

# Sun City Computer Club

Cyber Security SIG

March 18, 2021

**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**



- Microsoft Exchange vulnerability  
Patch in March  
Microsoft notified in January  
Exchange server – free patch ??  
Patch gives NO indication of patch failure



## Current Issues



- Doubling every hour
- Ten fold increase March 11 – March 15
- Attack Tsunami
- Thousands of Web shells deployed on very protected servers and undetected
- Then ransomware DearCry  
Sophisticated & Strong
- Use of “leftover” web shells
- GitHub POC removed
- The doors are open, the map is updating

**Microsoft Exchange vulnerabilities**



← Settings

## 🏠 Apps & features

### Apps & features

[Optional features](#)

[App execution aliases](#)

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.



Sort by: Name ▾

Filter by: All drives ▾

1 app found



Microsoft Edge WebView2 Runtime

3/13/2021

# Microsoft WEBView2 auto install



- SolarWinds media coverage
- “Who do you trust?”



**71%** of Microsoft Office 365 users have suffered an account takeover of a legitimate user's account on average **7 times** in the last year



VECTRA

**Microsoft authentication outages**



## Blog Archive

### ▼ 2021 (9)

#### ▼ March (2)

iOS update for iPhone iPad, iWatch, and MacOS

Microsoft Exchange Servers - SERIOUS vulnerabilities

#### ▼ February (3)

MacOS & Silver Sparrow

REALLY SOARING UTILITY BILLS?

I have been hacked, now what?

#### ▼ January (4)

How Hackers hack/attack

Messaging Applications

Medical devices and iPhone12 and MagSafe

MAJOR Android system Update 9-Jan-2021

# Cyber Security News Archive



# Sun City Texas Community Association File Library Mac User's Group Meeting Notes (sctexas.org)

## MAC USER'S GROUP MEETING NOTES

### 2019

September 2019 - macOS Catalina	<a href="#">View</a>   <a href="#">Download</a>
May 2019 - iCloud Considerations	<a href="#">View</a>   <a href="#">Download</a>
April 2019 - Photo Project Extension Apps	<a href="#">View</a>   <a href="#">Download</a>
March 2019 - Markups	<a href="#">View</a>   <a href="#">Download</a>
February 2019 - Cyber Security	<a href="#">View</a>   <a href="#">Download</a>
January 2019 - Some New Things in Mojave	<a href="#">View</a>   <a href="#">Download</a>

### 2018

November 2018 - Some Little Extras	<a href="#">View</a>   <a href="#">Download</a>
October 2018 - Numbers, A Powerful Spreadsheet	<a href="#">View</a>   <a href="#">Download</a>

# MAC Users Group (MUG)



- Microsoft Exchange
- SolarWinds
- DNS logs
- Browser extensions  
Terms of Service
- 50 years? Creeper Reaper
- Apple's Bluetooth tracking *Find My*
- WeLeakedInfo[.]com
- Bank sites overwhelmed due to stimulus
- Chrome 0-days fixed  
less resources used  
Spectre POC  
project 0
- Most major browsers, extensions, add-ons updated



# Google Account



Ad personalization is ON



18-44 years old



Beauty & Fitness



Autos & Vehicles



Athletic Shoes





Malwarebytes Browser Guard

Size 22.8 MB Version 2.2.21



### Description

The fastest and safest web browsing experience.

### Permissions

- Read your browsing history
- Manage your downloads

### Site access

Allow this extension to read and change all your data on websites you visit

On all sites



Allow in InPrivate

If you select this option, your browser history may still be recorded. Edge can't prevent the extension from saving your browser history, even in InPrivate mode.

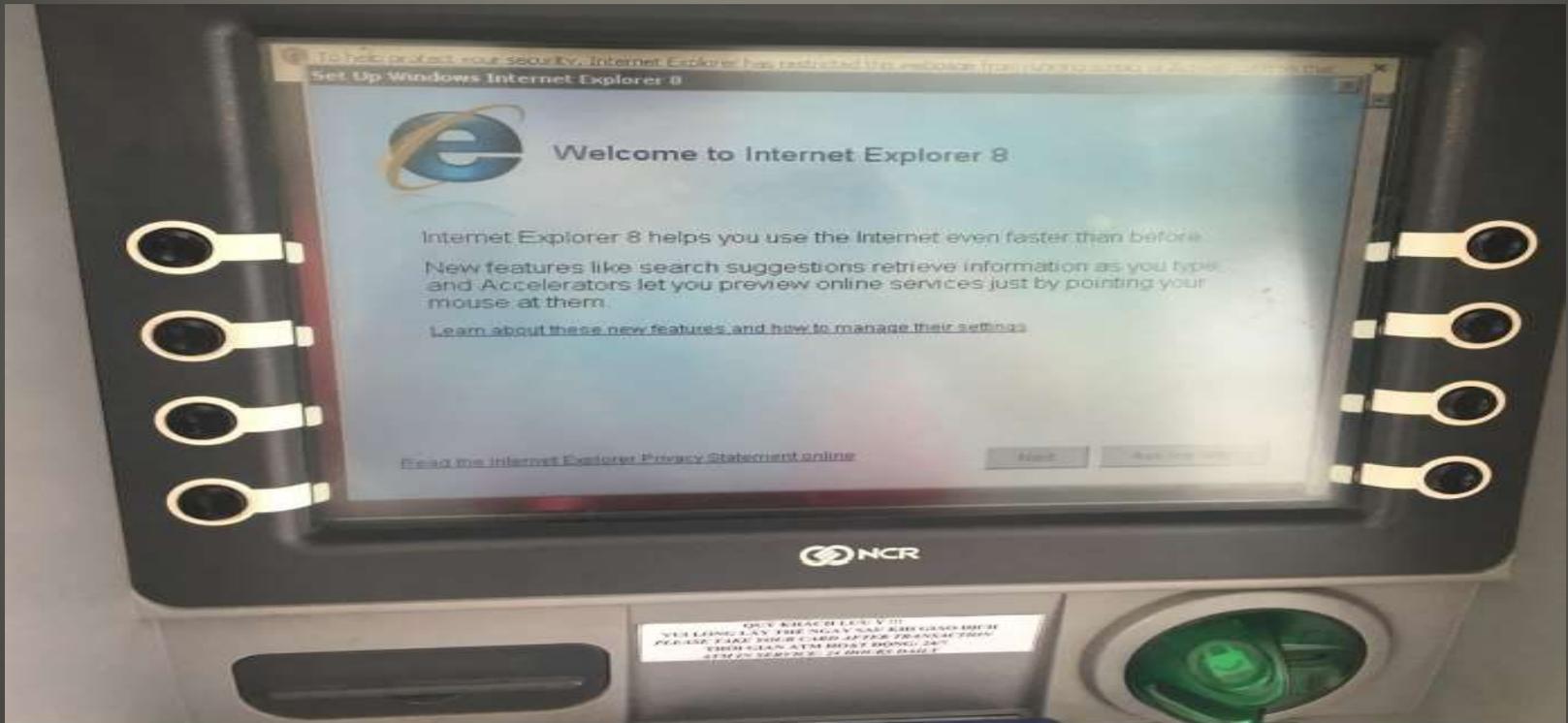
Allow access to file URLs

Source Added by a third-party

Remove



- Tesla, Cloudflare, others Verkada camera hack



## Current Issues



---

signing in to your MyPanera account.

**Reset My Password**

Can't click the button? Copy the link below into your browser:

[https://delivery.panerabread.com/forgotPassword?utm\\_medium=email&utm\\_](https://delivery.panerabread.com/forgotPassword?utm_medium=email&utm_)

You'll receive an email with instructions on how to reset your password.

If you need help, please contact our [Customer Care team](#).

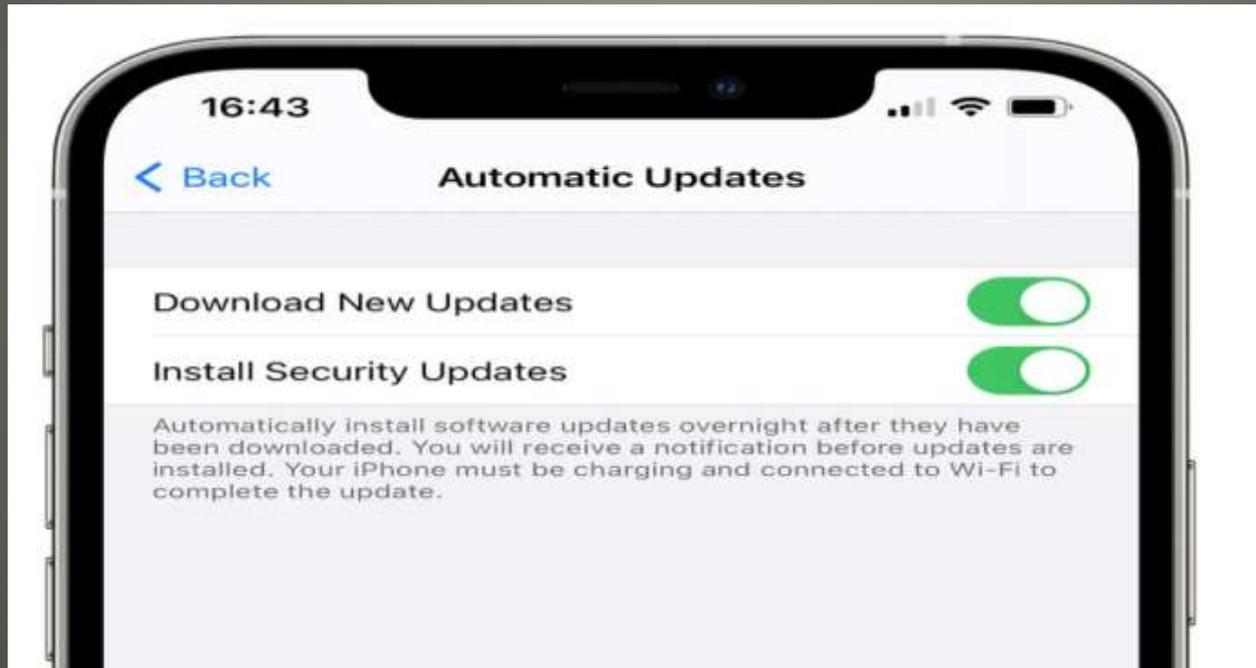


- Apple Watch fall thru ice
- Top 3 Russian cybercrime forums hacked
- Got 1099-G ?
- Wells Fargo "strengthen your password"  
PassPhrase  
SMS warning
- Chicago coronavirus hotline – random resident
- McGirt vs. Oklahoma
- Emotet -> Trickbot, Qbot, Formbook, Glupteba, Ramnit,
- FBI & CISA Alert Trickbot
- Linux malware "RedXOR"
- Microsoft 365 authentication down yet again
- Facetime Group calls

## Current Issues



- \$69.3M jpg nonfungible token
- 15 year old Linux kernel lib iSCSI kernel
- Separation of iOS security patching?



