Sun City Computer Club

Cyber Security SIG

December 3, 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

SCCCCyber

Monday, November 23, 2020

Cheap router equals Exploit?

Recent research finds "backdoor" in several hone routers sold at Walmart and Amazon.

A "backdoor" is a port that ANYONE on the Internet can gain access to your home router, thus your home network from anywhere.

The two KNOWN brands are Wavlink and Jetstream. If you have one of these brands or home routers, suggest you remove and purchase a more reputable brand.

Posted by John Jenkinson at 11:43 AM No comments:

Monday, November 16, 2020

Computer Club membership email fraud alert

Received today from Sun City Computer Club to my member email address:

a note from a club board member asking i purchase gift cards in the amount of $600, forward the card number(s) to that board member with reimbursement this Wednesday.

This is a fraud attempt. DO NOT purchase the gift cards. BE AWARE.

If you have received a similar email, report it to the FTC

https://reportfraud.ftc.gov

Posted by John Jenkinson at 10:37 AM No comments:

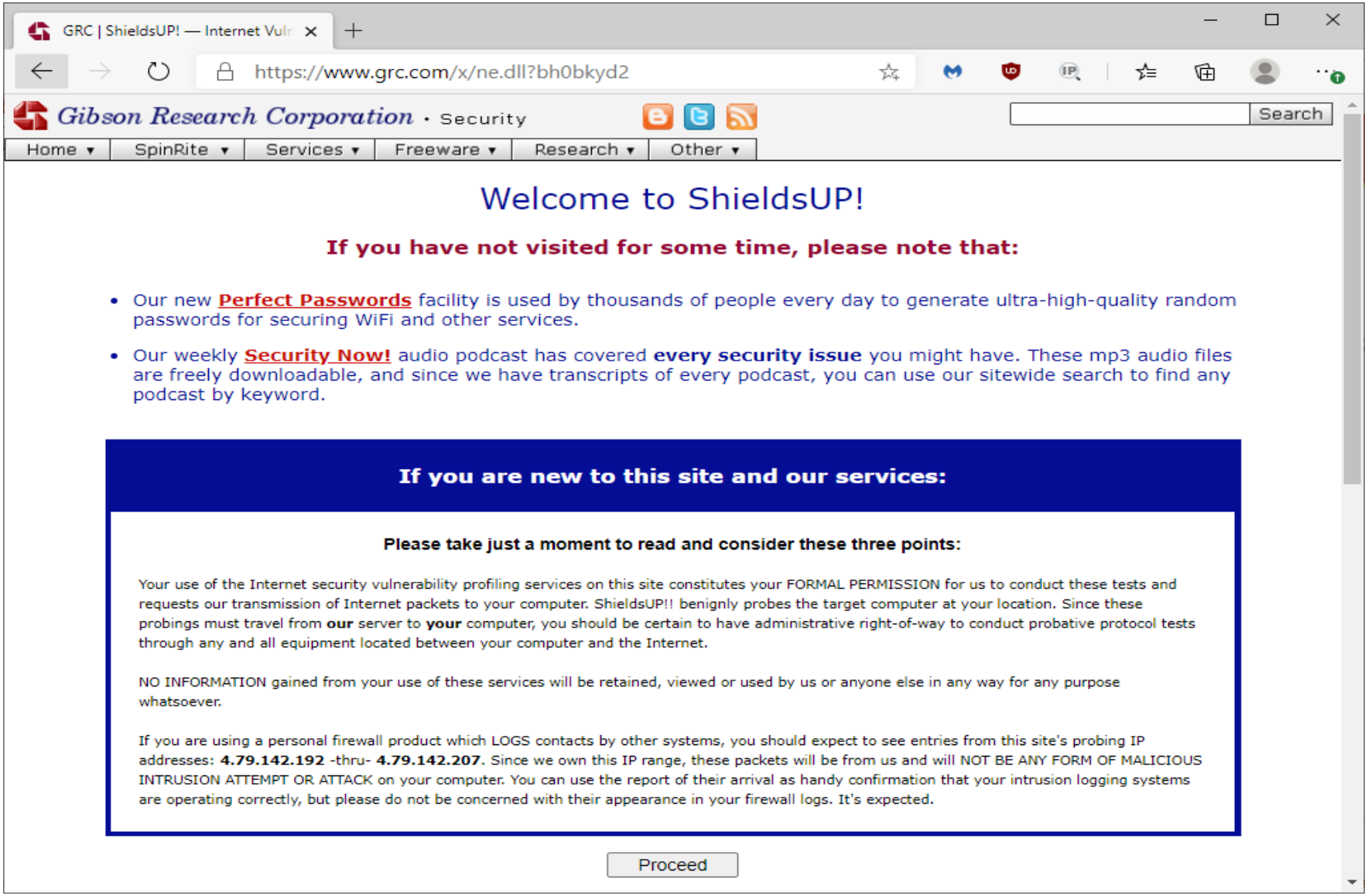
Thursday, October 22, 2020

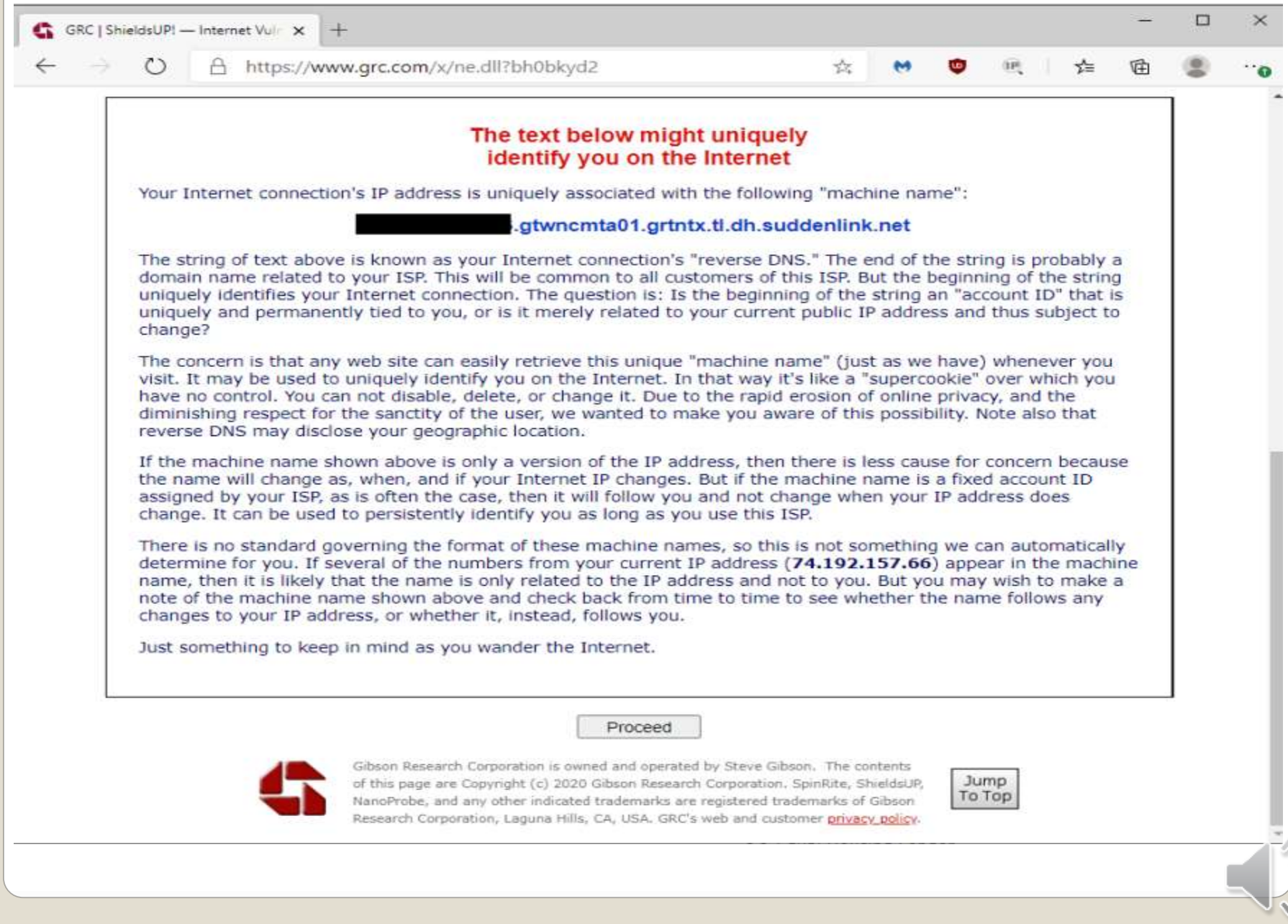
Updates abound

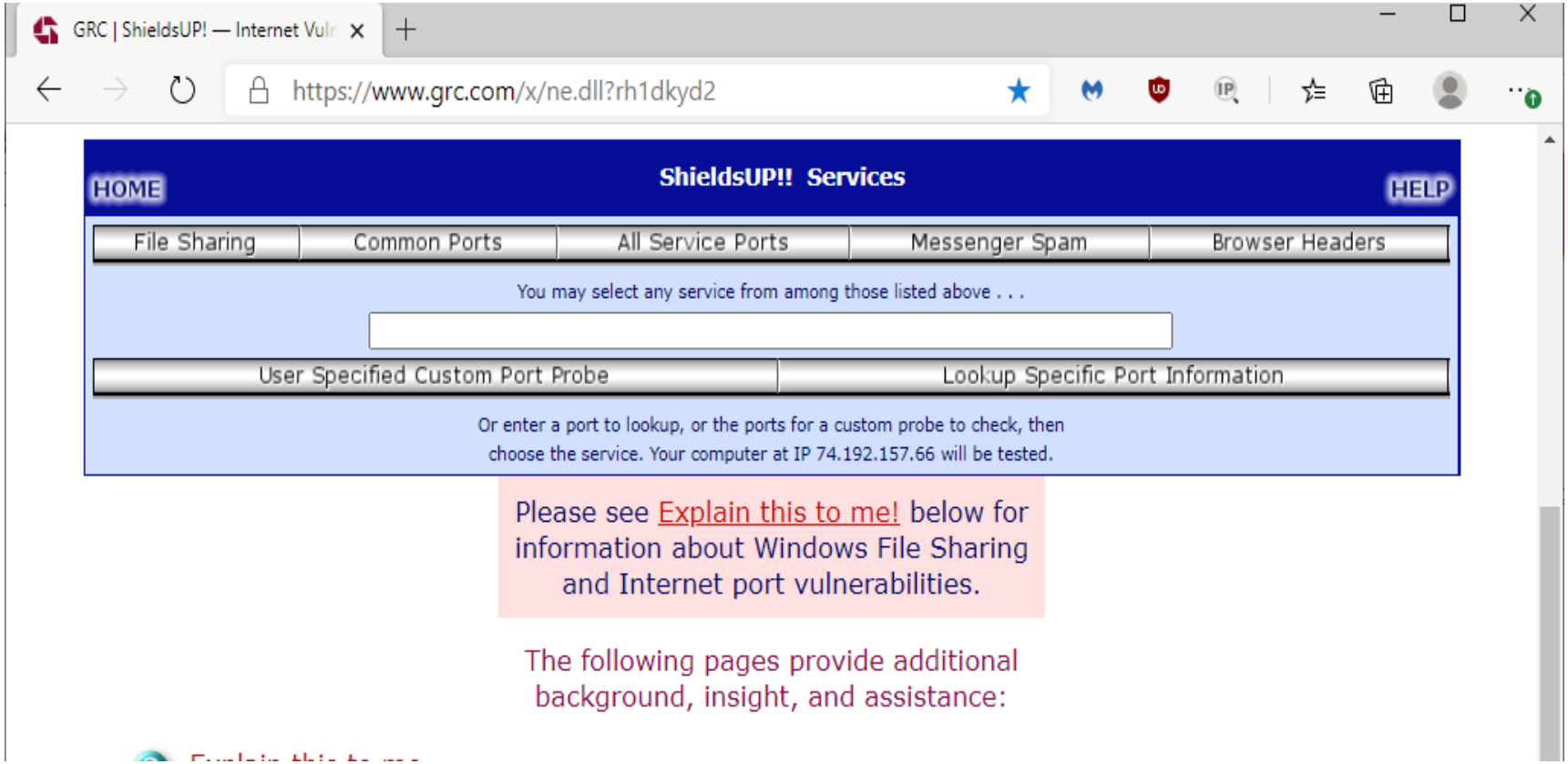
Blog Archive

- https://grc.com

ShieldsUP!!


GRC | ShieldsUP! — Internet Vuln
https://www.grc.com/x/ne.dll?bh0bkyd2
Gibson Research Corporation · Security
Search
Home
SpinRite
Services
Freeware
Research
Other
Welcome to ShieldsUP!
If you have not visited for some time, please note that:
Our new Perfect Passwords facility is used by thousands of people every day to generate ultra-high-quality random passwords for securing WiFi and other services.
Our weekly Security Now! audio podcast has covered every security issue you might have. These mp3 audio files are freely downloadable, and since we have transcripts of every podcast, you can use our sitewide search to find any podcast by keyword.
If you are new to this site and our services:
Please take just a moment to read and consider these three points:
Your use of the Internet security vulnerability profiling services on this site constitutes your FORMAL PERMISSION for us to conduct these tests and requests our transmission of Internet packets to your computer. ShieldsUP!! benignly probes the target computer at your location. Since these probings must travel from our server to your computer, you should be certain to have administrative right-of-way to conduct probative protocol tests through any and all equipment located between your computer and the Internet.
NO INFORMATION gained from your use of these services will be retained, viewed or used by us or anyone else in any way for any purpose whatsoever.
If you are using a personal firewall product which LOGS contacts by other systems, you should expect to see entries from this site's probing IP addresses: 4.79.142.192 -thru- 4.79.142.207. Since we own this IP range, these packets will be from us and will NOT BE ANY FORM OF MALICIOUS INTRUSION ATTEMPT OR ATTACK on your computer. You can use the report of their arrival as handy confirmation that your intrusion logging systems are operating correctly, but please do not be concerned with their appearance in your firewall logs. It's expected.
Proceed


