Sun City Computer Club

Cyber Security SIG
December 7, 2023
Perl Harbor Day

Questions, Comments, Suggestions welcomed at any time

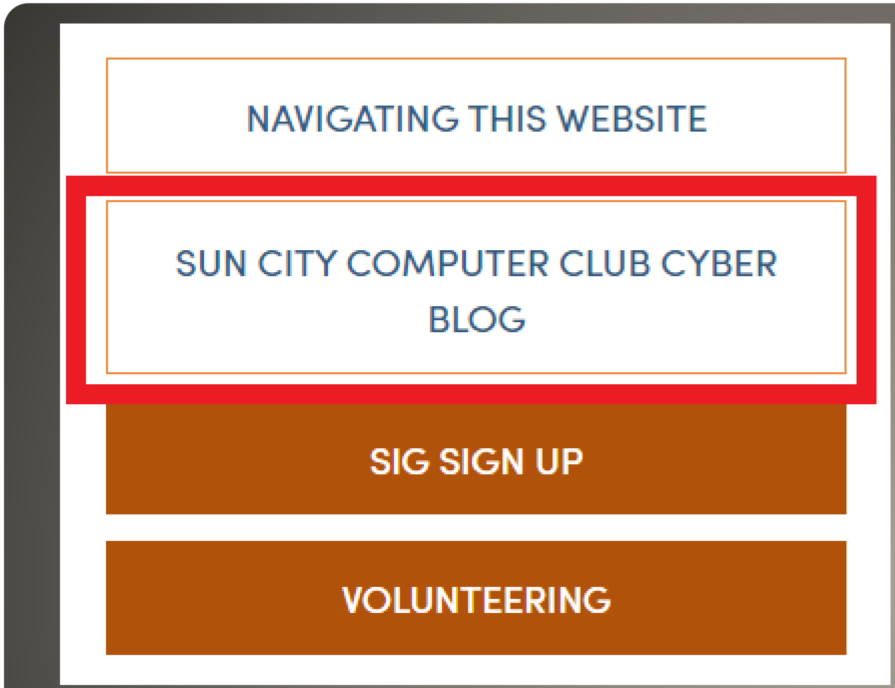
Even Now

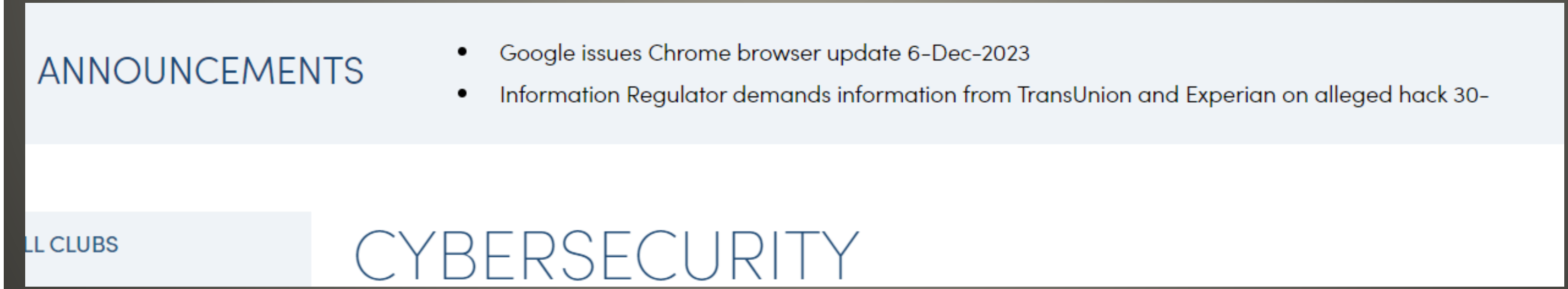
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

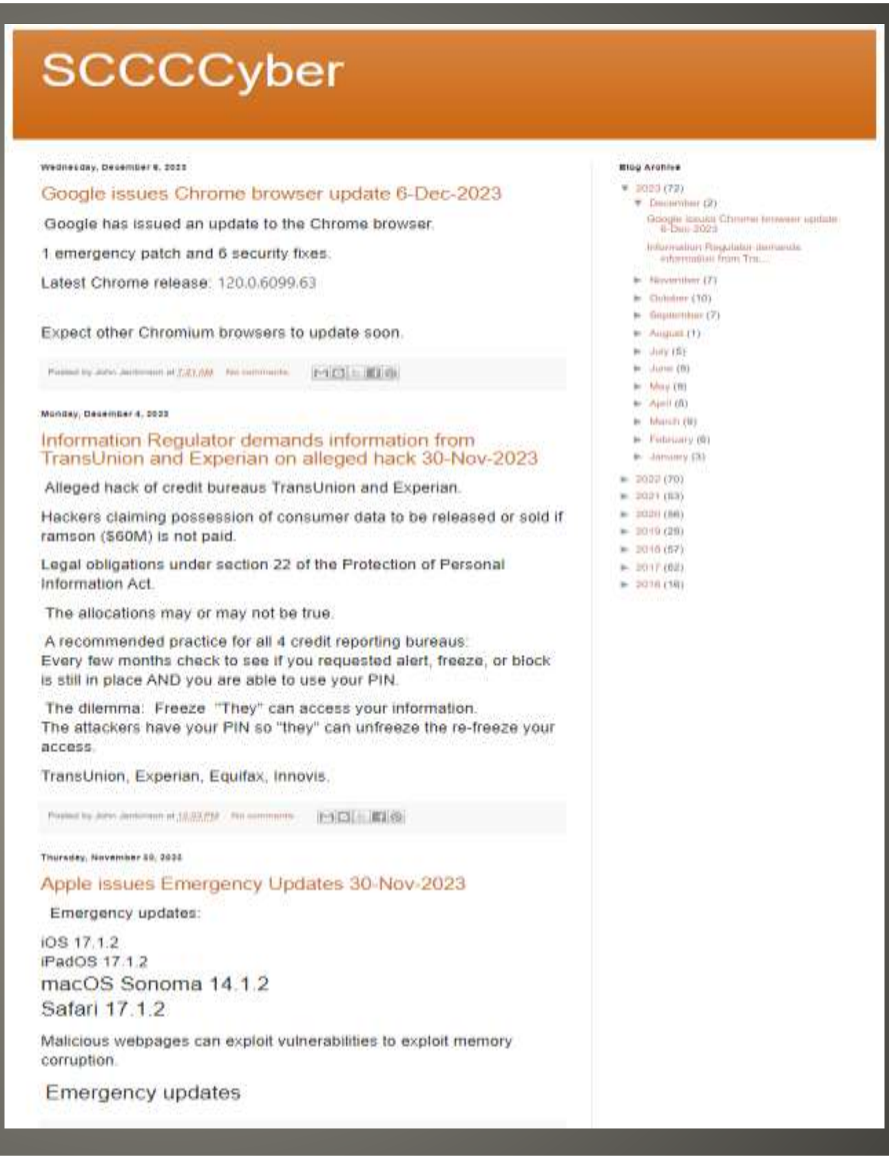
SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

News Blog




ANNOUNCEMENTS

- Google issues Chrome browser update 6-Dec-2023
- Information Regulator demands information from TransUnion and Experian on alleged hack 30-



SCCCyber

Wednesday, December 6, 2023

Google issues Chrome browser update 6-Dec-2023

Google has issued an update to the Chrome browser.

1 emergency patch and 6 security fixes.

Latest Chrome release: 120.0.6099.63

Expect other Chromium browsers to update soon.

Posted by John Jenkinson at 7:21 AM No comments:

Monday, December 4, 2023

Information Regulator demands information from TransUnion and Experian on alleged hack 30-Nov-2023

Alleged hack of credit bureaus TransUnion and Experian.

Hackers claiming possession of consumer data to be released or sold if ramson ($60M) is not paid.

Legal obligations under section 22 of the Protection of Personal Information Act.

The allocations may or may not be true.

A recommended practice for all 4 credit reporting bureaus:
Every few months check to see if you requested alert, freeze, or block is still in place AND you are able to use your PIN.

The dilemma: Freeze "They" can access your information.
The attackers have your PIN so "they" can unfreeze the re-freeze your access.

TransUnion, Experian, Equifax, Innovis.

Posted by John Jenkinson at 10:03 PM No comments:

Thursday, November 30, 2023

Apple issues Emergency Updates 30-Nov-2023

Emergency updates:

iOS 17.1.2
iPadOS 17.1.2
macOS Sonoma 14.1.2
Safari 17.1.2

Malicious webpages can exploit vulnerabilities to exploit memory corruption.

Emergency updates

Blog Archive

- ▼ 2023 (72)
  - ▼ December (2)
    - Google issues Chrome browser update 6-Dec-2023
    - Information Regulator demands information from Tra...
  - ► November (7)
  - ► October (10)
  - ► September (7)
  - ► August (1)
  - ► July (5)
  - ► June (8)
  - ► May (8)
  - ► April (8)
  - ► March (8)
  - ► February (6)
  - ► January (3)
- ► 2022 (70)
- ► 2021 (63)
- ► 2020 (86)
- ► 2019 (28)
- ► 2018 (57)
- ► 2017 (62)
- ► 2016 (16)

News Blog

- More detail at Windows SIG 12-December

Windows Copilot Security

EU

- eIDAS 2.0 Article 45 Browser trust
- Electronic IDentification And trust Services
- Async encryption Public & Private keys
- Public keys published via certificates
- Certificates published by Certificate Authorities
- Browsers have trusted stores of Certificate Authorities
- Corporations control their CA stores
- Proxies
- EU Fight terrorist and child abuse

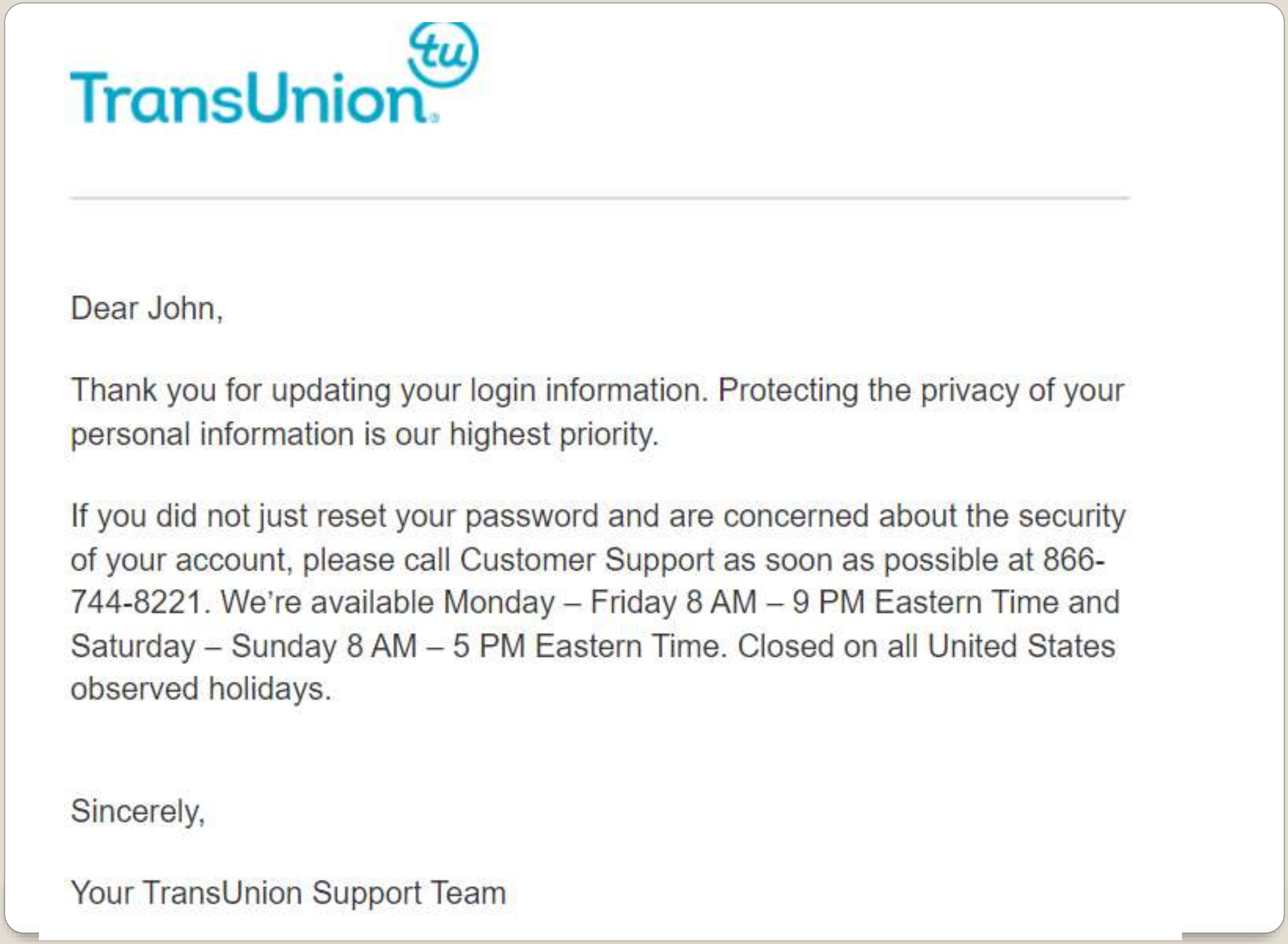
FCC stronger rules

- SIM swapping
- Port-out fraud

- Credit bureaus hacked?
  TransUnion & Experian
  Experian FTC troubles
  Transunion hacked March 2022
  Sensitive data stolen
  4 Credit bureaus   Innovis

DOUBLE CHECK CERTIFICATE
DOUBLE CHECK STATUS
Temporary unfreeze / block??

Credit bureaus hacked?



Dear John,

Thank you for updating your login information. Protecting the privacy of your personal information is our highest priority.

If you did not just reset your password and are concerned about the security of your account, please call Customer Support as soon as possible at 866-744-8221. We're available Monday – Friday 8 AM – 9 PM Eastern Time and Saturday – Sunday 8 AM – 5 PM Eastern Time. Closed on all United States observed holidays.

Sincerely,

Your TransUnion Support Team

Credit bureaus hacked

- $30M per bureau ransom
- Consumer data to be released?
- Criminals know more than you about you
- Alert, freeze, block

  they may have that too
- Your PIN ?

- Large(st) real estate services company
- Cyber attack
- Confusion home buyers/sellers
- “Where’s my money?”
- Mortgage payments

Fidelity National Financial

Passkeys

- Biometric
- No silly rules “a capital letter, special symbol”
- Passkeys public key asymmetric crypto
- Passwords secret key symmetric crypto

- Passwords
- Passphrases
- Passkeys
- Hardware keys
- Authenticators

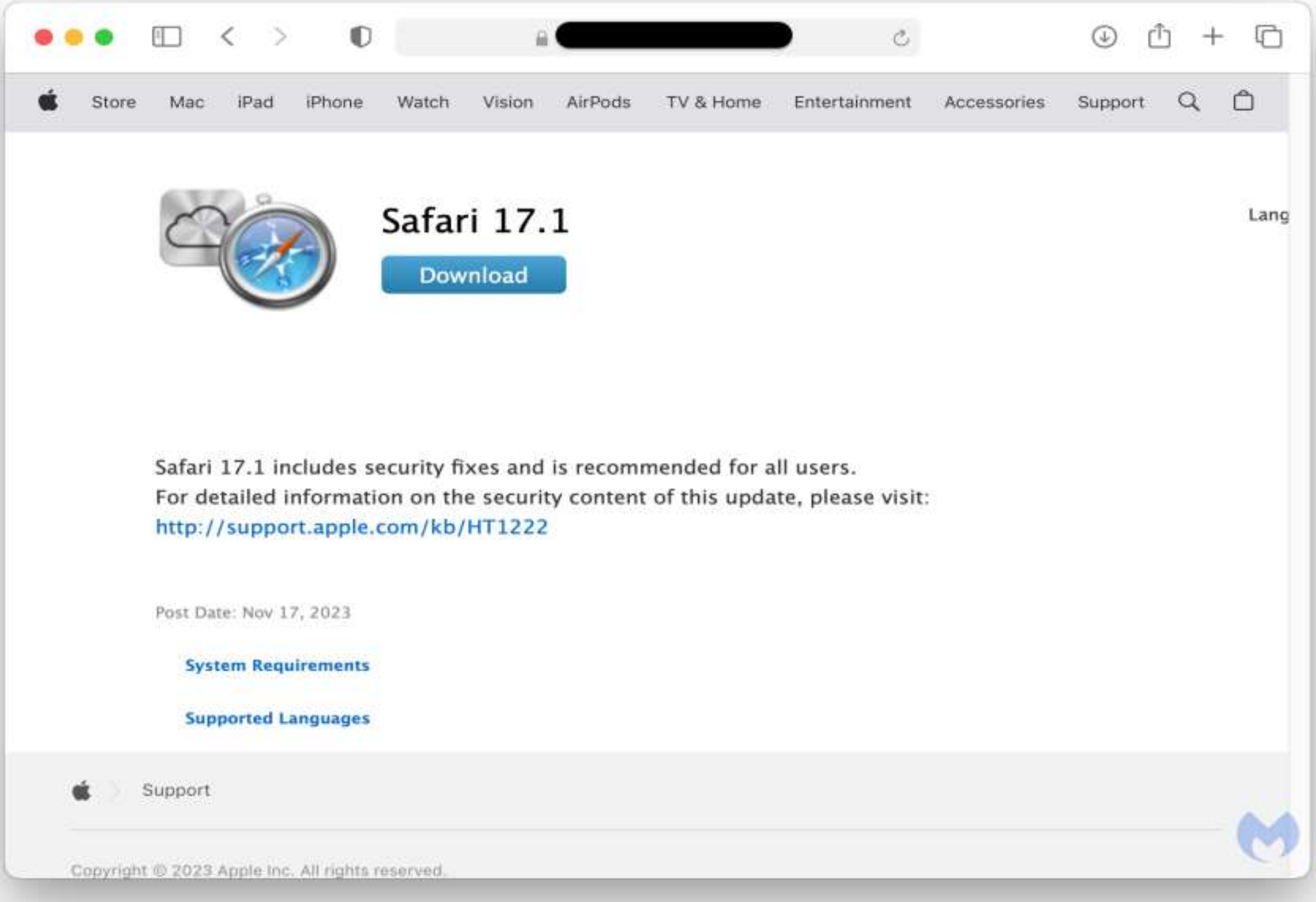
Fake Safari & Chrome Updates

- Atomic macOS Stealer
- iCloud Keychain info, CC numbers, crypto wallets
- Google Search Ads