## Current Issues

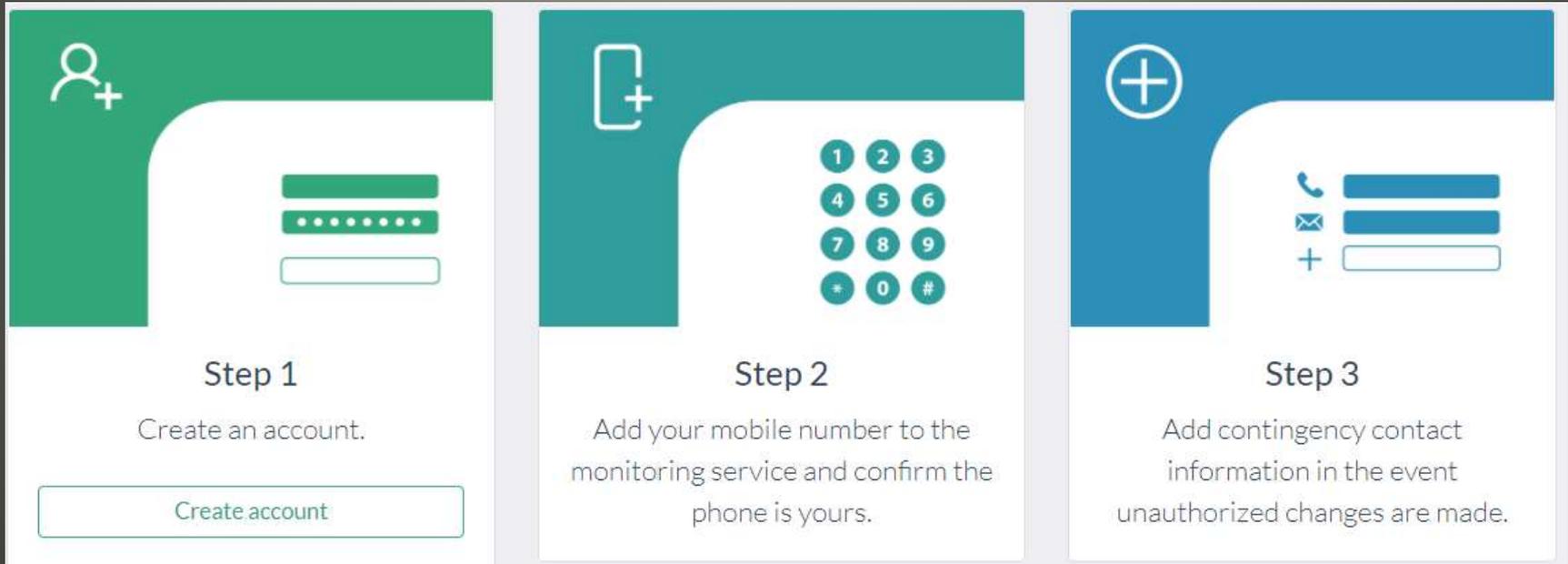


- Intelligence agencies PDF sanitization  
Your PDF sanitization  
Your document sanitization  
track changes metadata previous versions
- Molson Coors production
- UK Home Office & National Crime Agency  
UK resident's browsing History  
EU granted temp adequacy till July 1, 2021
- Spectre POC from Google M1 ?
- DoD supply chain study from congress
- Deep Fake AI "sing with the stars"
- Facetime group 31 random
- Windows 10 printer emergency patch

## Current Issues



- SMS mass messaging & marketing
- Letter of Authorization
- SMS authorization for SMS



**Sakari**



- iPhone

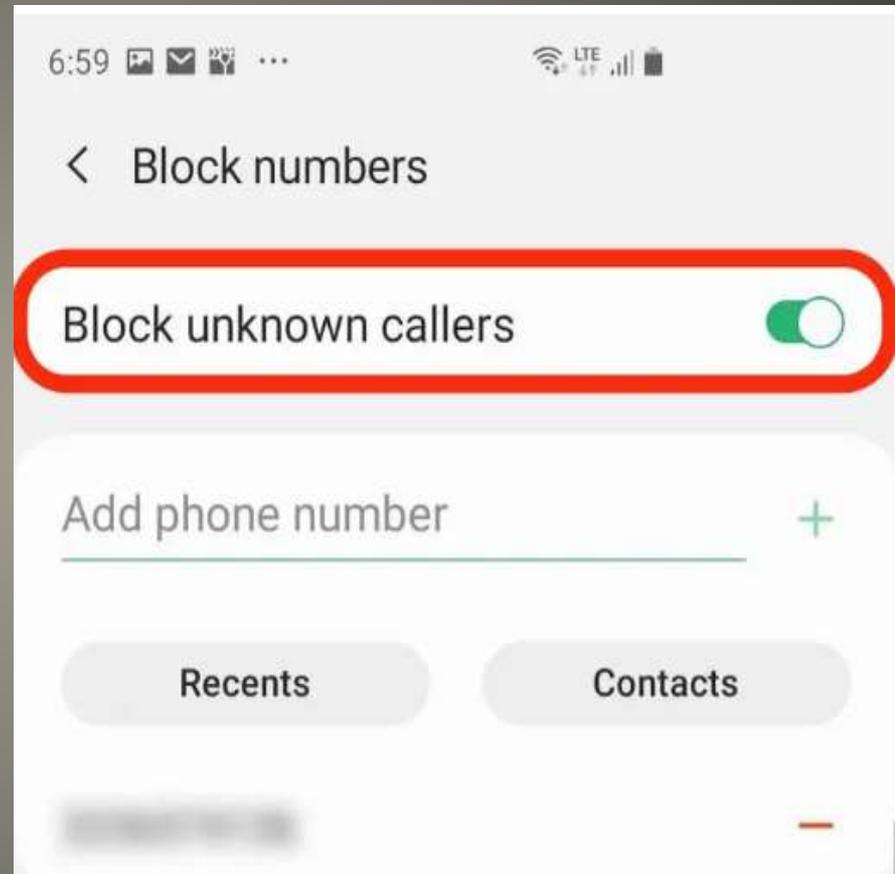
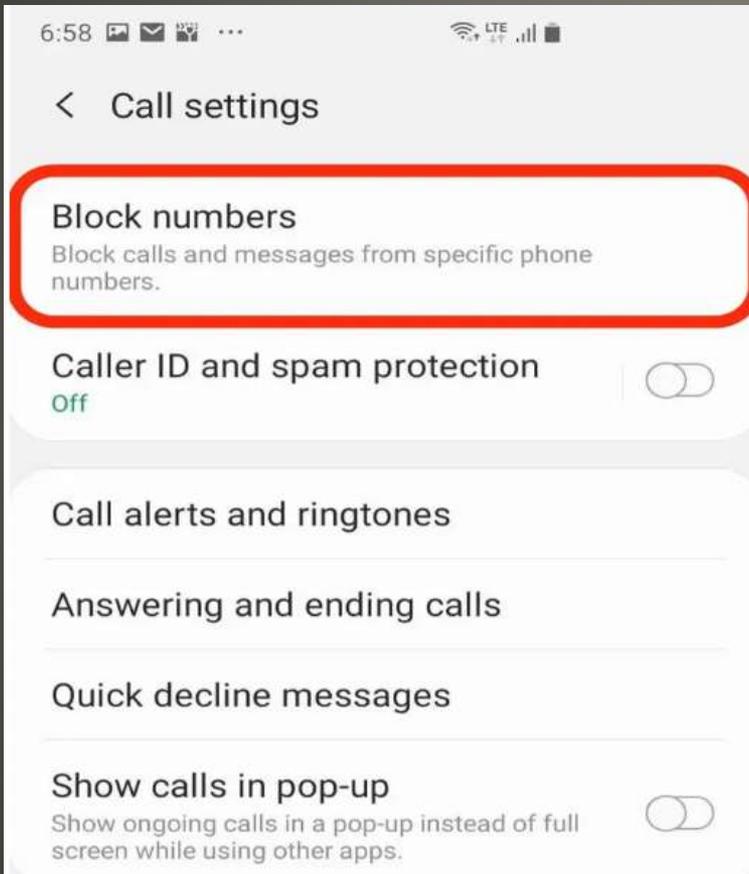
Settings > Phone > Silence Unknown Callers



# Robocalls



# • Android



# Robocalls





**Google Pixel**



- STIR/SHAKEN TRACED Act
- AT&T
  - Check or Manage Voicemail & Features
  - Call Protect
- T-Mobile
  - SCAM ID
    - Dial #ONI# (#664#) + call button
  - Scam Block
    - Dial #ONB# (#662#) + call button

## Major Carriers



- Verizon
  - Call Filter select phone models
  - Call Filter Plus \$2.99/mo.
  - Call Filter App > subscribe
  - Verizon account page
  - My Verizon App
- Suddenlink SPAM ROBO

## Major Carriers



- Nomorobo
- Niya
- Mr. Number
- RoboKiller
- YouMail
- ??
- *Consumer Beware*

## Third Party Apps



Extensions ✕

**Full access**  
These extensions can see and change information on this site.

	Avast Online Security		
	Malwarebytes Browser Guard		

**No access needed**  
These extensions don't need to see and change information on this site.

	Terms of Service; Didn't Read		
---	-------------------------------	---	---

 [Manage extensions](#)

