Sun City Computer Club

Cyber Security SIG

August 6, 2020

Questions, Comments, Suggestions welcomed at any time

Even Now

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

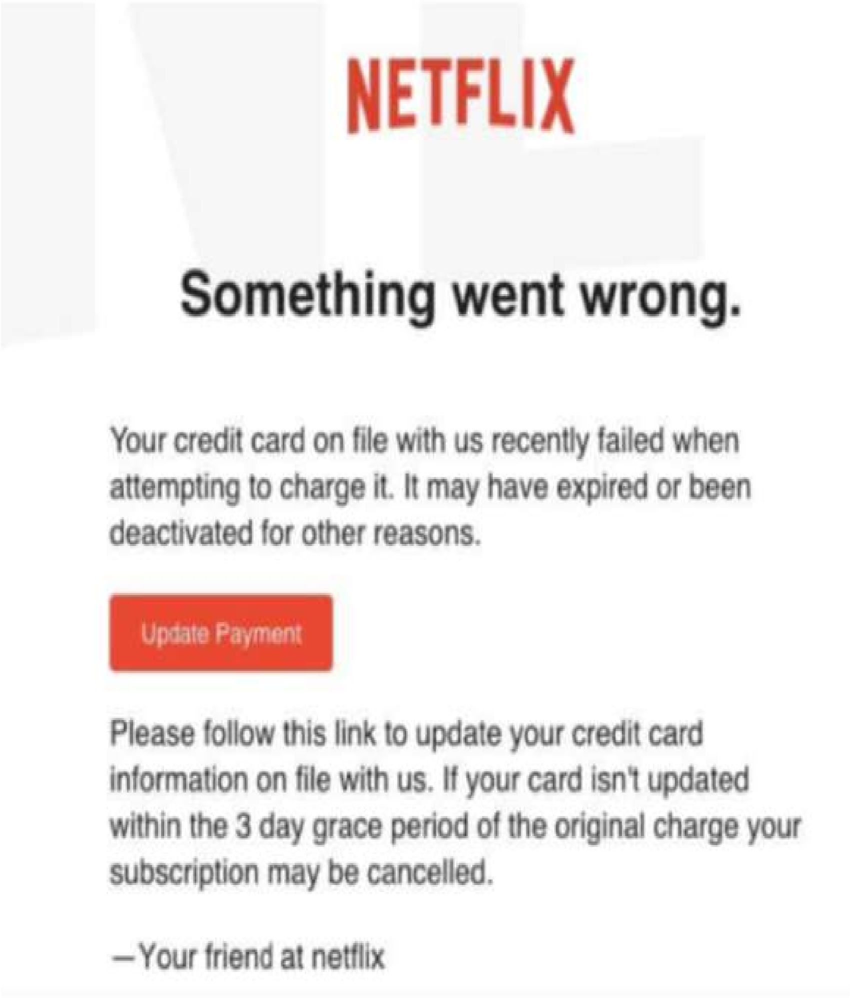
Audio Recording In Progress

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

- The twitter incident
  bitcoin scam
  could have been catastrophic
  stock speculation
  political
- Teenage Florida youth $700,000 the $180,000
- Bond hearing on zoom porn bombed

- SIGRed
- False Facebook ads
- Garmin down – ransomware?
  fitness tracking   FLIGHT TRACKING pilots
  Ransomware tax deductible?
  Custom decryptor   in memory encryption