  Now
- Clear Fake

  Safari & Chrome updates

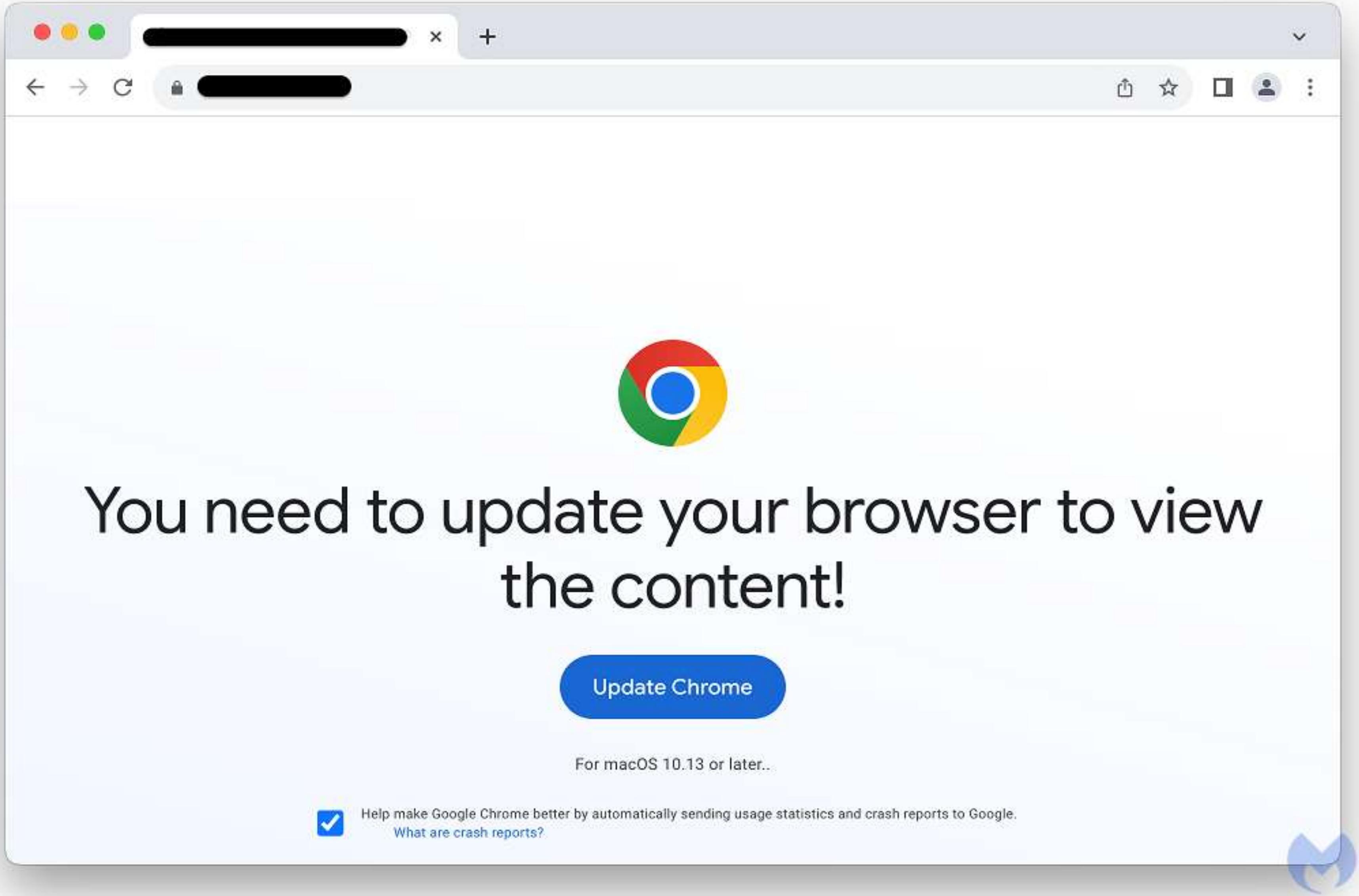
  was Windows malware



Safari 17.1

Safari 17.1 includes security fixes and is recommended for all users.
For detailed information on the security content of this update, please visit:
http://support.apple.com/kb/HT1222

Post Date: Nov 17, 2023



[redacted]

[redacted]

You need to update your browser to view the content!

For macOS 10.13 or later..

☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google.
What are crash reports?

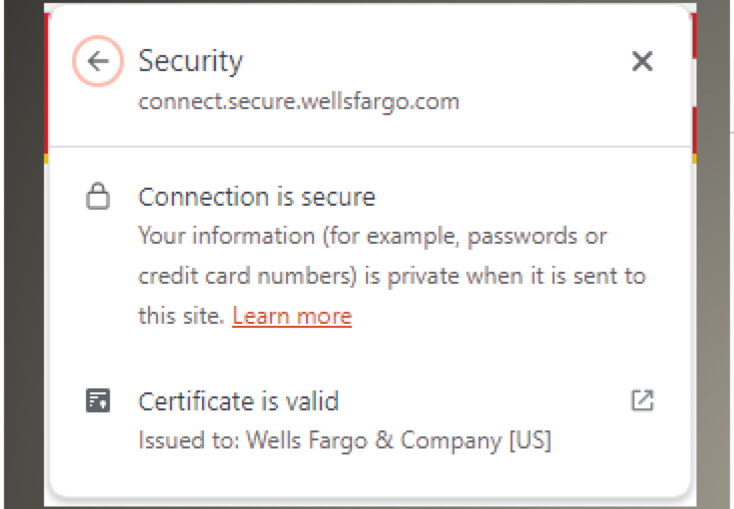
Protections

- Only update
  Safari – Apple Settings
  Chrome – Inside Chrome browser

Atomic macOS Stealer
Can and Will be re-deployed

MitM MFA

- Great increase in look-a-like domain names
- Corporations
- 50 -> 160 new look-a-like domain names per week
- Consumers as well
- May be followed by DoS
- Stealing tokens
- 24-hour lifetime
- Small display form factor
- Gamers
- Be suspicious anything look “off”
- Avoid unsolicited links
- CHECK Digital Certificate



Security

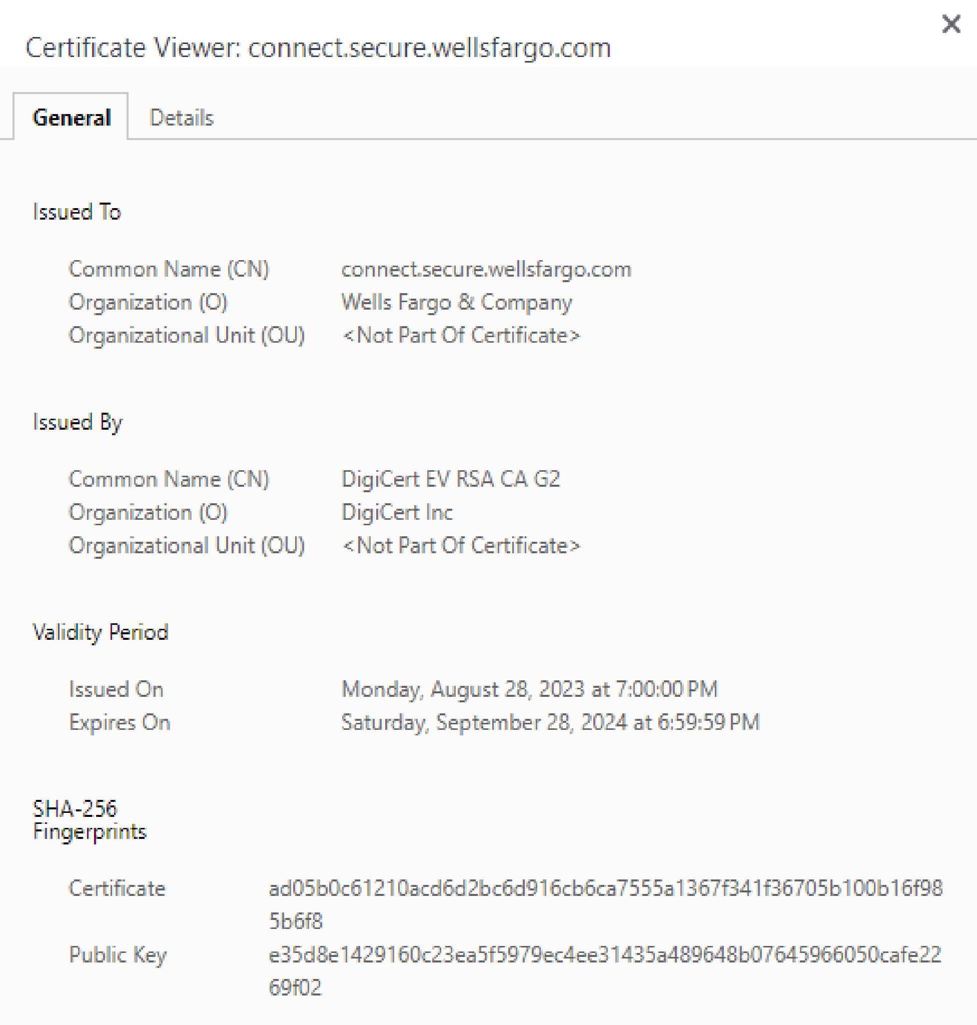
connect.secure.wellsfargo.com

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid

Issued to: Wells Fargo & Company [US]



Certificate Viewer: connect.secure.wellsfargo.com

Issued To

Common Name (CN)	connect.secure.wellsfargo.com
Organization (O)	Wells Fargo & Company
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	DigiCert EV RSA CA G2
Organization (O)	DigiCert Inc
Organizational Unit (OU)	<Not Part Of Certificate>

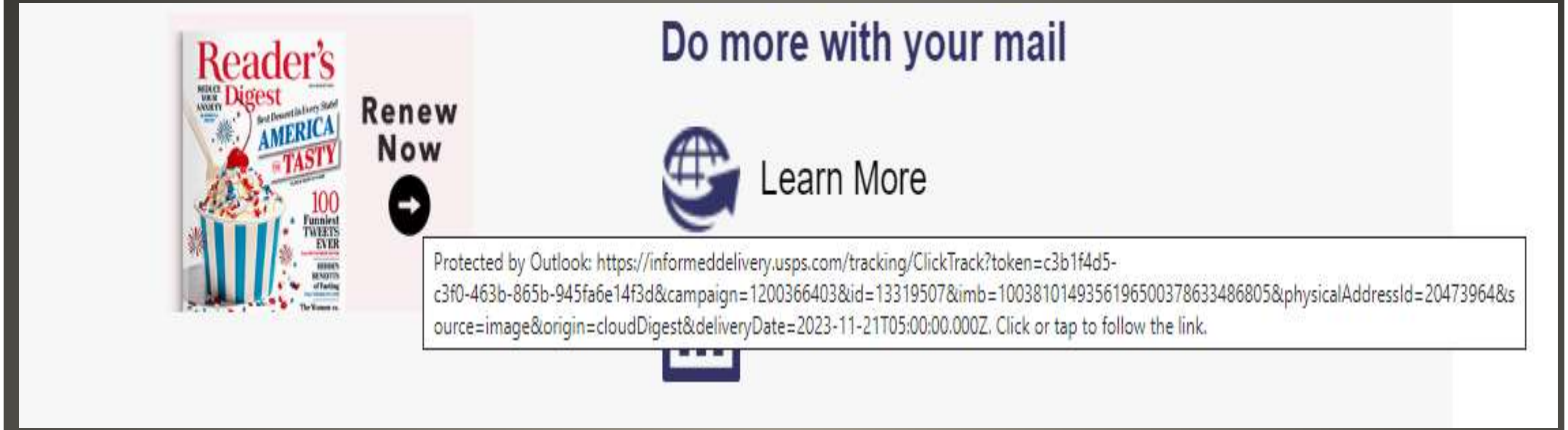
Validity Period

Issued On	Monday, August 28, 2023 at 7:00:00 PM
Expires On	Saturday, September 28, 2024 at 6:59:59 PM

SHA-256 Fingerprints

Certificate	ad05b0c61210acd6d2bc6d916cb6ca7555a1367f341f36705b100b16f985b6f8
Public Key	e35d8e1429160c23ea5f5979ec4ee31435a489648b07645966050cafe2269f02

Check Digital Certificate



Do more with your mail

Protected by Outlook: https://informeddelivery.usps.com/tracking/ClickTrack?token=c3b1f4d5-c3f0-463b-865b-945fa6e14f3d&campaign=1200366403&id=13319507&imb=10038101493561965003786334868058&physicalAddressId=20473964&source=image&origin=cloudDigest&deliveryDate=2023-11-21T05:00:00.000Z. Click or tap to follow the link.

USPS Informed Delivery Ads

- Sensors, microphones, cameras, car apps, company websites, dealership and vehicle telematics
- Then we connect to smart devices

Car data collections

Leica M11-P Camera

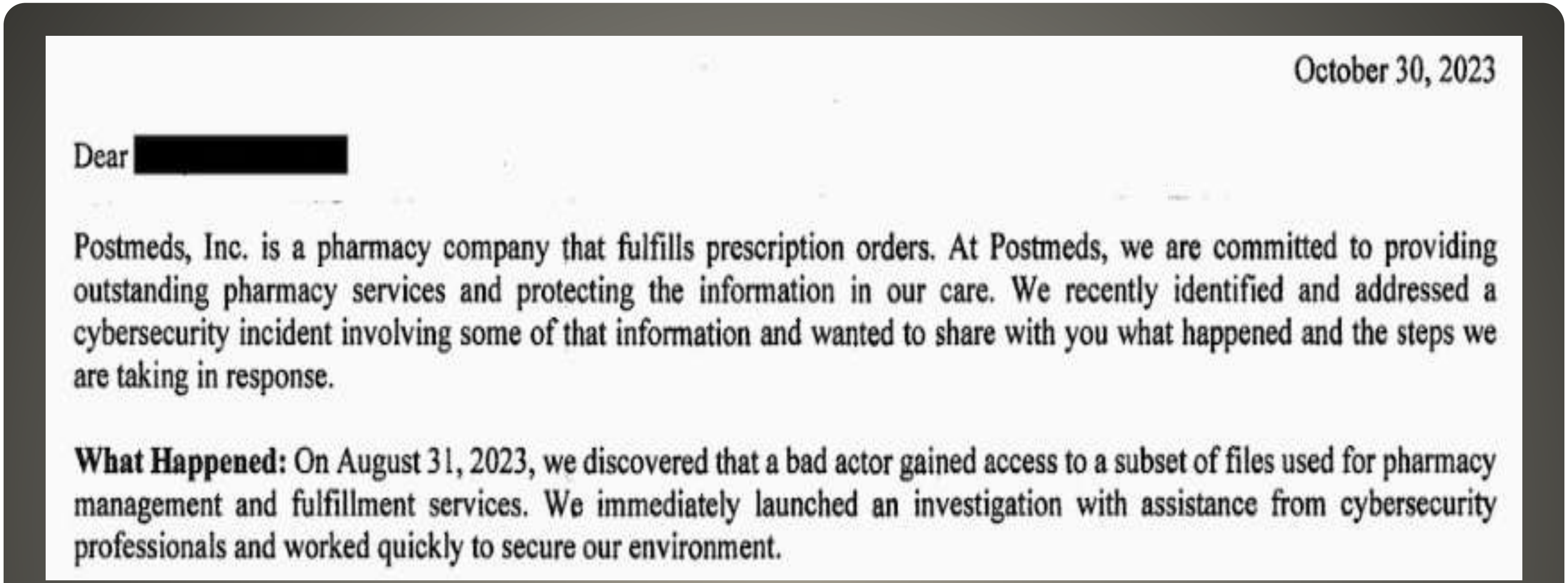
- Content credentials
- Meta Data
- Content Authority Initiative

+

- Project Origin
- Coalition for Content Provenance and Authenticity (C2PA)
- Toggle content credentials
- C2PA editing
- $9,195
- Smart Phones?
- Private key private??

- Hackers are users also

User Friendly



October 30, 2023

Dear [redacted]

Postmeds, Inc. is a pharmacy company that fulfills prescription orders. At Postmeds, we are committed to providing outstanding pharmacy services and protecting the information in our care. We recently identified and addressed a cybersecurity incident involving some of that information and wanted to share with you what happened and the steps we are taking in response.

What Happened: On August 31, 2023, we discovered that a bad actor gained access to a subset of files used for pharmacy management and fulfillment services. We immediately launched an investigation with assistance from cybersecurity professionals and worked quickly to secure our environment.

