Sun City Computer Club

Cyber Security SIG

December 16, 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

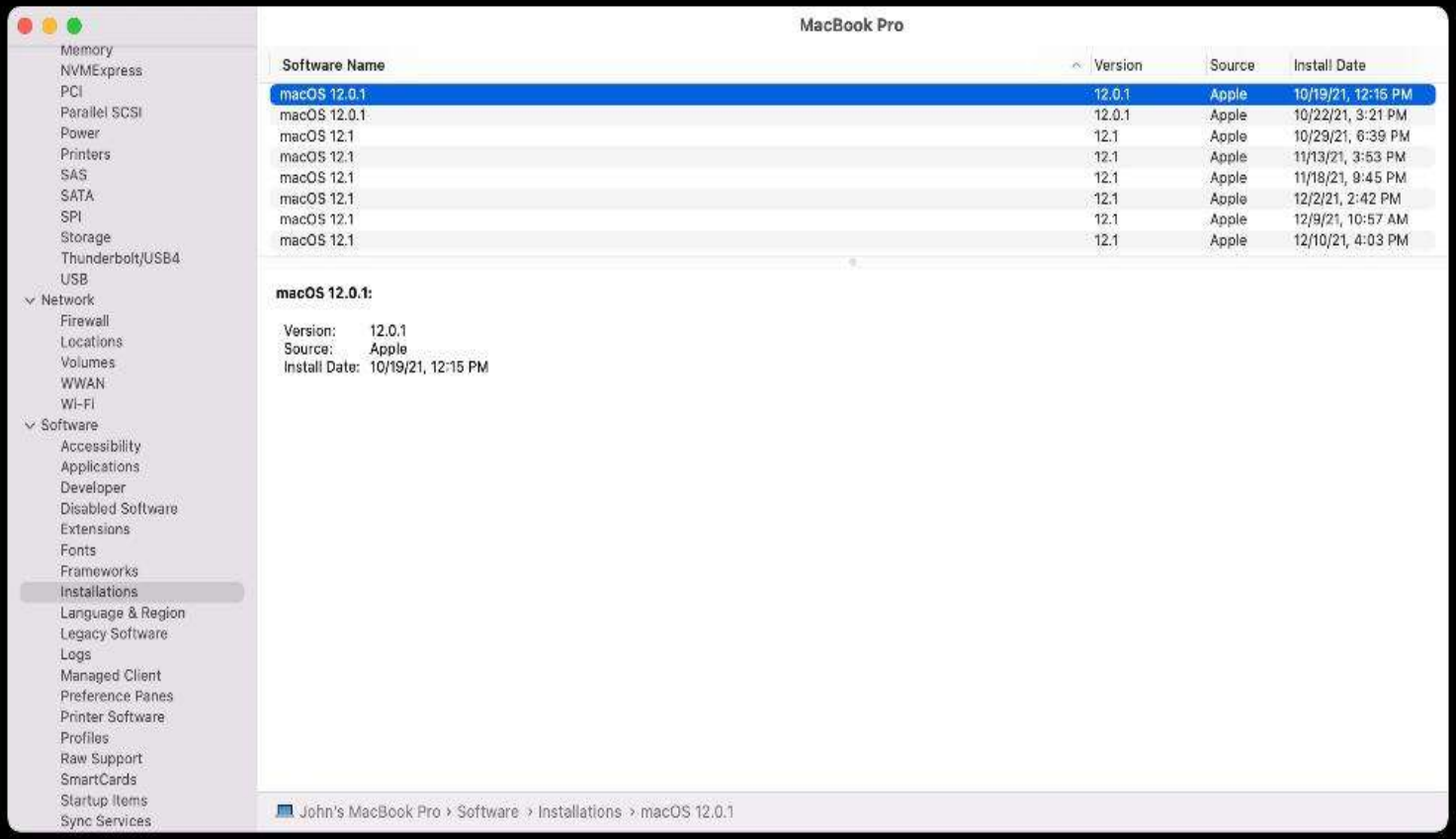
SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

- Ever want to be a presenter??

Presenter???

