Sun City Computer Club

Cyber Security SIG

July 6, 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

Computer Club Vimeo

- All Computer Club recordings moved
- Vimeo.com/sctxcompclub
- Follow
- SIGs
- Seminars
- Special Events

- Inclusion Home Bound, employed, …
- You, yes you can participate and present
- Members helping members
- Yet another Computer Club resource

Digital Lives after physical death

- Recent concept
- Keep it as you would want to leave it

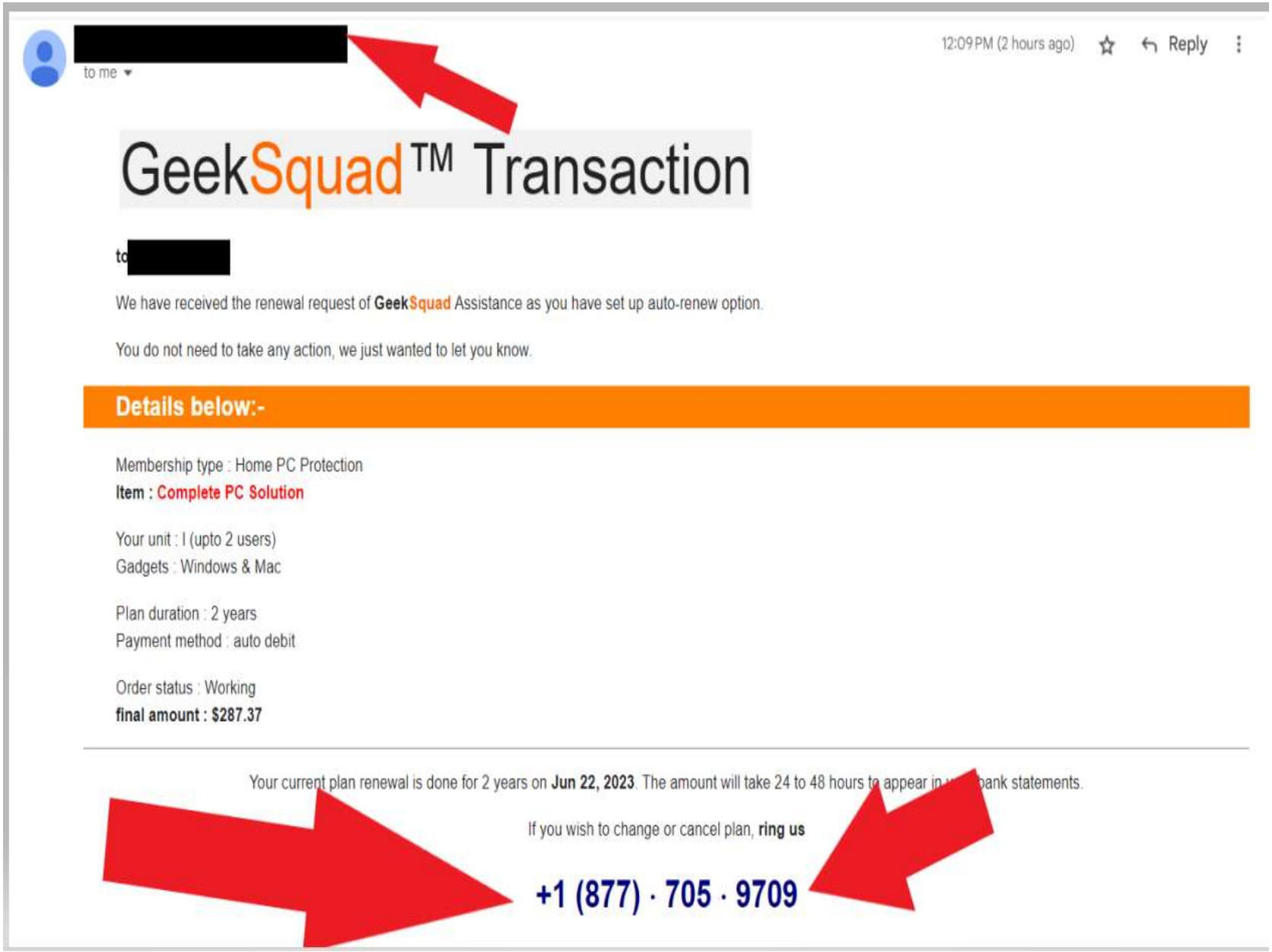
- Right to be forgotten
- Right to be remembered

