Sun City Computer Club

Cyber Security SIG
November 2, 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

SSD Fraud

- Channel 18 8am Scams Anti-Fraud Group
- Sun City Anti-Fraud Group Resources

  Sun City CA RESIDENT HOME

NRO PROGRAMS

Other Sun City Resources

- Scams and Computer Safety SIG
- AI Sig – new November 6th 10am
- Announcements
- WiKi
- SIGs
- Classes
- Cyber Security Sig News Blog / Archive
- Vimeo
- https://vimeo.com/sctxcompclub

Other Computer Club Resources

- Questions

“How do “they” know where I went to school?

See the OSINT information later in this presentation

PayPal?

Advantages and disadvantages slide later

Is AI in my computer?

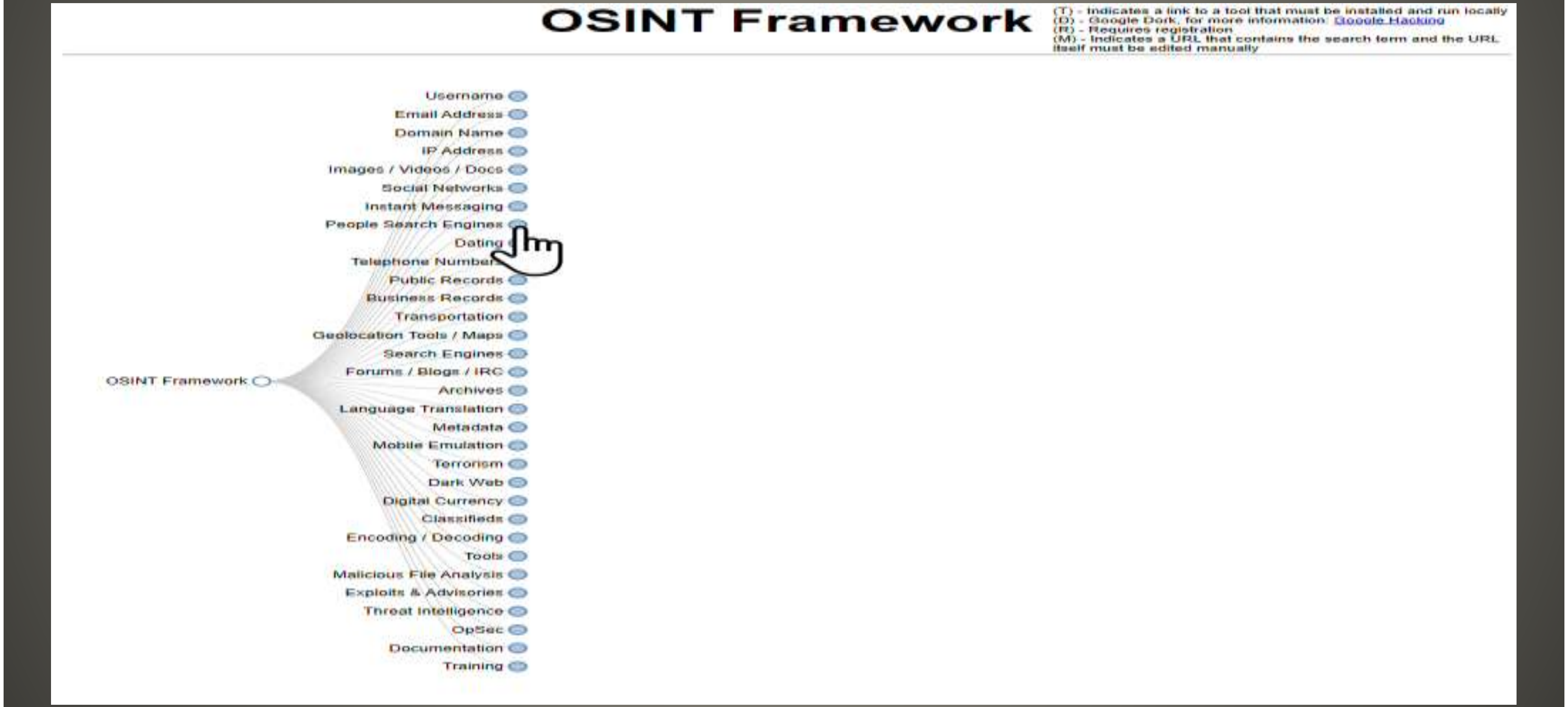
If you are running the latest Windows 11 23H2 version?

Yes

Scams and Computer Safety SIG

OSINT

- https://osintframework.com/
- Open Source Intelligence



OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: Google Hacking
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually

OSINT Framework

- Username
- Email Address
- Domain Name
- IP Address
- Images / Videos / Docs
- Social Networks
- Instant Messaging
- People Search Engines
- Dating
- Telephone Number
- Public Records
- Business Records
- Transportation
- Geolocation Tools / Maps
- Search Engines
- Forums / Blogs / IRC
- Archives
- Language Translation
- Metadata
- Mobile Emulation
- Terrorism
- Dark Web
- Digital Currency
- Classifieds
- Encoding / Decoding
- Tools
- Malicious File Analysis
- Exploits & Advisories
- Threat Intelligence
- OpSec
- Documentation
- Training

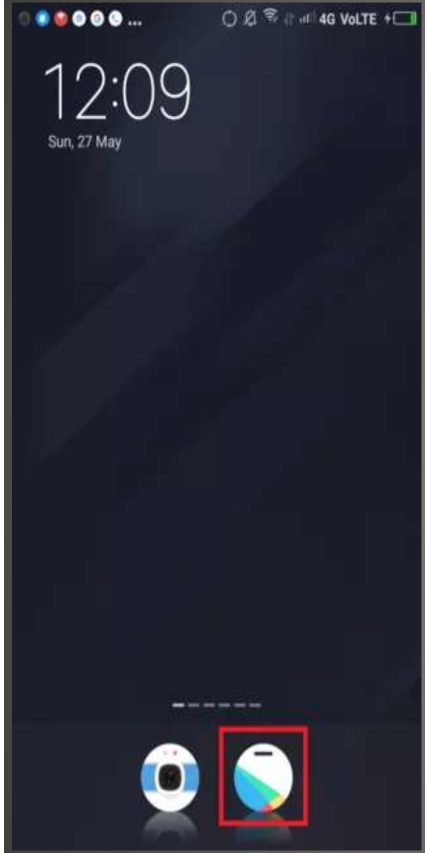
PayPal

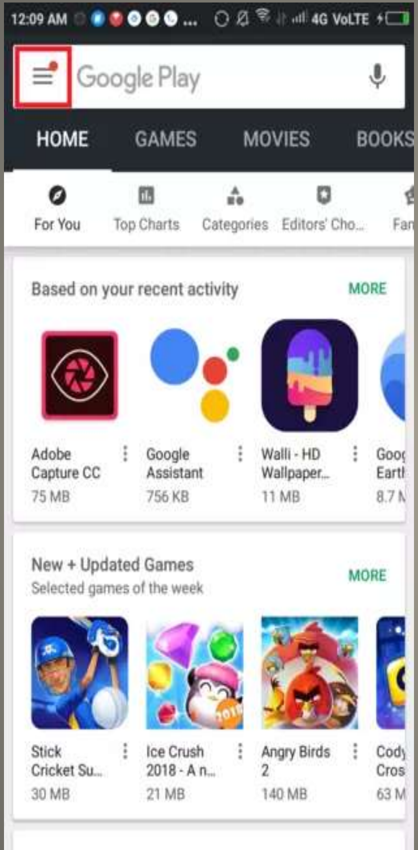
- Confusing fees
- Scammer target

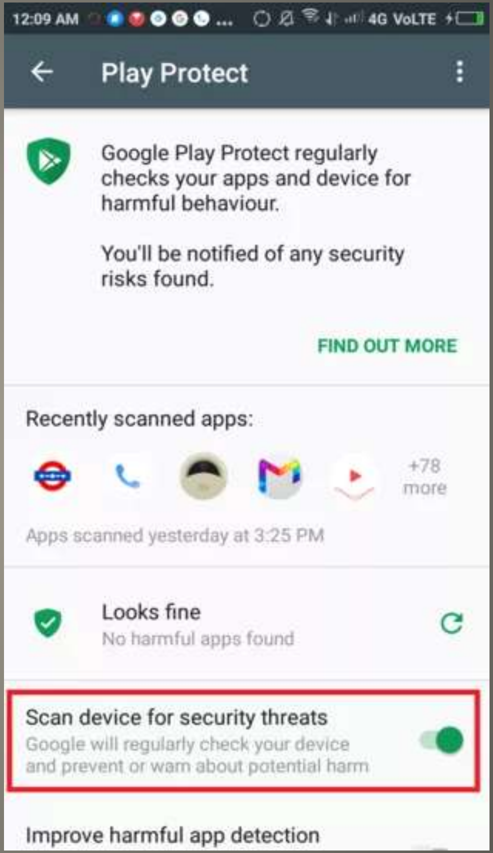
- No CC number at merchant
- Almost Instant remedy

- Ask Bing, Bard, ChatGPT

- Google Play Protect







Google Play Protect regularly checks your apps and device for harmful behaviour.

You'll be notified of any security risks found.

