

# Sun City Computer Club

Cyber Security SIG

May 5, 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???**





**Amazon Locker - Also across room lockers**

- Cinco de Mayo
  - World Password Day
  - Apple, Google, Microsoft
- Build support for passwordless sign-in  
Within a year  
Unique cryptographic token    passkey  
Helpful <-> Harmful  
FIDO Alliance  
Fast IDentity Online  
Found Phone

**May 5**

- ATMs
- Gas pumps
- Mobile vendors
- Dining
- Chain Retailers
- Online
- Storing entities

**Risky places to swipe credit cards**

- Notify Card Issuer
- Provide written statement  
Certified with delivery receipt  
Keep a copy
- New Card New PIN
- Monitor

- Notify Card issuer's Fraud Department
- Change your passwords
- Review current Credit Report
- Notify other financial institutions
- Report to FTC IdentityTheft.gov
- Fraud Alert to credit bureaus
- Contact Law Enforcement

**Credit Card theft steps**



- 42 million victims \$52B
- Safeguard foundational identity documents
- Freeze credit
- Read financial account statements
- Check explanations of benefits
- Complex & unique passphrases with MFA
- Monitor Credit Reports
- Collect Mail every day Informed Delivery
- Shred
- ID theft awareness, preparedness, understanding
- Scrub electronics
- Setup financial alerts
- Digital wallets
- Physical awareness

## **12 Steps Identity Theft Prevention**

Apple ID <[redacted]>

Sat 09/04/2022 04:13

To: [redacted]

Cc: [redacted]

Your Apple ID has been locked on Friday, April, 8 2022 for security reasons because you have reached the maximum number of invalid sign-in attempts

You cannot access your account and any Apple services

To unlock your account, you'll need some additional verification

VERIFY ACCOUNT

For your security and to ensure only you have access to your account, we will ask you to verify your identity

*Fake Apple mail*

Oh My

- Click on

VERIFY ACCOUNT

- Off to Website Spam
- Magical Mystery Tour  
Wall Cladding, Polytechnic schools, etc.

- Reminders:  
Report Spam

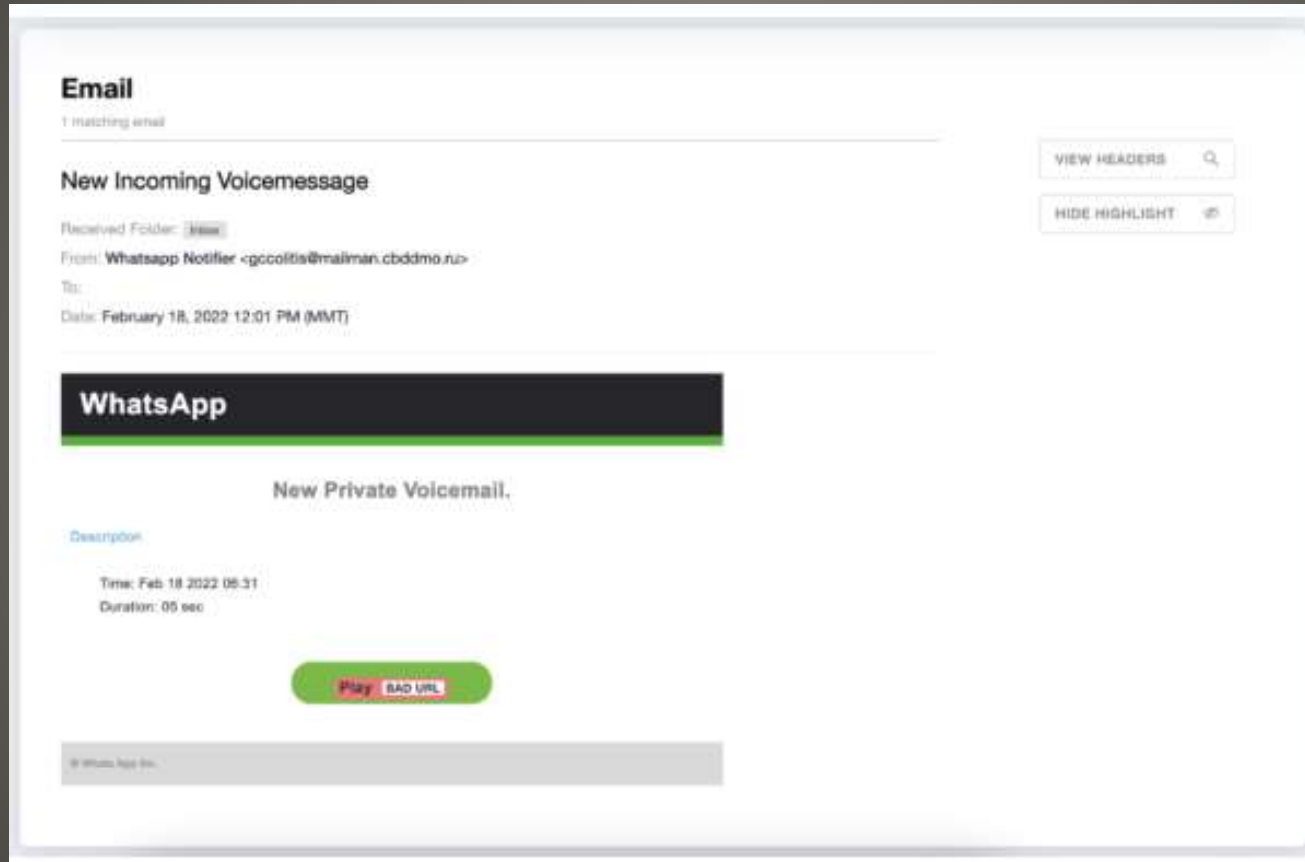
<https://www.usa.gov/stop-scams-frauds>

<https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages>

Think before the click

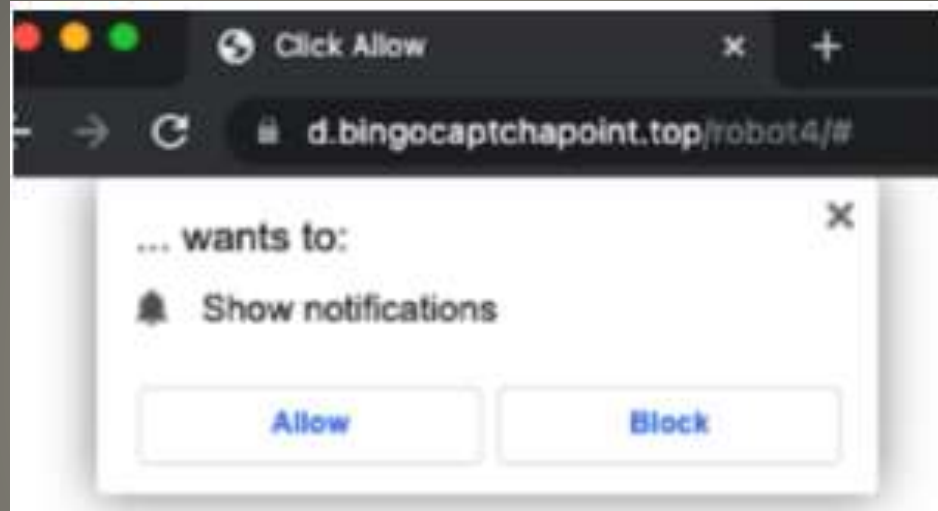
**We've seen this before - but**

- Fake WhatsApp “New Incoming Voicemail”



