Sun City Computer Club

Cyber Security SIG

March 3, 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

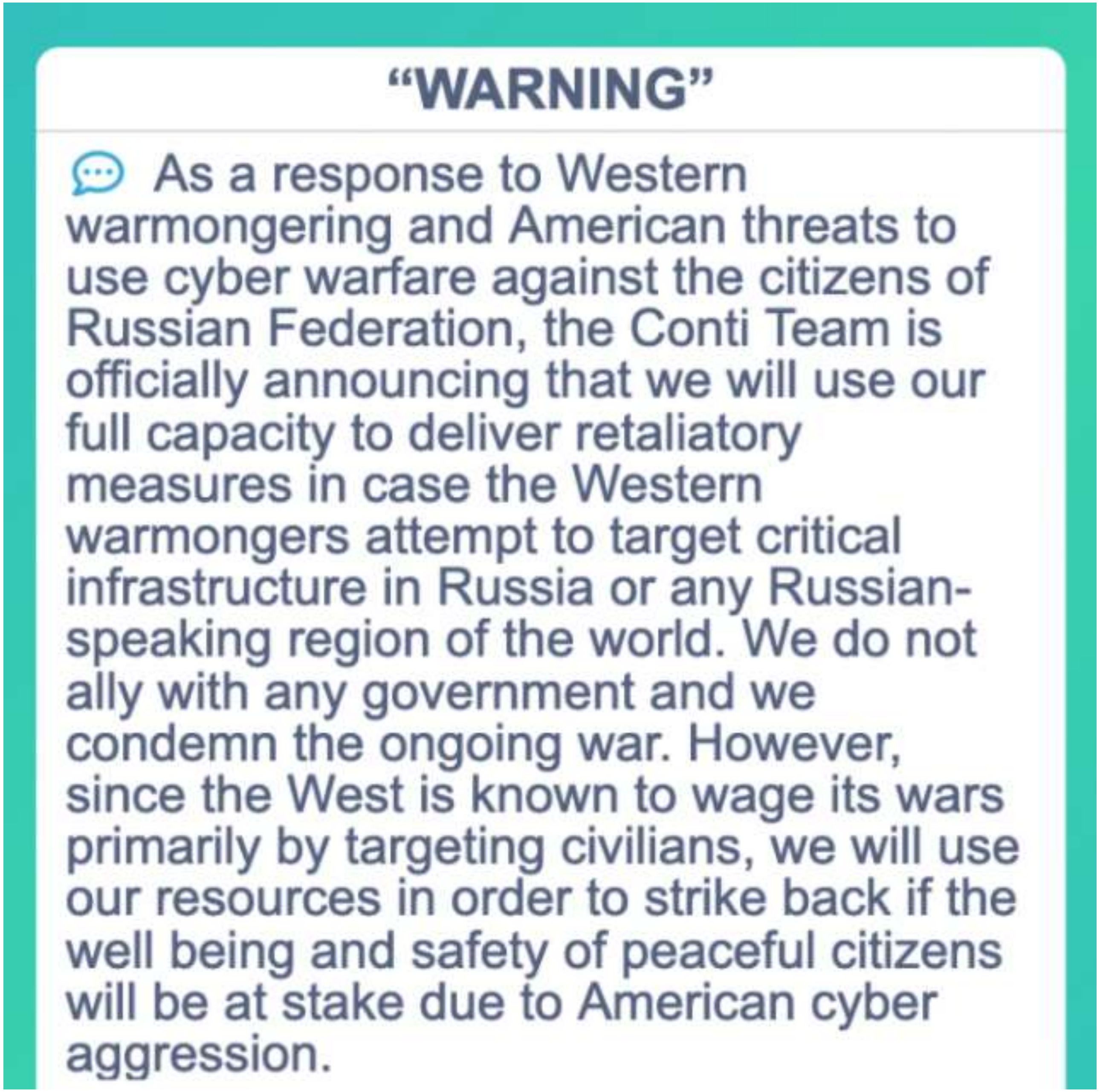
SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

Presenter???

- Ever want to be a presenter??

Cyber Hacktivism

- A actor has unprecedented power
- BGP & DNS
- Russia has tested self-isolation
- Ukraine has been tested – inoculated
- SWIFT and cyber currency



“WARNING”

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

- Thermobaric weapon
- Invasion map on live TV?

  Belarus
- Cyber attacks agriculture, commercial, finance, and energy sectors

  Digital Geneva Convention

  War Crimes
- Anonymous play Ukrainian National Anthem
- Twitter *Russian Oligarch Jets*
- Putin’s yacht “hell”
- Cyber warfare
- Last time Russia DDoS efforts
- Senate pass *Strengthening American Cybersecurity Act*

Current Issues

Data & death

- We live thru Digital lives as well
- Individuals own their data
- so do the platforms they inherit that data
- Helpful <-> harmful

  pics of grandkids <-> Political rant
- AI and machine learning
- LARGE numbers of deceased data stores
- “biggest archive of human behavior”
- Digital collective narrative
- Care of physical remains
- Care of digital remains

Death & Data

- Only living own assets/property
- Person & digital platform
- Crypto wallets & access
- Multi signature access
- Encryption – symmetric shared key

- Digital executor
- Passwords
- Biometric authentication
- Google Inactive Account Manager
- Facebook Legacy Contact

Current Issues

- WordPress sites receive forced patch
- WordPress UpdraftPlus vulnerability
- Xenomorph Android banking trojan

  Google Playstore

  3.48 million 3800 added per day
- QR codes easy   TOO Easy?

