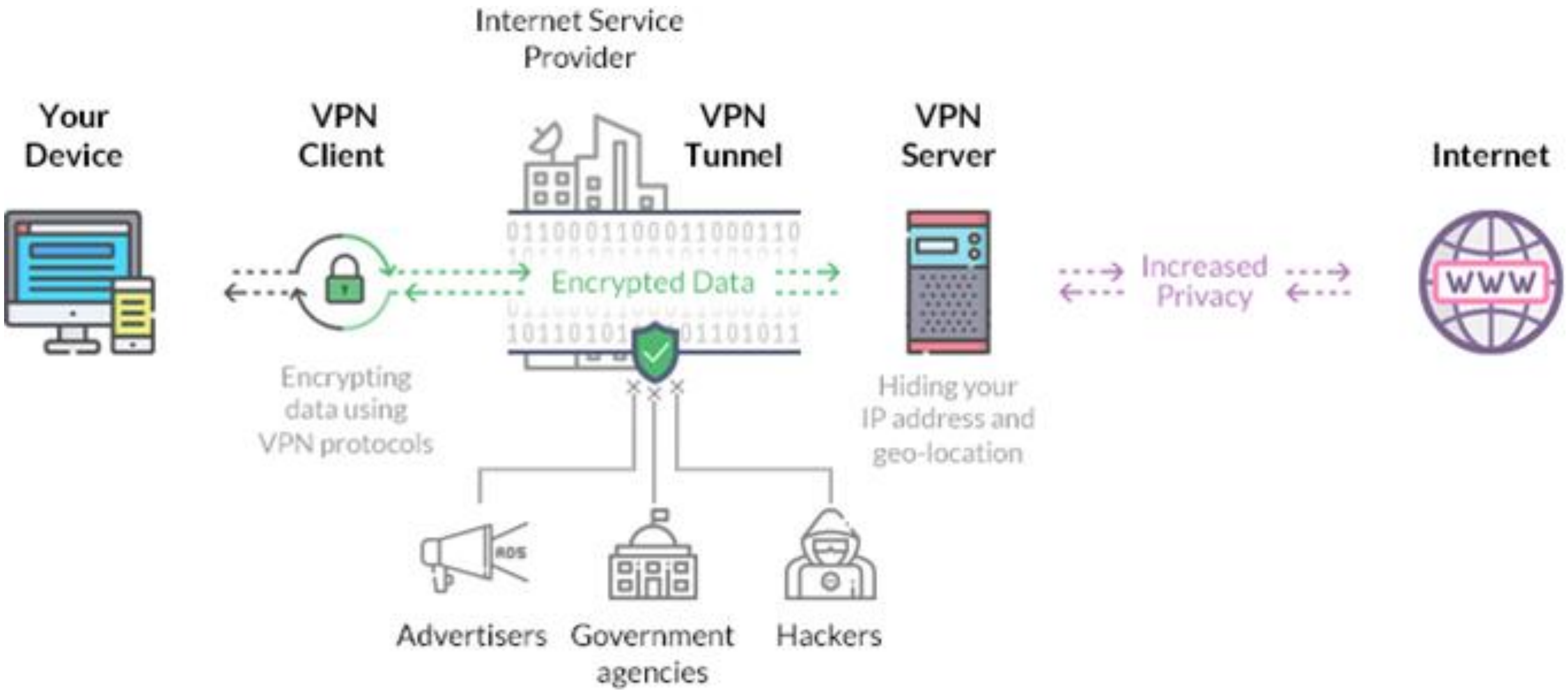
Text Message
Sat, Jan 18, 7:39 AM

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

Secure 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?



Social Media Safety

Adjust	Adjust privacy settings to limit who can see posts and personal information.
Be	Be cautious of accepting friend requests or following people you don't know.
Avoid	Avoid posting sensitive information such as home address, phone number, or financial information.
Think	Think twice before posting anything that could be used against you.
Make	Posting too much information can make it easier for cybercriminals to steal your identity or commit fraud.

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.

Common Methods of Online Tracking

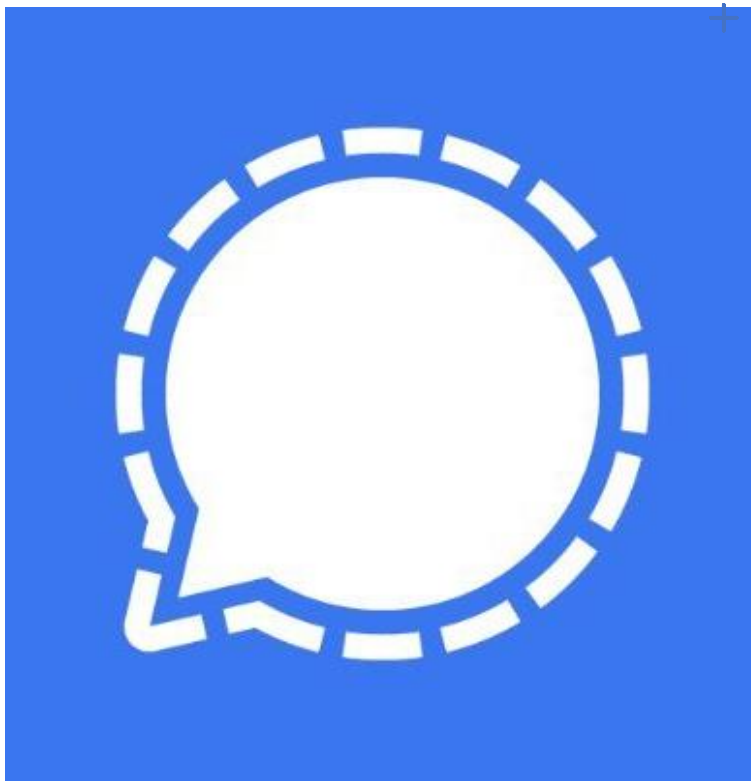
- IP address
- Browser cookies
- Submitted website data
- Browser/device fingerprinting
- Payment method correlation