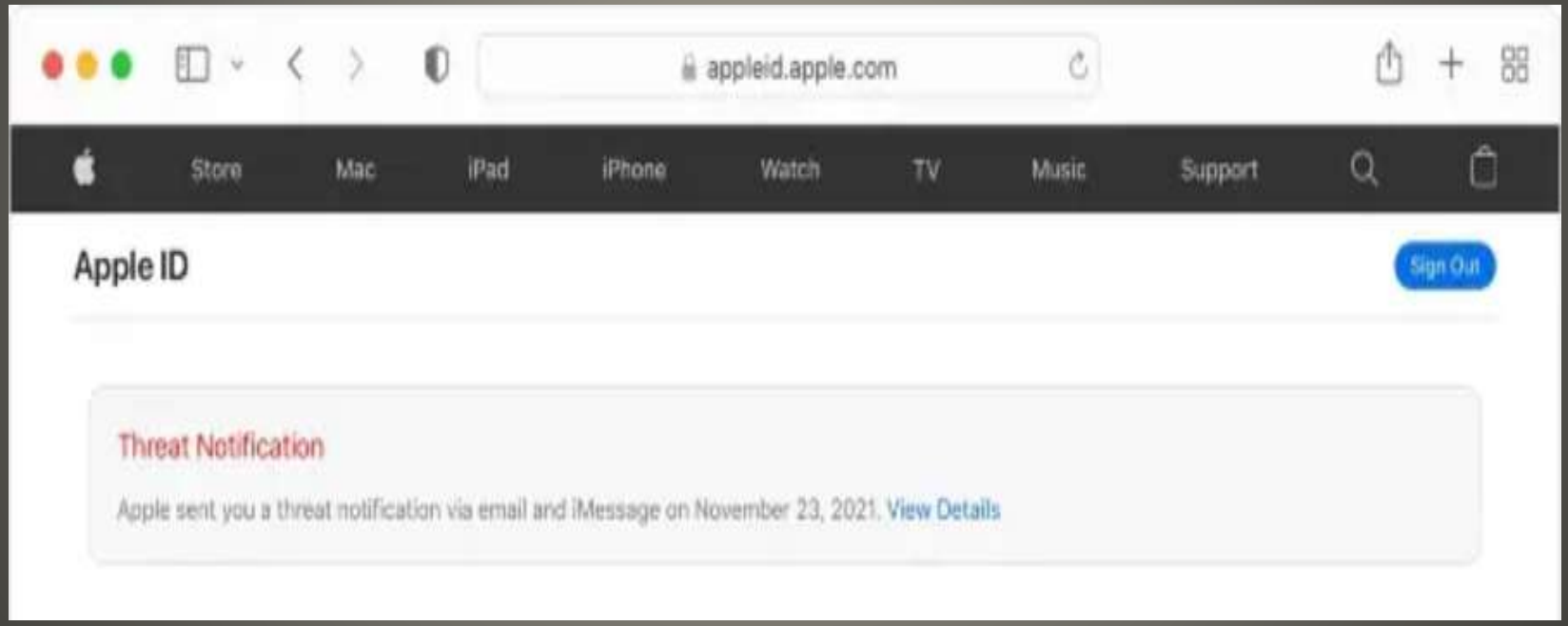
Current Issues

- Sun City NextDoor warning
  Error message call 1-888-822-5161
  $100 gift card AND prompt service (??)
  just $4.95 credit card number please
- Apple AirTags & high-end auto thefts
  Pay attention to AirTag alerts
  High end auto home relay
  Tracker Detect
  Pay attention Faraday cage
- Cox Communications data breach
- ChromeOS update 96.0.446.110
- Zoom 5.8.7 Update speed Fast/Slow
- Windows Default Browser Edge
  scheme Microsoft-edge://
- Monterey


MacBook Pro
Memory
NVMExpress
PCI
Parallel SCSI
Power
Printers
SAS
SATA
SPI
Storage
Thunderbolt/USB4
USB
Network
Firewall
Locations
Volumes
WWAN
Wi-Fi
Software
Accessibility
Applications
Developer
Disabled Software
Extensions
Fonts
Frameworks
Installations
Language & Region
Legacy Software
Logs
Managed Client
Preference Panes
Printer Software
Profiles
Raw Support
SmartCards
Startup Items
Sync Services
Software Name
Version
Source
Install Date
macOS 12.0.1 12.0.1 Apple 10/19/21, 12:15 PM
macOS 12.0.1 12.0.1 Apple 10/22/21, 3:21 PM
macOS 12.1 12.1 Apple 10/29/21, 6:39 PM
macOS 12.1 12.1 Apple 11/13/21, 3:53 PM
macOS 12.1 12.1 Apple 11/18/21, 9:45 PM
macOS 12.1 12.1 Apple 12/2/21, 2:42 PM
macOS 12.1 12.1 Apple 12/9/21, 10:57 AM
macOS 12.1 12.1 Apple 12/10/21, 4:03 PM
macOS 12.0.1:
Version: 12.0.1
Source: Apple
Install Date: 10/19/21, 12:15 PM
John's MacBook Pro › Software › Installations › macOS 12.0.1

