

Sun City Computer Club

Cyber Security SIG

July 7, 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??

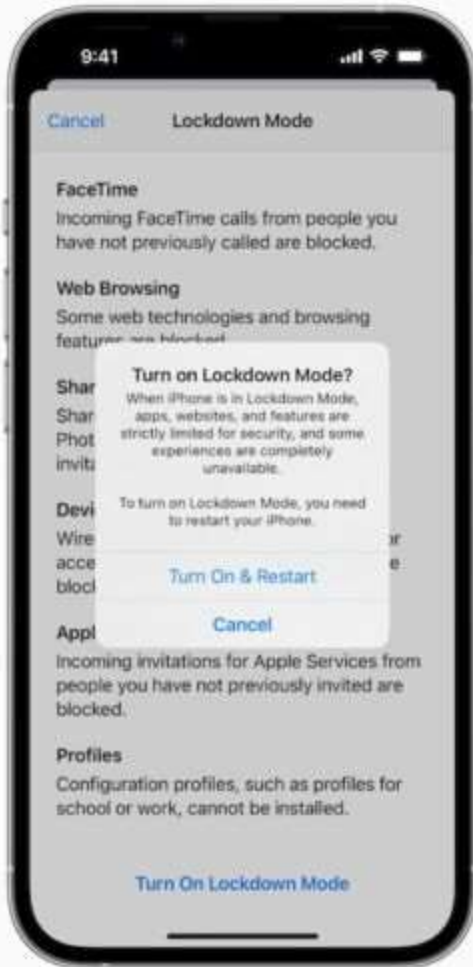
Presenter???

- BROWSER Updates
- Chrome OS 103.0.5060.114
- Marriott Data Breach
- MI5 & FBI heads warn of growing threat
*China biggest long-term threat
Bigger than that of every other major
country combined*
*Taiwan horrific business disruptions the
world has ever seen*
- Apple new Lockdown Mode
Messaging, WEB browsing, Devices, Profiles
- NIST announces first 4 quantum resistant
algorithms

Breaking News

- Chrome 103.0.5060.114
- Edge 103.0.1264.49
- Firefox 102.0.1
- Opera 89.0.4447.38
- Tor 11.0.14
- Brave 1.40.1.113
- Vivaldi 5.3.2679.68
- Safari 15.6 (17613.3.9.1.3)

