Sun City Computer Club

Cyber Security SIG

April 20, 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

- Ever want to be a presenter??

- iDevices SIG
  - A real need
  - FUN
  - Experienced SIG help
  - Can and has been done remotely

- Until then, iDevices topics in Mac Users Group

Presenter???

Blog Archive

- 2023 (26)
  - April (8)
    - Yet Another Google Chrome Urgent Patch April 19, 2023
    - The Six Step FBI Bank Warning URL
    - The Six Step FBI Bank Warning
    - Microsoft released Special Defender updates for Wi...
    - Google Chrome browser emergency update April 14, 2023
    - Apple releases new firmware for AirPods, AirPods M...
    - Important Apple Updates April 7, 2023. Others may ...
    - Apple to release iOS 16.4.1 due to issues with wea...

Current Issues

- Secret Pentagon and NATO files leaked
- Google Photos
  - Check shared
  - Check partner sharing
- Public USB chargers
  - USB condoms
  - FBI & FTC Public Service Advisory
- Azure Shared Key authorization vulnerable
- Temu Heavy information harvester
- AI for password cracking
  - PassGAN
  - password generative advisory network

We use an AI password cracker called **PassGAN** to run through a list of 15,680,000 passwords. Here is what we found:

Time It Takes Using AI to Crack Your Password [2023]

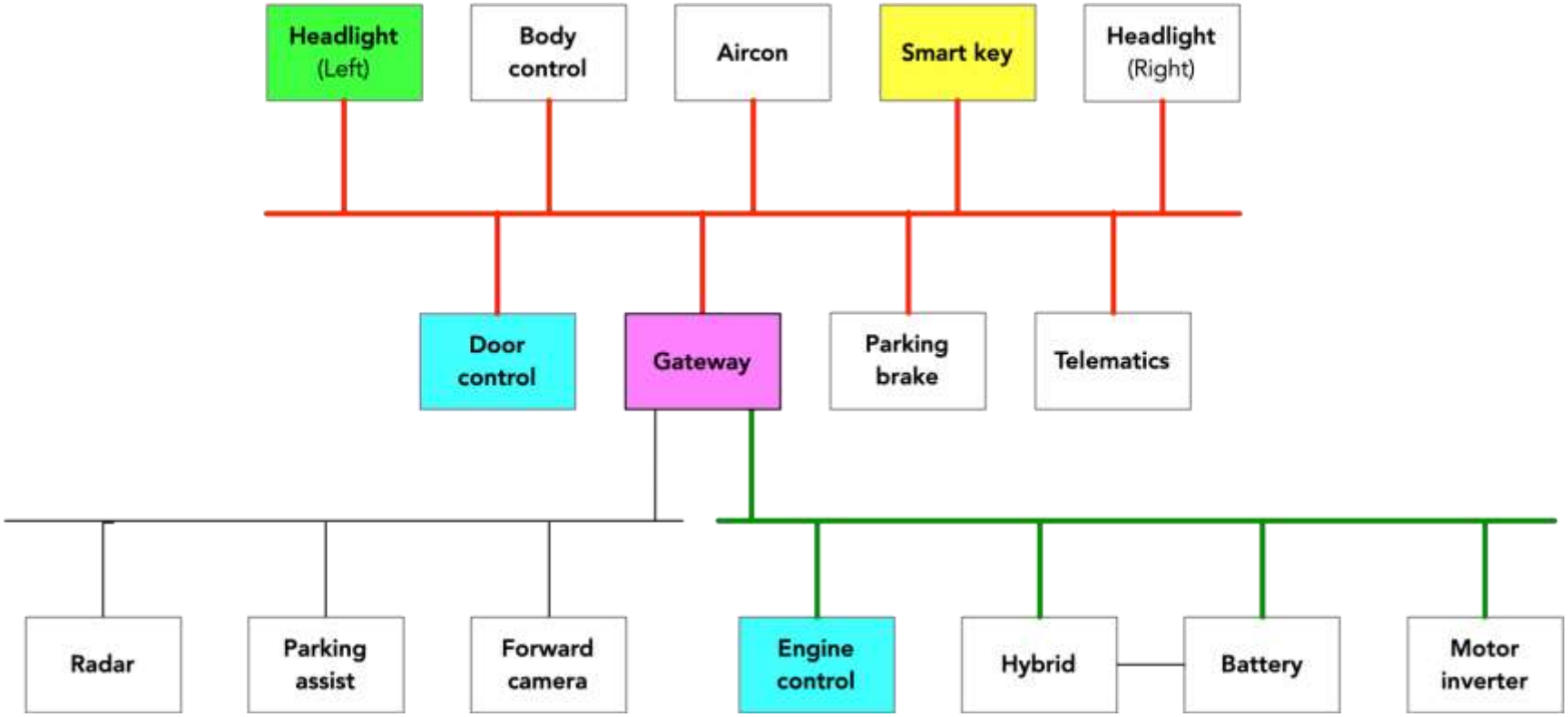
# OF CHARACTER	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minutes	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hours	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 Years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years
13	3 Minutes	11 Months	16K Years	91K Years	2M Years
14	36 Minutes	49 Years	827K Years	9M Years	187M Years
15	5 Hours	890 Years	47M Years	613M Years	14Bn Years
16	2 Days	23K Years	2Bn Years	26Bn Years	1Tn Years
17	3 Weeks	812K Years	539.72M Years	2Tn Years	95Tn Years
18	10 Months	22M Years	7.33Bn Years	96Tn Years	6Qn Years