Monterey

- Not perfect
- Detected on US diplomat's devices



Apple Pegasus Alert

Current Issues

- Smartwatches for children
  Updater with capability to load
  Android.Downloader.812.origin
  Android.Downloader.1049.origin
  Features: track wearer's location & route
  make & answer phone & video calls
  receive SMS & voice mail
  take pictures
  listen to surroundings
  Vendors servers with parents account access

Russia banned VPN services

- Hola! VPN, ExpressVPN, KeepSolid VPN unlimited, Nord VPN, Speedify VPN, IPVanish VPN, VyprVPN, Opera VPN, ProtonVPN, Betternet, Lantern, X-VPN, Cloudflare WARP, Tachyon VPN, PrivateTunnel
- Refusal to comply with Russian regulations

Current Issues

- Microsoft Edge tug-o-war
- Botnet using Bitcoin blockchain

  Glupteba botnet

  1000 new infections daily

  modern borderless technological embodiment of organized crime

  theft of Google users' credentials and data, mining of cryptocurrencies, sets up proxies to funnel traffic

VERY DIFFICULT TO DISRUPT

Current Issues

- HP printer vulnerabilities
  Print a formatted page
    wormable exploit
  USB - needs physical access
- Xsinator
  14 new types cross-site data leakage
  allowing controlled websites to harvest data from site visitors
  violate browser same-origin policies
  Usefulness – e.g. hotel site with map and/or public transport

BUT web site can use go-no go search of users Gmail inbox

https://xsinator.com/

0	Performance API Error Leak	Detect errors with Performance API.
1	Event Handler Leak [Object]	Detect errors with onload/onerror with object.
2	Event Handler Leak [Stylesheet]	Detect errors with onload/onerror with stylesheet.
3	Event Handler Leak [Script]	Detect errors with onload/onerror with script.
4	MediaError Leak	Detect status codes with MediaError message.
5	Style Reload Error Leak	Detect errors with style reload bug.
6	Request Merging Error Leak	Detect errors with request merging.
7	CORS Error Leak	Leak redirect target URL with CORS error.
8	Redirect Start Leak	Detect cross-origin HTTP redirects by checking redirectStart time.
9	Duration Redirect Leak	Detect cross-origin redirects by checking the duration.
10	Fetch Redirect Leak	Detect HTTP redirects with fetch API.
11	URL Max Length Leak	Detect server redirect by abusing URL max length.
12	Max Redirect Leak	Detect server redirect by abusing max redirect limit.
13	History Length Leak	Detect javascript redirects with History API.
14	CSP Violation Leak	Leak cross-origin redirect target with CSP violation event.
15	CSP Redirect Detection	Detect cross-origin redirects with CSP violation event.
16	WebSocket Leak [FF]	Detect the number of websockets on a page by exceeding the socket limit.
17	WebSocket Leak [GC]	Detect the number of websockets on a page by exceeding the socket limit.
18	Payment API Leak	Detect if another tab is using the Payment API.
19	Frame Count Leak	Detect the number of iframes on a page.
20	Media Dimensions Leak	Leak dimensions of images or videos.
21	Media Duration Leak	Leak duration of audio or videos.
22	Performance API Empty Page Leak	Detect empty responses with Performance API.
23	Performance API XSS Auditor Leak	Detect script/event handlers in a page with Performance API.
24	Cache Leak (CORS)	Detect resources loaded by page. Cache is deleted with CORS error.
25	Cache Leak (POST)	Detect resources loaded by page. Cache is deleted with a POST request.
26	Id Attribute Leak	Leak id attribute of focusable HTML elements with onblur.
27	CSS Property Leak	Leak CSS rules with getComputedStyle.
28	SRI Error Leak	Leak content length with SRI error.
29	ContentDocument X-Frame Leak	Detect X-Frame-Options with contentDocument.
30	Performance API X-Frame Leak	Detect X-Frame-Options with Performance API.
31	Performance API CORP Leak	Detect Cross-Origin-Resource-Policy header with Performance API.
32	CORP Leak	Detect Cross-Origin-Resource-Policy header with fetch.
33	CORB Leak	Detect X-Content-Type-Options in combination with specific content-type using CORB.
34	Download Detection	Detect downloads [Content-Disposition header].
35	Performance API Download Detection	Detect downloads [Content-Disposition header] with Performance API.
36	CSP Directive Leak	Detect CSP directives with CSP iframe attribute.
37	COOP Leak	Detect Cross-Origin-Opener-Policy header with popup.