- Current rights/practices probably not future rights/practices

- Ownership

Browser Updates

- Firefox 115.0
- Chrome 114.0.5735.199
- Edge 114.0.1823.67
- Brave 1.52.129
- Vivaldi 6.1.3035.111
- Duckduckgo Beta
- Tor 12.5


[redacted]
to me
12:09 PM (2 hours ago)
Reply
GeekSquad™ Transaction
to [redacted]
We have received the renewal request of GeekSquad Assistance as you have set up auto-renew option.
You do not need to take any action, we just wanted to let you know.
Details below:-
Membership type : Home PC Protection
Item : Complete PC Solution
Your unit : I (upto 2 users)
Gadgets : Windows & Mac
Plan duration : 2 years
Payment method : auto debit
Order status : Working
final amount : $287.37
Your current plan renewal is done for 2 years on Jun 22, 2023. The amount will take 24 to 48 hours to appear in
bank statements.
If you wish to change or cancel plan, ring us
+1 (877) · 705 · 9709

Current Issues

- UPS attack

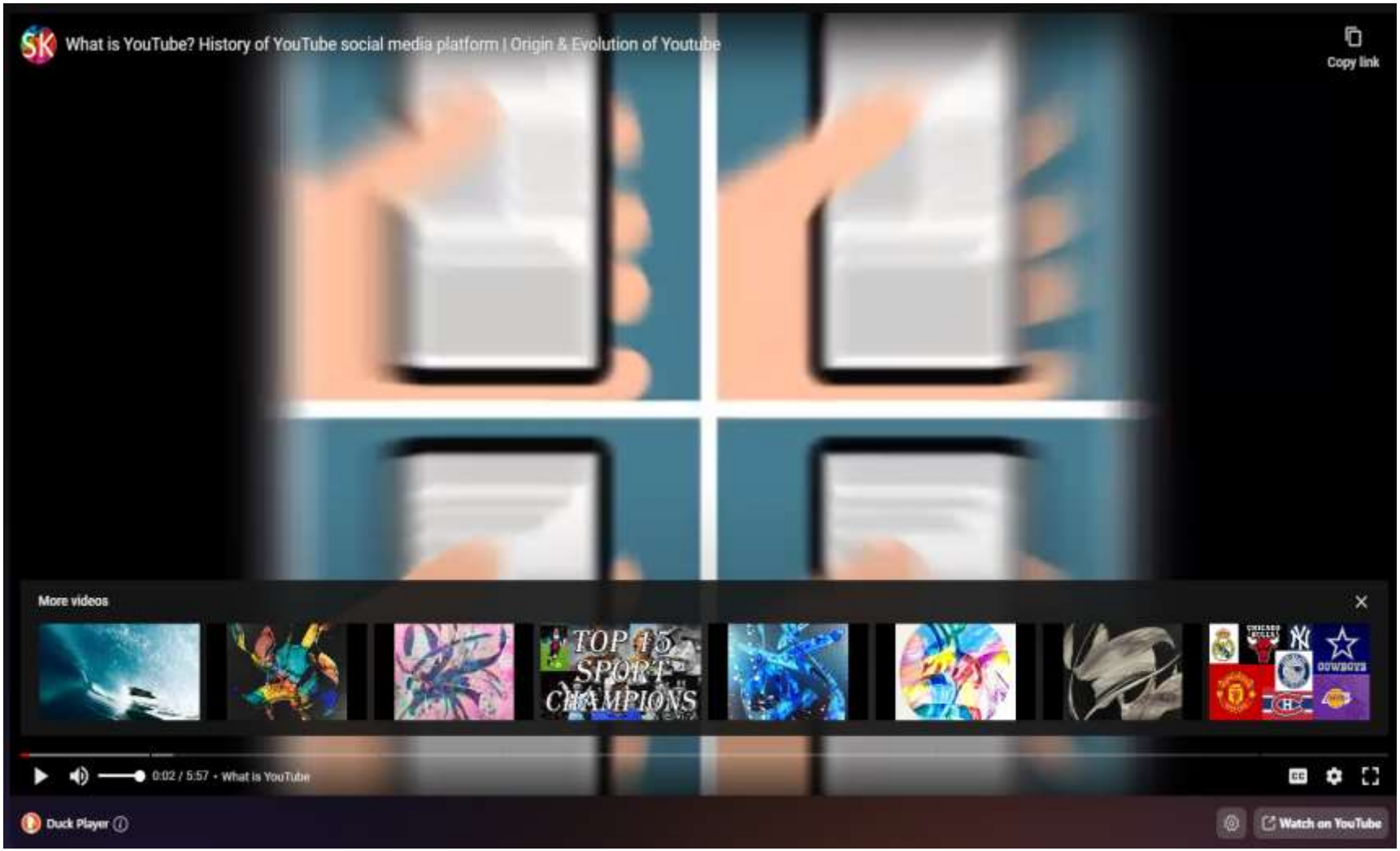
"UPS is aware that some package recipients have received fraudulent text messages demanding payment before a package can be delivered."