Recently scanned apps:

Apps scanned yesterday at 3:25 PM

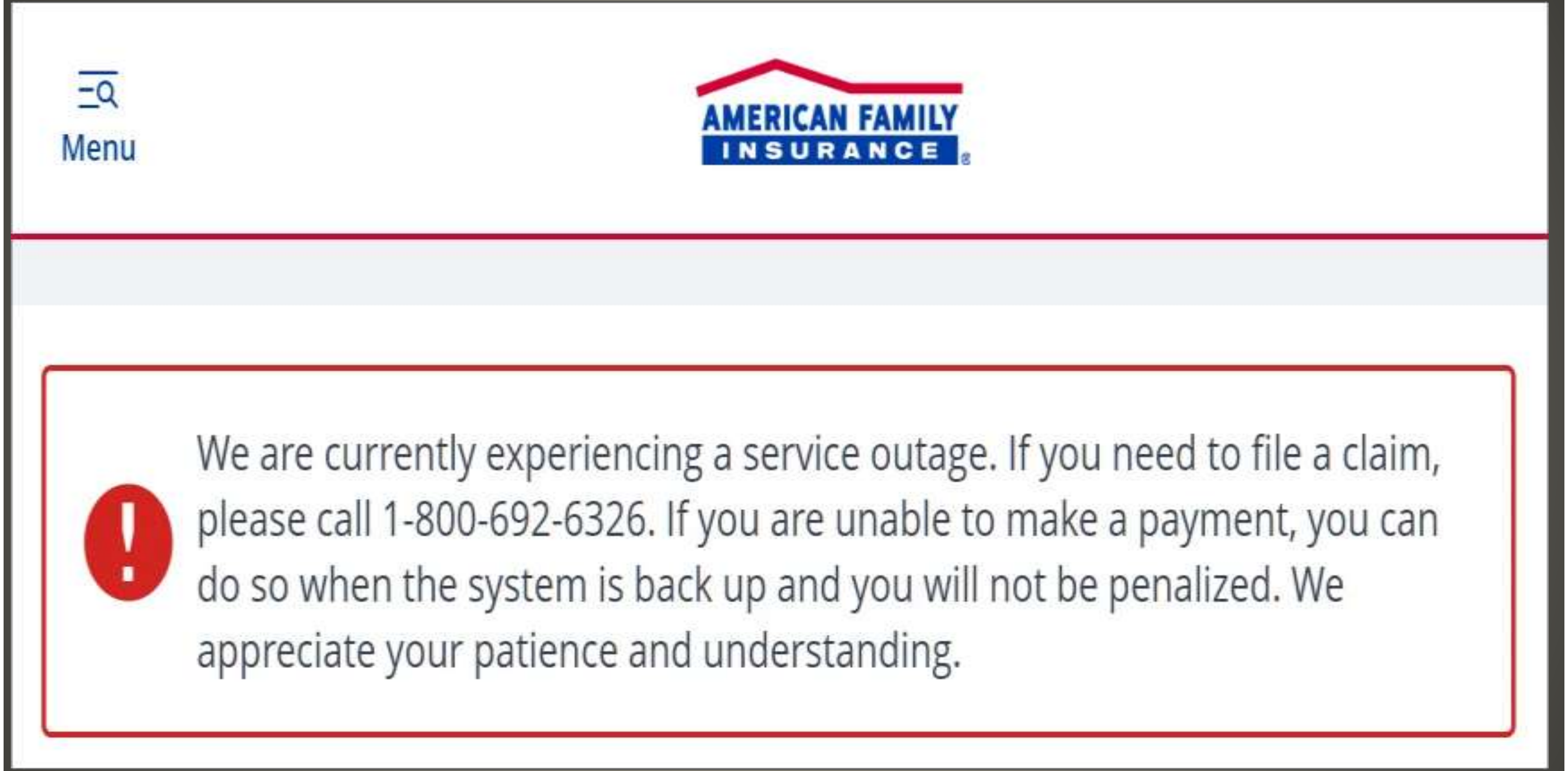
Looks fine
No harmful apps found

Scan device for security threats
Google will regularly check your device and prevent or warn about potential harm

Improve harmful app detection

Current Issues

- American Family Insurance confirms cyber attack



We are currently experiencing a service outage. If you need to file a claim, please call 1-800-692-6326. If you are unable to make a payment, you can do so when the system is back up and you will not be penalized. We appreciate your patience and understanding.

Current Issues

- An email of a neighbor's postal mail
- USPS Change of Address fraud
- Thief acquires name and address
- Change of Address via mail

  Not online, not in-person

  More authentication
- Access your mail at their address
- Financial statements
- Pharmacy delivery

- Got a change of address form?
- USPS should notify both ola and new address

  Contact local US Postal Inspection office

  1-877-876-2455

USPS Informed Delivery

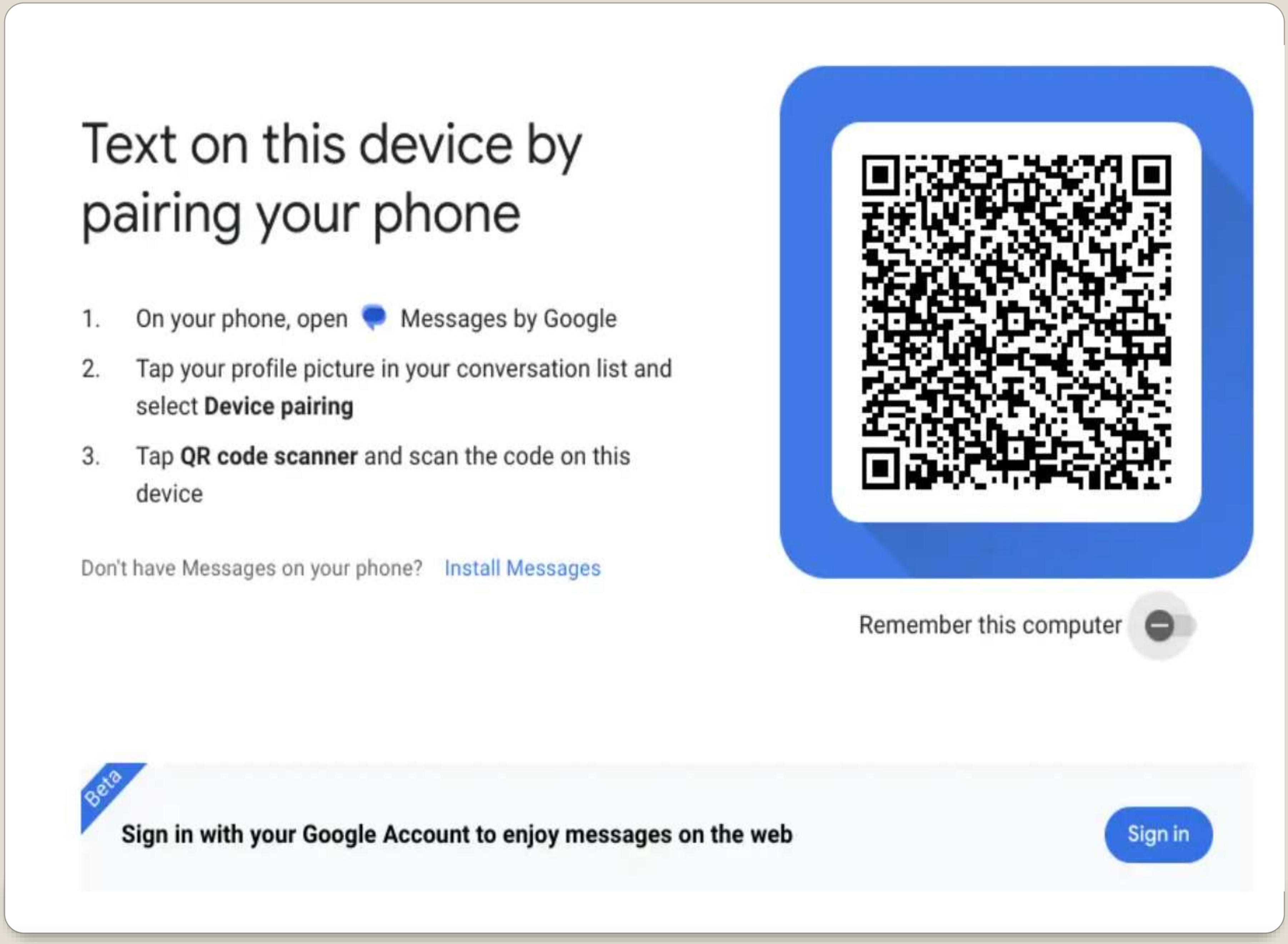
USPS Change of Policy

- Change NOT Activated without identification
- QR Code sent to email
- ???

- Cyber Security SIG August 17

Current Issues

- Chrome to test “hide my IP”
  Opt-in
- Privacy Badger
  un-rewrites Google rewritten links
  Google search result link rewritten
  routed thru Google Servers
  algorithmic tracker blocker
- North Korea attack crypto experts
  KANDYKORN Mac malware
- Google registry TLD .ing
  buy.ing $129,999/yr
- Bitwarden adding passkey support to password manager
- Google account paring for messages
  No cameras, no QR codes



Text on this device by pairing your phone

1. On your phone, open Messages by Google
2. Tap your profile picture in your conversation list and select **Device pairing**
3. Tap **QR code scanner** and scan the code on this device

Don't have Messages on your phone? Install Messages

Remember this computer

Beta

Sign in with your Google Account to enjoy messages on the web

- Facebook account take-over hijack

Identity theft, financial loss, emotional distress

No strong support from Facebook

weak passwords no multi factor

cookie theft session tokens

Buy session cookies 1,000 $80

Facebook support emails $50 for 100

Scams – your Facebook account

Fraud – linked payment methods

login with Facebook

Sale of old established Facebook accounts – value

Personal Information

Payment methods

Facebook

Facebook

- Locked out   -or-   account take over
- Check account phone number or email
- Logout of Facebook everywhere
- Facebook.com

  Forgot Account

  Follow instructions in phone or email

- No phone or email access

  Facebook.com/login/identify

  Fill out form   provide Identity proof

- PROTECT
  Strong passwords
  Multi-factor
  Suspicious links
  Security suites
  Report suspicious actions
  Identity protection services

