Sun City Computer Club

Cyber Security SIG

October 6, 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???

Other Sun City resources

- Community Association web site
- Login
- Clubs & Groups > NRO/Neighborhood > NRO
- NRO Programs > Anti-Fraud

Sun City Texas Community Association

NRO Anti-Fraud Group

RESIDENT HOME | LIFESTYLE & ACTIVITIES | CLUBS & NEIGHBORHOODS | FITNESS | GOLF | COMMUNICATIONS

My Profile | Account Statements | Resident Directory | My Neighborhood | My Memberships

- « ALL CLUBS
- « NRO
- ANTI-FRAUD
- GROUP MEMBERS
- CALENDAR
- MEETING AGENDAS AND MINUTES
- ALERTS
- REQUEST A FRAUD PRESENTATION
- PRESENTERS

ANTI-FRAUD

A PROGRAM WITH YOU IN MIND!

WHAT TO DO IF SCAMED

LEARN HOW TO REPORT A FRAUD

UPCOMING EVENTS

SEP 21 WED

Presentation for members of MH42 at Cowan Creek in the Salado Room

OCT 4 TUE

Presentation for members of MH3 at Legacy Hills in the Oaks Room

COVID TEST SCAM

MORE ABOUT HOW TO AVOID THIS SCAM!

ALERTS

How do you spot a Scam?	View | Download
Con-Games Fraud Scams	View | Download
CREDIT CARD INTEREST RATE REDUCTION Scam	View | Download
FRAUD ALERTS	View | Download
FRAUD AND OLDER ADULTS	View | Download
GIVING TO CHARITY	View | Download
HOW TO AVOID A SCAM FTC CONSUMER INFORMATION	View | Download
IDENTITY THEFT	View | Download
INTERNET FRAUD FBI	View | Download
TOP FRAUDS OF 2021	View | Download

Self Defense Club Self and Home Security SIG

Past Presentations:

Cybersecurity Risks and Scams

Outdoor Surveillance Cameras

Williamson County Sheriff

CA Community Standards Director

Safety Procedures

Georgetown Police Security

Safety and Protection Devices

Safety on the Sun City Trails

Public Service Announcement

FBI & CISA

October 04, 2022

Alert Number
I-100422b-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

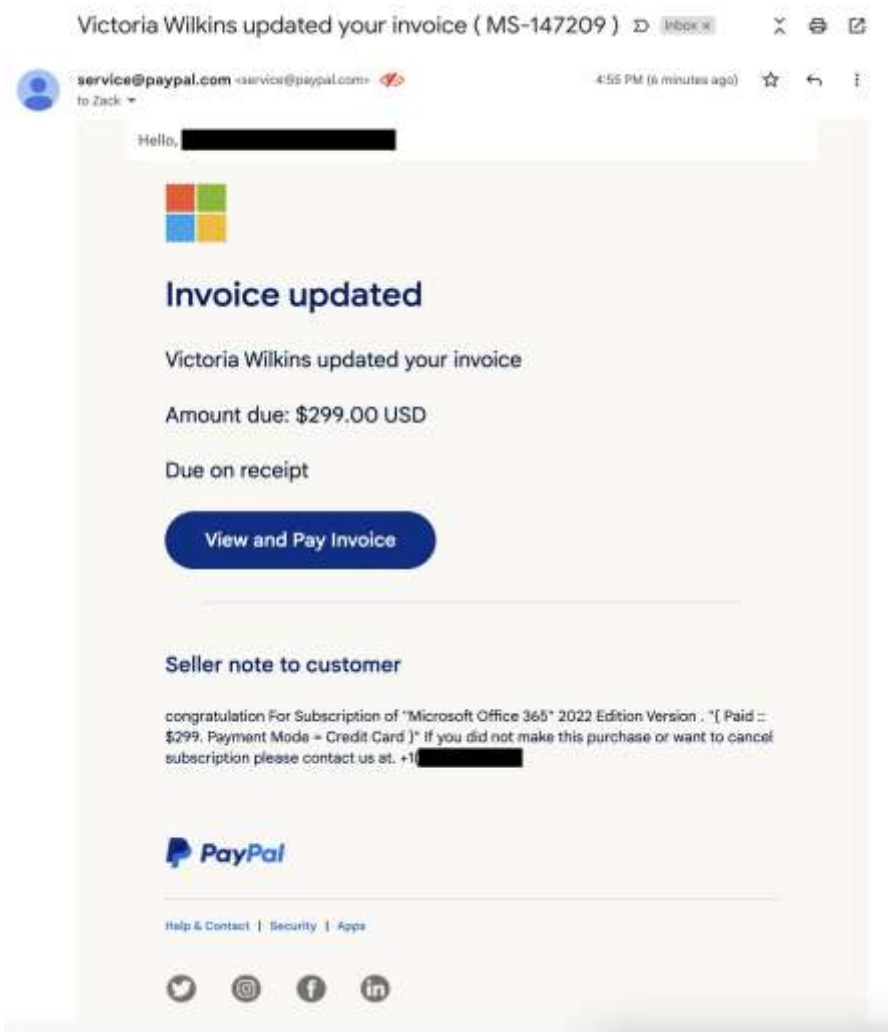
Malicious Cyber Activity Against Election Infrastructure Unlikely to Disrupt or Prevent Voting