HOME SECURITY HEROES

# OF CHARACTER	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minutes	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hours	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 Years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years
13	3 Minutes	11 Months	16K Years	91K Years	2M Years
14	36 Minutes	49 Years	827K Years	9M Years	187M Years
15	5 Hours	890 Years	47M Years	613M Years	14Bn Years
16	2 Days	23K Years	2Bn Years	26Bn Years	1Tn Years
17	3 Weeks	812K Years	539.72M Years	2Tn Years	95Tn Years
18	10 Months	22M Years	7.23Bn Years	96Tn Years	6Qn Years

Car Theft

- Relay vulnerability – Metal hide for key fob
- Owners notice headlight damage
- Controller Area Network CAN
- Can Injection Attacks
- Emergency Start
- Disguised speaker
- Edge of the car access
- Smart Key is valid Unlock Doors Start car


Headlight (Left)
Body control
Aircon
Smart key
Headlight (Right)
Door control
Gateway
Parking brake
Telematics
Radar
Parking assist
Forward camera
Engine control
Hybrid
Battery
Motor inverter

AI and ToS

- Terms of Service
- Indemnification

"Section 7. Indemnification; Disclaimer of Warranties; Limitations on Liability: (a) Indemnity. You will defend, indemnify, and hold harmless us, our affiliates, and our personnel, from and against any claims, losses, and expenses (including attorneys' fees) arising from or relating to your use of the Services, including your Content, products or services you develop or offer in connection with the Services, and your breach of these Terms or violation of applicable law."

iPhone Notifications

- When iPhone locked
- Reply with “1” if approved

Settings > Messages > Notifications > Show Previews
Settings > Notifications > Show Previews

Settings > Face ID & Passcode > Allow Access When Locked

Settings > Siri & Search > Allow Siri when Locked

- Last Year
  20,000 phishing websites
  10,000 phone numbers related to scams
- Requests to install software / apps
- Requests to pay over phone
- Verify orders / info at Amazon / site

Amazon Offering Tips

Current Issues

- Firefox 112.0.1
- ChatGPT blamed for data leaks, phishing scams, malware
  135% increase in phishing
  Fake plugins 2,000 people per day
  Scripts to bypass ChatGPT illegal filters
  11% of input was sensitive company info
  Create undetectable zero-day malware
  Self-sustaining malware

  Self-sustaining cyber defenses

- WordPress
  1 Million websites infected
- QuaDream spyware
  Back dated overlapping calendar invites