  Send Money, Open website, Open App

  Trusted source

  Check Site’s URL, Certificate, Reputation, etc.

  Check for sticker, look-a-like duplicate,

Current Issues

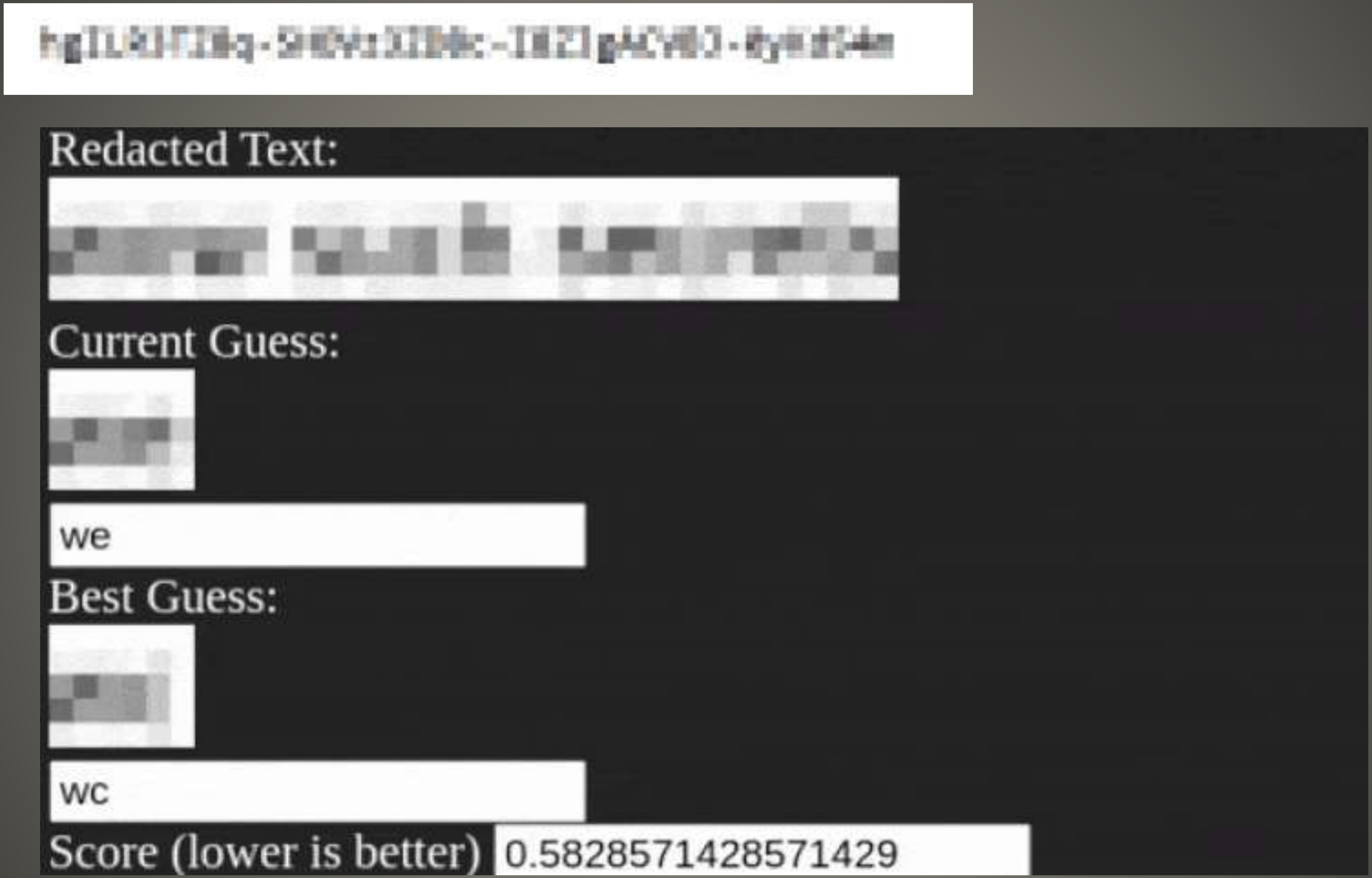
- QR codes
  Parking meters
  Stealing bicycles

- Daxin
- Most sophisticated back door malware
- More hardened the target
- More susceptible to Daxin
- Windows kernel driver
- Magic cookie key

Curent Issues

- How much is cyber criminals?
- They pay ransom => WE pay the ransom

Inflation



Redacted Text:

Current Guess:

we

Best Guess:

wc

Score (lower is better) 0.5828571428571429

Pixelated redaction

- A France father with social media addicted son
- Ukrainian DDoS attacks

  Evolution

  Asymmetric UDP attacks spoofing

  WEB

    usedtobe static HTTPS query -> Reply

    archives => applications

    applications single threaded interpretative

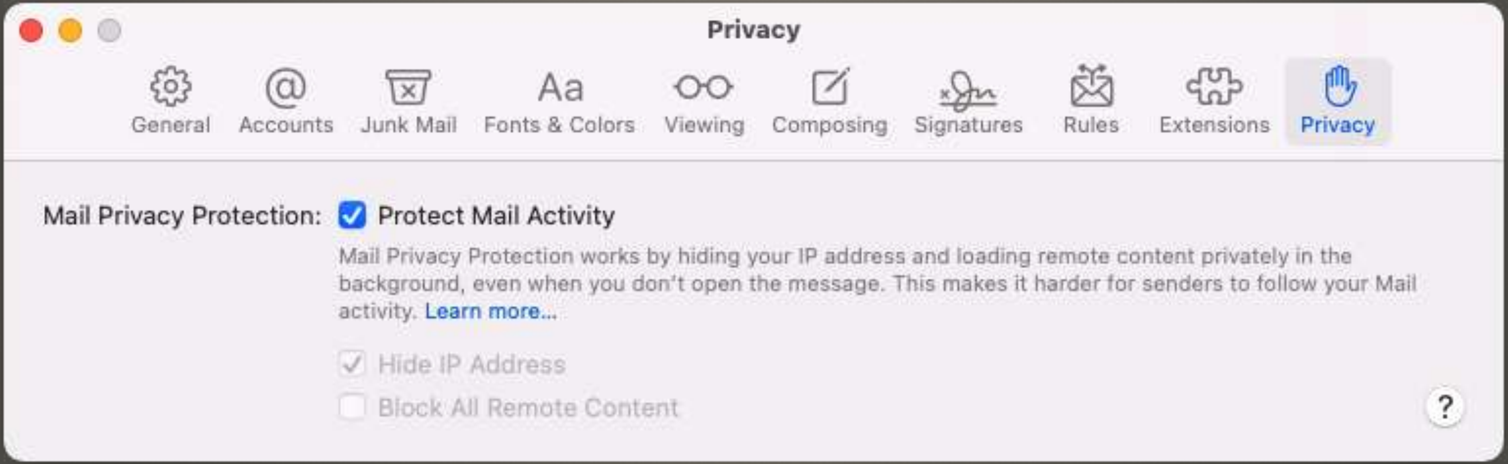
    distributed web gateways databases

  Ukraine Russia’s petri dish Botnet
- BGP hijack affecting South Korean crypto exchange

Current Issues

eMail privacy

- The pixel problem
- Images
- Richer experience
- Richer advertisers
- Apple
  - iPhone iPad
    - Settings -> Mail -> Privacy Protection
  - macOS
    - Mail -> Preferences Protect Mail Activity



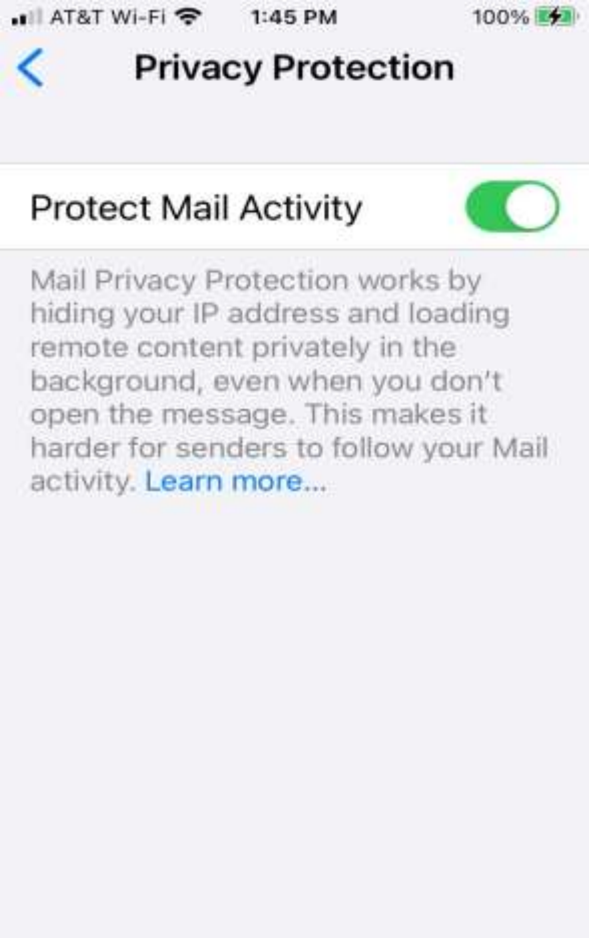
Mail Privacy Protection: ☑ Protect Mail Activity

Mail Privacy Protection works by hiding your IP address and loading remote content privately in the background, even when you don't open the message. This makes it harder for senders to follow your Mail activity. Learn more...

