Sun City Computer Club

Cyber Security SIG

October 19, 2023

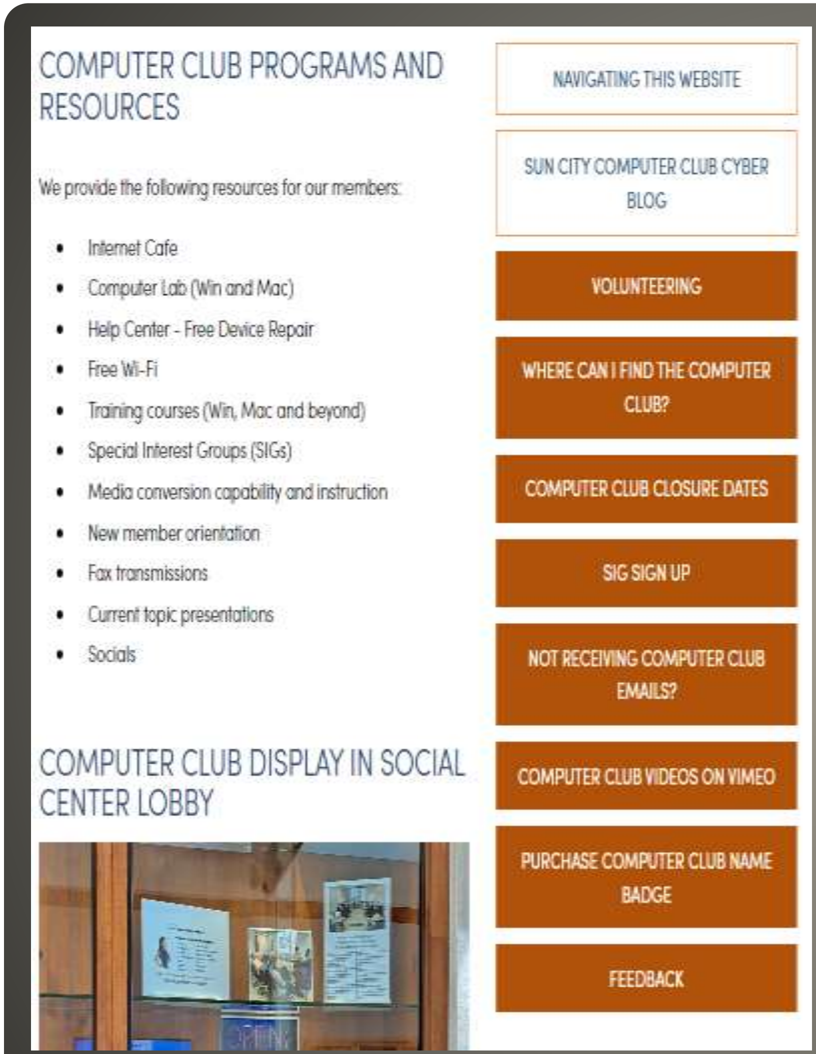
Questions, Comments, Suggestions welcomed at any time

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



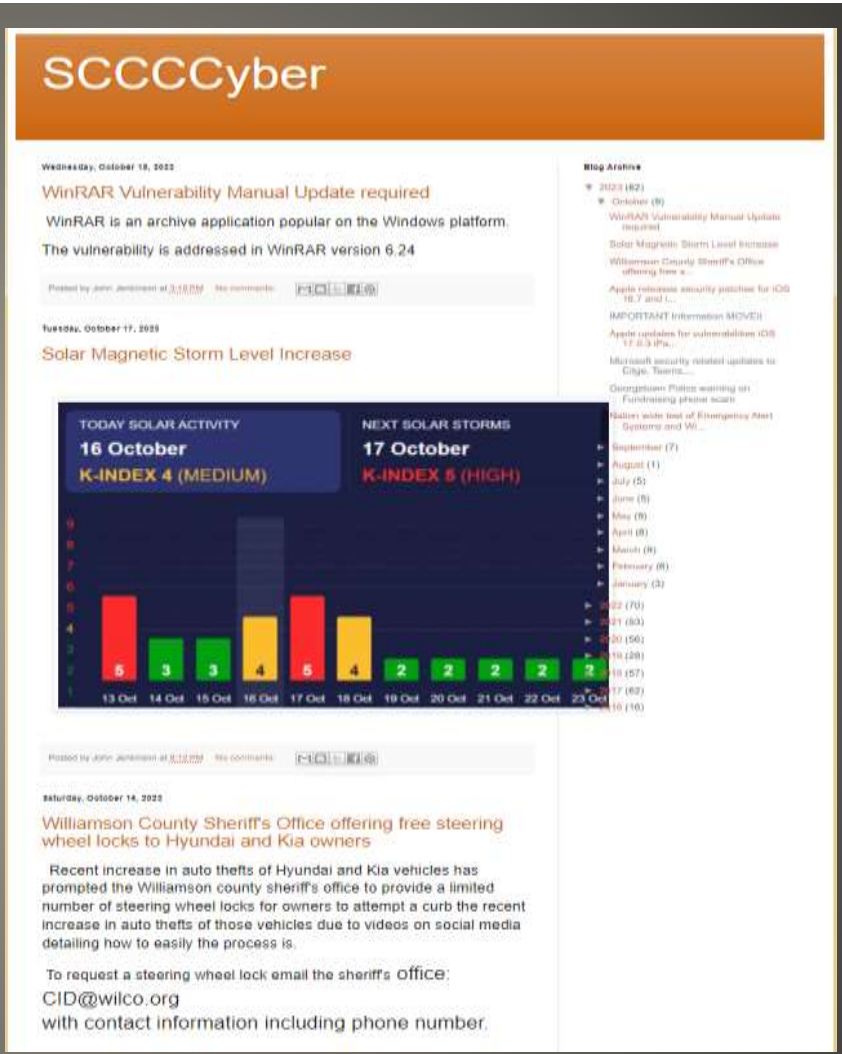
COMPUTER CLUB PROGRAMS AND RESOURCES

We provide the following resources for our members:

- Internet Cafe
- Computer Lab (Win and Mac)
- Help Center - Free Device Repair
- Free Wi-Fi
- Training courses (Win, Mac and beyond)
- Special Interest Groups (SIGs)
- Media conversion capability and instruction
- New member orientation
- Fax transmissions
- Current topic presentations
- Socials

COMPUTER CLUB DISPLAY IN SOCIAL CENTER LOBBY

NAVIGATING THIS WEBSITE
SUN CITY COMPUTER CLUB CYBER BLOG
VOLUNTEERING
WHERE CAN I FIND THE COMPUTER CLUB?
COMPUTER CLUB CLOSURE DATES
SIG SIGN UP
NOT RECEIVING COMPUTER CLUB EMAILS?
COMPUTER CLUB VIDEOS ON VIMEO
PURCHASE COMPUTER CLUB NAME BADGE
FEEDBACK
OPEN



SCCCyber

Wednesday, October 18, 2023

WinRAR Vulnerability Manual Update required

WinRAR is an archive application popular on the Windows platform.

The vulnerability is addressed in WinRAR version 6.24

Posted by John Jenkinson at 3:18 PM No comments:

Tuesday, October 17, 2023

Solar Magnetic Storm Level Increase

Posted by John Jenkinson at 8:12 PM No comments:

Saturday, October 14, 2023

Williamson County Sheriff's Office offering free steering wheel locks to Hyundai and Kia owners

Recent increase in auto thefts of Hyundai and Kia vehicles has prompted the Williamson county sheriff's office to provide a limited number of steering wheel locks for owners to attempt a curb the recent increase in auto thefts of those vehicles due to videos on social media detailing how to easily the process is.

To request a steering wheel lock email the sheriff's office:
CID@wilco.org
with contact information including phone number.