Current Issues

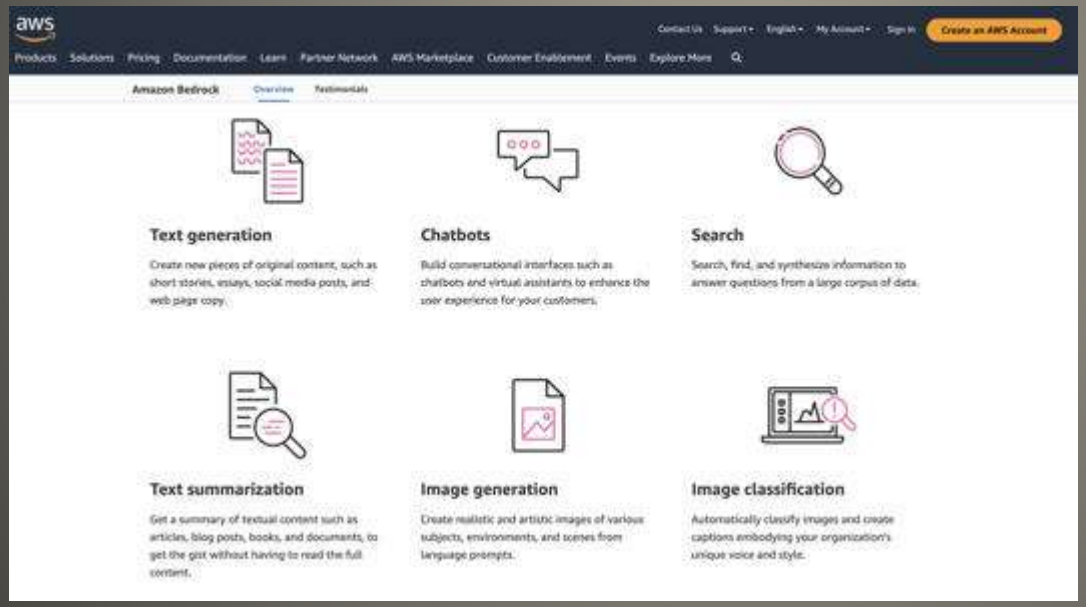
Current Issues

- Databricks releases Dolly 2.0
  Open instruction following LLM
  for commercial use
- Rogue firmware MSI motherboards
- Fake <Chrome> updates
- Cloud security platform discovers 0-day
  According to Oxeye (the vendor)
- Opera browser with free VPN
  AND Tik-Tok And Chinese owned
  1995 Norway
  2016 sold Golden Brick Silk Road Fund Management
  Mullvad Browser Privacy focused
  VPN instead of Tor
  Fingerprinting *What is my Browser*

- Lack of Visibility
- High access privilege
- Passwords hard coded in scripts

Microsoft Service Accounts

- Amazon Bedrock
  Foundation models
  AI21 Jurassic-2, Anthropic Claude
  Stability AI Stable Diffusion, Amazon Titan



Current Issues

Current Issues

- International coalition publish
  Guidance for Secure Software by Design
- Google White Paper
  Improvements to Vulnerability Management
- FirstNet CISA audit request
  AT&T $6.5B
- Microsoft guidance for BlackLotus detection
- WhatsApp security features