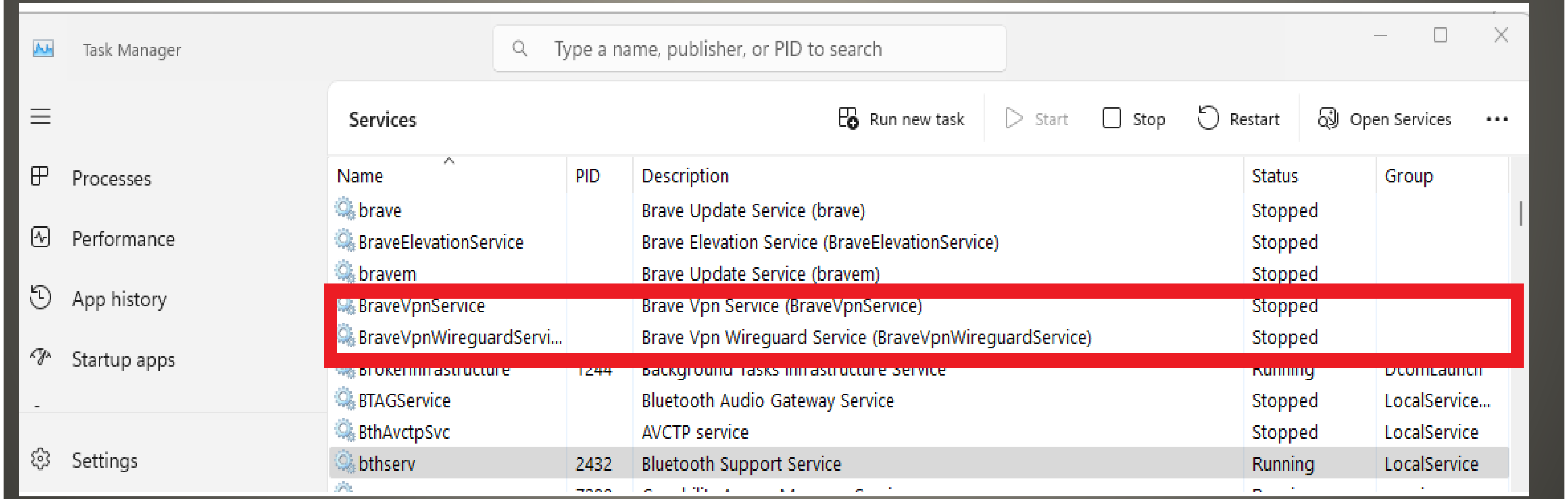
- Similar name
  Protect contacts

HELP A FRIEND - report

Facebook

- Brave offers VPN services
- Brave loads those VPN services

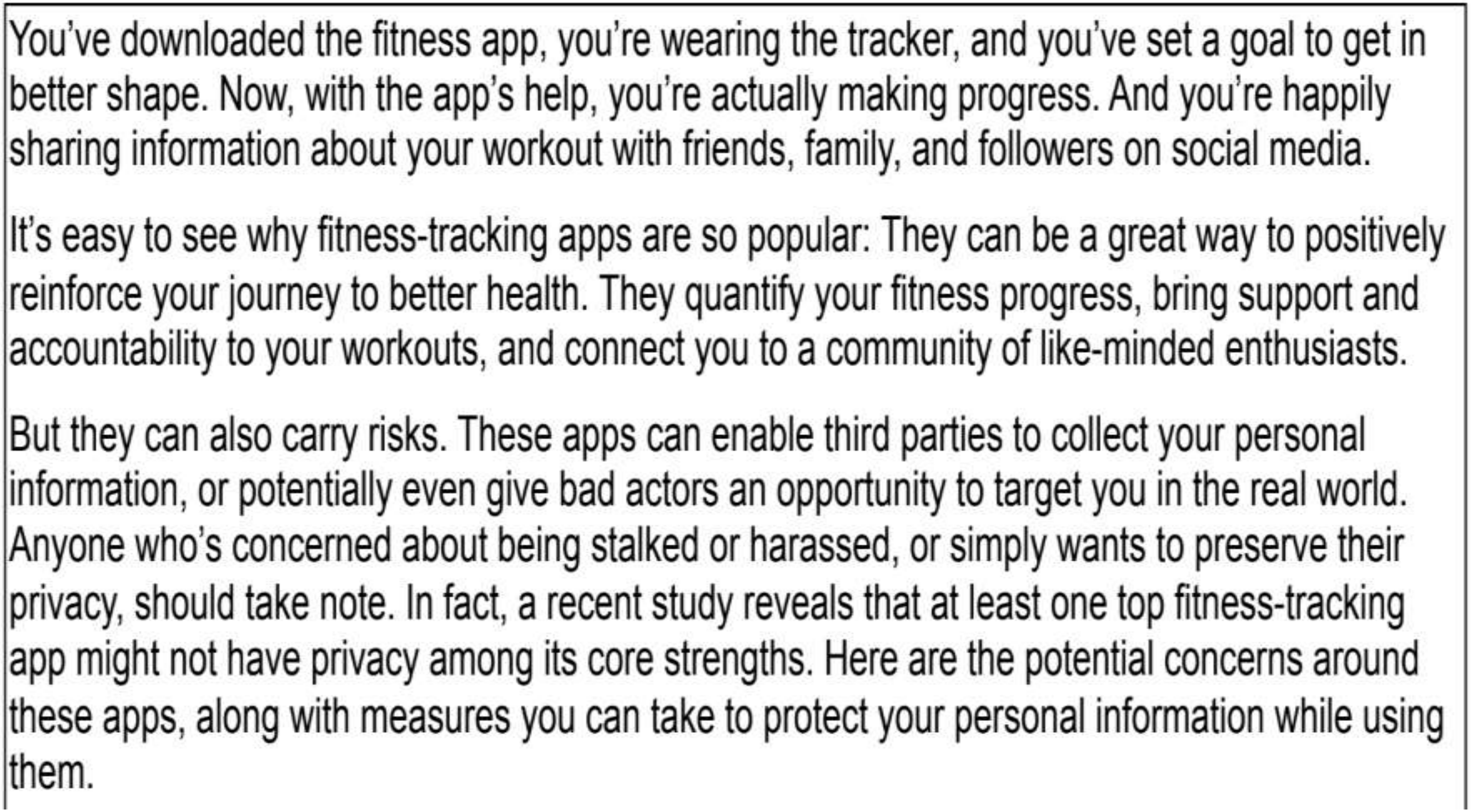
  Without notification nor permission
- Brave turns on those services if user subscribes



Name	PID	Description	Status	Group
brave		Brave Update Service (brave)	Stopped	
BraveElevationService		Brave Elevation Service (BraveElevationService)	Stopped	
bravem		Brave Update Service (bravem)	Stopped	
BraveVpnService		Brave Vpn Service (BraveVpnService)	Stopped	
BraveVpnWireguardServi...		Brave Vpn Wireguard Service (BraveVpnWireguardService)	Stopped	
BrokerInfrastructure	1244	Background Tasks Infrastructure Service	Running	DcomLaunch
BTAGService		Bluetooth Audio Gateway Service	Stopped	LocalService...
BthAvctpSvc		AVCTP service	Stopped	LocalService
bthserv	2432	Bluetooth Support Service	Running	LocalService

Brave VPN on Windows

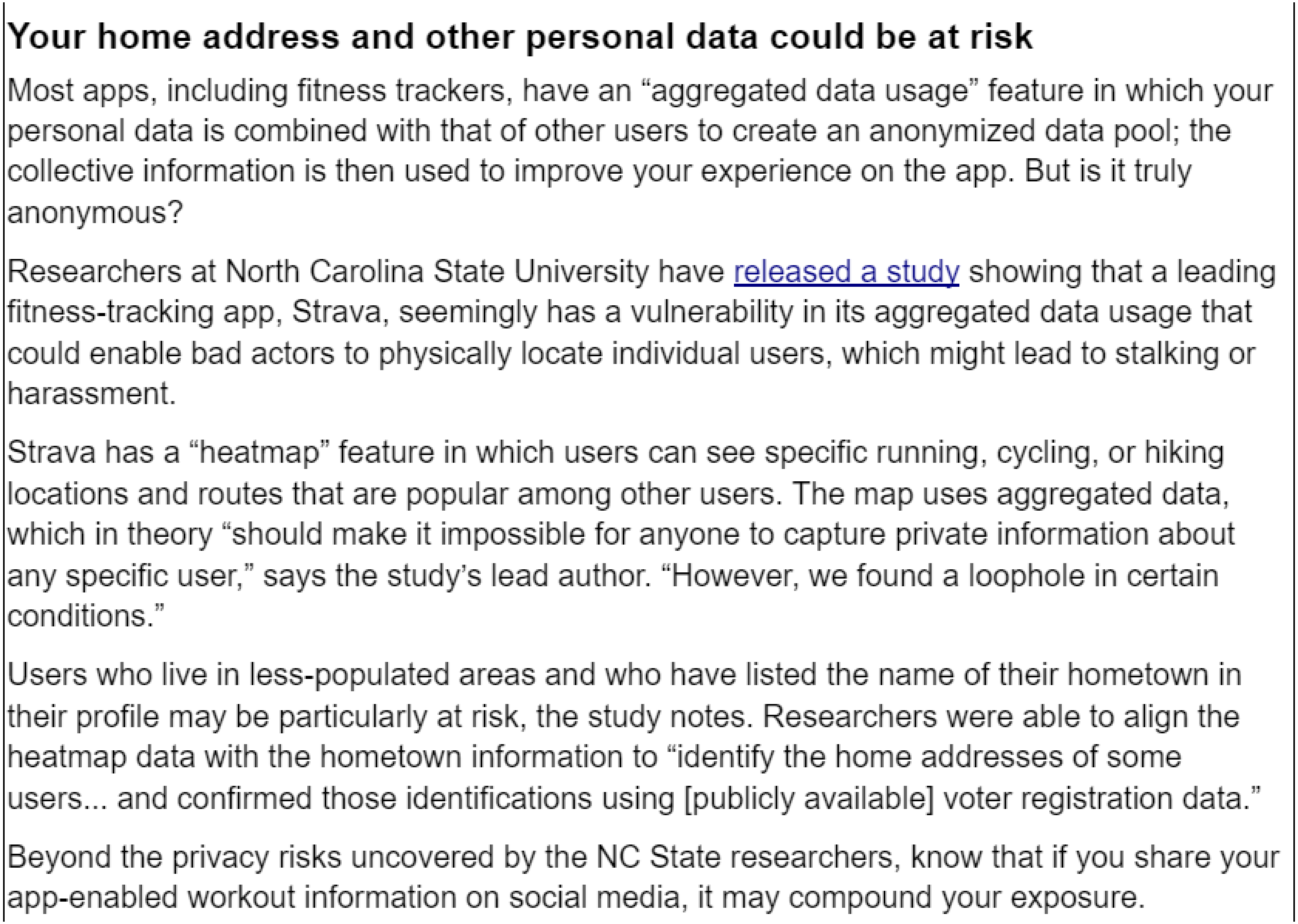
Busy getting in shape? Be sure to also exercise your right to privacy



You've downloaded the fitness app, you're wearing the tracker, and you've set a goal to get in better shape. Now, with the app's help, you're actually making progress. And you're happily sharing information about your workout with friends, family, and followers on social media.