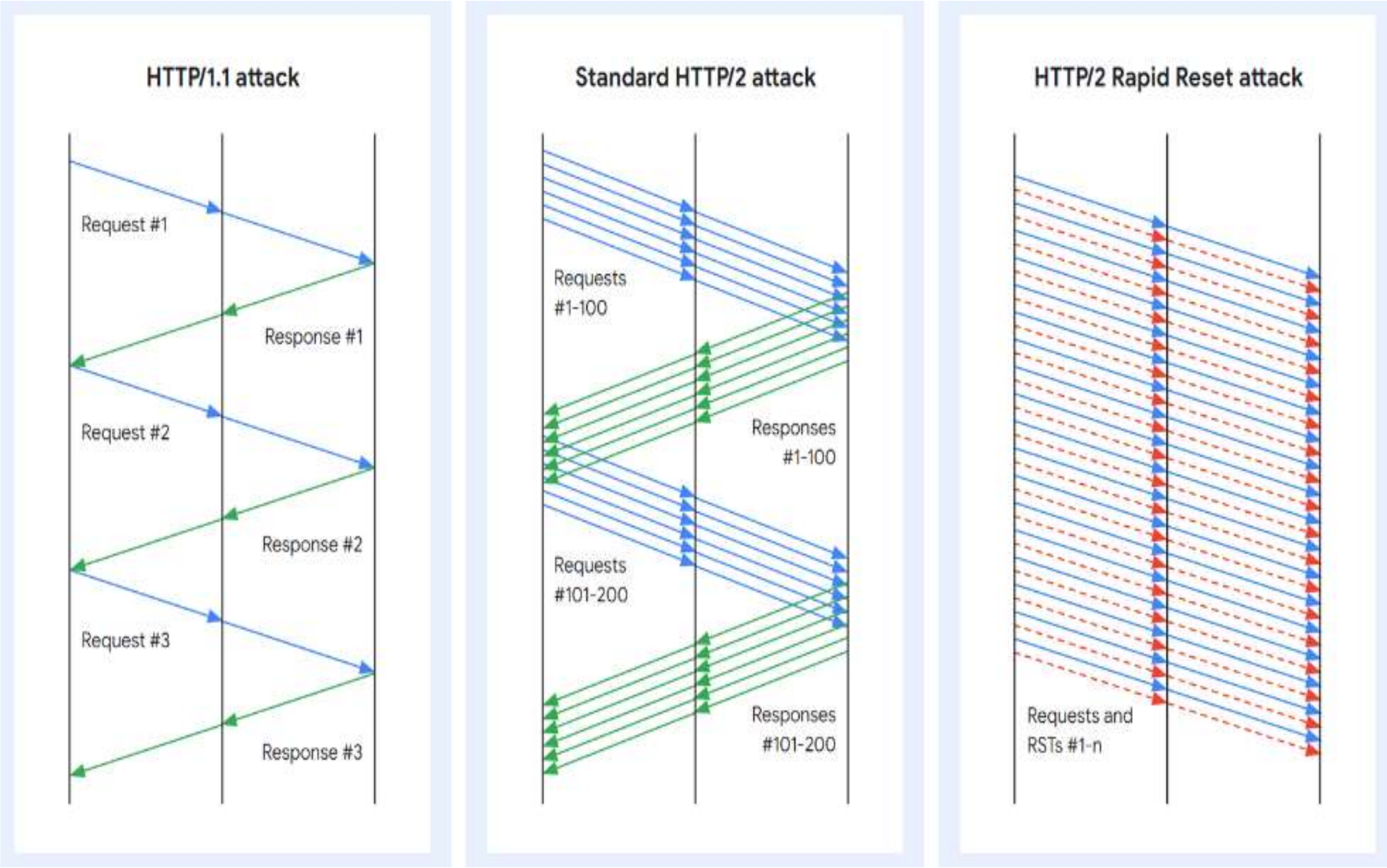
Blog Archive

- ▼ 2023 (82)
  - ▼ October (8)
    - WinRAR Vulnerability Manual Update required
    - Solar Magnetic Storm Level Increase
    - Williamson County Sheriff's Office offering free s...
    - Apple releases security patches for iOS 16.7 and i...
    - IMPORTANT Information MOVE!!
    - Apple updates for vulnerabilities iOS 17.0.3 iPa...
    - Microsoft security related updates to Edge, Teams,...
    - Georgetown Police warning on Fundraising phone scam
    - Nation wide test of Emergency Alert Systems and Wi...
  - ► September (7)
  - ► August (1)
  - ► July (5)
  - ► June (8)
  - ► May (8)
  - ► April (8)
  - ► March (8)
  - ► February (8)
  - ► January (3)
- ► 2022 (70)
- ► 2021 (83)
- ► 2020 (56)
- ► 2019 (28)
- ► 2018 (57)
- ► 2017 (62)
- ► 2016 (16)

Cyber Security Blog

DDoS Attack

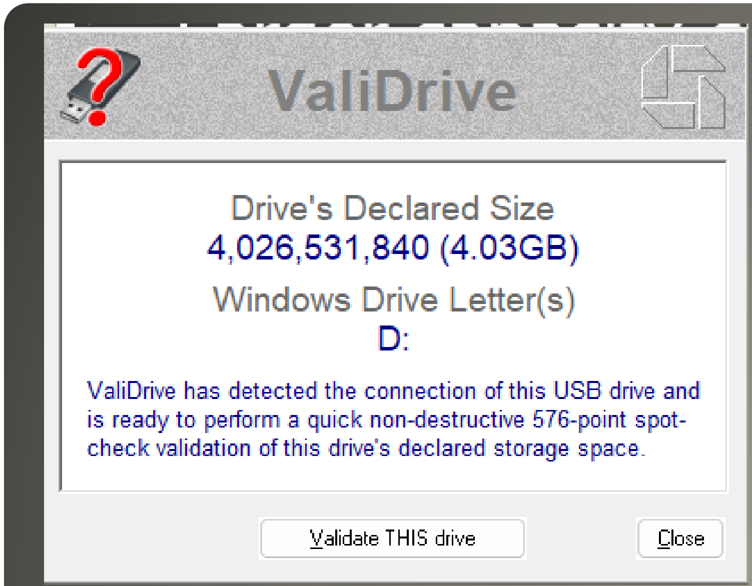
- Distributed Denial of Service
- 7.5 times Larger than previous record
- 398 Million requests per second
- Was 46 million requests per second
- (typical web 1-3 billion/sec)
- HTTP/2 “Rapid Reset” multistream
- 20,000 bots


HTTP/1.1 attack
Request #1
Response #1
Request #2
Response #2
Request #3
Response #3
Standard HTTP/2 attack
Requests #1-100
Responses #1-100
Requests #101-200
Responses #101-200
HTTP/2 Rapid Reset attack
Requests and RSTs #1-n

SSD Fraud

- Larger capacity claimed than available
- Your precious data – gone never written
- SO SLOW
- 12 1-2 terabyte drives from Amazon
- ALL FAILED
- ValiDrive Gibson Research
- NAND style needs high voltage 20 volts
- USB has 5 volts charge pump boost

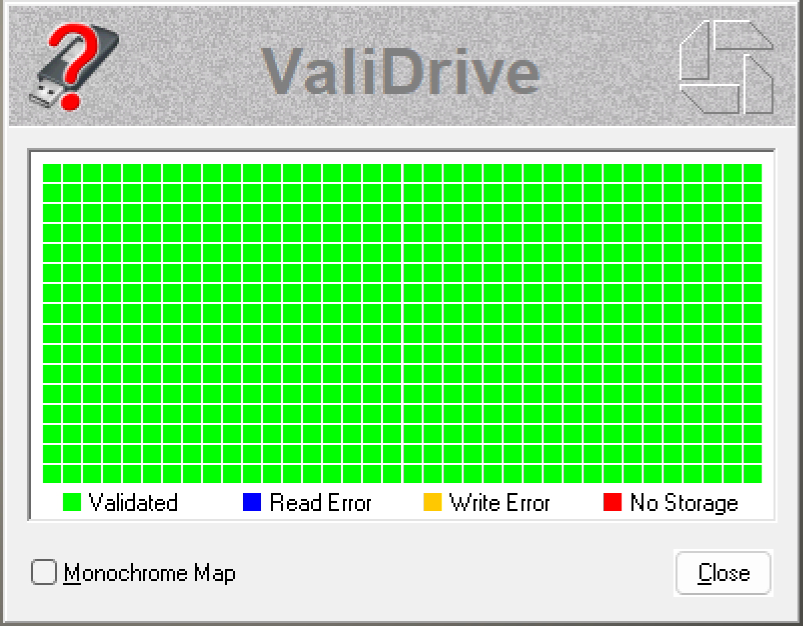
ValiDrive



Drive's Declared Size
4,026,531,840 (4.03GB)

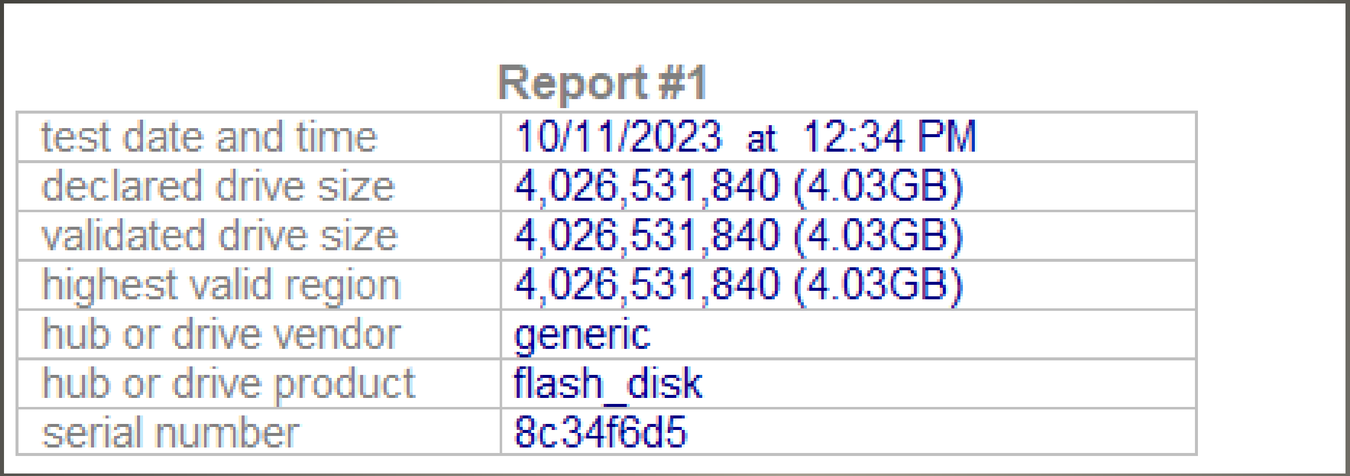
Windows Drive Letter(s)
D:

ValiDrive has detected the connection of this USB drive and is ready to perform a quick non-destructive 576-point spot-check validation of this drive's declared storage space.