GRC | ShieldsUP! — Internet Vul
https://www.grc.com/x/ne.dll?bh0bkyd2
The text below might uniquely identify you on the Internet
Your Internet connection's IP address is uniquely associated with the following "machine name":
[redacted].gtwncmta01.grtntx.tl.dh.suddenlink.net
The string of text above is known as your Internet connection's "reverse DNS." The end of the string is probably a domain name related to your ISP. This will be common to all customers of this ISP. But the beginning of the string uniquely identifies your Internet connection. The question is: Is the beginning of the string an "account ID" that is uniquely and permanently tied to you, or is it merely related to your current public IP address and thus subject to change?
The concern is that any web site can easily retrieve this unique "machine name" (just as we have) whenever you visit. It may be used to uniquely identify you on the Internet. In that way it's like a "supercookie" over which you have no control. You can not disable, delete, or change it. Due to the rapid erosion of online privacy, and the diminishing respect for the sanctity of the user, we wanted to make you aware of this possibility. Note also that reverse DNS may disclose your geographic location.
If the machine name shown above is only a version of the IP address, then there is less cause for concern because the name will change as, when, and if your Internet IP changes. But if the machine name is a fixed account ID assigned by your ISP, as is often the case, then it will follow you and not change when your IP address does change. It can be used to persistently identify you as long as you use this ISP.
There is no standard governing the format of these machine names, so this is not something we can automatically determine for you. If several of the numbers from your current IP address (74.192.157.66) appear in the machine name, then it is likely that the name is only related to the IP address and not to you. But you may wish to make a note of the machine name shown above and check back from time to time to see whether the name follows any changes to your IP address, or whether it, instead, follows you.
Just something to keep in mind as you wander the Internet.
Proceed
Gibson Research Corporation is owned and operated by Steve Gibson. The contents of this page are Copyright (c) 2020 Gibson Research Corporation. SpinRite, ShieldsUP, NanoProbe, and any other indicated trademarks are registered trademarks of Gibson Research Corporation, Laguna Hills, CA, USA. GRC's web and customer privacy policy.
Jump To Top



Click here to check your router now...

GRC's Instant UPnP Exposure Test


https://www.grc.com/x/ne.dll?rh1dkyd2
Gibson Research Corporation · Data Recovery
Search
Home
SpinRite
Services
Freeware
Research
Other
Shields UP!!
Port Authority Edition – Internet Vulnerability Profiling
by Steve Gibson, Gibson Research Corporation
Universal Plug n'Play (UPnP)
Internet Exposure Test
This Internet probe sends up to ten (10) UPnP Simple Service Discovery Protocol (SSDP) M-SEARCH UDP packets, one every half-second, to our visitor's current IPv4 address (74.192.157.66) in an attempt to solicit a response from any publicly exposed and listening UPnP SSDP service. The UPnP protocols were never designed to be exposed to the public Internet, and any Internet-facing equipment which does so should be considered defective, insecure, and unusable. Any such equipment should be disconnected immediately.
Your equipment at IP:
[redacted]
Is now being queried:
THE EQUIPMENT AT THE TARGET IP ADDRESS
DID NOT RESPOND TO OUR UPnP PROBES!
(That's good news!)

- Name
- DOB
- Address
- Contact Phone Number
- Medication
- Price
- Order number
- Micro QR code
- Distinction Yellow bag or HEB White bag

