Sun City Computer Club

Cyber Security SIG

September 15, 2022

Questions, Comments, Suggestions welcomed at any time

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

- Ever want to be a presenter??

Presenter???

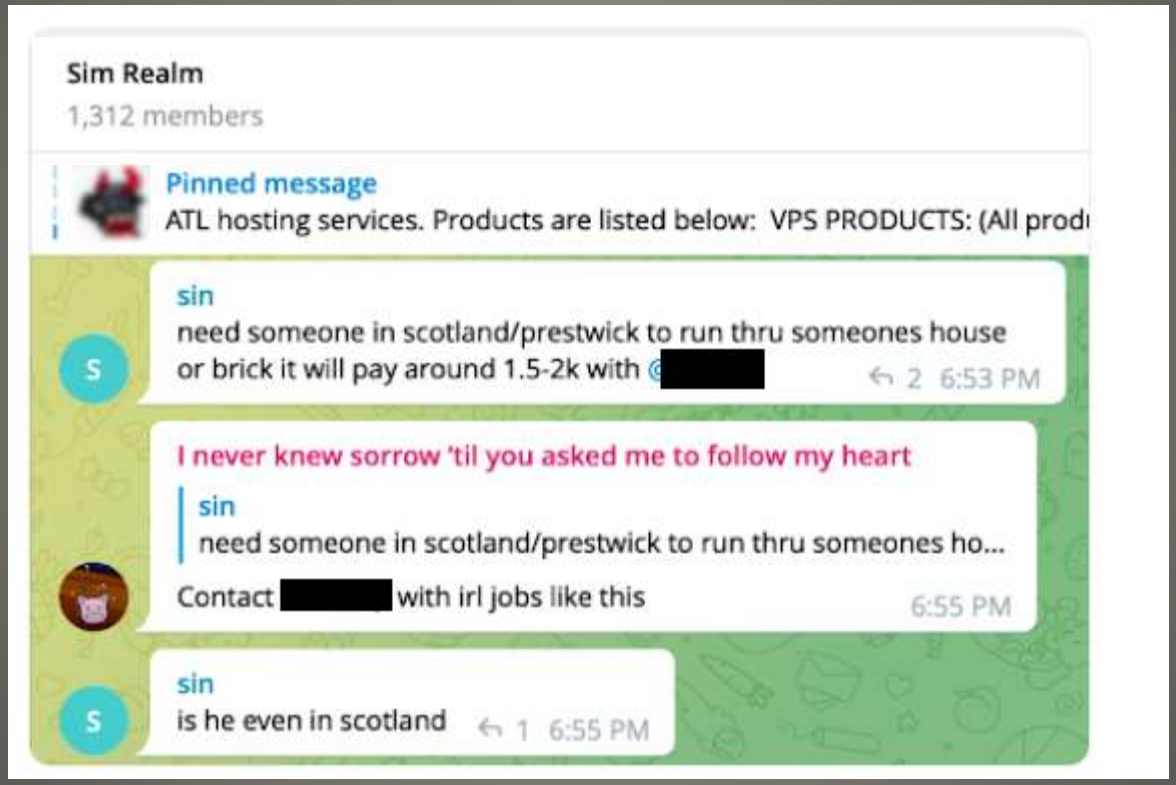
eMail tracking

- Trackers in eMail
- When, where, how, etc.
- HTML
- Plain text readers

- Plain text mode
- Disable images

Current Issues

- Violence-as-a-service
  Brickings, Fire bombings, Shootings



Current Issues

Current Issues

- SIM swappers against SIM swappers
- Hackers attacking Hackers
- Hotel room safe Master combination
  Hotel change combination
- Albania severs diplomatic ties with Iran
  Response to cyber attack
- Employers who collect:
  DoB, SSN, Bank details for payroll deposit
  BUT not a real job
- Quiet quitting
- Chilean government push back DST
- Student Loan Forgiveness scammer's target
- TikTok data leak that wasn't
- Crypto Heist
  We can recover your losses

- Free and open speech
- Free and open press

Competition
Privacy
Youth mental health
Misinformation & Disinformation
Illegal & abusive conduct
Algorithmic discrimination
Lack of transparency

Facebook admits “no idea what we have”

Tech Platform Accountability

Core Principles of Reform

- Promote competition in technology sector
- Provide robust federal protections for privacy
- Protect children
- Remove special legal protections for large tech
- Increase transparency of algorithms
- Stop discriminatory algorithmic decision making

Computer Lore

EvilProxy Service

- In computer networking, a proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources. A proxy server thus functions on behalf of the client when requesting service, potentially masking the true origin of the request to the resource server.

- Service "Here you do it"