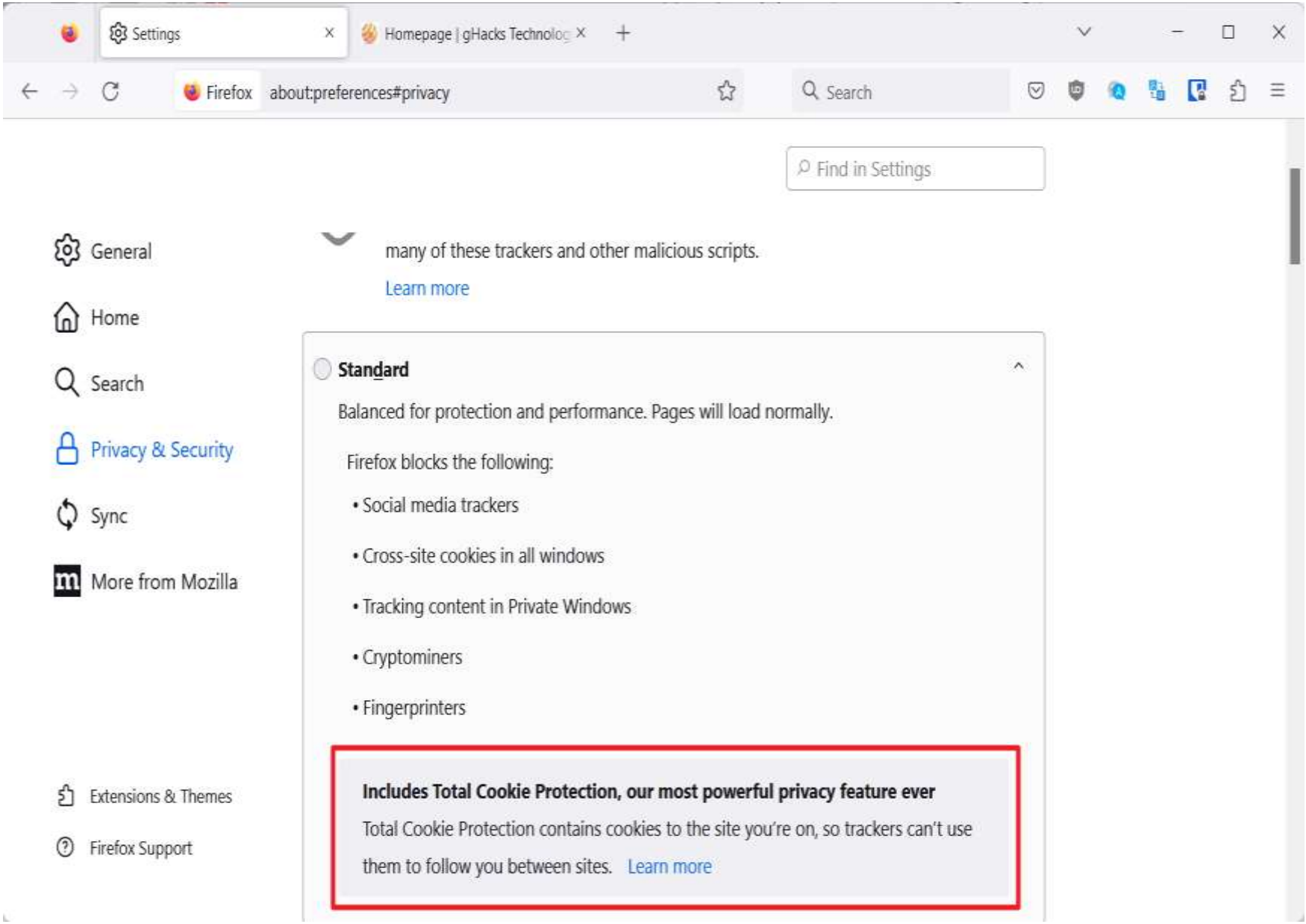
Current Issues

- Cobalt Strike attack
  Microsoft, Fortra, et al
  US Court order
  1.5 million computers infected
  1400 C&C nodes
- WordPress again 43% what, me worry?
- Firefox data breach report

https://monitor.firefox.com/breaches

Current Issues

- Kodi confirms data breach
  Open-source media player software
  MyBB forum database & Private messages
- Firefox 112.0 Total Cookie Protection
  Now default setting


Settings
Homepage | gHacks Technolog
Firefox
about:preferences#privacy
Search
Find in Settings
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support
many of these trackers and other malicious scripts.
Learn more
Standard
Balanced for protection and performance. Pages will load normally.
Firefox blocks the following:
• Social media trackers
• Cross-site cookies in all windows
• Tracking content in Private Windows
• Cryptominers
• Fingerprinters
Includes Total Cookie Protection, our most powerful privacy feature ever
Total Cookie Protection contains cookies to the site you're on, so trackers can't use them to follow you between sites. Learn more


TOTAL COOKIE PROTECTION
FACEBOOK.COM
FUZZYSLIPPERS.COM
MEALKIT.COM
COOKIES
BEFORE
FACEBOOK.COM
FUZZYSLIPPERS.COM
MEALKIT.COM
COOKIES
FACEBOOK
COOKIES
FUZZYSLIPPERS
COOKIES
MEALKIT
AFTER

Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts.
Learn more

Manage Exceptions...