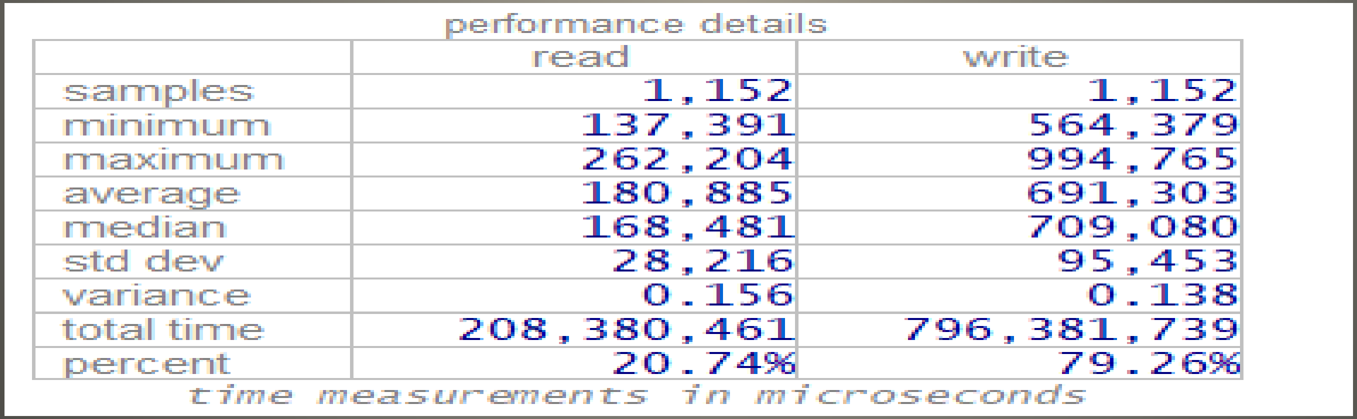
🟩 Validated 🟦 Read Error 🟨 Write Error 🟥 No Storage

☐ Monochrome Map



Report #1

test date and time	10/11/2023 at 12:34 PM
declared drive size	4,026,531,840 (4.03GB)
validated drive size	4,026,531,840 (4.03GB)
highest valid region	4,026,531,840 (4.03GB)
hub or drive vendor	generic
hub or drive product	flash_disk
serial number	8c34f6d5



performance details

	read	write
samples	1,152	1,152
minimum	137,391	564,379
maximum	262,204	994,765
average	180,885	691,303
median	168,481	709,080
std dev	28,216	95,453
variance	0.156	0.138
total time	208,380,461	796,381,739
percent	20.74%	79.26%

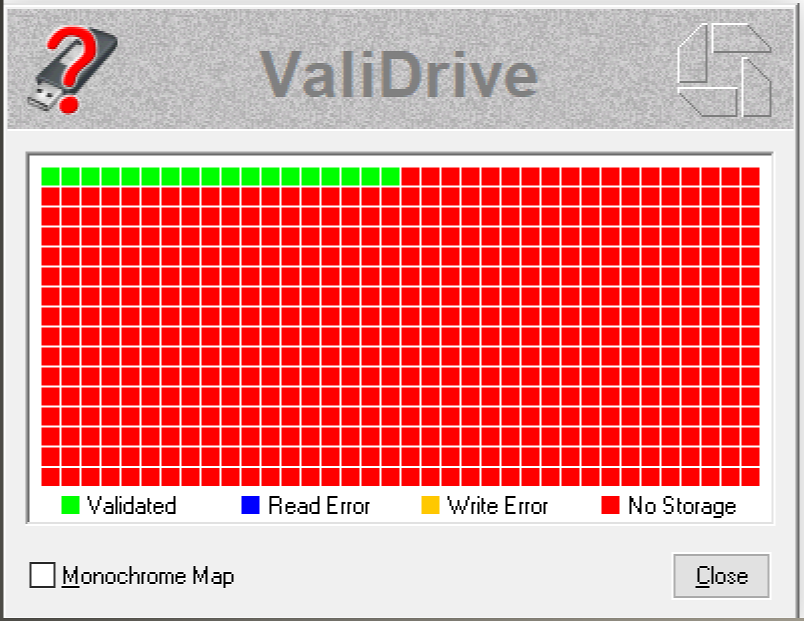
time measurements in microseconds

ValiDrive

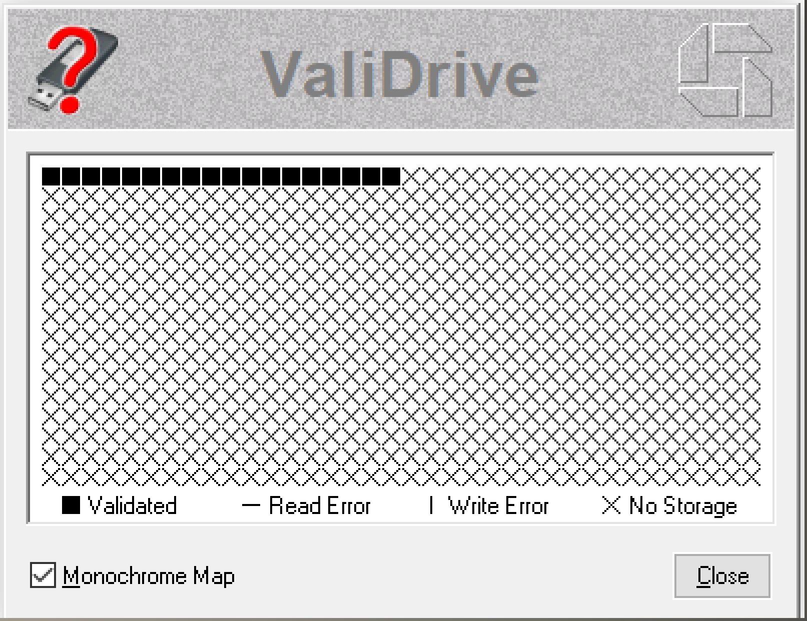
1TB
2TB
BLANBOK+
USB 3.0
1 TB
1TB
USB Flash Drive
Extreme
1TB
V30
A2
4K
2000GB
Dianww

ALL FAILED

ValiDrive



☐ Monochrome Map



☑ Monochrome Map

- 2TB Drive - 62 Gigabytes

- How to avoid scams & fraud
- How to recover/report scams & fraud

- Maby we are victim? Maby not?
  Notification of breach
  “Found your info on Dark WEB”

Middle ground

- DO NOT provide any more information

  Close down web page

  Hang up phone

  Delete and REPORT messages

  Ignore social media posts

  FILTER FILTER FILTER
- Disconnect from Internet and/or home network

  Airplane mode pull cable WiFi off
- Review what you may have given out

  That information may be coming back

Middle Ground

- CHANGE PASSWORD/PASSPHRASE
  UNIQUE and STRONG
  Enable/review multi factor authentication
- Contact bank, broker, service provider, etc.
- Use credit bureau services
- Scan your potentially affected device(s)
  Computer Club Help Center
- Check any and all available logs & indicators
- Strengthen your resolve and defenses
- Check, double check, recheck
  Bank & shopping accounts
  Social media posts, friends, contacts
- Notify contacts
- Look around – old devices? Unused VMs?
- Old devices on cloud services
- Email/messaging forwarding rules   Email filters   “Other folders”

Middle Ground

Middle ground

- Attitude adjustment

  Do everything right? Still a victim
- AWARENESS
- Defense in Depth

- Default configurations of software and applications
- Improper separation of user/administrator privilege
- Insufficient internal network monitoring
- Lack of network segmentation
- Poor patch management
- Bypass of system access controls
- Weak or misconfigured multifactor authentication (MFA) methods
- Insufficient access control lists (ACLs) on network shares and services
- Poor credential hygiene
- Unrestricted code execution

CISA NSA top 10 misconfigurations

Credit Bureau Credit Freeze

- https://www.equifax.com/personal/credit-report-services/credit-freeze/
- https://www.transunion.com/credit-freeze
- https://www.experian.com/freeze/center.html

Slack slack off

- Slack employees taking week off for:
- Ranger status
- Salesforce’s Trailhead online learning platform

- “How to use AI”
- How to use AI to satisfy this requirement

Current Issues

- 23andMe confirms data theft

  Credential stuffing

  “DNA relatives” Ashkenazi Jews

  Current political events causing SEVERE actions | leak victims

- Russia plans to build supercomputer

  10,000 to 15,000 Nvidia H100 GPUs

  Technology restrictions

- CISA warns of Adobe Acrobat Reader

  CVE-2023-21608 RCE

  Patched January 2023

Acrobat DC - 22.003.20282 (Win), 22.003.20281 (Mac) and earlier versions (fixed in 22.003.20310)

Acrobat Reader DC - 22.003.20282 (Win), 22.003.20281 (Mac) and earlier versions (fixed in 22.003.20310)

Acrobat 2020 - 20.005.30418 and earlier versions (fixed in 20.005.30436)

Acrobat Reader 2020 - 20.005.30418 and earlier versions (fixed in 20.005.30436)

- 23andMe confirms data theft

  Credential stuffing

  "DNA relatives"   Ashkenazi Jews

  Current political events causing SEVERE actions | leak victims
- So, several actors used 23andME account(s)

  Against 23andMe's terms of service

  And are now in possession of 7 million records

  Half or 23andMe's data
- With "DNA" relatives"?
- PII + Genetic information
- New SSN, Credit card, DL, Facebook, …

  Not so with DNA

  DNA "real record"
- $300 sale GlaxoSmithKline
- Your DNA – Family's DNA

23andMe

- Blackmail, Impersonation, biometric
- 4 million more records 17-Oct-2023
- Great Britain, wealthy