Browser versions as of this date





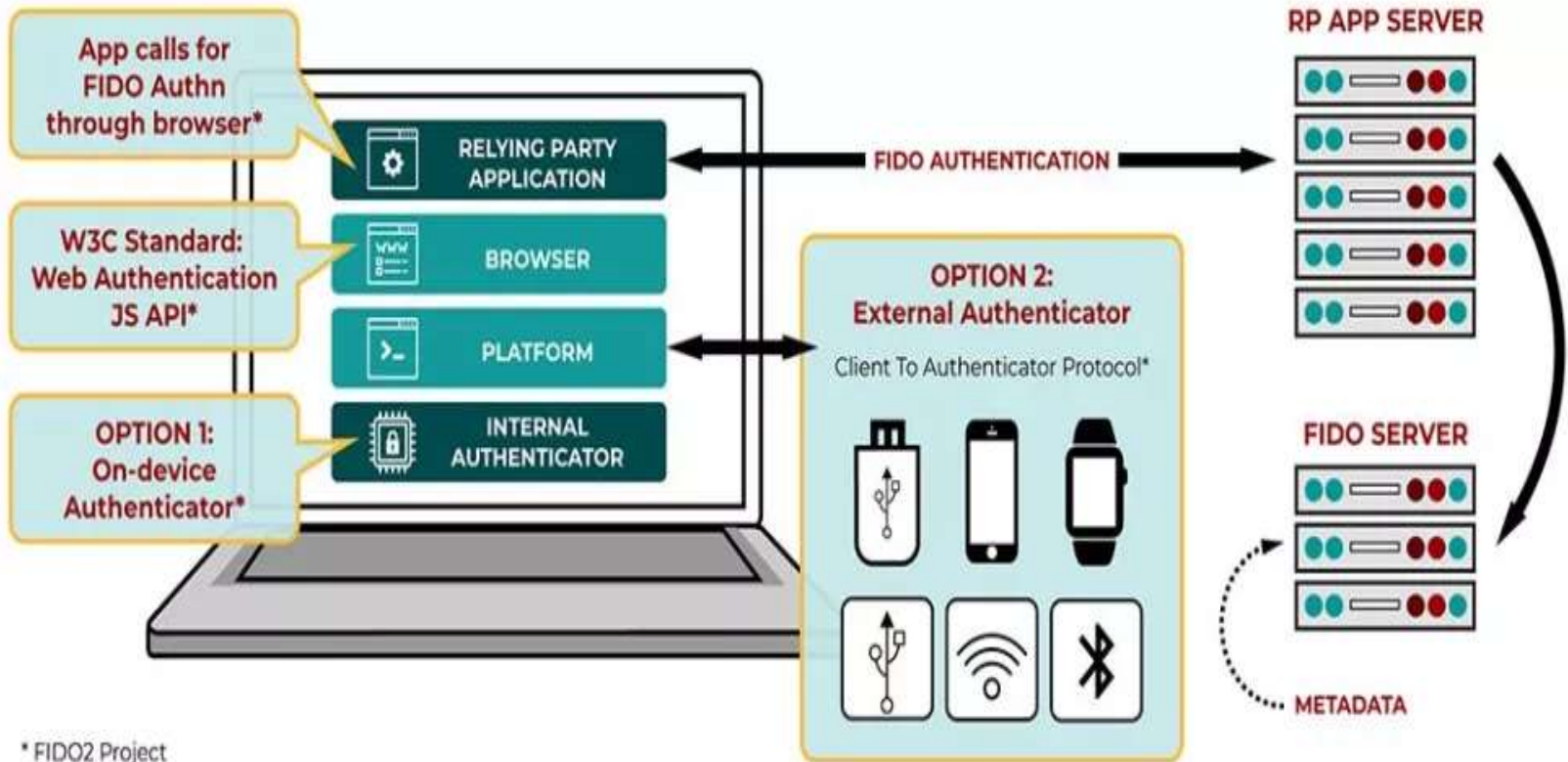
故 Internet Explorer

1995. 8. 17 ~ 2022. 6. 15

He was a good tool to
download other browsers.

- Lock users into vendor's ecosystems
- Client side easy & controlled
- Server side
- How to synch passkeys separate vendors
- If users can synch passkeys
Can attackers?

Passkeys



* FIDO2 Project

WE ARE TEMPORARILY CLOSED
AND WILL REOPEN ON MONDAY
6/20 FOR OUR NORMAL BUSINESS
HOURS OF 10AM-7PM. OUR MGT
TEAM WAS CAUGHT IN A SCAM
THAT DEFRAUDED US OF SIGNIFICANT
FINANCIAL RESOURCES. WE ARE
HEART-BROKEN AND EMBARRASSED
THAT THIS NEWS IS LAID BARE TO
OUR CUSTOMERS, BUT WANTED YOU TO
KNOW THAT WE DON'T TAKE OUR
INABILITY TO SERVE YOU LIGHTLY.
THX FOR YOUR UNDERSTANDING.
-STEVE SALADIN

SUMMER
CHICKEN
\$5
CREAMY CHEESE
TOMATO
IT

- “Want your receipt?”
Cash sales
Cancel transaction, give food & change
Pocket the rest
Report suspected fraud to IRS
- Tracking devices via Bluetooth signatures
Slight variations in signal
Data is encrypted
- Firefox Total Cookie Protection
Now on by default
But is it working?