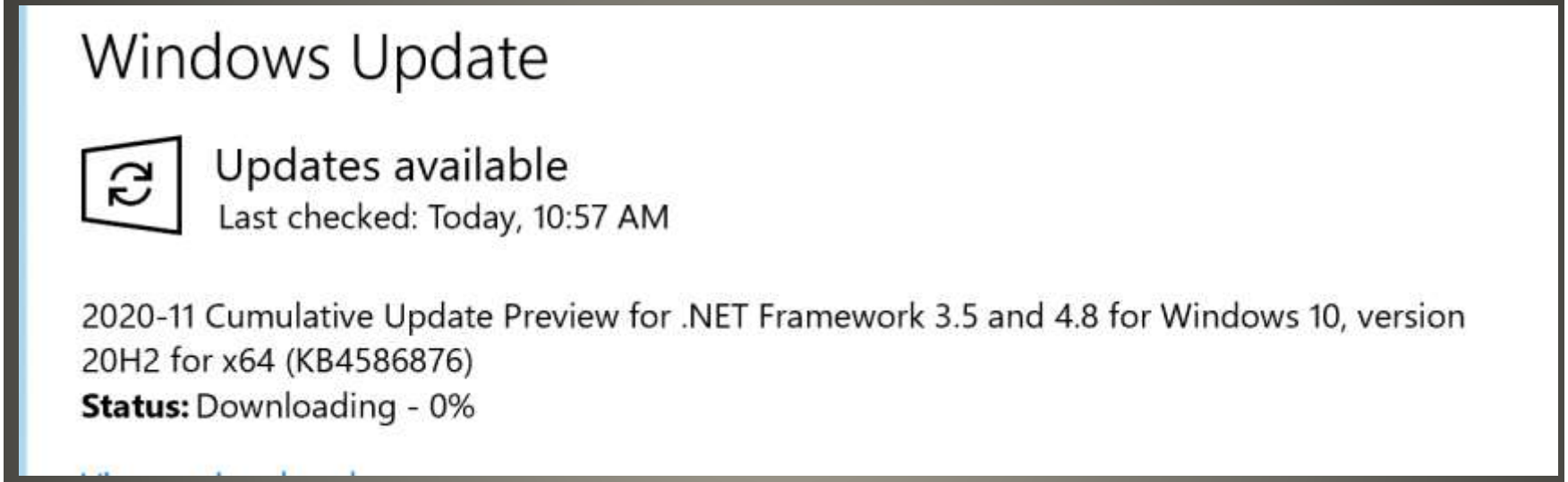
HEB Pharmacy plastic bag

Current Issues

- Ransomware on company's printers

> — EGREGOR —
>
> What happened?
>
> Your network was ATTACKED, your computers and servers were LOCKED.
> Your private data was DOWNLOADED.
>
> What does it mean?
>
> It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.
>
> How it can be avoided?
>
> In order to avoid this issue, you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and breach fixing AGREEMENT.