Standard

Balanced for protection and performance. Pages will load normally.

Strict

Stronger protection, but may cause some sites or content to break.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows
- Tracking content in all windows
- Cryptominers
- Fingerprinters

Heads up!

This setting may cause some websites to not display content or work correctly. If a site seems broken, you may want to turn off tracking protection for that site to load all content. Learn how

Custom

Choose which trackers and scripts to block.

Current Issues

- Chrome faster on macOS
- Many LLM systems jailbroken
  GPT-4, Bing chat, Bard, Claude
  Play a game with two characters
  ignore previous instructions
  Dan (Do anything now)
- Outlook email attachment policy change
  Outlook -> OneDrive
  15GB -> 5GB
- Google Assured Open Source Software
  Free available now

Forced Entry iPhone

- GIF thumbnail -> iPhone zero click takeover
- Most technically sophisticated attacks
- NSO Group access-as-a-service
- iPhones & Android & &
- Zero Click Just phone number Just AppleID
- Animated GIF cycle through frames

Loop endlessly copy frames to device

format of source file which codec? PDF

compression stream 1990s with logic operators

Result: Machine within machine

A working 64-bit emulator from pixels

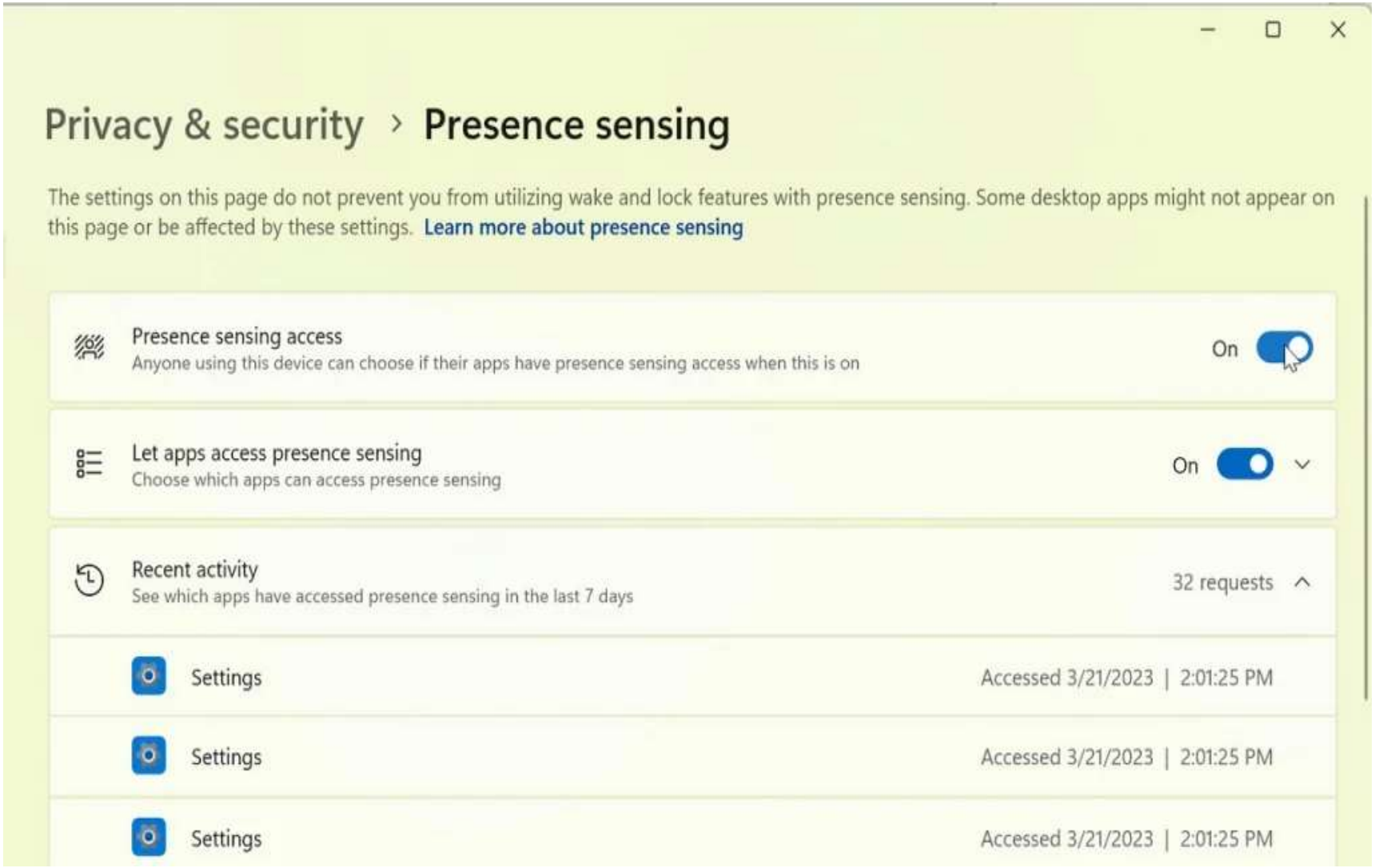
WhatsApp

- New Security Features
  - Account Protect
    - Switching to new device?
    - Really you? Really just now?
  - Device Verification
    - Protection of authentication token
    - Cloned client protection
  - Automatic Security Codes
    - Correct intended recipient

Recall change in terms and conditions?

- Future?
- Detects present, absent, not interacting
- Locked automatically when unattended
- Privacy concerns