Current Issues



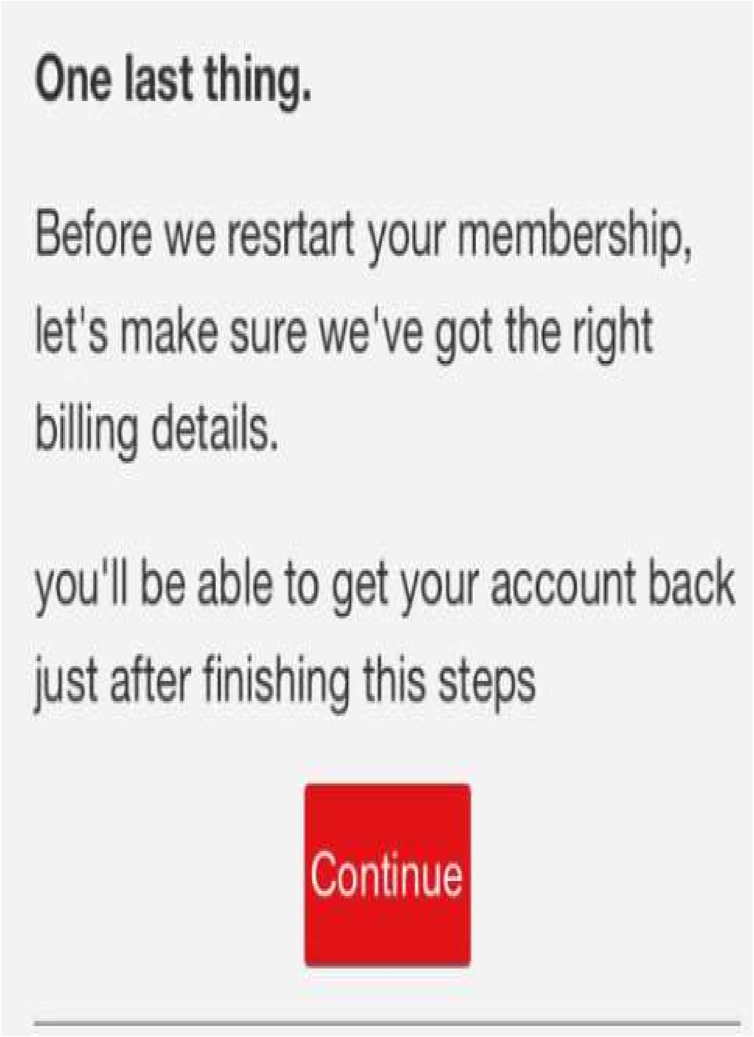
NETFLIX

Something went wrong.

Your credit card on file with us recently failed when attempting to charge it. It may have expired or been deactivated for other reasons.

Please follow this link to update your credit card information on file with us. If your card isn't updated within the 3 day grace period of the original charge your subscription may be cancelled.

—Your friend at netflix



One last thing.