Windows Update



Windows Update

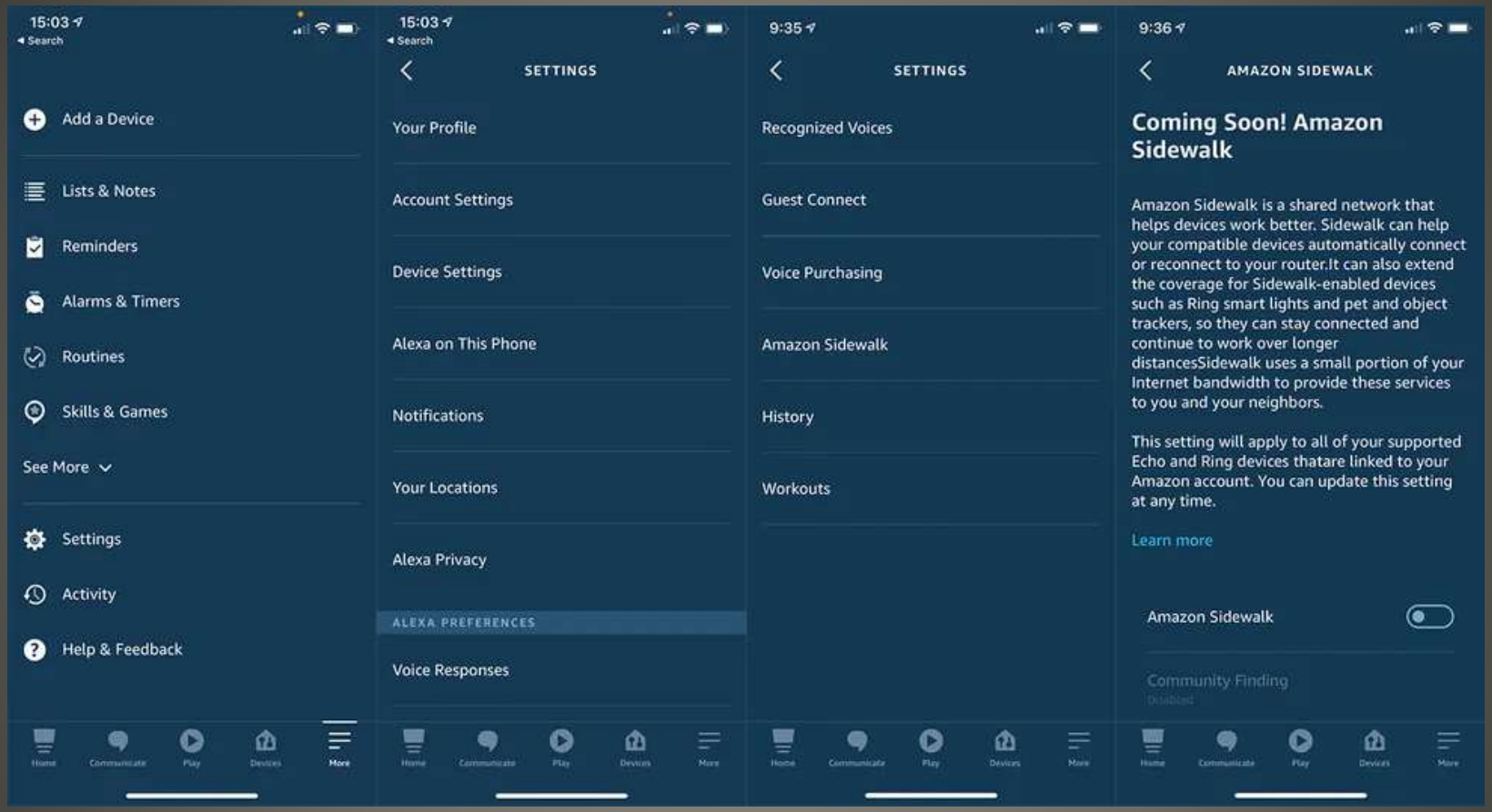
Current Issues

- TSA master keys photograph
- Zoom information leak via video

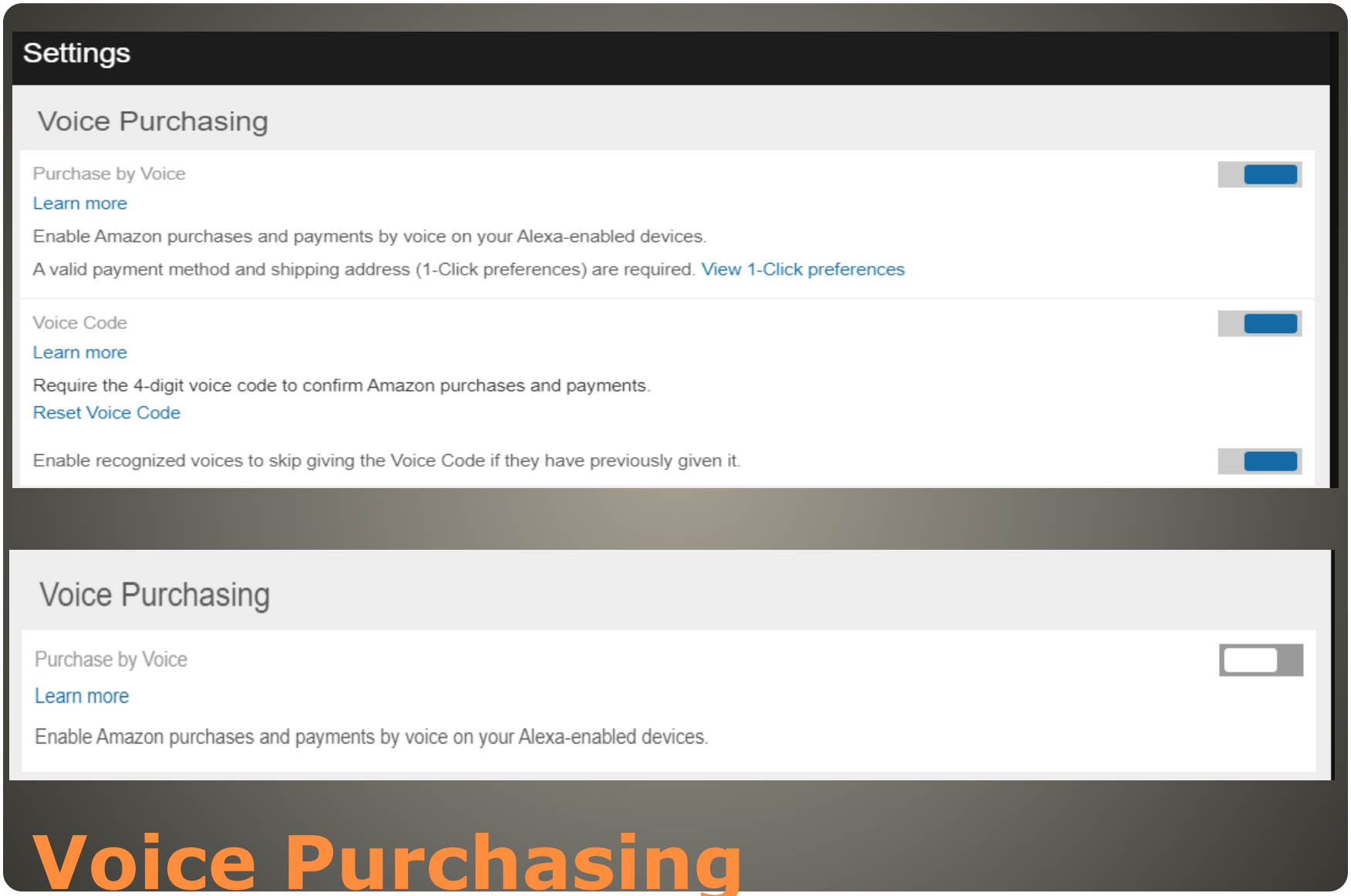
amazon sidewalk

Welcome to Amazon Sidewalk

Amazon Sidewalk is a shared network, coming later this year, that helps devices like Amazon Echo devices, Ring Security Cams, outdoor lights, and motion sensors work better at home and beyond the front door. When enabled, Sidewalk can unlock unique benefits for your device, support other Sidewalk devices in your community, and even open the door to new innovations like locating items connected to Sidewalk.