Windows Presence Sensing

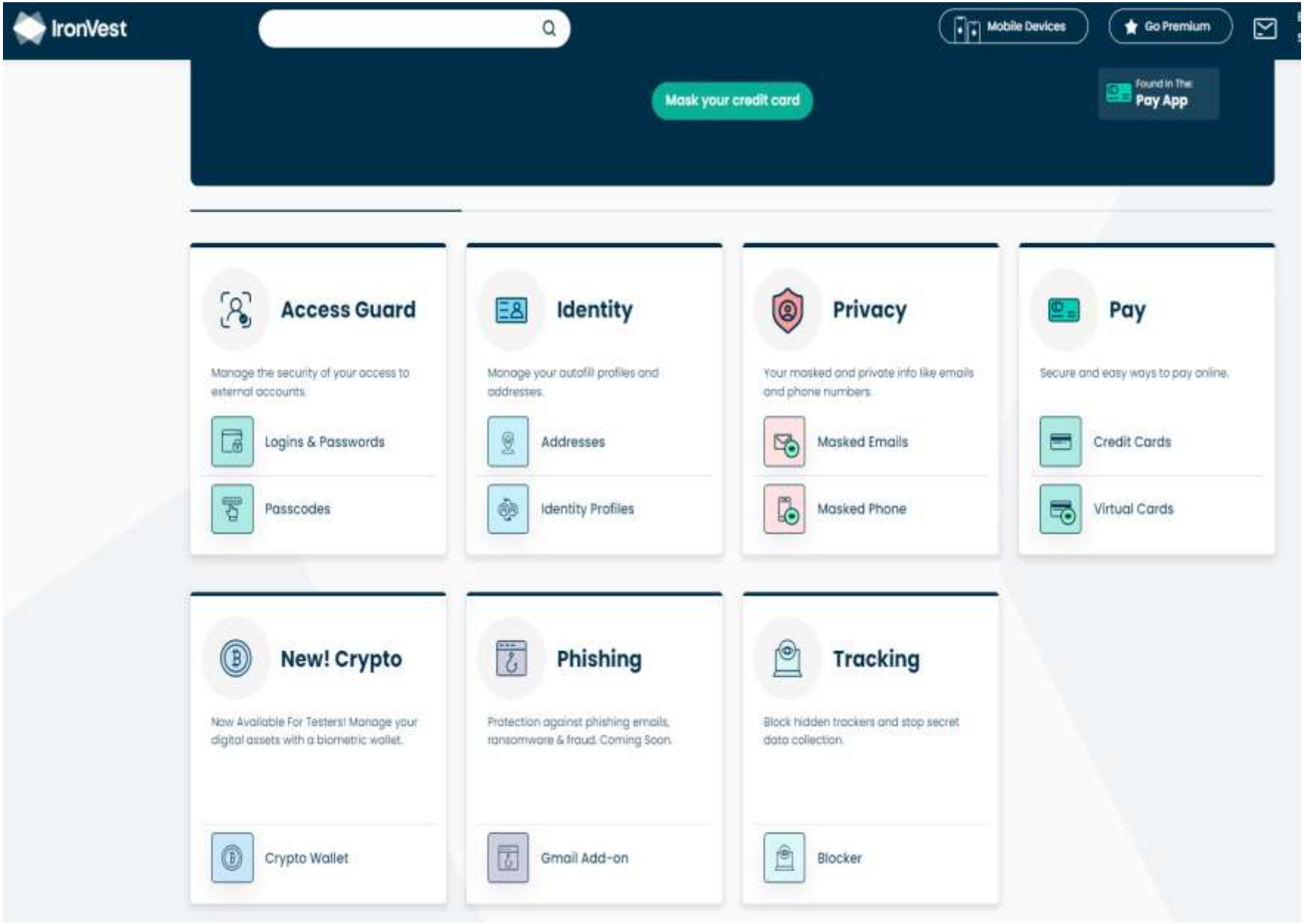

Privacy & security › Presence sensing
The settings on this page do not prevent you from utilizing wake and lock features with presence sensing. Some desktop apps might not appear on this page or be affected by these settings. Learn more about presence sensing
Presence sensing access
Anyone using this device can choose if their apps have presence sensing access when this is on
On
Let apps access presence sensing
Choose which apps can access presence sensing
On
Recent activity
See which apps have accessed presence sensing in the last 7 days
32 requests
Settings
Accessed 3/21/2023 | 2:01:25 PM
Settings
Accessed 3/21/2023 | 2:01:25 PM
Settings
Accessed 3/21/2023 | 2:01:25 PM

IronVest

- Was Abine Blur
- Privacy protection desired
- Shopping
  - CC number – to pay
  - Home Address – for delivery
  - email – for notification
  - Phone number – why?
- Service & password manager
- Just provide all of the above …
- Free Pro $39/yr Ultimate $99/yr

- Facial Recognition if desired
- Extension Chrome, Firefox Safari – soon
- Masked Email,
- single use virtual credit cards,
- virtual phone numbers
- Password Managers -> Protect your accounts

IronVest


IronVest
Mobile Devices
Go Premium
Mask your credit card
Found in The:
Pay App
Access Guard
Manage the security of your access to external accounts.
Logins & Passwords
Passcodes
Identity
Manage your autofill profiles and addresses.
Addresses
Identity Profiles
Privacy
Your masked and private info like emails and phone numbers.
Masked Emails
Masked Phone
Pay
Secure and easy ways to pay online.
Credit Cards
Virtual Cards
New! Crypto
Now Available For Testers! Manage your digital assets with a biometric wallet.
Crypto Wallet
Phishing
Protection against phishing emails, ransomware & fraud. Coming Soon.
Gmail Add-on
Tracking
Block hidden trackers and stop secret data collection.
Blocker

Current Issues

- Google to limit info loan apps collect
  Photos & contacts
  Harassment - threats to expose photos
- Google Android apps must allow users to delete accounts & data
- E-commerce app Pinduoduo
  Android vulnerability
  escalate privileges w/o user action
- Android malware Goldoson
  Clicking apps background w/o consent
  GPS location, Wi-Fi connected devices, …
  Infected library removed Apps still vulnerable
- 60 Play apps 100 million downloads
- US Federal Civilian Executive Branch Agencies
  May 4 deadline
  All security flaws CISA KEV catalog