Exploitable Safe Not Applicable Loading

UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0

#	XS-Leak	Description
0	Performance API Error Leak	Detect errors with Performance API.
1	Event Handler Leak (Object)	Detect errors with onload/onerror with object.
2	Event Handler Leak (Stylesheet)	Detect errors with onload/onerror with stylesheet.
3	Event Handler Leak (Script)	Detect errors with onload/onerror with script.
4	MediaError Leak	Detect status codes with MediaError message.
5	Style Reload Error Leak	Detect errors with style reload bug.
6	Request Merging Error Leak	Detect errors with request merging.
7	CORS Error Leak	Leak redirect target URL with CORS error.
8	Redirect Start Leak	Detect cross-origin HTTP redirects by checking redirectStart time.
9	Duration Redirect Leak	Detect cross-origin redirects by checking the duration.
10	Fetch Redirect Leak	Detect HTTP redirects with Fetch API.
11	URL Max Length Leak	Detect server redirect by abusing URL max length.
12	Max Redirect Leak	Detect server redirect by abusing max redirect limit.
13	History Length Leak	Detect javascript redirects with History API.
14	CSP Violation Leak	Leak cross-origin redirect target with CSP violation event.
15	CSP Redirect Detection	Detect cross-origin redirects with CSP violation event.
16	WebSocket Leak (FF)	Detect the number of websockets on a page by exausting the socket limit.
17	WebSocket Leak (GC)	Detect the number of websockets on a page by exausting the socket limit.
18	Payment API Leak	Detect if another tab is using the Payment API.
19	Frame Count Leak	Detect the number of iframes on a page.
20	Media Dimensions Leak	Leak dimensions of images or videos.
21	Media Duration Leak	Leak duration of audio or videos.
22	Performance API Empty Page Leak	Detect empty responses with Performance API.
23	Performance API XSS Auditor Leak	Detect scripts/event handlers in a page with Performance API.
24	Cache Leak (CORS)	Detect resources loaded by page. Cache is deleted with CORS error.
25	Cache Leak (POST)	Detect resources loaded by page. Cache is deleted with a POST request.
26	Id Attribute Leak	Leak id attribute of focusable HTML elements with onblur.
27	CSS Property Leak	Leak CSS rules with getComputedStyle.
28	SRI Error Leak	Leak content length with SRI error.
29	ContentDocument X-Frame Leak	Detect X-Frame-Options with ContentDocument.
30	Performance API X-Frame Leak	Detect X-Frame-Options with Performance API.
31	Performance API CORP Leak	Detect Cross-Origin-Resource-Policy header with Performance API.
32	CORP Leak	Detect Cross-Origin-Resource-Policy header with fetch.
33	CORB Leak	Detect X-Content-Type-Options in combination with specific content type using CORB.
34	Download Detection	Detect downloads (Content-Disposition header).
35	Performance API Download Detection	Detect downloads (Content-Disposition header) with Performance API.
36	CSP Directive Leak	Detect CSP directives with CSP iframe attribute.
37	COOP Leak	Detect Cross-Origin-Opener-Policy header with popup.

Export Results Clear Results

Mitigations

- UPDATE Update update
- Fit for purpose
- More secure eMail platforms
- More secure browsers
- More secure browser profiles
- Awareness Preparedness Understanding

eMail apps

- Claws Mail
  lightweight, fast, user-friendly
- The Bat!
  No free versions
- Kiwi for Gmail
- TouchMail

Your recommendations?

- Verizon Selects -> Verizon Custom Experience Plus
- Opt out before? Need to Opt out yet again

As a Verizon Selects participant, you will automatically be included in the Custom Experience Plus and Custom Experience programs.