- Telemarketers got your number?

- You called an 800, 888, and/or 900 number (they use caller I.D. technology and collect phone numbers).
- You applied for credit.
- You contribute to charities. Here's how you can spot fake donation scams.
- You're a registered voter.
- You bought anything, or entered any contest, and gave your phone number in the process.
- Your phone number is on your checks.
- You call a business, and they have caller I.D. (which, you should assume they do).

Duckduckgo browser beta

- Available for Windows BETA
- Rendering via WebView 2 based on Blink
- Blocks trackers BEFORE they load
- Password Manager
- Ad blocker - remove white space
- Secure video player
- “Fire” button single click delete history
- NO extensions - yet
- DuckPlayer YouTube w/o tracking


What is YouTube? History of YouTube social media platform | Origin & Evolution of Youtube
Copy link
More videos
TOP 15 SPORT CHAMPIONS
0:02 / 5:57 • What is YouTube
Duck Player
Watch on YouTube

iPhone

- Crypto analysis
- Rolling shutter speed 60K frames per second
- RGB analysis

- Cover the power LED for sensitive devices

Safari private browsing boost

- Private Browsing popup
- Advanced Tracking and Fingerprinting Protection: Helps prevent websites from tracking or identifying your device using advanced techniques.
- Enhanced Extension Control: Extensions with website access are off by default. They can be turned on later in Safari settings.
- iCloud Private Relay Location Privacy Enhancements: For Private Relay users, Private Browsing uses IP address locations based on your country and time zone, rather than your general location.”
- Removal of user-tracking info in URLs

Current Issues

- US military personnel unsolicited smartwatches
- YouTube using Ad blocker 3 video limit
- Brave browser Off The Record mode

