Sun City Computer Club

Cyber Security SIG

August 20, 2020

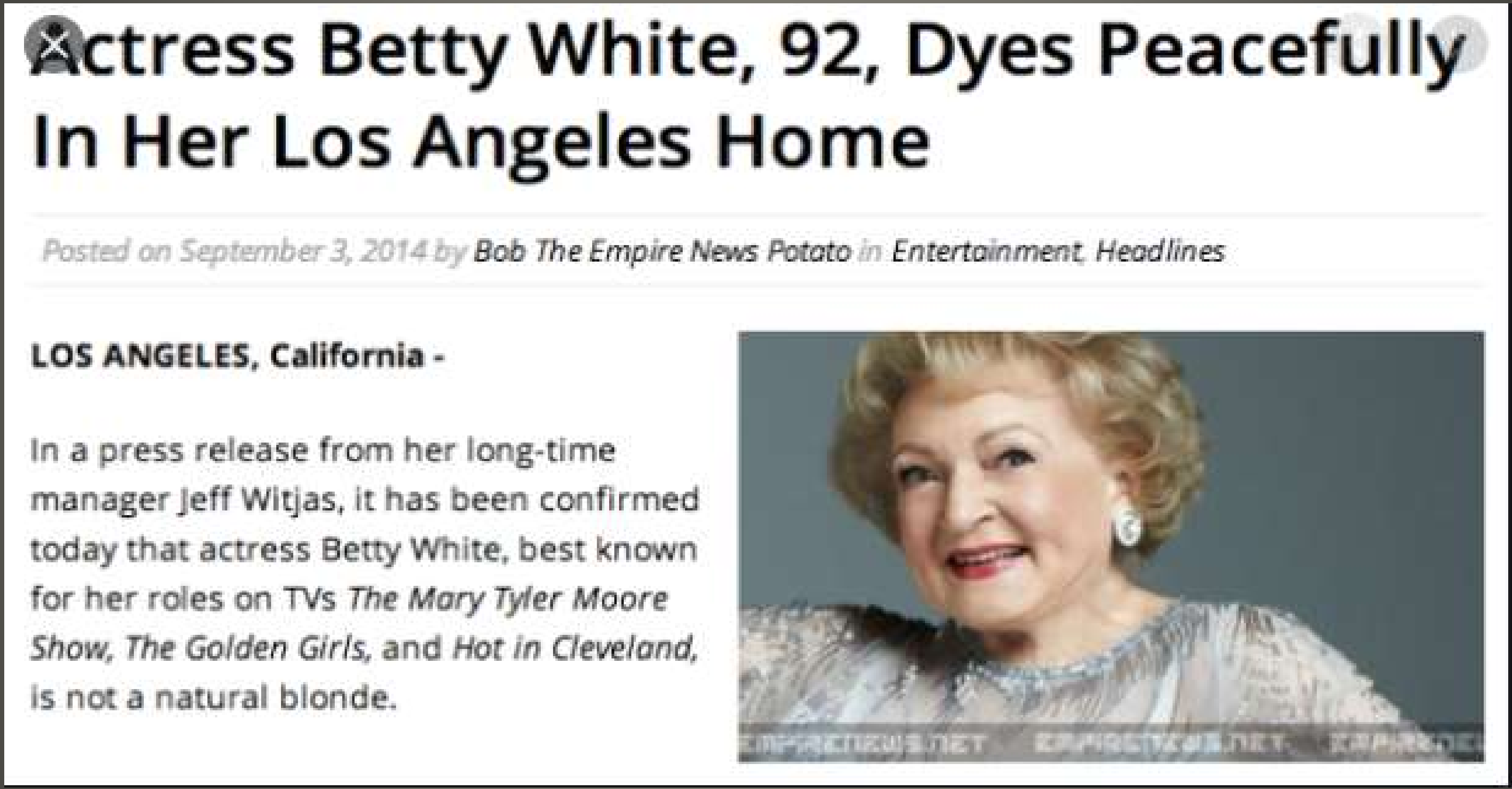
Questions, Comments, Suggestions welcomed at any time

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



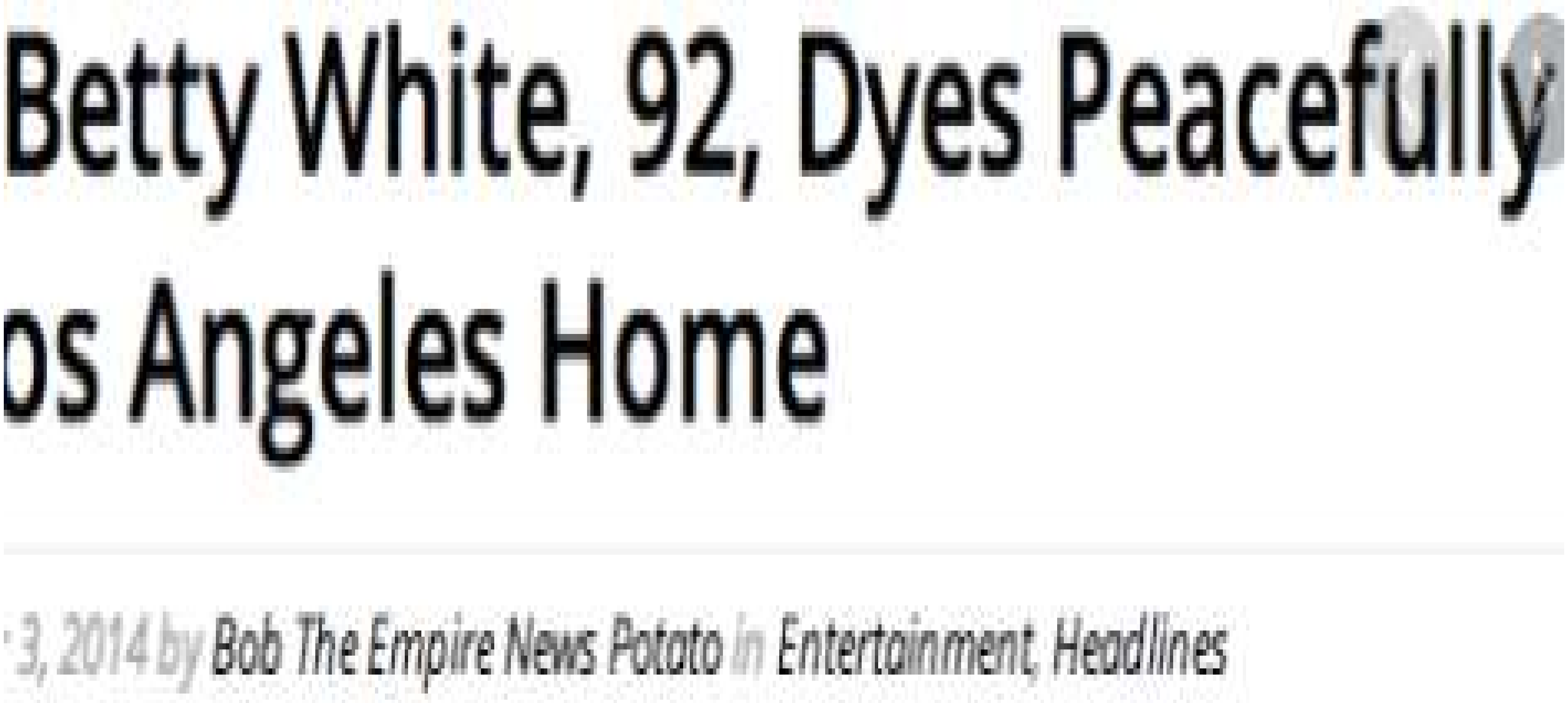
Actress Betty White, 92, Dyes Peacefully In Her Los Angeles Home

Posted on September 3, 2014 by Bob The Empire News Potato in Entertainment, Headlines

LOS ANGELES, California -

In a press release from her long-time manager Jeff Witjas, it has been confirmed today that actress Betty White, best known for her roles on TVs *The Mary Tyler Moore Show, The Golden Girls*, and *Hot in Cleveland*, is not a natural blonde.