Current Issues

- CloudFlare stopped and mitigated large attack
- CloudFlare down 19-June-2022
- Thieves steal Rolls Royce
 - Then this happens
- Mega unbreakable encryption
 - Anything BUT
 - Ok, we'll fix that/those
- Venmo & Zelle money transfer is money transfer
- Windows shortcut files making come back
- Milan based RCS Lab spyware
- Unsend iMessage issue
- Apple watch Movement Disorder API

Current Issues

- Apple to use “Binned-Down” M2 M3
- Fake voice mail notifications
Microsoft credentials

Current Issues

- Swimming Kickboard detection
SWOLF score
- Running stride, length, ground contact time, vertical oscillation
- Against yourself
- Multisport workout
- Medications
Add your own Reminders interaction
- Sleep metrics
- Heart Rate Zones
- AFib history

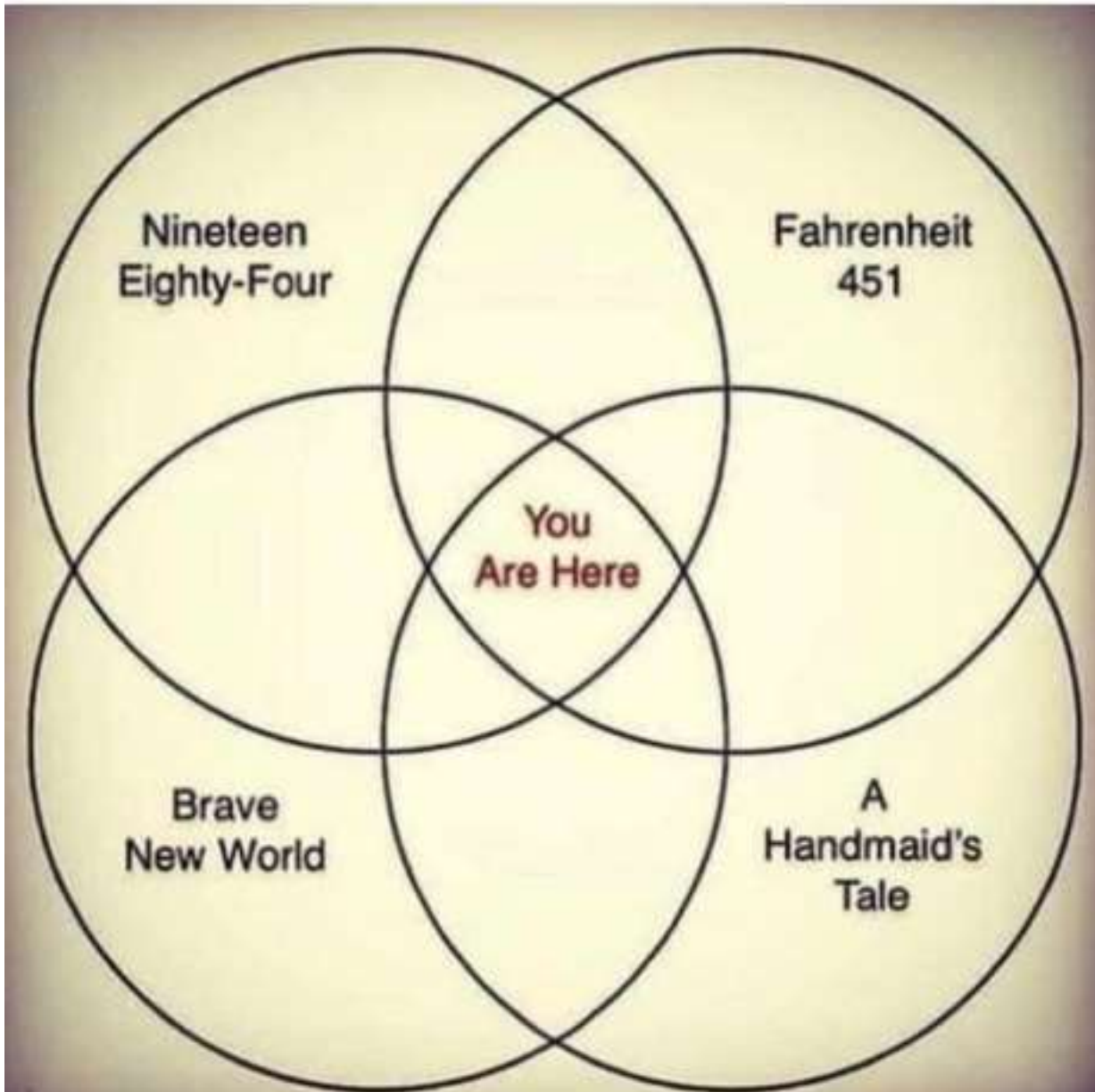
Apple Watch watchOS 9

"Grocery" would like to paste
from "Notes"