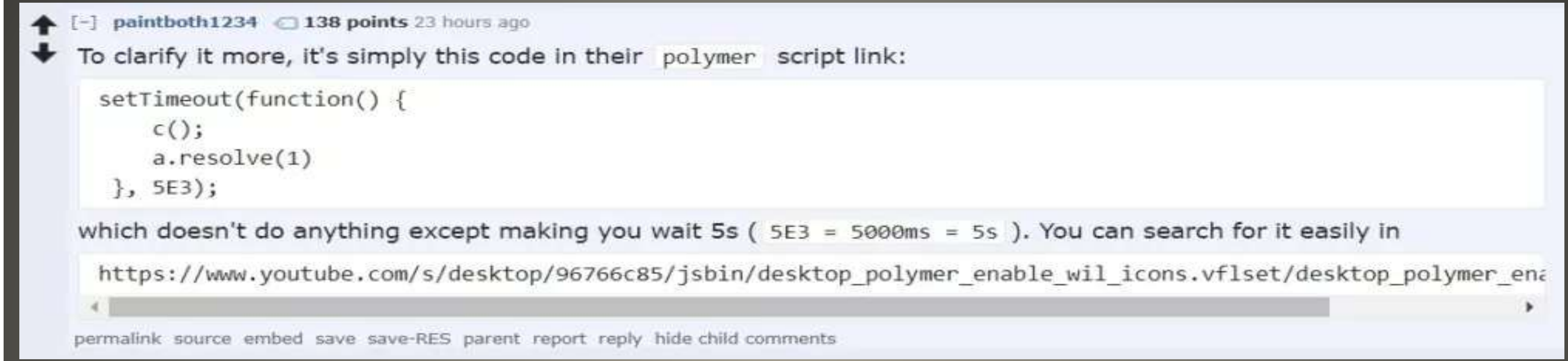
- HIMS and many more

Occurred in August Notification in October

Current Issues

- Ad Accelerator – Mute and fast forward YouTube ads
- iMessage bridge Nothing and Sunbird
  Pulled Severe privacy issues
  Log & retain messages
  Other users can gain access
- WhatsApp mods
  Trojan-spy.AndroidOS.CanesSpy
  Collects info of phone
  Contacts
  Microphone recordings

- YouTube 5 second delay? Ad view time



[–] paintboth1234 138 points 23 hours ago

To clarify it more, it's simply this code in their `polymer` script link:

```
setTimeout(function() {
    c();
    a.resolve(1)
 }, 5E3);
```

which doesn't do anything except making you wait 5s (`5E3 = 5000ms = 5s`). You can search for it easily in

```
https://www.youtube.com/s/desktop/96766c85/jsbin/desktop_polymer_enable_wil_icons.vflset/desktop_polymer_ena
```

permalink source embed save save-RES parent report reply hide child comments

- Zimbra Collaboration email server
  World governments attacked
- Social Links ChatGPT OSINT
  sentiment analysis
  Kicked off Facebook & Instagram
- FTC voice cloning challenge

Current Issues

- Tokelau dependent territory New Zealand .tk TLD
- Welltok data breach yet another MOVEit 8.5 million people
- Proton Drive available for Mac
- Apple Fingerprint Reader future?
- Henry Schein Healthcare cyber attack
- Gulf Air data breach
- Microsoft 365 browser extension shutdown
- ownCloud vulnerability
- CrushFTP
- ApacheMQ messaging
- Google Workspace design flaw?
- BLUFFS break secrecy of Bluetooth

Current Issues

BLUFFS

Series of exploits against standard

Core Specification 4.2 through 5.4

Session key derivation process

Past & future

Short key -> brute force

Windows Hello Fingerprint

- Windows Hello Fingerprint authentication
  Fingerprint sensor “match on Chip”
  Microsoft Secure Device Protection unused
  Dell, Lenovo, Microsoft
  Windows Hello facial scan, iris scan, fingerprint
  Sensors Goodix, Synaptics, ELAN
- Secure Device Protection Protocol
  Ensuring fingerprint device is trusted
  Ensuring fingerprint device is healthy
  Protecting input fingerprint device and host

Device owner physically present?
host trust genuine device
host trust device isn’t hacked or modified
data from device protected

Windows Hello Fingerprint

- SDCP

  end-to-end channel device – host

  Secure boot certificate & private key

  Dell

  Linux and Windows database

  Lenovo

  Key for encryption name & serial number

  Surface Cover

  USB clear text number of prints enrolled

Highly targeted attack - physical possession

Stolen

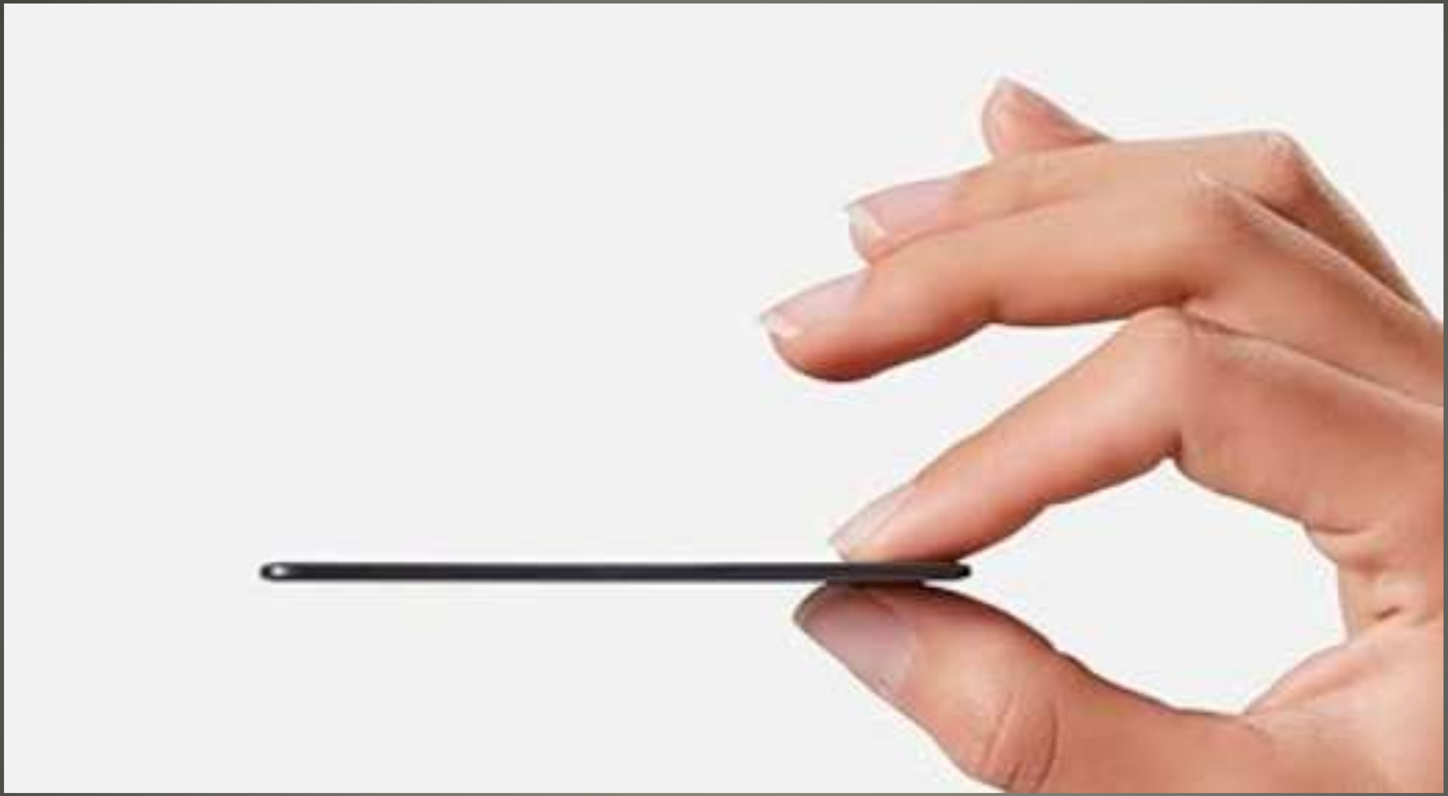
Ransomware Escalations

- Encryption
- DDoS Attacks
- Exfiltration for more ransom
- Release data   Sell data
- Notify victim’s customers
- Notify SEC

- Open-Source Intelligence
- onX Hunt
- Property Owner
- GPS & elevation

OSINT

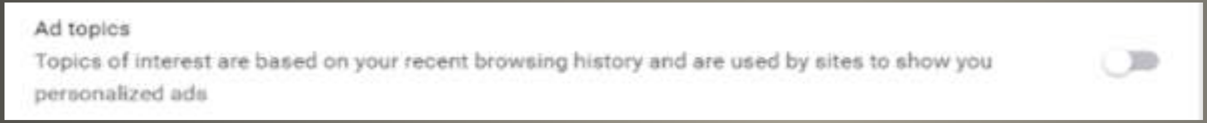
20 years later and all of these things fit in your pocket.



AirTag for wallets

- Really?
- Fit for Purpose

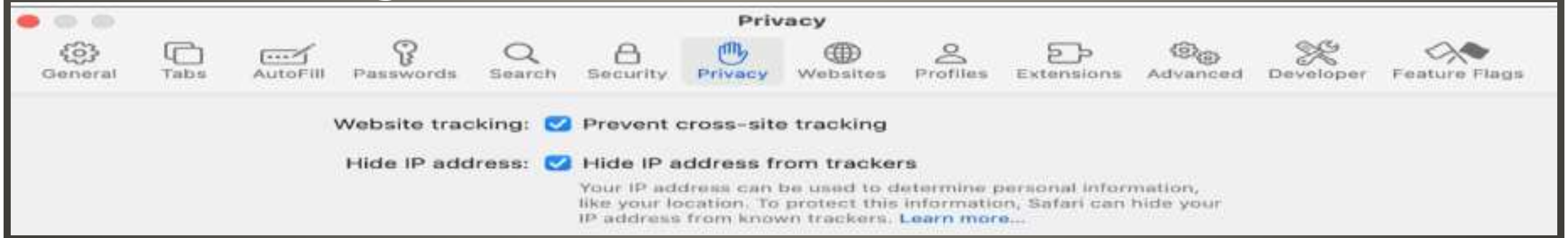
- Privacy Sandbox
- Third Party cookies > Privacy Sandbox
- Individuals > Groups



Ad topics

Topics of interest are based on your recent browsing history and are used by sites to show you personalized ads

- IP Protection
- Sites can not easily determine visitor’s IP
- IP routed through Google servers
- Thus, Google can



Website tracking: ☑ Prevent cross-site tracking

Hide IP address: ☑ Hide IP address from trackers

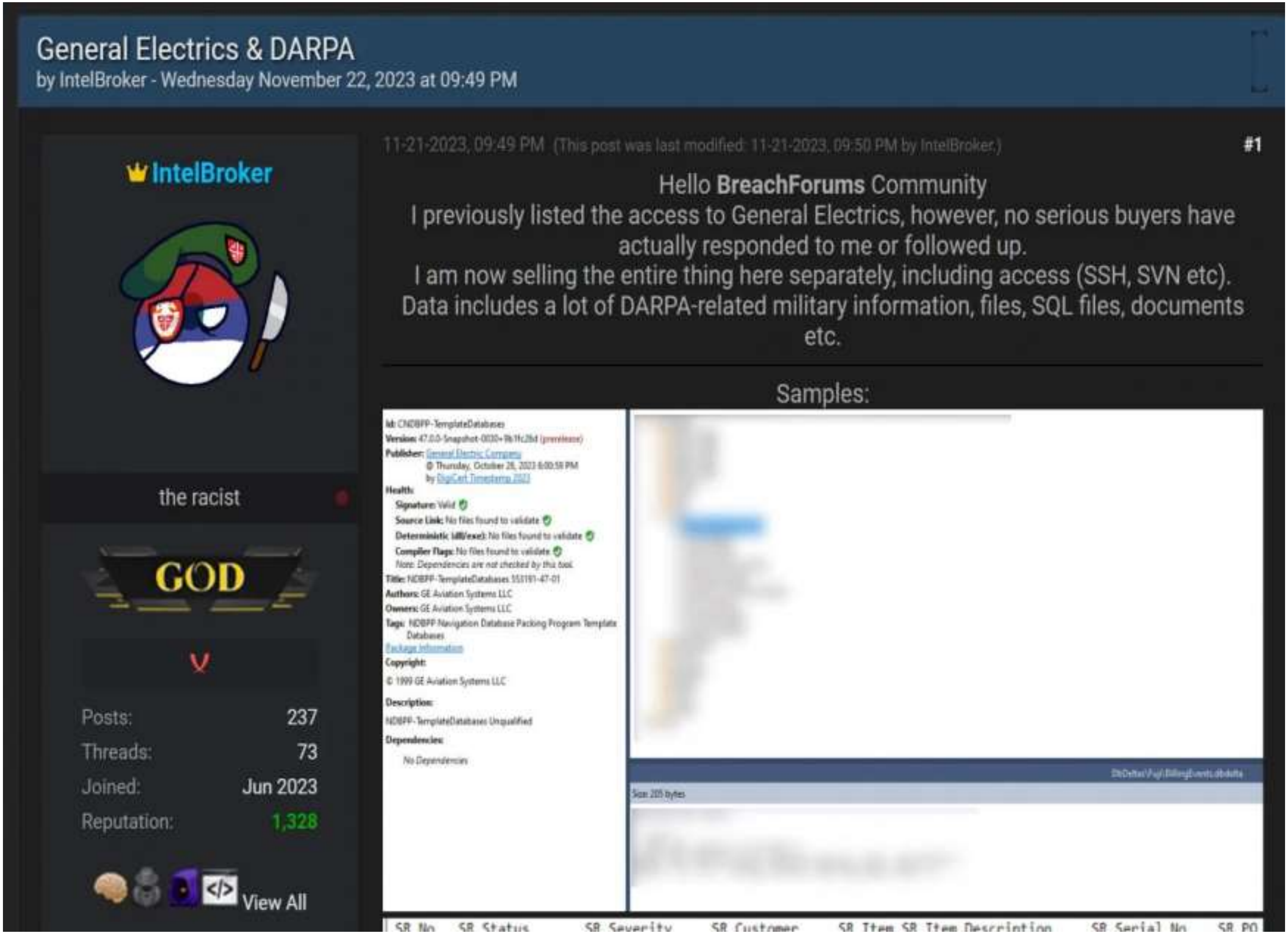
Your IP address can be used to determine personal information, like your location. To protect this information, Safari can hide your IP address from known trackers. Learn more...

Chrome Privacy

- Stronger protections w/o cellular or Internet
- USB and/or NFC
- Widely used/supported
- Most support multiple keys / methods

- Purchase costs
- What if no USB port nor NFC support?
- Sharing account? Sharing HW keys
- Keys can be lost

Hardware Security Keys



General Electrics & DARPA

by IntelBroker - Wednesday November 22, 2023 at 09:49 PM

11-21-2023, 09:49 PM (This post was last modified: 11-21-2023, 09:50 PM by IntelBroker.) #1

Hello **BreachForums** Community
I previously listed the access to General Electrics, however, no serious buyers have actually responded to me or followed up.
I am now selling the entire thing here separately, including access (SSH, SVN etc).
Data includes a lot of DARPA-related military information, files, SQL files, documents etc.

Samples:

Id: CNDBFP-TemplateDatabases
Version: 47.0.0-Snapshot-0030+9b1fc28d (prerelease)
Publisher: General Electric Company
@ Thursday, October 26, 2023 6:00:58 PM
by DigiCert Timestamp 2023
Health:
Signature: Valid ✓
Source Link: No files found to validate ✓
Deterministic (dll/exe): No files found to validate ✓
Compiler Flags: No files found to validate ✓
Note: Dependencies are not checked by this tool.
Title: NDBFP-TemplateDatabases 553191-47-01
Authors: GE Aviation Systems LLC
Owners: GE Aviation Systems LLC
Tags: NDBFP Navigation Database Packing Program Template Databases
Package Information
Copyright:
© 1999 GE Aviation Systems LLC
Description:
NDBFP-TemplateDatabases Unqualified
Dependencies:
No Dependencies

DbDeltas\Fuji\BillingEvents.dbdelta
Size 205 bytes

```
SR No   SR Status      SR Severity    SR Customer    SR Item SR Item Description    SR Serial No    SR PO
```

Lumma malware

- Lumma Stealer
- Restore expired Google authentication cookies
- Malware-as-a-service $1000/mo
- Rhadamanthys (copy?)