**Current Issues**

- Click the **Play**



**Current Issues**

- Receive notifications
- If So privileged position to redirect

The image displays two screenshots of a web proxy tool's interface, showing request headers and annotations for a redirect. The top screenshot shows a request to `GET /?u=3w8p605&o=pn1kfzq HTTP/1.1` with a `Referer: https://bingocaptchapoint.top/`. The bottom screenshot shows a request to `GET /kybgvmxg/?u=3w8p605&o=pn1kfzq&f=1&sid=t4~tylfrlynf31sucsx4wfynuv&fp=sn9HxAP5IXTFW4M%2Bk!` with a `Referer: https://best-prizes.life/`. Orange arrows and text annotations indicate a redirect from the first host to the second.

**Request 1:**

- Request Headers: `GET /?u=3w8p605&o=pn1kfzq HTTP/1.1`
- Client: `Domain added to Chrome's notifications`
- Miscellaneous: `Referer: https://bingocaptchapoint.top/`
- Security: `Connection: keep-alive`
- Transport: `Host: best-prizes.life`

**Request 2:**

- Request Headers: `GET /kybgvmxg/?u=3w8p605&o=pn1kfzq&f=1&sid=t4~tylfrlynf31sucsx4wfynuv&fp=sn9HxAP5IXTFW4M%2Bk!`
- Client: `Referer: https://best-prizes.life/`
- Security: `Connection: keep-alive`
- Transport: `Host: vshwde.saltpoorseed.xyz`

**Annotations:**

- `Redirect` (arrow pointing from `Host: best-prizes.life` to `Host: vshwde.saltpoorseed.xyz`)
- `Redirect to bogus offer page` (arrow pointing to `Host: vshwde.saltpoorseed.xyz`)

# Current Issues

Price

vshwde.saltpoorseed.xyz/kybgvmxg/7u=3w8p605&co=prn1kfzq&f=1&sid=t4--tylfrlynf31sucx4wfynuv...

## Chrome search contest 2022

### You've made the 5-billionth search.

Congratulations! You may be our next lucky winner!

Our last winner was Brad Jenkins from Los Angeles, who won a Samsung KU6179 Ultra HD TV on 14.05.2019 with his 5-billionth search.

Every time the 5-billionth search is reached, we proclaim a winner and reset the counter.

You may choose one of three hidden prizes below. In addition, you will be entered in our Hall of Fame and receive a winner's certificate.

Behind every box is a prize. Click on a box to uncover it.

For technical reasons, we are not allowed to keep your invitation open for more than 15 minutes.

Choose one of the prizes below and follow the instructions on your screen.

The malvertiser's fake "Chrome search contest"



- Keep Current

OS (windows, macOS, Linux, Chrome OS)

Apps WhatsApp, zoom, browsers,  
browser extensions, security suites,  
Windows Defender signatures, Gatekeeper  
signatures, etc.

- Remove Notification permissions

e.g. Chrome

Settings > Privacy & Security > Site Settings > Notifications

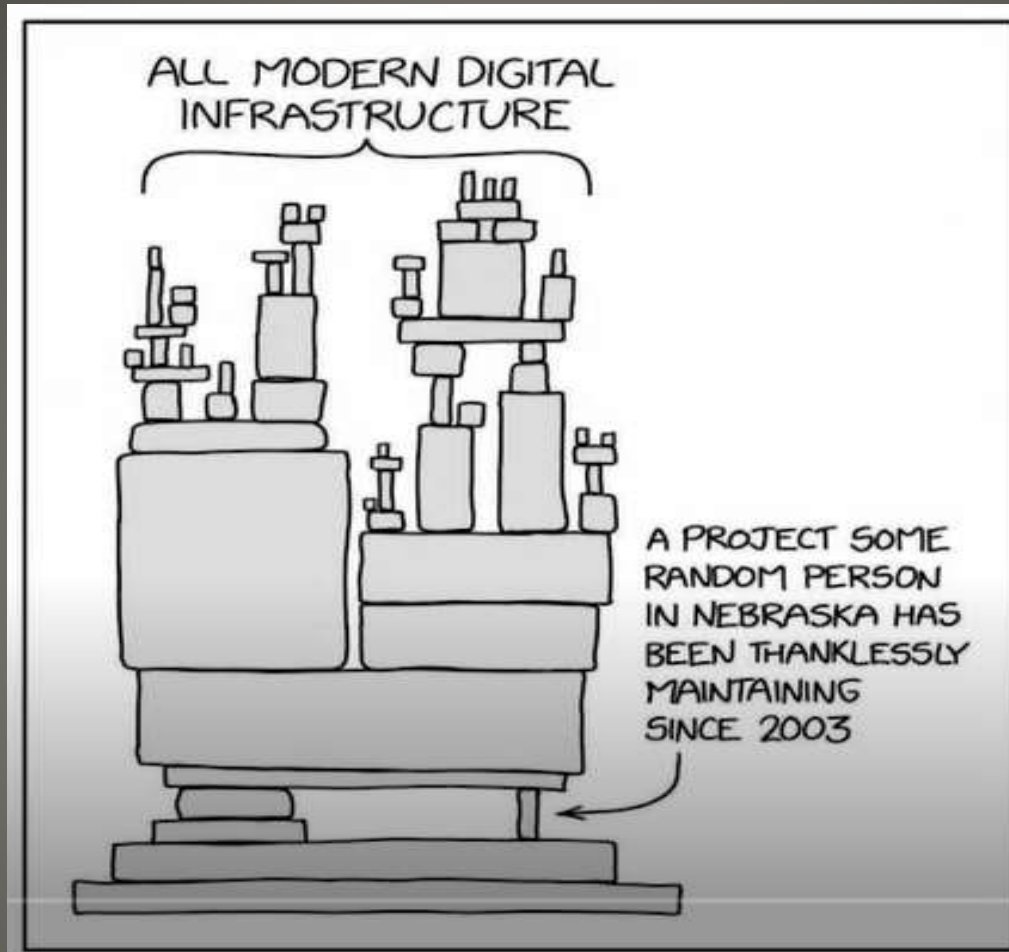


- US Administration seeking power to detect and destroy threatening drones
- Crypto theft increasing
  - Hardware wallets
  - Avoid crypto key capture methods
  - Thieves know
    - MFA hardware key and/or authenticator app
    - Monitor any exchanges
    - Separate email account for each exchange
    - Protonmail or similar
    - Double check wallet address (can be changed)
    - Use separate device for crypto usages