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) assess that any attempts by cyber actors to compromise election infrastructure are unlikely to result in large-scale disruptions or prevent voting. As of the date of this report, the FBI and CISA have **no** reporting to suggest cyber activity has ever prevented a registered voter from casting a ballot, compromised the integrity of any ballots cast, or affected the accuracy of voter registration information. Any attempts tracked by FBI and CISA have remained localized and were blocked or successfully mitigated with minimal or no disruption to election processes.

The public should be aware that election officials use a variety of technological, physical, and procedural controls to mitigate the likelihood of malicious cyber activity (e.g., phishing, ransomware, denial of service, or domain spoofing) affecting the confidentiality, integrity, or availability of election infrastructure systems or data that would alter votes or otherwise disrupt or prevent voting. These include failsafe measures, such as provisional ballots and backup pollbooks, and safeguards that protect against voting malfunctions (e.g., logic and accuracy testing, chain of custody procedures, paper ballots, and post-election audits). Given the extensive safeguards in place and distributed nature of election infrastructure, the FBI and CISA continue to assess that attempts to manipulate votes at scale would be difficult to conduct undetected.

Election systems that house voter registration information or manage non-voting election processes continue to be a target of interest for malicious threat actors. Cyber actors may also seek to spread or amplify false or exaggerated claims of cybersecurity compromises to election infrastructure; however, these attempts would not prevent voting or the accurate reporting of results.[a]

The FBI and CISA will continue to quickly respond to any potential threats, provide recommendations to harden election infrastructure, notify stakeholders of threats and intrusion activity, and impose risks and


Victoria Wilkins updated your invoice (MS-147209)
Inbox x
service@paypal.com
to Zack
4:55 PM (6 minutes ago)
Hello, [redacted]
Invoice updated
Victoria Wilkins updated your invoice
Amount due: $299.00 USD
Due on receipt
View and Pay Invoice
Seller note to customer
congratulation For Subscription of "Microsoft Office 365" 2022 Edition Version . "(Paid :: $299. Payment Mode = Credit Card)" If you did not make this purchase or want to cancel subscription please contact us at. +1[redacted]
PayPal
Help & Contact | Security | Apps

PayPal

- Actually sent from PayPal
- Logon to PayPal Invoice is there
- After calling in “Customer service … “
- Install this software then we’ll address this issue
  globalquicksupport.com
- Installed software allows remote control of computer