New Vulnerabilities

- Add thousands of devices to Mirai botnet

  Network video recorder

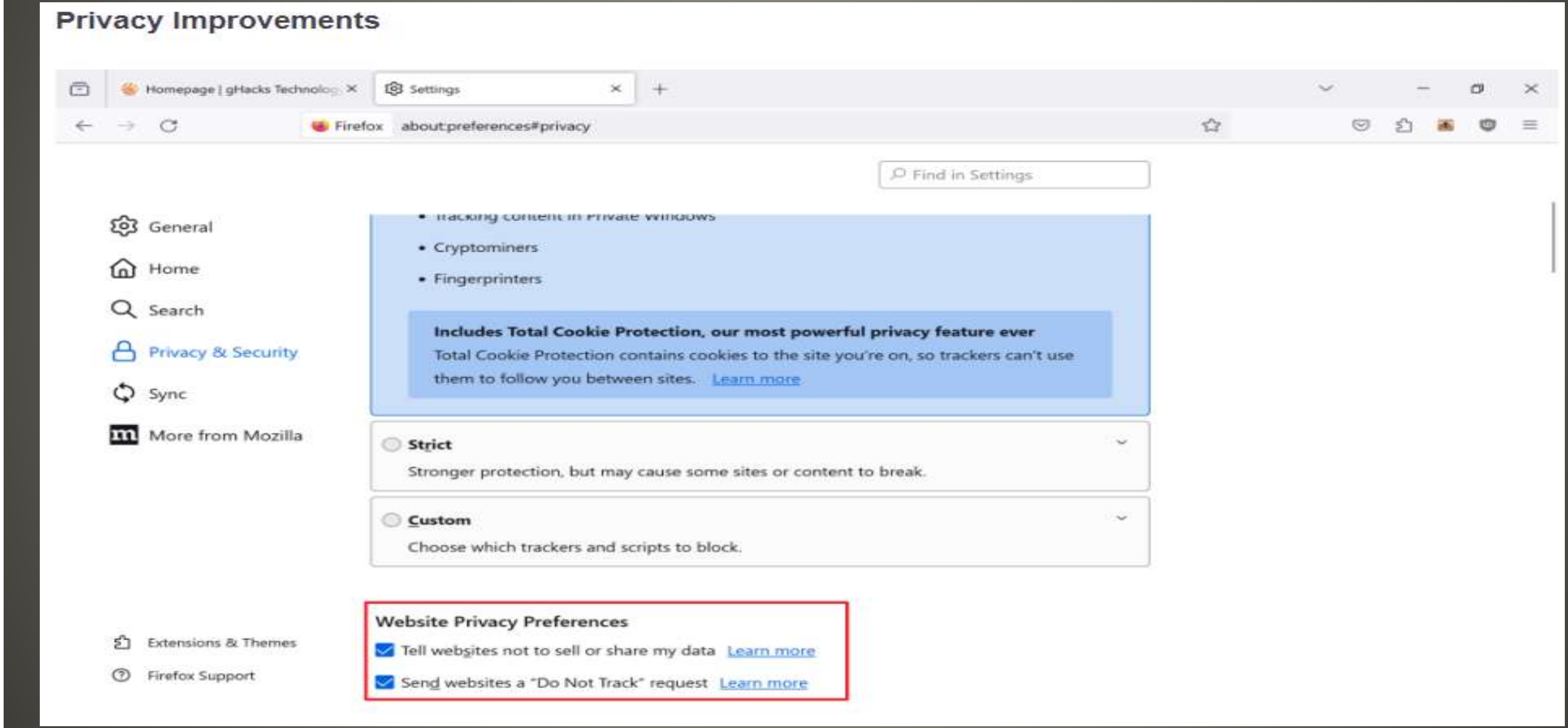
  Outlet-based wireless LAN route
- CyberLink multimedia company

  Installer with malware

  Code signing certificate stolen
- QR code scanned – posted LARGE BILL
- QR code Bank of America transfers

- Version 120.0

Global Privacy Control Opt-in



Privacy Improvements

- Tracking content in Private Windows
- Cryptominers
- Fingerprinters

Includes Total Cookie Protection, our most powerful privacy feature ever
Total Cookie Protection contains cookies to the site you're on, so trackers can't use them to follow you between sites. Learn more

○ **Strict**
Stronger protection, but may cause some sites or content to break.

○ **Custom**
Choose which trackers and scripts to block.

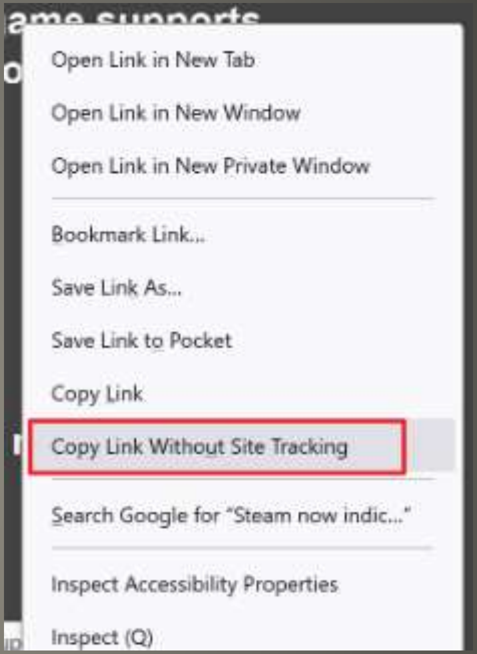
Website Privacy Preferences

☑ Tell websites not to sell or share my data Learn more

☑ Send websites a "Do Not Track" request Learn more

Firefox 120

- Copy Link without Site Tracking
  right-click to copy link



Open Link in New Tab

Open Link in New Window

Open Link in New Private Window

Bookmark Link...

Save Link As...

Save Link to Pocket

Copy Link

Copy Link Without Site Tracking

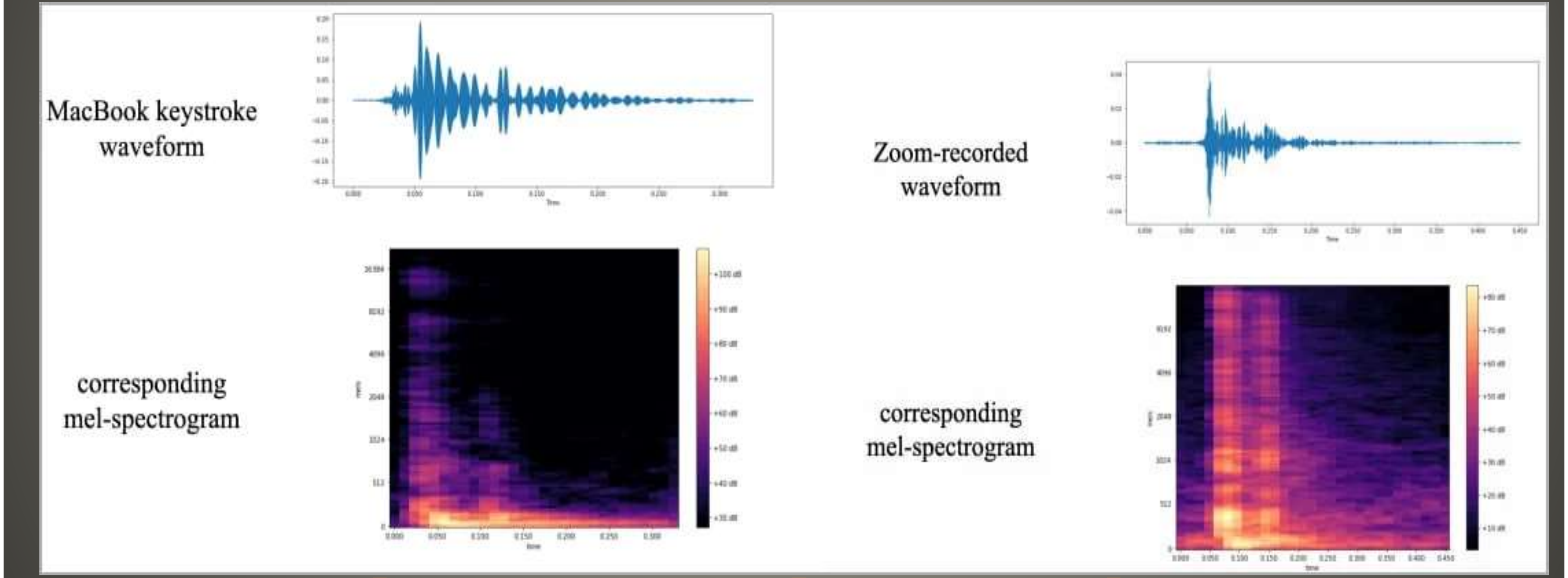
Search Google for "Steam now indic..."

Inspect Accessibility Properties

Inspect (Q)

Firefox 120

- Deep learning model
- 95% accuracy (using zoom 93%)
- Zoom Chat (text typed and sound)



Keystroke Acoustic attack 8/17/2023

Now exploited
Keystroke acoustic attack

- AI technology
- No need to compromise devices
- Listen as you enter password/passphrase
- Microphones, VoIP, smartwatch, …
- Protections:
- Disconnect Microphone
- Create null microphone
- Mix case
- MFA
- Enable alerts
- Updates
- Link cautions

HasMySecretLeaked checker

- Without exposing the secret(s)
- GitHub 10 million “secrets”
- Secret fingerprinting protocol
- Encrypts and hashes secret - locally

OpenAI backstory?

- CEO Sam Altman

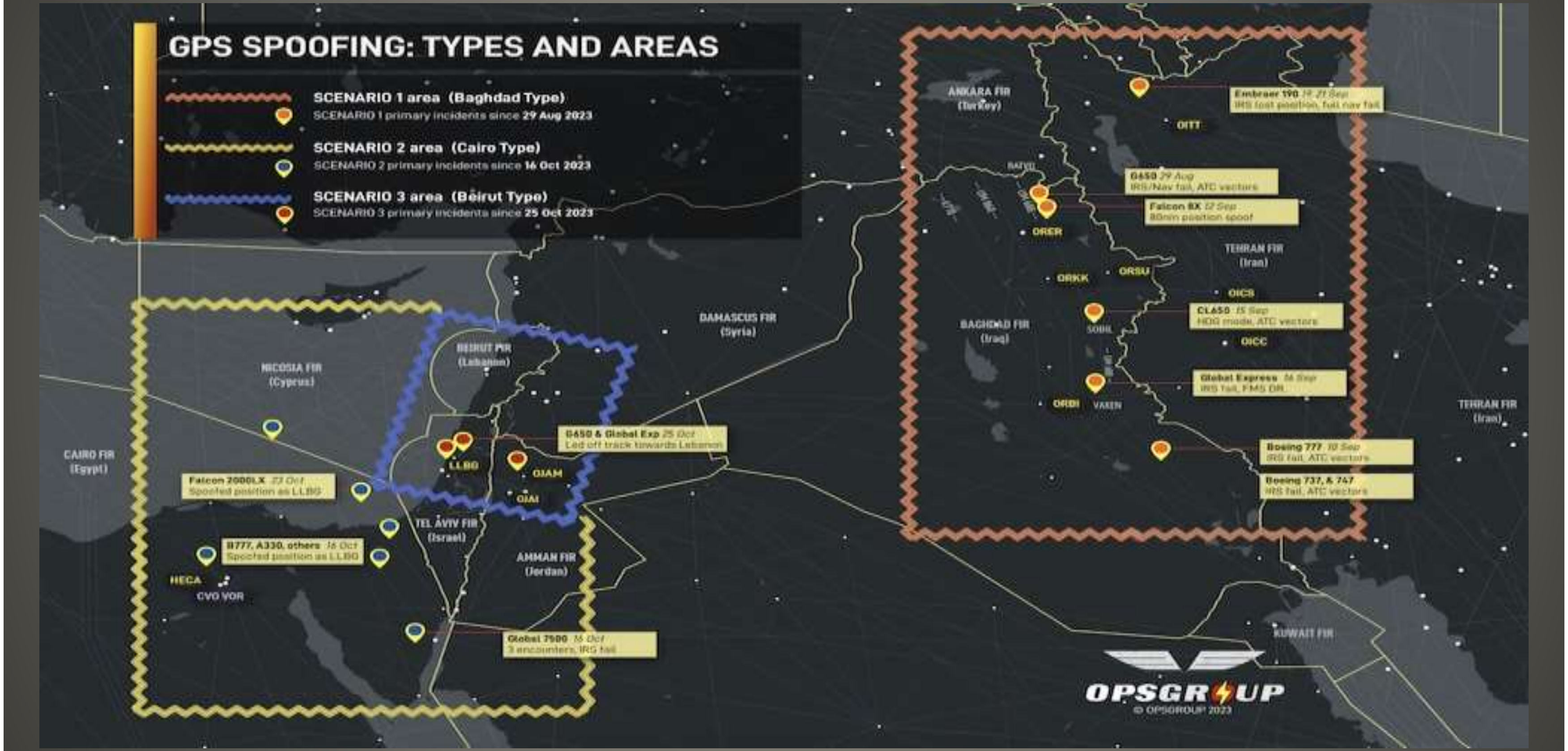
"on a personal note, just in the last couple of weeks, I have gotten to be in the room, when we sort of like push the sort of the veil of ignorance back and the frontier of discovery forward,“

- Reasoning
- Emergence
- Project Q* (Q star)

Current Issues

- DOJ surveillance program
  Hemisphere   NYT 2013 disclosure
  Lawful subpoena
  BUT storage of decades of data?
- Ukraine dismisses 2 top cybersecurity officials
  Western cybersecurity impact?
- Tor removes “risky” relays
- CitrixBleed – UK CTS (managed service provider)
  law firms
  hospitals
  Feds warned BUT
- US Supreme court   fifth amendment protections
  Passcodes
- Court sealed documents increment by one

- GPS spoofing attacks



GPS SPOOFING: TYPES AND AREAS

SCENARIO 1 area (Baghdad Type)
SCENARIO 1 primary incidents since 29 Aug 2023

SCENARIO 2 area (Cairo Type)
SCENARIO 2 primary incidents since 16 Oct 2023

SCENARIO 3 area (Beirut Type)
SCENARIO 3 primary incidents since 25 Oct 2023

Embraer 190 19, 21 Sep
IRS lost position, full nav fail

G650 29 Aug
IRS/Nav fail, ATC vectors

Falcon 8X 12 Sep
80nm position spoof

CL650 15 Sep
HDG mode, ATC vectors

Global Express 14 Sep
IRS fail, FMS DR

Boeing 777 10 Sep
IRS fail, ATC vectors

Boeing 737, & 747
IRS fail, ATC vectors

G650 & Global Exp 25 Oct
Led off track towards Lebanon

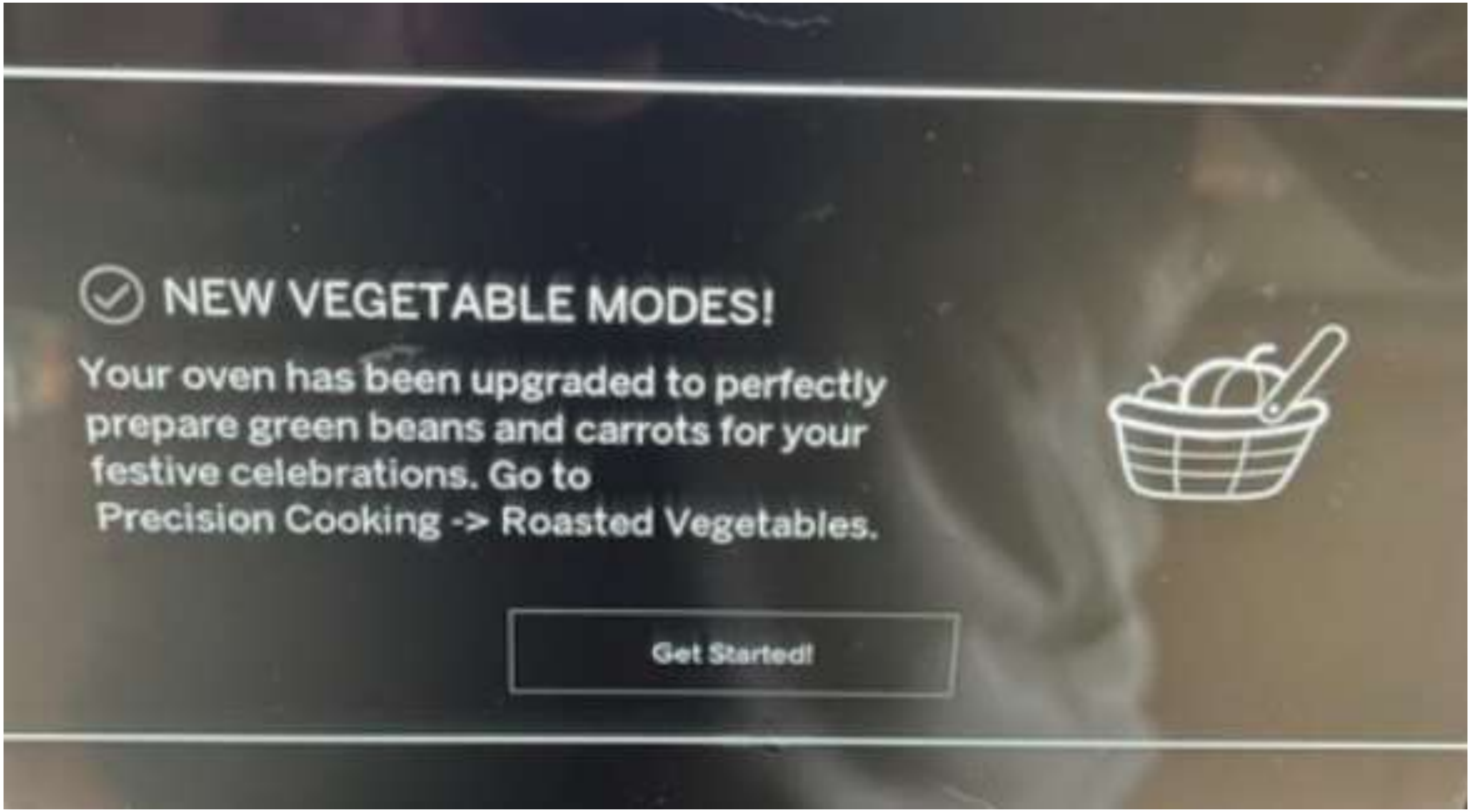
Falcon 2000LX 23 Oct
Spoofed position as LLBG

B777, A330, others 16 Oct
Spoofed position as LLBG

Global 7500 16 Oct
3 encounters, IRS fail

© OPSGROUP 2023

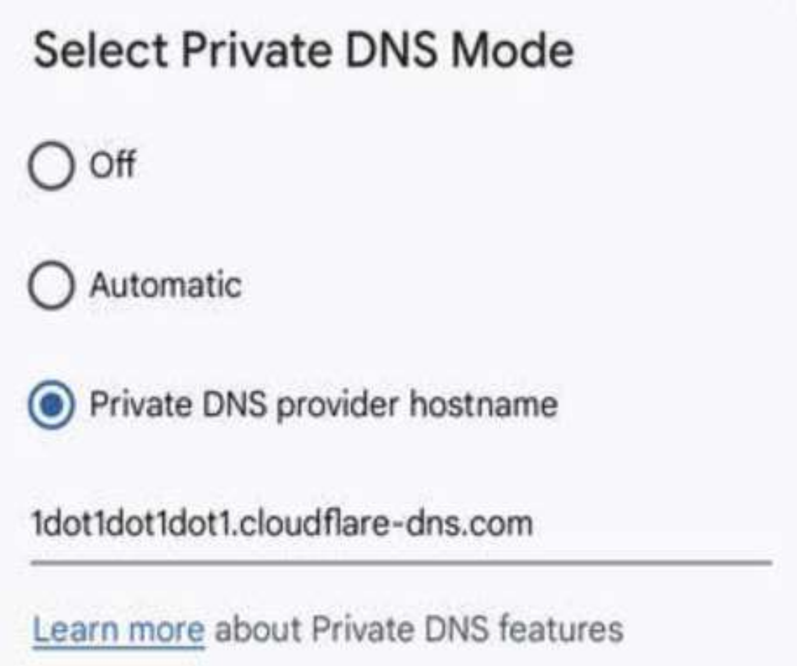
Current Issues



✓ NEW VEGETABLE MODES!