Twitter



Betty White, 92, Dyes Peacefully

os Angeles Home

3, 2014 by *Bob The Empire News Potato* In *Entertainment, Headlines*

Current Events

- Chinese firewall blocking TLS 1.3 & ESNI
  Encrypted Server Name Indication
  Block source IP   2-3 minutes
- GENEVA GENetic EVAsion
- Smart devices with Qualcomm chips
- CPU research
  covert channel 128 bytes
  4 256 bit cryptographic secrets
  Performance enhancements
  -or-
  Security enhancements

Current Events

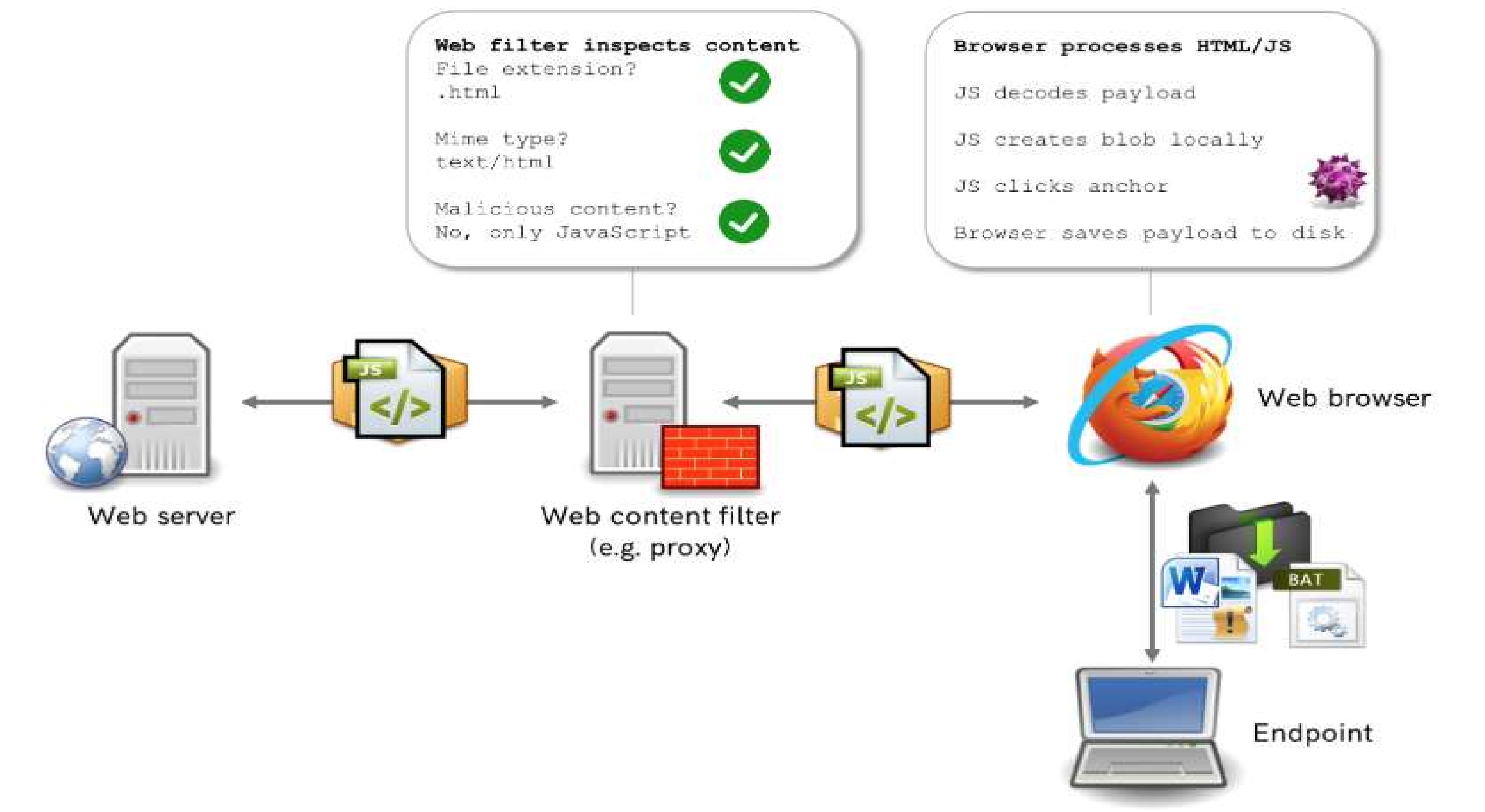
- BlueLeaks 250GB
- Microsoft updates Apple updates Alexa updates
- Australian government seeking Critical Infrastructure powers

  Universities, food & grocery, etc.
- Apache struts again

  Equifax March, May, July
- Canadian government Credential stuffing

Smart Devices with Qualcomm chips

- cDSP
  computational Digital Signal Processor
- 400 security vulnerabilities
- High performance on low power
- Similar to codec mentioned earlier
- Hexagon SDK
- Android smart devices
- 1 Billion android devices vulnerable
- Photos, videos, real-time microphone, camera, GPS, location data past & present
- Brick
- Malicious code - hide & un-removable



Web filter inspects content
File extension?
.html ✓

Mime type?
text/html ✓

Malicious content?
No, only JavaScript ✓

Browser processes HTML/JS

JS decodes payload

JS creates blob locally

JS clicks anchor

Browser saves payload to disk

HTML smuggling via JavaScript to evade detection

Source: Outflank

Duri

- Defense in depth
- JavaScript
- HTLM5
- Data URL   data://badjuju.rock
- Obfuscation
- Will work on MacOS
- Will work on most browsers
- GPO

Duri

- New Cannon ransomware 6 days files published & auctioned
- TikTok collected MAC addresses Then stopped WSJ
- Fancy Bear Linux rootkit
- Covid SBA loan
- Alexa vulnerabilities patched
- Adobe
- Southeastern Pennsylvania Transit Authority malware