# Browser Extensions



# Lay's Potato Chips: Lay's Crispy Subtitles

## Embed Video

▶ Save for \$5 ▶ Download FREE with PRO membership

Tweet



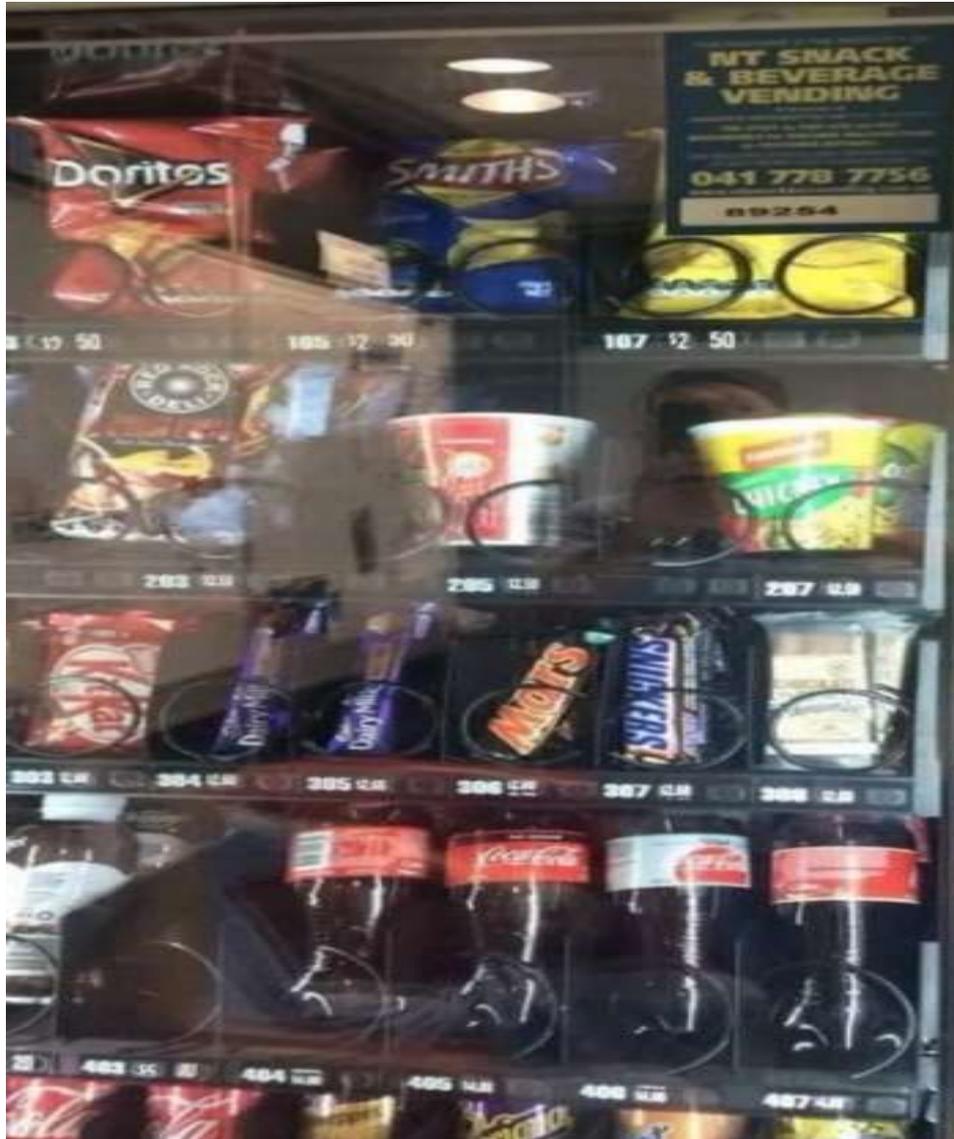
Top 6 this week

In their newest campaign, Lays Potato Chips have released a plug in for Google Chrome that detects the sounds of crunching chips and automatically turns subtitles on for the YouTube video you are watching. Happiness Saigon, an FCB alliance, knew that people love to snack while they're watching their favourite Youtubers, but when you're crunching and munching it can be hard to hear the audio. And Lays is the crispiest chip of all. To solve this problem, and make the video watching experience better for everyone, Crispy Subtitles was the answer. The team trained an AI on 178 hours of crispy chip crunch sounds gathered from around the world, to create a one-of-a-kind plugin which is able to detect and activate subtitles from the second it hears a crunch, so viewers can snack without missing a single thing. This revolution in snacking is available for free on the Google Chrome store globally.

Category	Confectionery & snacks
URL	<a href="https://chrome.google.com/webstore/detail/crispy-subtitles-from-lay/kokpckgbhcmobdddflajfcpmmfhkekn">https://chrome.google.com/webstore/detail/crispy-subtitles-from-lay/kokpckgbhcmobdddflajfcpmmfhkekn</a>
Client	Pepsico
Agency	Happiness Saigon
Production	Bliss Innovative Maker Studio
Country	Vietnam
Uploaded	5 March, 2021

# Browser Extensions





## WARNING

Do not use endoscopy equipment to steal chocolate from this vending machine.

Theft is a crime and next time the Police will be notified.

Theatre Committee

 A photograph of the vending machine's control panel. The panel features a blue overlay with the following text:
 

- 041 77877 56
- www.ntsnaackbev vending.com.au
- Starlight Supporter
- THIS VENDOR IS PROUDLY SUPPLIED AND SERVICED BY YOUR LOCAL SYDIA MEMBER
- Accepts Bills: \$5, \$10, \$20.
- Touch  To Start



- Find My  
Safety Alerts AirTags 3<sup>rd</sup> party devices
- Randomize MAC serial numbers
- Useful Mac Utilities
- Amphetamine

**Apple**





# Welcome to Amphetamine

Created with ♥ by William Gustafson

Amphetamine is a super-awesome, powerful, and flexible keep-awake utility for macOS. Even with all of its features and options, Amphetamine remains incredibly easy to use.

It only takes a few short steps to set up Amphetamine. Click Next to get started.

Don't show this window again

Next





## What does Amphetamine do?

Amphetamine keeps your Mac awake. And its displays. And its drives.

When Amphetamine is keeping your Mac awake it's called a "session." To start a session, click on Amphetamine in the menu bar and select a session duration. Alternatively, right/control click to start a session using the Default Duration. Change the Default Duration in Preferences → Sessions.

If you have a MacBook, and want to keep it awake while its display is closed this is now possible to achieve with Amphetamine. It is highly recommended you install Amphetamine Enhancer as a fail-safe, however.

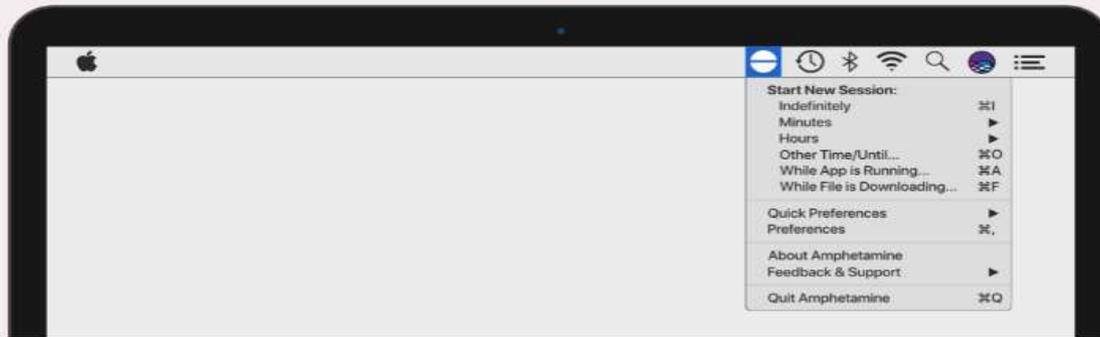
[Click Here to Learn More About Amphetamine Enhancer](#)

Don't show this window again

Previous

Next





## Where is Amphetamine?

Amphetamine lives in the menu bar at the top right corner of your screen.

By default, clicking on Amphetamine in the menu bar will show Amphetamine's menu. Right clicking (or control clicking) will start or stop a keep-awake session. You can switch this behavior if you want.

Amphetamine is highly customizable. You can change all kinds of things like the menu bar image, when notifications should appear, and what sounds to play in Amphetamine's Preferences.

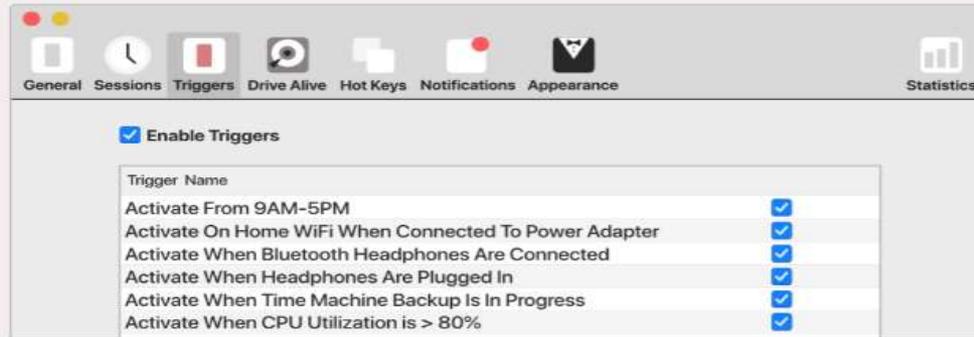
[Click Here to Locate Amphetamine](#)

Don't show this window again

Previous

Next





## What else does Amphetamine do?

Amphetamine can do a lot more than you think.

Triggers automate keeping your Mac awake based on things like its Wi-Fi connection, battery level, USB and Bluetooth device connections, time of the day, running applications, IP address, and much more. Visit Amphetamine's Preferences to set up your first Trigger, or click the button below to learn more.

Drive Alive keeps the drives connected to your Mac awake by periodically writing a tiny amount of data to each drive. Visit Amphetamine's Preferences to set up Drive Alive.

[Click Here to Learn More About Triggers](#)