Your oven has been upgraded to perfectly prepare green beans and carrots for your festive celebrations. Go to Precision Cooking -> Roasted Vegetables.

- Android version 9 or higher
- Settings > Network & Internet
- Private DNS
- dot1dot1dot1.cloudflare-dns.com
- Google DNS: dns.google
- Quad9: dns.quad9.net
- Open DNS: 208.67.222.222
- NextDNS: 45.90.28.0
- Comodo Secure 8.26.56.26
- OpenNIC: 192.95.54.3



Select Private DNS Mode

○ Off

○ Automatic

● Private DNS provider hostname

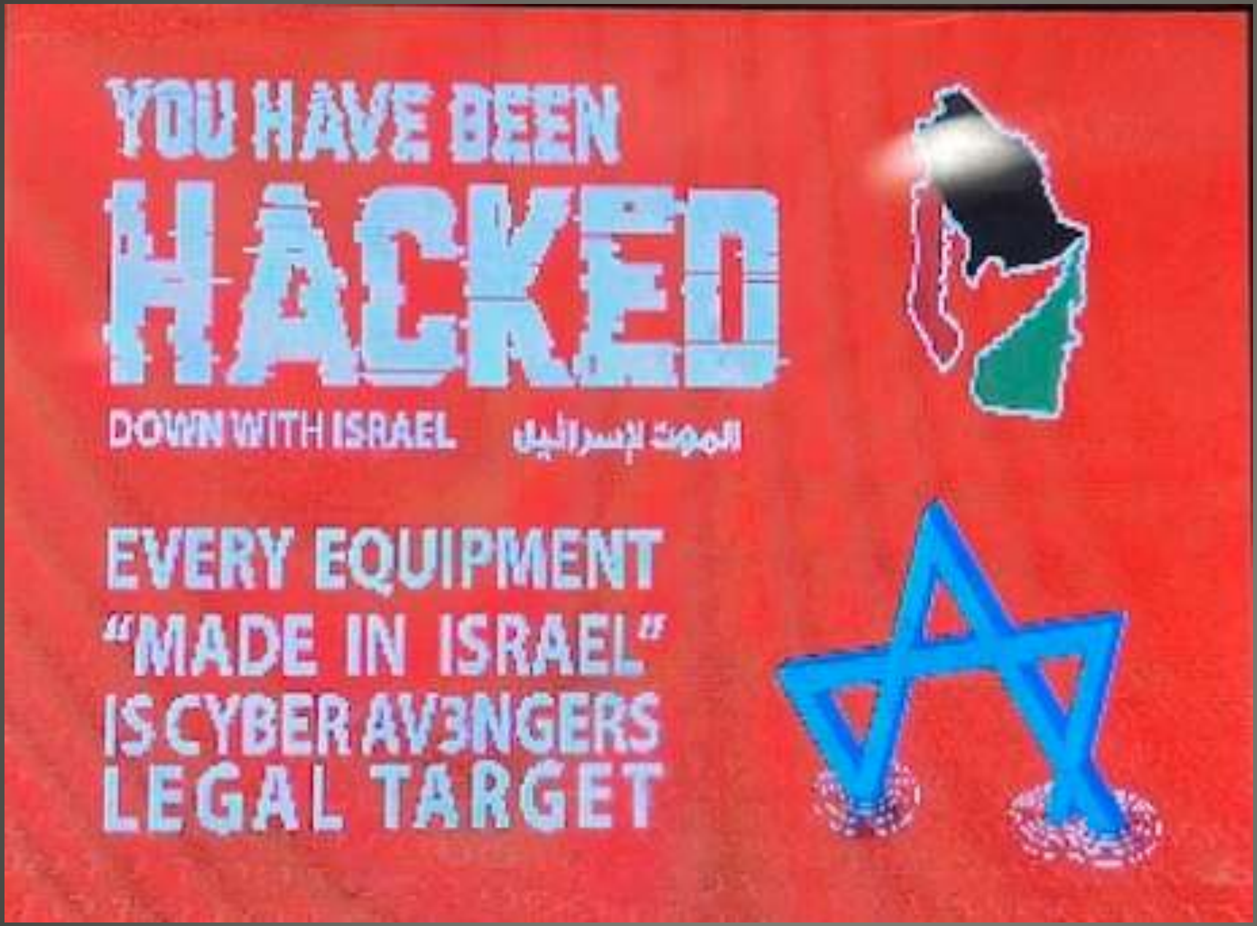
1dot1dot1dot1.cloudflare-dns.com

Learn more about Private DNS features

Android Private DNS

Current Issues

- FTC and Federal agent
  Ongoing investigation $30K
- Zoom Room vulnerability
- Samsung Galaxy S24 “First AI Phone”
- Okta data breach
  Was 134 customers ->
  All customers with support contacts
- Dollar Tree data breach 2 million customers
- CISA investigating water treatment plant breach
  Iran? PLC
- Zyxel NAS with Critical vulnerabilities
- OpenAI Custom Chatbots leak secrets



YOU HAVE BEEN HACKED

DOWN WITH ISRAEL الموت لإسرائيل

EVERY EQUIPMENT "MADE IN ISRAEL" IS CYBER AV3NGERS LEGAL TARGET

Unitronics PLCs - password 1111

- Chrome war on Ad Blockers

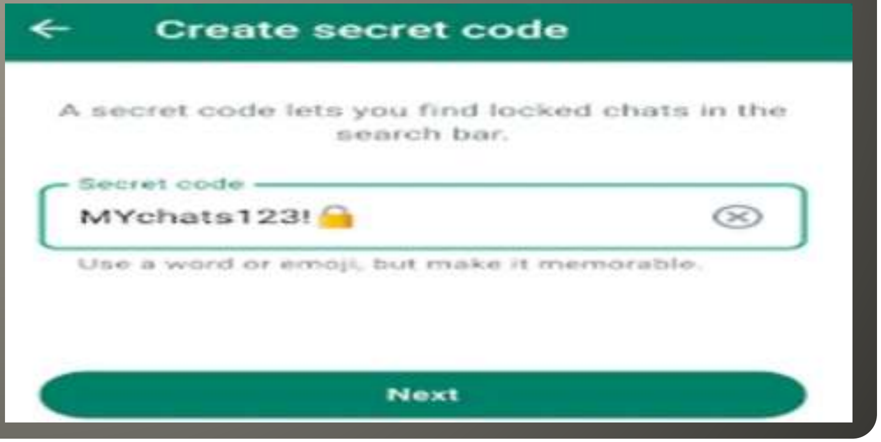
  Slower extension updates

  Manifest V3 extension platform

  Block ads on world’s biggest ad company
- WhatsApp protect chats Secret Code

  Chat Lock – separate folder

  Secret Code – find that folder



Create secret code

A secret code lets you find locked chats in the search bar.

Secret code: MYchats123! 🔒

Use a word or emoji, but make it memorable.

Current Issues

- Encrypts traffic Before ISP
- Clears or does not log history

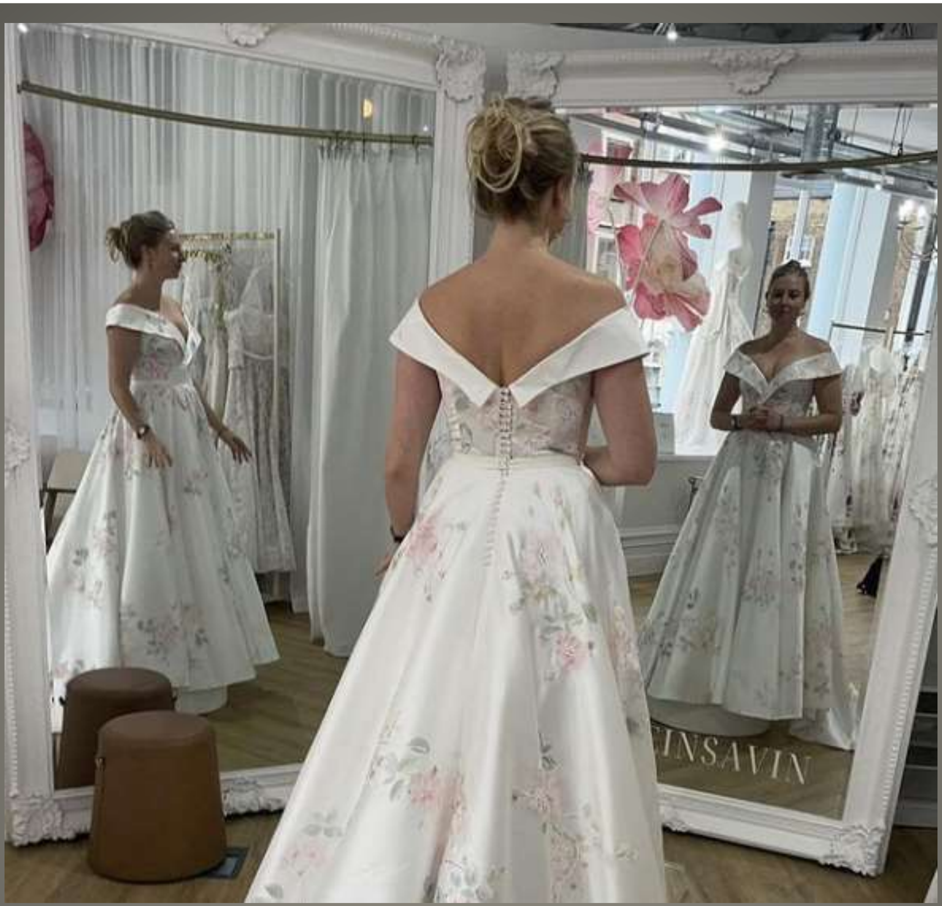
- Public or shared devices
- Private surfing
- Booking travel – price increase
- Hides IP address
- Multiple email accounts
- Sensitive search

Private Browsers

- Tor
- Brave
- Vivaldi
- DuckDuckGo

- Avast Secure Browser *
- Bromite
- Ecosia
- Epic Privacy Browser
- I2P

Private Browsers



AI in camera processing - mirror

Chrome reverse image search

- Recently replaced by Google Lens
- Google Lens – snap picture ask
- Google reverse image – search where
- Google – camera icon load picture
- Not quite the same
- **chrome://flags/#enable-lens-standalone** **Enable Lens Feature in Chrome** Disable Relaunch

- Right click on image
- **Search image with Google**

Microsoft Outlook App

- Windows Mail & classic Outlook replacement
- Microsoft Store
- New Design
- Email & Calendar
- Generative AI
- Cloud integration - Microsoft Cloud integration
- Credentials provided used by Microsoft

Wrapper around Microsoft’s cloud services

Current Issues

- Amazon ban sale Flipper Zero
  Credit Card skimming
  Pranks
- Adobe Flash Player ghost?
  Potential for issues?
  December 2020
- Mobile password managers on Android
  AutoSpill
  1Password, LastPass, Keeper, Enpass
  Even if JavaScript disabled
  Vendors working on a fix
- HTC Global Services – IT services Cyber attack
- TEXAS BITCOIN MINING OPERATION SHUTDOWN BY HOST’S ARMED SECURITY

A 125MW Bitcoin mining facility run by Rhodium Enterprises was forced to shutdown last week by Rockdale, TX site operator and Riot Platform’s subsidiary Whinstone Inc. after armed security entered the premises.

- Surveil smartphone users via push notifications
- Senator Ron Wyden letter to DOJ
- Repeal / modify policies hindering public discussions
- Then Apple
- "In this case, the federal government prohibited us from sharing any information," the company said in a statement. "Now that this method has become public we are updating our transparency reporting to detail these kinds of requests.‟
- Which governments and how long?
- Encryption of notification message, BUT metadata

Push Notifications

- Bot management & security platform

Breaking-Bad-Bots-Bot-Abuse-Analysis-and-Other-Fraud-Benchmarks

- 73% web & app traffic malicious Q3 2023
- SMS toll fraud, web scraping, card testing and more
- Bots, intelligent bots, human fraud farms
- Bots – 167% increase
- Intelligent bots 291% increase
- Human fraud farms 49% increase
- Generative AI Cybercrime-as-a-service

Arkose Labs study

Arkose Labs study

- Travel & hospitality

  scrape prices, reviews, availability

  Book with stolen credit cards / loyalty points
- Gift cards – redeeming & reselling
- Arkose Labs – consortium biggest companies
- Fake accounts, credential stuffing, SMS toll fraud

  First steps for targeted attacks
- SMS toll fraud

  Create fake accounts with premium toll charges

  Generate traffic

  Financial loss -

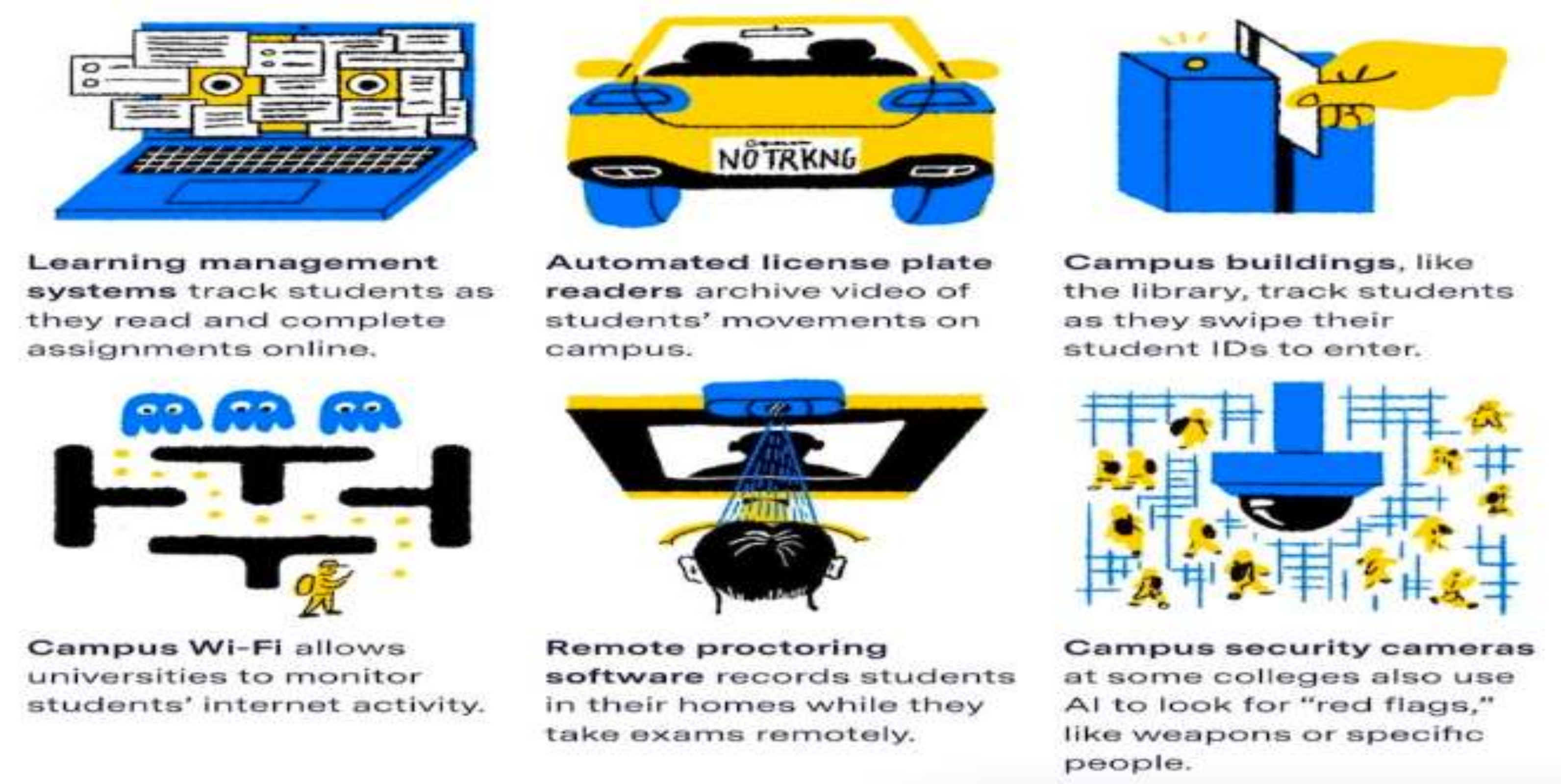
Google Mail

- Resilient and Effective Text Vectorizer
  RETVec
  Natural language processing
  Harmful messages prevented

Vulnerable Microsoft Exchange Servers

- 30,635
- Exchange Server 2007 – 275 instances
- Exchange Server 2010 – 4062 instances
- Exchange Server 2013 – 26,298

- Mt. San Antonio College Los Angeles
- Surveillance



Learning management systems track students as they read and complete assignments online.