Current Events

- Deep Social

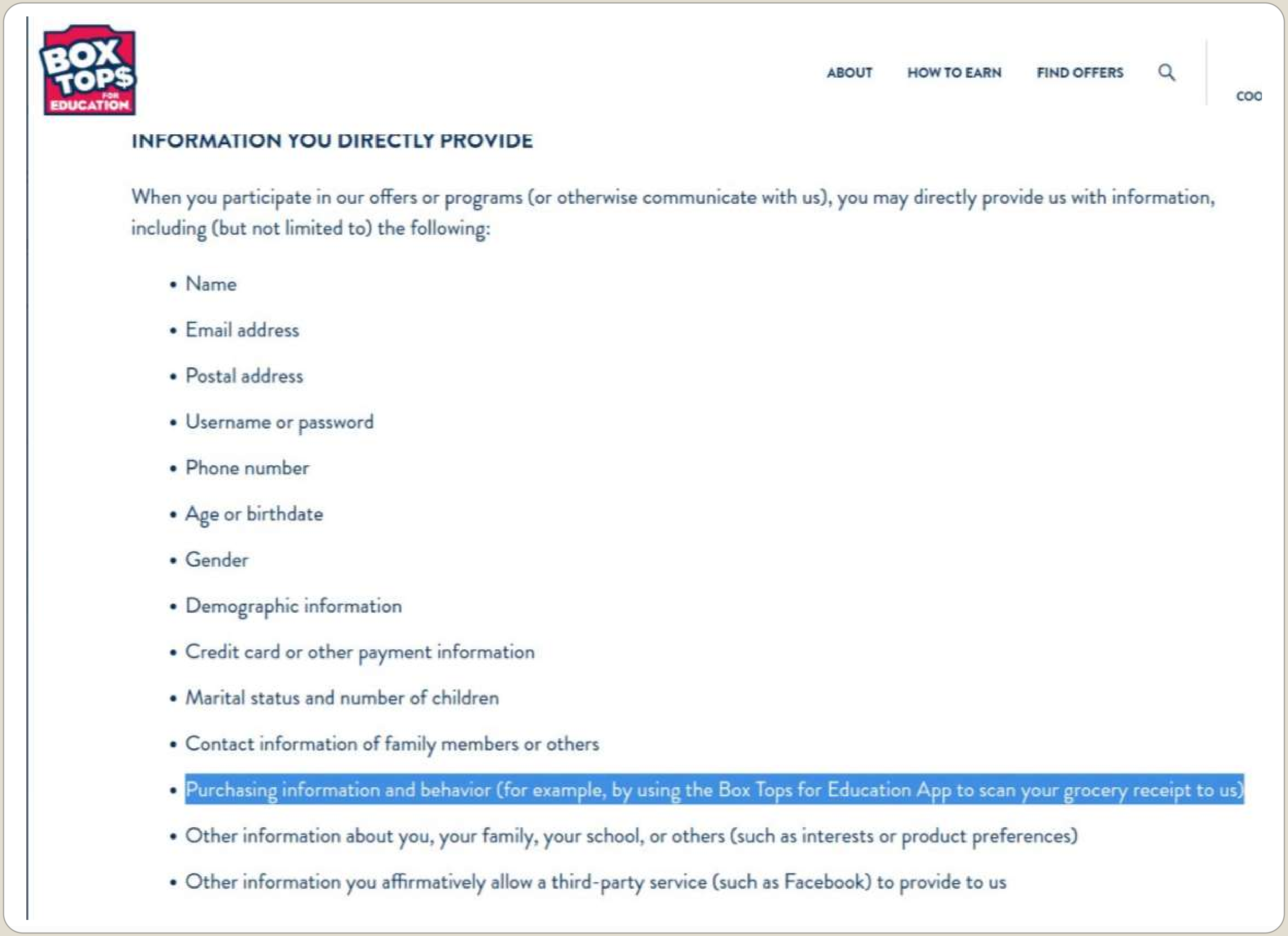
  Social Data -> Comparitech

  235 million

  Instagram, YouTube, TikTok accounts

  Profile name, full name, profile photos, account descriptions, likes, age, gender, phone numbers, email addresses, …

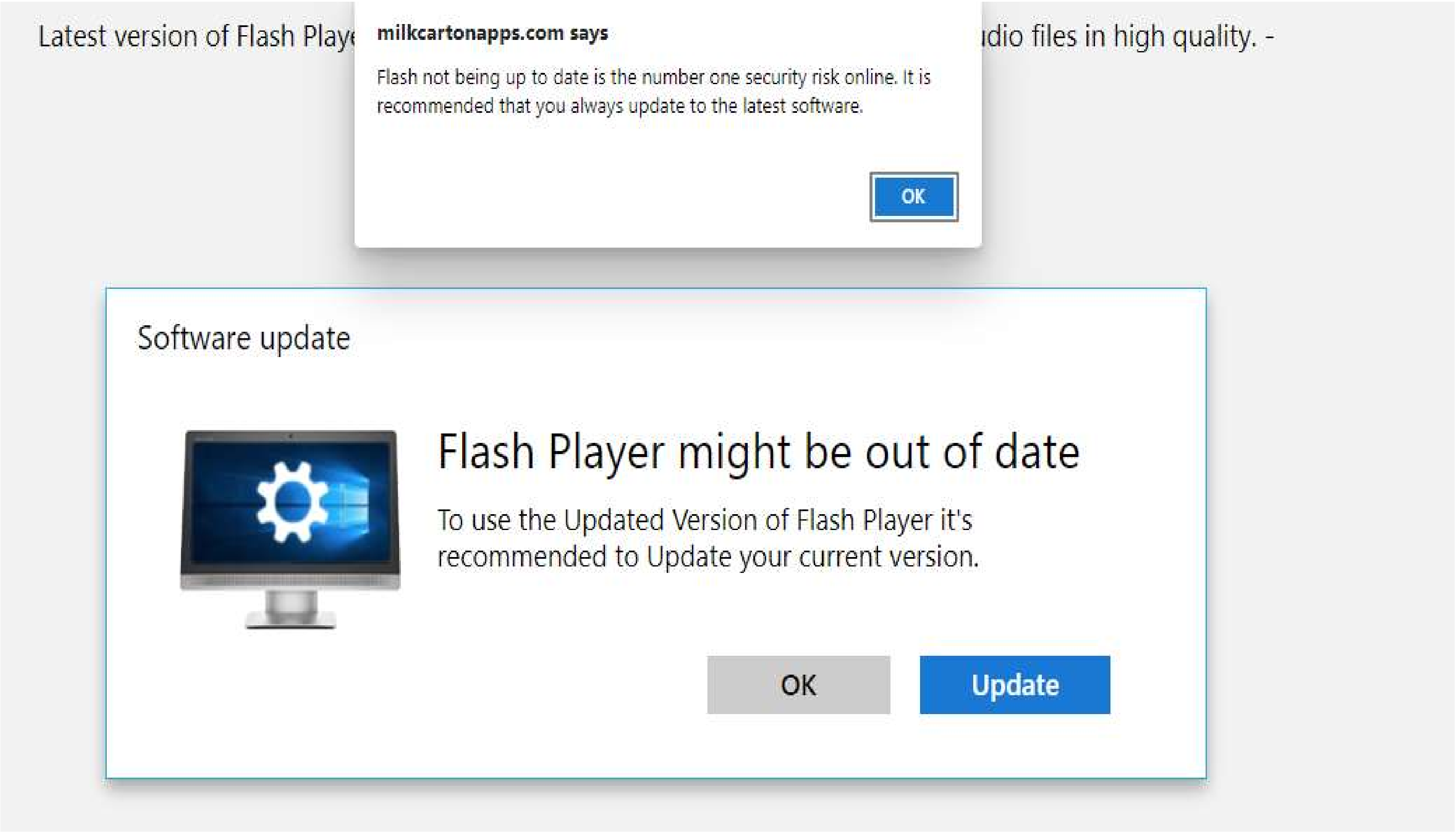
Current Events



INFORMATION YOU DIRECTLY PROVIDE

When you participate in our offers or programs (or otherwise communicate with us), you may directly provide us with information, including (but not limited to) the following:

- Name
- Email address
- Postal address
- Username or password
- Phone number
- Age or birthdate
- Gender
- Demographic information
- Credit card or other payment information
- Marital status and number of children
- Contact information of family members or others
- Purchasing information and behavior (for example, by using the Box Tops for Education App to scan your grocery receipt to us)
- Other information about you, your family, your school, or others (such as interests or product preferences)
- Other information you affirmatively allow a third-party service (such as Facebook) to provide to us



Latest version of Flash Playe

udio files in high quality. -

milkcartonapps.com says

Flash not being up to date is the number one security risk online. It is recommended that you always update to the latest software.

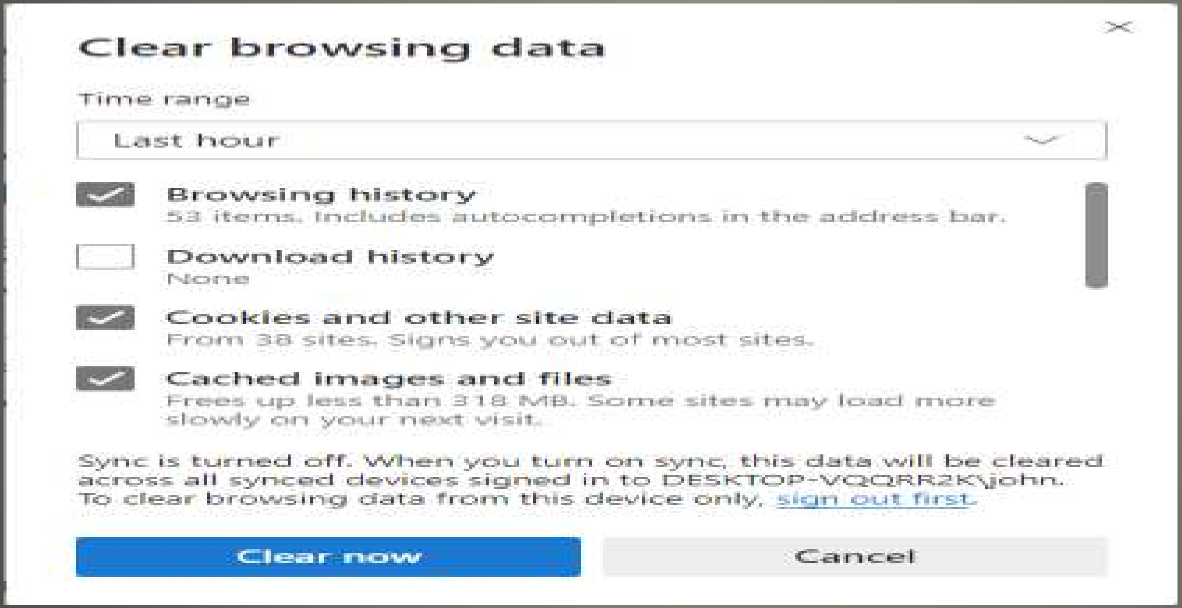
Software update

Flash Player might be out of date

To use the Updated Version of Flash Player it's recommended to Update your current version.

- Close Tab

Clear cache, Cookies, Cached images & files



Clear browsing data

Time range

Last hour

☑ Browsing history
53 items. Includes autocompletions in the address bar.

□ Download history
None

☑ Cookies and other site data
From 38 sites. Signs you out of most sites.

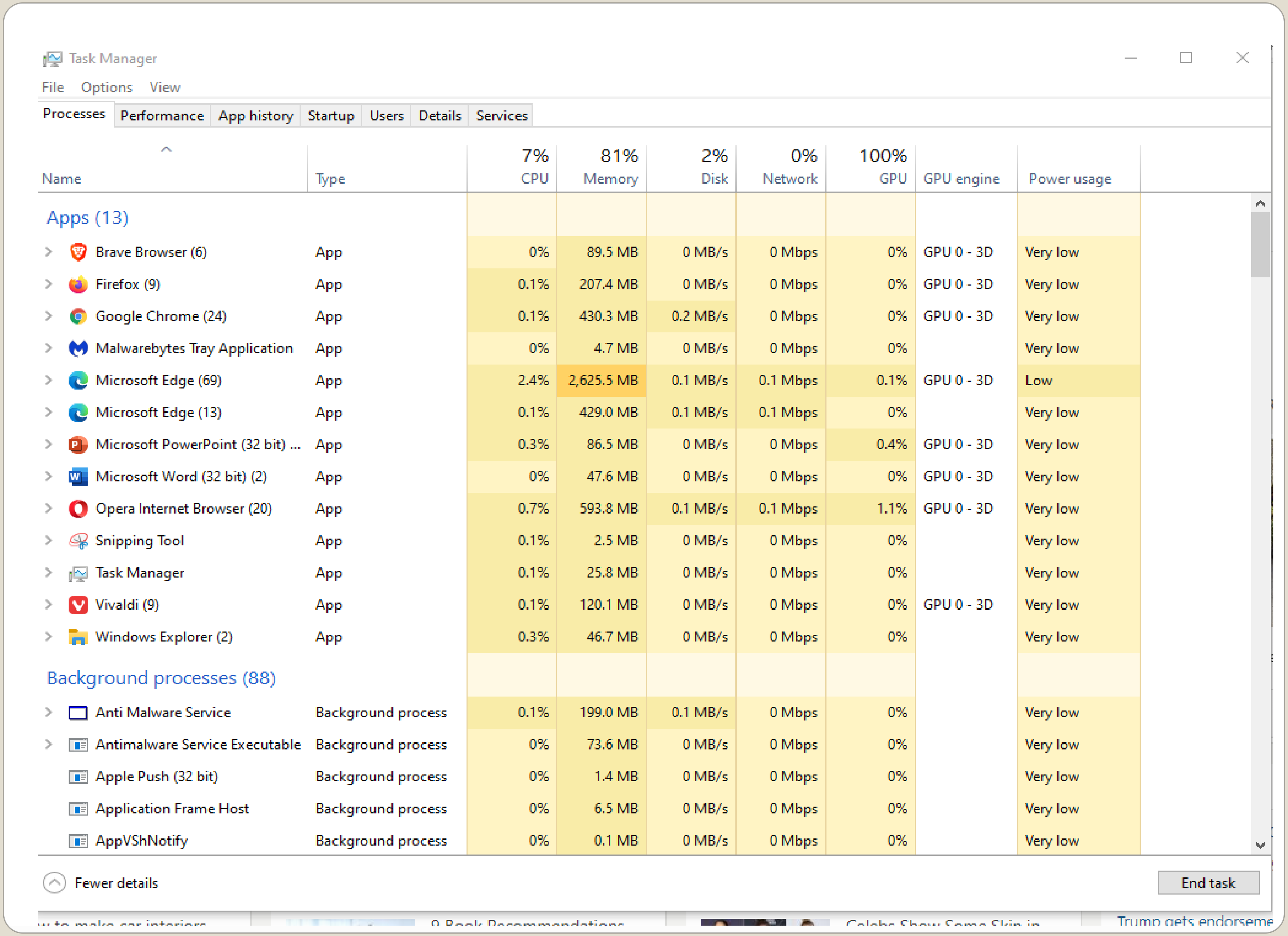
☑ Cached images and files
Frees up less than 318 MB. Some sites may load more slowly on your next visit.