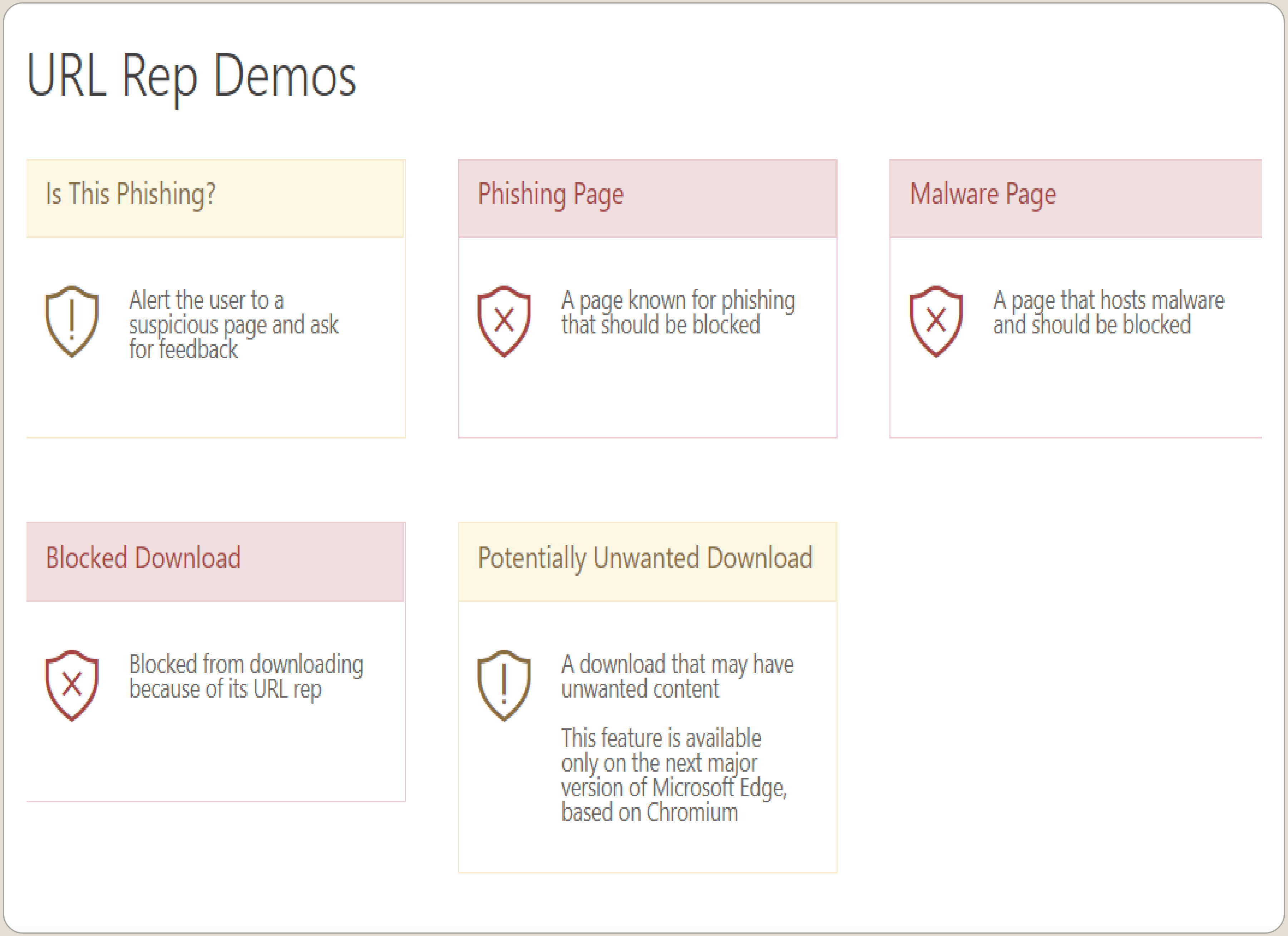
Before we resrtart your membership, let's make sure we've got the right billing details.

you'll be able to get your account back just after finishing this steps

- Fake sales to legitimate foreign addresses
- Send low worth product with tracking
- Satisfaction survey
- Sell collected account info
- Monitor feedback
- Offer refund

  “just give us credit card to refund funds”

Reputation building



URL Rep Demos

Is This Phishing?