It's easy to see why fitness-tracking apps are so popular: They can be a great way to positively reinforce your journey to better health. They quantify your fitness progress, bring support and accountability to your workouts, and connect you to a community of like-minded enthusiasts.

But they can also carry risks. These apps can enable third parties to collect your personal information, or potentially even give bad actors an opportunity to target you in the real world. Anyone who's concerned about being stalked or harassed, or simply wants to preserve their privacy, should take note. In fact, a recent study reveals that at least one top fitness-tracking app might not have privacy among its core strengths. Here are the potential concerns around these apps, along with measures you can take to protect your personal information while using them.



Your home address and other personal data could be at risk

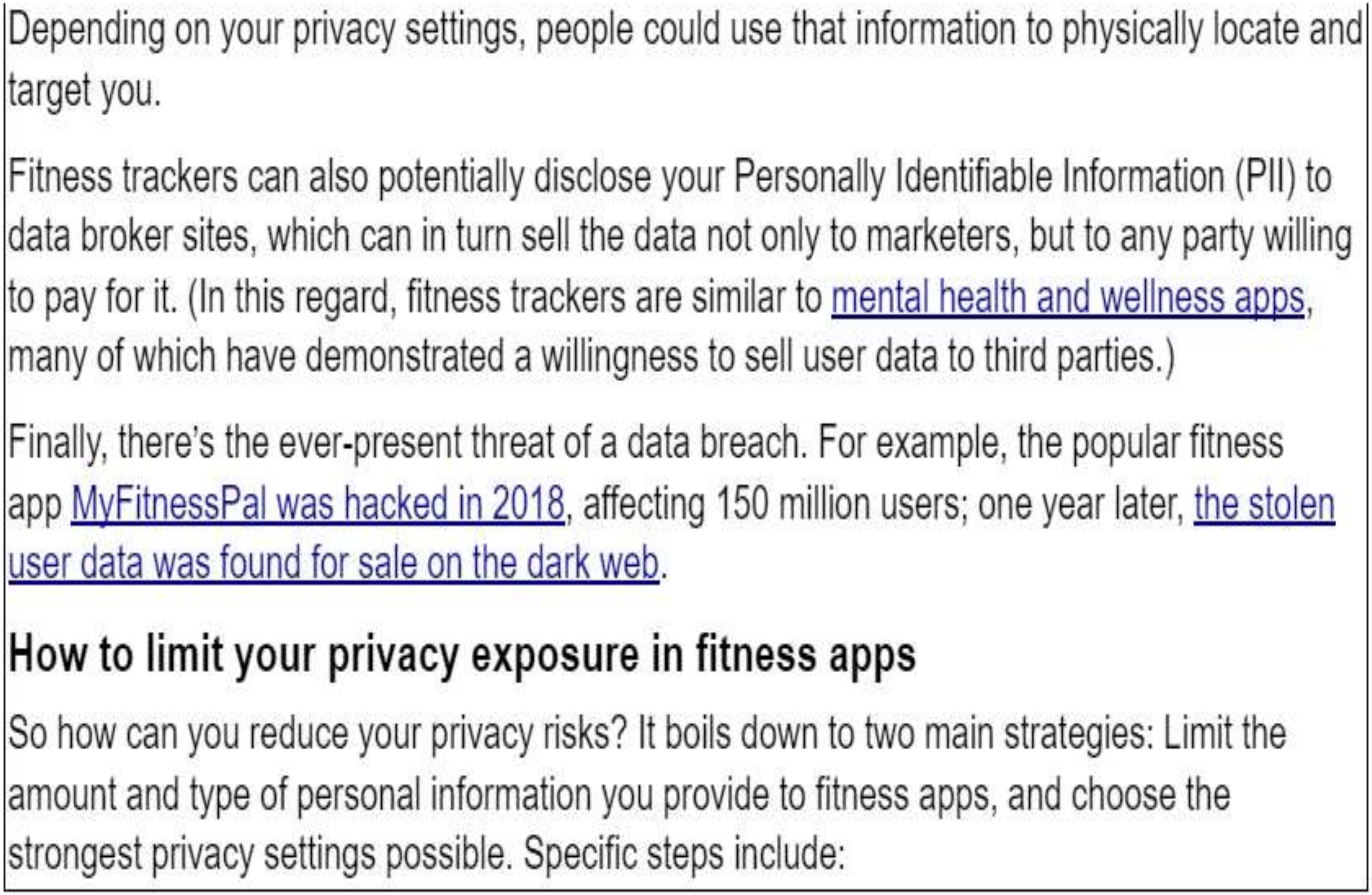
Most apps, including fitness trackers, have an “aggregated data usage” feature in which your personal data is combined with that of other users to create an anonymized data pool; the collective information is then used to improve your experience on the app. But is it truly anonymous?

Researchers at North Carolina State University have released a study showing that a leading fitness-tracking app, Strava, seemingly has a vulnerability in its aggregated data usage that could enable bad actors to physically locate individual users, which might lead to stalking or harassment.

Strava has a “heatmap” feature in which users can see specific running, cycling, or hiking locations and routes that are popular among other users. The map uses aggregated data, which in theory “should make it impossible for anyone to capture private information about any specific user,” says the study’s lead author. “However, we found a loophole in certain conditions.”

Users who live in less-populated areas and who have listed the name of their hometown in their profile may be particularly at risk, the study notes. Researchers were able to align the heatmap data with the hometown information to “identify the home addresses of some users... and confirmed those identifications using [publicly available] voter registration data.”

Beyond the privacy risks uncovered by the NC State researchers, know that if you share your app-enabled workout information on social media, it may compound your exposure.



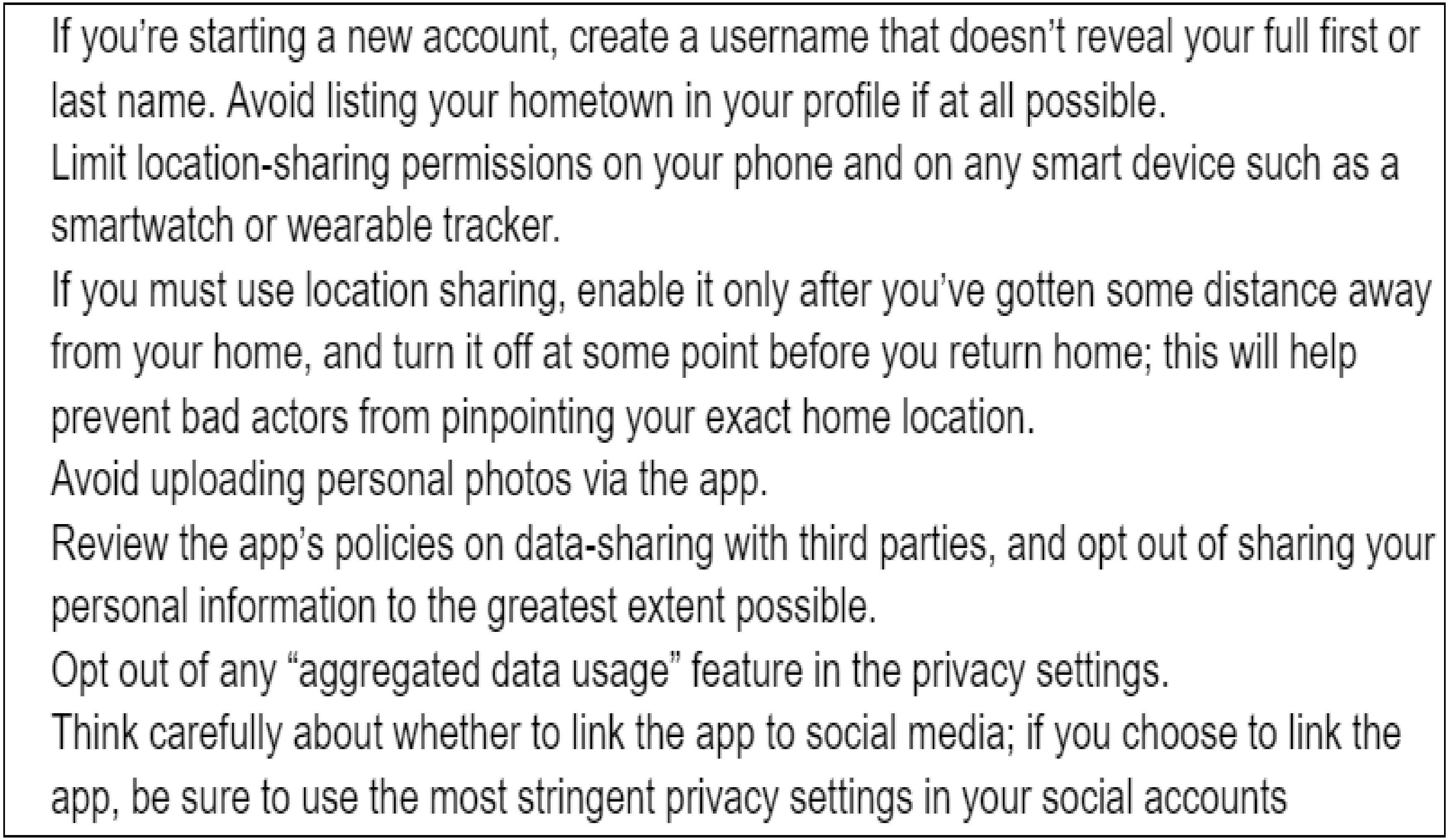
Depending on your privacy settings, people could use that information to physically locate and target you.