- Sense of Urgency
- Arms Race

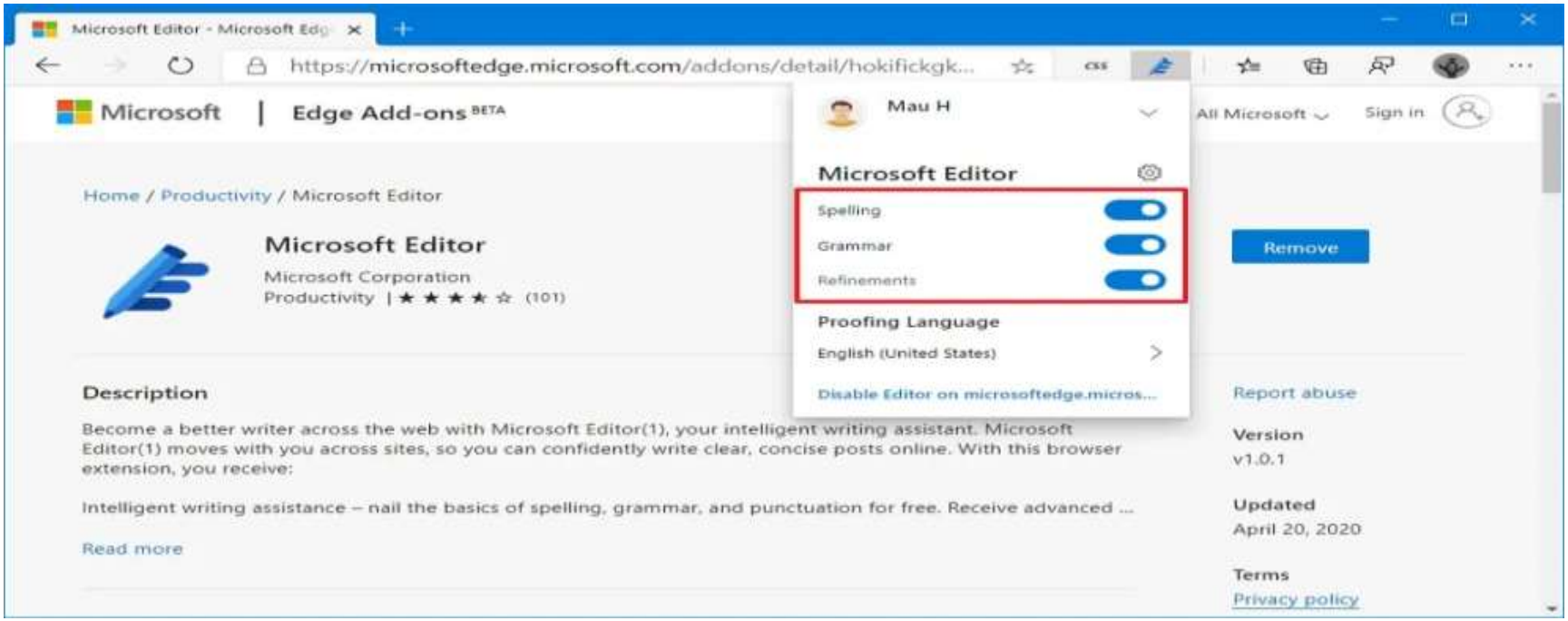
Current Issues

- Deep Fakes AGT Live
- Multi-persona impersonation
- TAILS
- Safer WEB Browsing seminars
- Extended spellcheck
  - Chrome & Edge
  - transmit form data
  - PII
  - Passwords
  - Chrome Extended Spellcheck
  - Edge Microsoft Editor
- Show Password

Spell check

Check for spelling errors when you type text on web pages

- (•) Basic spell check
- ( ) Enhanced spell check
  Uses the same spell checker that's used in Google search. Text that you type in the browser is sent to Google.



Spell Check

- Passwords (passphrases)
- If not in local machine's spell checker library

  Send it to Google or Microsoft or …

#	Host	Method	URL
657	https://passport.alibabacloud.c...	POST	/register/check_enter_email.do?_input_...
332	https://www.googleapis.com	POST	/spelling/v2/spelling/check?key=AIzaS...
312	https://www.googleapis.com	POST	/spelling/v2/spelling/check?key=AIzaS...