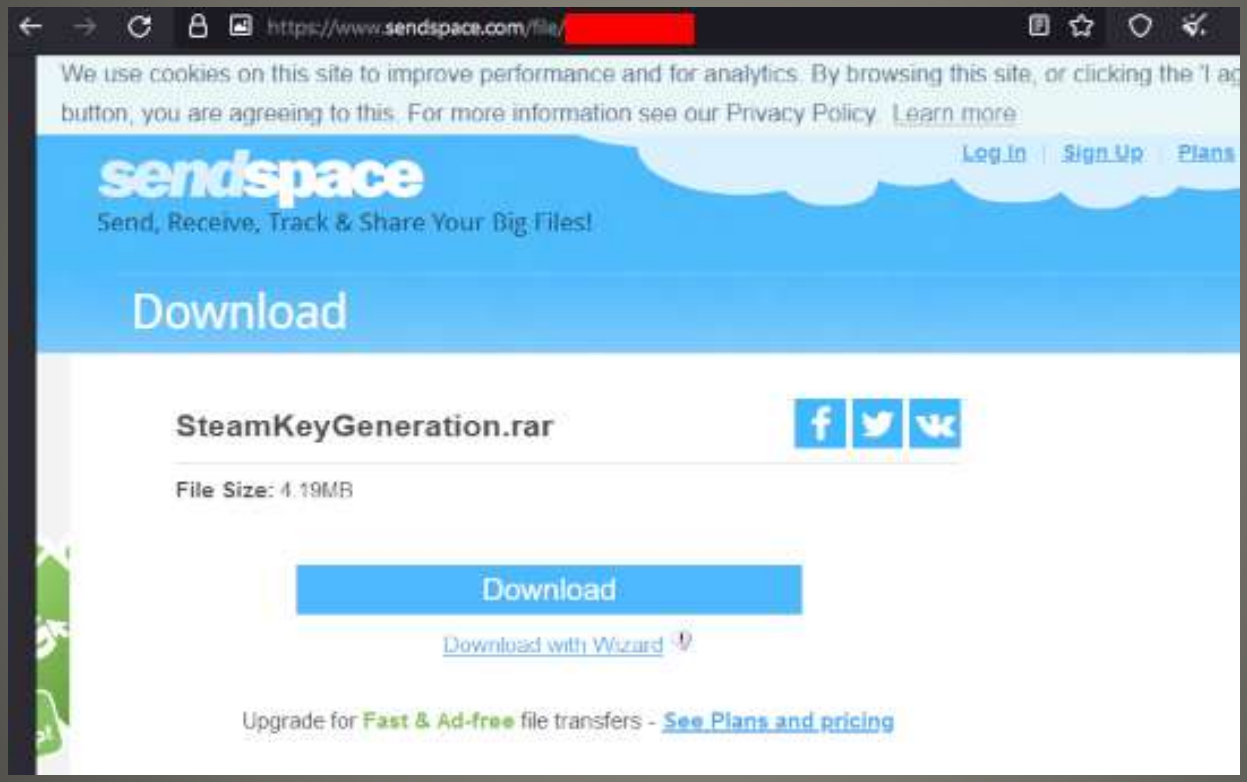
If you recently opted out of participating in Verizon Selects, you will still be included in the Custom Experience program unless you opt out.