Automated license plate readers archive video of students' movements on campus.

Campus buildings, like the library, track students as they swipe their student IDs to enter.

Campus Wi-Fi allows universities to monitor students' internet activity.

Remote proctoring software records students in their homes while they take exams remotely.

Campus security cameras at some colleges also use AI to look for "red flags," like weapons or specific people.

College - privacy

- Increasing attack on customers
- Asking forums for more victims
- Admin portals -> guest records
- Pay criminals, not hotels

Booking.com

- Initial report 0.1% of customers
- Now 50% of customers
- Opt-in DNA Relatives
- Notifications “Data exposed”
- Not a data breach
- Just unauthorized access
- “a significant number of files containing profile information about other users’ ancestry.”
- Force password change & MFA
- US National Security Agency director:

  My account is unique – no credential stuffing
- Scraped data not breached data
- Changes to ToS
- Users can opt-out within 30 days of notice

23andMe

- Android December 2023 update

  85 vulnerabilities

  Critical zero-click RCE vulnerability

  CVE-2023-40088

  2023-12-01   2023-12-05

  Your Vendor May Vary
- Apple 6G modem chip
- Lenovo Chromebox Micro   Pixel size
- ExpressVPN support to Apple TVs

  Ability to watch region-locked content

  Ability not permission
- iTunes app discontinued Apple TV update
- Nissan investigating data breach
- Predatory loan apps – stealing Android data

Current Issues

- Microsoft 365 browser extension shutdown January 15, 2024

Williamson Co. EMS said 'data event' affected personal information of patients

On Aug. 10, EMS Management and Consultants, Inc. (EMS|MC) mailed notice letters to patients for a transition of their accounts as the new billing vendor for Williamson County EMS. However, during the mailing process, officials said the letter was mailed "as the ambulance point of pickup rather than the home address of the patient." The mis-mailed letters included patients' name, medical account number, incident number, date of transport and the balance due.

The notice can be read here.

Current Issues

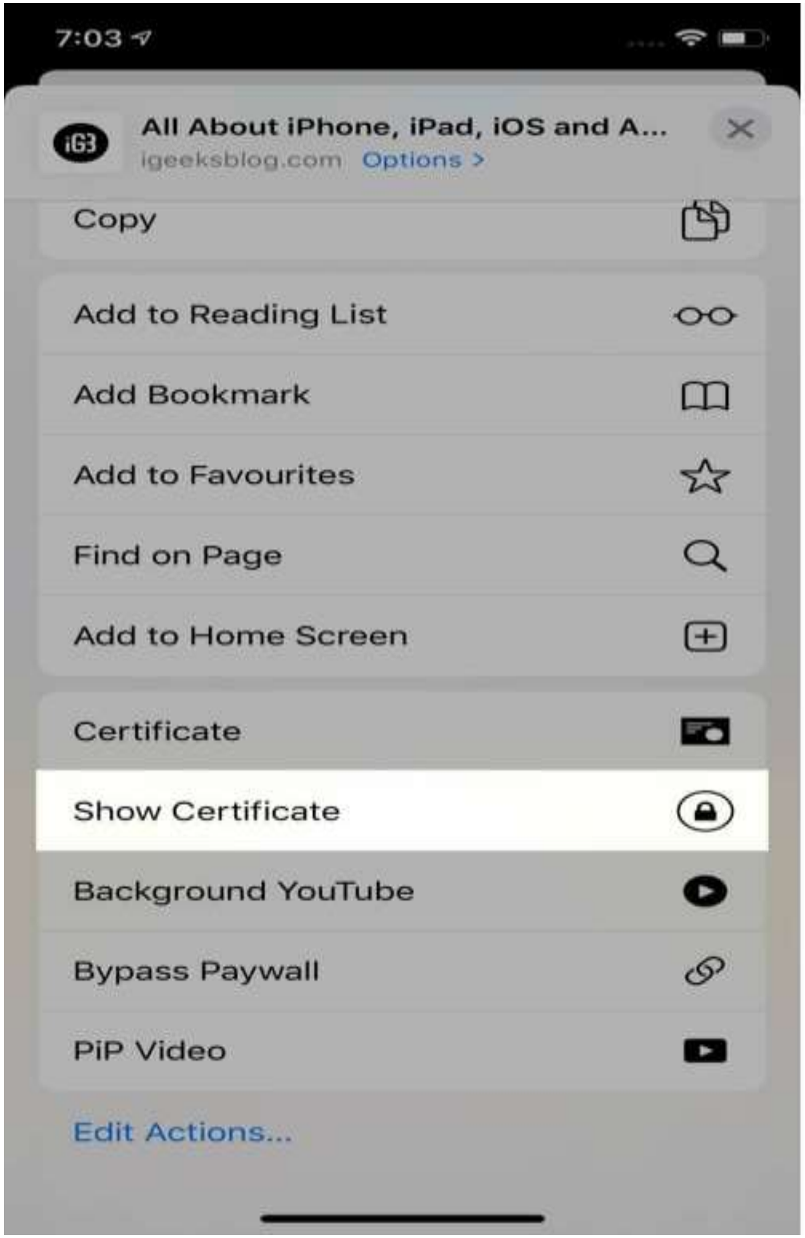
Mac Proxy malware Pirated software

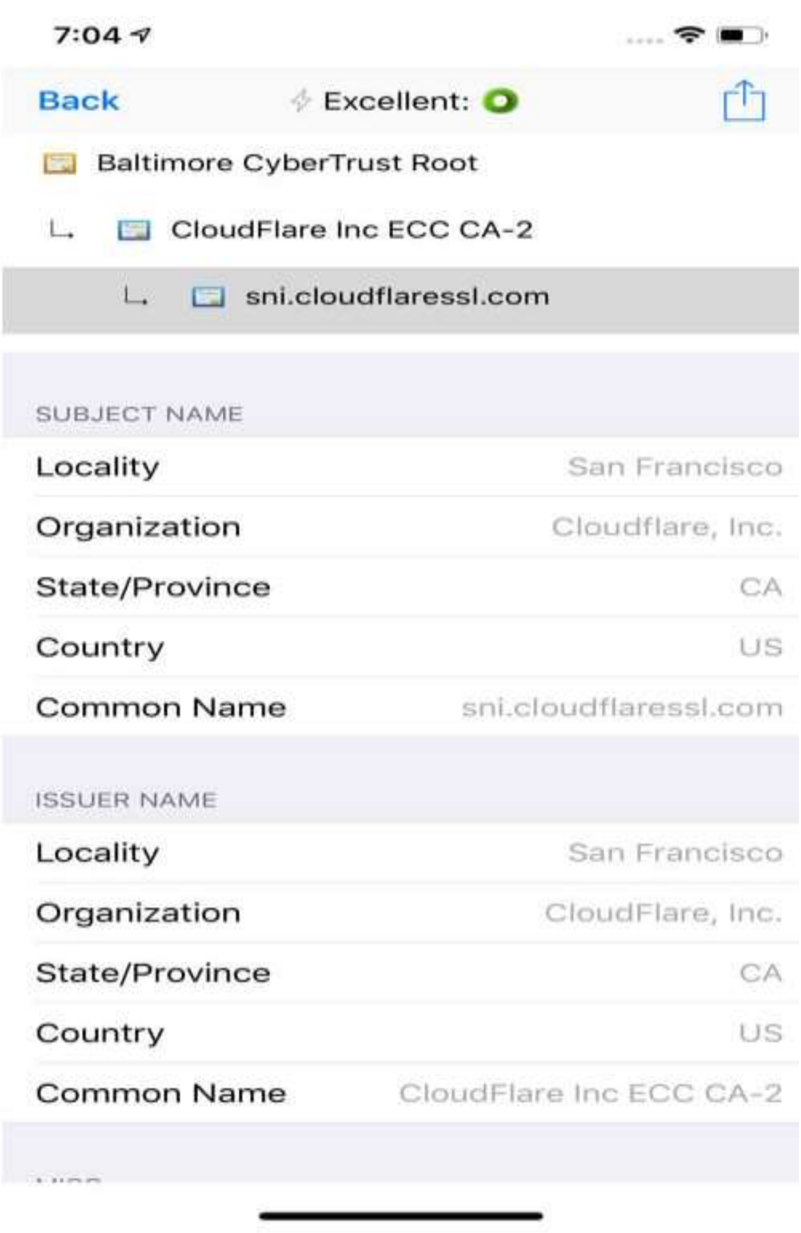
- Bundled in popular copyrighted macOS software
- Proxy trojan malware infects computers, turning them into traffic-forwarding terminals used to anonymize malicious or illegal activities such as hacking, phishing, and transactions for illicit goods.
- 4K Video Donwloader Pro
- Aissessoft Mac Data Recovery
- Aiseesoft Mac Video Converter Ultimate
- AnyMP4 Android Data Recovery for Mac
- Downie 4
- FonePaw Data Recovery
- Sketch
- Wondershare UniCoM101nverter 13
- SQLPro Studio
- Artstudio Pro

Quishing

- Quick Response
- URLs, text, map addresses, …
- Restaurant, parking meters
- Friends, family, clubs
- No Link
- iPhone Safari

  Share icon





Baltimore CyberTrust Root

└ CloudFlare Inc ECC CA-2

└ sni.cloudflaressl.com

SUBJECT NAME

Locality	San Francisco
Organization	Cloudflare, Inc.
State/Province	CA
Country	US
Common Name	sni.cloudflaressl.com

ISSUER NAME

Locality	San Francisco
Organization	CloudFlare, Inc.
State/Province	CA
Country	US
Common Name	CloudFlare Inc ECC CA-2

- Check Digital Certificate BEFORE Entering sensitive information

Check Digital Certificate

- CISA warning (again)
  Adobe Cold Fusion vulnerability
  March
  Yet 2 recent detected incidents
- iPhone third-party keyboards with keyloggers
- WhatsApp Chat Lock (May) Device passcode or biometrics now Secret Code – separate password
- Montana TikTok ban Jan 1 oversteps state power
  Violates first amendment
  Anti-China not Montana citizen protections
  Project Texas Oracle move to Austin
- EU Cyber Resilience Act
  Processes to receive reports of vulnerabilities
  Support for 5 years
  Automatic security updates
  Data confidentiality via encryption
  Inform authorities of any attacks
  3 years to take affect

Current Issues

- One gang’s statistics:
  90 victims of 329 organizations
  $107 million $9M - $1.2M
  Better cryptocurrency tracking
  Better cyber insurance reporting

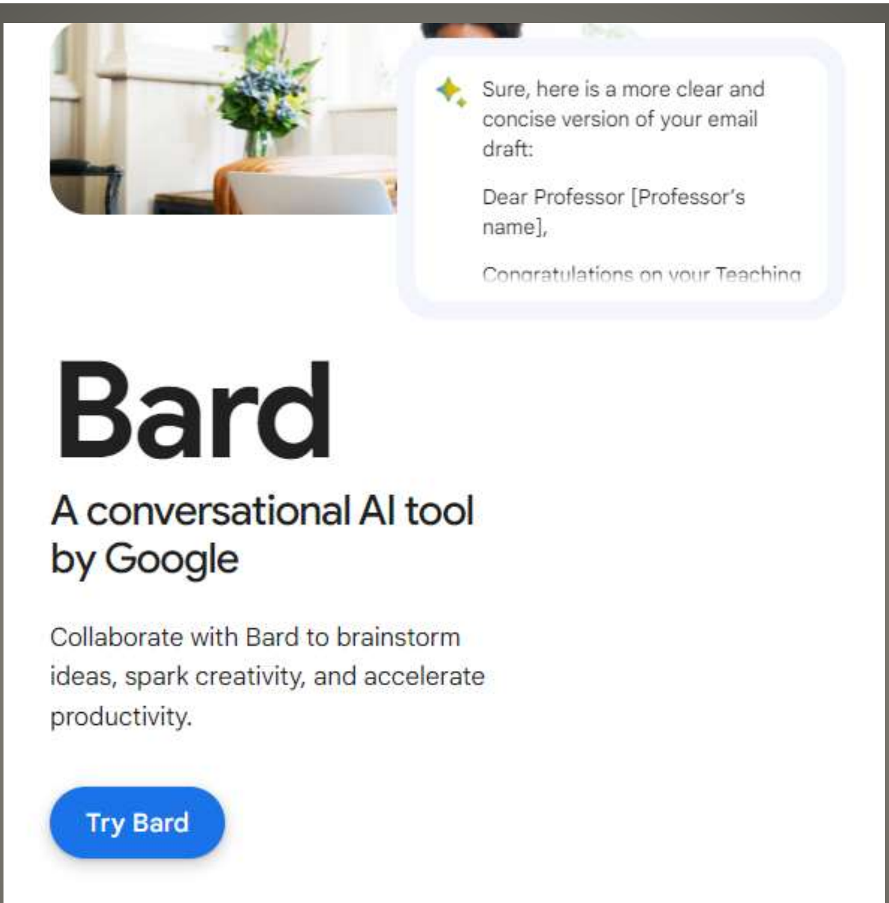
Ransomware

- Google announced 6-Dec-2023
- Gemini
- 3 Levels

  Nano, Pro, Ultra

  Advanced soon
- Pro available for trial (English only)
- bard.google.com

Bard update



Sure, here is a more clear and concise version of your email draft:

Dear Professor [Professor's name],

Congratulations on your Teaching

Bard

A conversational AI tool by Google

Collaborate with Bard to brainstorm ideas, spark creativity, and accelerate productivity.

- Device takeover
- Android, Linux, macOS, iDevices
- Authentication bypass
- Connect to susceptible device(s)
- Inject keystrokes
- Code execution of victim
- Bluetooth keyboard
- Attack from Linux computer in close range
- Android 4.2.2
- iDevice & macOS Magic Keyboard
- CVE-2023-45866

New Bluetooth flaw

UEFI firmware

- LogoFAIL
- Easy   Every manufacturer   Level of control
- Remotely executed post-exploit
- Bypass boot kit detections
- Unified Extensible Firmware Interface
- Manufacturer’s Logo   -   graphics rendering
- Fileless malware
- Place logo image -or- reflash firmware

- Meta Messenger end-to-end encryption

  By default

  Group chat requires opt-in

  Instagram <-> Facebook no longer

  next week

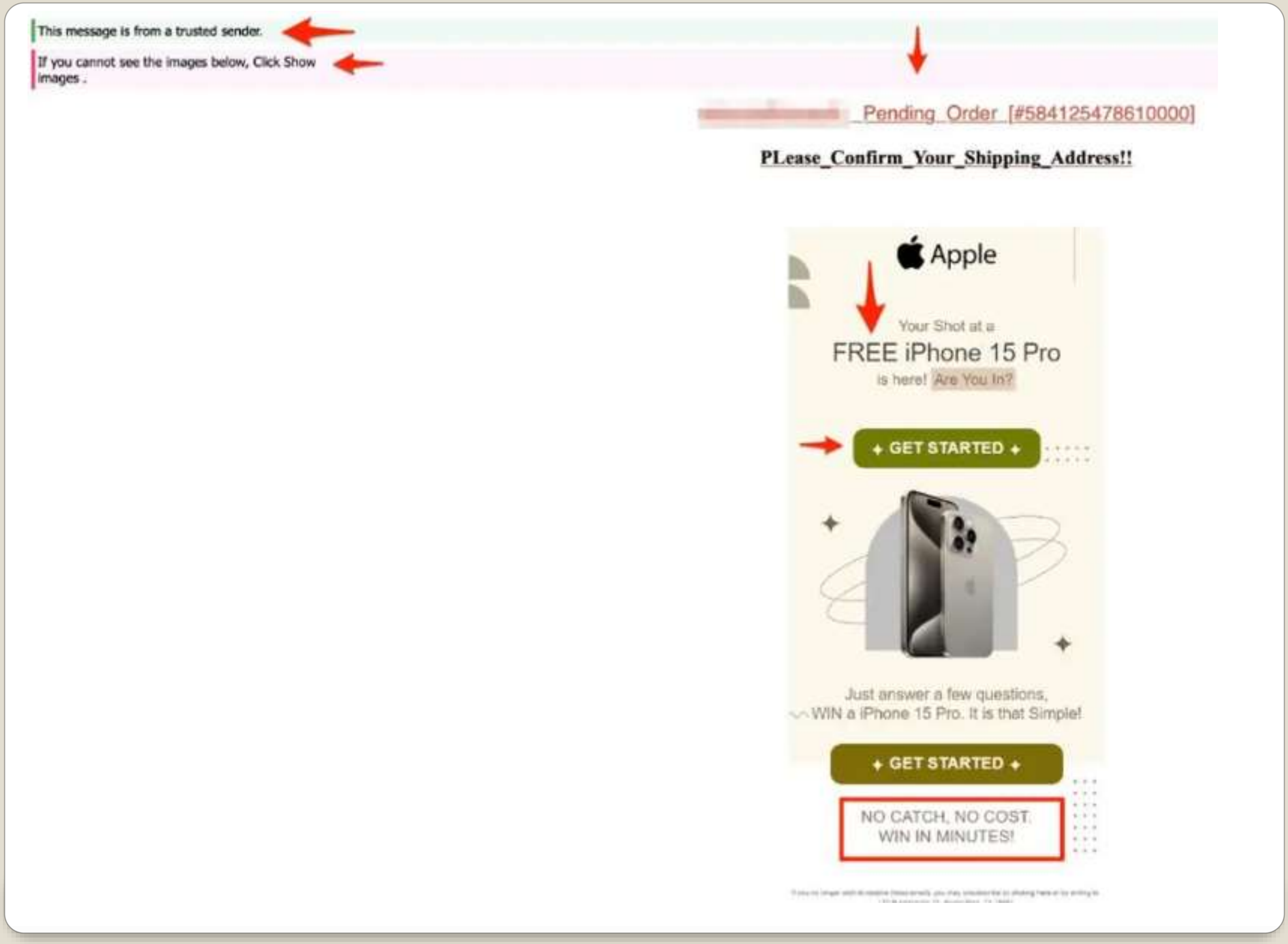
Current Issues

Phishing emails

Fox News

Kurt Knutson, CyberGuy

https://www.foxnews.com/tech/dont-fall-for-these-7-fake-phishing-emails



This message is from a trusted sender.