☑ Hide IP Address

□ Block All Remote Content

macOS



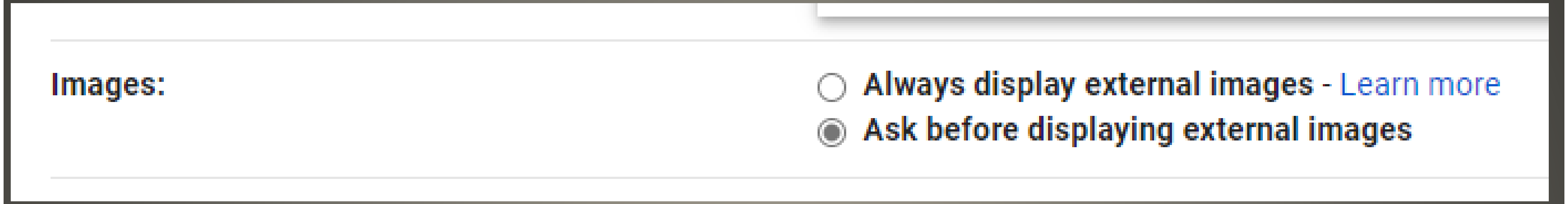
Privacy Protection

Protect Mail Activity

Mail Privacy Protection works by hiding your IP address and loading remote content privately in the background, even when you don't open the message. This makes it harder for senders to follow your Mail activity. Learn more...

iPhone

- Gmail Settings General



Images:

○ Always display external images - Learn more

● Ask before displaying external images

eMail clients

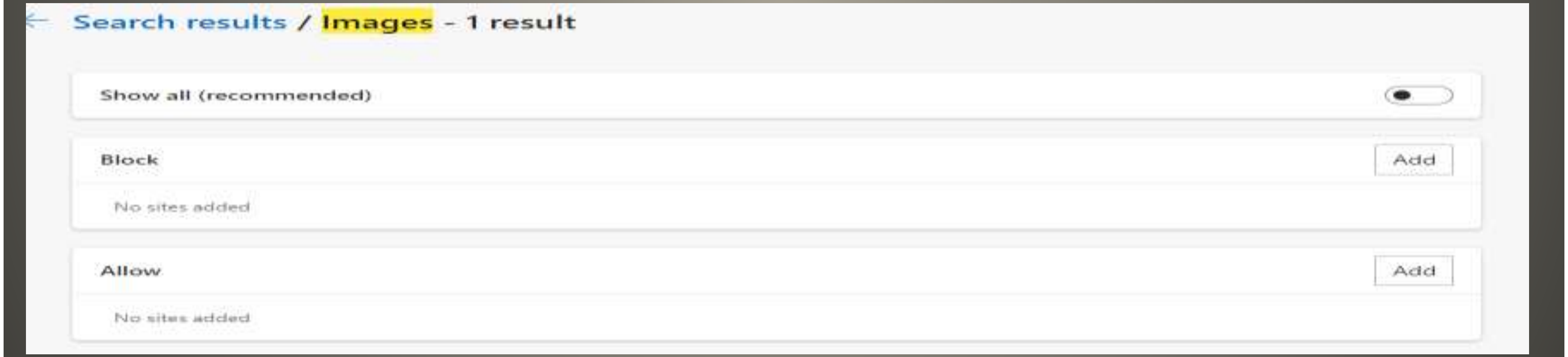
- Yahoo

Settings -> More Settings -> View Email

Ask before showing external images

- Outlook

Search Images



Search results / Images - 1 result

Show all (recommended)

Block

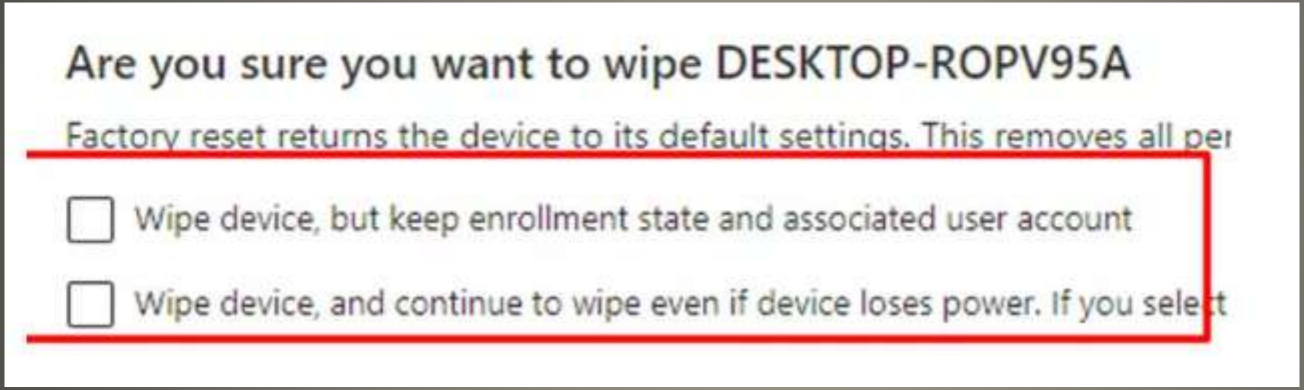
No sites added

Allow

No sites added

eMail Clients

- Windows Intune disk wipe function
  Leaves Windows.old folder
  And turns off Bitlocker