Fitness trackers can also potentially disclose your Personally Identifiable Information (PII) to data broker sites, which can in turn sell the data not only to marketers, but to any party willing to pay for it. (In this regard, fitness trackers are similar to mental health and wellness apps, many of which have demonstrated a willingness to sell user data to third parties.)

Finally, there’s the ever-present threat of a data breach. For example, the popular fitness app MyFitnessPal was hacked in 2018, affecting 150 million users; one year later, the stolen user data was found for sale on the dark web.

How to limit your privacy exposure in fitness apps

So how can you reduce your privacy risks? It boils down to two main strategies: Limit the amount and type of personal information you provide to fitness apps, and choose the strongest privacy settings possible. Specific steps include:



If you're starting a new account, create a username that doesn't reveal your full first or last name. Avoid listing your hometown in your profile if at all possible.

Limit location-sharing permissions on your phone and on any smart device such as a smartwatch or wearable tracker.

If you must use location sharing, enable it only after you've gotten some distance away from your home, and turn it off at some point before you return home; this will help prevent bad actors from pinpointing your exact home location.

Avoid uploading personal photos via the app.

Review the app's policies on data-sharing with third parties, and opt out of sharing your personal information to the greatest extent possible.

Opt out of any "aggregated data usage" feature in the privacy settings.

Think carefully about whether to link the app to social media; if you choose to link the app, be sure to use the most stringent privacy settings in your social accounts

- Generative Artificial Intelligence
- Cloud Services
- SPAM & Phishing more dangerous
- Link-based 67%
- Compromised websites attachments 33%

Email security threats

Current Issues

- North Korea remote workers

  Hired by US companies

  Paid for home Internet

- Prompt injection into resumes

  Near invisible keywords to trigger AI

- Surveillance tower in Mexico

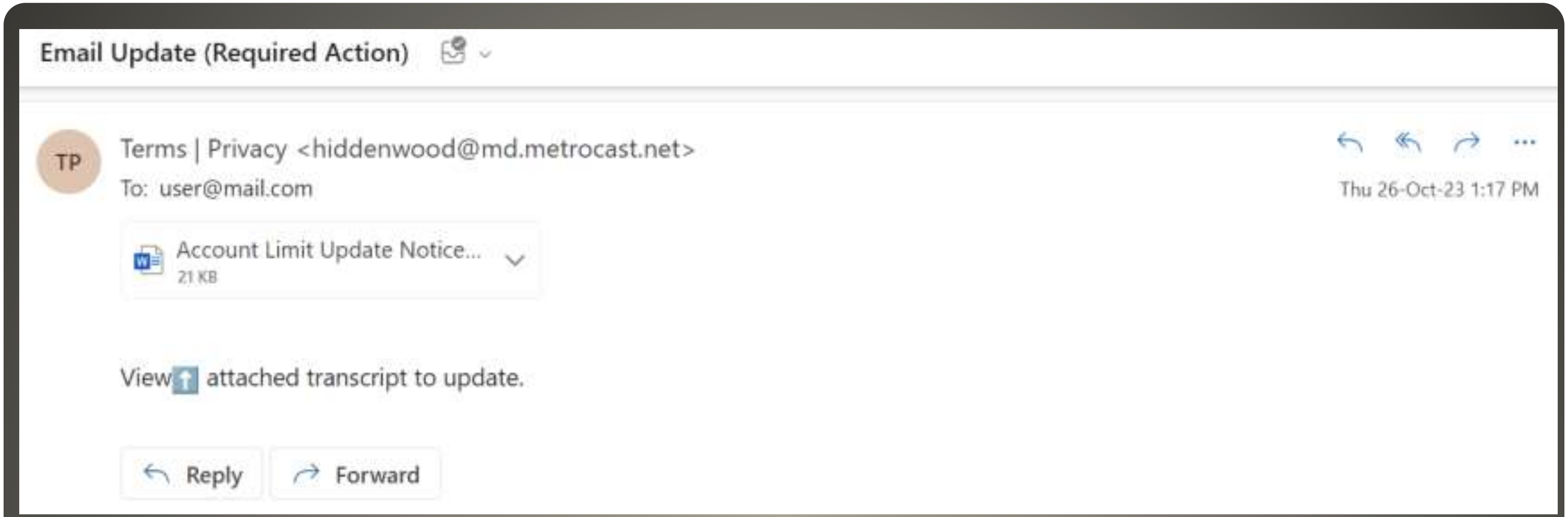
  20 storied high, 1791 license plate readers

  3000 pan-tilt-zoom cameras

  Deal with State of Texas?

- Who repairs your devices?

https://www.cbc.ca/news/business/marketplace-tech-repair-snooping-1.7000775



Email Update (Required Action)

Terms | Privacy <hiddenwood@md.metrocast.net>

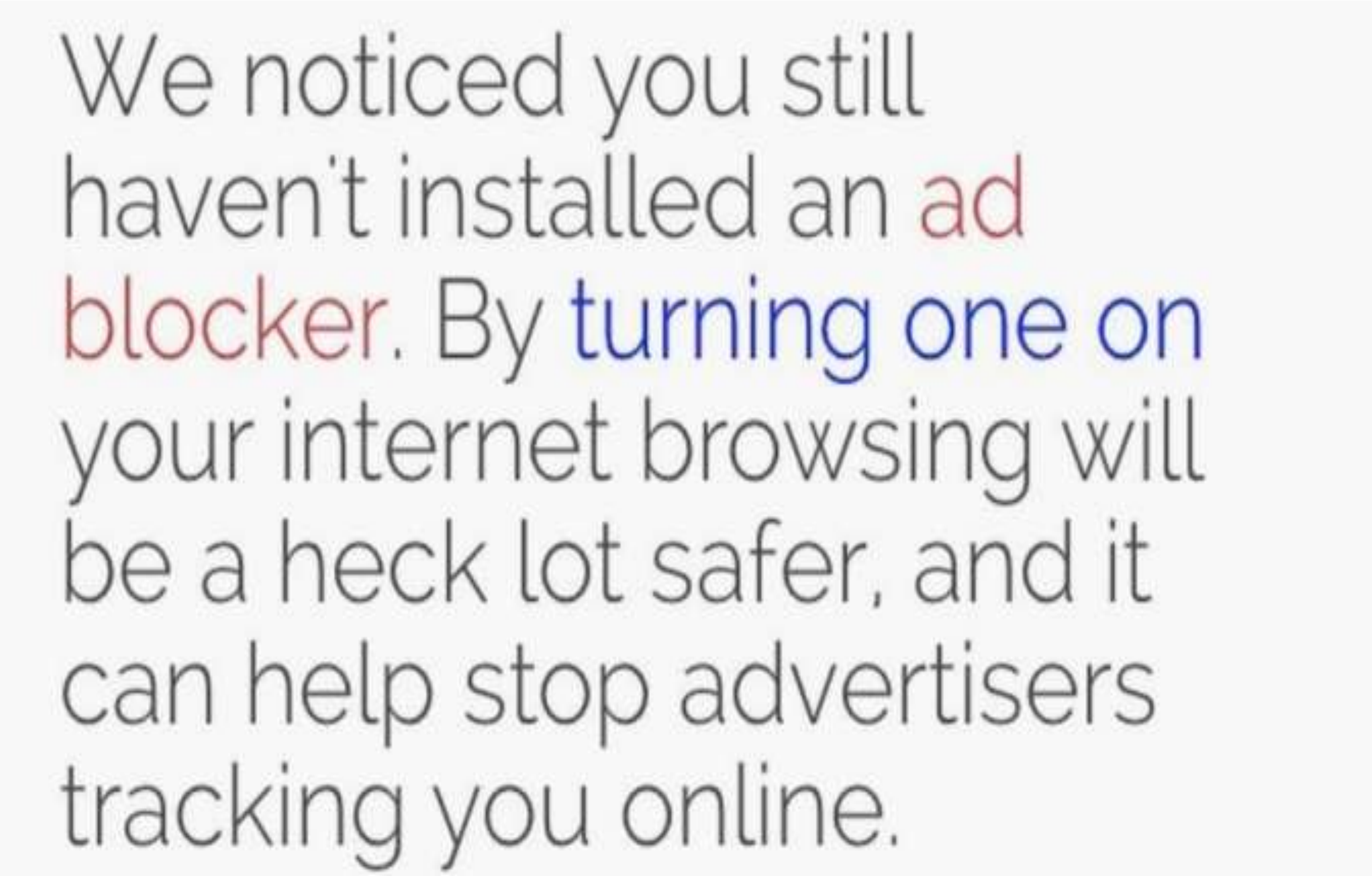
To: user@mail.com

Thu 26-Oct-23 1:17 PM

Account Limit Update Notice...
21 KB

View⬆️ attached transcript to update.

Please No



We noticed you still haven't installed an ad blocker. By turning one on your internet browsing will be a heck lot safer, and it can help stop advertisers tracking you online.

