Sun City Computer Club

Cyber Security SIG
March 21, 2024

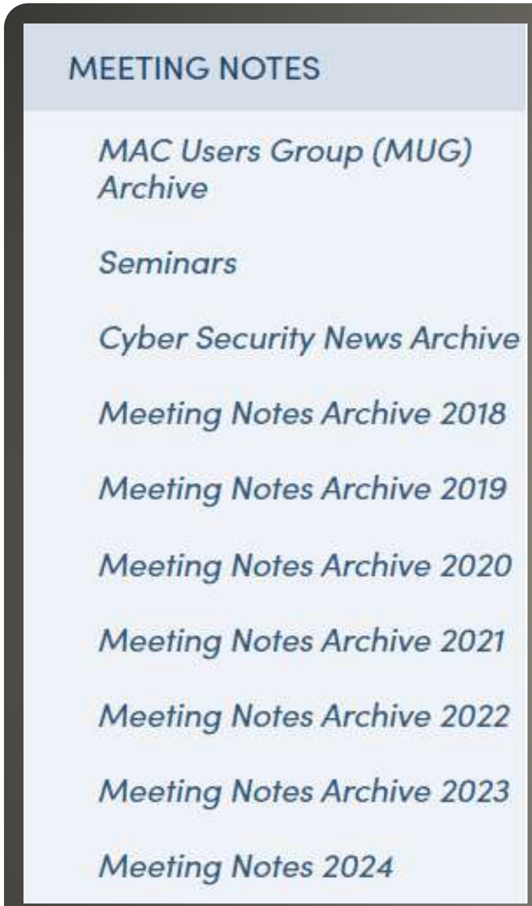
Questions, Comments, Suggestions welcomed at any time

Even Now

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

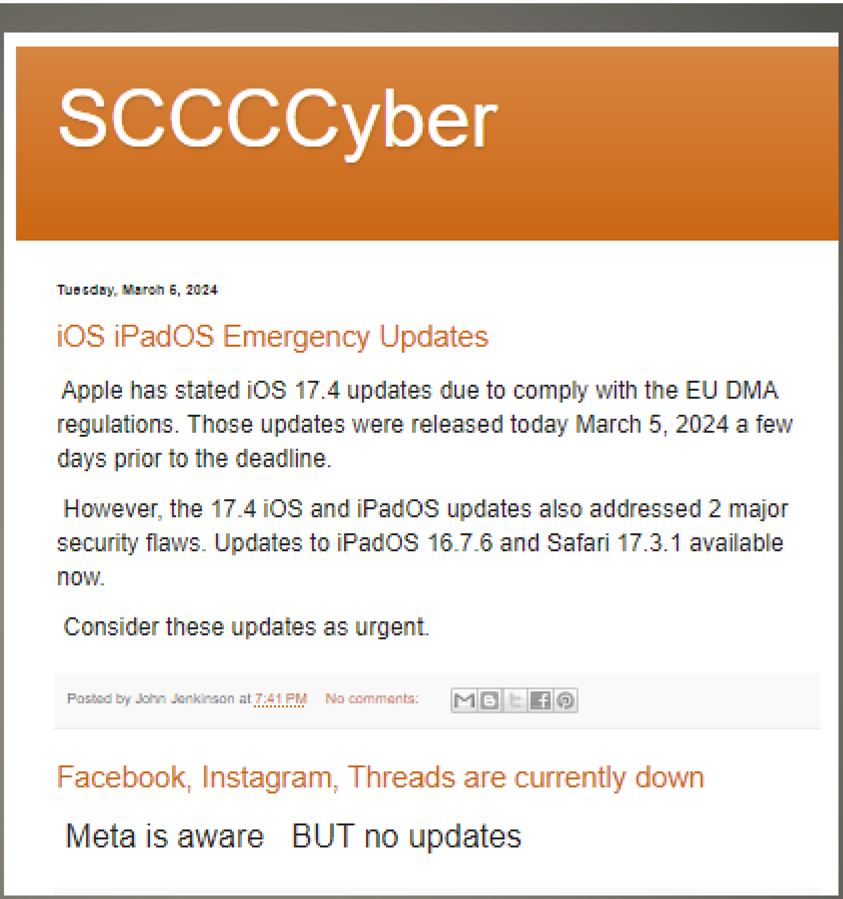
Audio Recording In Progress

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



MEETING NOTES

- MAC Users Group (MUG) Archive
- Seminars
- Cyber Security News Archive
- Meeting Notes Archive 2018
- Meeting Notes Archive 2019
- Meeting Notes Archive 2020
- Meeting Notes Archive 2021
- Meeting Notes Archive 2022
- Meeting Notes Archive 2023
- Meeting Notes 2024



SCCCCyber

Tuesday, March 5, 2024

iOS iPadOS Emergency Updates

Apple has stated iOS 17.4 updates due to comply with the EU DMA regulations. Those updates were released today March 5, 2024 a few days prior to the deadline.

However, the 17.4 iOS and iPadOS updates also addressed 2 major security flaws. Updates to iPadOS 16.7.6 and Safari 17.3.1 available now.

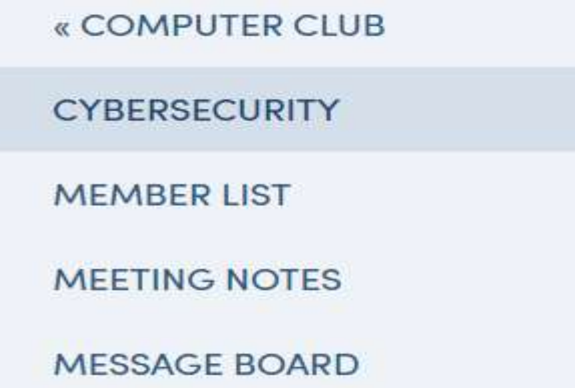
Consider these updates as urgent.