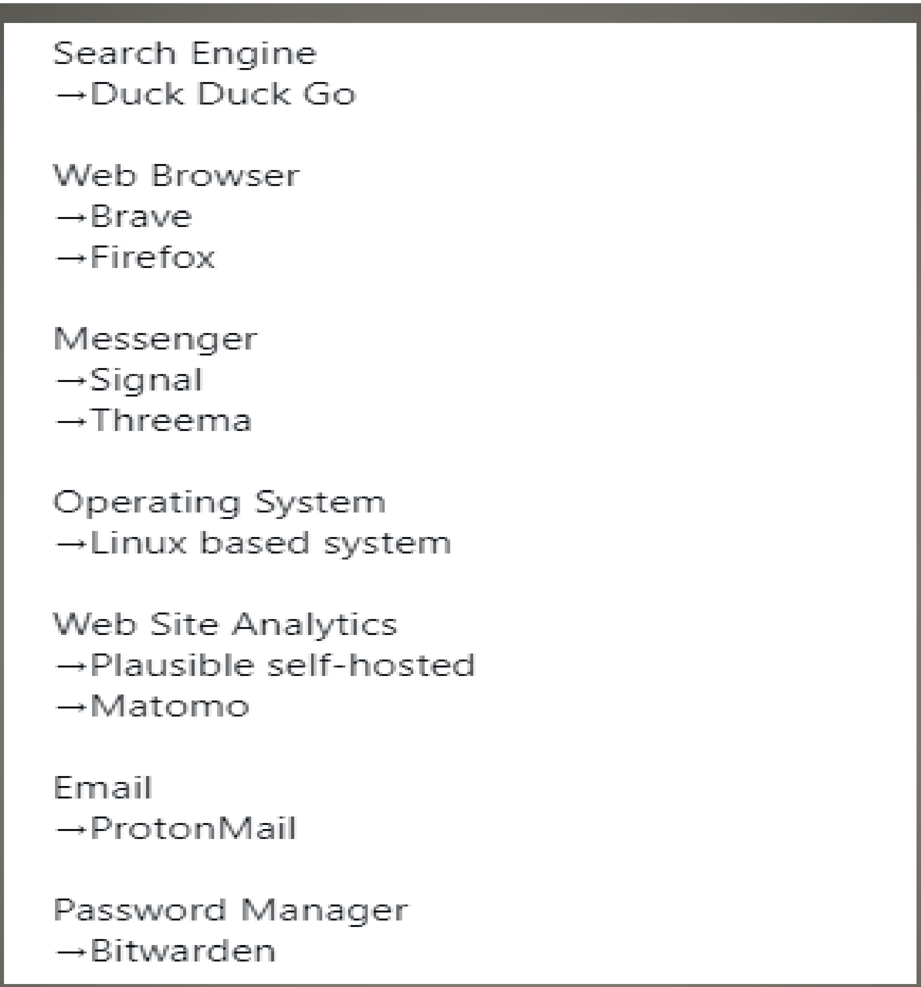
Are you sure you want to wipe DESKTOP-ROPV95A

Factory reset returns the device to its default settings. This removes all per

□ Wipe device, but keep enrollment state and associated user account

□ Wipe device, and continue to wipe even if device loses power. If you select

Current Issues



Search Engine
→Duck Duck Go

Web Browser
→Brave
→Firefox

Messenger
→Signal
→Threema

Operating System
→Linux based system

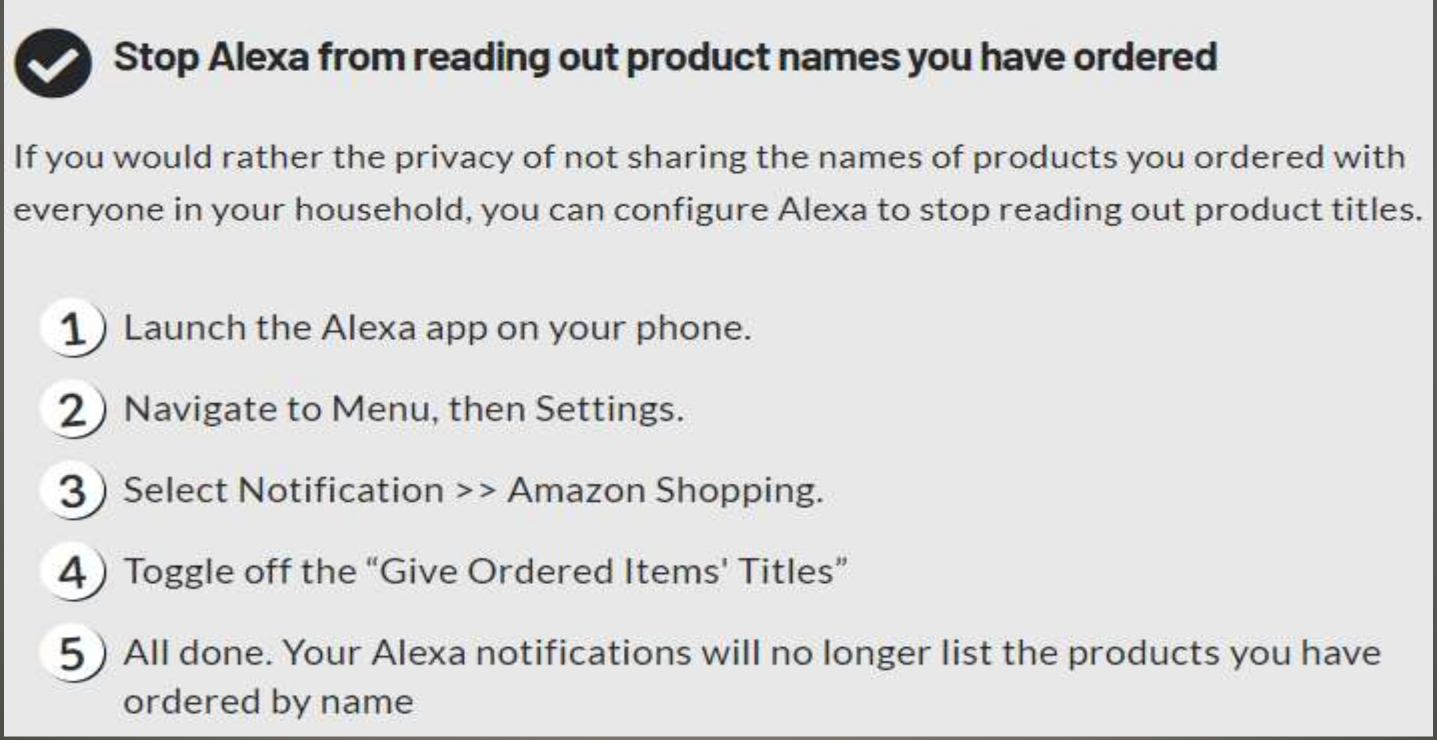
Web Site Analytics
→Plausible self-hosted
→Matomo