## Current Issues

- Android devices with Qualcomm or MediaTek audio decoder chips  
Remote code execution vulnerability  
Just play a song or audio clip
- Is that cash under my windshield wiper?
- VERY very serious Java vulnerability  
Elliptic Curve Digital Signature Algorithm  
Java 15 and newer  
Fake TLS certificates, MFA codes, auth credentials, and similar  
Fixed April 2022  
Doctor Who blank Identity card

## Current Issues



# Growing API cyber threats



# DuckDuckGoing



# Quacking



**Did you google it?**

- Cybersecurity and Infrastructure Security Agency
- Exploited Vulnerabilities catalog
- Must Patch immediately mandates
- Sad:

*Zimbra Collaboration Suite* Java based Linux

2005 LiquidSys name change Zimbra

Yahoo purchased then sold to VMWare

then sold to Telligent Systems

changed name Zimbra sold to Synacor

Ukraine CERT warns of exploit against their  
government agencies

2005 -> today

**CISA catalog**

- Corporate catalog of apps
- Change Board rigor
- Cost of Patch => cost of exploit
- Exploit chaining
- Island Hopping
- Small and cheaper things going to be updated?

**Must Patch**

- BIOS – POST, start and check fans, check firmware, spin up hard disks, verify boot sector, check memory, load boot sector, boot sector loads OS, check which OS to load, ...
- Toggle in boot code
- BIOS in ROM
- Not Smart BUT Not modifiable
- Now smart & modifiable
- Lenovo UEFI “mistake”
- Malware in the firmware
- Re-install replace disk etc. Malware in firmware survives
- Fail to remove development drivers in released UEFI
- *SecureBackDoor* and *SecureBackDoorPeim*

## Lenovo UEFI



- Check ALL vendors firmware
- “What, me worry?”
- Probably safe
- BUT
- Is your bank safe?
- Your online credit card merchant?

**UEFI BIOS Disk Firmware**

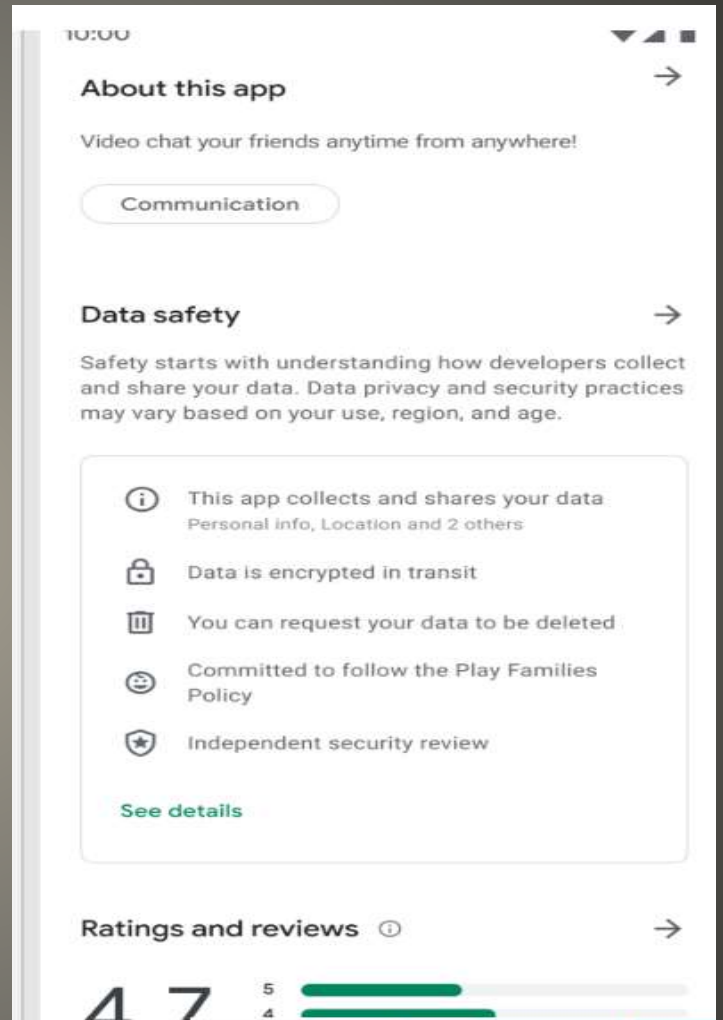
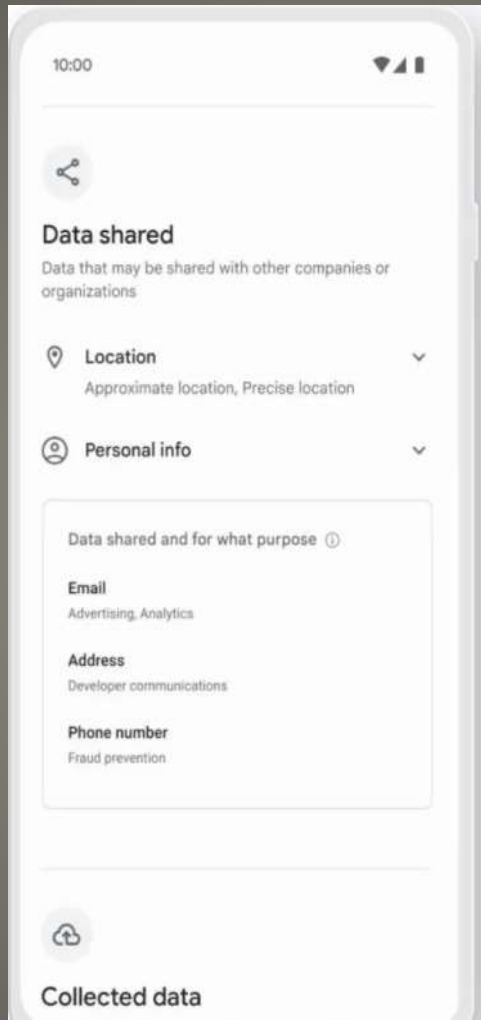
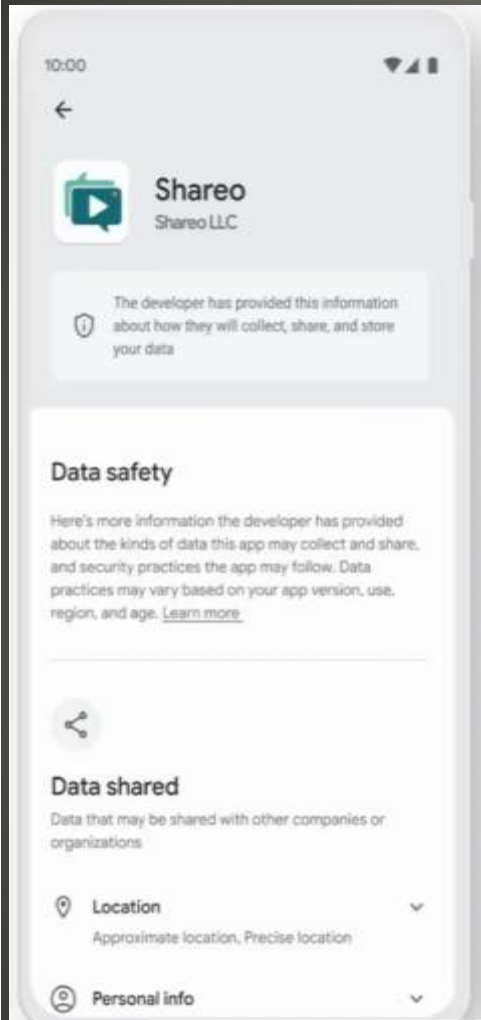