  Version 1.53

  OTR vs Incognito / Private

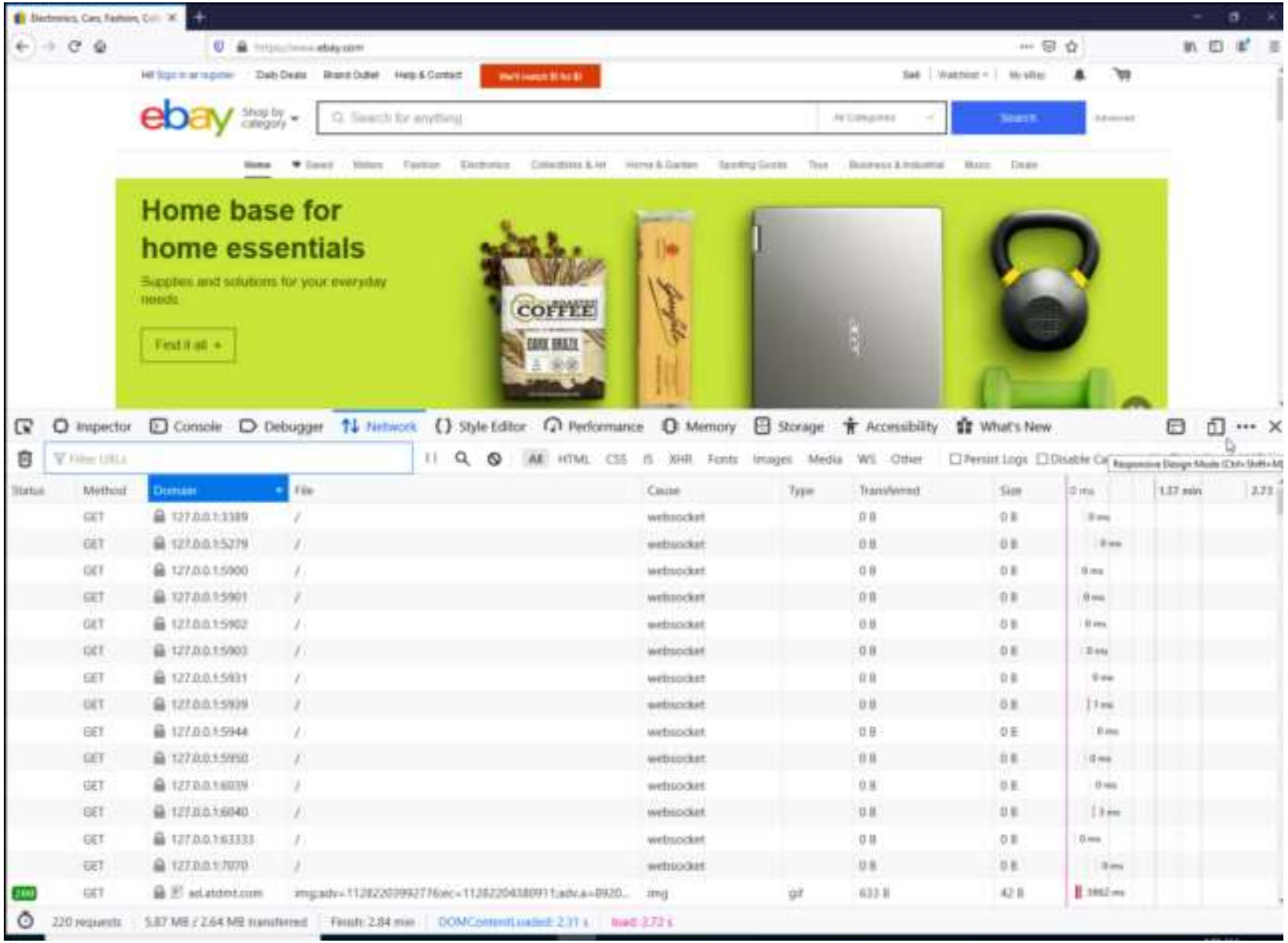
  Version 1.54

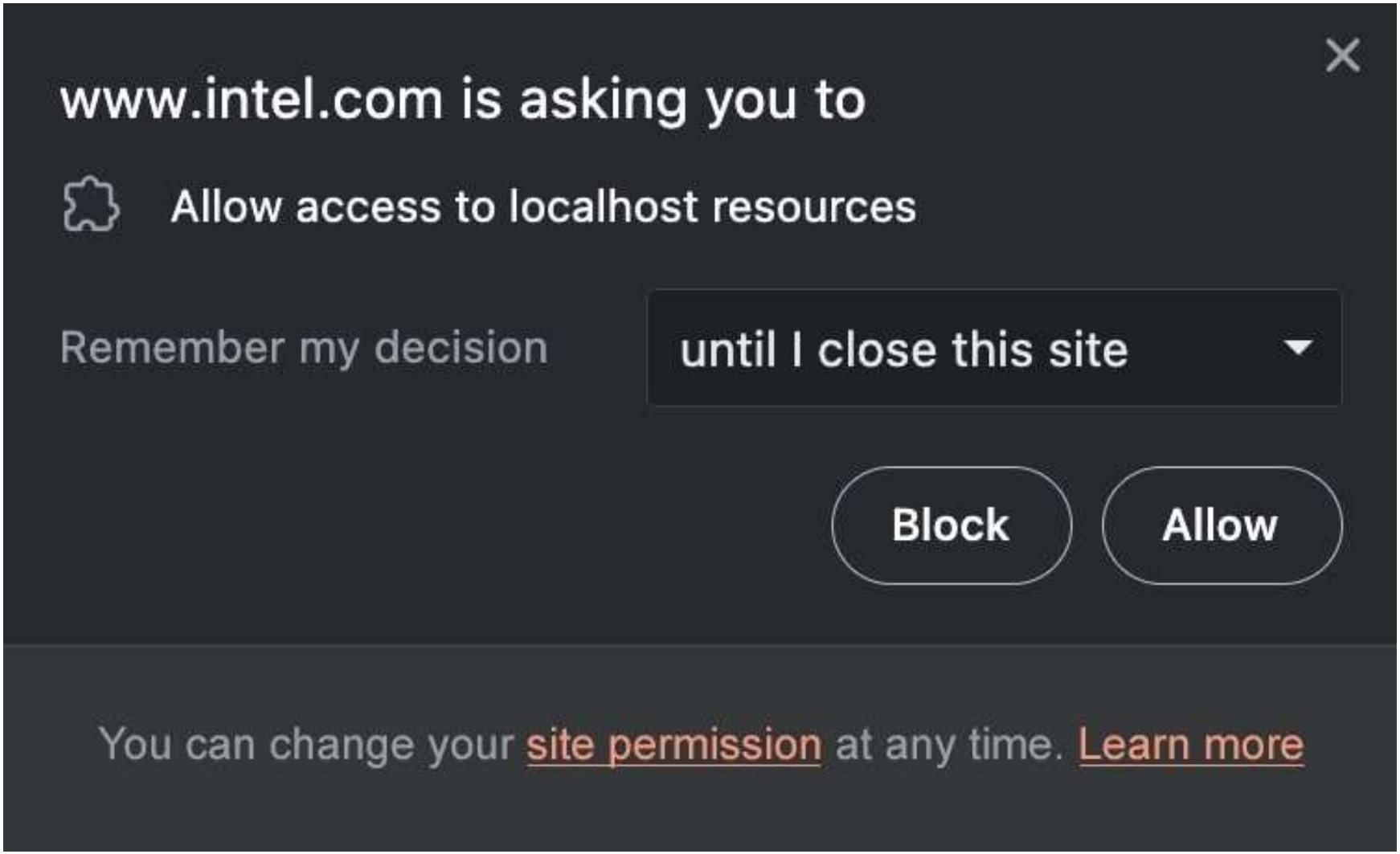
  Block website port scanning

  eBay, Best Buy, Kroger, Macys

  Fingerprint browsers Cookie

  Scan local IP 127.0.0.1


ebay
Home base for home essentials
Supplies and solutions for your everyday needs
Find it all
COFFEE
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
What's New
Status
Method
Domain
File
Cause
Type
Transferred
Size
GET
127.0.0.1:3389
127.0.0.1:5279
127.0.0.1:5900
127.0.0.1:5901
127.0.0.1:5902
127.0.0.1:5903
127.0.0.1:5931
127.0.0.1:5939
127.0.0.1:5944
127.0.0.1:5950
127.0.0.1:6039
127.0.0.1:6040
127.0.0.1:63333
127.0.0.1:7070
websocket
220 requests
5.87 MB / 2.64 MB transferred
Finish: 2.84 min
DOMContentLoaded: 2.31 s
load: 2.72 s


www.intel.com is asking you to
Allow access to localhost resources
Remember my decision
until I close this site
Block
Allow
You can change your site permission at any time. Learn more