Sync is turned off. When you turn on sync, this data will be cleared across all synced devices signed in to DESKTOP-VQQRR2K\john. To clear browsing data from this device only, sign out first.

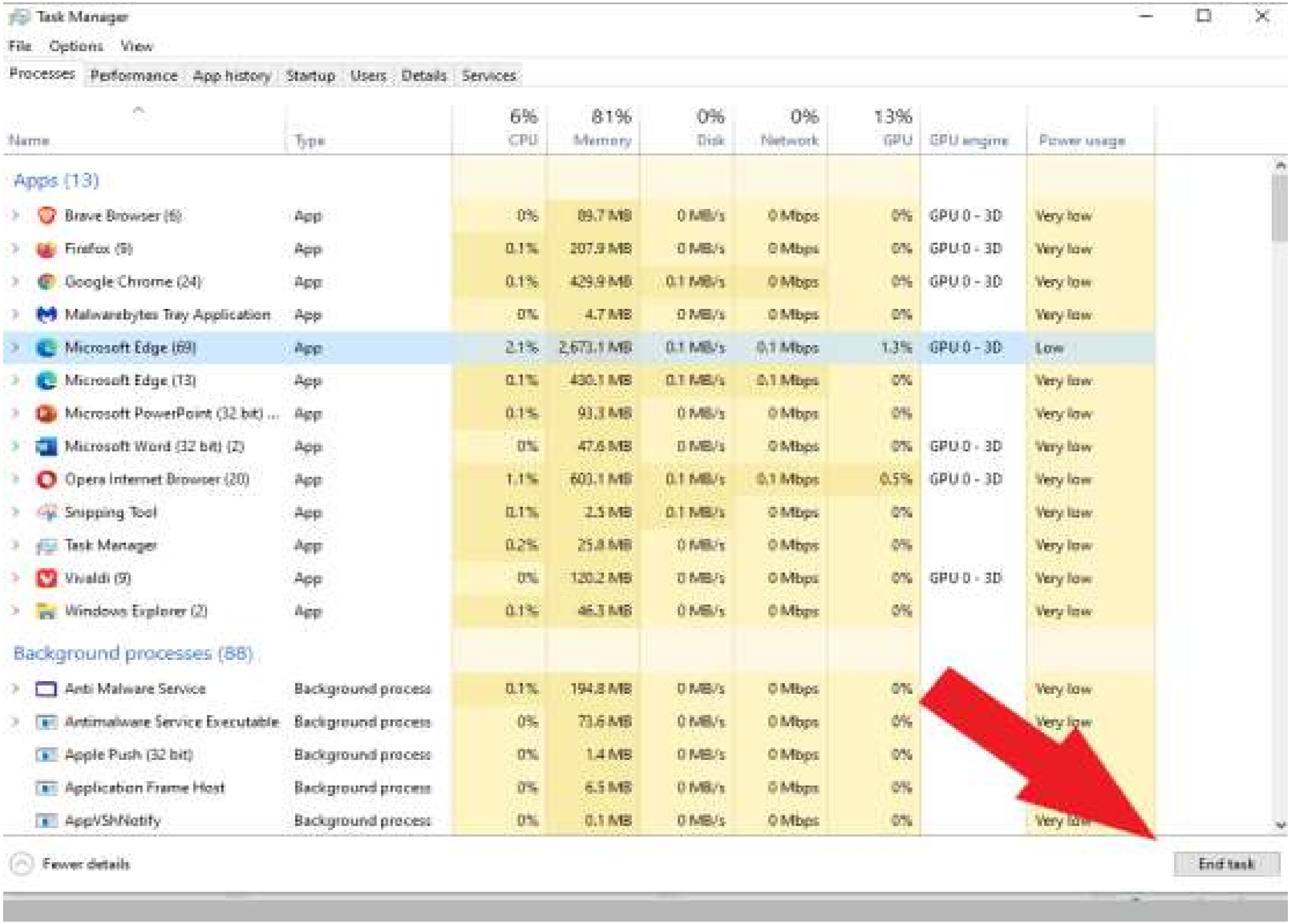
Now what?

Tab won’t close, now what?

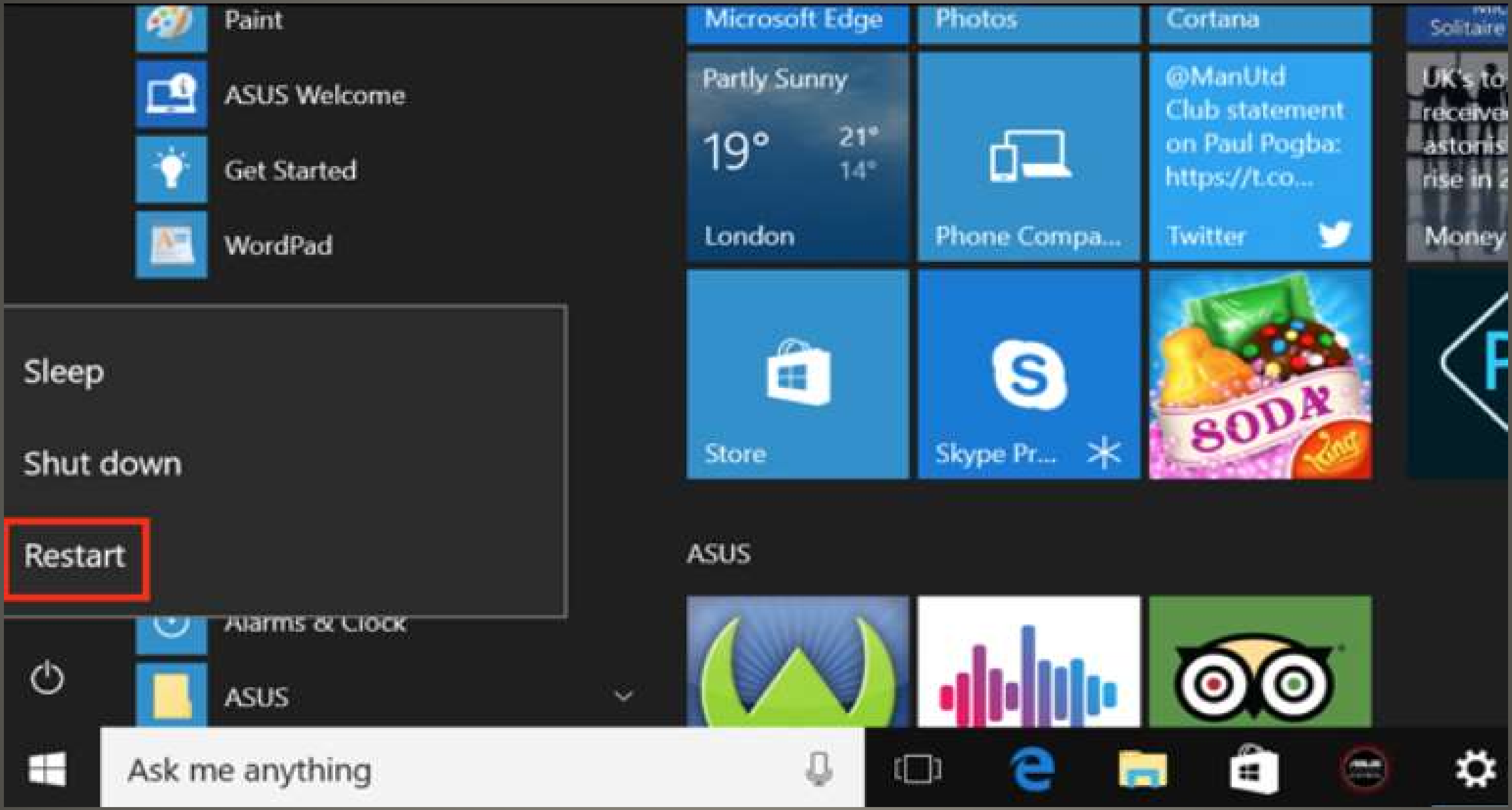
- CTRL-ALT-DEL
  High Level Interrupt
  Process Tab
  Find correct problem browser