- Everscale blockchain wallet WEB version withdrawn
- SmartPhone Radiation  
Specific Absorption Rate (SAR)  
Watts/Kg  
Lower "safe" rate 2 watts/Kg  
2020 Motorola Edge 1.79 watts/Kg  
Google Pixel 6, iPhone 13 Pro, iPhone 12  
1.00 watts/Kg  
Goggle Pixel 5A .47 watts/Kg
- DoD DIB-VDP year long pilot

## Current Issues

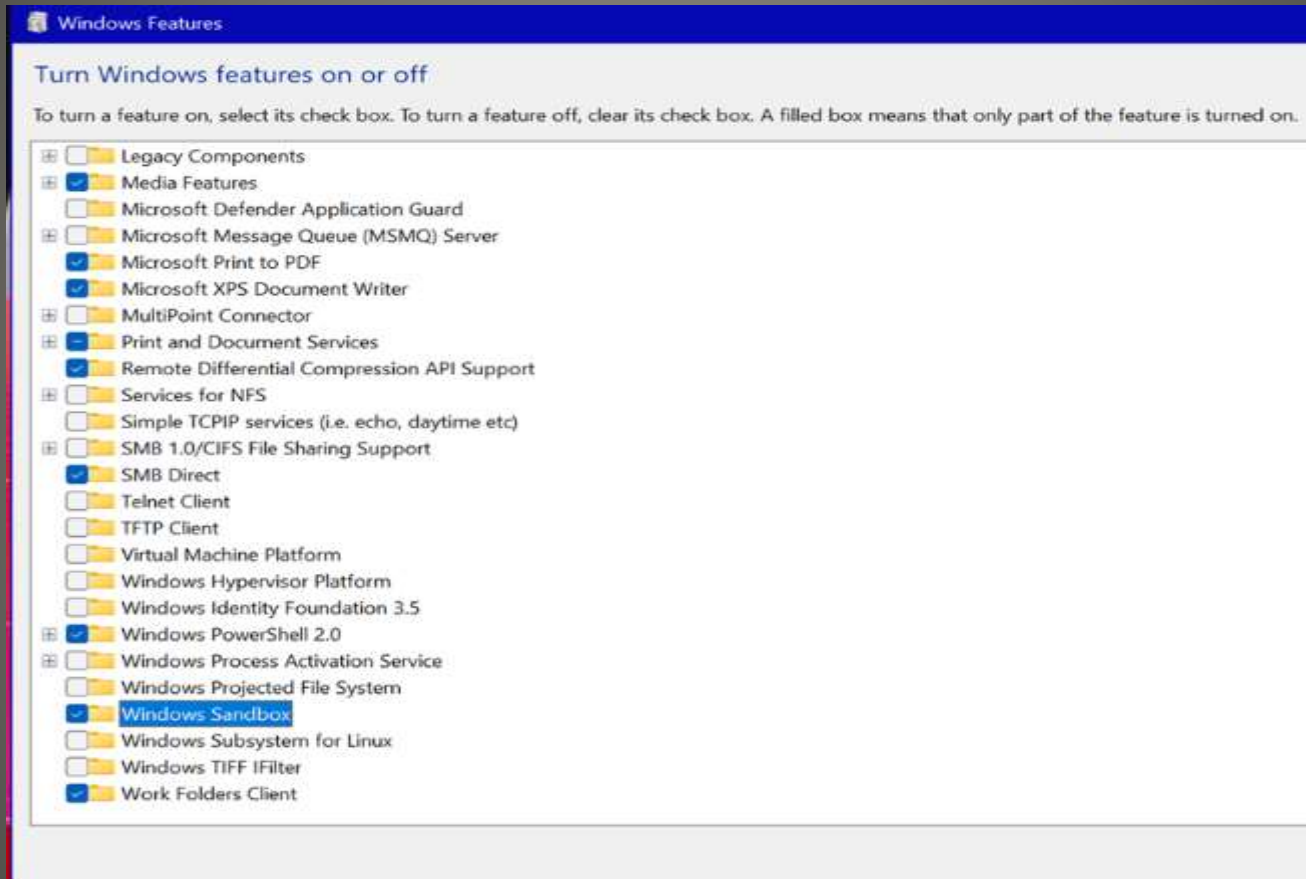
- Connecticut privacy law  
Awaiting governor's signature  
Joins similar laws: California, Colorado,  
Virginia, Utah  
July 2023

**Current Issues**



# Google Play Store "Data Safety"

- Windows Sandbox enabled



## 3 Data Protection Privacy settings

- BitLocker

### BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

#### Operating system drive

Windows (C:) BitLocker off



 Turn on BitLocker

#### Fixed data drives

Small Games (D:) BitLocker off

Small HDD (F:) BitLocker off

#### Removable data drives - BitLocker To Go

Document Back Up (H:) BitLocker off

# 3 Data Protection Privacy settings

- Ransomware Protection

### Ransomware protection

Protect your files against threats like ransomware, and see how to restore files in case of an attack.

#### Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.