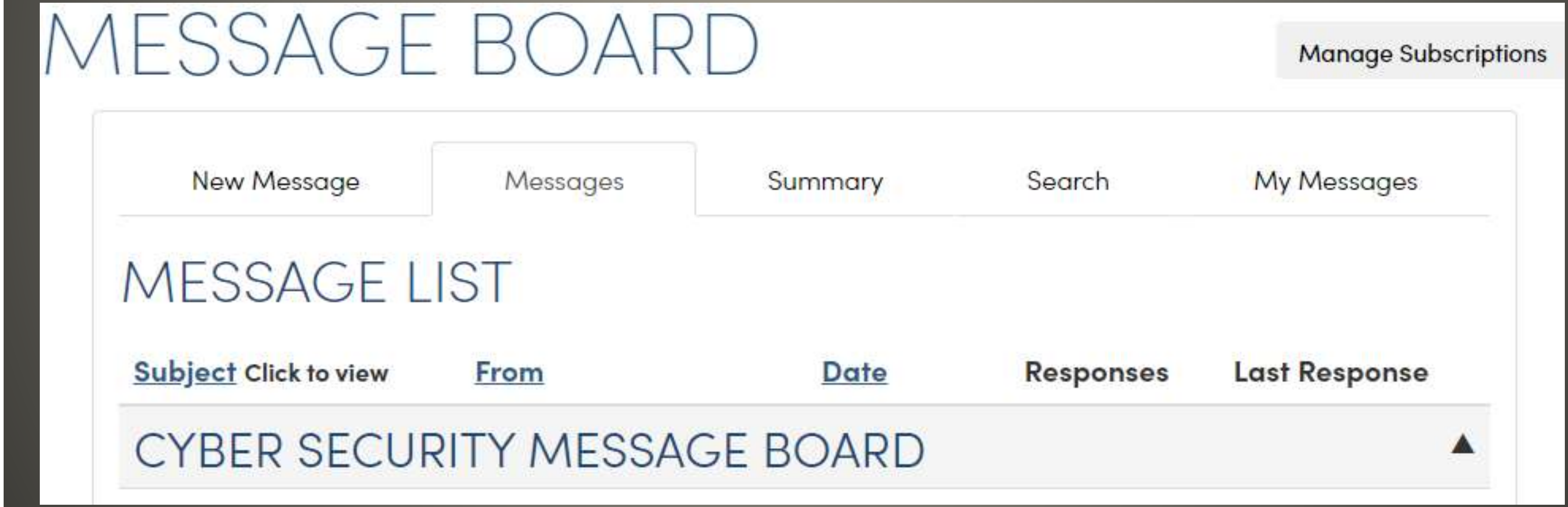
Posted by John Jenkinson at 7:41 PM No comments:

Facebook, Instagram, Threads are currently down

Meta is aware BUT no updates

Cyber Security SIG News





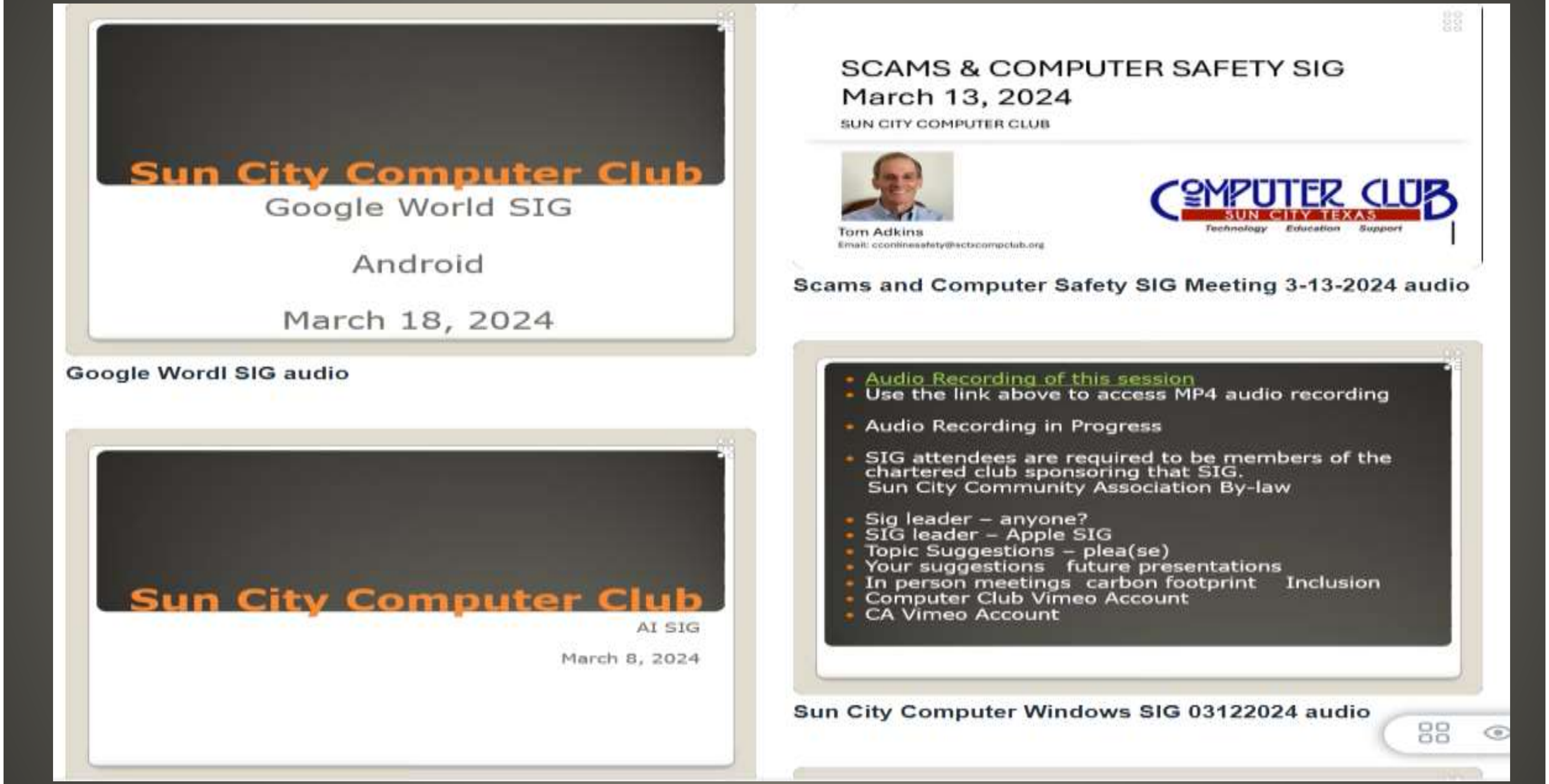
MESSAGE BOARD

MESSAGE LIST

Subject Click to view	From	Date	Responses	Last Response
CYBER SECURITY MESSAGE BOARD ▲				

Cyber Secuity SIG News

- https://vimeo.com/sctxcompclub



Sun City Computer Club
Google World SIG

Android

March 18, 2024

Google Wordl SIG audio

SCAMS & COMPUTER SAFETY SIG
March 13, 2024
SUN CITY COMPUTER CLUB

Tom Adkins
Email: cconlinesafety@sctxcompclub.org

Scams and Computer Safety SIG Meeting 3-13-2024 audio

Sun City Computer Club
AI SIG
March 8, 2024

- Audio Recording of this session
- Use the link above to access MP4 audio recording
- Audio Recording in Progress
- SIG attendees are required to be members of the chartered club sponsoring that SIG.
  Sun City Community Association By-law
- Sig leader – anyone?
- SIG leader – Apple SIG
- Topic Suggestions – plea(se)
- Your suggestions future presentations
- In person meetings carbon footprint Inclusion
- Computer Club Vimeo Account
- CA Vimeo Account

Sun City Computer Windows SIG 03122024 audio

Other SIG News

Microsoft Password Spraying

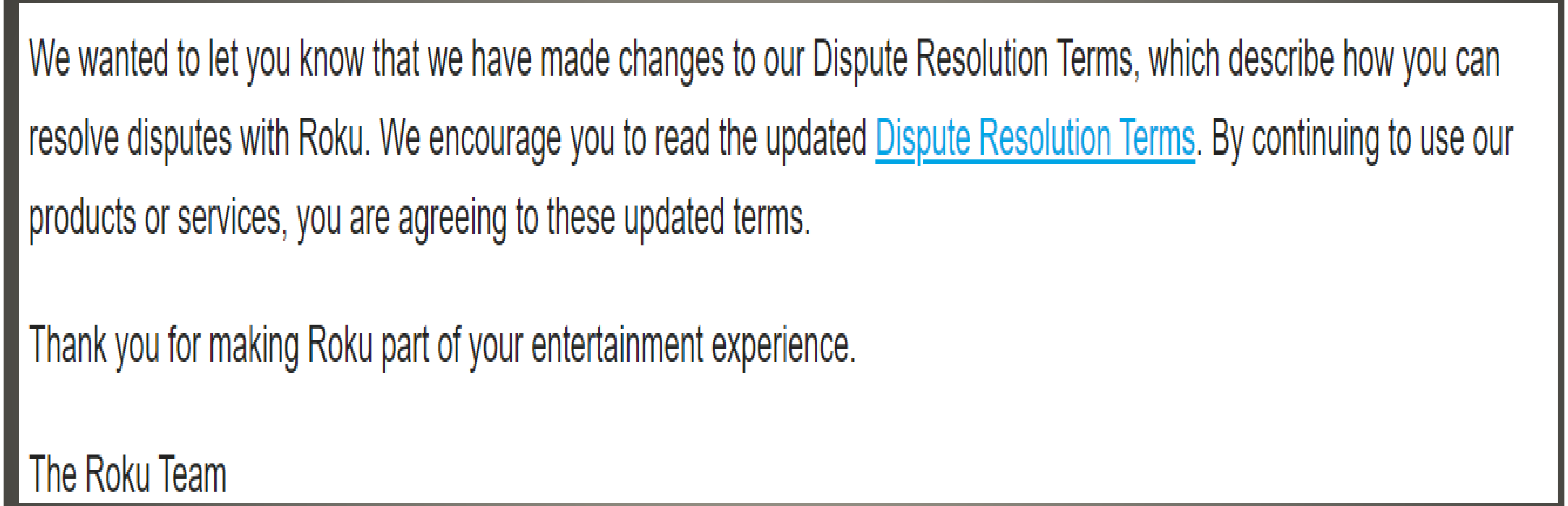
- Kremlin ?? January
- Microsoft

  emails to-from customers

  Source code
- Password Spraying
- Not Brute Force
- 1 account Many passwords
- 1 password   Many accounts
- Bypasses a lot of protections

- Chinese targeted misinformation attacks
  Local focus
  Slow down US development efforts
  Very targeted
- Roku Terms of Service
  Agree or Opt-out via mailed letter
- CISA hacked
  Cybersecurity & Infrastructure Security Agency
  "Protect against Ivanti vulnerabilities"
- French government departments
  Conventional attacks, intensity unprecedented
- 15,000 Roku users records for sale $0.50/each
  Credential stuffing
  Roku Disable ACR
  Settings > Privacy > Smart TV Experience > Use info from TV inputs OFF
  Settings > Privacy > Personalized Ads > Don't personalize my ads
- Tuta mail new quantum-resistant encryption TutaCrypt
- Truth Social outage

Current Issues



We wanted to let you know that we have made changes to our Dispute Resolution Terms, which describe how you can resolve disputes with Roku. We encourage you to read the updated Dispute Resolution Terms. By continuing to use our products or services, you are agreeing to these updated terms.