Quishing

- Super Bowl Ad QR Code
- Phishing -> Smishing -> Quishing
- Helpful <-> Harmful
- DON’T SCAN
- Open website, download malware
- Bypass most filters (no words/text/links)

- Android QR scanner
  Add to Google Wallet

- Never Scan QR codes

  Use known good contact methods
- THINK before providing:

  Personal Information

  Banking information

  Brokerage information

  Credit/debit/banking numbers/info
- Unsolicited => information gathering

Current Issues

- Flipper Zero Bluetooth Spam

  Android and Windows

  Spoof advertising packets

  transmit to devices in range

  Non-Stop mode

Android

Settings > Google > Nearby Share > Off

Settings > Connected Devices > Connection Preferences > Nearby Share

Windows

Settings > Bluetooth & devices > Devices > Device settings > Show notifications to connect using Swift Pair > Off

- 23andMe - getting worse?
- Freelance North Korean workers
- Colorado Supreme Court upholds
  Keyword search warrants
  Names of innocent
  constitutionally protected search history
- Google and Apple
  Disable live traffic maps Israel & Gaza
- Pro Russia hackers target Roundcube email services
  Capture email to forward to attacker's server
- CCleaner customer data stolen
- Apple private Wi-Fi MAC address
  iOS 14 – never worked
  Exposed IP addresses when Lockdown mode
  Fixed iOS 17.1
- Microsoft Secure Future Initiative AI

Current Issues

- SolarWinds RCE vulnerabilities
  Access Rights Manager

Why do I care?
Your data they’ve collected
Your data they’ve bought

Your data now sold

Current Issues

SolarWinds

- SEC Suit
- Failure to publicly disclose alleged cyber security failures
- Thousands of customer organizations

  Nine federal agencies
- 2020
- “publicly disclose vulnerabilities”
- Russia

- YouTube v. Ad Blockers

  Should require user consent and notification
  Spyware
  Re-enable accounts
  Delete all personal data so obtained

- Incogni - Personal data removal tool

  Regulatory requirement to remove personal data
  Time consuming - knowledge of all data sources
  180 data sources
  Sign-up - give up info you are trying to protect
  Tied to VPN provider
  No mobile app
  One email address
  Little detail

Current Issues

- Permission Slip by CR
- Every app   Every service   What purpose?
- Yet another data miner?
- "We do not sell your personal information in a way that most people would think of as a sale. However, we do participate in online targeted advertising and use analytics which allows tech companies, in exchange for our use of their services, to use user information collected from our App to improve their own products and to improve the services they provide to others. Under some laws, this is considered our "sale" of your user data to third parties. You can opt-out of this as provided in the “How to Submit a Request” section below.“
- Authorized agent
- California law   Colorado law

Consumer Reports

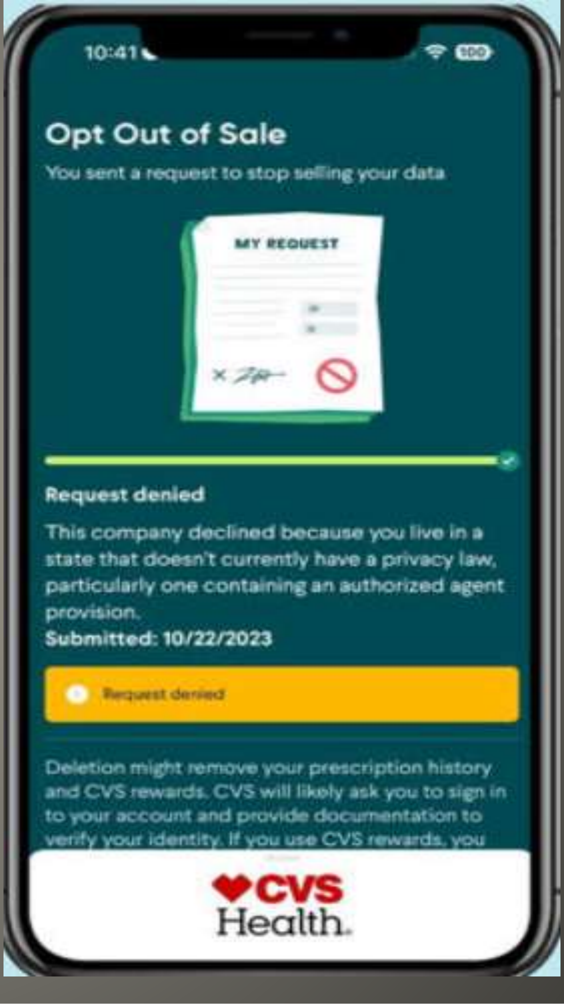
Privacy

- Time to (re)scrub your personal data
- CVS, Lowes, Yahoo, Spokeo
- Each company

  What they collect

  e.g. account info, biometrics, communications, location, demographics, identifiers, jobs & education, purchases, preferences, online tracking, other
- Do Not Sell My Data
- Delete My Account
- Mobile phone

  Colorado, California, …
- Other email addresses



10:41

Opt Out of Sale

You sent a request to stop selling your data

Request denied

This company declined because you live in a state that doesn't currently have a privacy law, particularly one containing an authorized agent provision.

Submitted: 10/22/2023

Request denied

Deletion might remove your prescription history and CVS rewards. CVS will likely ask you to sign in to your account and provide documentation to verify your identity. If you use CVS rewards, you

CVS Health.

How did they get my personal data?

- We give it up
- Public records
- Online activity

  Cookies, web beacons, device identifiers, … …
- Offline activity

  Physical purchases, subscriptions, surveys, loyalty programs, events attended, …
- People search services
- Marketing and advertising
- Risk mitigation
- Fraud prevention

- Contact Key Verification - beta
- Opt-in
- Alert iMessage Key distribution service
  unverified key
  new device added
- More secure in person, FaceTime, other
- End-to-end encryption 2011
- iOS 14 BlastDoor
- iOS 16 Lockdown Mode
- iOS 17 CKV

Apple iMessage

Apple CKV

- Six requirements

  Secure source of truth

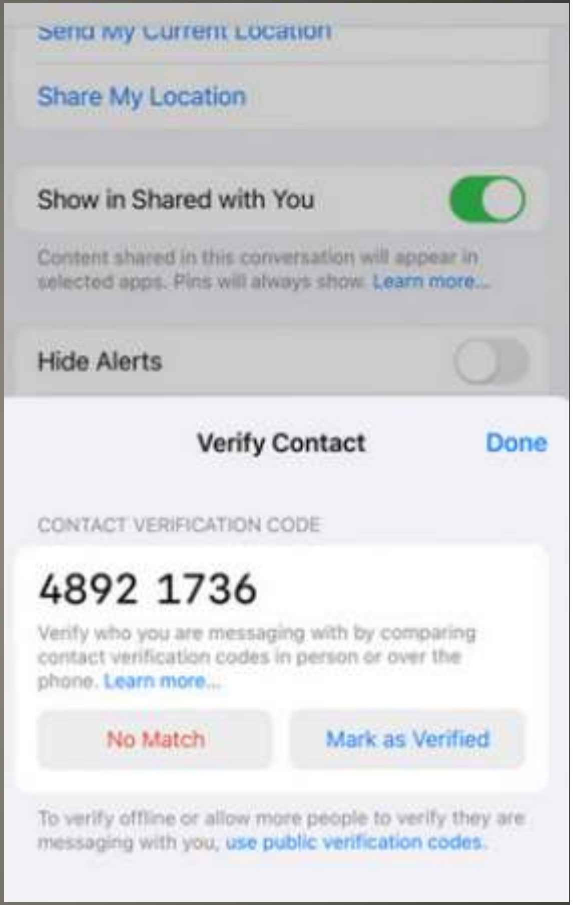
  Automatically verify

  Synchronize source of truth

  Detect Split views

  Scale

  Notify users



Send My Current Location

Share My Location

Show in Shared with You ●

Content shared in this conversation will appear in selected apps. Pins will always show. Learn more...

Hide Alerts ○

Verify Contact Done

CONTACT VERIFICATION CODE

4892 1736

Verify who you are messaging with by comparing contact verification codes in person or over the phone. Learn more...

No Match

Mark as Verified

To verify offline or allow more people to verify they are messaging with you, use public verification codes.

- Okta’s Support Unit breach
  Cloudflare and 1Password affected
- Wyze Cam v3 firmware RCE flaw
  PoC gives root shell
  Firmware update Oct 22, 2023
  4.36.11.7071
  Network isolation
- Microsoft system level ban unauthorized Xbox accessories
  error 0x82d60002 - you’ve got 2 weeks
  competitive advantage online games
- VBScript Microsoft support to end
- NTLM protocol to be discontinued
- cURL vulnerabilities

Current Issues

- Security Features
- Anonymity & Data Protection
- Open Source
- Regular Updates
- User Friendly
- Community & Support