Don't Allow Paste

Allow Paste



iOS 16



- Settings > Privacy & security
App permissions

Let desktop apps access your microphone On 

Desktop apps that have previously accessed your microphone are listed here

-  Microsoft PowerPoint
Last accessed 6/22/2022 | 3:38:25 PM
-  Zoom
Last accessed 6/22/2022 | 3:38:37 PM

**Windows What is accessing
Microphone Camera Location**

The screenshot shows the Windows Settings application with the 'Privacy & security' > 'Location' page open. The left sidebar lists various settings categories, with 'Privacy & security' selected. The main content area shows the 'Allow location override' toggle is turned on. Below this, the 'Recent activity' section displays a list of applications that have accessed the device's location in the last week. The list includes 'Windows Web Experience Pack' and several instances of 'Microsoft Teams'. At the bottom, there are links for 'Privacy resources' and 'Get help'.

Settings

Privacy & security > Location

Find a setting

- System
- Bluetooth & devices
- Network & internet
- Personalization
- Apps
- Accounts
- Time & language
- Gaming
- Accessibility
- Privacy & security
- Windows Update

Allow location override
Allow apps like Remote Desktop to set this device's location. On

Recent activity
See which apps have accessed your location in the last week. 15 requests

App	Last accessed
Windows Web Experience Pack	6/13/2022 5:31:22 AM
C:\Users\divya\AppData\Local\Microsoft\Edge\SxS\Application\msedge.exe	5/31/2022 3:54:50 PM
Microsoft Teams	5/31/2022 3:53:30 PM
Microsoft Teams	5/31/2022 3:29:24 PM
Microsoft Teams	5/31/2022 3:29:16 PM
Microsoft Teams	5/31/2022 3:24:20 PM
Microsoft Teams	5/31/2022 3:24:13 PM
Microsoft Teams	5/31/2022 3:00:29 PM
Microsoft Teams	5/31/2022 3:00:22 PM
Microsoft Teams	5/31/2022 3:00:10 PM

View more activity

Privacy resources
About these settings and your privacy | Privacy dashboard | Privacy Statement

Get help

Location

Extension Fingerprints

Star 83

Chrome extensions can be detected by fetching their web accessible resources. These are files inside an extension that can be accessed by web pages. The detected extensions can be used to track you through browser fingerprinting. This scan only detects extensions from the Chrome Web Store. [Read more](#)

0.006% of users share the same extensions

Hash: 9bb45cd8d19fb696d66b5157fdbb7f34

Extension	Detected
Google Docs Offline	True
ColorZilla	True
User-Agent Switcher for Chrome	True
Phantom	True
Buffer	True

Generating an Extensions Fingerprint

Source: BleepingComputer

Browser Extensions fingerprint

- Gmail, Outlook, iCloud email addresses
“+”
subscribe myemail@gmail+NYT

Mail tracking



Brave Search

- *Goggles* feature

User defined set of rules applied to search results

Brave Search



sun city texas



All

Images

News

Videos

Goggles^{BETA}

Info Feedback

United States Safe search: Moderate Any time



1. Sun City Texas 5.54 miles
4.5 ●●●●● TripAdvisor (178)
Georgetown, TX



2. Sun City Texas 6.43 miles
newhomesource.com
701 Silver Spur Blvd, 78633, Georgetown



Brave Search Goggles

sun city texas



All

Images

News

Videos

Goggles^{BETA}

Info Feedback

United States

Safe search: Moderate

Discover

Tech blogs

Goggles 101 (brave)

Rerank results to boost content on tech blogs. List of tech blogs drawn from several sources (blogsurf.io, refined.blog, et al), and not vetted or endorsed by Brave.