Safe Browsing

- Use private search engine: Examples: Brave search, StartPage, Duckduckgo
- Use a private & secure browser: Examples: Brave, Mozilla Firefox
- Look for the padlock icon in the address bar => secure connection (HTTPS)
- Be cautious about pop-up ads and never click on them
- Avoid downloading files or software from untrusted websites

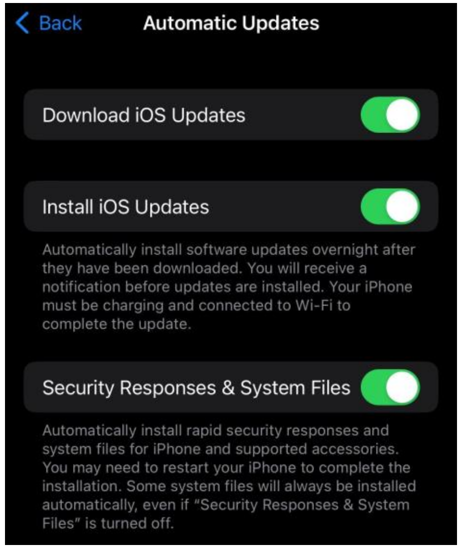
Secure Messaging – Why?
Example: Signal

- 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.



< Back Automatic Updates

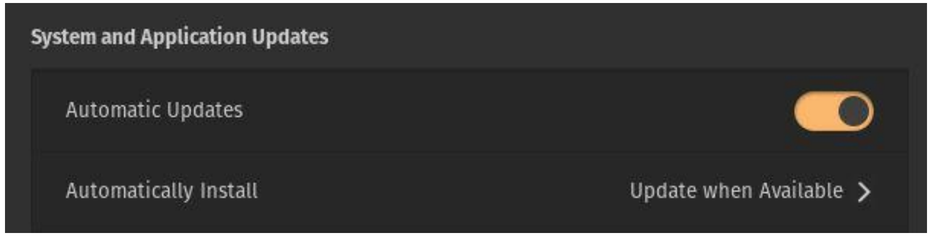
Download iOS Updates ●

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 ●

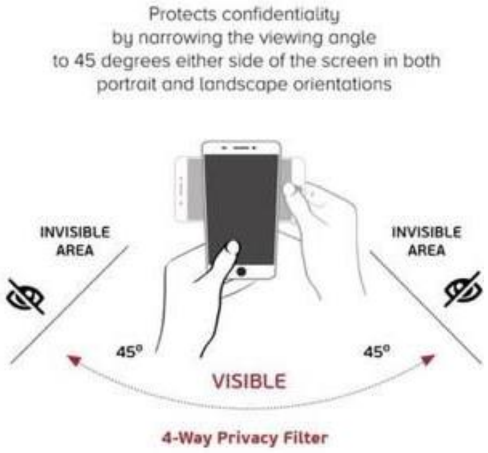
Automatically Install Update when Available >

Miscellaneous Tips

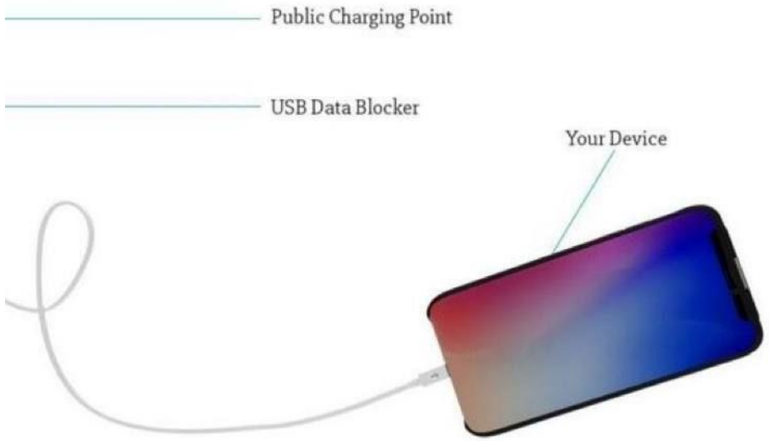
- Beware of "Juice Jacking": a cyberattack that can occur when you charge your device in a public area. Stay safe by using a plug-to-outlet charger or a **data blocker** to prevent unauthorized access to your data.
- Use a **privacy screen** for your phone and laptop to protect your screen from prying 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.

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



Who are we?

null NEU is the student chapter of null, the open security community.

We are a non-profit organization run by student volunteers and officially recognized by the Khoury College of Computer Sciences.

Our mission is to spread security awareness, create a centralized knowledge base for security-related information, and promote advanced security research.

Call to Action!

- To get involved, simply visit our website at https://bio.link/null_neu.

- Click on the "Membership Sign Up" button and fill out the form.