#### Ransomware data recovery

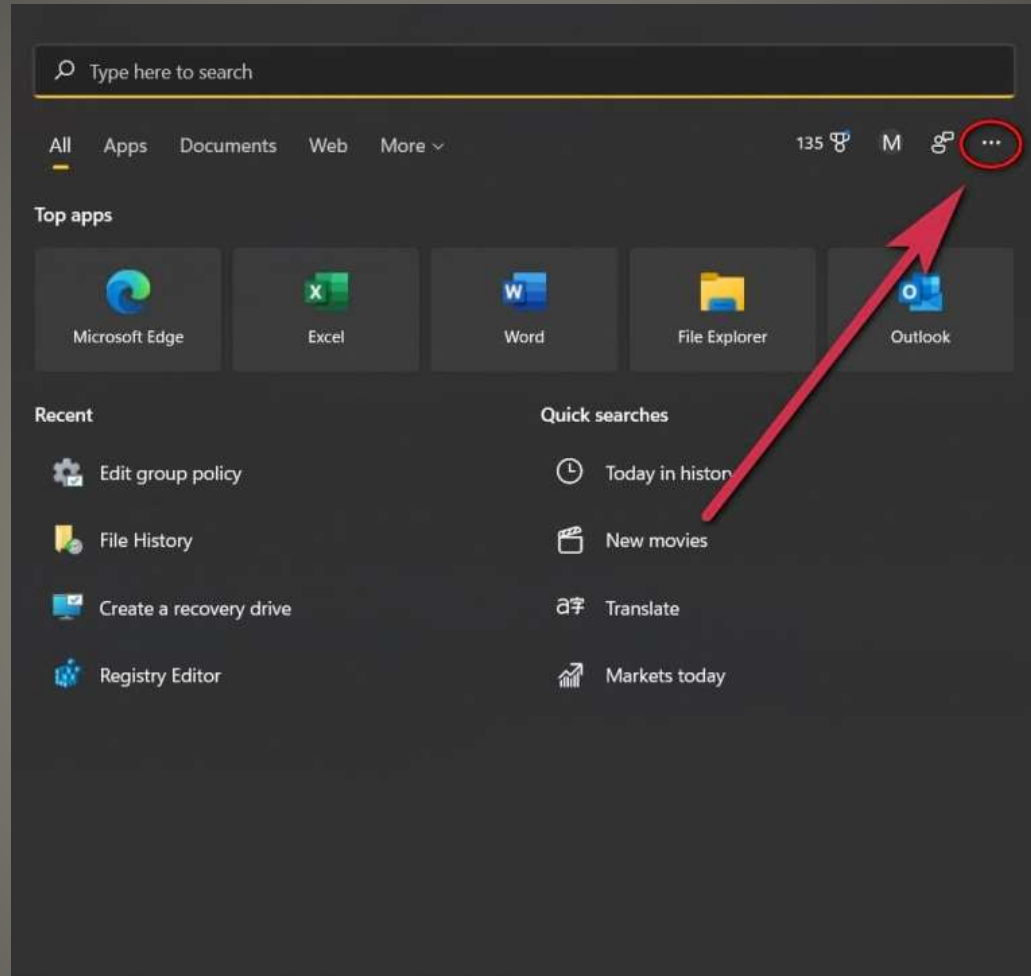
You may be able to recover files in these accounts in case of a ransomware attack.

Set up OneDrive for file recovery options in case of a ransomware attack.

[Set up OneDrive](#)

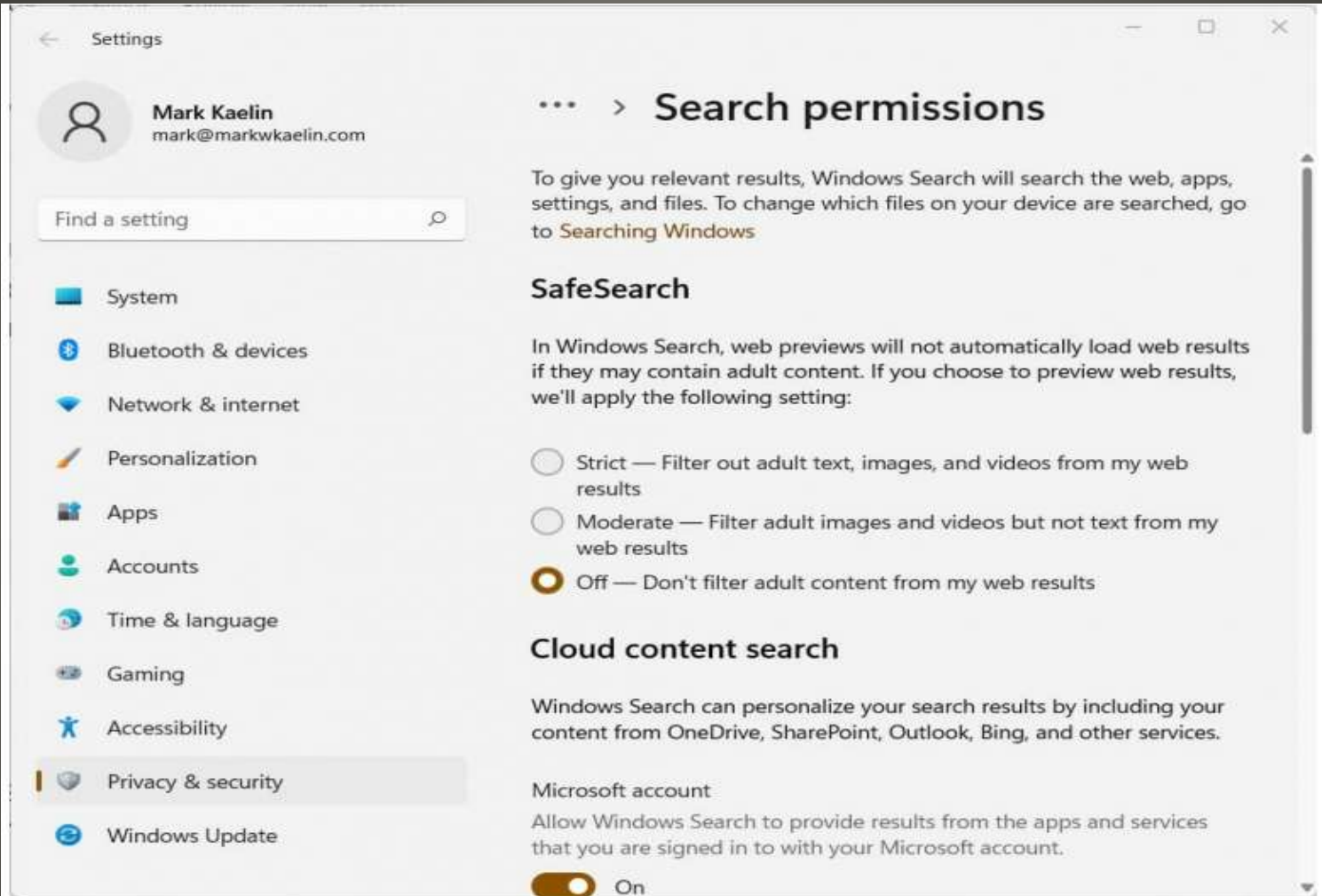
## 3 Data Protection Privacy settings

- MFA
- Passphrase strong & Unique
- Avoid phishing, smishing, fake websites
- Keep security suites signatures up-to-date
- antispyware app and/or browser extensions
- Secure home networks
- Use data encryption
- Limit Bluetooth, wi-fi
- Avoid open Wi-Fi
- Disable autocomplete
- Clear browser history
- Keep systems up-to-date
- 3-2-1 backup
- Shutdown
- Virtualization
- Control PII
- Control IT discards