Request

Pretty Raw Hex

```
1 POST /spelling/v2/spelling/check?key=
  AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw HTTP/2
2 Host: www.googleapis.com
3 Content-Length: 66
4 Content-Type: application/json
5 Sec-Fetch-Site: none
6 Sec-Fetch-Mode: no-cors
7 Sec-Fetch-Dest: empty
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0
  Safari/537.36
9 Accept-Encoding: gzip, deflate
0 Accept-Language: en-US,en;q=0.9
1
2 {
    "text":"sharepassword*123",
    "language":"en",
    "originCountry":"CAN"
  }
```

Response

Pretty Raw Hex Render

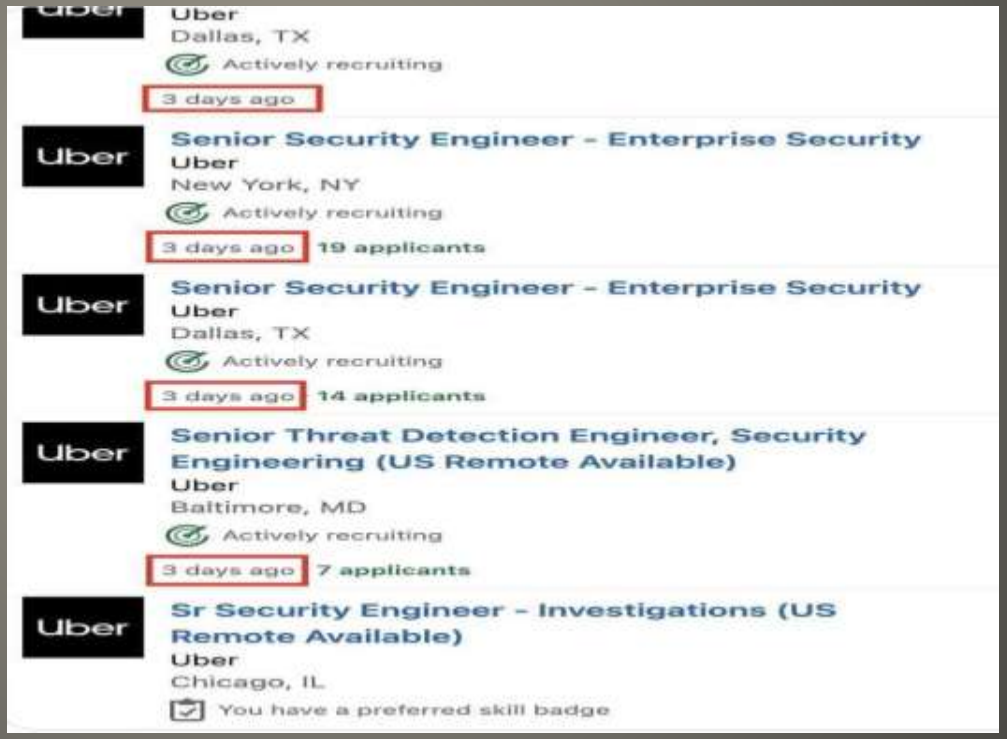
```
1 HTTP/2 200 OK
2 Etag: "mnuQSrnYbS95-Q5C0TEA65xp_PU"
3 Content-Type: application/json; charset=UTF-8
4 Vary: Origin
5 Vary: X-Origin
6 Vary: Referer
7 Date: Mon, 12 Sep 2022 07:19:03 GMT
8 Server: ESF
9 Cache-Control: private
10 Content-Length: 233
11 X-Xss-Protection: 0
12 X-Frame-Options: SAMEORIGIN
13 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443";
   ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443";
   ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;
    v="46,43"
14
15 {
16   "spellingCheckResponse": {
17     "misspellings": [
18       {
19         "charStart": 0,
20         "charLength": 13,
21         "suggestions": [
22           {
23             "suggestion": "share password"
24           }
25         ]
26       }
27     ]
```