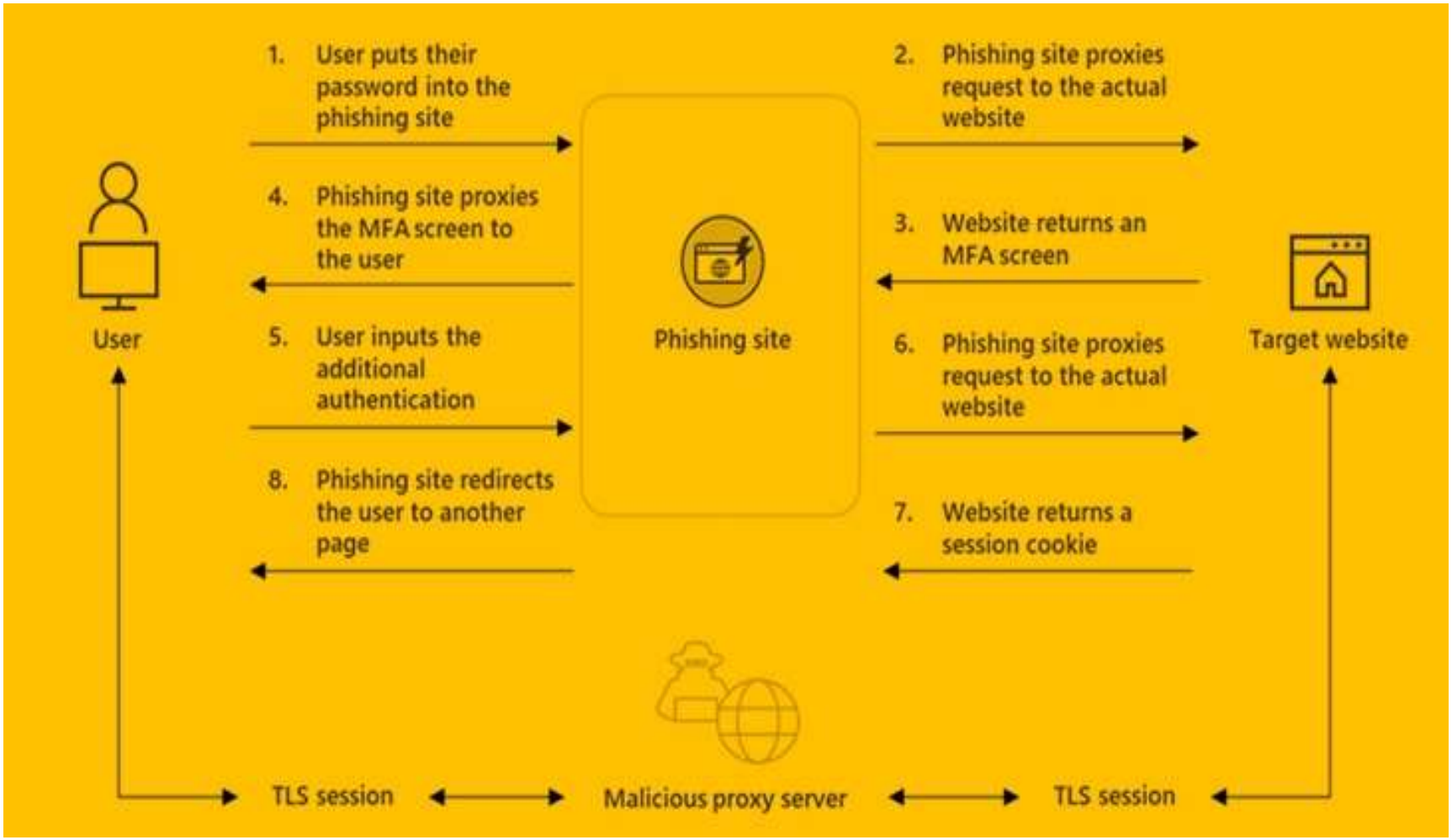
- HTTP is stateless
- Authentication requires many connections
  Each is stateless
- Add multi factor authentication - more complex
- End result Authentication token

EvilProxy Service

- Effortless ability
  Intercept

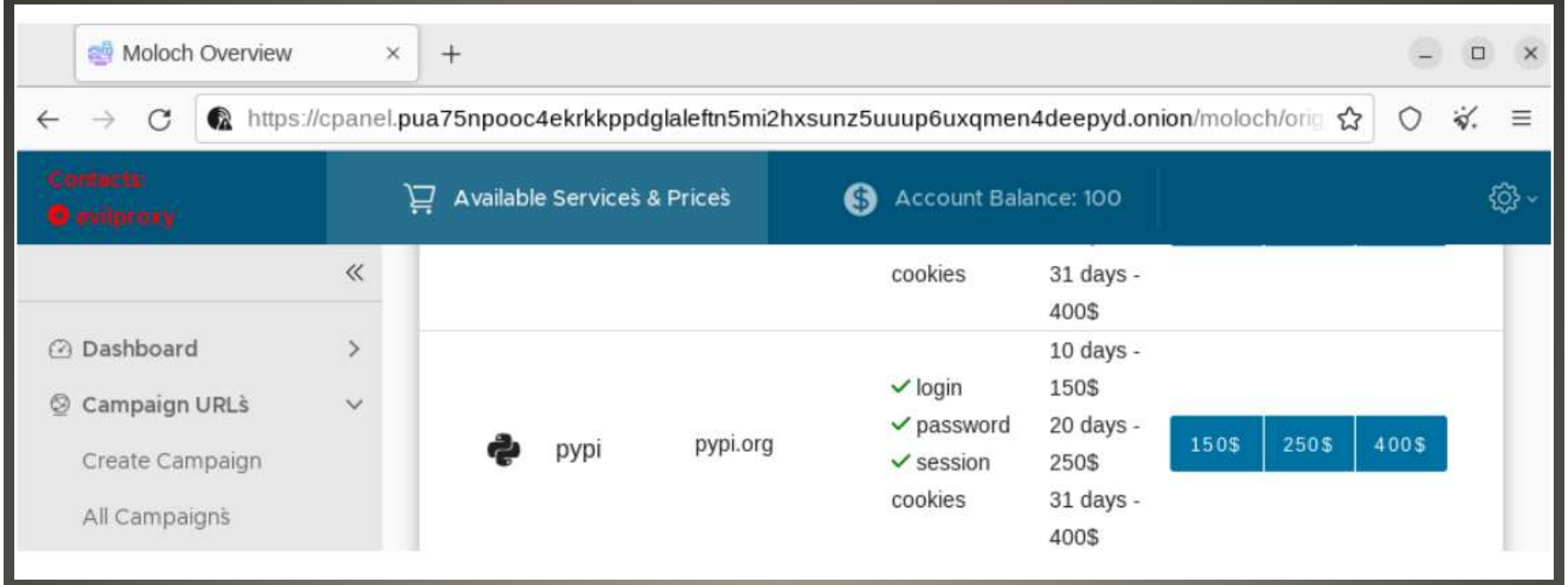
SMS, Oauth, multi-factor authentication flows
Login with Facebook, Google, etc.
Provide SMS code
Give up code in Authenticator app