Verizon

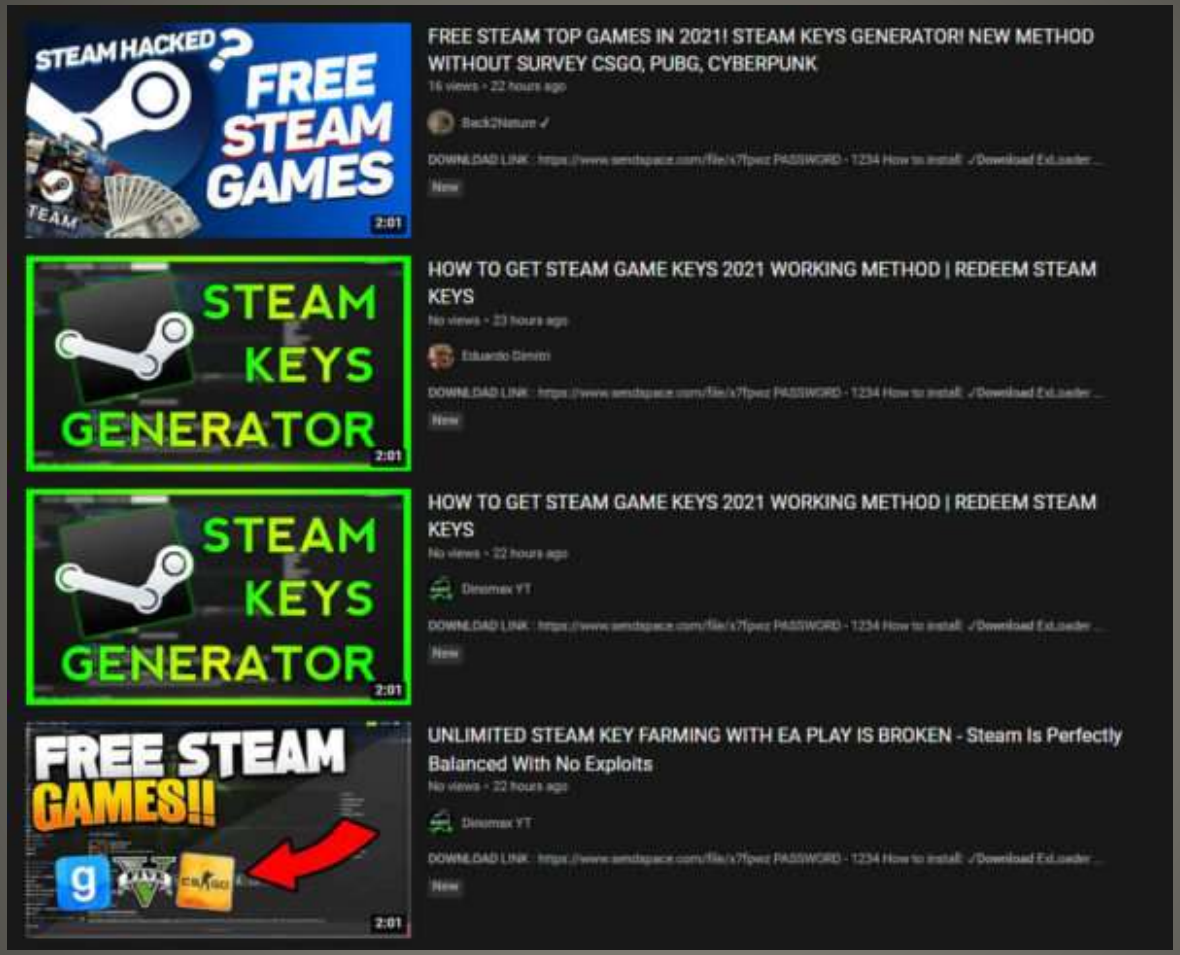
WordPress

- Open-Source content management system
- 1.6 million sites under attack 12/10/2021
- From 16,000+ IP addresses
- Weakness 4 plugins & 15 Epsilon themes
- Goal – take over attacked sites for malicious actions
- *users_can_register*
- *default_role*