If you cannot see the images below, Click Show images .

[redacted] Pending Order [#584125478610000]

PLease_Confirm_Your_Shipping_Address!!

Your Shot at a

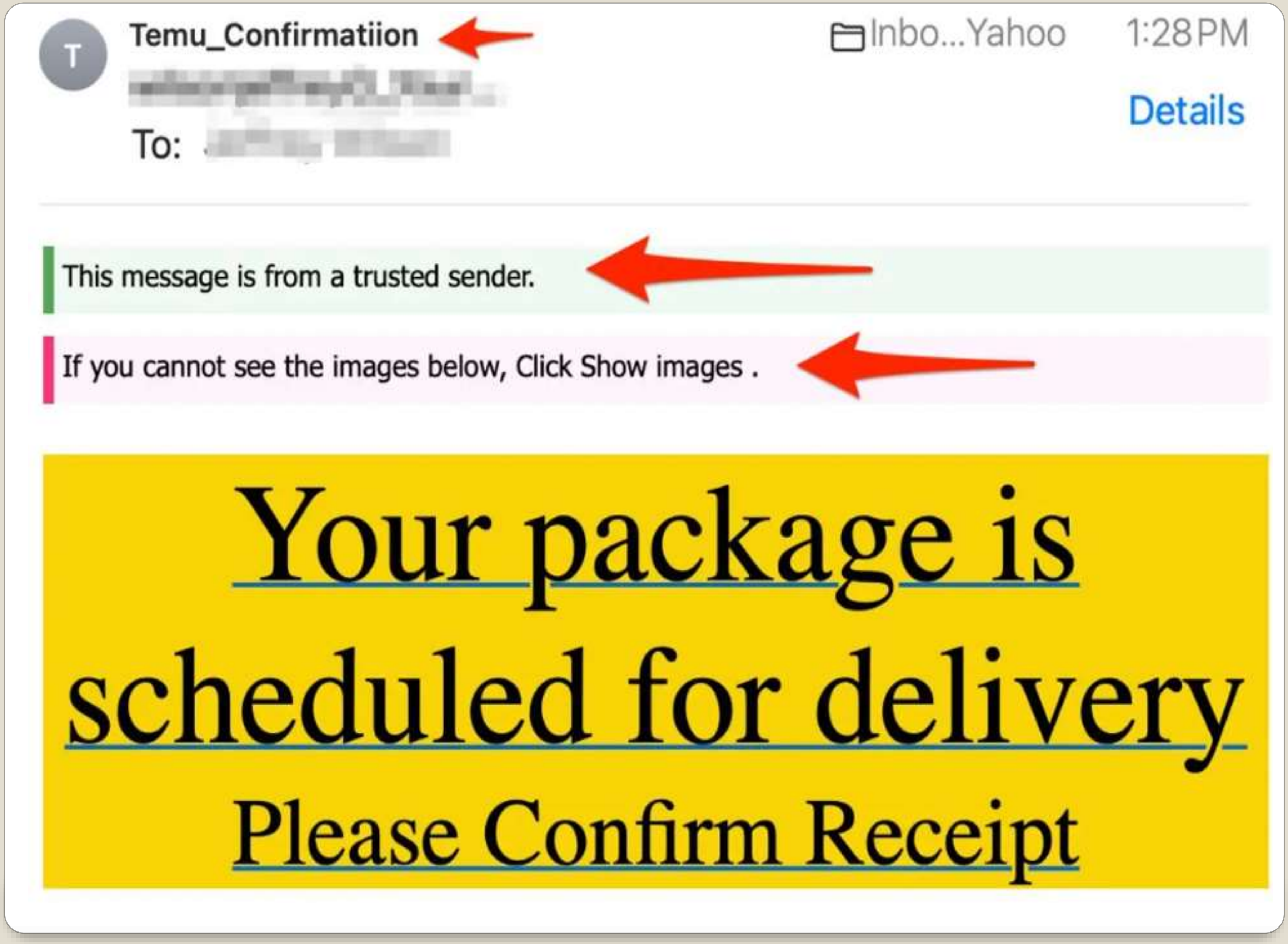
FREE iPhone 15 Pro

is here! Are You In?

Just answer a few questions,
WIN a iPhone 15 Pro. It is that Simple!

NO CATCH, NO COST.
WIN IN MINUTES!

[illegible]



Temu_Confirmatiion

[redacted]

To: [redacted]

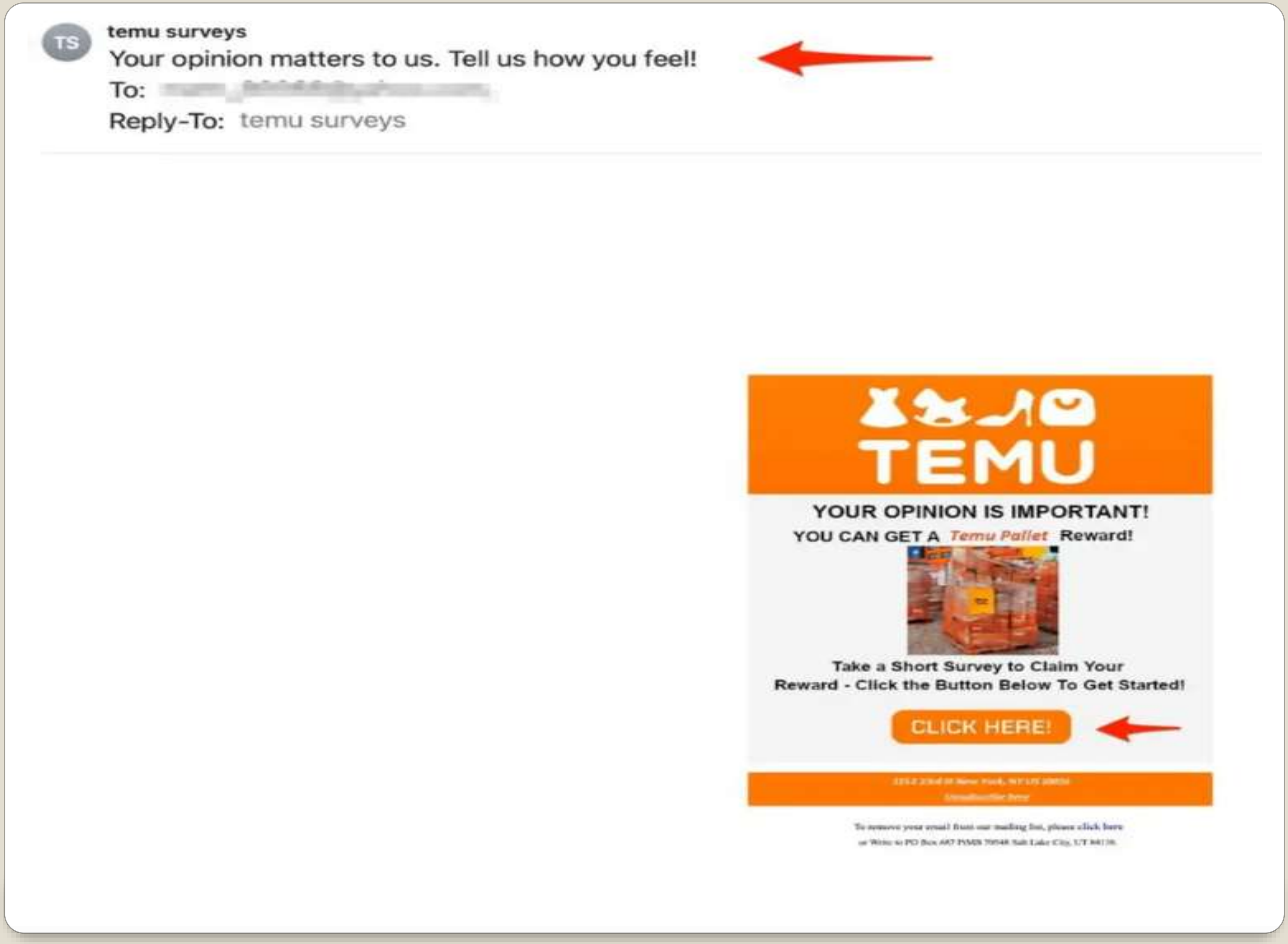
1:28 PM

This message is from a trusted sender.

If you cannot see the images below, Click Show images .

Your package is scheduled for delivery

Please Confirm Receipt



TS

temu surveys

Your opinion matters to us. Tell us how you feel!

To: [redacted]

Reply-To: temu surveys

YOUR OPINION IS IMPORTANT!

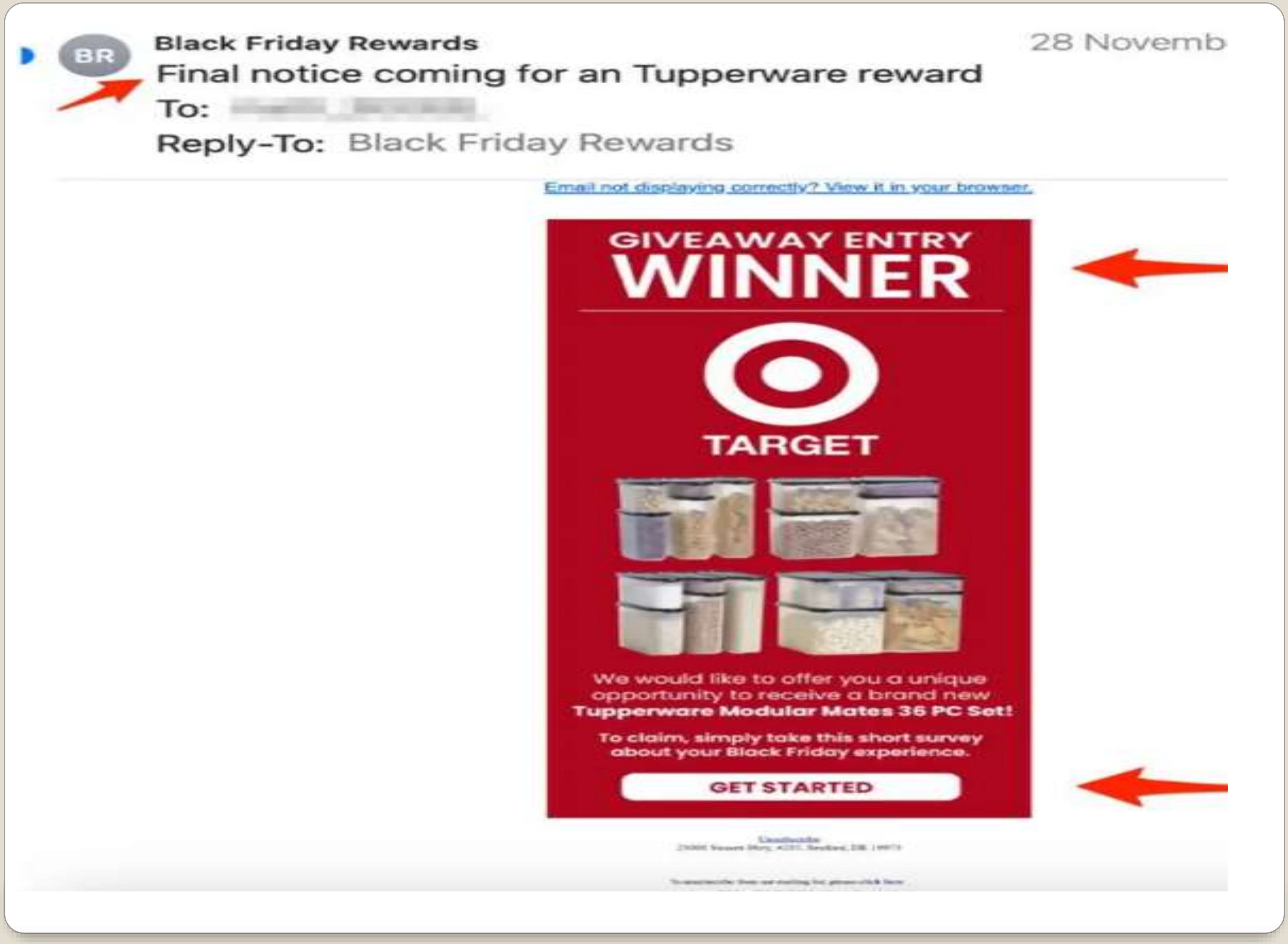
YOU CAN GET A ***Temu Pallet*** **Reward!**

Take a Short Survey to Claim Your Reward - Click the Button Below To Get Started!

[illegible] New York, NY US [illegible]

Unsubscribe here

To remove your email from our mailing list, please click here or Write to PO Box 487 PMB 70548 Salt Lake City, UT 84136.



Black Friday Rewards

28 Novemb

Final notice coming for an Tupperware reward

To: [redacted]

Reply-To: Black Friday Rewards

Email not displaying correctly? View it in your browser.

GIVEAWAY ENTRY

WINNER

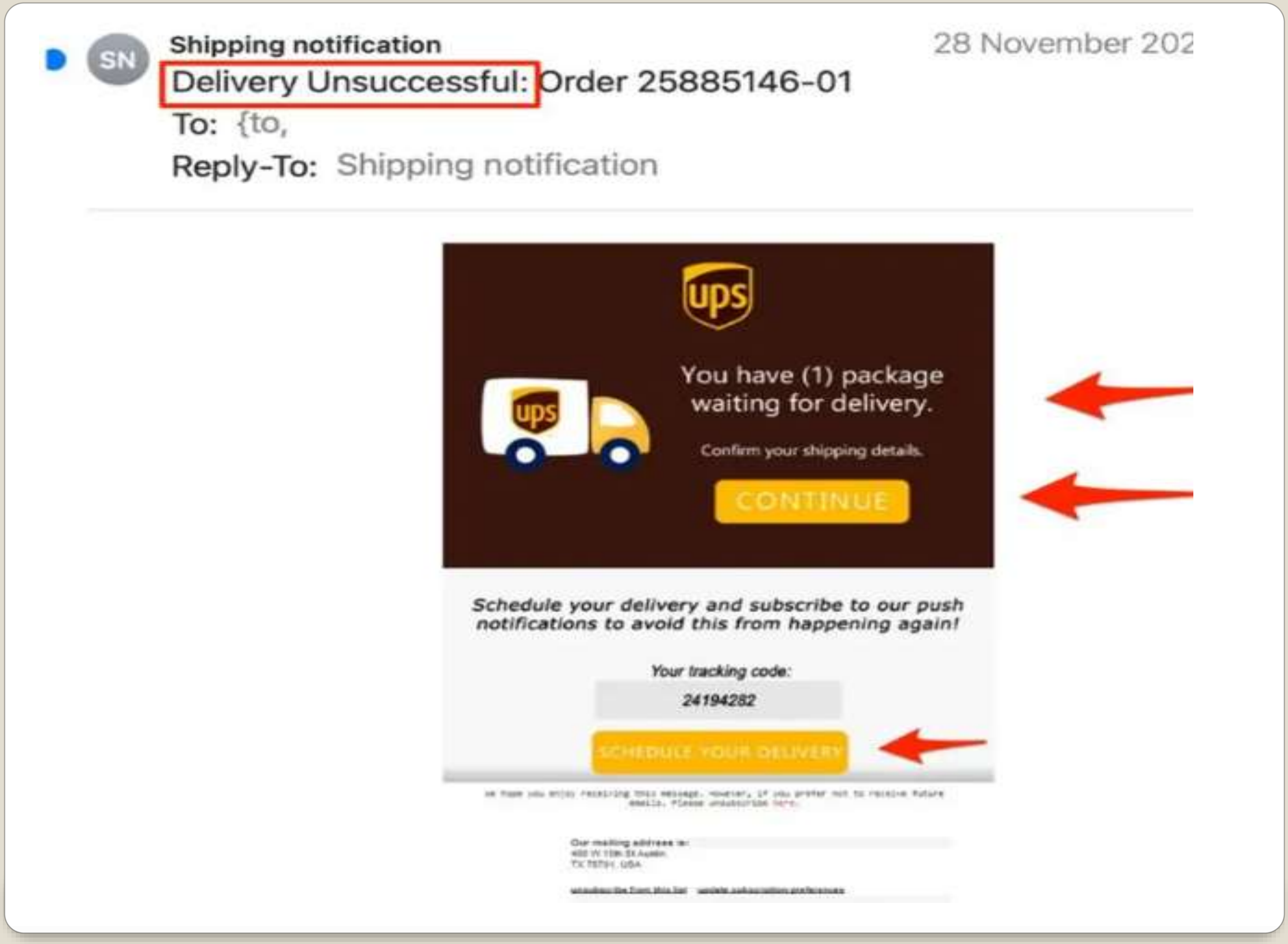
TARGET

We would like to offer you a unique opportunity to receive a brand new **Tupperware Modular Mates 36 PC Set!**

To claim, simply take this short survey about your Black Friday experience.