- PII
- Medical Condition
- Clinic name
- Hospital street address
- Network topology
- Any/Everything

Spell Check

Current Issues

- WordPress
- LastPass
- Grand Theft Auto 6 code leak
- Uber



- Windows
- macOS
- iOS & iPadOS
- Lenovo BIOS & UEFI
- Every browser & extension

Patch Patch Patch

Current Issues

- Lloyd's of London Cyber Insurance
- NotPetya $1.4 B
- ViaSat service Ukraine – German wind turbine
- Ransomware
  Ransom millions
  Cleanup tens of millions
- Spectre mitigation compute 70%
  spectre_v2=off
- use-after-free
  Google Chrome
- MFA fatigue
- Akami CDN flaw

Current Issues

- American Airlines
  Passport number, driver's
- Chaos cross platform malware
  Linux & Windows
  FreeBSD, small office routers, enterprise servers
  ARM, Intel, PowerPC, MIPS, …
  Known CVEs, stolen SSH keys
  Connected device enumeration, new features
  Reboot?
- Cox communications Tucson
- Optus thousands with hundreds points
- LAUSD data released – no ransom

Current Issues

- Walmart
  - Money transfer service
  - Video surveillance systems & biometrics
  - “Be your own model” “choose my model”
- Firefox 105 fixes 7 security issues
- Meta in-app browser tracking capability
- US Customs and Border Protection
  - 37,000 searches per year
  - 10,000 seizures & copying
- Zoom updates for security
- Microsoft Exchange Servers Vulnerability x2

- Etc.
- Protective glass on picture frames
- Smart Boards
- Video camera resolution
  70p 10mm and up

Video Camera & eyeglasses


Settings
General
Video
Audio
Share Screen
Chat
Zoom Apps
Background & Effects
Recording
Profile
Statistics
Keyboard Shortcuts
Accessibility
Virtual Backgrounds
Video Filters
Avatars
BETA
None
Huh?

Video Camera & eyeglasses

- Etc.
- Protective glass on picture frames
- Smart Boards
- Video camera resolution
  70p 10mm and up