VEHICLE PRIVACY LABEL™

Manufacturer Policies & Terms: Click Buttons for Details

KIA Collects

Identifiers	Biometrics	Location	Synched Phones	User Profiles
YES	NO	YES	SILENT	YES

KIA Shares/Sells to

Affiliates	Service Providers	Insurance	Government	Data Brokers
YES	YES	SILENT	YES	SILENT

REVIEW COMPLETED, LAST UPDATED BY PRIVACY4CARS ON 02/28/23

Reviewed Public Documents*

UNIQUE DOCUMENTS	WORDS	READ TIME**
4	53,743	269 min

Main Privacy Policy Last updated: 01/01/23	14,131 Reading Level: 15th Grade***	71 min
Main TOS Last updated: 05/18/21	10,780 Reading Level: 17th Grade***	54 min
Vehicle Owners Privacy Policy Last updated: 01/01/23	8,664 Reading Level: 16th Grade***	43 min
Vehicle Owners TOS Last updated: 08/05/22	20,168 Reading Level: 15th Grade***	101 min

Privacy4cars

- Private Browsing upgrades in Safari
  - Private browsing windows locked
  - Require secondary authentication
  - FaceID/TouchID or passcode
- Tracking URL removal
  - Private or All browsing
  - Unknown trackers completely removed

iOS 17
Privacy & Security improvements

- Shared passwords
  iOS 17, iPadOS 17, Sonoma
  Passwords & Passkeys
  Shared media accounts, utility bills, …
  Access, Add, Remove, Change

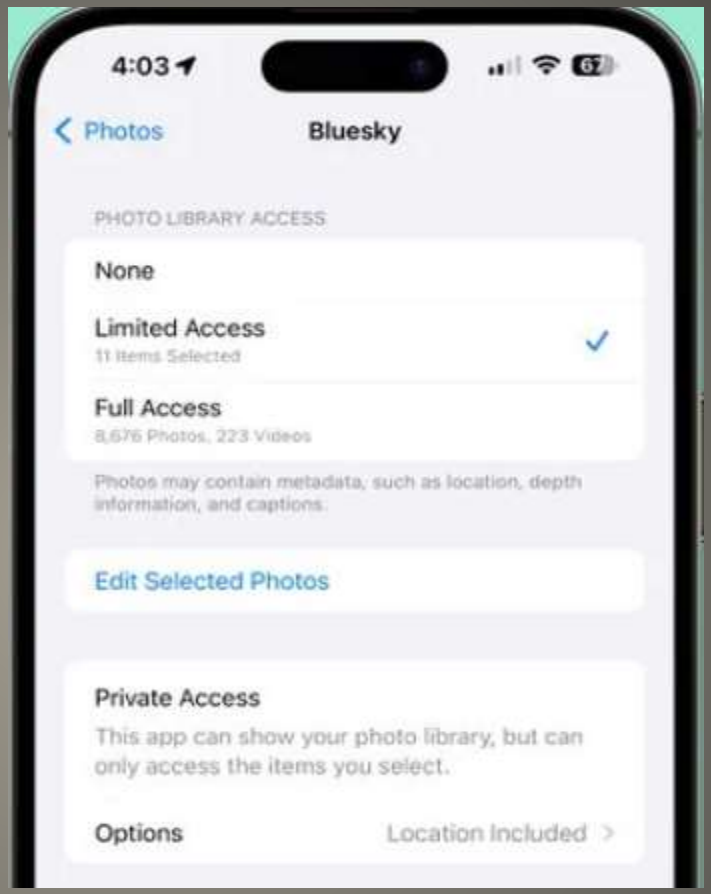
iOS 17
Privacy & Security improvements

- Passcode resets
  Change passcode then forgot passcode
  72-hour grace period
  Expire previous passcode