- Heavy advertising on YouTube



Free Steam Games

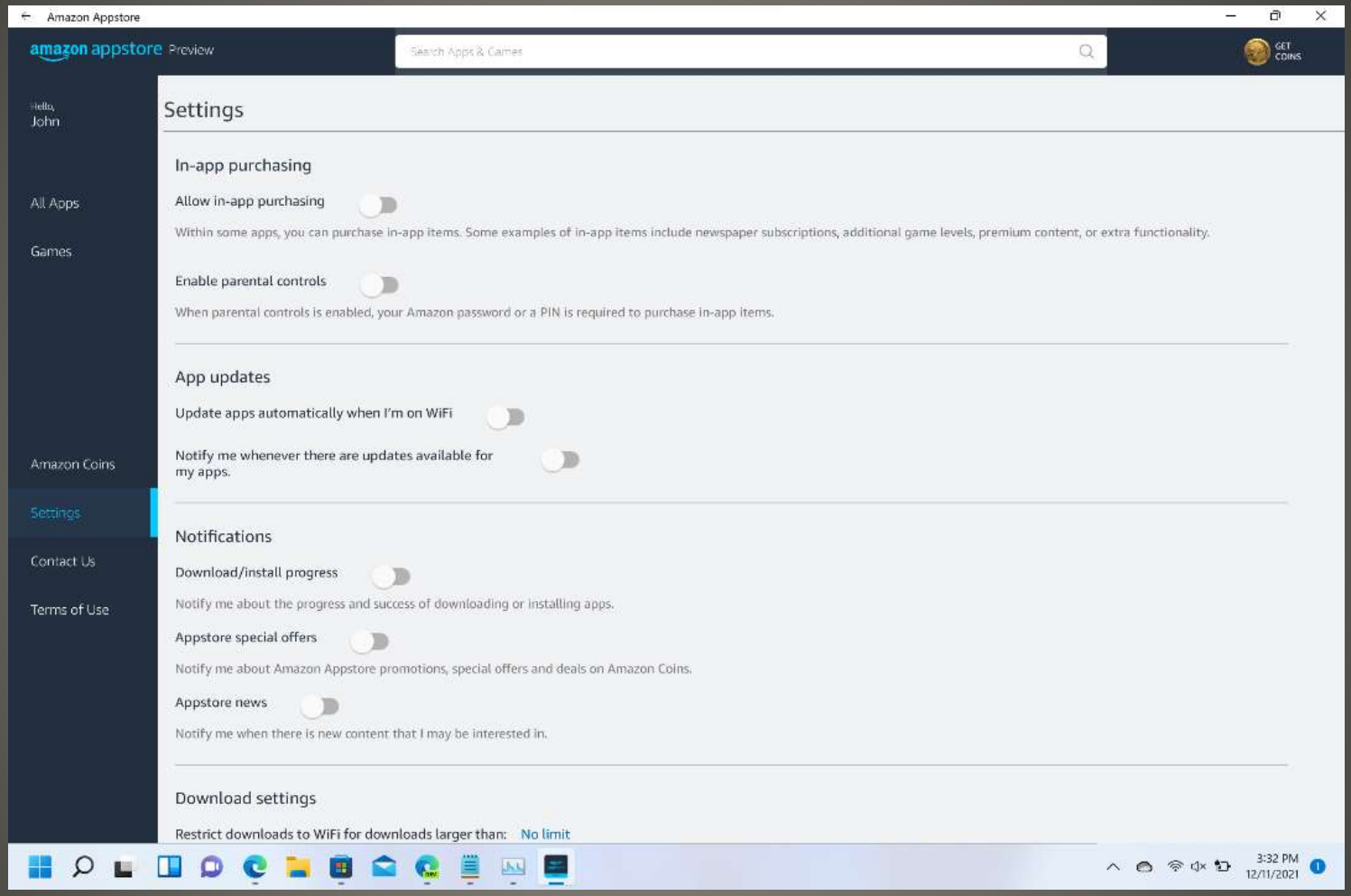


Free Steam Games

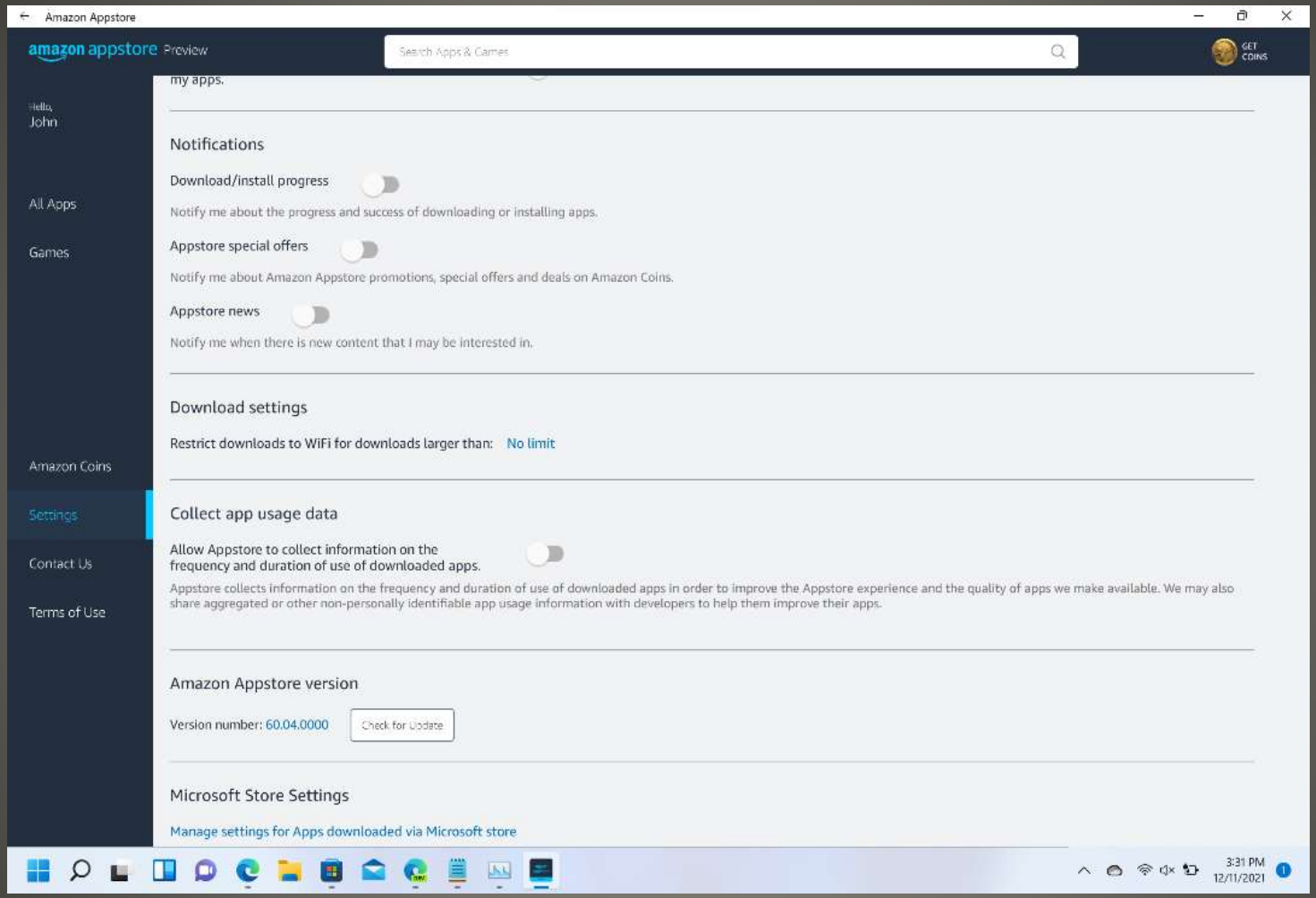
- Tax software
- Windows
- You name it

- You get *it*

Beware the free or discount

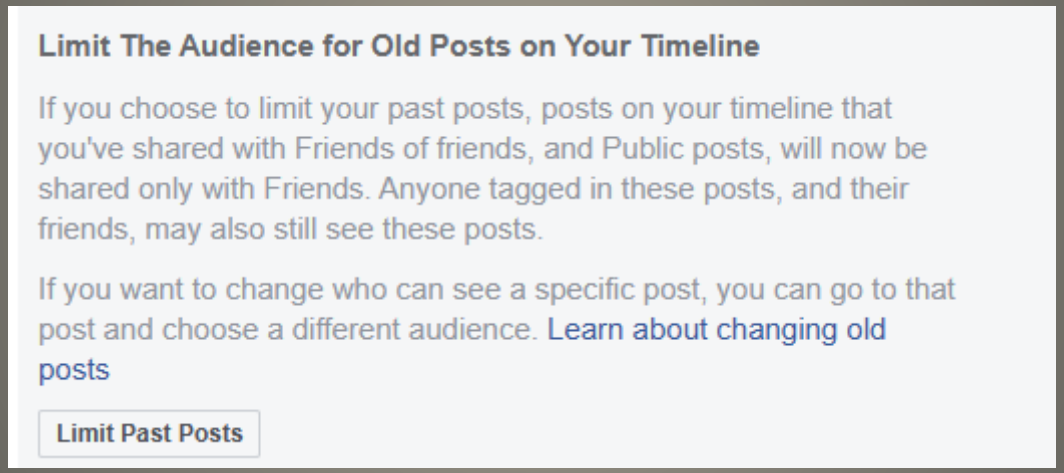


Amazon App Store for Android



Amazon App Store for Android

- Limit audience for old Facebook posts desktop
  Settings & Privacy > Settings > Privacy



Facebook

- Limit audience for all Facebook posts
  mobile
  Menu > Settings & Privacy > Settings
  scroll Audience and Visibility

Facebook

Get Back into Facebook

- Login with Facebook
- Forgot password?
- Facebook account takeover
- Forgot?

  email password reset - email taken over?

  No Longer have access to these
- Hacked

https://www.facebook.com/hacked

- No joy? Hacked.com $499 $299

Mitigations

- Yearly review New Year Resolution
- Connected Apps
- Who can view your contacts
- Facebook **Privacy Checkup**

“At 7:30 AM PST, an automated activity to scale capacity of one of the AWS services hosted in the main AWS network triggered an unexpected behavior from a large number of clients inside the internal network. This resulted in a large surge of connection activity that overwhelmed the networking devices between the internal network and the main AWS network, resulting in delays for communication between these networks. These delays increased latency and errors for services communicating between these networks, resulting in even more connection attempts and retries. This led to persistent congestion and performance issues on the devices connecting the two networks."

Amazon Web Services

Amazon Web Services