23andMe

- Of the 78% of IoT devices with known vulnerabilities on customer networks, 46% are not
- patchable.
- • Since 2019, attacks targeting open-source software have grown on average 742%.
- • Fewer than 15% of non-governmental organizations (NGOs) have cybersecurity experts on
- staff.
- • Coin-mining activity was found in 4.2% of all incident response engagements.
- • 17% of intrusions involved known remote monitoring and management (RMM) tools.
- • Adversary in the middle (AitM) phishing domains grew from 2,000 active domains in June
- 2022 to more than 9,000 by April 2023.
- • 156,000 daily business eMail compromise attempts were observed between April 2022 and
- April 2023.
- • 41% of the threat notifications Microsoft sent to online services customers between July
- 2022 and June 2023 went to critical infrastructure organizations.
- • The first quarter of 2023 saw a dramatic surge in password-based attacks against cloud
- identities.
- • Microsoft blocked an average of 4,000 password attacks per second over the past year.
- • Approximately 6,000 MFA fatigue attempts were observed per day.
- • The number of token replay attacks has doubled since last year, with an average of 11
- detections per 100,000 active users in Azure Active Directory Identity Protection.
- • DDoS attacks are on the rise, with around 1,700 attacks taking place each day, cumulating
- at up to 90 terabits of data per second (Tbps).
- • State-sponsored activity pivoted away from high-volume destructive attacks in favor of
- espionage campaigns.
- • 50% of destructive Russian attacks observed against Ukrainian networks occurred in the first
- six weeks of the war.
- • Ghostwriter continues to conduct influence campaigns attempting to sow distrust between
- Ukrainian populations and European partners who support Kyiv—both governmental and
- civilian.
- • Iranian operations have expanded from Israel and the US to target Western democracies and
- NATO.

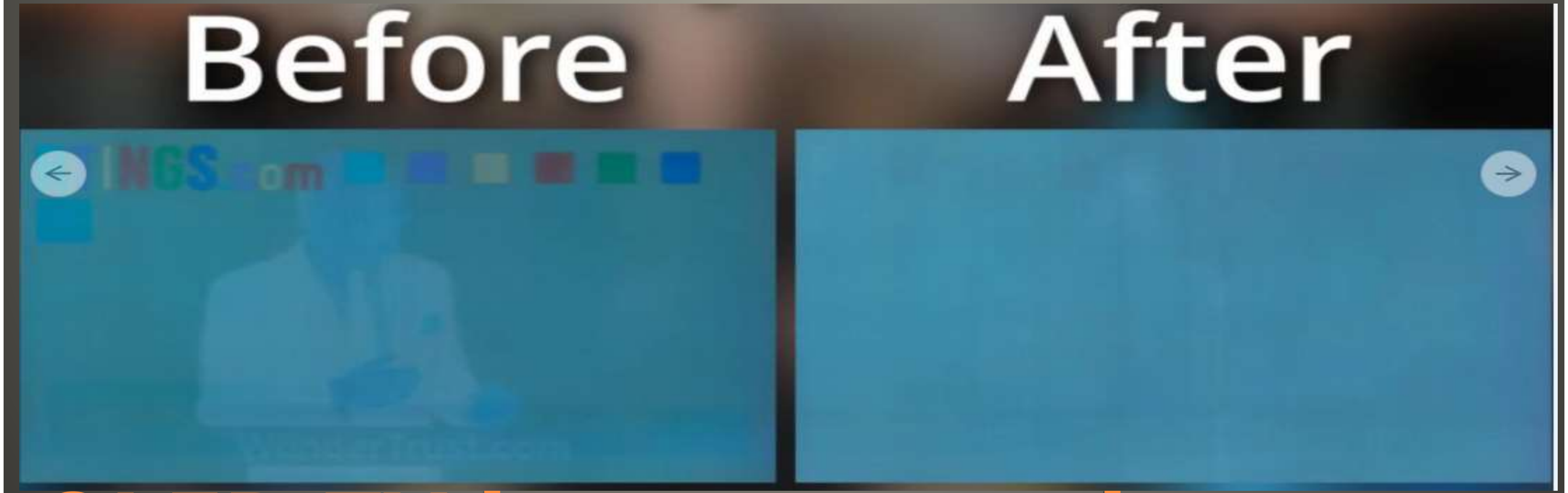
Microsoft Digital Defense report 2023

- Google vs Sonos’ patent infringement case
  Remove restrictions in multiple devices
- Curl version 8.4.0 released 11/11/2023
  libcurl and curl
  printers, cars, …
  docker base images
- Billboard truck Harvard campus
  Doxing student names & faces
  Statement
  Harvard Undergraduate Palestine Solidarity Committee
- 23andMe Doxing
- Google Docs export with HTML exports
  get tracking info added on
  Now, calendar invites
- MOVEit update 2,300 reported companies
  Sony 7,000 current and former employees

Current Issues

- Doxing or doxxing is the act of publicly providing personally identifiable information about an individual or organization, usually via the Internet. Wikipedia

- TV compensation cycles CAN auto-fix if they run
- Untreated temporary image retention Device cool down
- TFT threshold shift – compensation cycle



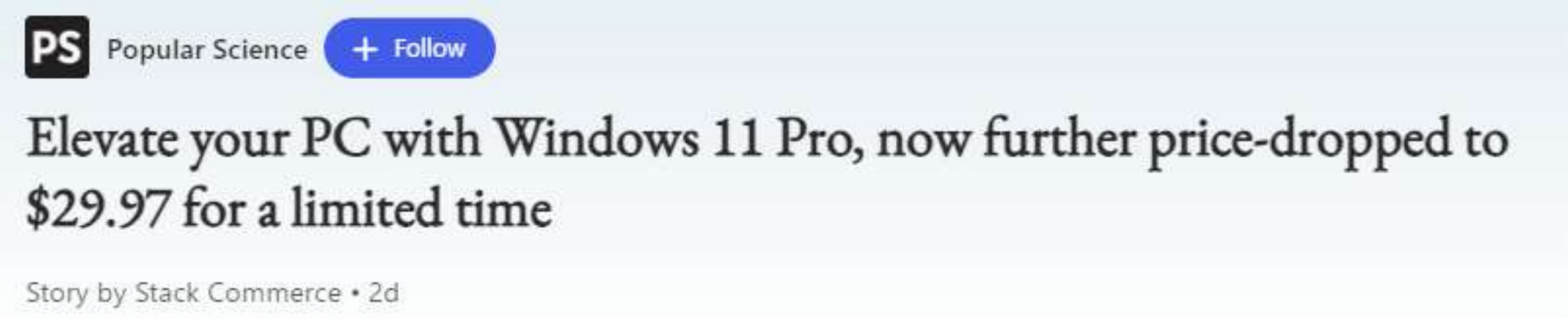
OLED TV image retention

- Proposed standard (ECH)
- Improves encryption and metadata protections
- Chrome, Firefox, Cloudflare
- Removes hostname from cleartext TLS

- Understanding
- Preparedness
- Awareness

- Defeats Pirate blocking efforts

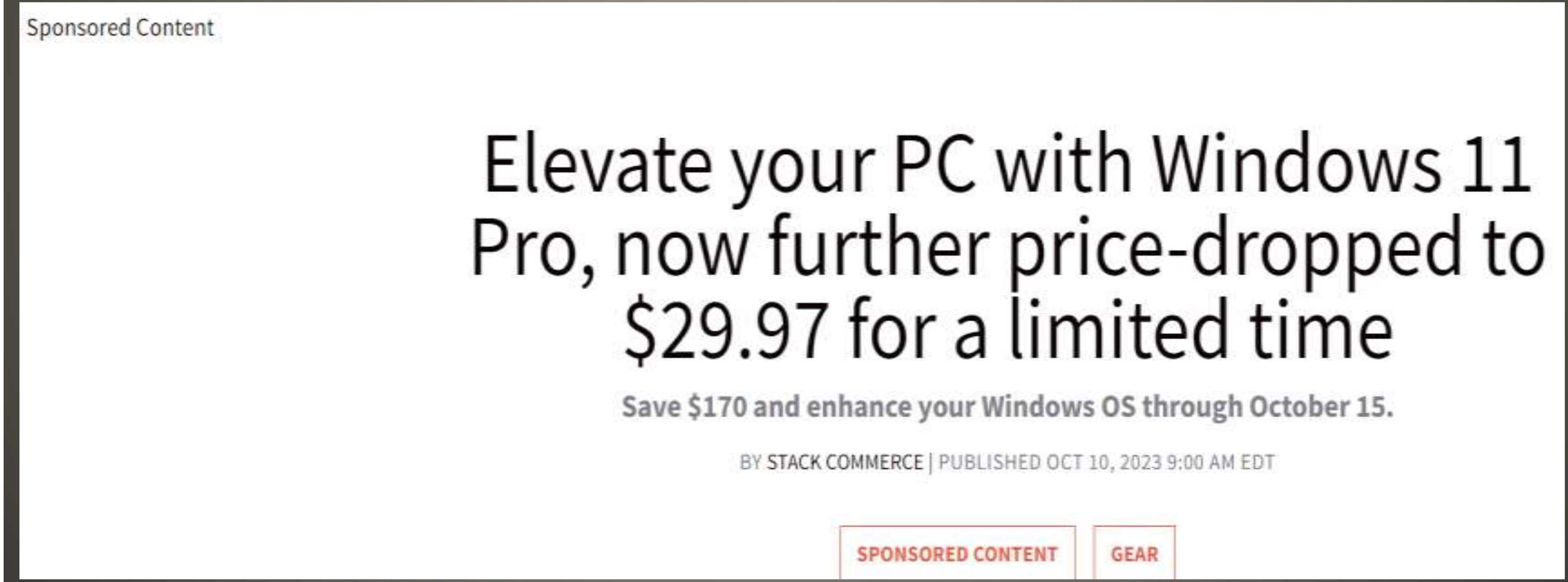
Encrypted Client Hello from last time



Popular Science

Elevate your PC with Windows 11 Pro, now further price-dropped to $29.97 for a limited time