Alert the user to a suspicious page and ask for feedback

Phishing Page

A page known for phishing that should be blocked

Malware Page

A page that hosts malware and should be blocked

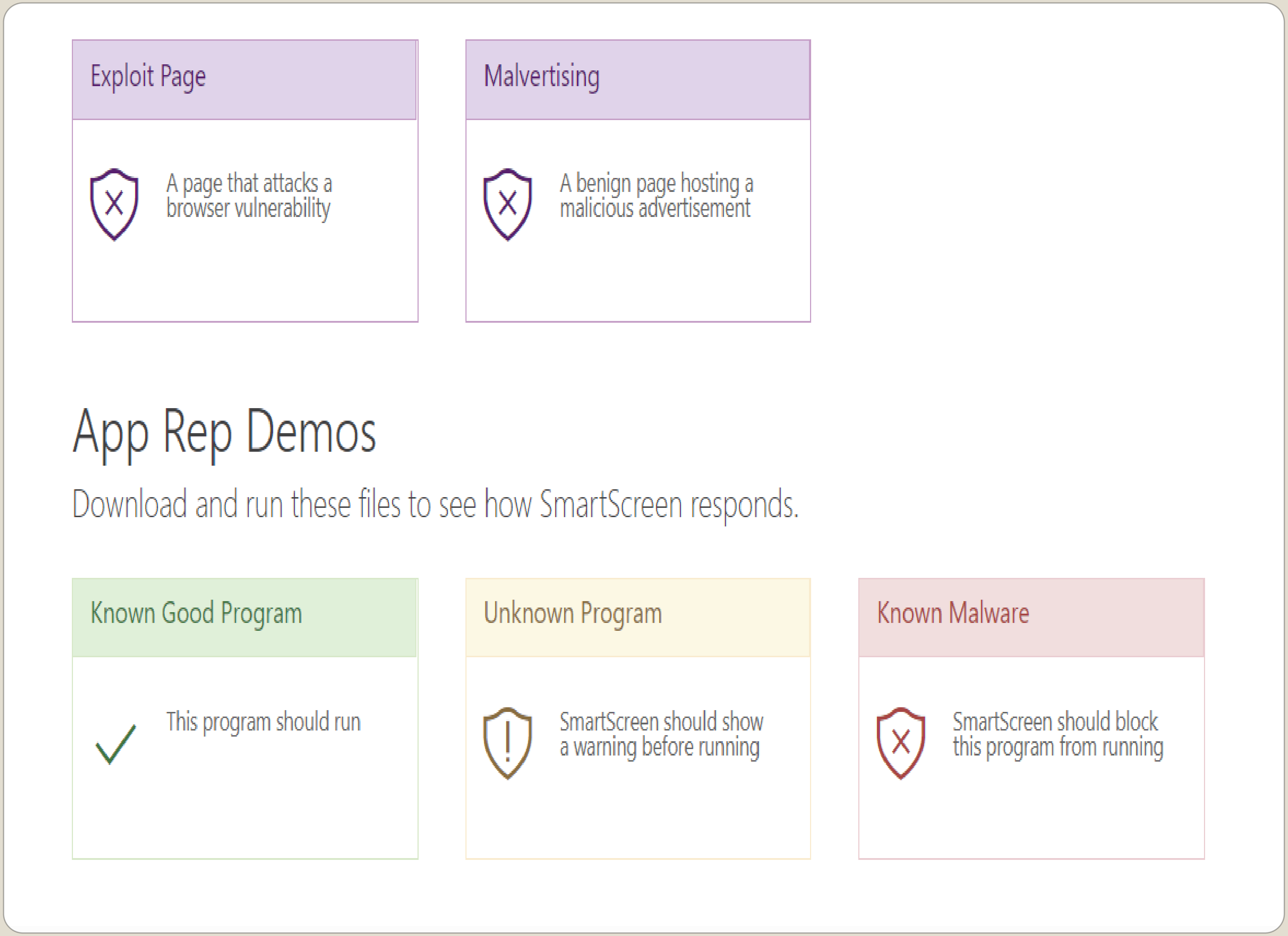
Blocked Download

Blocked from downloading because of its URL rep

Potentially Unwanted Download

A download that may have unwanted content

This feature is available only on the next major version of Microsoft Edge, based on Chromium



Exploit Page

A page that attacks a browser vulnerability

Malvertising

A benign page hosting a malicious advertisement

App Rep Demos

Download and run these files to see how SmartScreen responds.