==========================

Tails

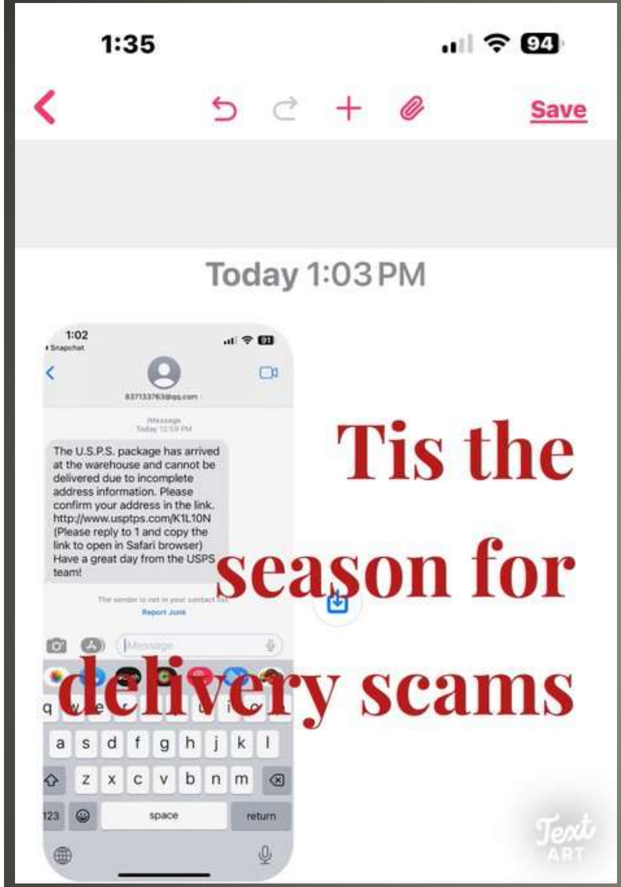
Qubes OS

Whonix

Linux Mint with Cinnamon

PureOS

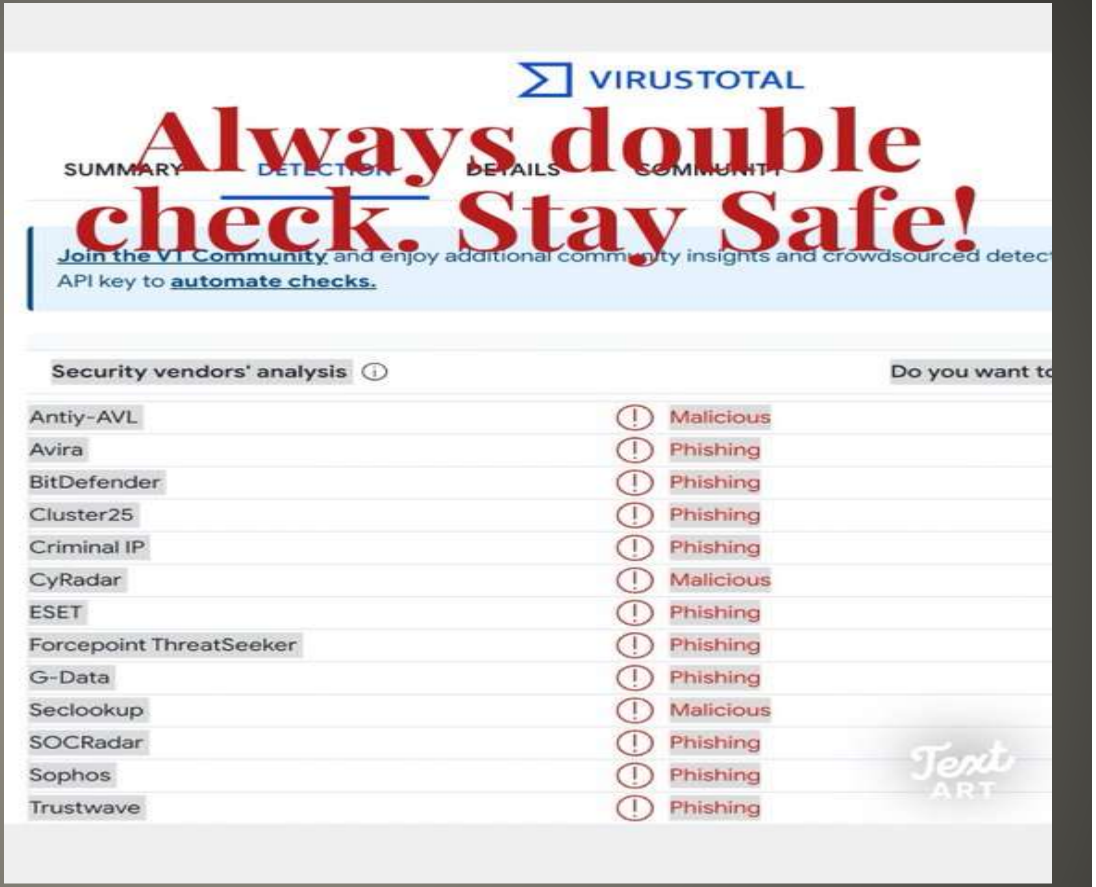
Privacy focused Operating Systems



Today 1:03 PM

The U.S.P.S. package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link. http://www.usptps.com/K1L10N (Please reply to 1 and copy the link to open in Safari browser) Have a great day from the USPS team!

Tis the season for delivery scams



Always double check. Stay Safe!

Join the VT Community and enjoy additional community insights and crowdsourced detec
API key to automate checks.

Security vendors' analysis	Do you want to
Antiy-AVL	Malicious
Avira	Phishing
BitDefender	Phishing
Cluster25	Phishing
Criminal IP	Phishing
CyRadar	Malicious
ESET	Phishing
Forcepoint ThreatSeeker	Phishing
G-Data	Phishing
Seclookup	Malicious
SOCRadar	Phishing
Sophos	Phishing
Trustwave	Phishing

VirusTotal

- 20,000 enterprises
- Wide-scale compromise
- Citrix Netscaler
- October 10 patch available
- Patch & reboot – session tokens persist
- Replay session token – in

  No credentials, no MFA just in

  Junk to crash OpenID, leak memory

  exploited late August
- Not an easy patch
- Cisco --- IOS XE
- Ghidra (NSA tool) before & after patch
- snprintf

CitrixBleed

Why do I care?

- The data leaked, stolen, analysed
- Is yours and mine and those we care about

Artificial Intllegence
Machine Learning
Large Language Models

AI

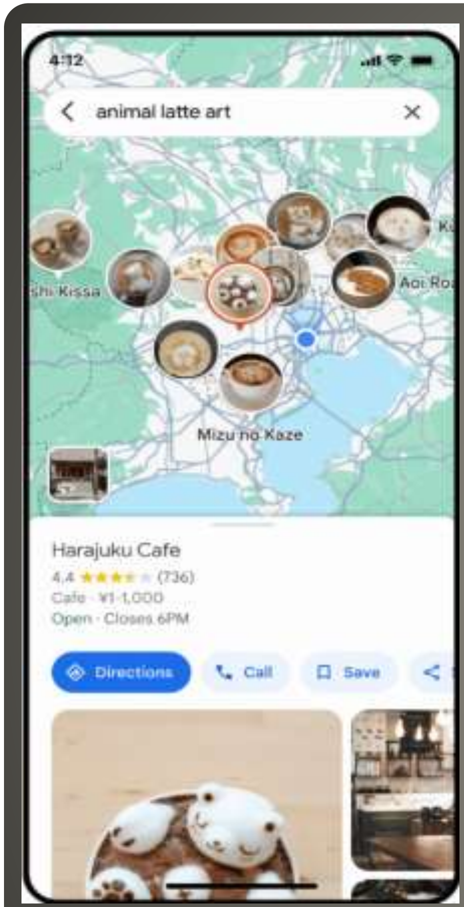
- Chat GPT   Sydney
- AI Hallucination
- AI Emergent Properties
- IoT Sig AI Presentation

- How they are built

  Intellectual property
- How they work

  They don’t know
- Emergent Properties
- Hallucination
- Powers of persuasion
- AI Anxiety
- Inaccurate Health information
- Technology Addiction
- Health data Privacy
- Harassment & cyberbullying

AI more powerful   more secretive



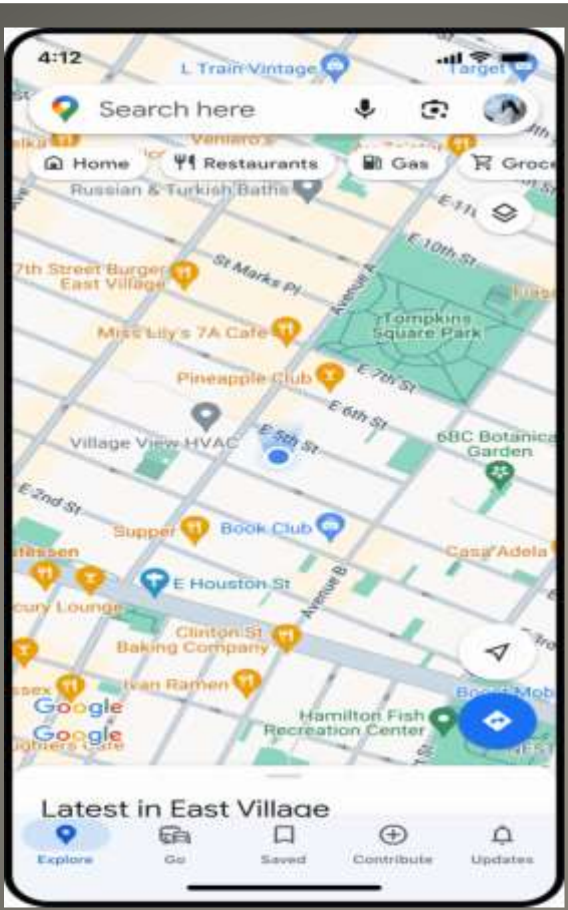
animal latte art

Harajuku Cafe

4.4 ★★★★☆ (736)