Email
→ProtonMail

Password Manager
→Bitwarden

Free tools for Privacy

- Alexa yellow ring Notifications



Stop Alexa from reading out product names you have ordered

If you would rather the privacy of not sharing the names of products you ordered with everyone in your household, you can configure Alexa to stop reading out product titles.

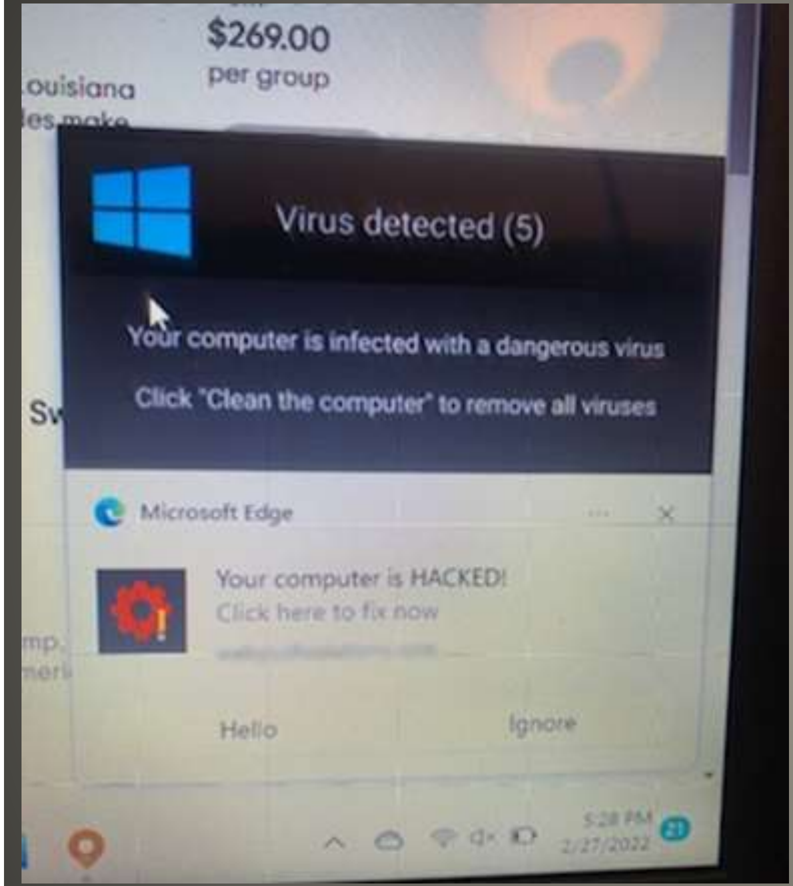
1. Launch the Alexa app on your phone.
2. Navigate to Menu, then Settings.
3. Select Notification >> Amazon Shopping.
4. Toggle off the “Give Ordered Items' Titles”
5. All done. Your Alexa notifications will no longer list the products you have ordered by name

Alexa shopping notifications

- National Security Memorandum 8
- NSA 30 days to begin update

  Commercial National Security Algorithm Suite
- Intelligence Agencies identify any and all instances NOT in compliance with NSA approved quantum Resistant Algorithms