Don't show this window again

Previous

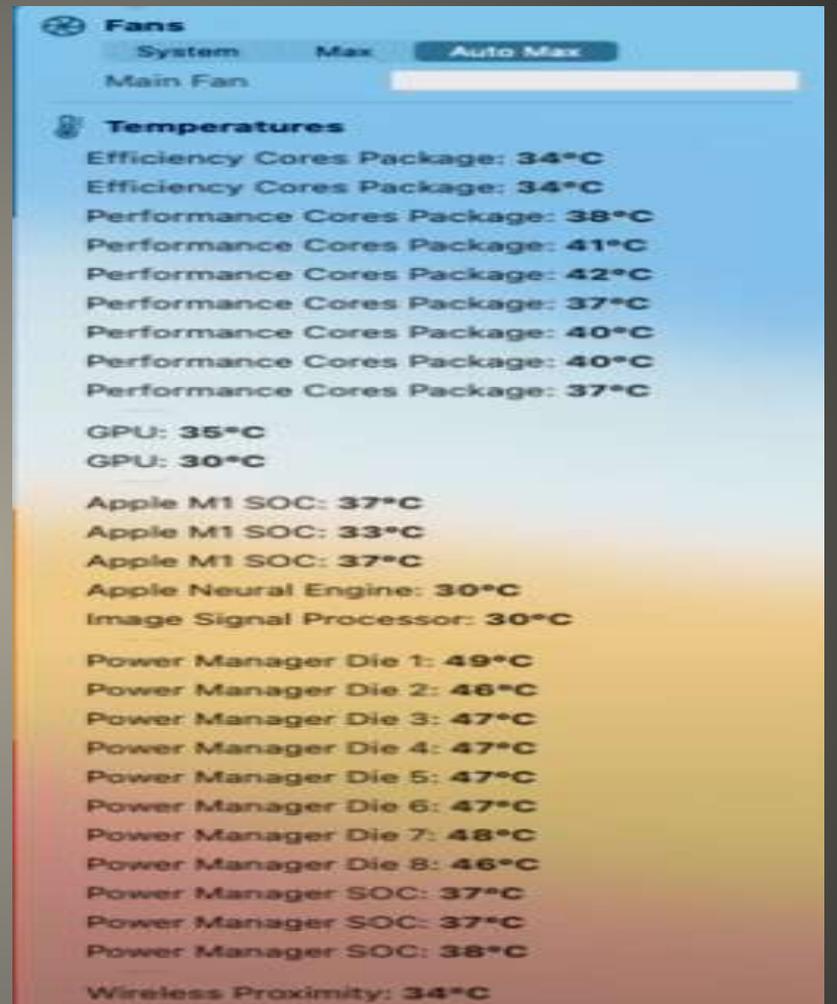
Next



**Your favorite MAC app?**

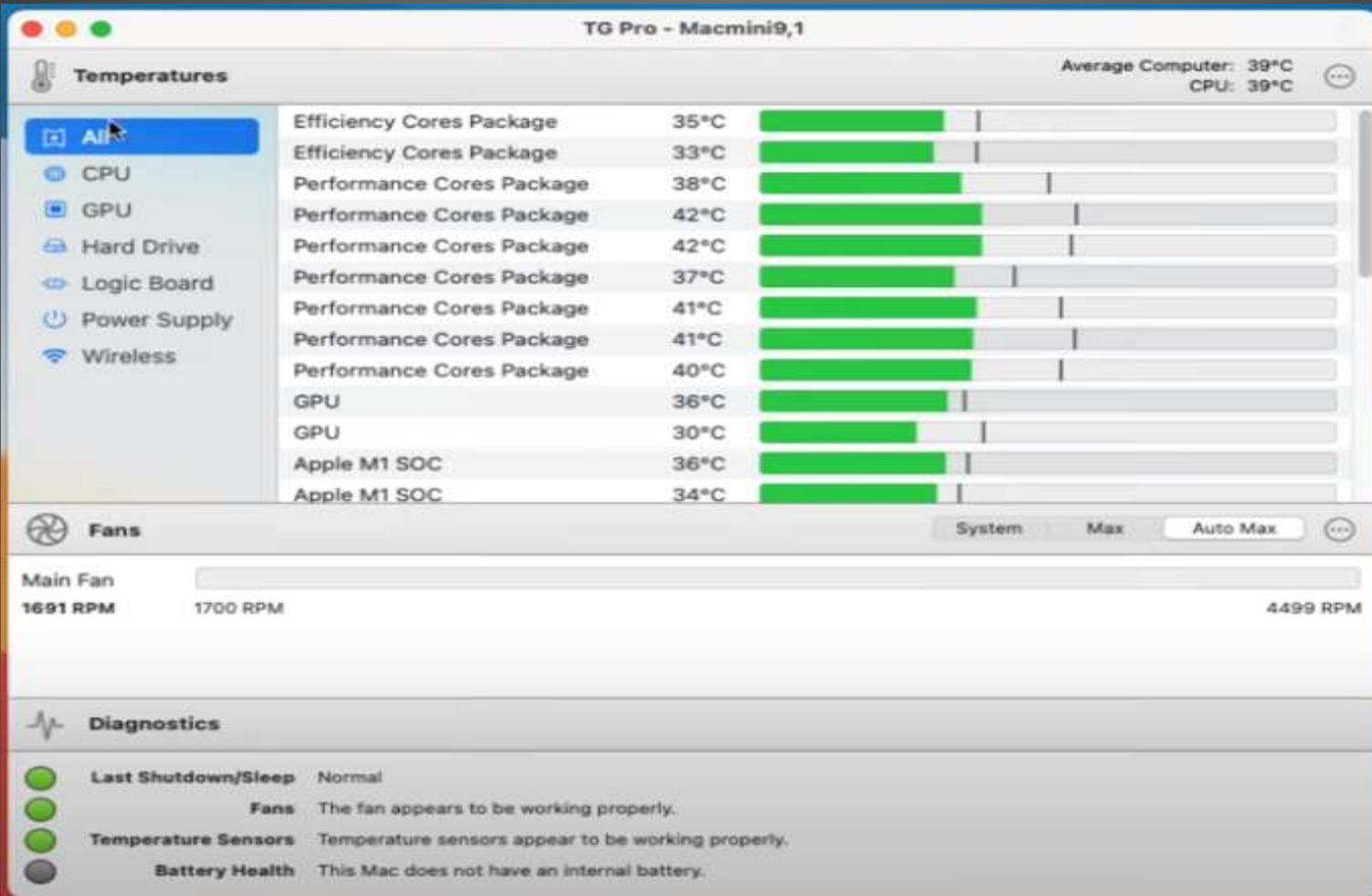


- Rendering on laptop
- Notarized by Apple



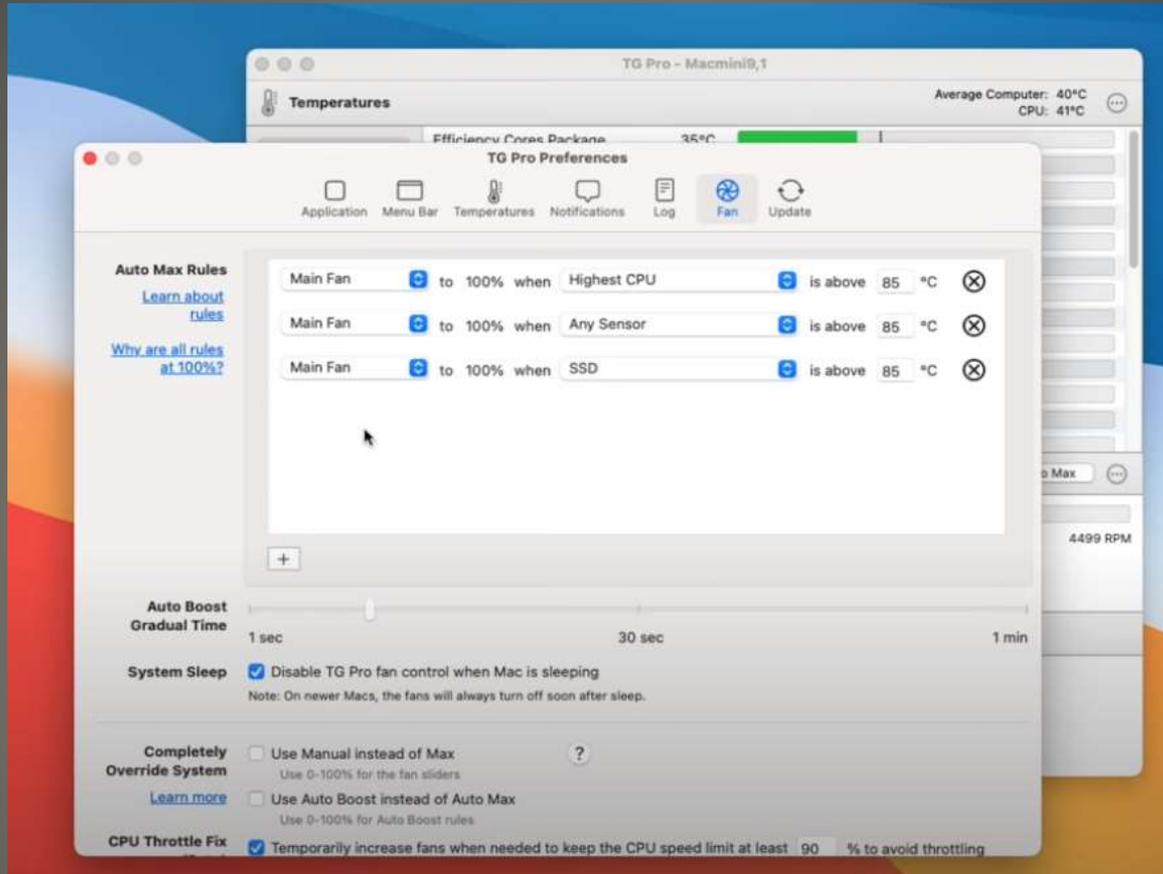
## TG Pro Fan Speed & Temperature





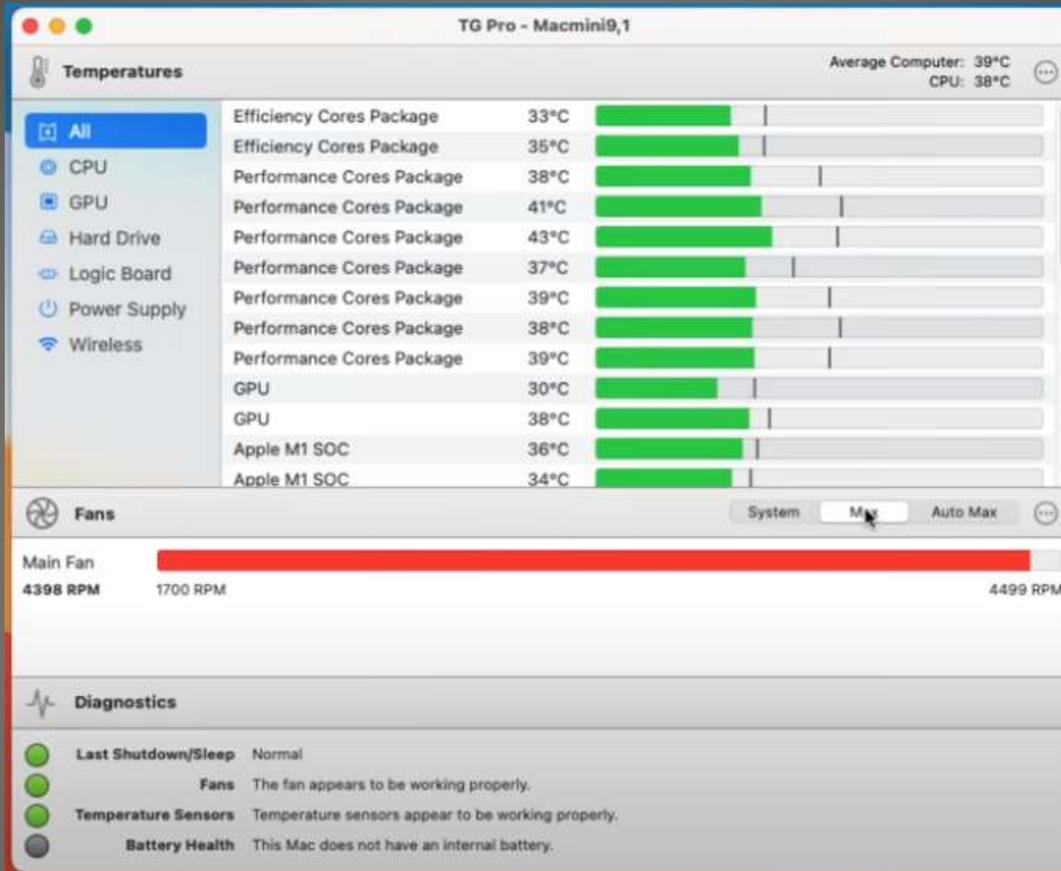
TG Pro





# TG Pro Fan control





# TG Pro





## Hardware turned fan off

This model of Mac will safely turn the fan off when the CPU is running at low capacity.