Public

About this Goggle

Hacker News / 1k short

Goggles 101 (brave)

Prioritizes domains popular with the Hacker News community, minus those that would rank among the top 1000 most-viewed websites.

Public

About this Goggle

No Pinterest

Goggles 101 (brave)

Rerank results to remove pages / threads hosted on Pinterest.

Public

About this Goggle

Left sources

AllSides.com (allsides-news)

Rank results to boost content from left-leaning news sources.

Public

About this Goggle

Show more →

Goggles is in beta. [Learn more.](#)

 Feedback

Tech blogs

Goggles 101 (brave)

Rerank results to boost content on tech blogs. List of tech blogs drawn from several sources (blogsurf.io, refined.blog, et al), and not vetted or endorsed by Brave.

Public

About this Goggle +

Hacker News / 1k short

Goggles 101 (brave)

Prioritizes domains popular with the Hacker News community, minus those that would rank among the top 1000 most-viewed websites.

Public

About this Goggle +

No Pinterest

Goggles 101 (brave)

Rerank results to remove pages / threads hosted on Pinterest.

Public

About this Goggle +

Left sources

AllSides.com (allsides-news)

Rank results to boost content from left-leaning news sources.

Public

About this Goggle +

Right sources

AllSides.com (allsides-news)

Rank results to boost content from right-leaning news sources.

Public

About this Goggle +

Rust programming

Goggles 101 (brave)

Rerank results to boost content related to the Rust programming language.

Public

About this Goggle +

Copycats removal

Goggles 101 (brave)

Rerank results to remove "copycat" content (e.g. StackOverflow threads or GitHub translations).

Public

About this Goggle +

1k short

Goggles 101 (brave)

Rerank results to remove pages found on the top 1,000 most-viewed websites. List of top sites drawn from tranco-list.eu. Up-ranked sites not vetted or endorsed by Brave.

Strict

Stronger protection, but may cause some sites or content to break.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows (includes tracking cookies)
- Tracking content in all windows
- Cryptominers
- Fingerprinters

Heads up!

This setting may cause some websites to not display content or work correctly. If a site seems broken, you may want to turn off tracking protection for that site to load all content. [Learn how](#)

Firefox Query Parameter Stripping

- https://www.engadget.com/example.html?fbclid=aa7-V4yb6Yfit_9_Pd

- Facebook and others
- Changes with user's interaction
- Other sites use the same technique

Olytics: oly_enc_id=, oly_anon_id=

Drip: __s=

Vero: vero_id=

HubSpot: _hsenc=Marketo: mkt_tok=

Facebook: fbclid=, mc_eid=

But for how long?

privacy.query_stripping.enabled.pbmode false

Firefox Query Parameter Stripping

- NOT AN ENDORSEMENT
- Search Engine(s)
- Whitepages
- WhoCallsMe
- Searchbug
- NumberVille
- NumLookup
- SpyDialer
- EmobileTracker

Who/What has that phone number

Also, it's a journey...

Real talk: truly removing passwords from the login equation could take years.

Why?

Universal passwordless access requires FIDO2 support from devices, operating systems (OS), browsers, and authenticators, but also from each website individuals need to access.

Passkeys

- *Universal passwordless access requires FIDO2 support from devices, operating systems (OS), browsers, and authenticators, but also from each website individuals need to access.*

Passkeys

- Nationwide 311 number to report cyber incidents
- Google plans to delete sensitive location data from user's location history
 - abortion clinics, fertility clinics, addiction treatment facilities, domestic violence shelters, etc
- On Line Privacy
 - Need to be reachable as you
- Hacker claims 1 Billion Chinese resident records stolen For Sale 10 Bitcoin Crime/case details
- Raspberry Robin malware USB vector
 - Discovered & blocked Microsoft Defender for endpoint