Story by Stack Commerce • 2d



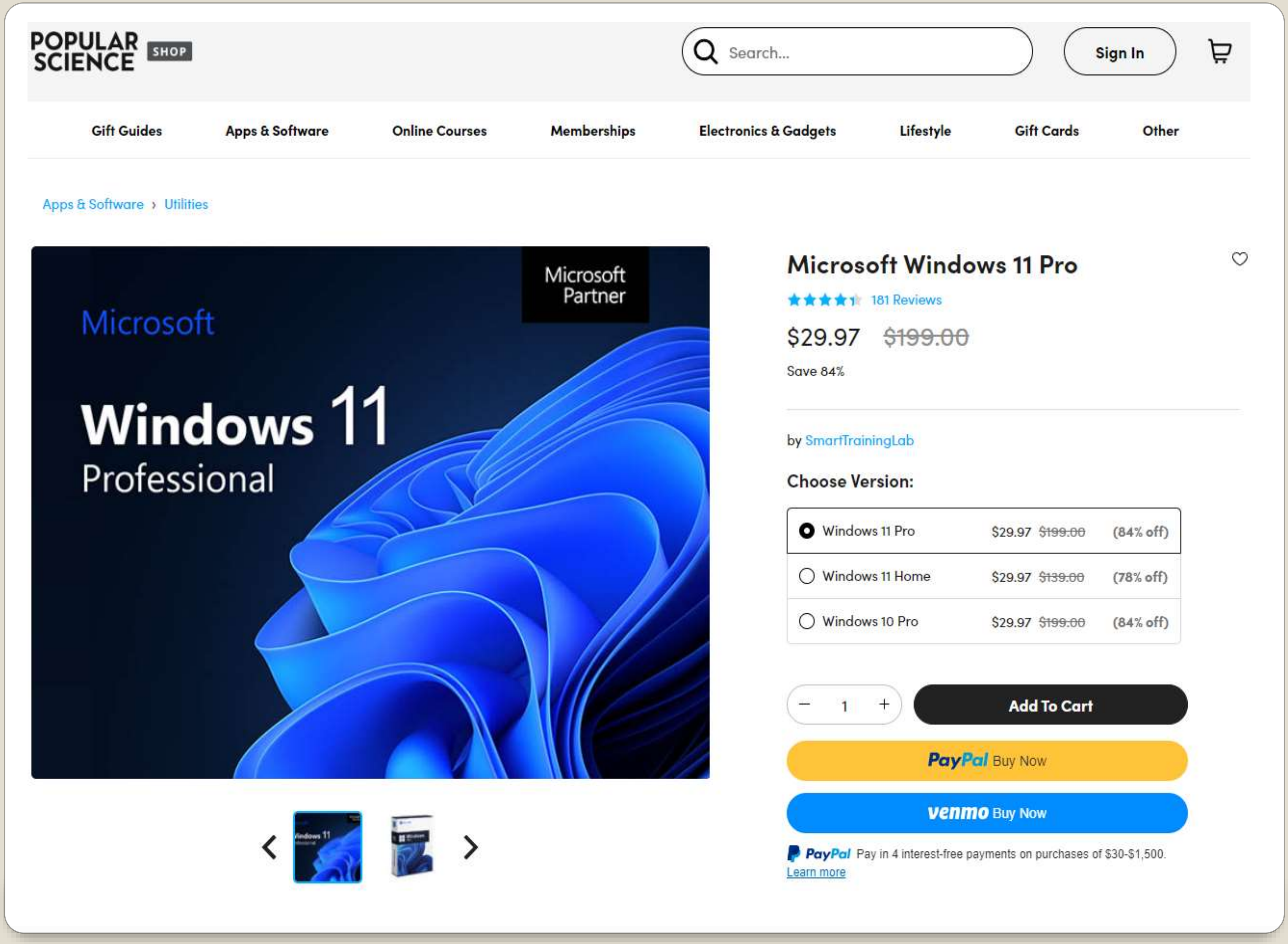
Sponsored Content

Elevate your PC with Windows 11 Pro, now further price-dropped to $29.97 for a limited time

Save $170 and enhance your Windows OS through October 15.

BY STACK COMMERCE | PUBLISHED OCT 10, 2023 9:00 AM EDT

Questionable Money Saver?



Apps & Software › Utilities

Microsoft Windows 11 Pro

★★★★☆ 181 Reviews

$29.97 ~~$199.00~~

Save 84%

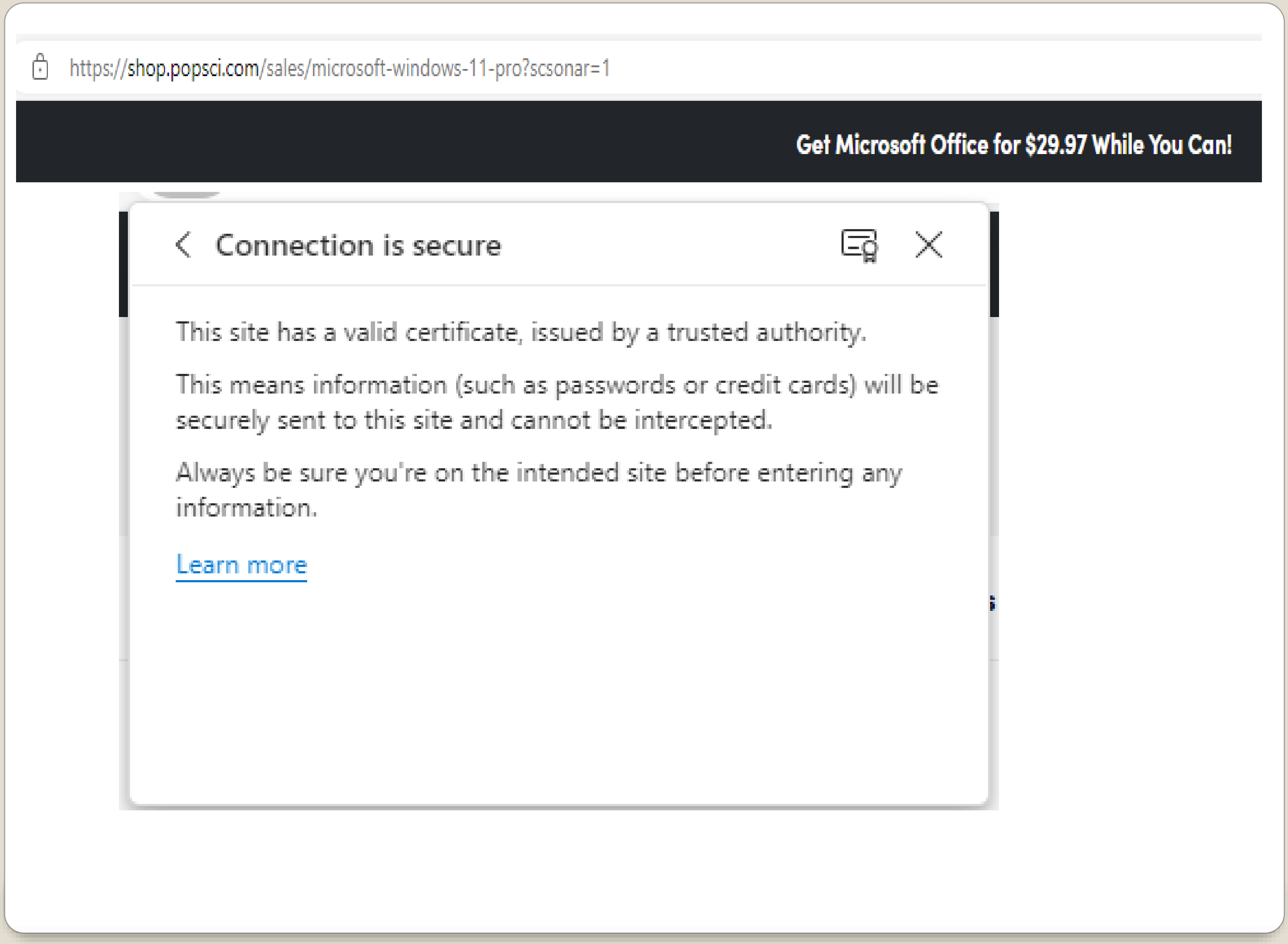
by SmartTrainingLab

Choose Version:

● Windows 11 Pro	$29.97	~~$199.00~~	(84% off)
○ Windows 11 Home	$29.97	~~$139.00~~	(78% off)
○ Windows 10 Pro	$29.97	~~$199.00~~	(84% off)

− 1 +

PayPal Pay in 4 interest-free payments on purchases of $30-$1,500.
Learn more



https://shop.popsci.com/sales/microsoft-windows-11-pro?scsonar=1

Get Microsoft Office for $29.97 While You Can!