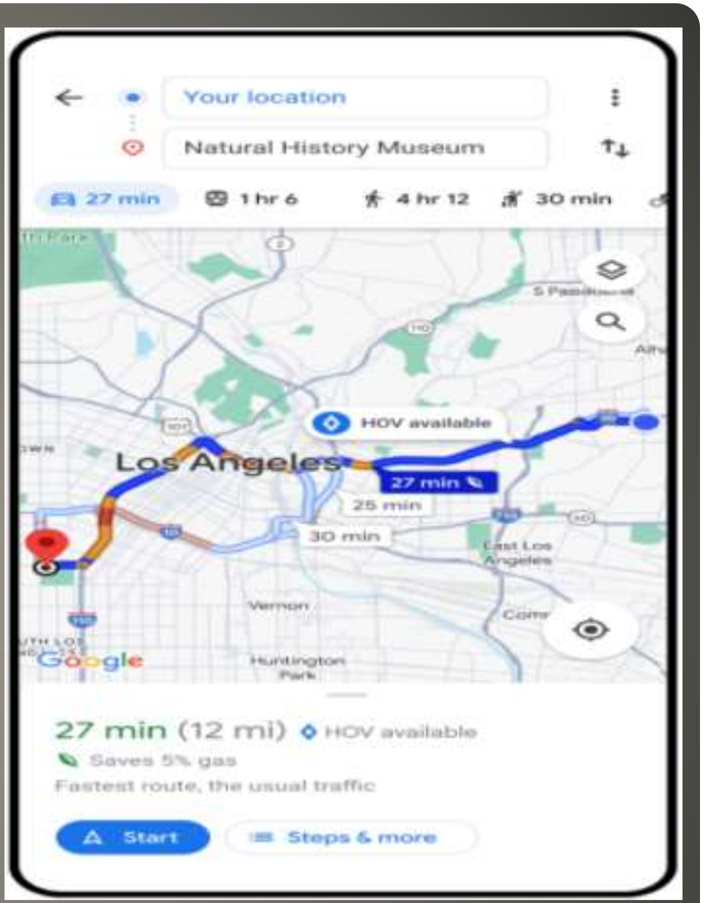
Cafe · ¥1-1,000

Open · Closes 6PM



Search here

Latest in East Village



Your location

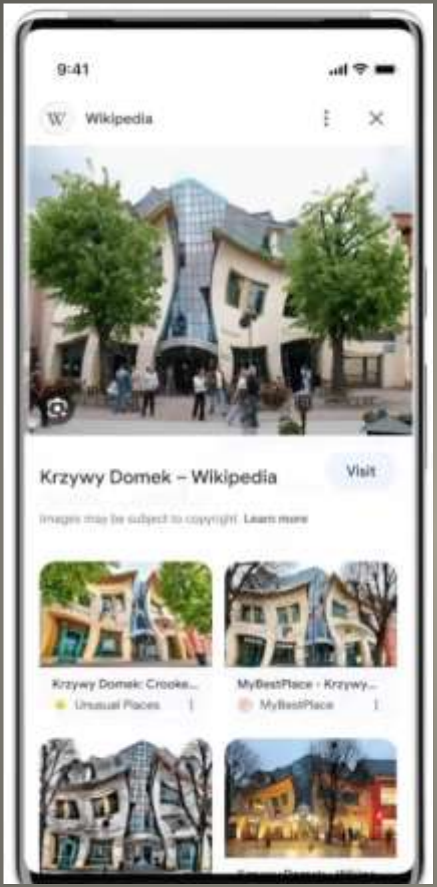
Natural History Museum

27 min (12 mi) HOV available

Saves 5% gas

Fastest route, the usual traffic

Google Maps AI boost



Google Image Verification tool

- Shutdown

"deactivated Microsoft-generated polls for all news articles" and is "investigating the cause of the inappropriate content."

Microsoft news article polls

Google Bug Bounty

- Generative AI Attacks

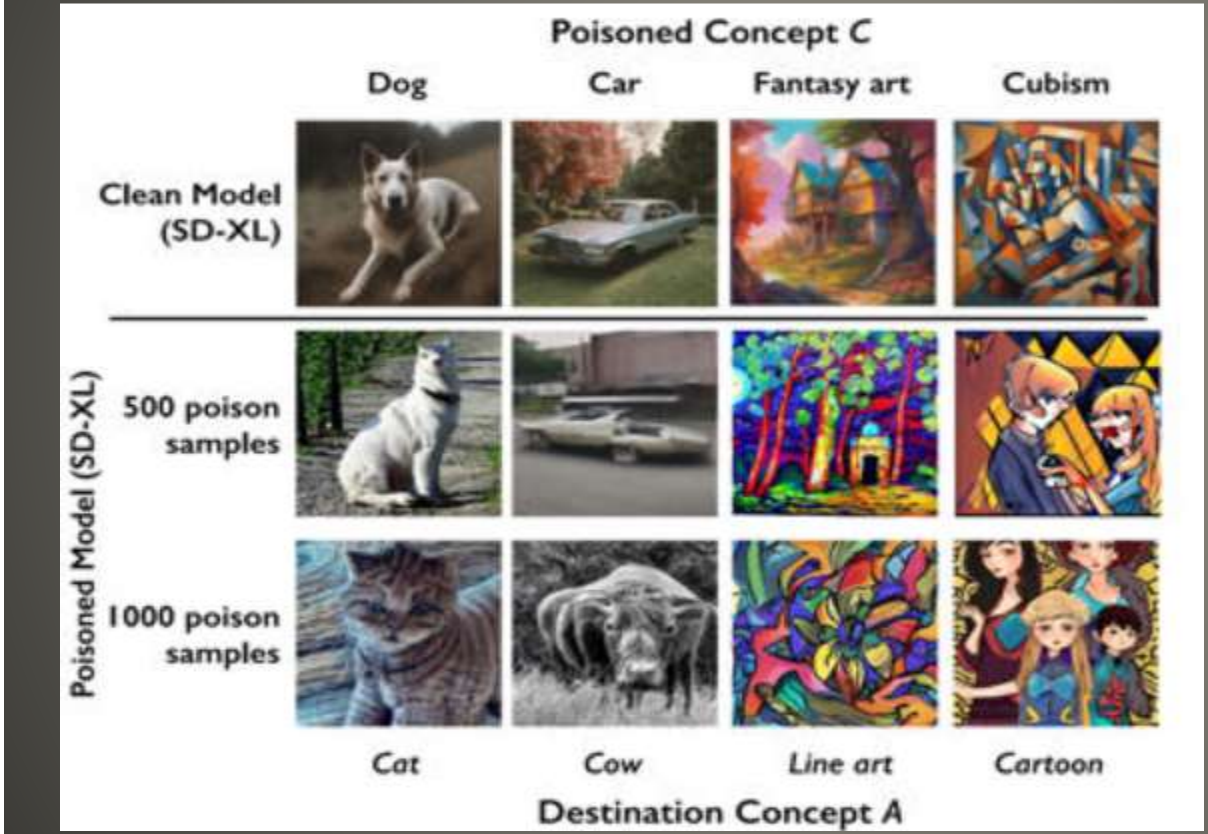
- Chatbots “talk to books”
- Conversational companions
- *Solution Tree*
- *Retrieval Augmented Generation*
- Mary Shelly’s *Frankenstein*
- That monster vs AI monster?
- AI suggests reader might identify with monster loneliness, rejection, desire companionship

YouAI Book AI

- Coding Art & Science
- WatsonX IBM training on company data
- Privacy and Regulatory requirements
- Watson Code Assistant
- Decades old Cobol (1959)
- 70% global banking apps Cobol & mainframe
- Who knows Cobol?
- Convert Cobol – Java
- On Mainframe

WatsonX

- “poison” Images
- “Confuse” AI



Nightshade

LLEMMA

- Math focused Open Source AI

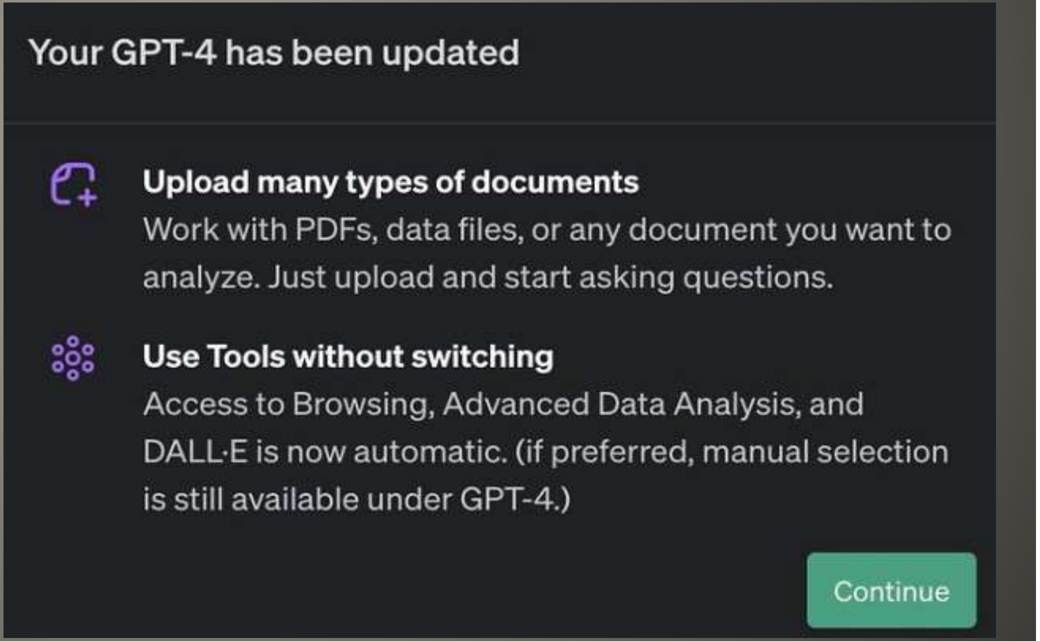
- Video game
- Created ChatGPT, Midjourney, DALL-E 3

Angry Pumpkins

Humane AI Pin

- Rethinking smart phone
- Last presentation 10-19-2023

- “All Tools” - less context switching
- Enhanced document analysis capabilities PDF
- Updated knowledge cutoff date
- DALL-E 3
- DevDay event
- ChatGPT Plus



Your GPT-4 has been updated

Upload many types of documents
Work with PDFs, data files, or any document you want to analyze. Just upload and start asking questions.

Use Tools without switching
Access to Browsing, Advanced Data Analysis, and DALL·E is now automatic. (if preferred, manual selection is still available under GPT-4.)

Multimodal GPT-4

- New Standards for AI Safety and Security
- Protecting Americans' Privacy
- Advancing Equity and Civil Rights
- Standing Up for Consumers, Patients, and Students
- Supporting Workers
- Promoting Innovation and Competition
- Advancing American Leadership Abroad
- Ensuring Responsible and Effective Government Use of AI

Biden Administration AI Executive Order

- Cloud computing presentation from ChatGPT please
- LinkedIN followed up with cloud message Oracle Cloud
- The ChatGPT presentation was point on

AI & me

- Anonymous and secure AI chatbot
- Leo
- Brave browser 1.60

Brave

Artificial General Intelligence

- Google DeepMind AI lab co-founder
- 2028 50-50%
- Computational power growth
- Data quality growth

- The measure of human intelligence?

- The lifetime
- Power consumption

- EMP

- Recovery Seminar - soon
- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com