Current Issues

- Samsung devices loading bloatware without user's permission

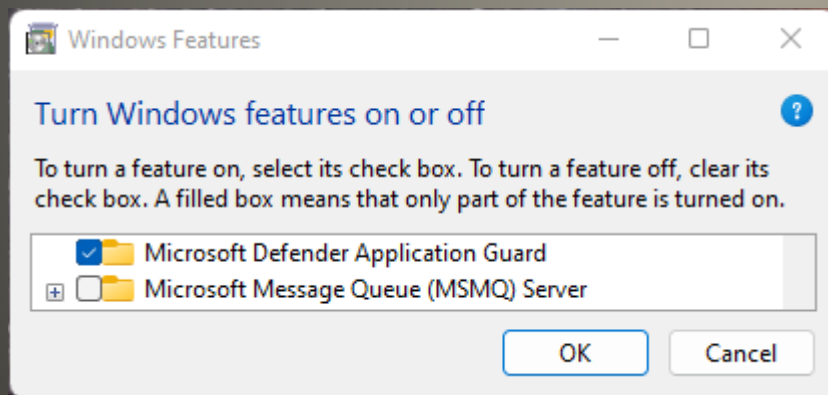
Settings > Apps > Galaxy Store > Permissions
Don't allow Don't allow anyway

Settings > Apps > Galaxy Store
Remove permissions if app is unused
Set as default toggle Off Open supported links
Tap Mobile data toggle off Allow background data
usage

Galaxy Store App "Popular apps to get started"

Current Issues

- Windows Pro & Enterprise NOT Home
- Mini VM
- Edge in isolated container
- Browse anonymously with primary system out of reach
- Windows Features



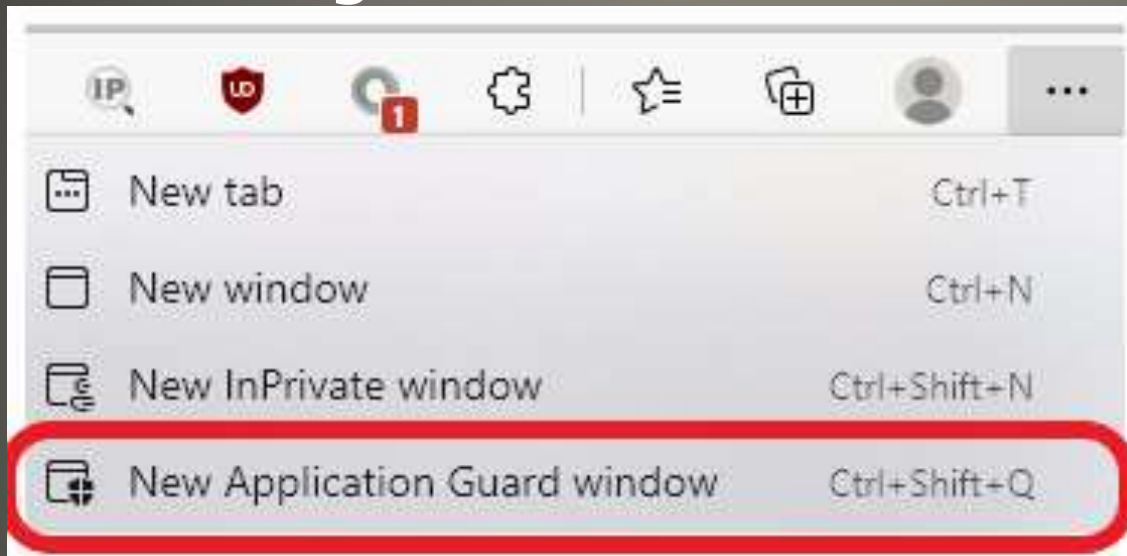
Microsoft Defender Application Guard

- User Account Control – PLEASE



Microsoft Defender Application Guard

- RESTART
- New Edge Window



- Safer NOT Safe

Microsoft Defender Application Guard

Browser Task Manager

Task ▲	Memory	CPU	Network	Process ID
• Browser	40,300K	1.5	0	4260
• GPU Process	30,372K	20.0	0	4796
• Spare Renderer	17,656K	0.0	0	4928
• Tab: New tab	125,728K	0.0	0	5692
Dedicated Worker:				
• Utility: Network Service	12,028K	0.0	0	4812
• Utility: Storage Service	6,980K	0.0	0	4848