CAPTURE and USE authentication token


1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
4. Phishing site proxies the MFA screen to the user
3. Website returns an MFA screen
User
Phishing site
Target website
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
8. Phishing site redirects the user to another page
7. Website returns a session cookie
TLS session
Malicious proxy server
TLS session

- Fill out a few fields
- Add features
- Create Campaign

EvilProxy Service



EvilProxy Service

EvilProxy Service

- Links to Links
- Ad removal
- Trackers
- Cookies & flavours
- Man in the middle MitM
- Many in the middle
- Encrypted traffic? - we do that too/also
- Usernames, passphrases, PII IN THE CLEAR

- https://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web

EvilProxy Service

EvilProxy Service

- Attack developers, software repositories
- Caution
  URLs – were readable/typeable
  Site “looks right”
  URL “looks right”
  Site “behaves right”
  Our cyber hygiene is strong
  All is swell

  Or NOT

EvilProxy Service

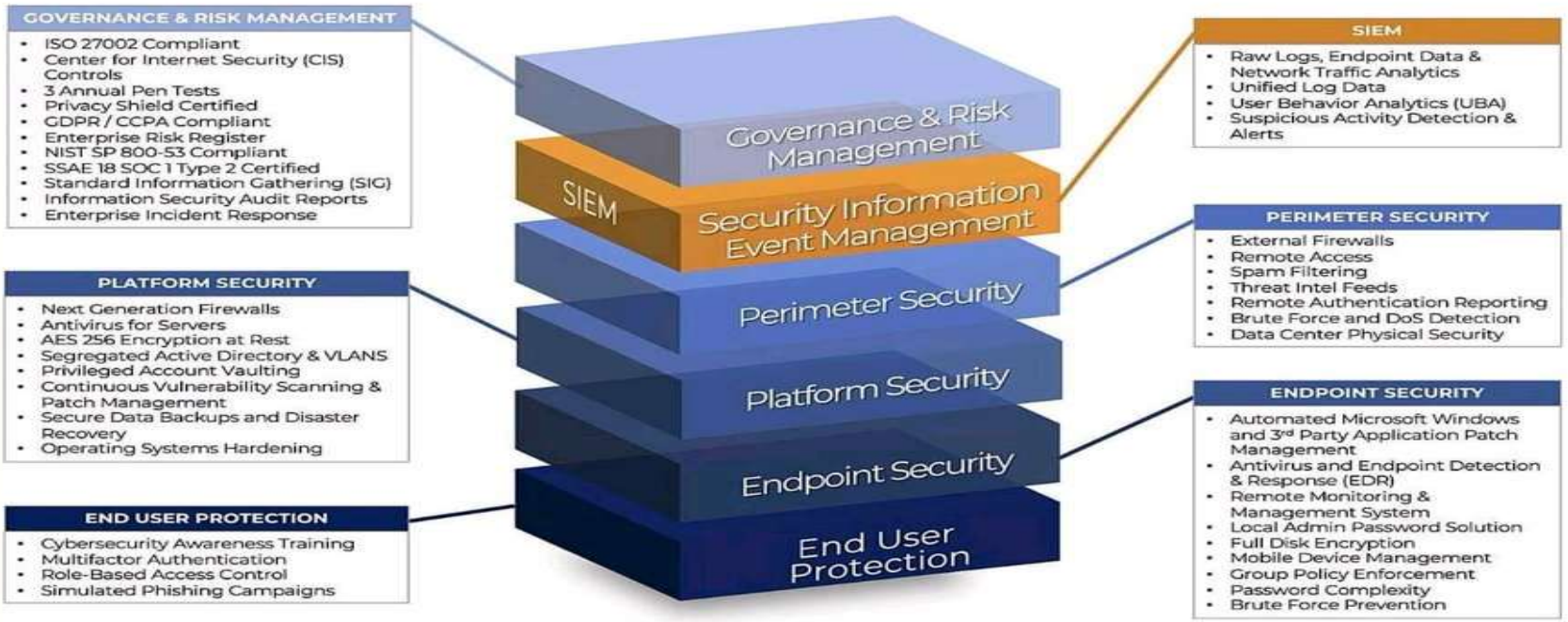
- EvilProxy Service VERY well protected
- Payments via Telegram
- New customers well vetted
- Tor hosting
- Learning efforts against defences
- Any “new” malware is not new for long
- Low skill vs Well protected sites
- Pay, Click, reap

EvilProxy Service

- Awareness, Preparedness, Understanding
- Phishing platform

- Hover over links
- CHECK URL
- UPDATES
- Browser & Email fit for purpose

A Bird's Eye View of



Defense-in-Depth Structure Of Cybersecurity

20 Ways to Block Mobile Attacks

Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!

WiFi

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

Browser

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.

Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

Smishing (phishing via SMS)

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

Vishing (voice phishing)

- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.

KnowBe4
Human error. Conquered.