Cyber Security Order



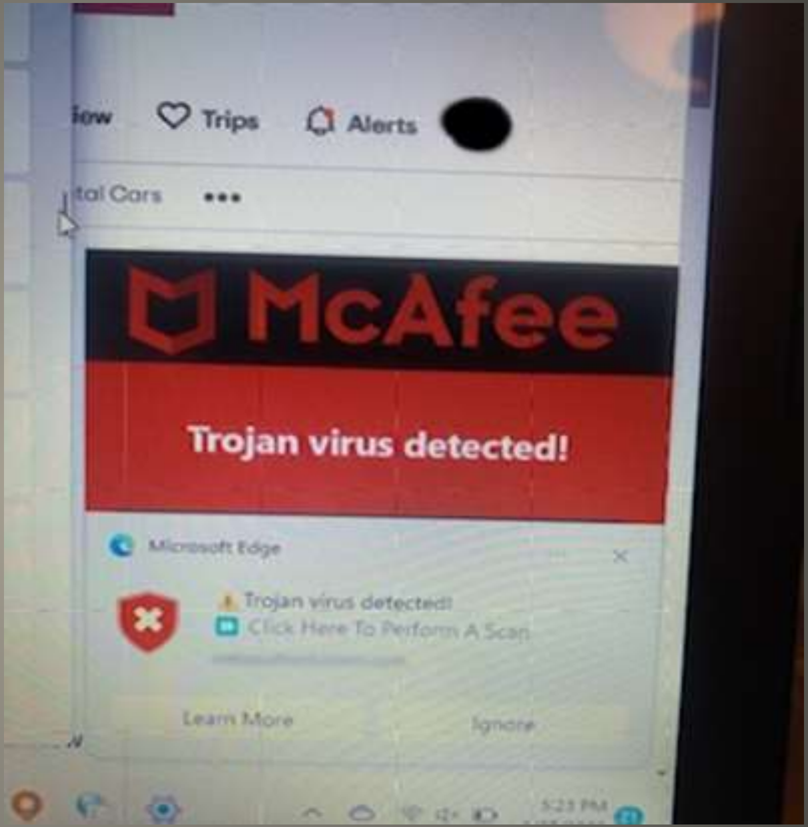
Virus detected (5)

Your computer is infected with a dangerous virus

Click "Clean the computer" to remove all viruses

Microsoft Edge

Your computer is HACKED!
Click here to fix now



Trojan virus detected!

Microsoft Edge

⚠ Trojan virus detected!
Click Here To Perform A Scan

Browser Notifications

Browser

- Version Updates
- Check before each “sensitive” visit
- Extensions for safer browsing:

HTTPS Everywhere

EFF & ToR

Most browsers

Privacy Badger

Stops tracking

Color Coded sites

uBlock Origin

Site block list

Malwarebytes Browser Guard

Avira Browser Safety

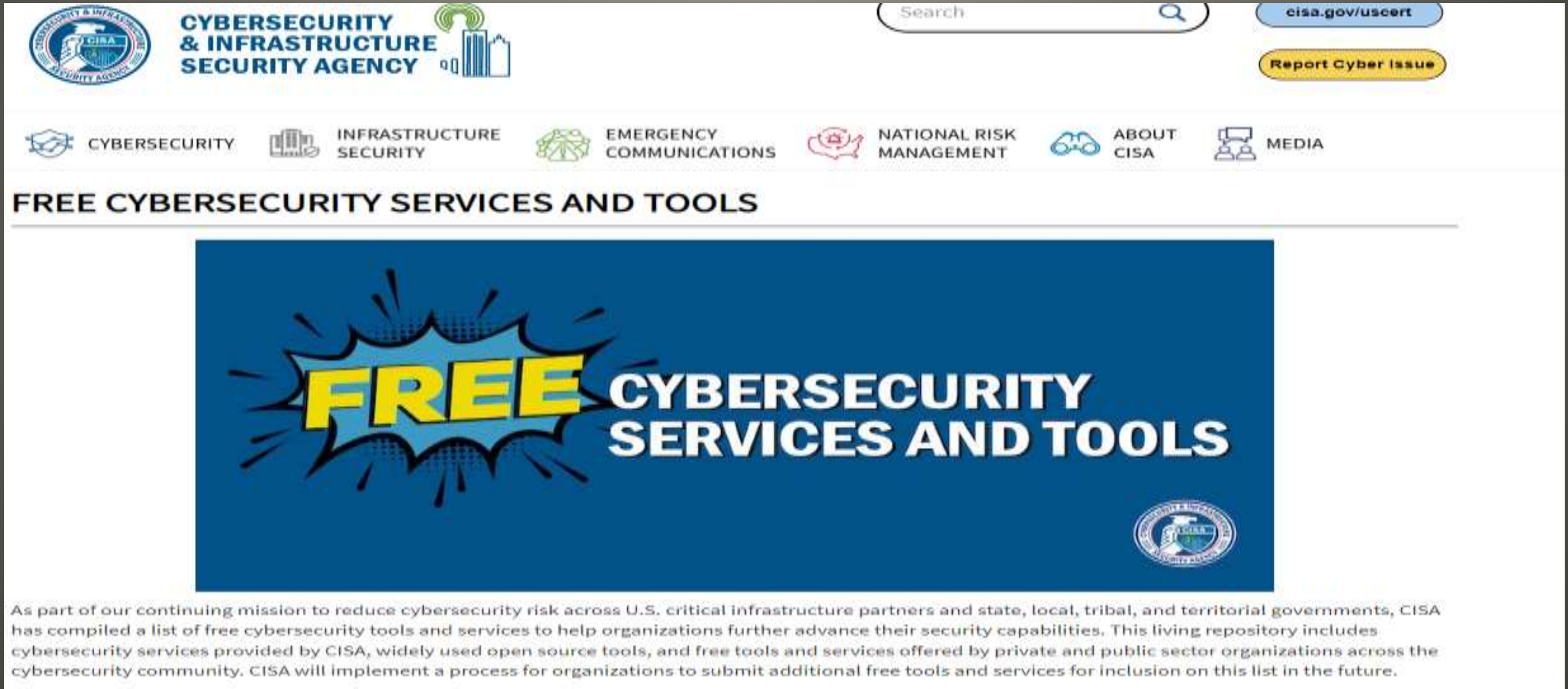
ClearURLs

- Wiper attacks spread “accidently”
- SpaceX satellite service Ukraine

Current Issues

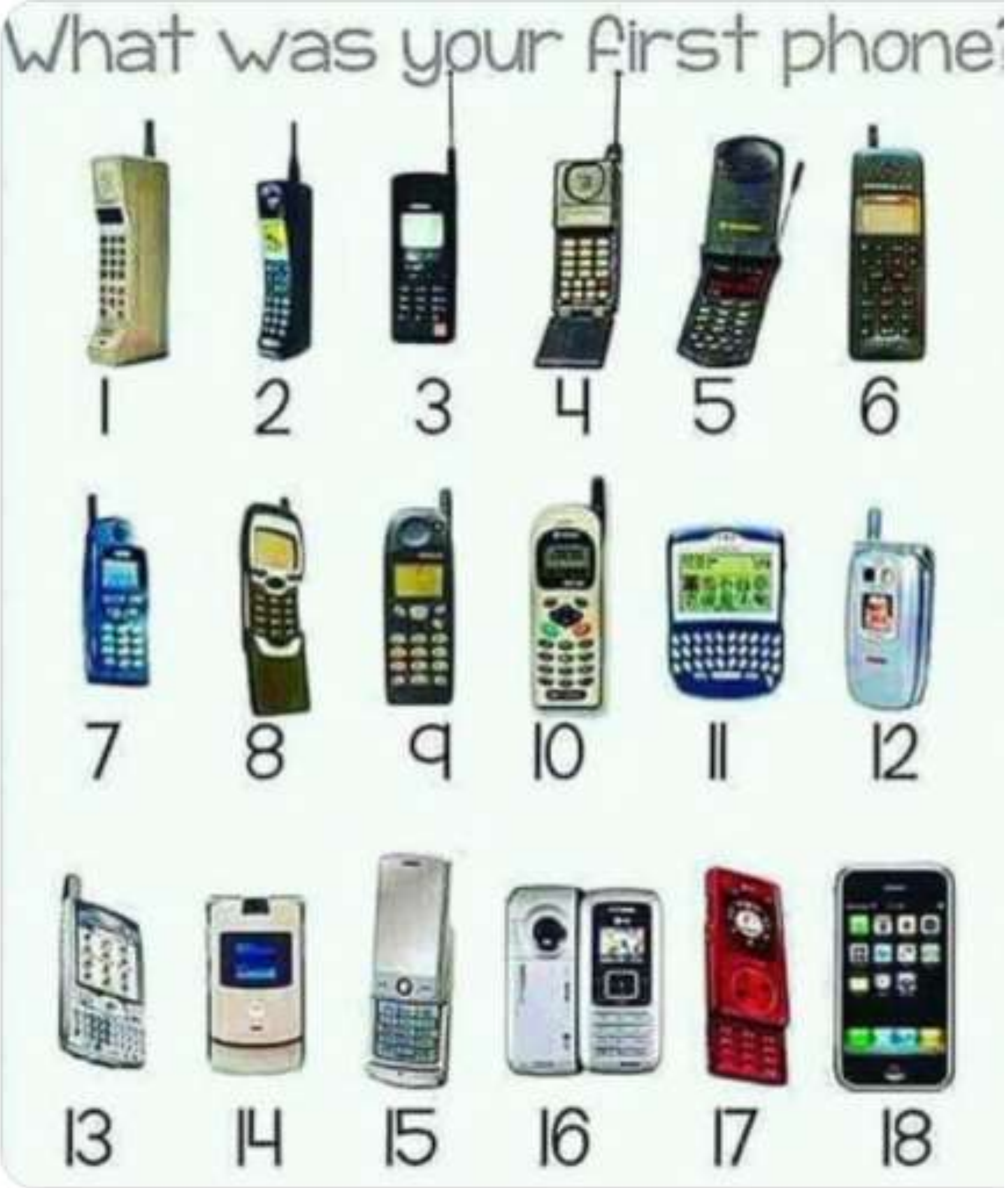
CISA Free Tools

- Cybersecurity & Infrastructure Security Agency
- https://www.cisa.gov/free-cybersecurity-services-and-tools



FREE CYBERSECURITY SERVICES AND TOOLS

As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. CISA will implement a process for organizations to submit additional free tools and services for inclusion on this list in the future.


What was your first phone?
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

- 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