iOS 17
Privacy & Security improvements

iOS 17
Privacy & Security improvements

- Photo Library Access
  - Apps need explicit permissions
  - Limited Access
    - Only images you select
    - View in app or
    - Settings > Privacy & Security > Photos
  - Full Access
    - All images & videos
    - Your device informs on total
  - None
  - Add Photos only



iOS 17
Privacy & Security improvements

- Calendar Access
  Settings > Privacy & Security > Calendars
  Note Calendars plural
  Full Access
  Add Events Only
  None

Full access: location, time, invitees, attachments, notes,

iOS 17
Privacy & Security improvements

- Passkeys
  Automatically adds passkey to Apple ID
  iOS, iPadOS, Sonoma
  Biometrics as choice

iOS 17
Privacy & Security improvements

- Home Activity History
  30-day history
  door locks, garage doors, contact sensors
  Who & When

iOS 17
Privacy & Security improvements

Current Issues

- Proton password manager Proton Pass
- Mockingjay process injection technique
  w/o space allocation, setting permissions, starting a thread
  a vulnerable DLL
  subverts security layers
- Threads a meta twitter

Instant Messaging more secure

- End-to-End encryption
  - Lessens insider threat
  - Law enforcement
  - Signal, WhatsApp (personal chats), iMessage,
  - Option for Facebook Messenger & Telegram
- Disappearing messages
  - WhatsApp, Signal, Telegram
  - You choose length/time
- Lock individual conversations
  - Lock entire app Lock conversations

- Check & Recheck contact options
  Who can read, respond, etc.
  Temporary photos/videos (stories)
- Got backups? Know where they are?
- Multi logins

Instant Messaging more secure

Current Issues

- WhatsApp Pink No No Please No Malicious
- LetMeSpy Poland based spyware hacked Customer data leaked
- Android update causing large false 911 calls
- Rustbucket macOS malware
  - Advanced persistence
  - Now a .NET version
  - Rogue PDF reader - malicious PDF infection
  - Adds plist file

/Users/<user>/Library/LaunchAgents/com.apple.systemupdate.plist

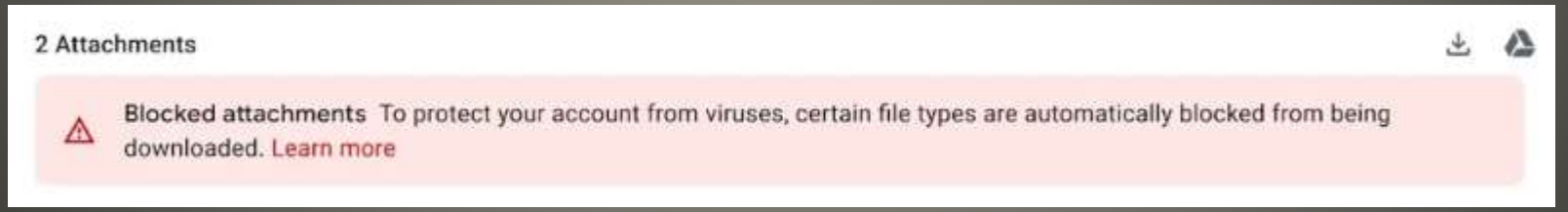
Rings around Alexa

- Pulsing yellow
  Notification
  Missed a reminder
- Solid red
  Mute and/or camera off
  Error
- Blue light with spinning light-blue segment
  Alexa listening in direction of light-blue segment
- Spinning Orange
  Setup mode or service outage
- Pulsing green
  Incoming call
- Spinning green
  Someone dropped in
- Purple light
  Do Not Disturb on
- Spinning white
  Alexa guard