Passkey

- iOS 16
- First steps other providers other features
- Google, Apple, Microsoft
- Will require web site follow-up / support
- Fast Identity Online FIDO
- Multi Factor Authentication
- Cryptography
- Passkey (keys) kept in a cloud
- Connected to your device(s)
- Authentication to desired site
- Associate your account to a passkey on device
- Your device using biometric or mobile auth

- NO PASSWORD
- NO Password prompt
- NO password phishing
- No password breach

Passkey

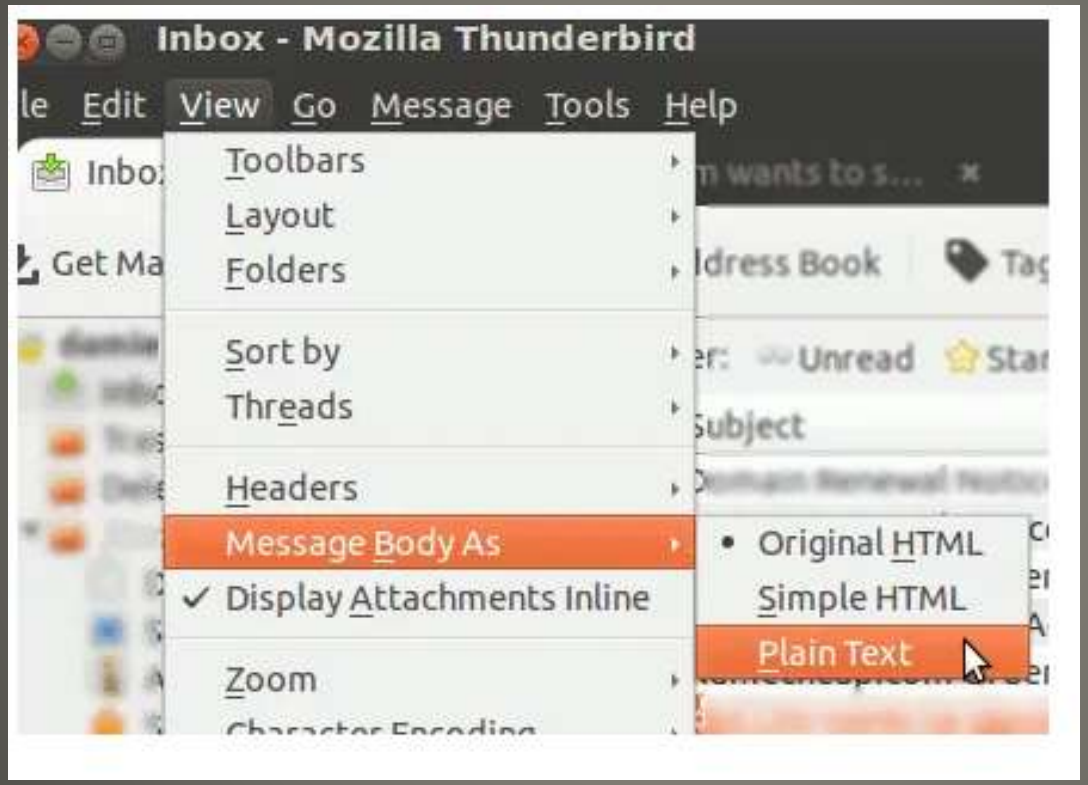
- Gmail

eMail tracking

- Outlook

eMail tracking

- Thunderbird



eMail tracking

- Text based email
- https://en.wikipedia.org/wiki/Text-based_email_client
- Text based browser

eMail addresses

- Universal Identifier
- Persistent
- Leaked via breach
- Providers with some privacy
  - DuckDuckGo
  - Apple
  - Firefox
  - Proton

eMail addresses

- Multiple
- Fit for Purpose
- Privacy

eMail addresses

- Apple
  Hide My Email

Works well within Apple ecosystem

Cost

eMail addresses

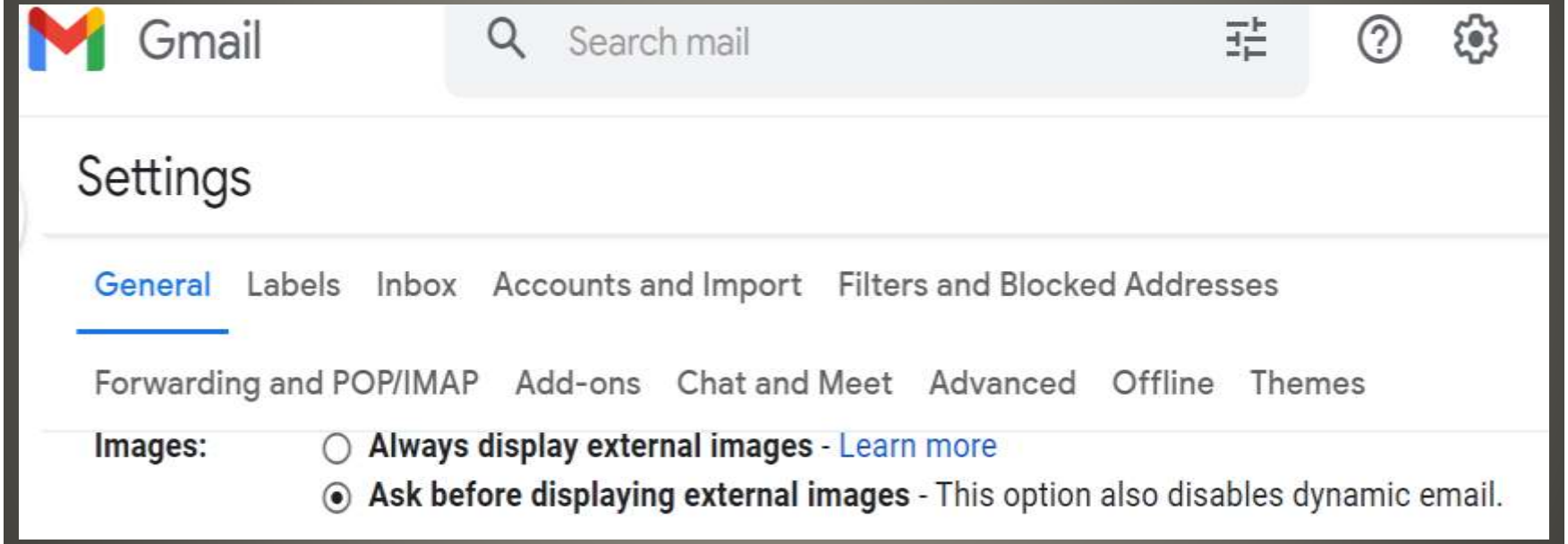
- DuckDuckGo
- Privacy as mission statement
- DuckDuckGo extension for most browsers