Once the system turns it back on, fan control in the app will be available.

OK

Do not show this message again



- Fast + Small > Hot
- Roku
- MacBook Lap combustible table top
- First degree burn 118 Fahrenheit

**Global Warming**



### SENSORS

Air Flow Proximity	101°	
Battery Sensor 1	86°	
Battery Sensor 2	87°	
CPU Core 1	120°	
CPU Core 2	118°	
CPU Cores	119°	
CPU Proximity	111°	
CPU System Agent Core	120°	
DDR3 Proximity	102°	
Intel GPU	118°	
Palm Rest	86°	
Palm Rest 2	85°	
Platform Controller Hub PECI	126°	
Right Fin Stack	99°	
SSD	103°	

SSD 100°

Fan 0 rpm

CPU Package Core	1.11 W	
CPU Package GPU	0.07 W	
CPU Package Total	3.65 W	
System Total	15.36 W	

CPU Vcore	1.87 V	
DC In	16.40 V	
PBus	12.62 V	

CPU (CPU, I/O)	0.34 A	
Charger (BMON)	0.37 A	
DC In	0.74 A	
SSD 3.3V	0.01 A	

Ambient Light 0 lx



### SENSORS

Air Flow Proximity	108°	
Battery Sensor 1	86°	
Battery Sensor 2	87°	
CPU Core 1	158°	
CPU Core 2	158°	
CPU Cores	158°	
CPU Proximity	156°	
CPU System Agent Core	158°	
DDR3 Proximity	134°	
Intel GPU	158°	
Palm Rest	87°	
Palm Rest 2	86°	
Platform Controller Hub PECI	171°	
Right Fin Stack	127°	
SSD	112°	

SSD 111°

Fan 3073 rpm

CPU Package Core	0.53 W	
CPU Package GPU	0.04 W	
CPU Package Total	3.09 W	
System Total	11.52 W	

CPU Vcore	1.87 V	
DC In	16.41 V	
PBus	12.62 V	

CPU (CPU, I/O)	0.29 A	
Charger (BMON)	0.38 A	
DC In	0.69 A	
SSD 3.3V	0.02 A	

Ambient Light 0 lx



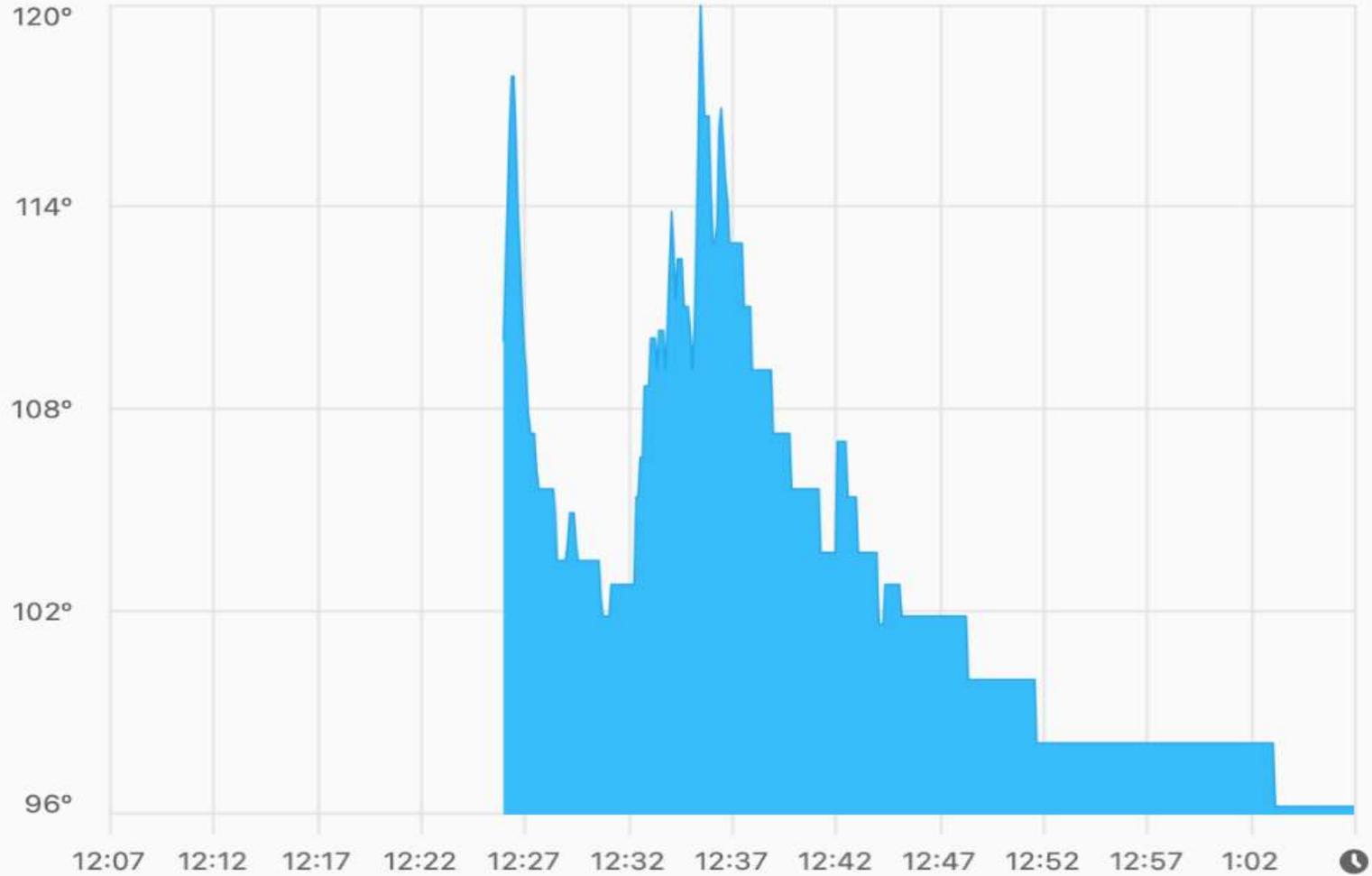
1 Hour

24 Hours

7 Days

30 Days

Hide This Sensor



- Users & Groups -> Login Items

Users & Groups

Search

Current User

Guest User Off

Login Options

Password Login Items

These items will open automatically when you log in:

Item	Kind	Hide
Backup and Sync from Google	Application	<input checked="" type="checkbox"/>
aText	Application	<input checked="" type="checkbox"/>
Spectacle	Application	<input checked="" type="checkbox"/>
ZoomOpener	Unknown	<input type="checkbox"/> ⚠
mInstaller	Application	<input checked="" type="checkbox"/>
Flycut	Application	<input checked="" type="checkbox"/>

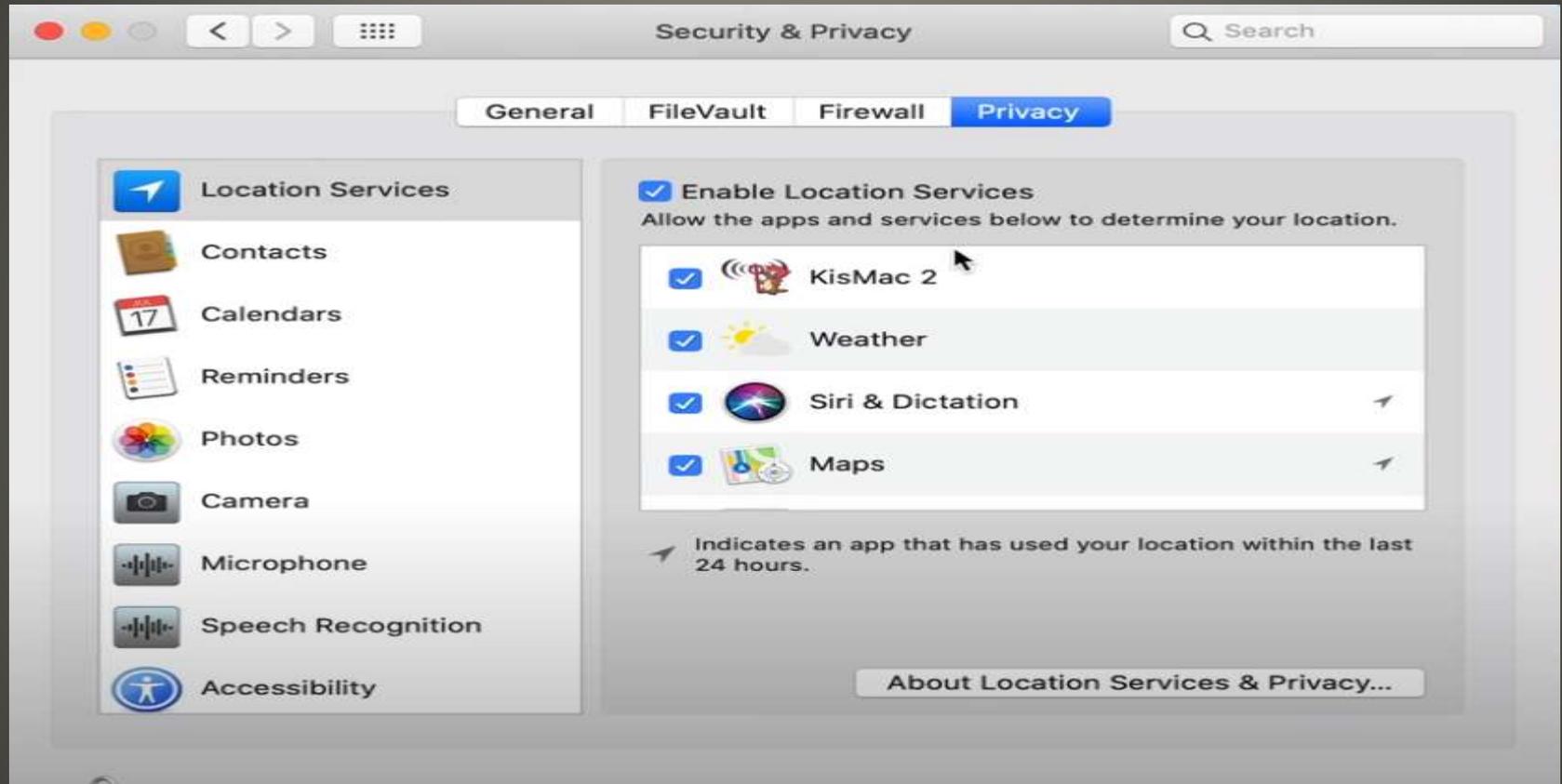
To hide an application when you log in, select the checkbox in the Hide column next to the application.