Thank you for making Roku part of your entertainment experience.

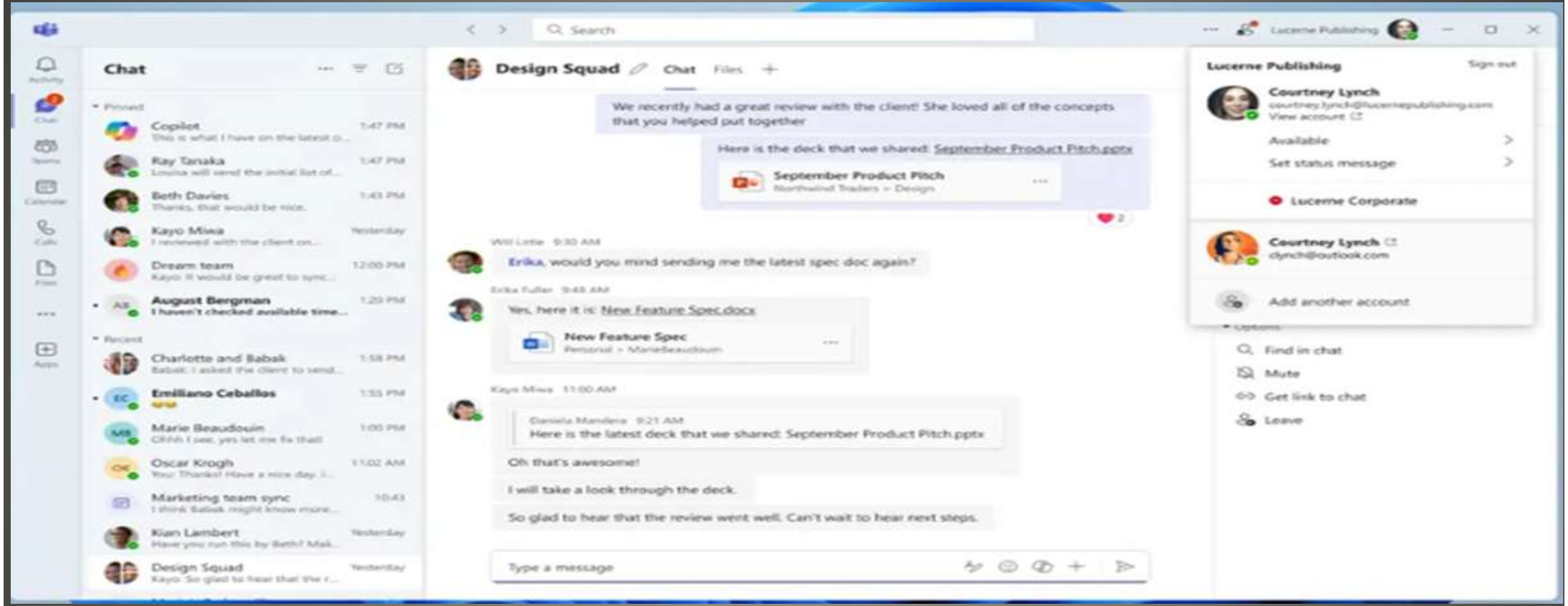
The Roku Team

Roku Notification

- Simultaneous and heterogeneous multithreading (SHMT)
- OS/2
- Some Alabama state government offices DoS attack
- WhatsApp blocks screenshots of contact profile pictures
  Screenshot of mini-profile or profile preview still allowed
- Telecom exec unauthorized SIM swaps
  $1,000/each
- Unsafe safes
  S&G SECURAM backdoor access
  US DoD ban use of those safes
  Don’t ask, Don’t tell
- Glassdoor – attaching real names to reviews
  After Glassdoor support requests

Current Issues

- Microsoft Teams > Single app Personal & Work



Copilot 1:47 PM
This is what I have on the latest o...

Ray Tanaka 1:47 PM
Louisa will send the initial list of...

Beth Davies 1:43 PM
Thanks, that would be nice.

Kayo Miwa Yesterday
I reviewed with the client on...

Dream team 12:00 PM
Kayo: It would be great to sync...

August Bergman 1:20 PM
I haven't checked available time...

Charlotte and Babak 1:58 PM
Babak: I asked the client to send...

Emiliano Ceballos 1:55 PM

Marie Beaudouin 1:00 PM
Ohhh I see, yes let me fix that!

Oscar Krogh 11:02 AM
You: Thanks! Have a nice day, I...

Marketing team sync 10:43
I think Babak might know more...

Kian Lambert Yesterday
Have you run this by Beth? Mak...

Design Squad Yesterday
Kayo: So glad to hear that the r...

We recently had a great review with the client! She loved all of the concepts that you helped put together

Here is the deck that we shared: September Product Pitch.pptx

September Product Pitch
Northwind Traders > Design

Will Little 9:30 AM
Erika, would you mind sending me the latest spec doc again?

Erika Fuller 9:48 AM
Yes, here it is: New Feature Spec.docx

New Feature Spec
Personal > MarieBeaudouin

Kayo Miwa 11:00 AM
Daniela Mandera 9:21 AM
Here is the latest deck that we shared: September Product Pitch.pptx

Oh that's awesome!

I will take a look through the deck.

So glad to hear that the review went well. Can't wait to hear next steps.