- Some customers were aware of using AWS
- Some were not
- Ring, Netflix, Prime Video, Roku, etc.
  Amazon package delivery chain
  Colleges postpone final exams
  Roomba refused to work
  Automatic cat litter and food machines …
- Fastly, Facebook
- Economics of scale <-> Complexity

Log4j

- Zero-day remote code execution vulnerability
- *Minecraft* users
- Older java runtimes, appliance front ends, older application environments, etc.
- A wealth of apps
- Large cloud services also affected
- And twitter
- BOTH client and server any/everything
- RCE Remote Code Execution!!
- First Ever CVSS score of 10?
- Log everything rationale

- ALLOW REMOTE ACCESS TO YOUR/THEIR COMPUTER

Log4j

- Everywhere known and unknown
- Apache products
- Open-source projects
- Frameworks
- NSA’s Ghidra
- Apple, Amazon, Twitter, Cloudflare, Steam, Biadu, etc.
- Canadian government 4000 websites shutdown
- Minecraft chat message compromise
- Apple cloud compromised by 1 user changing their iPhone’s name
- Change a Tesla auto’s name

Log4j

- Mitigation?
- Add line -Dlog4j2.formatMsgNoLookups=true

MORE OPTIONS JVM flags

- Apache releases Log4j version 2.15.0
- CVE-2021-44229

Log4j

- Cyber Security SIG NEWSBLOG article
- Coin mining, credential theft, exfiltrating data, lateral movement, …

https://log4shell.huntress.com/

For your testing

- You can be the victim of a victim

- Awareness, Preparedness, Understanding
- Holiday, Year end, last minute, scarcity, …

- Script kiddies
- ScriptKidiots

- CA system outage
- Apple updates everything
- Apple store & Microsoft store

- Boxed holiday gift – without patches

- Metasploit

- Web Scripts

- 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