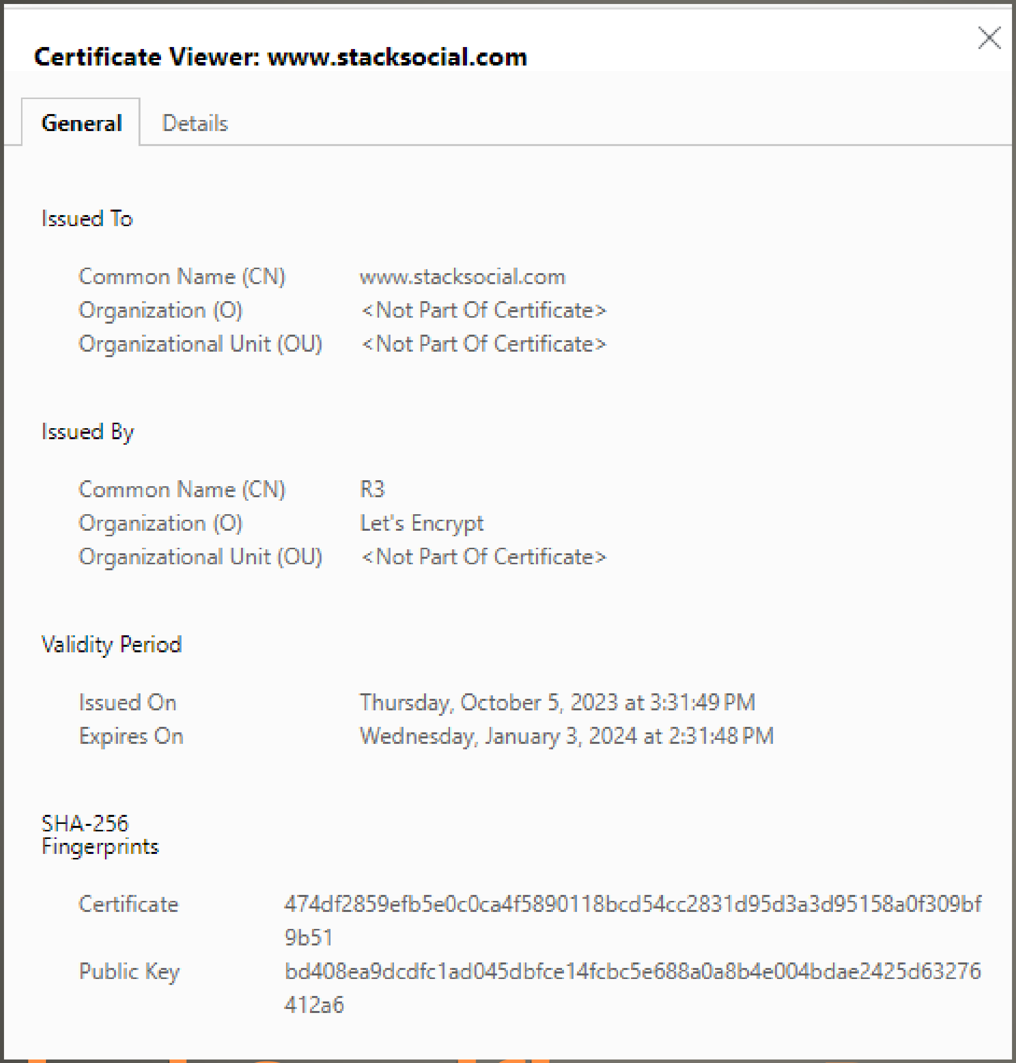
Connection is secure

This site has a valid certificate, issued by a trusted authority.

This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.

Always be sure you're on the intended site before entering any information.

Learn more



Certificate Viewer: www.stacksocial.com

Issued To

Common Name (CN) www.stacksocial.com
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>

Issued By

Common Name (CN) R3
Organization (O) Let's Encrypt
Organizational Unit (OU) <Not Part Of Certificate>

Validity Period

Issued On Thursday, October 5, 2023 at 3:31:49 PM
Expires On Wednesday, January 3, 2024 at 2:31:48 PM

SHA-256 Fingerprints

Certificate 474df2859efb5e0c0ca4f5890118bcd54cc2831d95d3a3d95158a0f309bf9b51
Public Key bd408ea9dcdfc1ad045dbfce14fcbc5e688a0a8b4e004bdae2425d63276412a6

Digital Certificate Details

- Lock icon does NOT mean the site is

  Safe

  Secure
- Just the traffic is encrypted

  Until delivered to site

  -or-

  Until delivered to attacker
- Not 90+% of sites are HTTPS with Lock
- The Lock icon can and may be overlaid

Revisit Lock details

Revisit “hover over”

- Refer – off to (many) other sites
- May revert to HTTP

- eMail addresses
- Burner email addresses
- eMail aliases

- FBI & CISA AvosLocker ransomware advisory

  Open Source and commercial tools

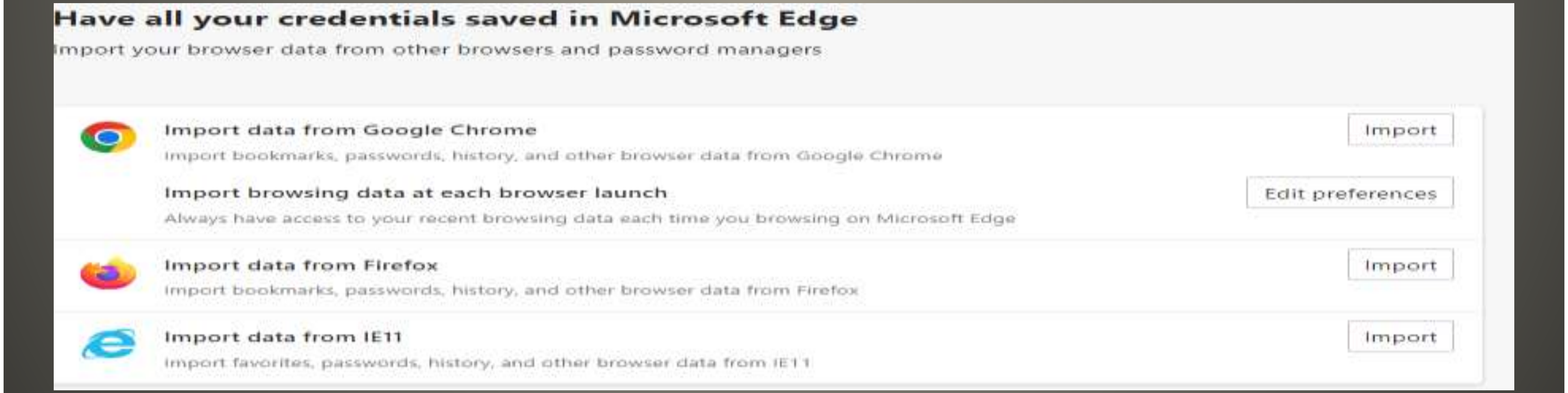
- Microsoft Edge snooping on Chrome browsing activity

  Part of changing browsers

  Import history, passwords, etc.

  Edge can copy Chrome browser data

  edge://settings/profiles



Have all your credentials saved in Microsoft Edge

Import your browser data from other browsers and password managers

Import data from Google Chrome

Import bookmarks, passwords, history, and other browser data from Google Chrome

Import browsing data at each browser launch

Always have access to your recent browsing data each time you browsing on Microsoft Edge