Click the lock to make changes.

**Unnecessary Login Items**



- Security & Privacy -> Location Services



**Unnecessary Location Services**

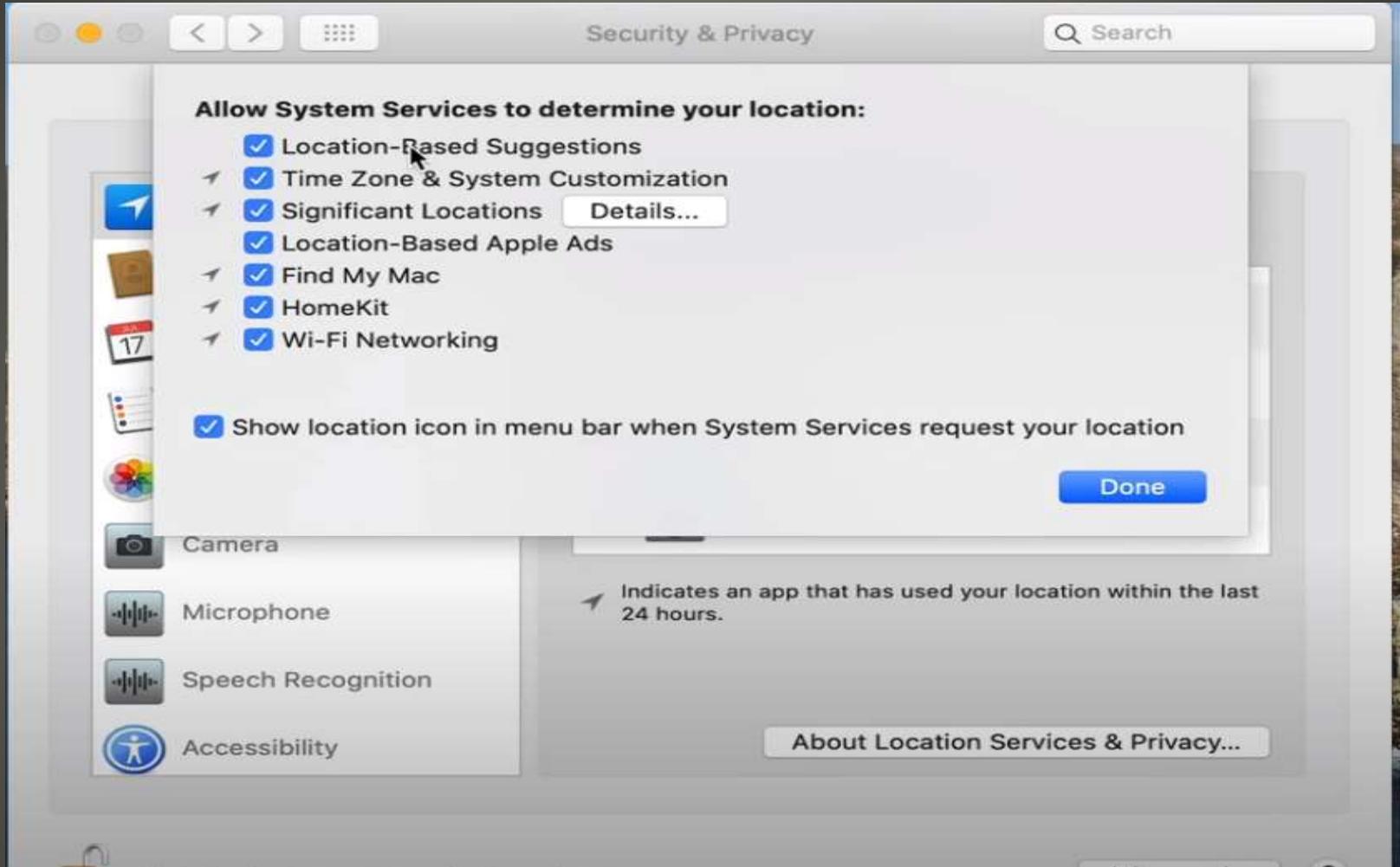


# • Security & Privacy



**Unnecessary System Services**





**Unnecessary System Services**



**Allow System Services to determine your location:**

- Location-Based Suggestions
- Time Zone & System Customization
- Significant Locations [Details...](#)
- Location-Based Apple Ads
- Find My Mac
- HomeKit
- Wi-Fi Networking

Show location icon in menu bar when System Services request your location

[Done](#)

Camera

Microphone

Speech Recognition

Accessibility

Indicates an app that has used your location within the last 24 hours.

[About Location Services & Privacy...](#)

# System Services - Location





# MAC Analytics





# Limit Ad Tracking



## Notifications

Search

Notification Center shows your alerts in the upper-right of your screen, without interrupting what you're doing. Show and hide Notification Center by clicking its icon in the menu bar.



### Do Not Disturb



#### Books

Badges, Sounds, Banners



#### Calendar

Badges, Sounds, Alerts



#### Coda 2

Off



#### Creative Cloud

Off



#### DaisyDisk

Off



#### FaceTime

Badges, Sounds, Banners



#### Final Cut Pro

Badges, Sounds, Alerts



#### Final Cut Pro

Badges, Sounds, Banners

### Turn on Do Not Disturb in Notification Center

Banners and alerts will be hidden and notification sounds will be silenced.



### Turn on Do Not Disturb:

- From: 10:00 PM to: 7:00 AM
- When the display is sleeping
- When the screen is locked
- When mirroring to TVs and projectors

### When Do Not Disturb is turned on:

- Allow calls from everyone
- Allow repeated calls

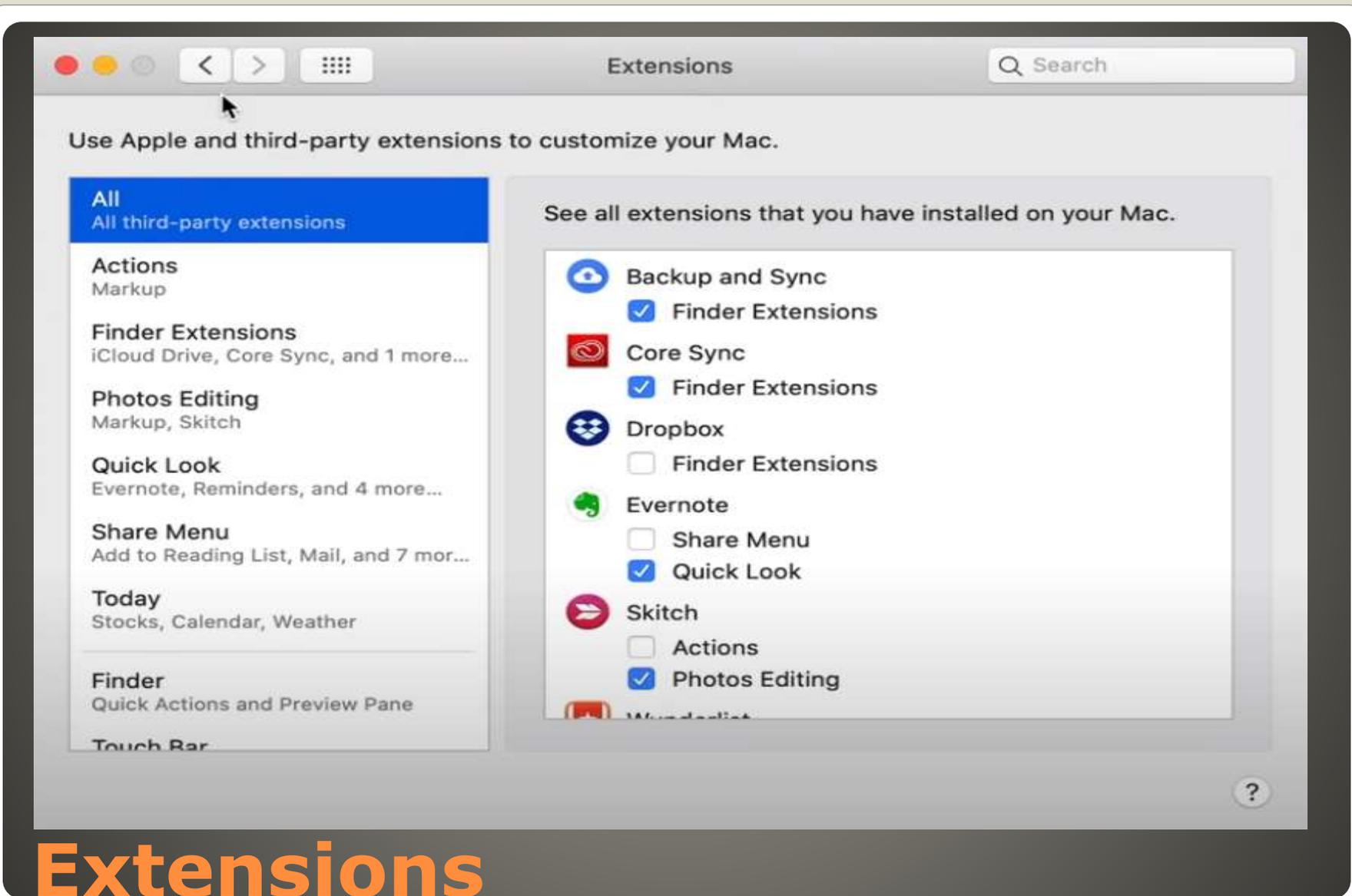
When enabled, a second call from the same person within three minutes will not be silenced.