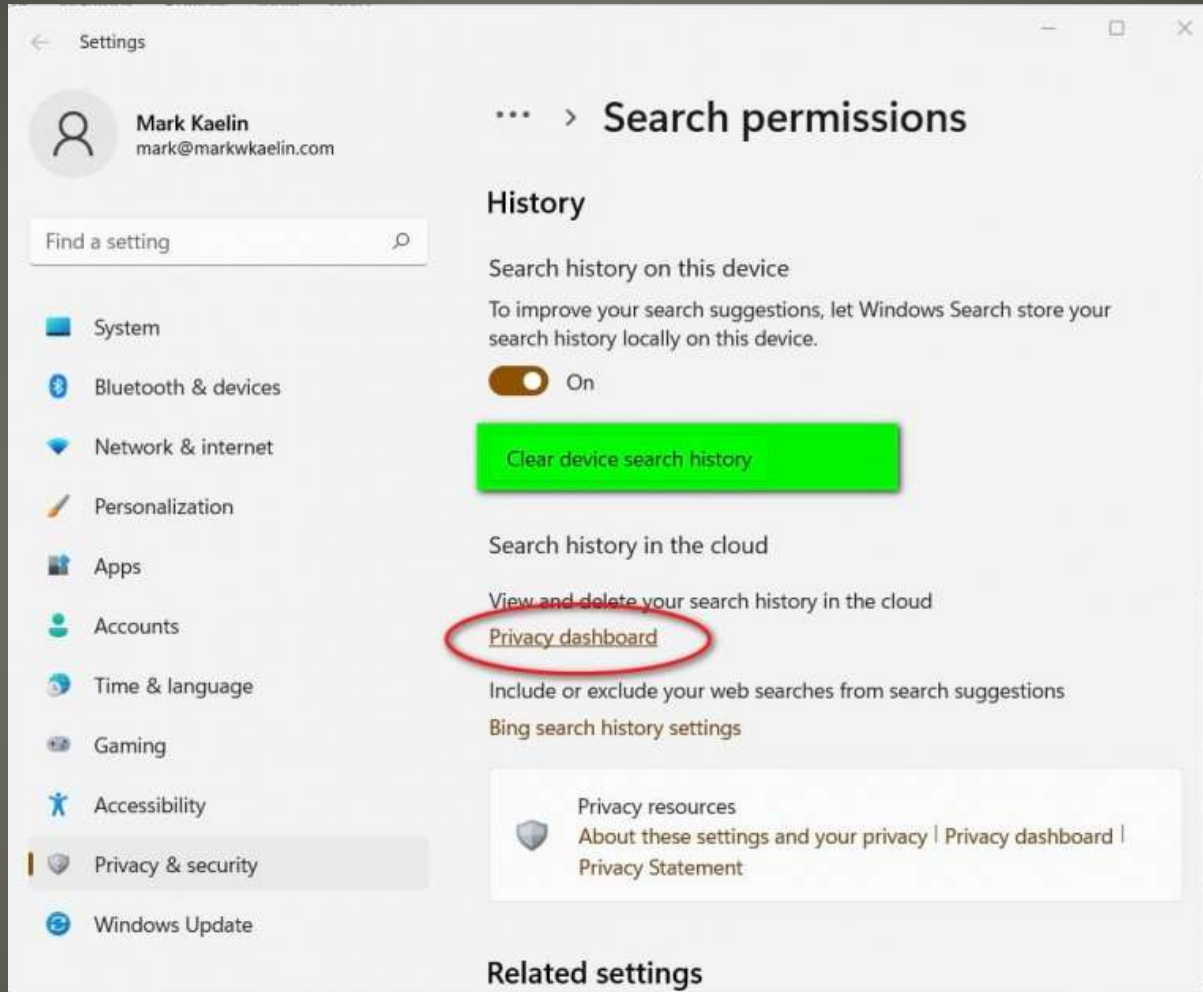


# Privacy Dashboard Windows





# Privacy Dashboard Windows



**Privacy Dashboard Windows**

# Stay in control of your privacy

Sign in to manage your data.

[SIGN IN WITH MICROSOFT >](#)



## Privacy settings

- Manage browse data**  
Sign in to view and clear browse data that we collect when you use Cortana and Microsoft Edge.
- Review location data**  
See and clear location info that we collect when you use Microsoft products and services.

- Clear your search history**  
View and delete information about your Bing search activity.
- Edit Cortana's Notebook**  
Manage what Cortana knows about you to provide personalized recommendations.

## Other privacy settings

- Windows**  
Change any of your privacy settings on your Windows 10 device by going to Start > Settings > Privacy. [Privacy settings in Windows 10](#)
- Xbox**  
Adjust your Xbox privacy settings on either your console or by signing in to Xbox.com. [Xbox privacy and online safety](#)
- Microsoft Teams**  
Export chat history, media files, and contacts from your personal Microsoft Teams account. Only data stored when using your personal account will be exported. [Export my personal Teams data](#)
- Microsoft News Community**  
To adjust your privacy settings, sign in to Microsoft News Community. [Manage community privacy](#)
- Marketing preferences**  
Sign in to manage promotional communications associated with your Microsoft account. If you don't have a Microsoft account, you can [request a link to manage promotional communications by email](#).
- Contact our privacy team**  
If you're not able to find what you're looking for, or you have a privacy question or concern—[contact our privacy team](#).

- Apps and services**  
Manage apps and services that are allowed to access your data. [Apps and services that can access your data](#)
- Office**  
View your privacy settings in any Office product by going to File > Options > Trust Center. [Settings in Trust Center](#)
- Skype**  
Edit who can see your profile in Skype and other privacy settings by signing in to your account at Skype.com. [Skype settings](#)
- Ad preferences**  
Choose whether you would like to see interest-based advertising. [Ad settings](#)
- Other Microsoft products**  
Learn how to view and manage your data in some of our other products and services. [Privacy info for Microsoft products](#)

## Privacy at Microsoft

[Learn about our commitment to your privacy >](#)

- Beanstalk Farms
  - decentralized finance project
  - majority stake system
  - proportional votes based on digital currency owned
  - hacker used flash loan from another decentralized finance project
  - to gain controlling stake
  - to approve \$182 million to his wallet



- Fraud Prevention

“Cards with enhanced fraud prevention now use information about your account, device and location to share fraud assessments with your payment network.”