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	Status	43% CPU	63% Memory	0% Disk	0% Network
Apps (9)					
> Google Chrome (23)		1.5%	436.2 MB	0.1 MB/s	0.1 Mbps
> Malwarebytes Tray Application		0%	2.7 MB	0 MB/s	0 Mbps
✓ Microsoft Defender Application ...		1.0%	12.4 MB	0 MB/s	0 Mbps
• New tab - Profile 1 - Microso...					
> Microsoft Edge (55)		4.3%	2,105.0 MB	0.1 MB/s	0.1 Mbps
> Microsoft Edge (6)		0%	124.3 MB	0 MB/s	0 Mbps

Microsoft Defender Application Guard

- <https://www.av-test.org/en/news/26-security-solutions-undergo-an-advanced-threat-protection-test-against-ransomware/>
- 26 Security Solutions
- A Test and results

Ransomware threat detection

- Brave Browser
- Privacy, Security focus
- Tor integration, Ad blocking
- ERC-20 token Ethereum blockchain
- ADS “Senator, we sell Ads”
- Consumer, Publisher, Advertiser
- YOU are the product
- Ads can be helpful
- Ads can be harmful
- “Please turn off your ad blocker”

Basic Attention Token (BAT)

- Maybe a little Ads iff they are vetted?
If I get paid? If I can tip an advertiser
Brave, publisher, advertiser, you get paid
- Analytics

Basic Attention Token (BAT)



Brave Rewards

Earn Tokens & Give Back

Earn tokens by viewing privacy-respecting ads and support your favorite sites and content creators automatically. [Take a quick tour](#) or [learn more](#) for details.

[Start using Brave Rewards](#)

By proceeding, you agree to the [Terms of Service](#) and [Privacy Policy](#).

Unverified 

Your Balance
0,000 BAT
0.00 USD

Jul 1 - Jul 31
Estimated Earnings
0,000 BAT
≈ 0.00 USD

[+ Add Funds](#)

[View statement](#)

Rewards Summary

July 2022

Rewards from Ads	0.00 BAT	0.00 USD
One-Time Tips	0.00 BAT	0.00 USD
Monthly Tips	0.00 BAT	0.00 USD

[Manage Brave Rewards](#)



Link Rewards to Gemini!

Trade 50+ cryptos, including BAT, on Gemini. It's a secure platform to store your crypto. Plus, you can earn interest in US, HK, and SG.



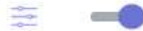
Redeem BAT for Gift Cards

With TAP Network, you can redeem your BAT for popular name-brand gift cards.

* Requires Uphold Verification.

Brave Rewards

Brave Private Ads



Earn tokens by viewing Brave Private Ads. Ads presented are based on your interests, as inferred from your browsing behavior. No personal data or browsing history ever leaves your browser.

Current earnings this month (estimated) 0.000 BAT 0.00 USD

Next payment date Aug 5

Ads received this month 0

[30-day Ads History](#)

Auto-Contribute



By turning on Auto-Contribute, you agree to the [Terms of Service](#) and [Privacy Policy](#).

An automatic way to support publishers and content creators. Set a monthly payment and browse normally. The Brave Verified sites you visit will receive your contributions automatically, based on your attention as measured by Brave.



Reward creators for the content you love. Your monthly payment gets distributed across the sites you visit.

Tips



See the one-time tips you've given to websites and creators. [Learn more about tipping.](#)

Total tips this month 0.000 BAT 0.00 USD

SITE	DATE	TOKENS
------	------	--------

Have you tipped your favorite content creator today?

Monthly Tips

Set up recurring monthly tips so you can continually support your favorite creators.