Notification Center sort order: Recents



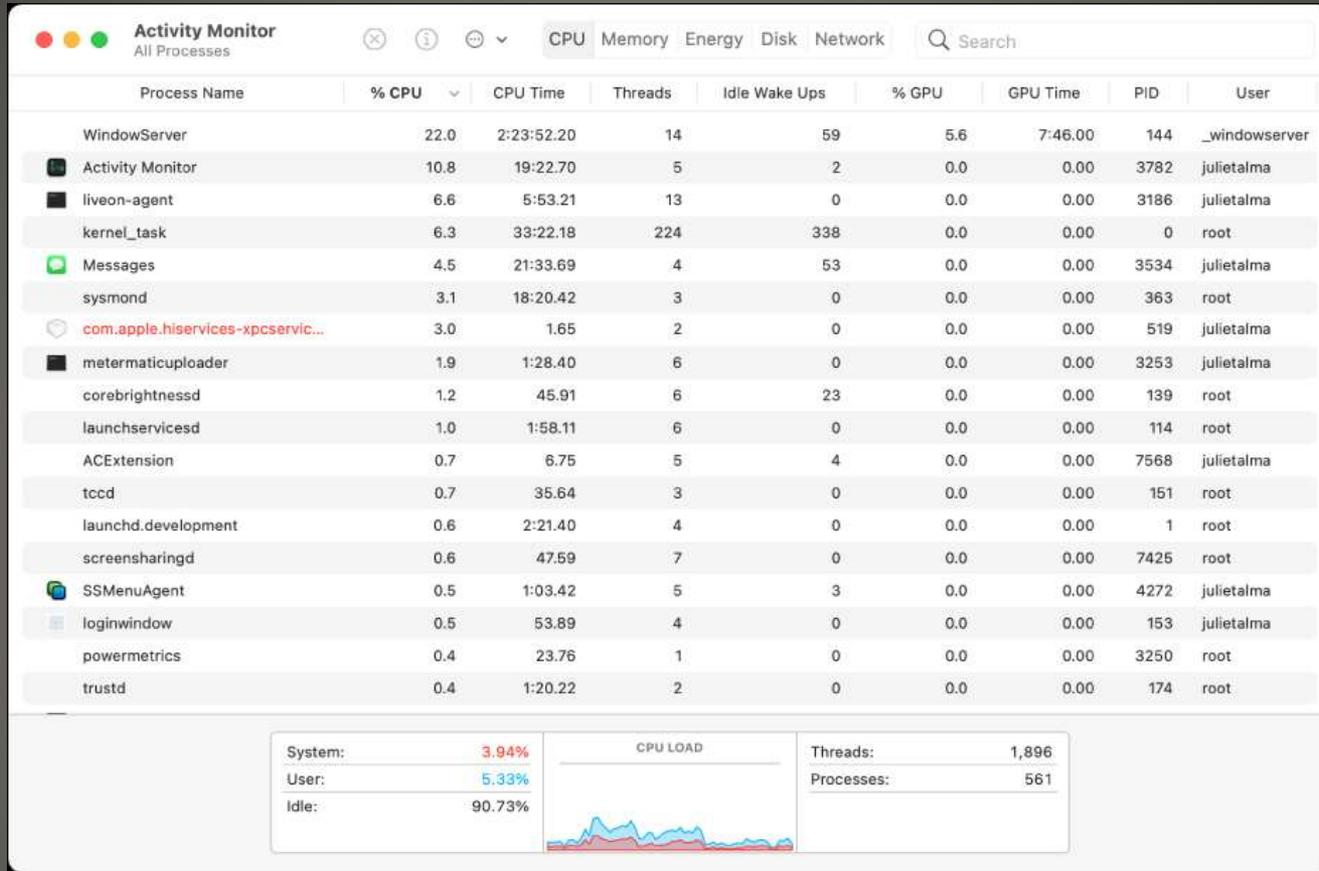
# Notifications zoom





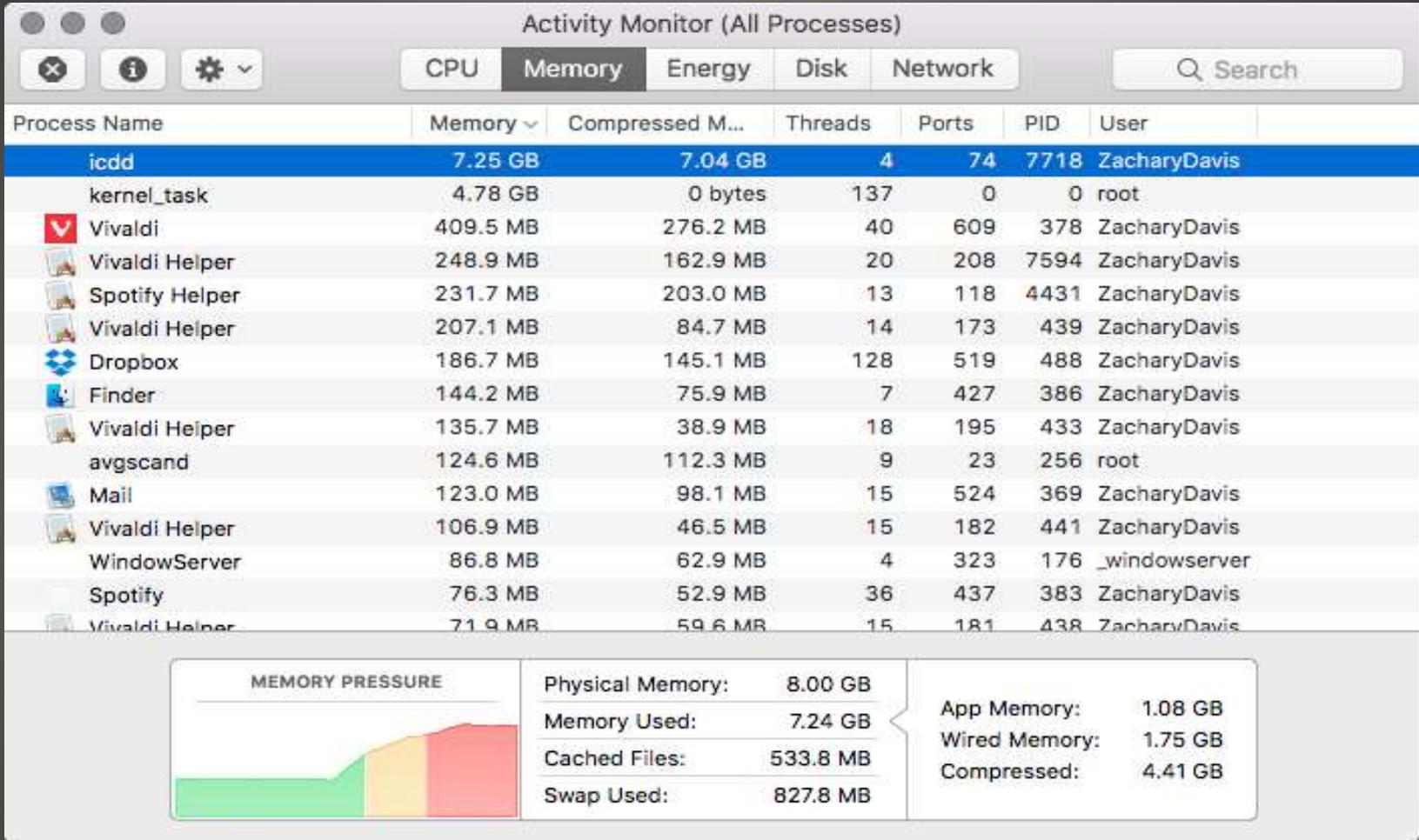
# Extensions





# MacOS Activity Monitor - CPU





# MacOS Activity Monitor - Memory

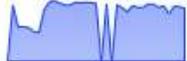


Activity Monitor (Applications in last 8 hours)

CPU | Memory | **Energy** | Disk | Network

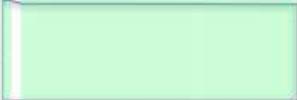
App Name	Energy Impact	Avg Energy Impact	App Nap	Graphics Card	User
Messages	0.0	0.03	Yes	Integrated	zach
Google Chrome	0.3	5.21	Yes	Integrated	zach
System Information	0.0	-	Yes	Integrated	zach
Safari	0.0	1.33	Yes	Integrated	zach
System Preferences	0.0	0.04	Yes	Integrated	zach
Finder	0.0	-	No	Integrated	zach
Activity Monitor	0.3	0.00	No	Integrated	zach
Image Capture Extension	0.0	0.01	No	Integrated	zach
iTunes	0.9	0.98	No	Integrated	zach
Preview	0.0	0.03	No	Integrated	zach
Kerbal Space Program	176.5	0.27	No	High Performan	zach
iTunes Helper	0.0	0.00	No	Integrated	zach
smcFanControl	0.0	0.08	No	Integrated	zach
SlimBatteryMonitor	0.0	0.00	No	Integrated	zach
AppleSpell.service	0.0	0.01	No	Integrated	zach
Time Machine	0.0	0.50	-	-	-
Spotlight	0.0	-	-	-	-

ENERGY IMPACT



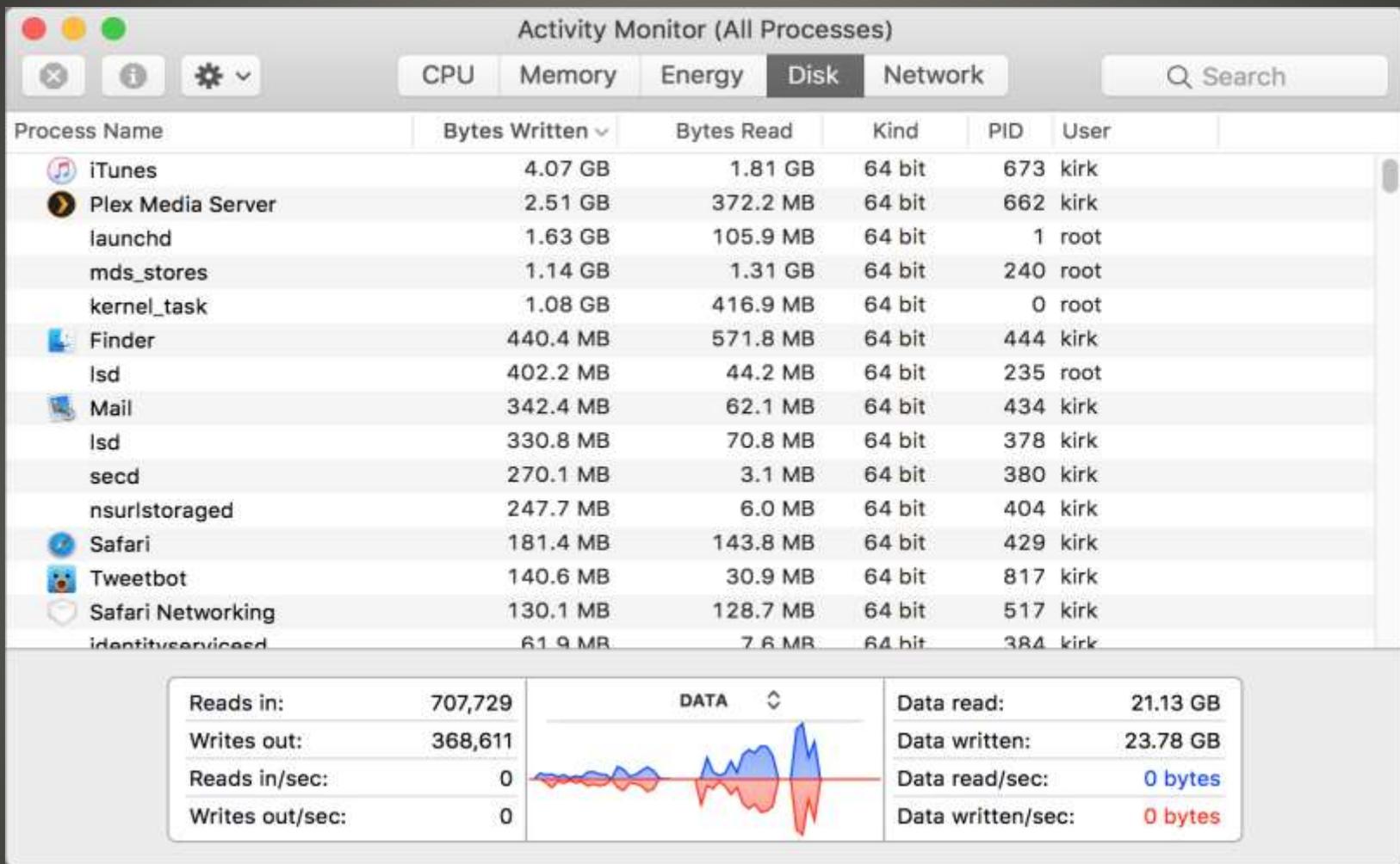
Graphics Card:	High Perf.
Remaining charge:	95%
Battery Is Charged	
Time on AC:	4:08