Current Issues

- Use of ChatGPT AI to windup to telemarketers
  Jolly Rodger Telephone $1.99/mo
  Permission from telephone co
  Whitelist contacts
- Gmail client-side encryption improvement
  Red dot if recipient unable to be encrypted

Warning if attachment may have security issues



Current Issues

- Dollar General - No checkout lane
  Just Walk Out technology
  yeahbut NOT alcohol check age ID
- Google Chrome Privacy Sandbox popup

- Apple facial recognition reputation
  Well earned A LOT of technology
  Some Samsung as well
  26 smartphones tested
  14 models failed
  Photo of owner unlockedm

Facial recognition
Photo recognition

Retail Media Networks

- Loyalty cards
- Help vendors
- Help you but at what costs?
- Read that small print? Agree?
- They then sell the data
- Bluetooth beacons

- Accurate data

- Louisiana office of motor vehicles
  6 million records
  names, addresses, DoB, driver license numbers, SSN, vehicle registrations, …
  CLOP gang “we deleted any/all” info
  government, education, police, …
  SQL injection

MOVEit

CISA adds 8 flaws

- Known Exploited Vulnerabilities
- 6 Samsung smart phones

- CVE-2021-25394 (CVSS score: 6.4) - Samsung mobile devices race condition vulnerability
- CVE-2021-25395 (CVSS score: 6.4) - Samsung mobile devices race condition vulnerability
- CVE-2021-25371 (CVSS score: 6.7) - An unspecified vulnerability in the DSP driver used in Samsung mobile devices that allows loading of arbitrary ELF libraries
- CVE-2021-25372 (CVSS score: 6.7) - Samsung mobile devices improper boundary check within the DSP driver in Samsung mobile devices
- CVE-2021-25487 (CVSS score: 7.8) - Samsung mobile devices out-of-bounds read vulnerability leading to arbitrary code execution
- CVE-2021-25489 (CVSS score: 5.5) - Samsung Mobile devices improper input validation vulnerability resulting in kernel panic

- 2 D-Link devices

- CVE-2019-17621 (CVSS score: 9.8) - An unauthenticated remote code execution vulnerability in D-Link DIR-859 Router
- CVE-2019-20500 (CVSS score: 7.8) - An authenticated OS command injection vulnerability in D-Link DWL-2600AP

- Federal Civilian Execrate Branch required to patch by July 20

- US government organizations
- Multiple industry sectors

CISA warning ongoing DDoS

Current Issues

- Fortinet firewalls
  Serious security bug
- Operation Triangulation
  Kaspersky analysis
  Many months
  iOS 15.7
  VERY well hidden
  Nation state? Nation state surveillance?
- Solar flare July 2 19:14 GMT
- Microsoft data breach??
- CISA, FBI, et al Truebot malware warning

Devices

Current Issues

- ChatGPT – textual
- Bard images if they help with answer
  or ask for relevant illustration
  Images have caption & credit
  Explicit ask for pictures ala google images
- Apple smart monitor
  smart Home monitor when not in use

Wi-Fi beacon

- Is “saved Wi-Fi network name” in range?
- Is that Really *Wendy’s*?
- VPN for any public Wi-Fi
- But is this really “Saved Wi-Fi network name”?
- Tool to analyze Beacon Management Frames
  Vendor, BSSID, channel, etc.
  Match – probably trustworthy
  Mismatch – probably not
  tool detect Airbase-ng (fake access points)

Snappy

- Python script Trustwave’s GitHub
- Python capability
- Android Pydroid, Qpython, Termux
- iDevices Pythonista, Juno

Text Messages from eMail

- To: <phone number>@<gateway domain>
- https://freecarrierlookup.com/

- Military Encryption
- Bluetooth - never connected to Internet
- Push Button
- All selected password in one place - if lost?
- Fills in passwords at selected website

PasswordPocket

Alexa hack possible?

- Alexa on home network?
- Segmentation
- Alexa hack Alexa
- Alexa light on w/o trigger?
- Skills
- Change wake word
  Multi Factor Authentication

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com