Known Good Program

This program should run

Unknown Program

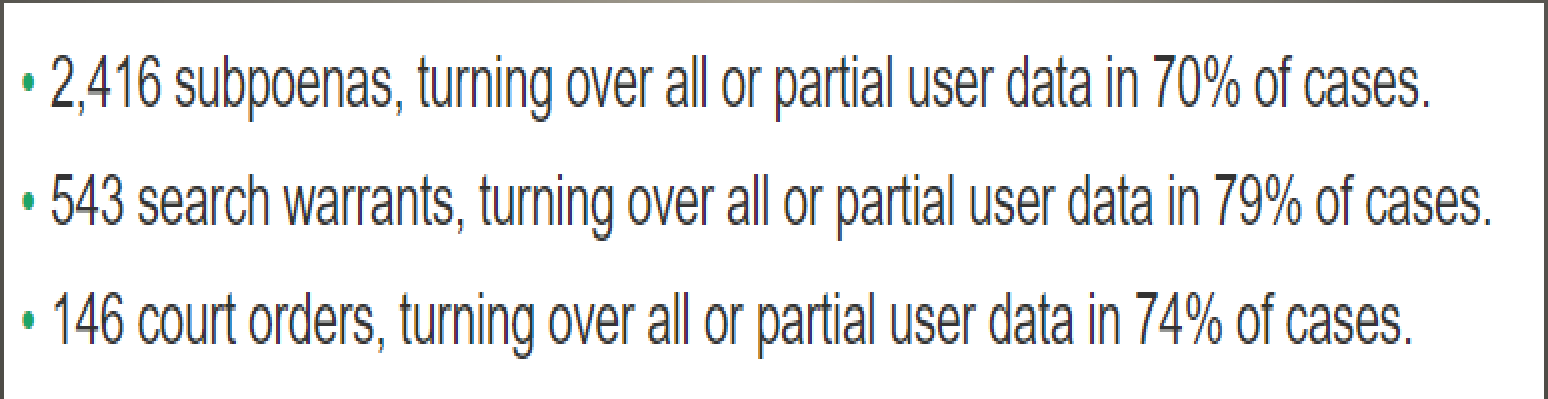
SmartScreen should show a warning before running

Known Malware

SmartScreen should block this program from running

Amazon & customer data

- Law Enforcement
- 23% more subpoenas
- 29% more court orders
  than last year
- Not FISA



- 2,416 subpoenas, turning over all or partial user data in 70% of cases.
- 543 search warrants, turning over all or partial user data in 79% of cases.
- 146 court orders, turning over all or partial user data in 74% of cases.

- Shlayer trojan
  Link to fake Adobe flash update MAC
- Microsoft Download Center SHA-1 removal
  Movie Maker via attackers
- Emotet botnet with GIFs
- TikTok purchase by Microsoft?
- QNAP NAS devices - then firmware deny
- Instacart bank account drain
- DoH for exfiltration
- Firefox Lockwise export
- Zoom 6digit PIN w/o rate limiting

Current Events

GRUB

- GRUB2 grub.cfg EFI system partition
- BootHole
- Then 7 CVEs
- Update Installers, bootloaders, shims
- New shims signed by Microsoft 3rd party UEFI CA

- Basic Input Output System BIOS
- Extensible Firmware Interface EFI
- Unified Extended Firmware Interface UEFI

- Set your “zoom” name to Zoom

  “Zoom is requesting access to your computer”

  Allow
- CCleaner Windows Defender
- CCleaner Microsoft Defender

  Potentially Unwanted Application

  Microsoft Forum ban report 10/10/2019

  Registry issue
- Pulse Secure VPN *server* credentials dump
- Rite Aid facial recognition technology

  8 years ago

Current Events

More Current Events

- EU sanctions

  Individuals & entities from China, Russia, North Korea

  6 individuals & 3 institutions

  Assets frozen

  No asset transfers to

  No entry into EU

  Unanimity from 27 members

  Cyber Sanctions Regime

Stingray revisit

- Stingrays & dirtboxes
- Use of *National Security* loophole?
- Cell site simulator IMSI catcher
- Evidence via other means
- NDA Price   Maintenance & training
- Force 2G encryption
- Malware to turn on microphone
- Malware to turn off speaker
- Send false SMS messages to/from victim
- Software defined radio
- Wi-Fi, cellular, Bluetooth, ZigBee, etc. RADIO

- 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

QUESTIONS ?