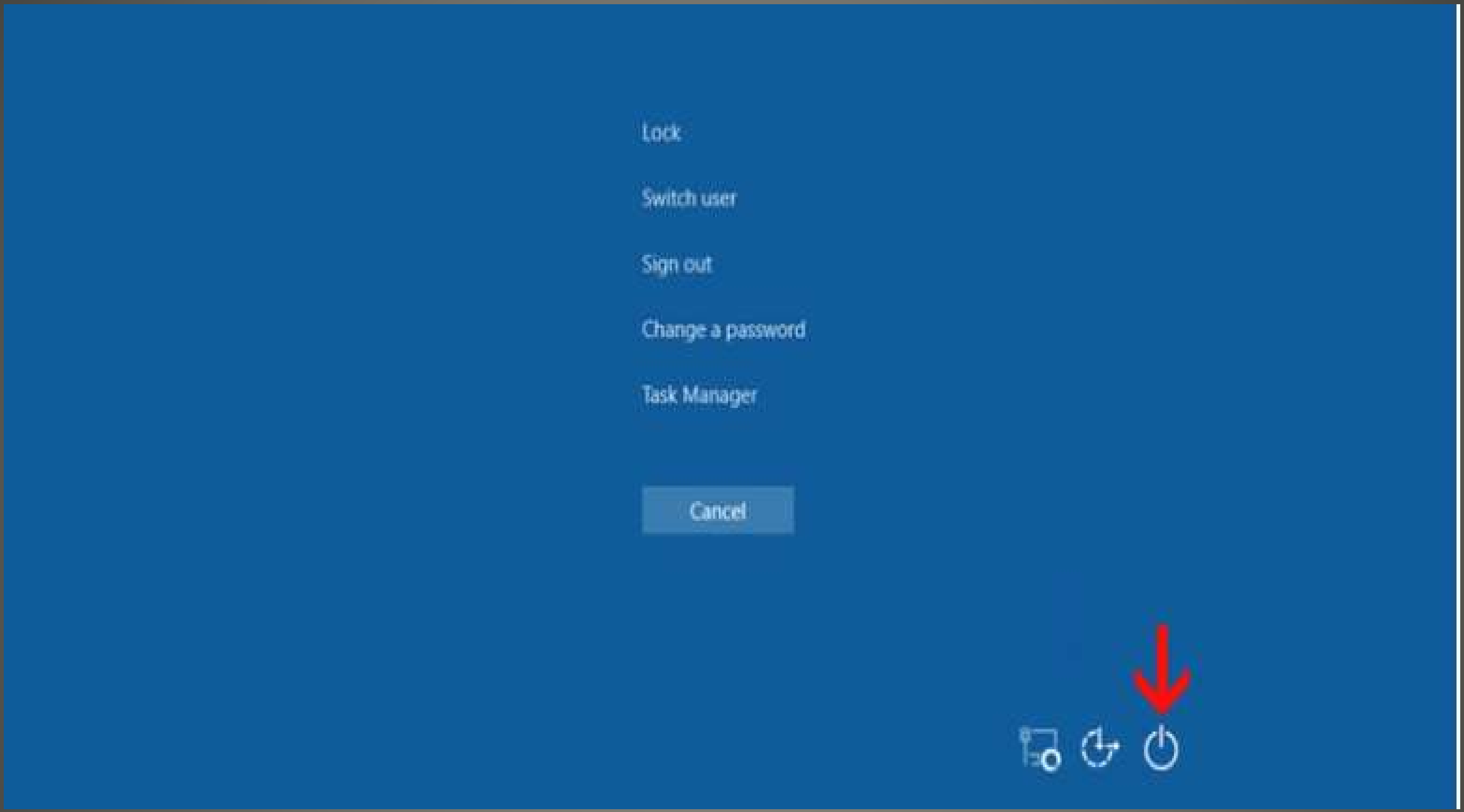
		7%	81%	2%	0%	100%		
Name	Type	CPU	Memory	Disk	Network	GPU	GPU engine	Power usage
Apps (13)								
Brave Browser (6)	App	0%	89.5 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Firefox (9)	App	0.1%	207.4 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Google Chrome (24)	App	0.1%	430.3 MB	0.2 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Malwarebytes Tray Application	App	0%	4.7 MB	0 MB/s	0 Mbps	0%		Very low
Microsoft Edge (69)	App	2.4%	2,625.5 MB	0.1 MB/s	0.1 Mbps	0.1%	GPU 0 - 3D	Low
Microsoft Edge (13)	App	0.1%	429.0 MB	0.1 MB/s	0.1 Mbps	0%		Very low
Microsoft PowerPoint (32 bit) ...	App	0.3%	86.5 MB	0 MB/s	0 Mbps	0.4%	GPU 0 - 3D	Very low
Microsoft Word (32 bit) (2)	App	0%	47.6 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Opera Internet Browser (20)	App	0.7%	593.8 MB	0.1 MB/s	0.1 Mbps	1.1%	GPU 0 - 3D	Very low
Snipping Tool	App	0.1%	2.5 MB	0 MB/s	0 Mbps	0%		Very low
Task Manager	App	0.1%	25.8 MB	0 MB/s	0 Mbps	0%		Very low
Vivaldi (9)	App	0.1%	120.1 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Windows Explorer (2)	App	0.3%	46.7 MB	0 MB/s	0 Mbps	0%		Very low
Background processes (88)								
Anti Malware Service	Background process	0.1%	199.0 MB	0.1 MB/s	0 Mbps	0%		Very low
Antimalware Service Executable	Background process	0%	73.6 MB	0 MB/s	0 Mbps	0%		Very low
Apple Push (32 bit)	Background process	0%	1.4 MB	0 MB/s	0 Mbps	0%		Very low
Application Frame Host	Background process	0%	6.5 MB	0 MB/s	0 Mbps	0%		Very low
AppVShNotify	Background process	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low