Courtney Lynch
courtney.lynch@lucernepublishing.com

Courtney Lynch
clynch@outlook.com

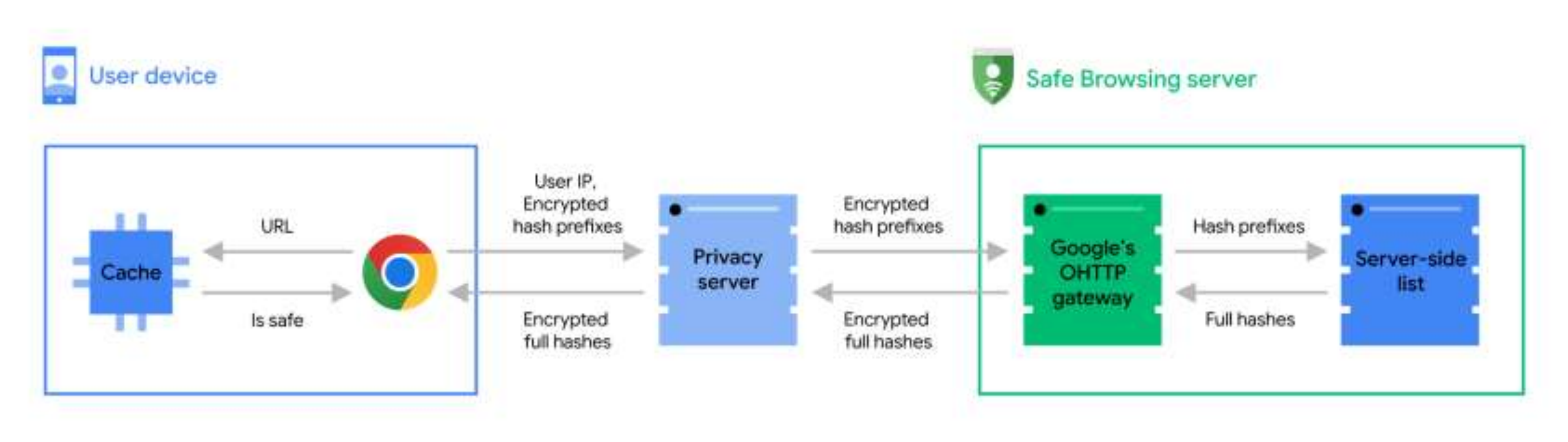
- Google Chrome Safe Browsing change

Was browser problem URL list updated 1-2 times per hour

Now server-side list - malicious sites last 10 minutes

Desktop & iOS now Android soon

Enhanced mode Opt-in



Google Chrome Safe Browsing

- When you visit a site, Chrome first checks its cache to see if the address (URL) of the site is already known to be safe (see the “Staying speedy and reliable” section for details).
- If the visited URL is not in the cache, it may be unsafe, so a real-time check is necessary.
- Chrome obfuscates the URL by following the URL hashing guidance to convert the URL into 32-byte full hashes.
- Chrome truncates the full hashes into 4-byte long hash prefixes.
- Chrome encrypts the hash prefixes and sends them to a privacy server.
- The privacy server removes potential user identifiers and forwards the encrypted hash prefixes to the Safe Browsing server via a TLS connection that mixes requests with many other Chrome users.
- The Safe Browsing server decrypts the hash prefixes and matches them against the server-side database, returning full hashes of all unsafe URLs that match one of the hash prefixes sent by Chrome.
- After receiving the unsafe full hashes, Chrome checks them against the full hashes of the visited URL.
- If any match is found, Chrome will show a warning.

Google Chrome Safe Browsing

- Maybe the most interesting part here is the privacy server. Google actually partnered with CDN and edge computing specialist Fastly to use Fastly’s Oblivious HTTP privacy server. This server sits between Chrome and Safe Browsing and strips out any identifying information from the browser request.

- Fastly built this system as a privacy service that can sit between users and a web application and anonymize their metadata while still being able to exchange data with a web application, for example. These servers, Google stresses, are operated independently by Fastly (a cynic may look at this whole scheme and say that even Google doesn’t trust itself to not snoop on your browsing data…).

- Thanks to all of this, Google’s Safe Browsing service should never see your IP address. Meanwhile, Fastly won’t see these URLs either, because they are encrypted by the browser, using a public-private key that Fastly has no access to.

Google Chrome Safe Browsing

OnStar Smart Driver

- Optional service
- Gaming – badges – speed limits, gentle braking
- Insurance rates – up
- GM sharing select insights with LexisNexis

  Other automakers, insurance co, data brokers

  Privacy policies

  No national legislation except TikTok

- EquiLend breach

  No worries – Now worries
- UK fighting attacks on fiber infrastructure

  Chop cables, fire
- Last time Red Sea cables 4 of 15

  West African coast Deep
- Onerep remove your personal info from 200 sites

  Onerep CEO created many PII search sites
- States attempts to limit voter's data from doxxing

  1993 law requiring public disclosure

  Postcard during past elections
- LockBit convection October 2022 raid
- Incognito Market

  Dark web narcotics site - extorting vendors & users

  Publishing transactions - with holding funds
- Unclassified US spy chiefs testify to congress