- Firefox
- Firefox Relay

- Proton
- Proton Mail

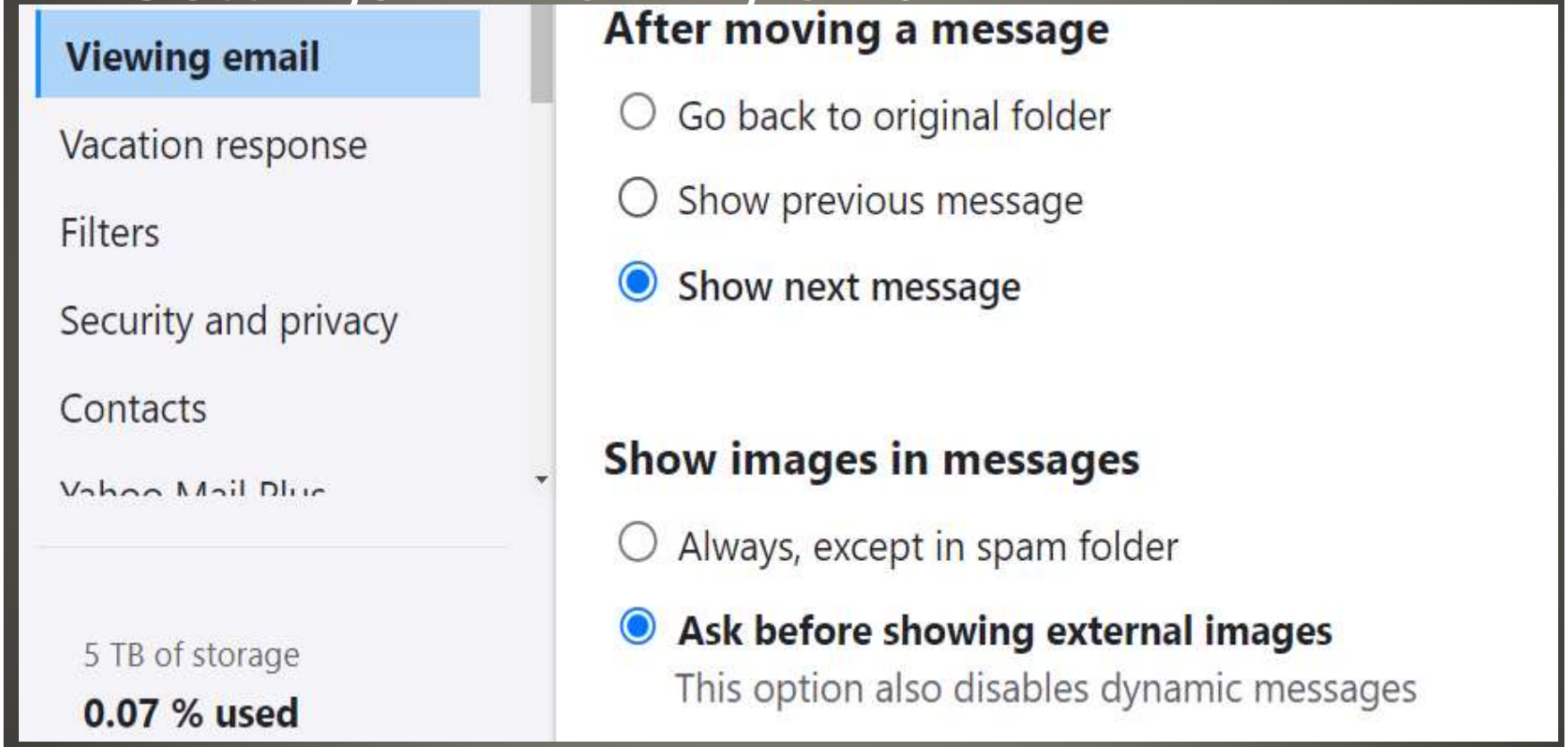
eMail addresses

- Gmail
  Settings > General > Images



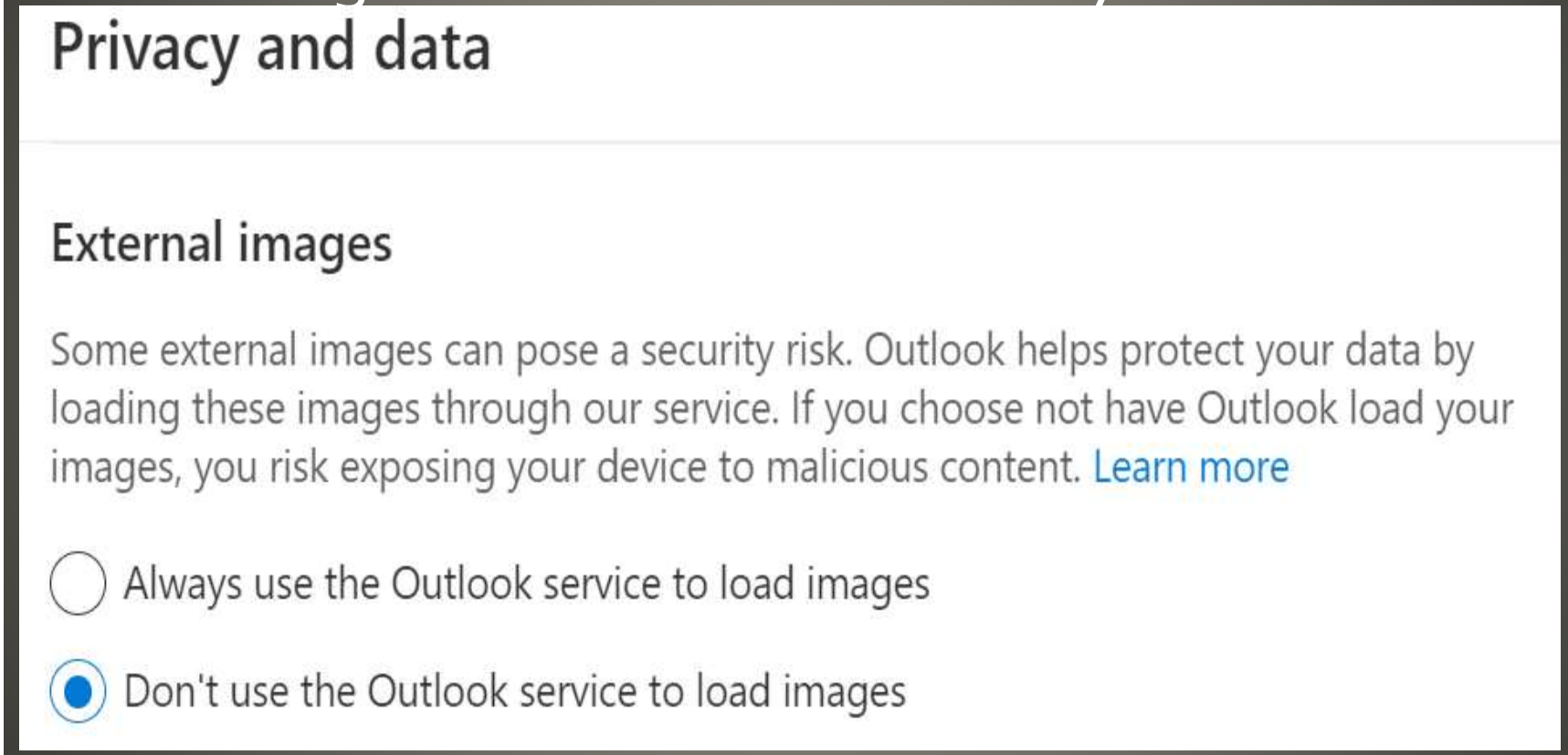
Download Images disable

- Yahoo
  Settings > Viewing email



Download Images disable

- Outlook
  Settings > General > Privacy and data