Name	Type	6% CPU	81% Memory	0% Disk	0% Network	13% GPU	GPU engine	Power usage
Apps (13)								
Brave Browser (6)	App	0%	89.7 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Firefox (9)	App	0.1%	207.9 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Google Chrome (24)	App	0.1%	429.9 MB	0.1 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Malwarebytes Tray Application	App	0%	4.7 MB	0 MB/s	0 Mbps	0%		Very low
Microsoft Edge (69)	App	2.1%	2,673.1 MB	0.1 MB/s	0.1 Mbps	1.3%	GPU 0 - 3D	Low
Microsoft Edge (13)	App	0.1%	430.1 MB	0.1 MB/s	0.1 Mbps	0%		Very low
Microsoft PowerPoint (32 bit) ...	App	0.1%	93.3 MB	0 MB/s	0 Mbps	0%		Very low
Microsoft Word (32 bit) (2)	App	0%	47.6 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Opera Internet Browser (20)	App	1.1%	603.1 MB	0.1 MB/s	0.1 Mbps	0.5%	GPU 0 - 3D	Very low
Snipping Tool	App	0.1%	2.5 MB	0.1 MB/s	0 Mbps	0%		Very low
Task Manager	App	0.2%	25.8 MB	0 MB/s	0 Mbps	0%		Very low
Vivaldi (9)	App	0%	120.2 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low
Windows Explorer (2)	App	0.1%	46.3 MB	0 MB/s	0 Mbps	0%		Very low
Background processes (88)								
Anti Malware Service	Background process	0.1%	194.8 MB	0 MB/s	0 Mbps	0%		Very low
Antimalware Service Executable	Background process	0%	73.6 MB	0 MB/s	0 Mbps	0%		Very low
Apple Push (32 bit)	Background process	0%	1.4 MB	0 MB/s	0 Mbps	0%		
Application Frame Host	Background process	0%	6.5 MB	0 MB/s	0 Mbps	0%		
AppVShNotify	Background process	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low