Currently some Visa cards

\*Currently no way to opt out

Current Location ??

**Apple Wallet new feature**

- Some VPNs have features regulators do not like
- Torrenting
- Copyright infringement
- Pirating
- No Log
- Thwarting Law Enforcement
- Result: Block BitTorrent and enabling logs

## **VPNs and Hollywood**

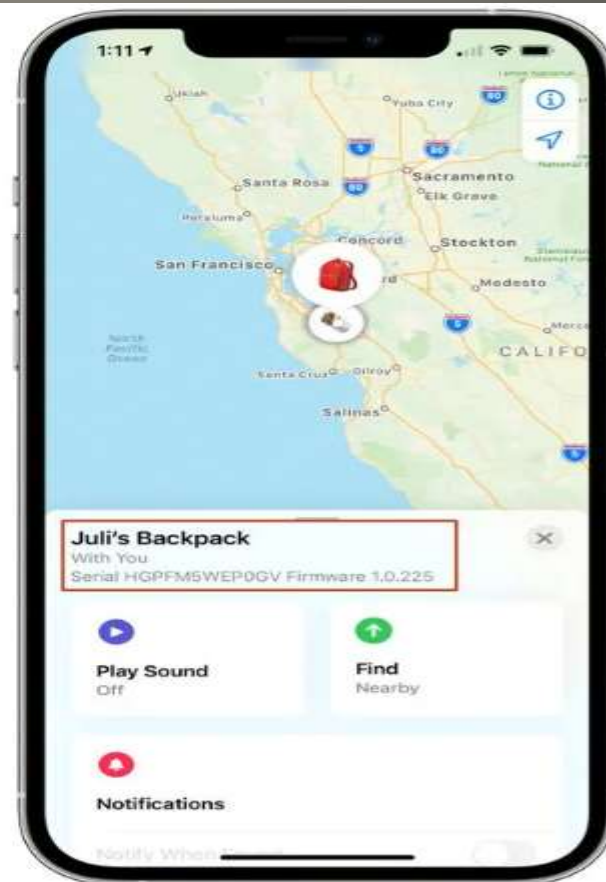
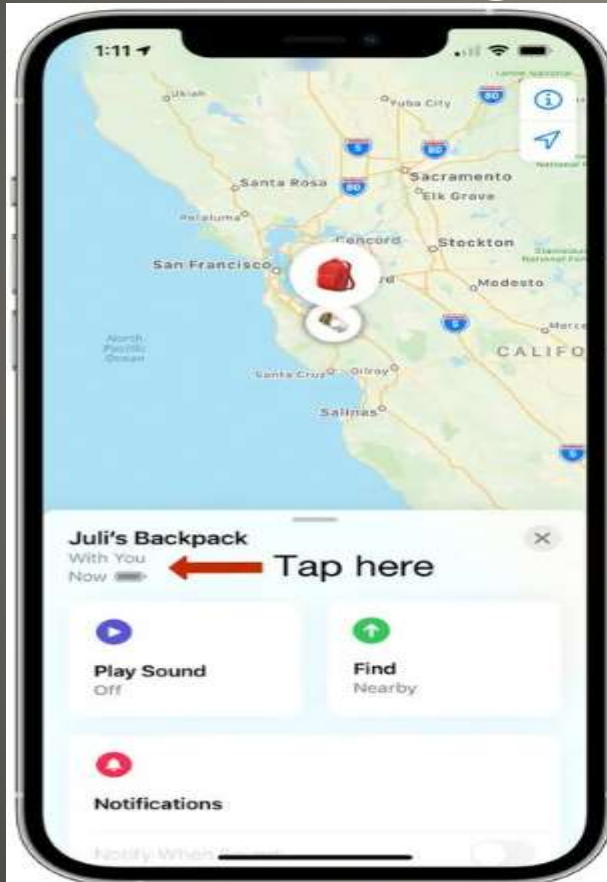
- Firmware updates
- 1.0.
- 225 -> 1.0.291 -> 1.0.301



**Apple AirTags**



- Find My -> Items
- Select an AirTag





CVE	Vulnerability Name	Vendor and Product	Type
<a href="#">CVE-2021-44228</a>	Log4Shell	Apache Log4j	Remote code execution (RCE)
<a href="#">CVE-2021-40539</a>		Zoho ManageEngine AD SelfService Plus	RCE
<a href="#">CVE-2021-34523</a>	ProxyShell	Microsoft Exchange Server	Elevation of privilege
<a href="#">CVE-2021-34473</a>	ProxyShell	Microsoft Exchange Server	RCE
<a href="#">CVE-2021-31207</a>	ProxyShell	Microsoft Exchange Server	Security feature bypass
<a href="#">CVE-2021-27065</a>	ProxyLogon	Microsoft Exchange Server	RCE
<a href="#">CVE-2021-26858</a>	ProxyLogon	Microsoft Exchange Server	RCE
<a href="#">CVE-2021-26857</a>	ProxyLogon	Microsoft Exchange Server	RCE
<a href="#">CVE-2021-26855</a>	ProxyLogon	Microsoft Exchange Server	RCE
<a href="#">CVE-2021-26084</a>		Atlassian Confluence Server and Data Center	Arbitrary code execution
<a href="#">CVE-2021-21972</a>		VMware vSphere Client	RCE
<a href="#">CVE-2020-1472</a>	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
<a href="#">CVE-2020-0688</a>		Microsoft Exchange Server	RCE
<a href="#">CVE-2019-11510</a>		Pulse Secure Pulse Connect Secure	Arbitrary file reading
<a href="#">CVE-2018-13379</a>		Fortinet FortiOS and FortiProxy	Path traversal

## 5 Eyes Top 15 Exploited Vulnerabilities

- Microsoft Exchange
- Two weeks exposure > Exploit  
Monthly patching not fast enough
- Perhaps that is their point
- If so, ...