Amazon Sidewalk



Voice Purchasing

- Comcast data cap

Current Issues

- TinyCheck stalkerware detection
- GoDaddy certificate compromises
- Microsoft Pluton chip
- MobileIron MDM flaw
- BGP taskforce
- MacOS zip file phishing attack
- Site Notifications

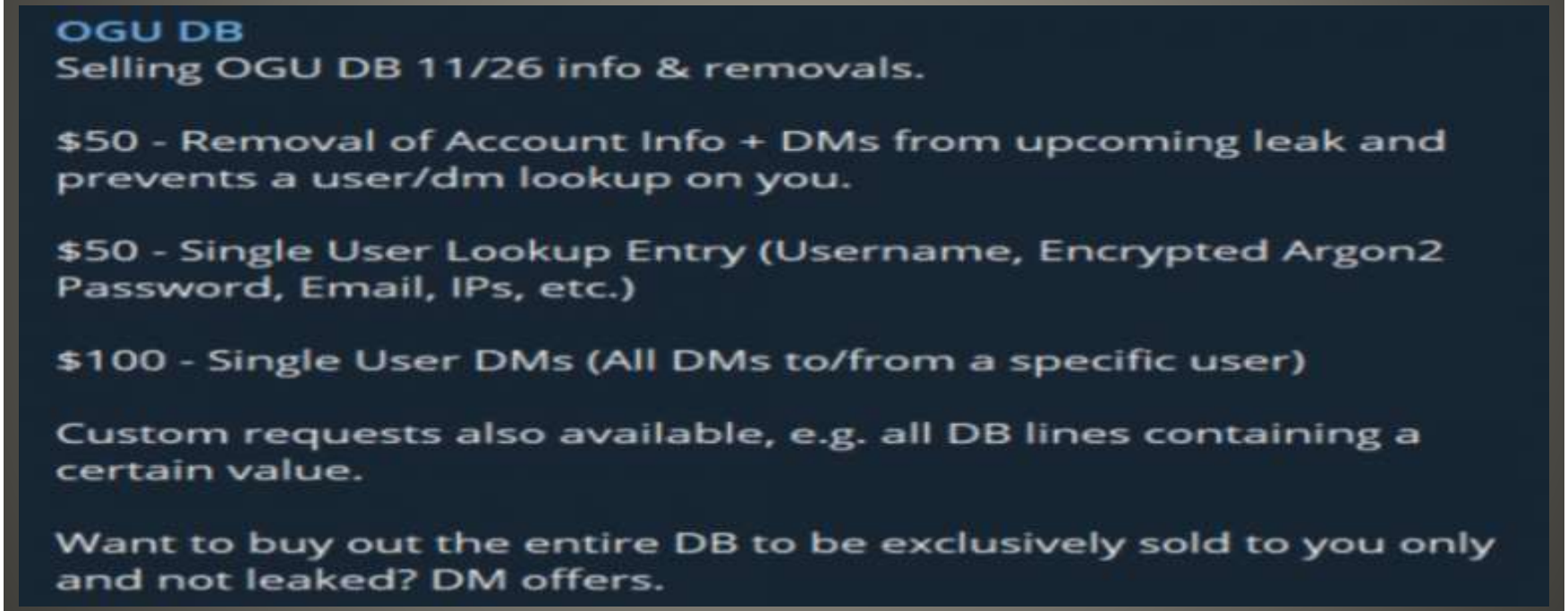
Current Issues

Current Issues

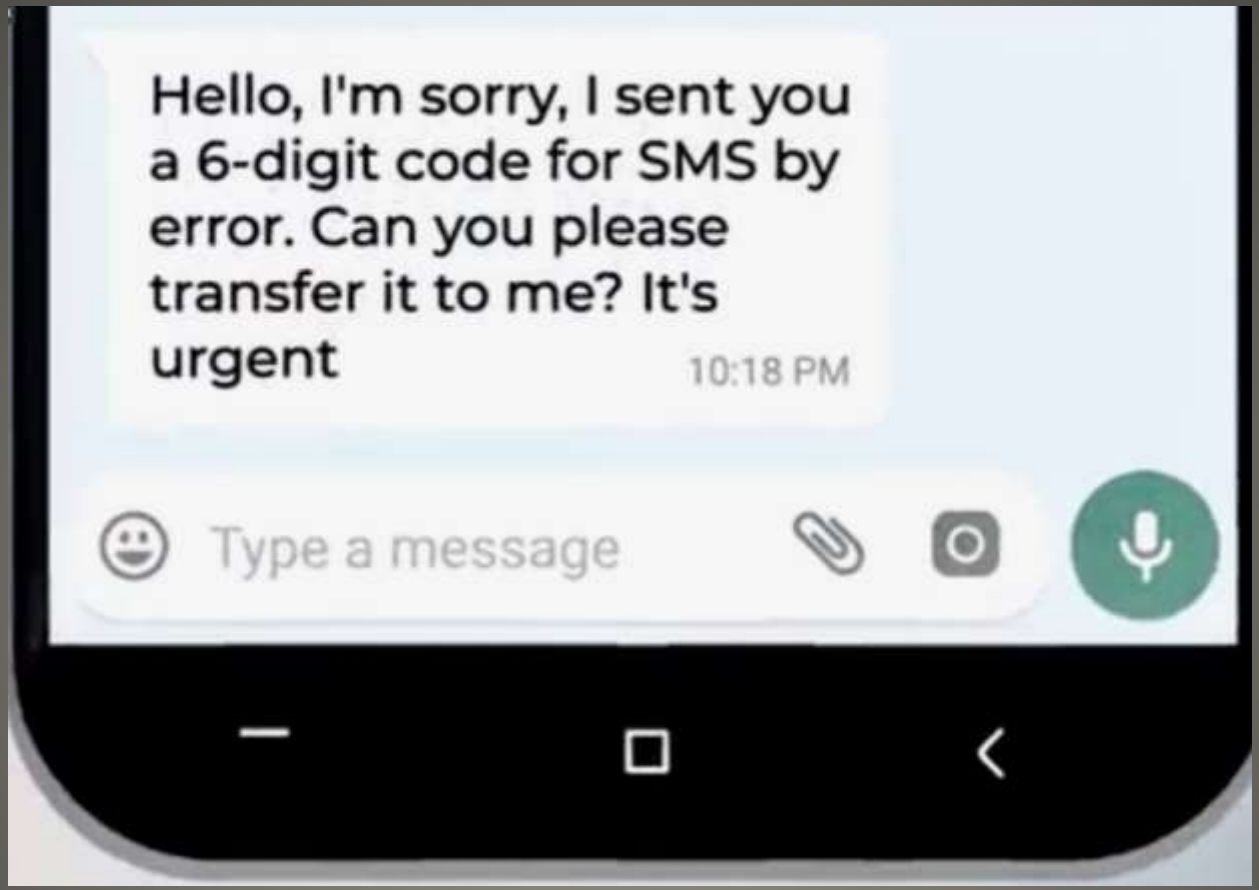
- iOS zero-click radio proximity exploit
- Wormable
- ANY/EVERYthing and keychain
  Wi-Fi caution

- Trickbot UEFI

- Check Washing
- OGUsers hacked yet again
  Users asked to pay



Current Issues



What's App current attack

- Spying?
- Shift or add-on to other monitoring
- Zoom attention tracking

Microsoft 365 Analytics

CPU EXPERT

Learn more about CPUs for desktops, laptops, and mobile devices

Home | CPU Benchmark | CPUs Rank | Stress Test | Help | Contacts

Testing results for "Apple M1"