BATTERY (Last 12 hours)



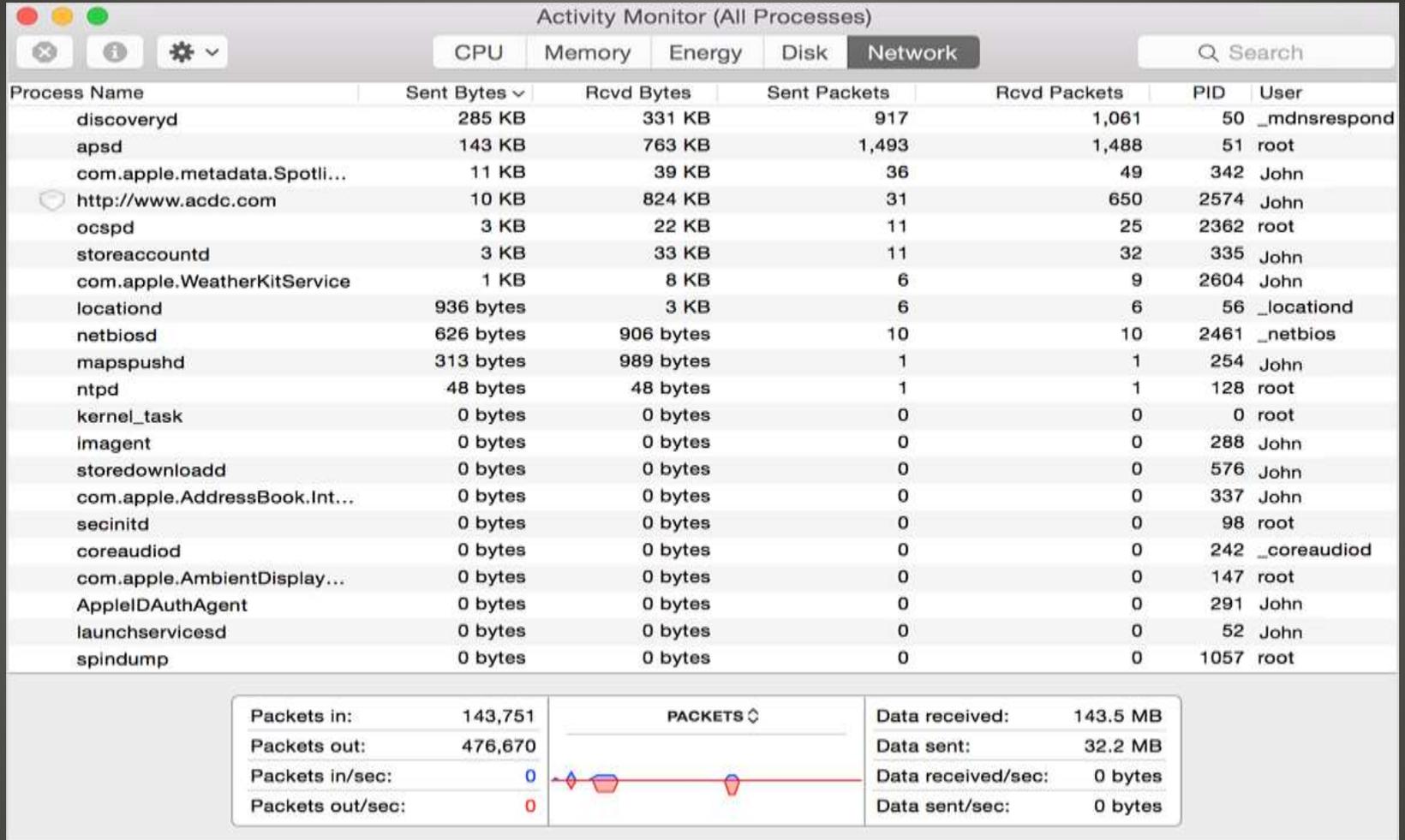
# MacOS Activity Monitor - Energy





# MacOS Activity Monitor - Disk





# MacOS Activity Monitor - Network



The screenshot shows the macOS Activity Monitor window with the 'CPU' tab selected. The main table lists various processes with columns for Process Name, % CPU, CPU Time, Threads, and Idle Wake Ups. A context menu is open over the table, showing a list of columns that can be added to the view. The bottom of the window displays system statistics and a CPU load graph.

Process Name	% CPU	CPU Time	Threads	Idle Wake Ups
photoanalysisd	97.8	59:13:36.59	5	0
Activity Monitor	9.9	1:10.08	6	2
CoreServicesUIAgent	9.5	22.72	4	0
WindowServer	6.6	3:57:31.24	8	17
logd	4.2	4:41:39.34	4	0
App Store	3.9	11:25.01	26	90
fseventsd	3.7	4:08:14.71	12	29
kernel_task	3.2	20:14:13.72	188	351
coreaudiod	2.7	29:07.17	9	87
Microsoft Word	2.6	1:48:49.32	15	12
hidd	1.3	1:44:41.73	6	0
mds_stores	1.1	2:10:00.76	7	0
mds	1.0	1:49:52.23	9	26
Firefox	1.0	1:12:46.03	70	1
launchservicesd	0.8	14:16.87	4	0
sysmond	0.8	27.37	3	0
photolibraryd	0.7	17.75	3	0
bluetoothd	0.4	47:52.63	4	0
Google Chrome Helper	0.4	12:03.22	10	2
Google Chrome	0.3	44:21.02	33	1
FirefoxCP Web Content	0.3	21.82	35	6
Google Chrome Helper (Renderer)	0.3	28.91	16	2

- Process ID
- User
- % CPU
- CPU Time
- % GPU
- GPU Time
- # Threads
- # Ports
- Real Memory
- Real Private Memory
- Real Shared Memory
- Sudden Termination
- Sandbox
- Restricted
- Idle Wake Ups
- Energy Impact
- App Nap
- Sent Bytes
- Sent Packets
- Received Bytes
- Received Packets
- Purgeable Memory
- Memory
- Compressed Memory
- Bytes Written
- Bytes Read
- Preventing Sleep

System: 4.76%  
 User: 15.00%  
 Idle: 80.23%

CPU LOAD

Threads:  
Processes

# MacOS Activity Monitor – add columns





```

john — top — 103x34
Processes: 472 total, 3 running, 2 stuck, 467 sleeping, 1501 threads
Load Avg: 5.58, 3.63, 3.16 CPU usage: 23.20% user, 15.7% sys, 61.72% idle
SharedLibs: 389M resident, 48M data, 29M linkedit.
MemRegions: 43668 total, 1440M resident, 137M private, 562M shared.
PhysMem: 6322M used (1648M wired), 1869M unused.
VM: 2388G vsize, 2317M framework vsize, 271926(0) swapins, 295277(0) swapouts.
Networks: packets: 411135/281M in, 202446/35M out. Disks: 1792147/23G read, 964493/13G written.

PID    COMMAND      %CPU TIME    #TH    #WQ    #PORT MEM    PURG    CMPRS    PGRP    PPID    STATE
70     RTProtection 99.3 38:59.44 7/1    5/1    105    35M     0B      3100K    70     1     running
141    WindowServer 14.0 23:32.79 12     5      1048   629M-   20M     42M-    141    1     sleeping
0      kernel_task  11.7 14:26.47 186/4  0      0      150M+   0B      0B      0      0     running
21123  screencaptur 10.4 00:00.36 4      2      170+   7120K+  12K     0B      21123  1     sleeping
21111  top           3.9  00:01.71 1/1    0      34     4204K   0B      0B      21111  21094 running
369    backupd      2.5  09:10.23 6      5      1165   13M     0B      1564K   369    1     stuck
8993   gamecontroll 1.7  00:14.15 5      4      61     1488K   0B      416K    8993   1     sleeping
21122  screencaptur 1.1  00:00.13 3      2      54     2148K+  0B      0B      1389   1389  sleeping
86     logd         1.1  01:13.28 4      3      1477   4596K   0B      200K    86     1     sleeping
486    suggestd    0.9  00:14.48 6      5      350-   12M-    2368K   3224K   486    1     sleeping
8856   iStat Menus 0.7  17:22.37 4      2      288+   27M-    2988K   8680K   8856   1     sleeping
21091  Terminal    0.6  00:02.20 8      3      219    28M     6220K   0B      21091  1     sleeping
1      launchd     0.2  03:22.08 4      3      5382   27M     0B      12M     1      0     stuck
96     mds         0.1  34:58.18 7      4      452    24M+   0B      5588K   96     1     sleeping
8851   iStatMenusHe 0.1  05:55.21 5      4      507    11M     0B      860K    8851   1     sleeping
81     powerd      0.1  00:26.65 4      3      131    1612K   0B      208K    81     1     sleeping
370    mds_stores  0.1  10:49.49 6      4      104    43M-    15M     16M     370    1     sleeping
79     configd     0.1  00:03.48 7      1      455+   2564K   0B      472K    79     1     sleeping
407    cfprefsd    0.1  00:27.88 4      3      458    1232K   296K    100K    407    1     sleeping
132    notifyd    0.1  00:25.69 2      1      631    1588K   0B      132K    132    1     sleeping
106    contextstore 0.1  00:15.69 3      2      130+   3664K+  320K    1116K   106    1     sleeping
136    AirPlayXPCh 0.0  03:04.30 8      4      167    1844K   0B      860K    136    1     sleeping
73     fseventsds 0.0  00:47.72 10     1      255    2580K   0B      256K    73     1     sleeping
1390   Finder      0.0  00:56.87 6      3      420    59M     1972K   14M     1390   1     sleeping
222    usbd        0.0  00:00.11 2      1      49     872K+   0B      388K    222    1     sleeping

```

# Linux commands in terminal app



- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Chicken Little  
Tortoise & Hare

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes  
Cyber Security SIG meetings, NEWSBLOG  
Internet

- Questions, suggestions, comments?

**SCCCCyber@gmail.com**



QUESTIONS ?