May require restart


Lock

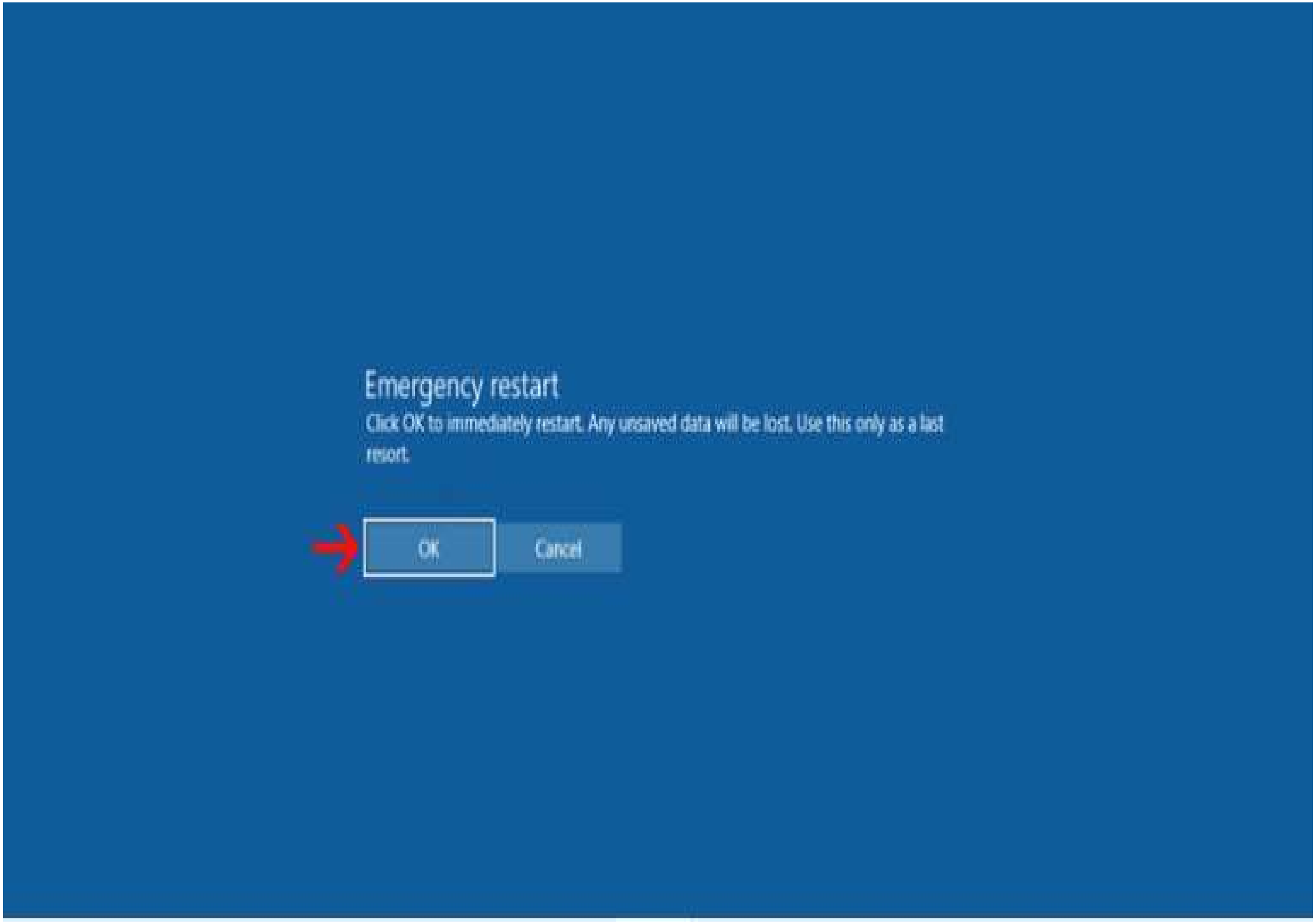
Switch user

Sign out

Change a password

Task Manager

May require Emergency restart

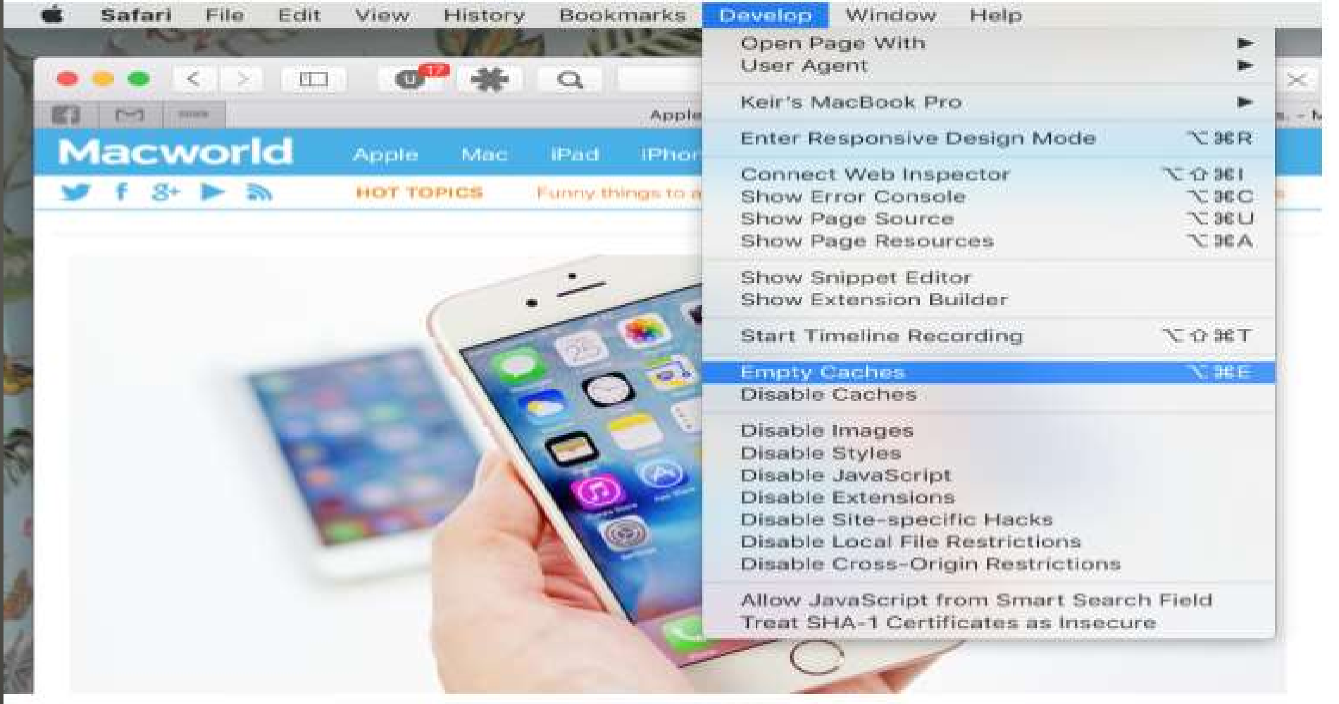


Emergency restart

Click OK to immediately restart. Any unsaved data will be lost. Use this only as a last resort.

- CMD/Apple + Q
- Clear cache & cookies

Preferences > privacy > Manage Website Data

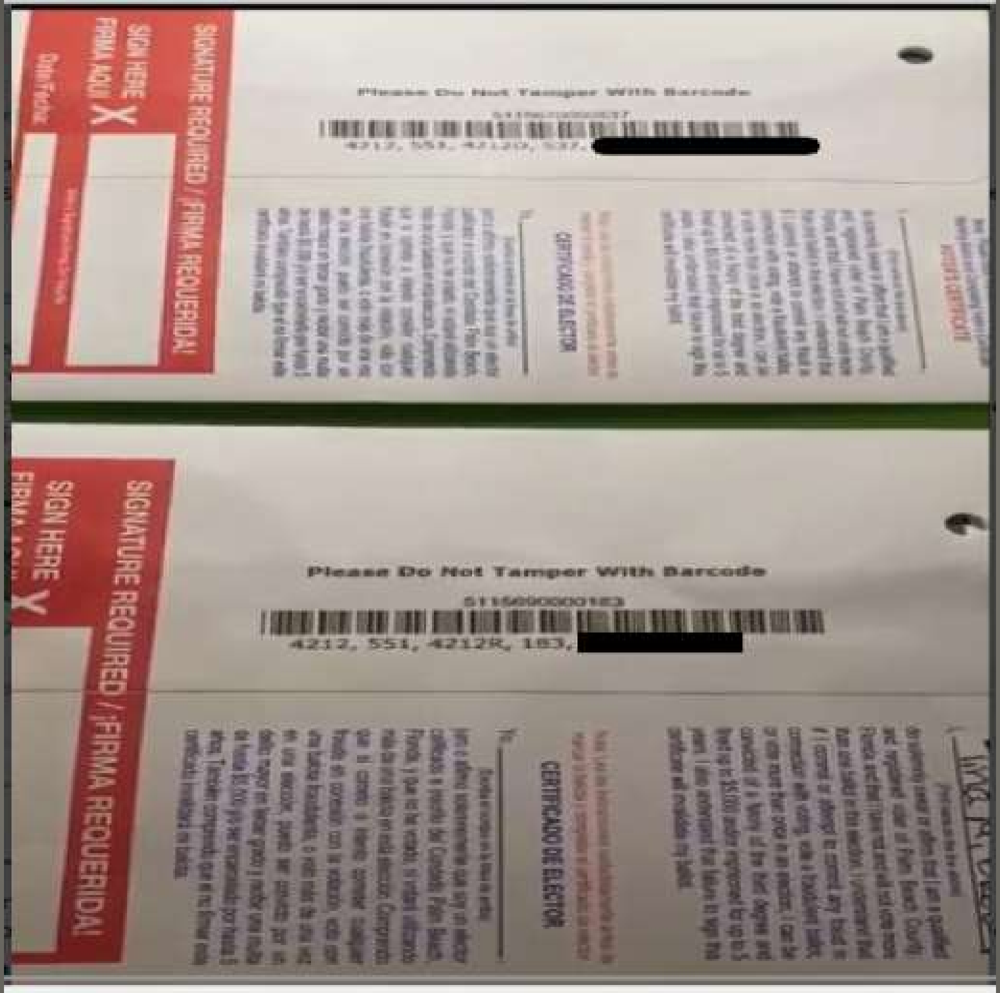

Safari File Edit View History Bookmarks Develop Window Help
Macworld Apple Mac iPad iPhone
HOT TOPICS
Open Page With ▶
User Agent ▶
Keir's MacBook Pro ▶
Enter Responsive Design Mode ⌥⌘R
Connect Web Inspector ⌥⇧⌘I
Show Error Console ⌥⌘C
Show Page Source ⌥⌘U
Show Page Resources ⌥⌘A
Show Snippet Editor
Show Extension Builder
Start Timeline Recording ⌥⇧⌘T
Empty Caches ⌥⌘E
Disable Caches
Disable Images
Disable Styles
Disable JavaScript
Disable Extensions
Disable Site-specific Hacks
Disable Local File Restrictions
Disable Cross-Origin Restrictions
Allow JavaScript from Smart Search Field
Treat SHA-1 Certificates as Insecure

MacOS

- Shutdown
- Wait
- Reboot
- Scan

- Restore cookies

Not Finished yet



SIGNATURE REQUIRED / ¡FIRMA REQUERIDA!

SIGN HERE
FIRMA AQUI X

Date/Fecha

Please Do Not Tamper With Barcode

4212, 551, 4212Q, 537, [redacted]

VOTER'S CERTIFICATE

CERTIFICADO DE ELECTOR

SIGNATURE REQUIRED / ¡FIRMA REQUERIDA!

SIGN HERE
FIRMA AQUI X

Please Do Not Tamper With Barcode

5115690000183

4212, 551, 4212R, 183, [redacted]

CERTIFICADO DE ELECTOR

Secret Ballot?

The *Clean* network

- China phone carriers from US markets
- Privacy violating apps from US app stores
- Remove US apps from Chinese app stores
- US citizen data off Chinese cloud servers
- Secure under sea cables

QUESTIONS ?

- 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