- Not just eyeglasses
  eyes
  Any reflective object

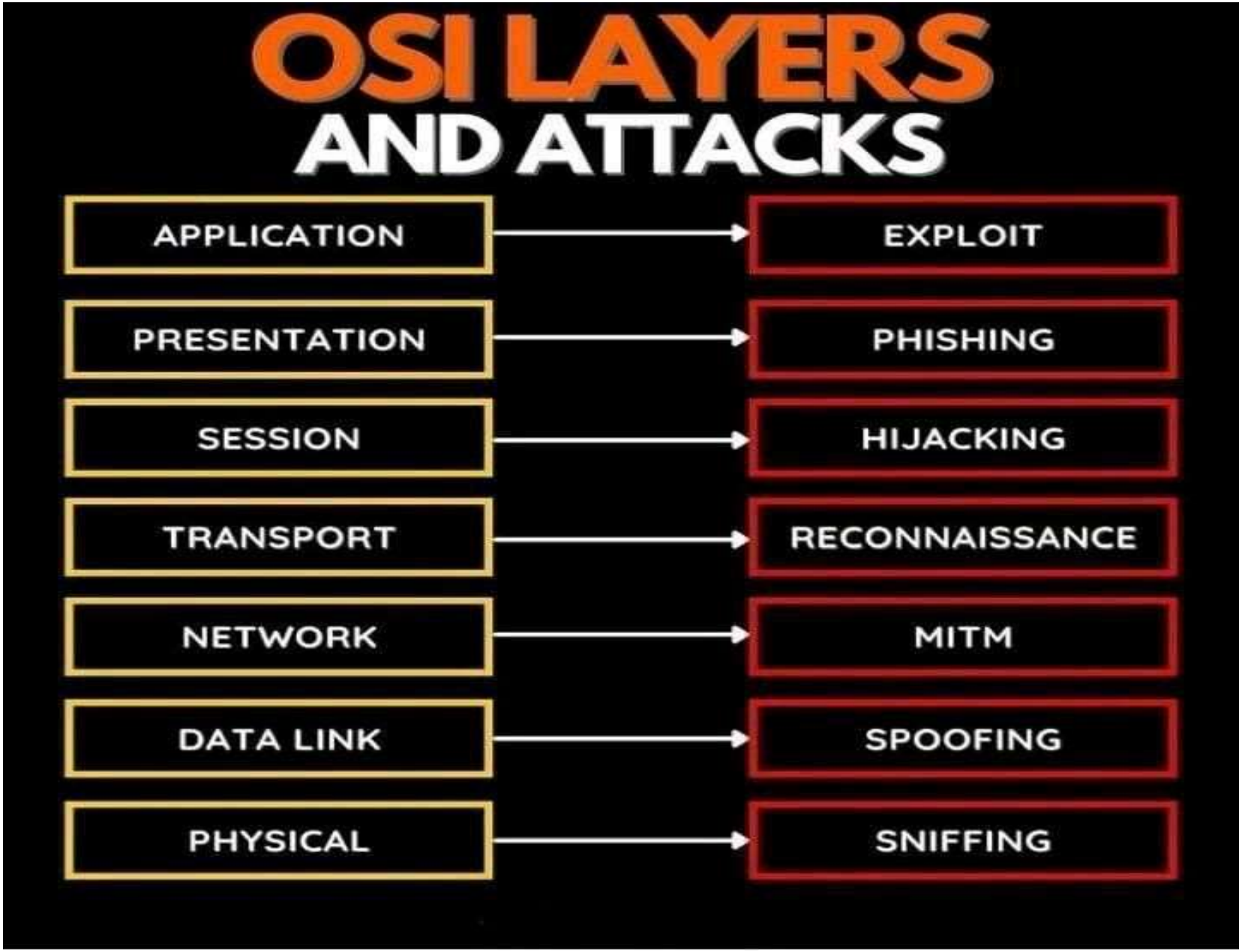
Resolution Helpful <-> Harmful

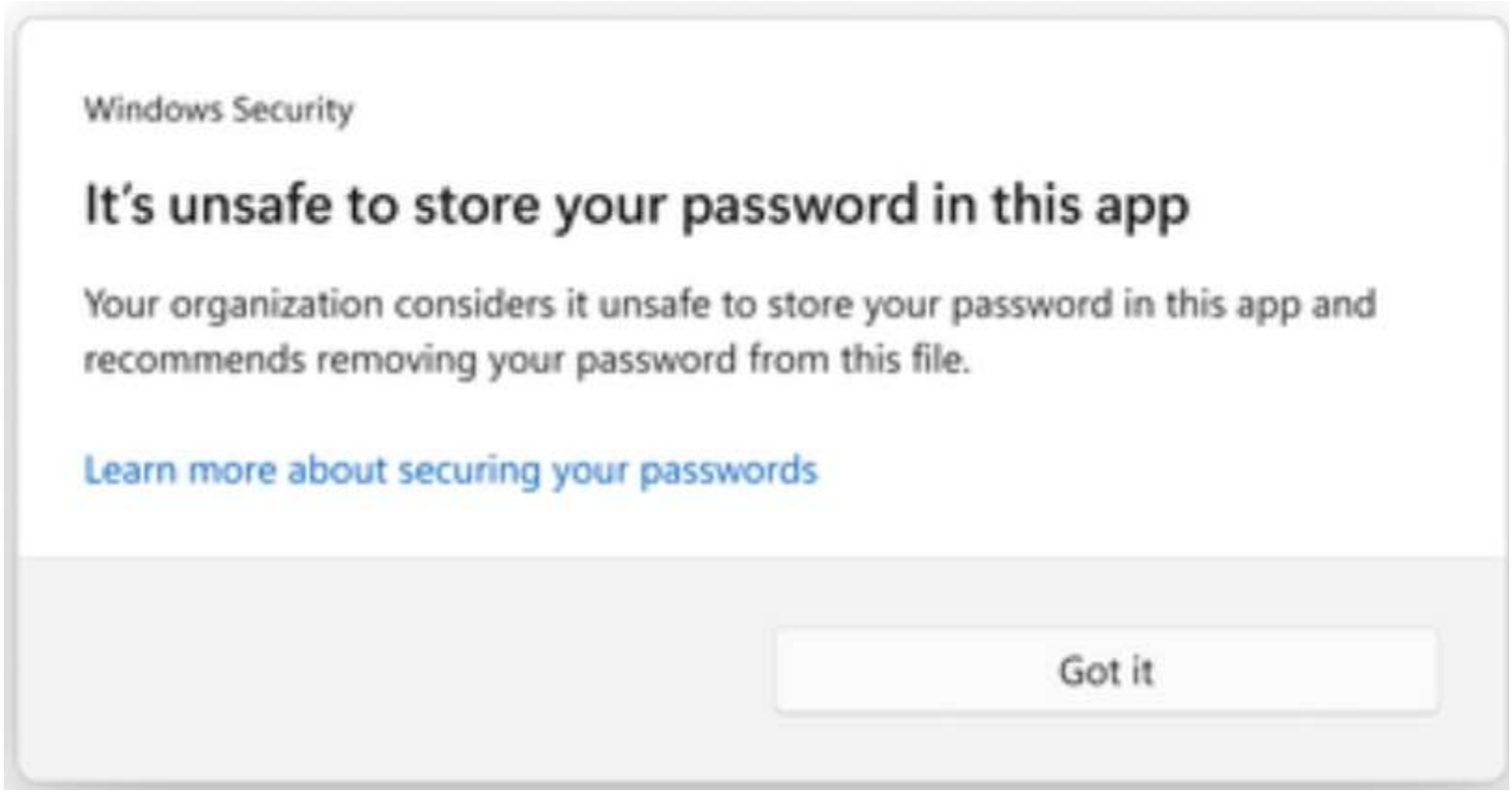
eSIM


You no longer need a physical SIM card.
Activate your eSIM during iPhone setup.
For more information, go to
apple.com/esim.

Current Issues

- 15-year-old Python flaw unpatched
  CVE-2007-4559
  path transversal vulnerability in tarfile module
- Morgan Stanley $35M fine
  Failure to scrub storage devices prior sale
- Iranian state-sponsored actors lurk Albanian Government more than a year
- Iran ban Signal and other
- NSA & CISA guidance
  Securing OT and ICS systems
- Optus data breach
- American Airlines learned of data breach via phishing campaign
- Microsoft Teams clear text password storage


OSI LAYERS
AND ATTACKS
APPLICATION
EXPLOIT
PRESENTATION
PHISHING
SESSION
HIJACKING
TRANSPORT
RECONNAISSANCE
NETWORK
MITM
DATA LINK
SPOOFING
PHYSICAL
SNIFFING


Windows Security
It's unsafe to store your password in this app
Your organization considers it unsafe to store your password in this app and recommends removing your password from this file.
Learn more about securing your passwords
Got it

Digital Dust

- WiFi Access points privacy agreements
- Psychological aspects of living online
- Samsung privacy policy update

  October 1

  Account creation: name, age, addresses, gender, etc.

  AND

  Credit card, credentials, photos, contacts, text logs, voice recordings, location data – precise, nearby Wi-Fi, cell towers

  Cookies, pixels, web beacons, etc.

  Device info: IP address, device model, apps, etc.

  Service Improvements, fight fraud,

- And then Android …

Digital Dust

- Hacking Google
  - Operation Aurora
  - Threat Analysis Group
  - Detection and Response
  - Red Team
  - Bug Hunters
  - Project Zero

Hackers are Internet's immune system

YouTube

- 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