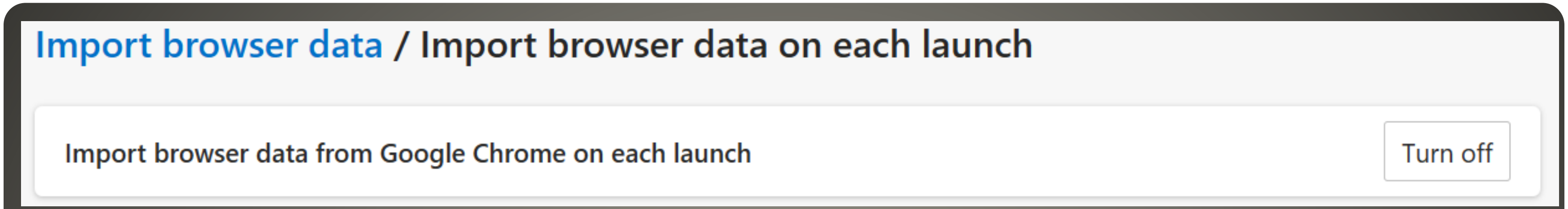
Import data from Firefox

Import bookmarks, passwords, history, and other browser data from Firefox

Import data from IE11

Import favorites, passwords, history, and other browser data from IE11

Current Issues



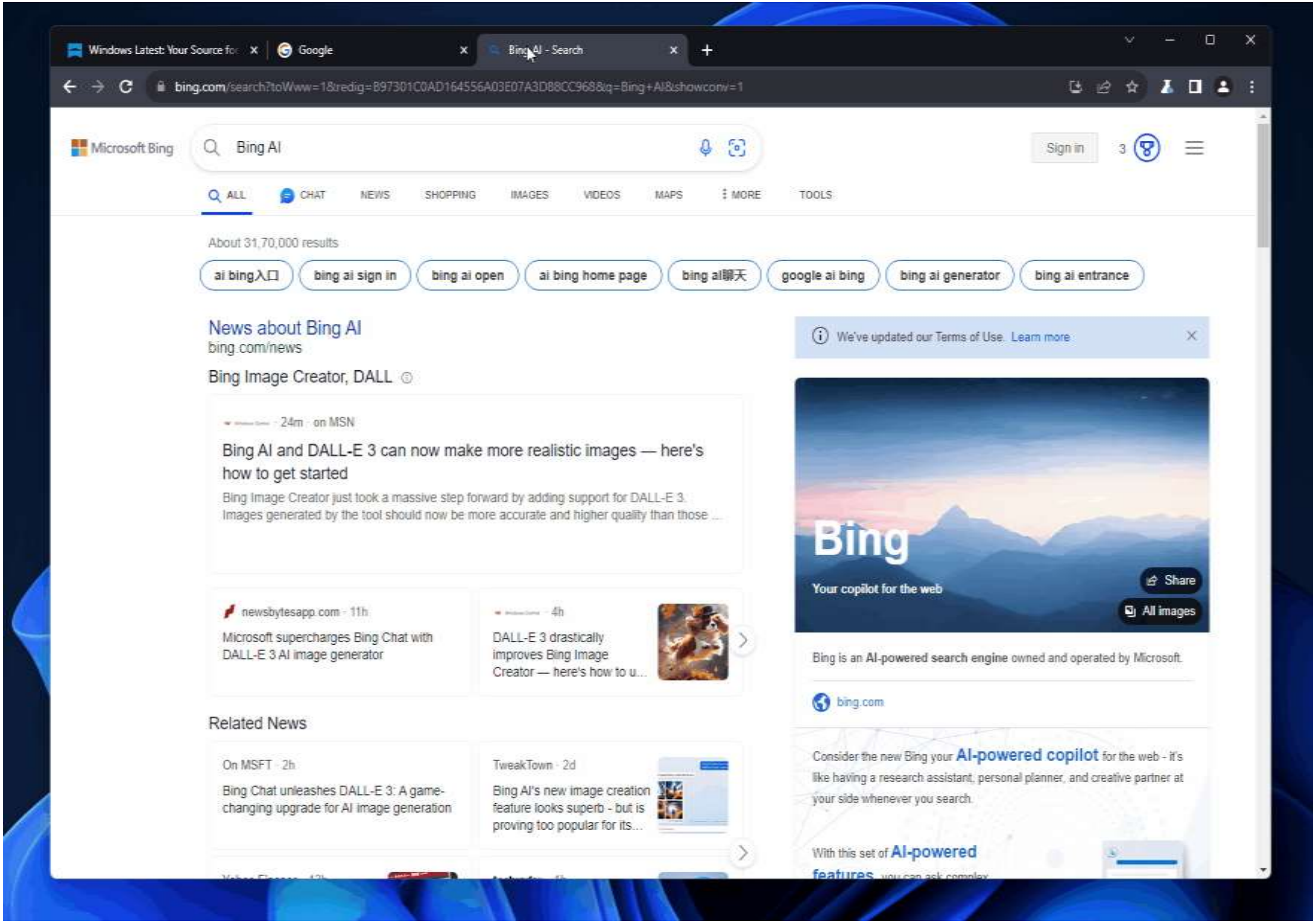
Import browser data / Import browser data on each launch

Import browser data from Google Chrome on each launch

Current Issues

- Bay Area restaurant’s Instagram scam
  GreatResturant vs. GreatResturant_
  Very good copy of GreatResturant’s Instagram page
  Collect $$ for reservation
- Atlassian Confluence servers
  FBI & CISA “patch immediately”
- SSN last 4
  XXX-YY-1234
  predictable given birth or first enroll location
  XXX – State
  YY – Group
- Amazon to buy $1B of Microsoft licenses
- YouTube Ad blockers
  Malicious content vs. YouTube
  Subscribe = less privacy

Current Issues



About 31,70,000 results

News about Bing AI
bing.com/news

Bing Image Creator, DALL

24m · on MSN

Bing AI and DALL-E 3 can now make more realistic images — here's how to get started

Bing Image Creator just took a massive step forward by adding support for DALL-E 3. Images generated by the tool should now be more accurate and higher quality than those ...

newsbytesapp.com · 11h
Microsoft supercharges Bing Chat with DALL-E 3 AI image generator

4h
DALL-E 3 drastically improves Bing Image Creator — here's how to u...

Related News

On MSFT · 2h
Bing Chat unleashes DALL-E 3: A game-changing upgrade for AI image generation

TweakTown · 2d
Bing AI's new image creation feature looks superb - but is proving too popular for its...

We've updated our Terms of Use. Learn more

Bing
Your copilot for the web

Bing is an AI-powered search engine owned and operated by Microsoft.

bing.com

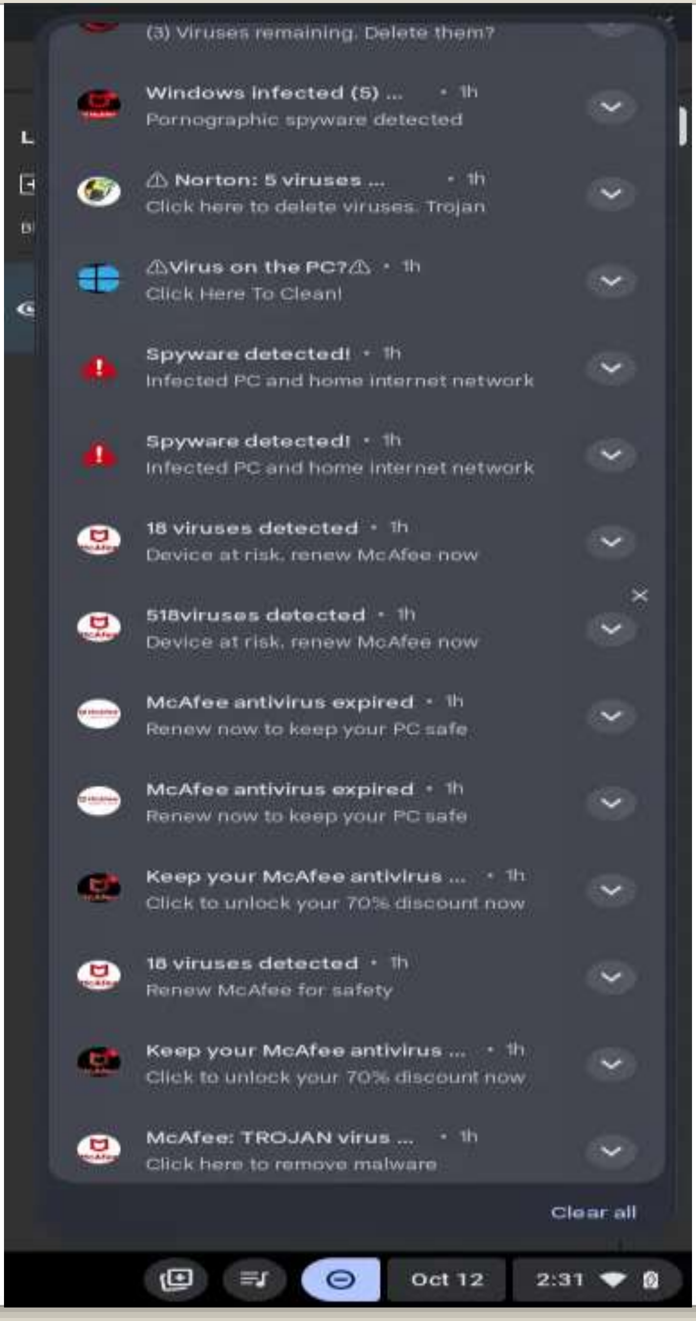
Consider the new Bing your AI-powered copilot for the web - it's like having a research assistant, personal planner, and creative partner at your side whenever you search.

With this set of AI-powered features, you can ask complex

- ChromeOS

  Linux, Sandboxing, Verified boot, Automatic updates, Safe browsing, Gmail spam elimination
- Websites dump into Chrome Notifications
- “Send us money”
- So, probably not

Chromebook has a Virus?



(3) Viruses remaining. Delete them?

Windows infected (5) ... • 1h
Pornographic spyware detected

⚠ Norton: 5 viruses ... • 1h
Click here to delete viruses. Trojan

⚠Virus on the PC?⚠ • 1h
Click Here To Clean!