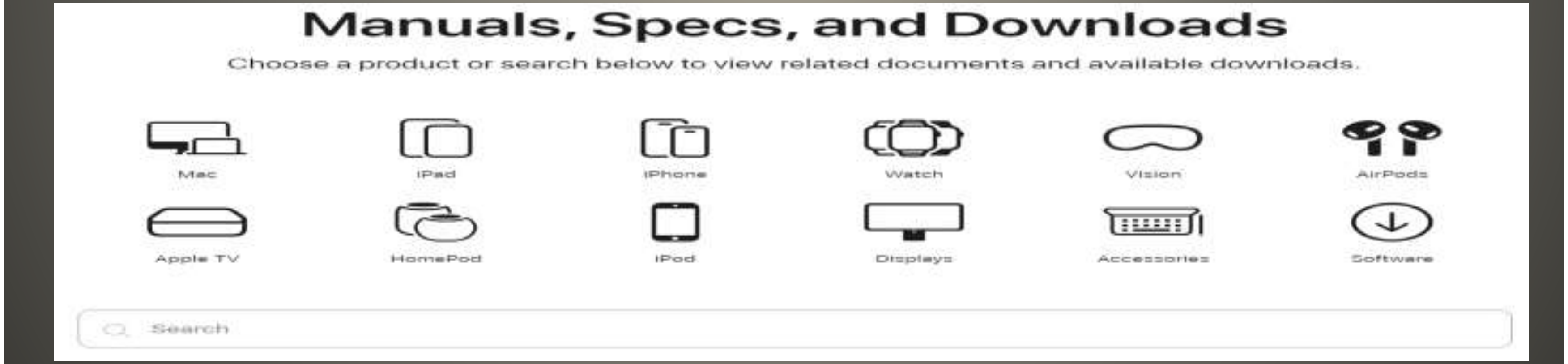
  spyware, ransomware defense, purchase of bilk commercial data
- IMF email hacked

Current Issues

Current Issues

- Nasdaq-listed pharmaceutical company
  Crinetics Pharmaceuticals
  “we discovered and fixed this incident”
  LockBit “not so fast”
  LockBit recent news
- Apple launches All-in-One
  Manuals, Specs, and Downloads website

https://support.apple.com/en-us/docs



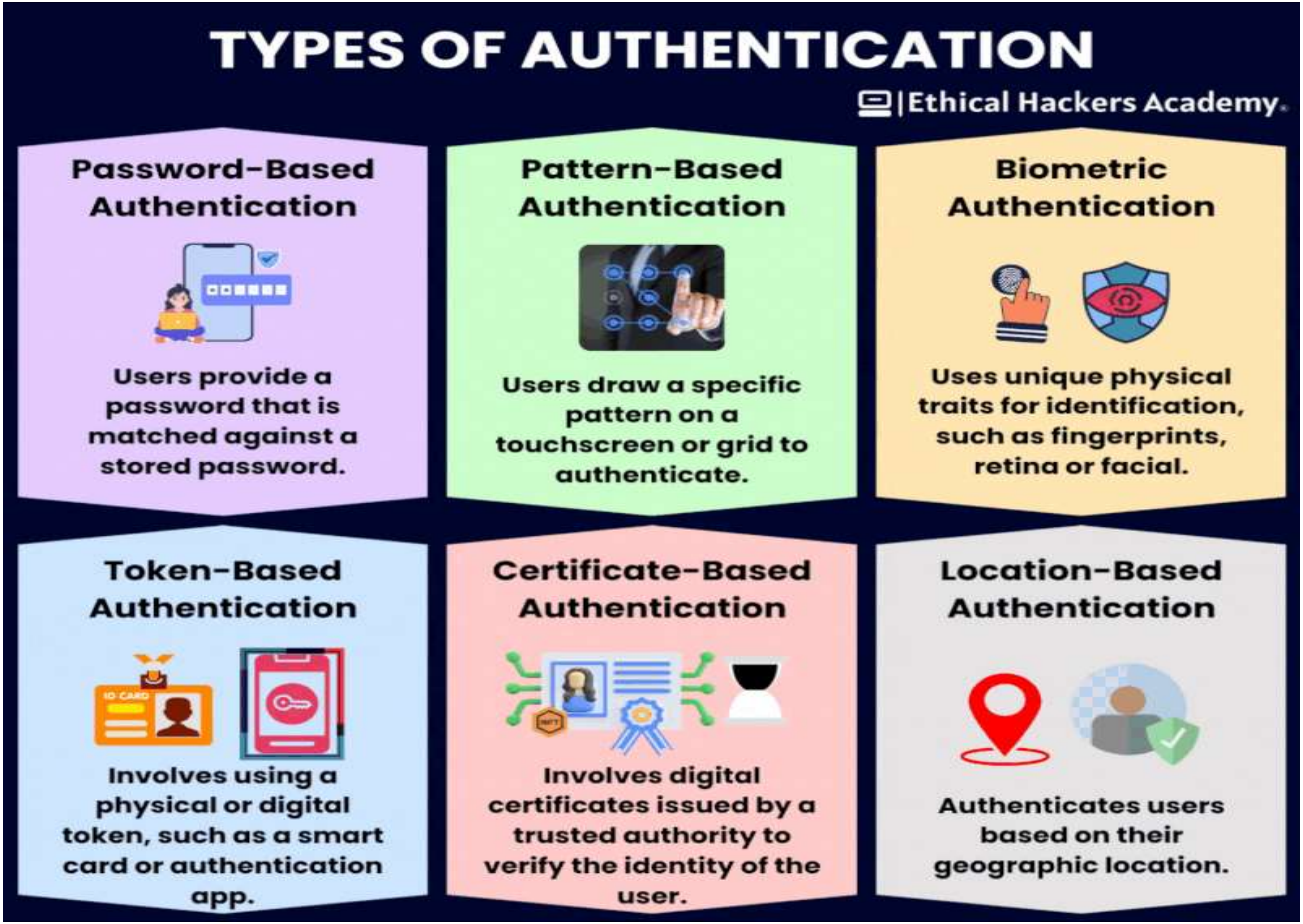
Manuals, Specs, and Downloads

Choose a product or search below to view related documents and available downloads.