Download Images disable

War Shipping

- Cheap custom device
- Shipped INTO Victim
- Usually returned Clean exfiltration
- Device appears to be victim’s Guest WiFi

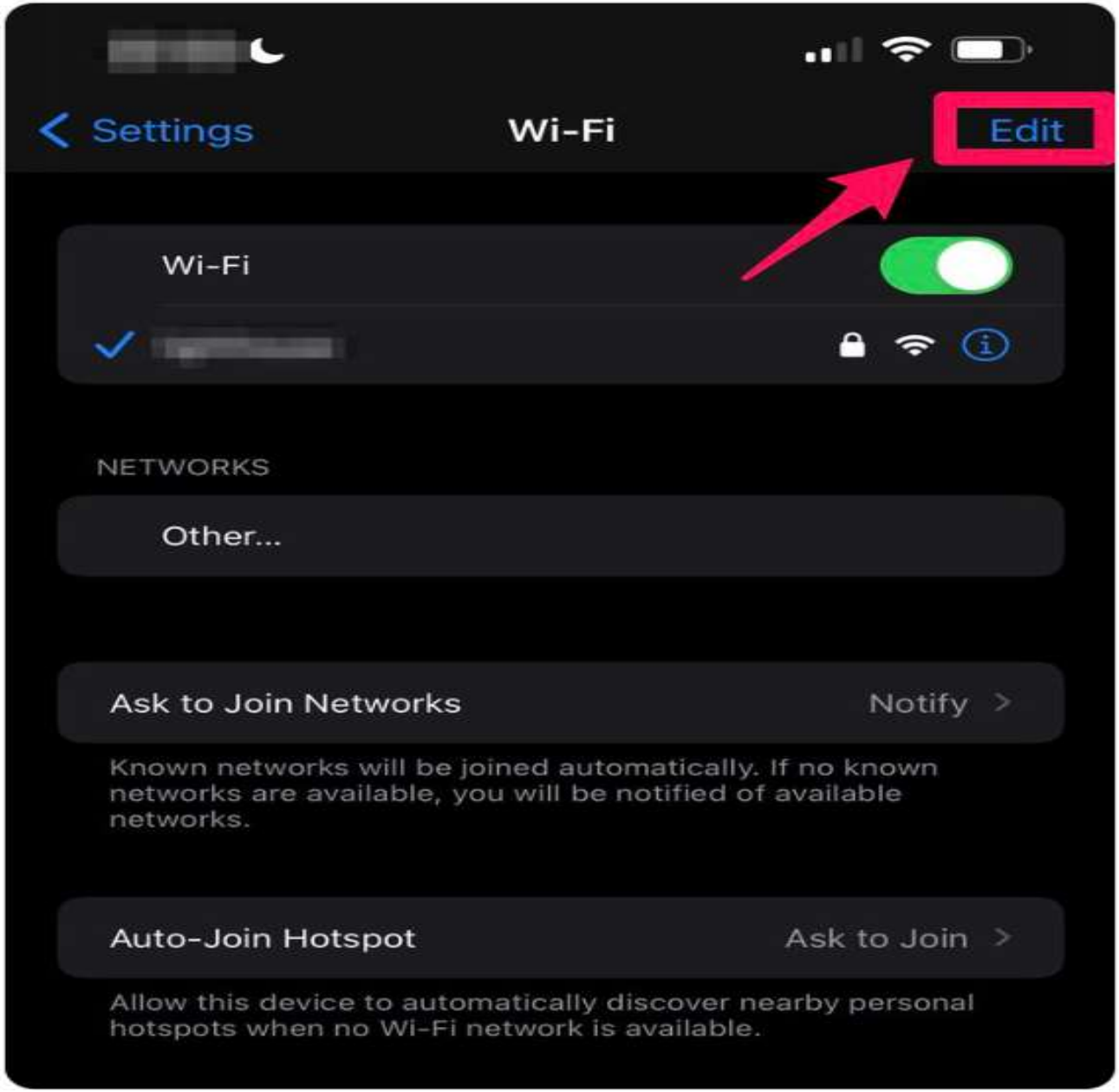
- Network blinking LED
- Potato chip bag
- Laser on windows
  Glass windows
- Conference room
- A/V room