AMD Ryzen Threadripper 3970X 32-Core, 64-Thread Unlocked Desktop Processor, without Cooler

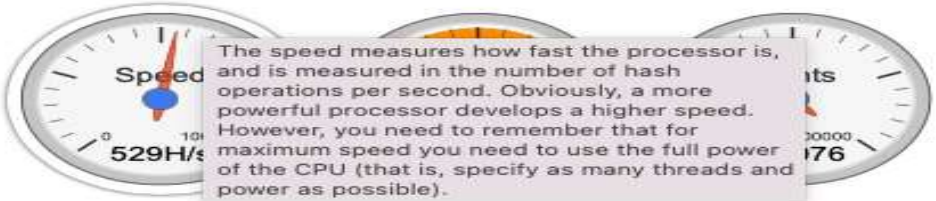
- An astonishing 32 cores and 64 processing threads for serious designers and artists
- Incredible 4. 5 GHz max boost frequency, with a huge 144MB cache
- Unlocked, with new automatic overclocking feature

$2,252.47

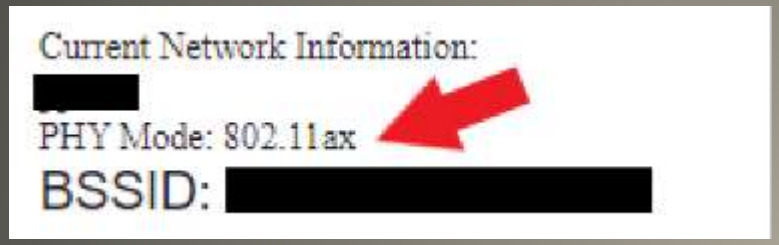
Buy amazon

Rank	Score	Speed
1431/94305	173076	529H/s

CPU	Apple M1
GPU	Apple GPU
Points	173076
Initial Rank	1431/94305
Current Rank	1431/94305
Speed	~529H/s
Threads	32
Duration	327s
Start Date	1 December 2020, 21:04:05
Finish Date	1 December 2020, 21:09:32
Browser	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.1 Safari/605.1.15
Permalink	https://cpux.net/b/o7f5t2



- 802.11ax
- WPA3 encryption



Wi-Fi 6


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