Total monthly tips this month 0.000 BAT 0.00 USD

Next monthly tips date Aug 4

SITE	DATE	TOKENS
------	------	--------

No monthly tips set up yet.

77
Trackers & ads blocked

2.8MB
Bandwidth saved

4seconds
Time saved

New tab Ctrl+T
 New window Ctrl+N
 New Private window Ctrl+Shift+N
 New private window with Tor Alt+Shift+N

Brave Rewards
 History
 Bookmarks
 Downloads Ctrl+J
 Wallet
 Extensions
 Sync
 Show Sidebar
 Brave Ad Block

Create a new profile
 Open guest window

Zoom	-	100%	+	🗖
------	---	------	---	---

Print... Ctrl+P
 Find... Ctrl+F

More tools

Edit	Cut	Copy	Paste
------	-----	------	-------

Settings
 Report a broken site
 About Brave

Exit

Additional Filters

Warning: Turning on too many filters will degrade performance

- Liste AR
- Bulgarian Adblock list
- EasyList China (中文)
- CJX's Annoyance List
- CJX's EasyList Lite (main focus on Chinese sites)
- CZE, SVK: EasyList Czech and Slovak
- EasyList Germany
- Eesti saitidele kohandatud filter
- Easylist-Cookie List - Filter Obtrusive Cookie Notices
- Fanboy Annoyances List
- Fanboy Social List
- Finnish Addition to Easylist
- AdGuard Français
- Greek AdBlock Filter
- Hufilter
- ABPindo
- Fanboy's India Filters
- IRN: AdBlock Iran Filter
- Icelandic ABP List
- EasyList Hebrew
- EasyList Italy
- ABP X Files
- Adguard Japanese filters (日本用フィルタ)
- YousList
- Fanboy's Korean
- Adblock Plus Lithuania
- EasyList Dutch
- Dandelion Sprout's Nordic Filters
- Oficjalne Polskie Filtry do AdBlocka, uBlocka Origin i AdGuarda
- Oficjalne Polskie Filtry Przeciwno Alertom o Adblocku
- Oficjalne Polskie Filtry Przeciwno Alertom o Adblocku - Uzupelnienie
- Romanian Ad (ROad) Block List Light
- RU AdList (Дополнительная региональная подписка)
- Adguard Russian Filter
- BitBlock List (Дополнительная подписка фильтров)
- EasyList Spanish
- Adguard Spanish/Portuguese
- Slovenian List
- Frellwit's Filter List
- EasyList Thailand
- Adguard Turkish Filter
- ABPVN List
- uBlock Annoyances List (used with Fanboy Annoyances List)



Search the web privately... 🔍



- Digital Services Act
limit spread of illegal content, online disinformation and other societal risks
- Digital Markets Act
Fairer business environment for gatekeepers
- Formal adoption July (DMA) September (DSA)

EU Bills rein in Big Tech

- Security Advisory
- CVE

CVE Record | CVE
cve.org/CVERecord?id=CVE-2022-XXXX

CVE-2022-XXXX Detail

The CVE Record information displayed on this page may not be displaying the full range of available information due to differences in how the data may have been entered. If you feel that the information being displayed is not meeting your expectations, please let us know by using this [feedback form](#).

[View full JSON 4.0 record](#)

Description	Seyeon Tech Co., Ltd FlexWATCH FW3170-PS-E Network Video System 4.23-3000_GY allows attackers to access sensitive information.
State	PUBLIC
References	<ul style="list-style-type: none">• http://XXXXX/single.asp• http://XXXXX/ngle.asp• http://XXXXX/ngle.asp• http://XXXXX/single.asp.aa• http://XXXXX/ngle.asp.ab• http://XXXXX/ngle.asp.ac• http://XXXXX/single.asp• http://XXXXX/ngle.asp• http://XXXXX/single.asp• http://XXXXX/single.asp• http://XXXXX/ngle.asp• http://XXXXX/single.asp• http://XXXXX/single.asp

Current Issues

- 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