**Top Exploited**

- Microsoft report Russian Cyber Warfare  
250 operations by 6 separate groups

[Hybrid War in Ukraine](#)

[Ukraine An overview of Russia's cyberattack activity in Ukraine](#)

[Microsoft details rampant cyber warfare corresponding to Russian invasion](#)

[Russia has launched hundreds of cyberattacks against Ukraine](#)

[Russia wages "relentless and destructive" cyberattacks to bolster Ukraine invasion](#)


**Current Issues**


- Cloudflare block huge DDoS attack  
15.3 million requests/second  
HTTPS requests  
Source Cloud computers not botnets
- French Fiber Optic cable attack  
Criminal
- Research of higher speed copper wiring
- Using pupil reflection in smartphone selfies
- Russia using tech savvy prisoners


## Current Issues

- “Built-in” Cloudflare powered VPN
- Canary Edge
- 1GB each month
- Microsoft Account login
- PII purged every 25 hours


**Microsoft Edge Secure Network**


 Print Ctrl+P

 Web capture Ctrl+Shift+S


 Share

 Find on page Ctrl+F

 Read aloud Ctrl+Shift+U

 Secure Network

More tools >

 Settings Ctrl + X

 Help and feedback >

- 60 Minutes FBI Director Interview  
China Threat “Unprecedented”  
Spying, espionage, ...  
Corporate board  
Culture smaller private government divide
- Selfie drone

**Current Issues**



- Annual Transparency Report

Office of the Director of National Intelligence

FBI

"searched emails, texts and other electronic communications of as many as 3.4 million U.S. residents without a warrant" between the period of December 2020 and November 2021.

**Current Issues**

- Freedom of Information and Privacy Acts  
Dear FBI *who am I?* 1967 law 1974 law  
Method 1 FBI FOIA online portal

<https://efoia.fbi.gov/#home>

## FBI: eFOIPA

### FBI Records: Freedom of Information/Privacy Acts (FOIPA)

**Due to the COVID-19 pandemic, the FBI has adjusted its normal operations and is unable to timely process Freedom of Information/Privacy Act (FOIPA) requests received via the eFOIPA portal or by standard mail. Given limited staffing to ensure safety, you can expect delays in both the acknowledgement and substantive response to your FOIPA request. We apologize for this inconvenience and appreciate your understanding during this national emergency.**

Welcome to the FBI's new eFOIPA submission portal. This system is designed to allow requesters to submit and receive responses to Freedom of Information Act and Privacy Act (FOIPA) requests electronically. The eFOIPA portal's normal operating hours are 24 hours a day seven days a week. To submit an eFOIPA request to the FBI, select the "Electronic FOIPA (eFOIPA)" option below. To make a standard FOIPA request, select the "Paper FOIPA" option below. Please note that if you opt to make a standard FOIPA request, all correspondence that you will receive from the FBI will occur through standard mail. The FBI would like to thank you in advance for your cooperation and looks forward to receiving and responding to your request. If you have any additional questions or experience any issues while using the eFOIPA system, please e-mail [FOIPAQuestions@fbi.gov](mailto:FOIPAQuestions@fbi.gov) for assistance. To report a matter concerning national security or another federal crime, submit a tip at [tips.fbi.gov](https://tips.fbi.gov).

Please select one of the following:

Paper FOIPA 

Electronic FOIPA (eFOIPA) 

- Or Sample Letter
- <https://www.fbi.gov/services/information-management/foipa/sample-fbi-foia-request-letter>
- How much will you pay?
- Depends
- Use FOIPA request number to check status
- Perhaps file appeal  
Director of the Office of Information Policy

**FOIA**



**5 MB then 62,500 cards 4-day load**

- **Do Not Track** did not track
  - Global Privacy Control
  - <https://globalprivacycontrol.org/>
- Microsoft Edge Canary

● GPC signal detected.

Test against the reference server.

**GLOBALPRIVACYCONTROL**

ABOUT

SPEC

DOWNLOAD

ORGANIZATIONS

GET INVOLVED

PRESS

FAQ

## Take control of your privacy.

Online privacy should be accessible to everyone. It starts with a simpler way to exercise your rights.

GET STARTED

GET INVOLVED

# Global Privacy Control

● GPC signal detected.

Test against the reference server.

**Global Privacy Control**



# Interacting with Global Privacy Control

## Server-side detection

A user agent's Global Privacy Control setting is attached to HTTP requests as the `Sec-GPC` request header. This header's value will be `"1"` if enabled, and not present otherwise. Interacting with this will vary depending on the application back-end. Example code is Nodejs/Express.

Header present 🍷

```
Sec-GPC: "1"
```

```
1 app.get("/", function(req, res) {
2   const gpcValue = req.header('Sec-GPC')
3   if (gpcValue === "1") {
4     // signal detected, do something
5   }
6 })
```

## Client-side detection

The `navigator.globalPrivacyControl` property enables client-side script to determine a user agent's Global Privacy Control setting. This value mirrors the value sent in the `Sec-GPC` header; it will equal `true` if the `Sec-GPC` header sent is equal to `"1"`, and `false` otherwise.

DOM signal present 🍷

```
navigator.globalPrivacyControl: true
```

```
1 const gpcValue = navigator.globalPrivacyControl
2 if (gpcValue) {
3   // signal detected, do something
4 }
```

## .well-known

Businesses may host a `.well-known/gpc.json` resource that indicates to clients how they respond to a Global Privacy Control signal. This is a JSON file hosted at the `.well-known/gpc.json` endpoint.

`.well-known/gpc.json` present 🍷

```
{
  "gpc": true,
  "version": 1
}
```

# Global Privacy Control



● GPC signal not detected.

Please download a browser or extension that supports it.

**Browsers yet to support**

- HTTP signal through the DOM
- Person's request to not share PII with 3<sup>rd</sup> parties
- Intended to work with legal frameworks to make the request enforceable
- DoNotTrack
- Widening disconnect business and their site
- "We accept your cookies" or no go

## Global Privacy Control



Firefox about:config



privacy.global

Show only modified preferences

privacy.globalprivacycontrol.enabled

true



privacy.globalprivacycontrol.functionality.enabled

true



privacy.global

Boolean  Number  String










privacy.globalprivacycontrol.was\_ever\_enabled

true



# Firefox

	Abine	<a href="#">LEARN MORE</a>
	Brave Privacy Browser	<a href="#">LEARN MORE</a>
	Disconnect	<a href="#">LEARN MORE</a>
	DuckDuckGo Privacy Browser	<a href="#">LEARN MORE</a>
	Firefox	<a href="#">LEARN MORE</a>
	OptMeowt by privacy-tech-lab	<a href="#">LEARN MORE</a>
	Privacy Badger by EFF	<a href="#">LEARN MORE</a>

# Global Privacy Control

- California
- Soon Colorado
  
- Yeahbut
  
  
- Optmeowt

**Global Privacy Control**



# Settings

Adjust extension settings

Settings

Domain List

About



## Enable

Sends 'Do Not Sell' signals to every visited domain



## Domain List

Sends 'Do Not Sell' signals according to the custom Domain List



## Disable

Does not send any 'Do Not Sell' signals

### Domain List Export & Import

Export Domain List

Import from File

# Optmeowt

- 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](mailto:SCCCCyber@gmail.com)**