Unsubscribe
[illegible]

To unsubscribe from our mailing list please click here



Shipping notification

28 November 202

Delivery Unsuccessful: Order 25885146-01

To: {to,

Reply-To: Shipping notification

You have (1) package waiting for delivery.

Confirm your shipping details.

Schedule your delivery and subscribe to our push notifications to avoid this from happening again!

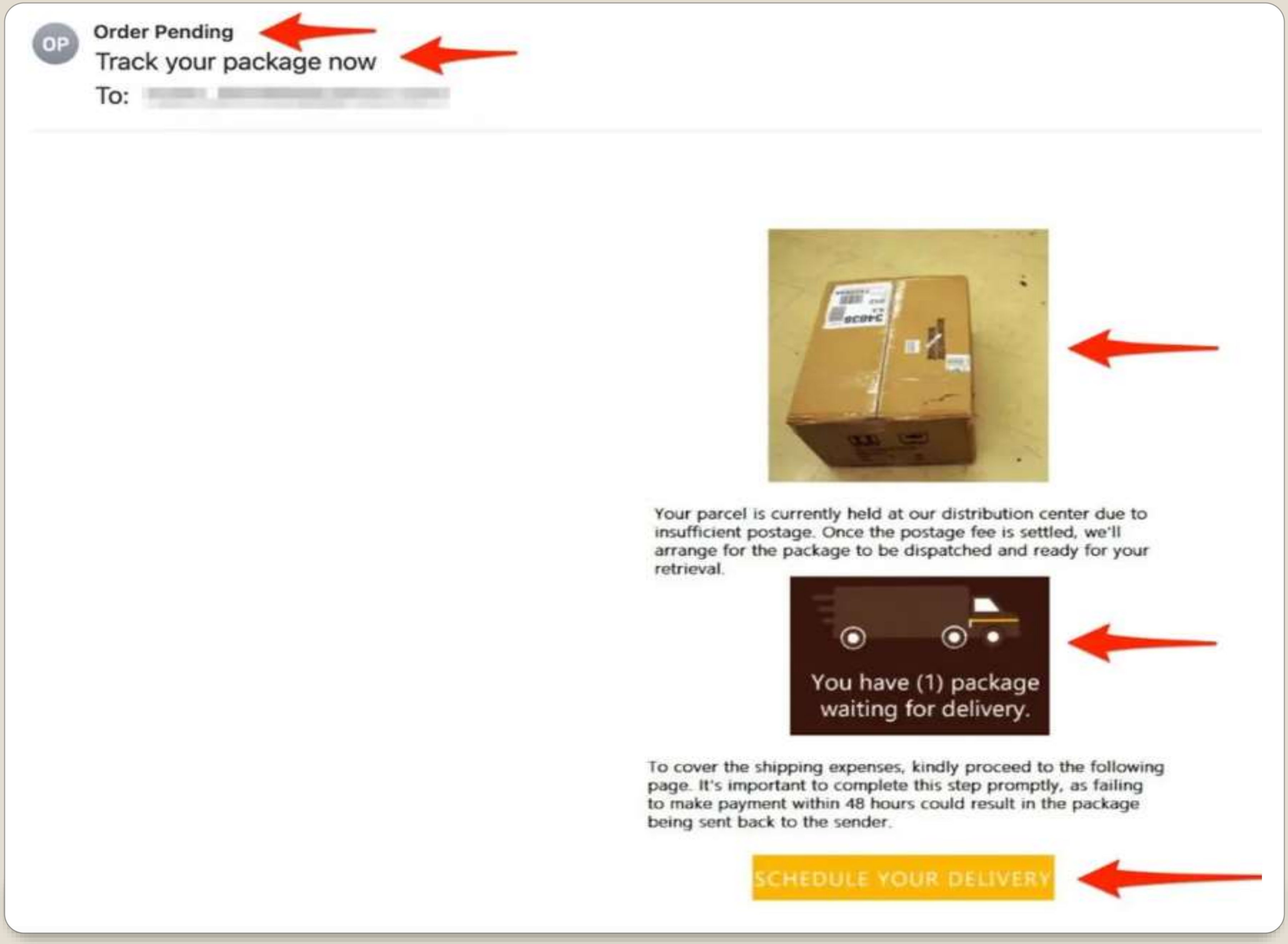
Your tracking code:

24194282

We hope you enjoy receiving this message. However, if you prefer not to receive future emails, Please unsubscribe here.

Our mailing address is:
400 W 15th St Austin
TX 78701, USA

unsubscribe from this list update subscription preferences



OP

Order Pending

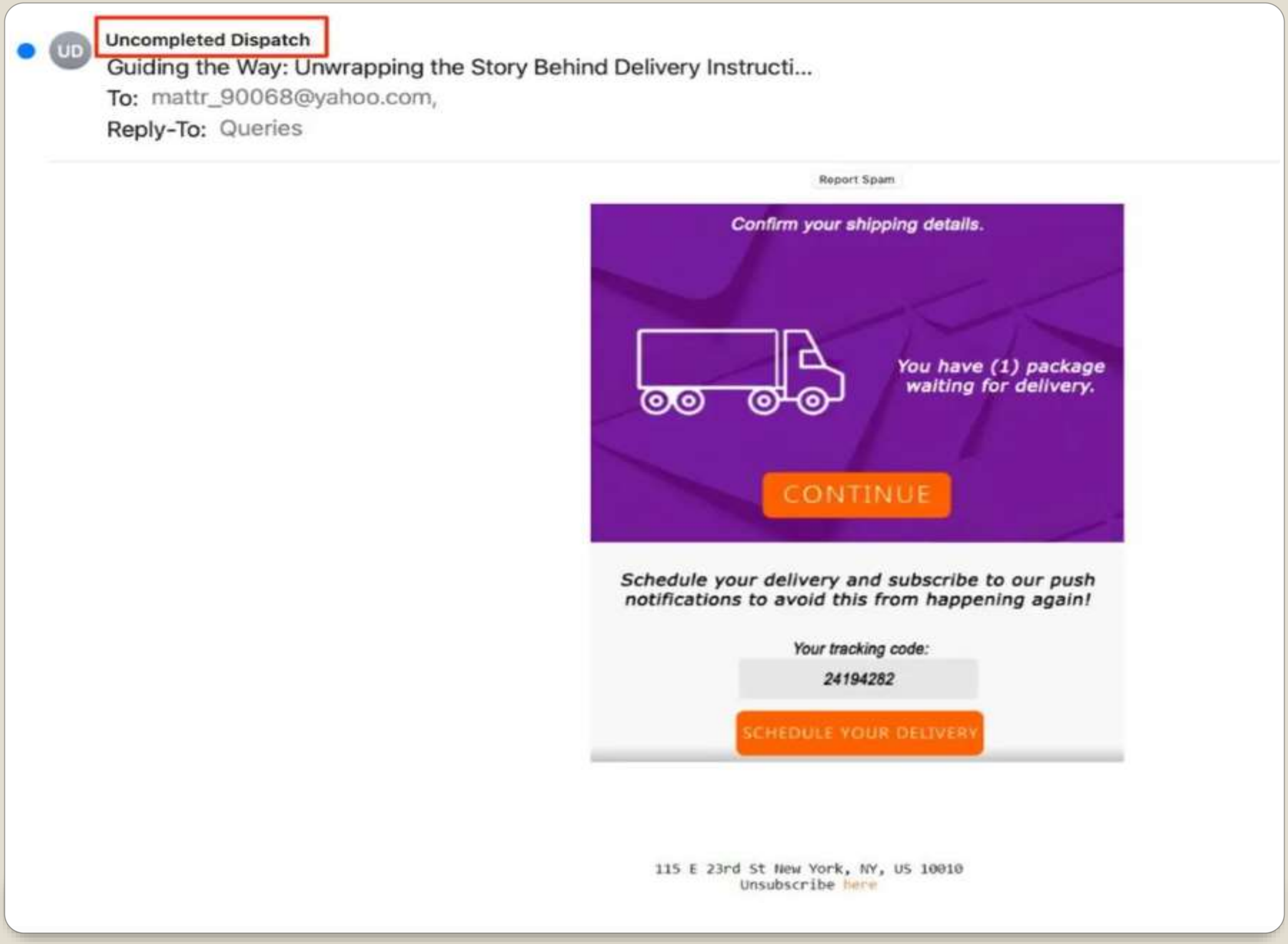
Track your package now

To: [redacted]

Your parcel is currently held at our distribution center due to insufficient postage. Once the postage fee is settled, we'll arrange for the package to be dispatched and ready for your retrieval.

You have (1) package waiting for delivery.

To cover the shipping expenses, kindly proceed to the following page. It's important to complete this step promptly, as failing to make payment within 48 hours could result in the package being sent back to the sender.



Uncompleted Dispatch

Guiding the Way: Unwrapping the Story Behind Delivery Instructi...

To: mattr_90068@yahoo.com,

Reply-To: Queries

Confirm your shipping details.

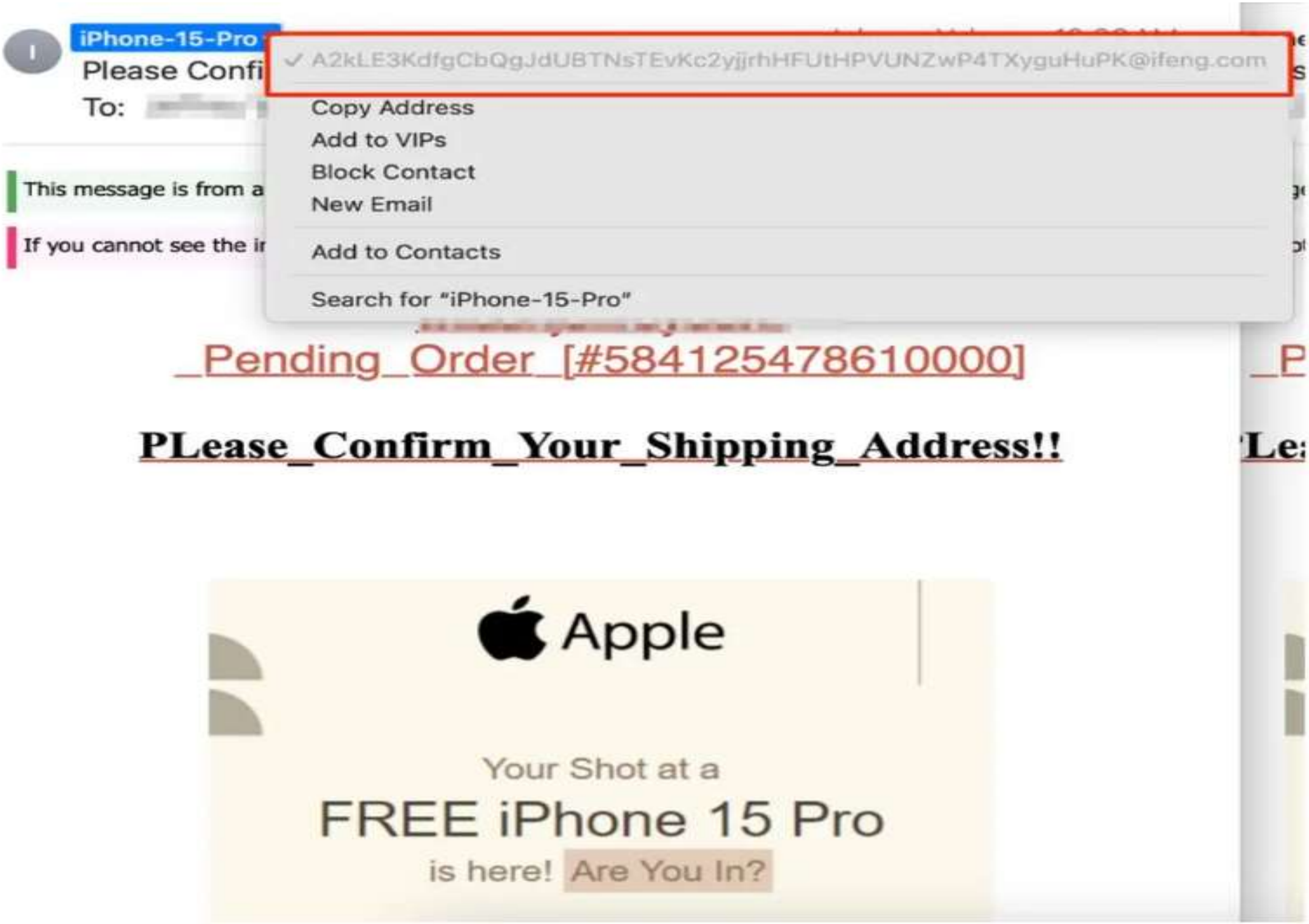
You have (1) package waiting for delivery.

Schedule your delivery and subscribe to our push notifications to avoid this from happening again!

Your tracking code:

24194282

115 E 23rd St New York, NY, US 10010
Unsubscribe here



iPhone-15-Pro

Please Confi

To: [redacted]

This message is from a

If you cannot see the i

✓ A2kLE3KdfgCbQgJdUBTNsTEvKc2yjjrhHFUtHPVUNZwP4TXyguHuPK@ifeng.com

[redacted]

_Pending_Order_[#584125478610000]

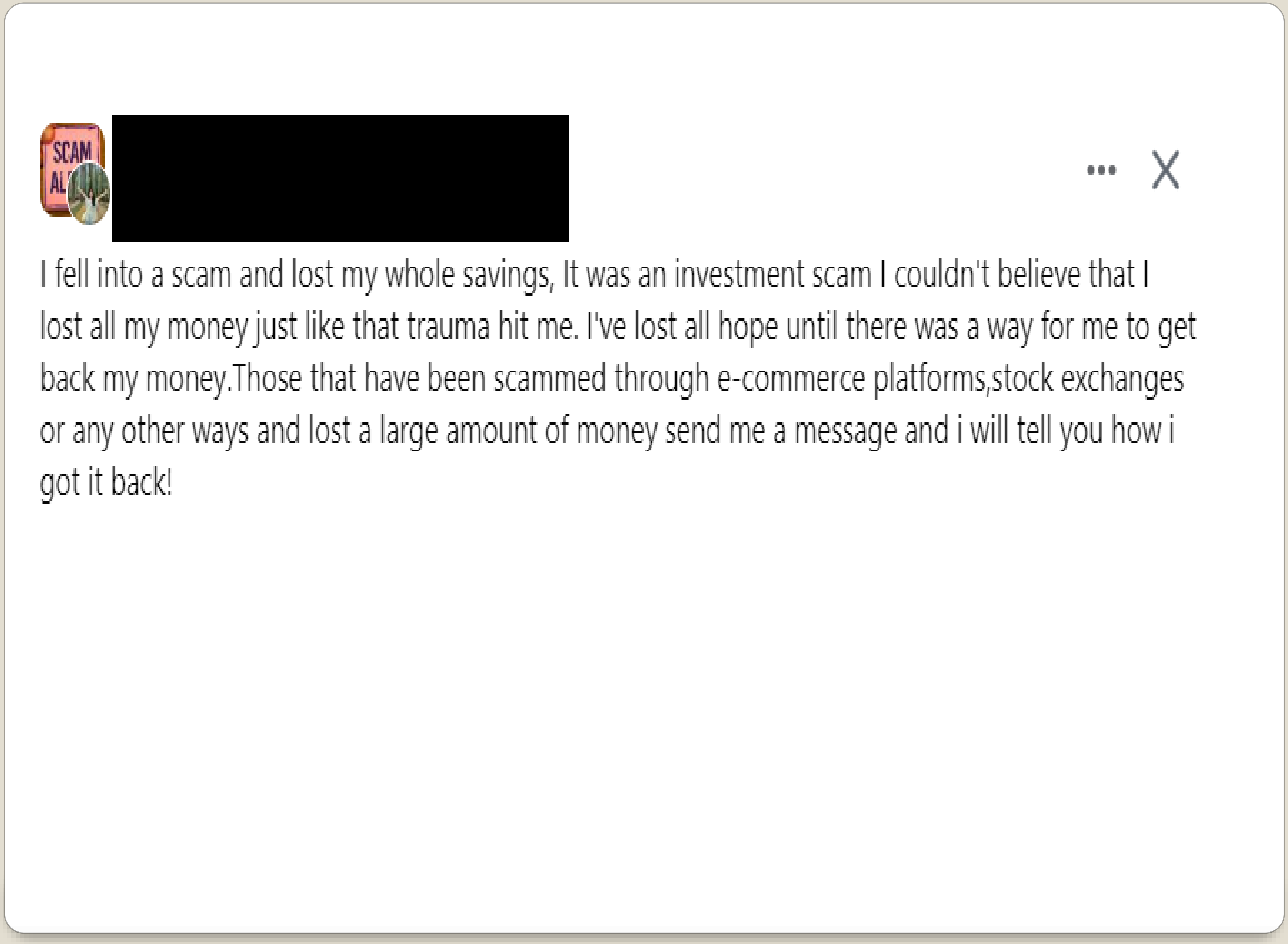
PLease_Confirm_Your_Shipping_Address!!

Apple

Your Shot at a

FREE iPhone 15 Pro

is here! Are You In?



[redacted]

I fell into a scam and lost my whole savings, It was an investment scam I couldn't believe that I lost all my money just like that trauma hit me. I've lost all hope until there was a way for me to get back my money.Those that have been scammed through e-commerce platforms,stock exchanges or any other ways and lost a large amount of money send me a message and i will tell you how i got it back!

- 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