Corporation Data exfiltration

- In-person transactions with Internet strangers

Internet transactions

- Meet at a police station where you can exchange and photocopy each others' identification papers, such as a driver's license. Do NOT carry cash to this location.
- Photocopy the license or identification paper, or use your phone to photograph it.
- Email the ID information to a friend, or to someone trusted (not to yourself).
- If you're selling at home, or going to someone's home, never be outnumbered. If you're at home, make sure you have two or three people there — and tell the person who is coming that you will have others with you.
- At home or an apartment, NEVER let someone go anywhere unaccompanied. Always make sure they are escorted.
- Never let more than one group come to your home at one time to buy or sell.
- Beware of common scams, like checks for an amount higher than the amount of the deal; "cashier's checks" that are forged and presented when the bank is closed.
- If you are given a cashier's check, money order or other equivalent, call the bank — at the number listed online, not a number the buyer gives you — to verify the validity of the check.


Settings
Wi-Fi
Edit
Wi-Fi
NETWORKS
Other...
Ask to Join Networks
Notify
Known networks will be joined automatically. If no known networks are available, you will be notified of available networks.
Auto-Join Hotspot
Ask to Join
Allow this device to automatically discover nearby personal hotspots when no Wi-Fi network is available.

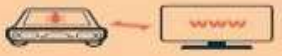
15 TYPES OF CYBER ATTACKS

Man-In-The-Middle (MitM)

This type of cyber attack happens when a hacker introduces himself/herself between your network connection and a server.

Phishing & Spearphishing

The phishing attack is where cyber-terrorism attackers send you fraudulent emails with clickable links.



Drive-By Attacks

Cyber terrorists frequently use drive-by attacks to spread malware. They target insecure websites.

Botnets Attacks

Botnets are a collection of system networks which attackers have injected malware.

Social Engineering Attacks

These cyber threats include email phishing which is arguably the most common type of social engineering cyber attack.

SQL Injection Attacks

SQL means a Structured Query Language. An SQL injection cyberterrorism attack happens when the cyber-terrorist injects malicious code in an SQL server.

Malware Attacks

Malicious software is any undesirable software injected into your system without your approval.

Cross-Site Scripting (XSS)

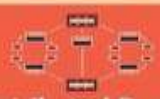
This type of cyber attack makes use of a third-party website to inject malicious JavaScript codes into the target's web browser.

Password Attacks

Cyber terrorists leverage on password authentication mechanism to gain access to user's information.

Denial Of Service (DoS)

DoS attack is one of the most widespread types of cyber attacks which is done by making a resource unavailable to the user.



Distributed Denial Of Service (DDoS)

This attack occurs when many compromised network devices all over the world flood the bandwidth of the target system.

Inside Attack & Data Breaches

An insider attack is one of the most dangerous. This commonly occurs through the activities of disgruntled employees or ex-employees.

Cryptojacking Attacks

Cryptojacking attackers target the bandwidth of users' computer and processing power to mine cryptocurrency.