- December 2023
- Nissan Motor Corporation
- Nissan Financial Services Australia & New Zealand
- Reported by Akira ransomware group
- Breach extended to customers & employees

  Mitsubishi, Renault, Skyline, Infinity, LDV, Ram
- 10% victims had crucial government identification documents stolen
- 4,000 Medicare documents
- 7500 Driver’s Licenses
- 220 passports
- 1,300 tax file numbers
- Loan transactions
- Employment records

Nissan Data Breach



TYPES OF AUTHENTICATION

|Ethical Hackers Academy.

Password-Based Authentication

Users provide a password that is matched against a stored password.

Pattern-Based Authentication

Users draw a specific pattern on a touchscreen or grid to authenticate.

Biometric Authentication

Uses unique physical traits for identification, such as fingerprints, retina or facial.

Token-Based Authentication

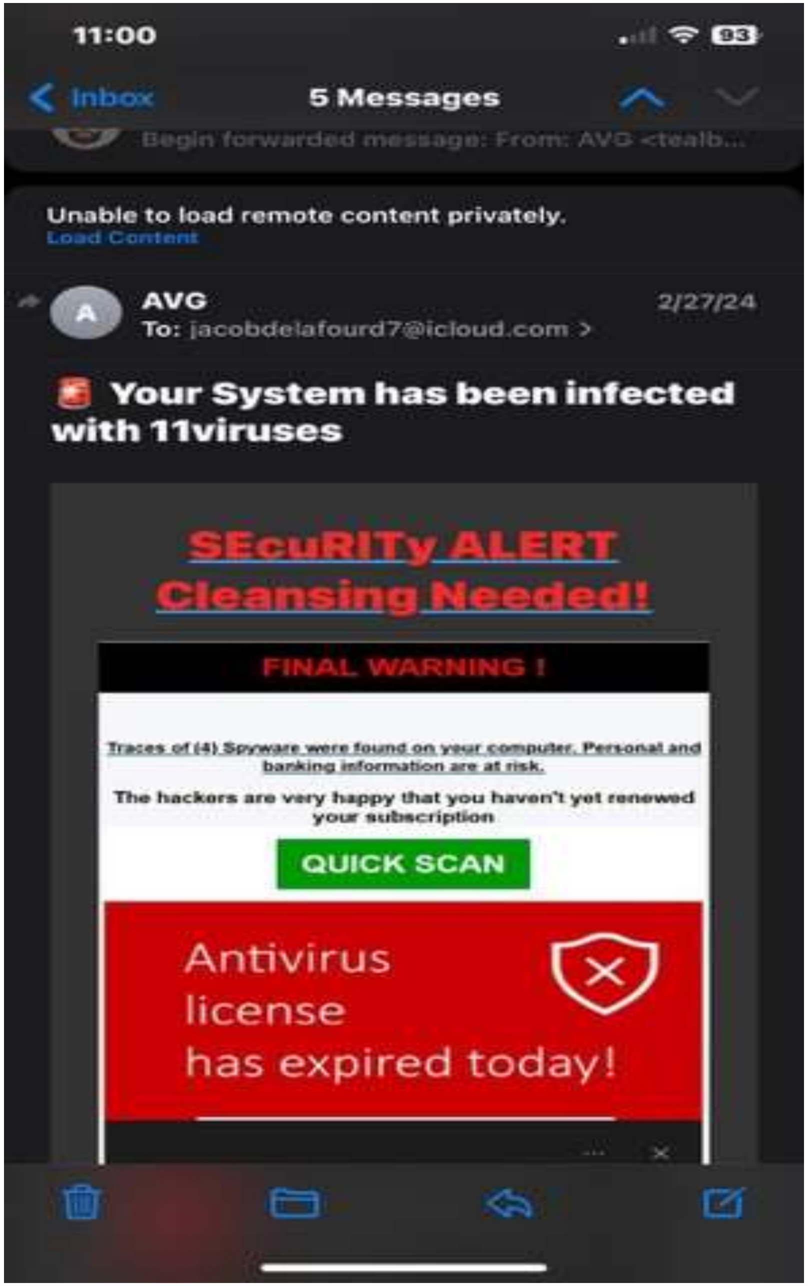
Involves using a physical or digital token, such as a smart card or authentication app.

Certificate-Based Authentication

Involves digital certificates issued by a trusted authority to verify the identity of the user.

Location-Based Authentication

Authenticates users based on their geographic location.



Begin forwarded message: From: AVG <tealb...

Unable to load remote content privately.
Load Content

AVG 2/27/24
To: jacobdelafourd7@icloud.com >

🚨 Your System has been infected with 11viruses

SEcuRITy ALERT
Cleansing Needed!

FINAL WARNING !