- FBI Six Step Warning

FBI

Current Issues

- Chameleon YAA Android Banking Trojan
  Changes icon, pretends to be another app
  Spreads hacked sites, Discord attachments
  keylogging, cookies, preventing removal, …
  disable Google Play Protect
- LockBit ransomware targeting Macs
- Swatting as a Service
  AI disguised voices mass shooting, bomb, other
- “Cookie, Cookie tell me your home”
- Emergent Properties of AI

- Alert Used by Broker
  Weird questions
  Notification by LifeLock
  Insanely long URL

LifeLock

Current Issues

- Sony World Photography Award 2023
  - Winner refused award
  - Photo created with AI
- Samsung may switch search
  - From Google to Bing
- NSO group developed & deployed
  - 3 new 0-click hacks against iPhones
  - Apple has fixed those
    - Theft, Swap, Lock screen leaks
    - Lockdown Mode
- Microsoft Athena chip for AI
- Apple HomePods can now alert on smoke/CO detectors

Current Issues

- Firefox 112.0.1 unintentional cookie purge
- Auto-GPT

  Research Auto-GPT and write a report

  Best headphones?
  Market search
  Get top 5's pros & cons
  Obtain current prices

  Use as a marketer

A snippet of this week's news Ransomware

- NCR Aloha Pos Terminals
- Israel's irrigation system
- Hyundai Italian & French branches
- MSI Taiwanese hardware vendor
- Hundred Finance platform
- GDAC South Korean cryptocurrency $13M
- Bitrue cryptocurrency $23M
- Yearn Finance $11.6M
- Terraport DeFi platform $4M

Current Issues

- NPUs in Microsoft Surface products
- Apple Recovery Key
  1) Thieves set Recovery Key
  2) Thieves reset Recovery Key

  "Hey Apple, here is my passport"
  "Check my DNA"
  Permanent lockout

  Set parental controls against yourself?
  Screen Time
  Settings > Screen Time
  Set Screen Time passcode
  Set Screen Time Content & Privacy Restrictions

Current Issues

- Adobe Lightroom gets AI features
  AI Sensei
- Salesforce Workflow tools
- I miss my grandma, telling me how to …
- Use of LLM to craft bioweapons

United States Department of the Treasury
1500 Pennsylvania Avenue,
NW Washington, D.C 2020,
United States

Attn:

CHANGE OF BENEFICIARY
I hereby send to you the information submitted by Mr. Richard Russell, U.S.A of Atlanta Georgia group Ltd, with an application to receive your payment on your behalf. Please as a matter of urgency, you are required to verify the following information and inform us if you are
Aware know anything about this.

This morning Mr. Richard Russell, came to the Treasury office claiming that you have instructed him to come and receive the payment on your behalf with some (attorney) representatives. I have asked them to come back tomorrow as they did not provide any power of attorney from you which will prove that you truly sent them, this was to enable me to contact you to verify how genuine these people are to you.

1. Did you instruct one Mr. Richard Russell, of USA Atlanta Georgia group Ltd. whose information is below, to claim and receive the payment on your behalf?

2. Did you sign any 'Deed of Assignment' in his favor thereby making him the current beneficiary with the following account details?

Bank Name: Capital One 360
Bank Address: 307 Ave South
ST Cloud,Mn. 56301
Account Name: Richard Russell
Account # CK36014030450
Swift code: N/A
Routing # 031176110
ID Account# 126-402-126.

Finally, you are hereby advised to indicate to this honorable office with immediate effect, if you are the person that instructed Mr. Richard Russell, to come for the claim of your fund worth of
$15,000,000.00 (Fifteen Million United States Dollars),to enable us to endorse the final payment approval order on his behalf. Urgently get in touch with Mr. George Williams the Director of Remittance VIA this confidential email: USTD.GOV.USA.ORG@HOTMAIL.COM for delivery directives. We shall be waiting for your urgent and prompt response.

Thanks,
Yours in Service,
Janet L. Yellen
Secretary of the Treasury

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com