Eavesdropping Attack

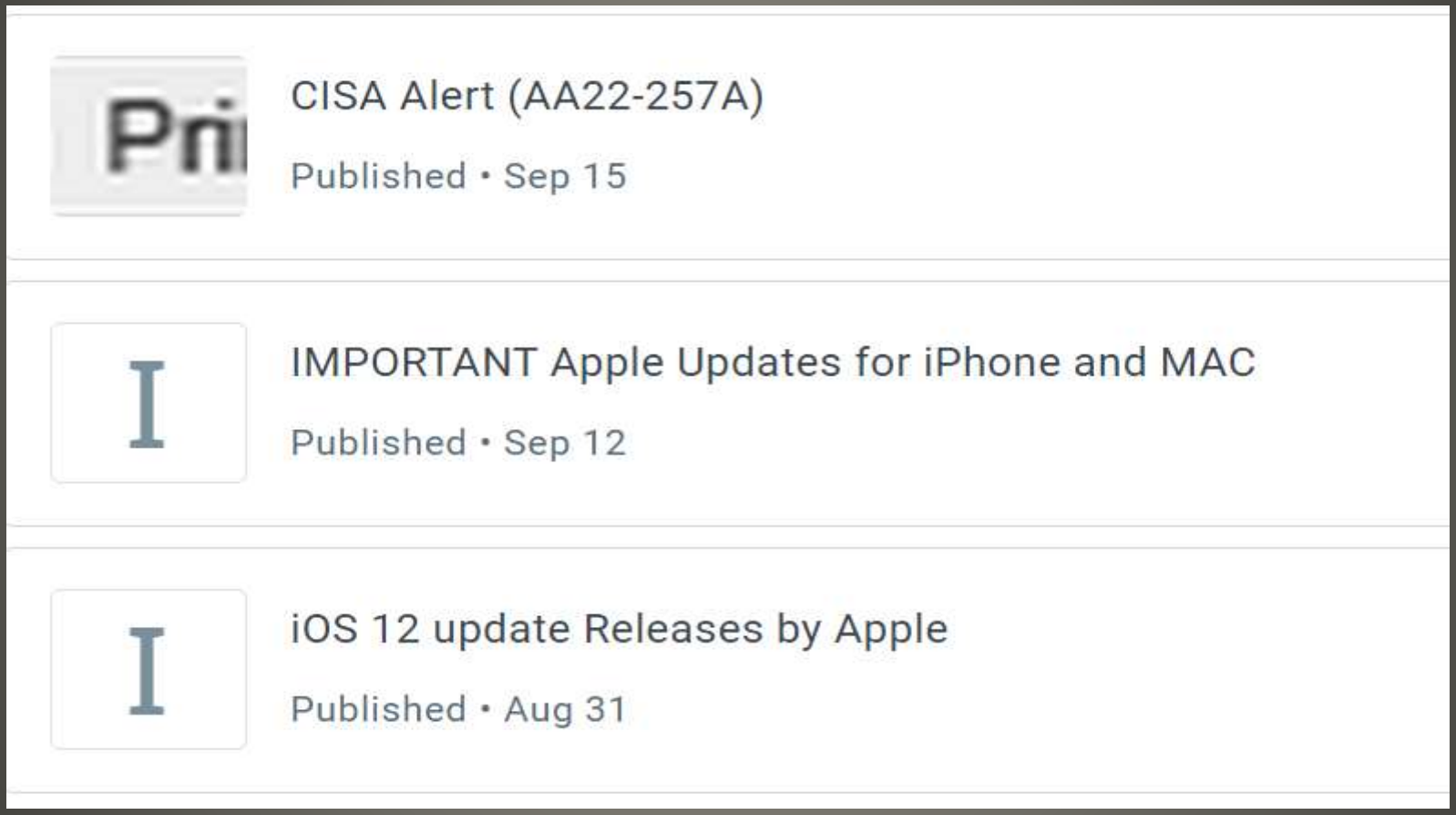
Eavesdropping cyber threats occur when attackers intercept user's network traffic.

Crypto Mining Malware Attacks

The crypto mining malware attacks also target crypto miners and exchanges and hijack their computer's processing power.

Current Issues

- Multi-persona impersonation



Alert (AA22-257A)

More Alerts

Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations

Original release date: September 14, 2022

Summary

This joint Cybersecurity Advisory (CSA) is the result of an analytic effort among the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), U.S. Cyber Command (USCC) - Cyber National Mission Force (CNMF), the Department of the Treasury (Treasury), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), and the United Kingdom's National Cyber Security Centre (NCSC) to highlight continued malicious cyber activity by advanced persistent threat (APT) actors that the authoring agencies assess are affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC). **Note:** The IRGC is an Iranian Government agency tasked with defending the Iranian Regime from perceived internal and external threats. Hereafter, this advisory refers to all the coauthors of this advisory as "the authoring agencies."

Actions to take today to protect against ransom operations:

- Keep systems and software updated and prioritize remediating known exploited vulnerabilities.
- Enforce MFA.
- Make offline backups of your data.

This advisory updates joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, which provides information on these Iranian government-sponsored APT actors exploiting known Fortinet and Microsoft Exchange vulnerabilities to gain initial access to a broad range of targeted entities in furtherance of malicious activities, including ransom operations. The authoring agencies now judge these actors are an APT group affiliated with the IRGC.

Since the initial reporting of this activity in the FBI Liaison Alert System (FLASH) report APT Actors Exploiting Fortinet Vulnerabilities to Gain Access for Malicious Activity from May 2021, the authoring agencies have continued to observe these IRGC-affiliated actors exploiting known vulnerabilities for initial access. In addition to exploiting Fortinet and Microsoft Exchange vulnerabilities, the authoring agencies have observed these APT actors exploiting VMware Horizon Log4j vulnerabilities for initial access. The IRGC-affiliated actors have used this access for follow-on activity, including disk encryption and data extortion, to support ransom operations.

The IRGC-affiliated actors are actively targeting a broad range of entities, including entities across multiple U.S. critical infrastructure sectors as well as Australian, Canadian, and United Kingdom organizations. These actors often operate under the auspices of Najee Technology Hooshmand Fater LLC, based in Karaj, Iran, and Afkar System Yazd Company, based in Yazd, Iran. The authoring agencies assess the actors are exploiting known vulnerabilities on unprotected networks rather than targeting specific targeted entities or sectors.

This advisory provides observed tactics, techniques, and indicators of compromise (IOCs) that the authoring agencies assess are likely associated with this IRGC-affiliated APT. The authoring agencies urge organizations, especially critical infrastructure organizations, to apply the recommendations listed in the Mitigations section of this advisory to mitigate risk of compromise from these IRGC-affiliated cyber actors.

For a downloadable copy of IOCs, see AA22-257A.stix.

For more information on Iranian state-sponsored malicious cyber activity, see CISA's Iran Cyber Threat Overview and Advisories webpage and FBI's Iran Threat webpage.

Download the PDF version of this report: pdf, 836 kb

- Ever want to be a presenter??

Presenter???

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com