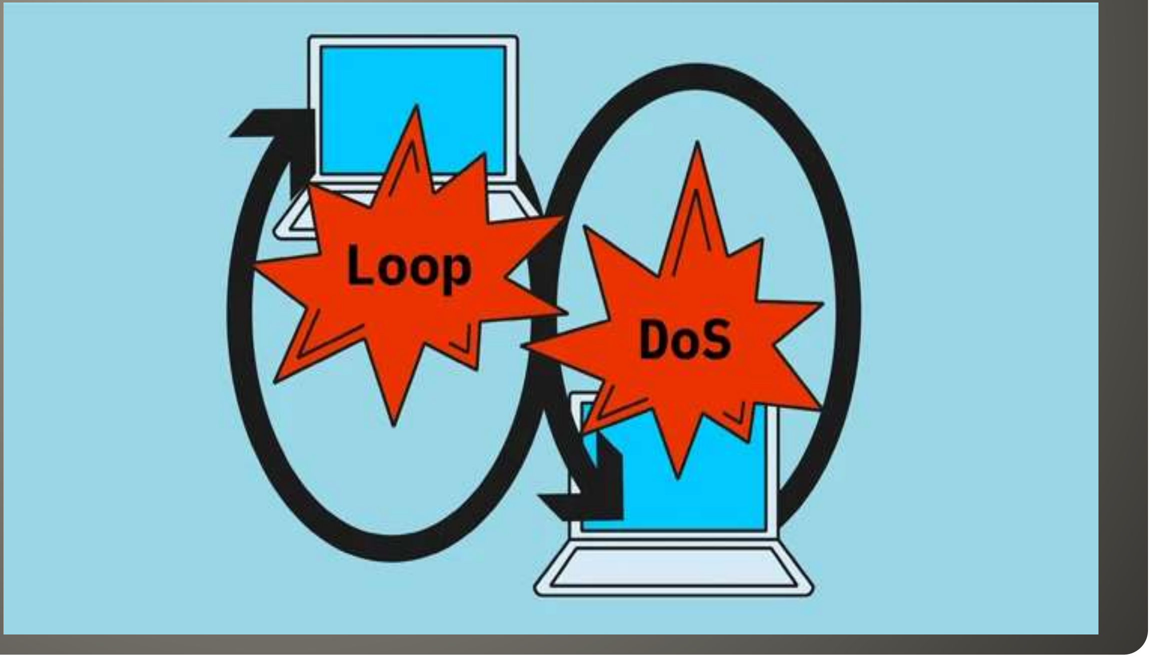
Traces of (4) Spyware were found on your computer. Personal and banking information are at risk.

The hackers are very happy that you haven't yet renewed your subscription

QUICK SCAN

Antivirus
license
has expired today!

- Spoofed UDP vulnerability
- Attacker “spoofs” UDP traffic to victim A
- From victim B
- Traffic has error(s)
- Victim A responds to spoofed victim B “error”
- Victim A and Victim B respond to each other’s errors forever



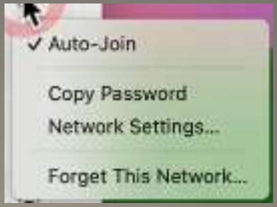
Loop DoS

Secure a Mac

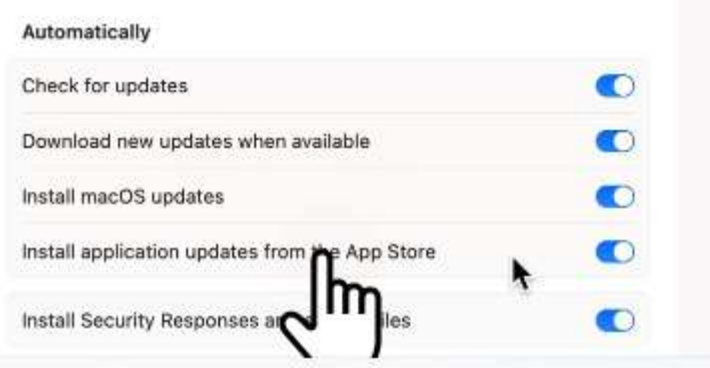
- System Preferences -> System Settings
- Mac account passwords Strong & UNIQUE
  No Hint Passphrase
  AppleID Recovery Code 2FA
- Lock Screen
  Require password after screen saver or display is turned off
  Show message when locked - Return lost Mac
- Privacy & Security
  - Allow applications downloaded from
    - App Store
    - App Store and Identified Developers
      - Apple Certificate

  FileVault Prevents data access w/o logon
- General > Sharing > File Sharing
  - Other sharing methods
  - Out & About See your Mac

- Siri & Spotlight
  Siri Allow when locked
- Network > Wi-Fi
  Known Networks
  Other Networks



- Safari > General
  Open “safe” files after downloading
  Safari > Websites > Notifications
  Allow Deny
- General > Software Updates
- Time Machine drive encryption
- Firmware password
- FindMy



Automatically

Check for updates ●
Download new updates when available ●
Install macOS updates ●
Install application updates from the App Store ●
Install Security Responses a les ●

Secure a Mac

- Malawi Passport System – ransomware
- Scotland & Ireland National Health Service breach
- Change Healthcare United Healthcare
- McDonalds global IT outage

"Notably, this issue was not directly caused by a cybersecurity event; rather, it was caused by a third-party provider during a configuration change."

Third-party – single point of failure
Third-party – increase attack surface
Third-party – limit access to required data

- Fujitsu data breach
- Reverse reporting?

  Report the few that have yet to realize incidents
- Walmart now owns Vizio and its data

  Automatic Content Recognition (ACR)
  Microphones and/or Cameras Video conference / Facetime
  Cut cord
  Forget Wi-Fi
- Apple AirTags firmware 2.0.73   from 2.0.61 (October)
- Gmail mass mailer rules 1-Apr-2024

Current Issues

- Surface Pro 10
- Surface Laptop 6
- For business
- $2799 -> $1199
- Copilot any/everywhere

Microsoft AI PCs

Smuggling

- Email smuggling March 7 presentation
- HTML smuggling
- Payload embedded in external JSON file
- Data harvesting
- Google Docs   PDF bank/financial statement
- CAPTCHA barrier – prevent URL scan, email security
- Government impersonation

- Minneapolis Public Schools
  Ransomware – Did not pay – Data released
  SSN, school security details, sexual assault info, psychiatric holds
  108 K-12 school systems *reported* attacks
  Data of K-12 more valuable
  Child allergies, suspensions, Household income
  Not deleted
  Lifelong
  Not just ransomware incidents – Data is more valued
  Information gives no indication of being stolen
  Info stealers more value than the ransom so no ransomware
  No reporting No notifications

  Up protections for SSN, birth certificates, etc.
  INFORM YOUR CHILD, GRANDCHILD, FAMILY, FRIENDS

IMPORTANT

- 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