Spyware detected! • 1h
Infected PC and home internet network

Spyware detected! • 1h
Infected PC and home internet network

18 viruses detected • 1h
Device at risk, renew McAfee now

518viruses detected • 1h
Device at risk, renew McAfee now

McAfee antivirus expired • 1h
Renew now to keep your PC safe

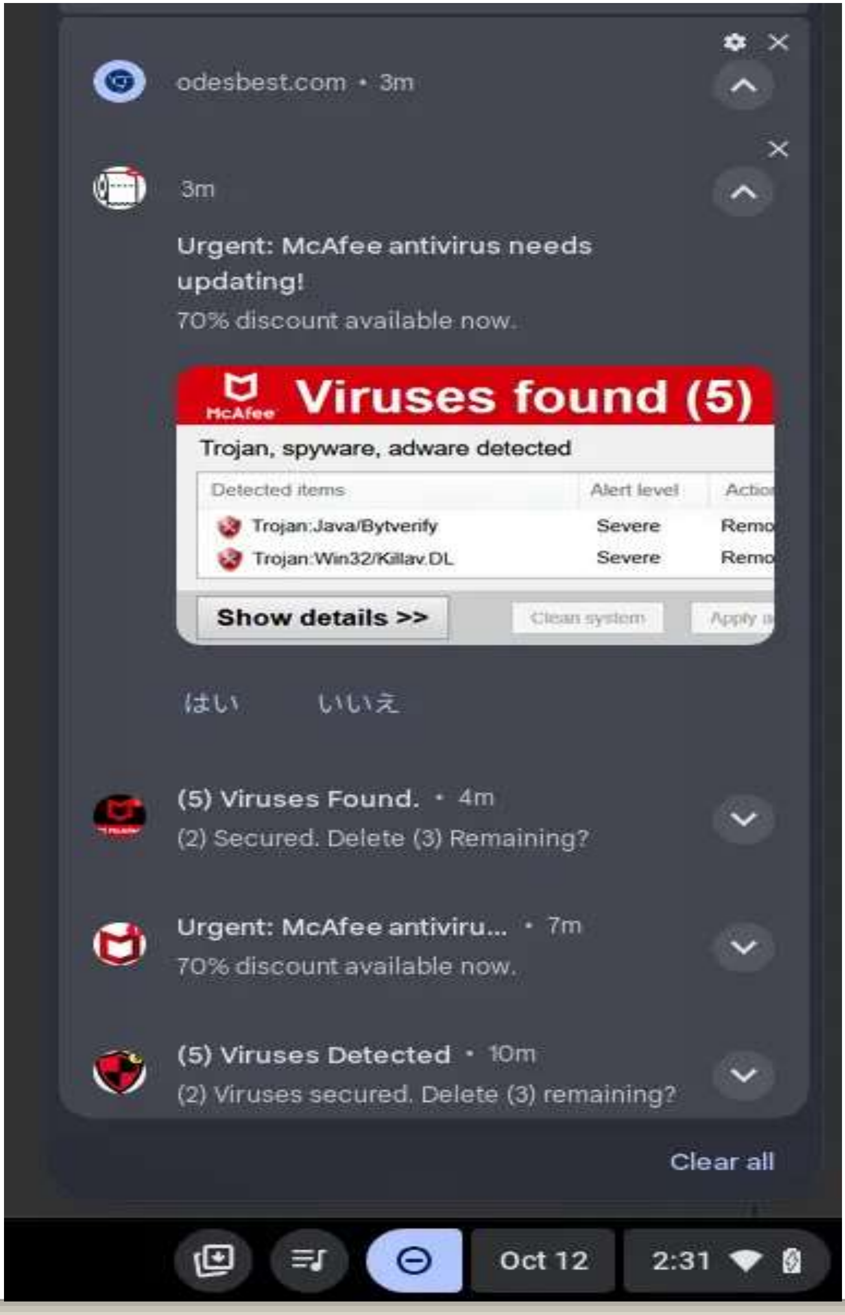
McAfee antivirus expired • 1h
Renew now to keep your PC safe

Keep your McAfee antivirus ... • 1h
Click to unlock your 70% discount now

18 viruses detected • 1h
Renew McAfee for safety

Keep your McAfee antivirus ... • 1h
Click to unlock your 70% discount now

McAfee: TROJAN virus ... • 1h
Click here to remove malware



odesbest.com • 3m

3m

Urgent: McAfee antivirus needs updating!
70% discount available now.

Viruses found (5)
Trojan, spyware, adware detected

Detected items	Alert level	Actio
Trojan:Java/Bytverify	Severe	Remo
Trojan:Win32/Killav.DL	Severe	Remo

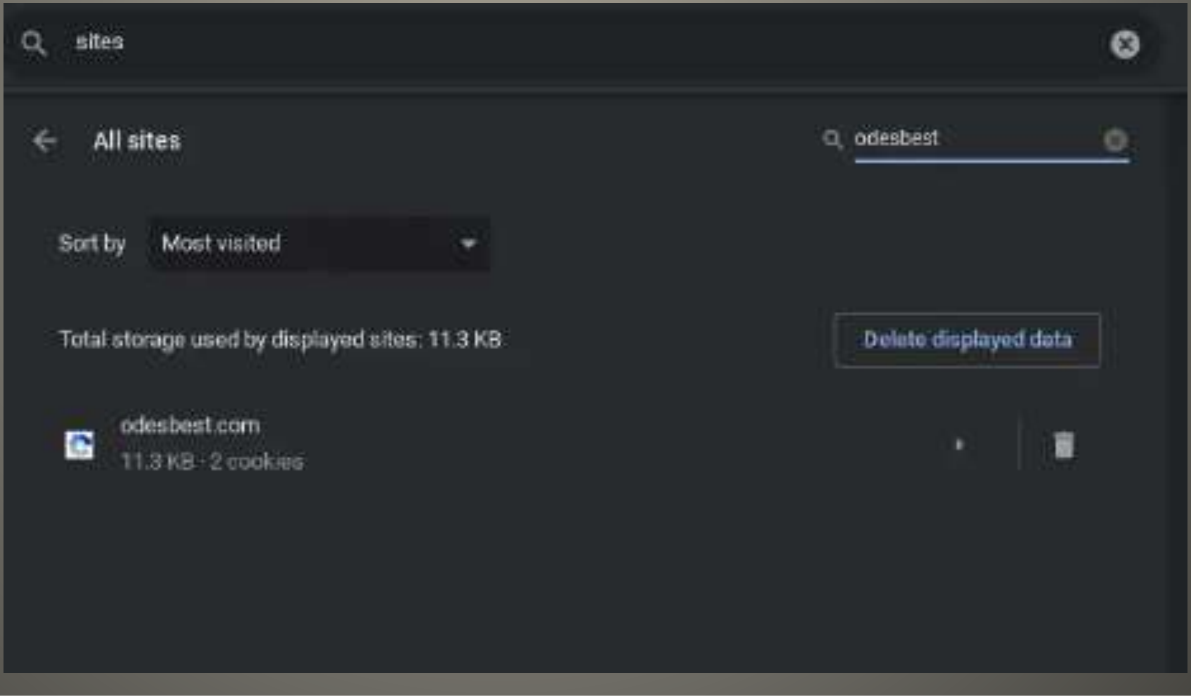
はい　いいえ

(5) Viruses Found. • 4m
(2) Secured. Delete (3) Remaining?

Urgent: McAfee antiviru... • 7m
70% discount available now.

(5) Viruses Detected • 10m
(2) Viruses secured. Delete (3) remaining?

- Chrome > Settings > Privacy and security
- Site Settings
- Odesbest – deceptive web site
- exploits browser push notifications



sites

All sites

odesbest

Sort by Most visited

Total storage used by displayed sites: 11.3 KB

odesbest.com
11.3 KB · 2 cookies

A Fix

Current Issues

- MACE Act

  Modernizing the Acquisition of Cyber Security Experts

- Reset Printers, routers, wireless access points, disk drives,

  Before next recycle event, or ….

  Stickers ???

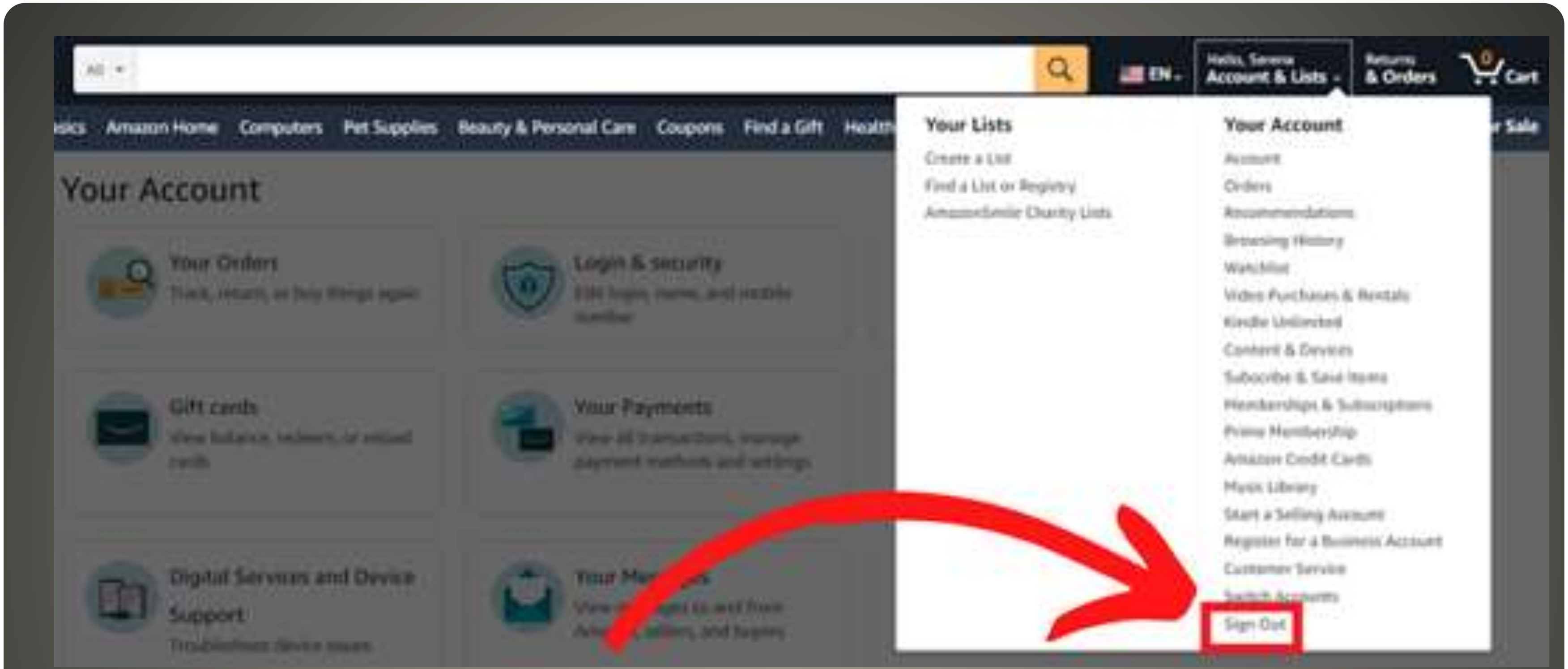
  Our modern cars

- ServiceNow

  Unauthenticated attackers extract data

  Since 2015

- Catalytic converter thefts 1215%
- Amazon needs explicit sign out



Your Account

Your Orders
Track, return, or buy things again

Login & security
Edit login, name, and mobile number

Gift cards
View balance, redeem, or reload cards

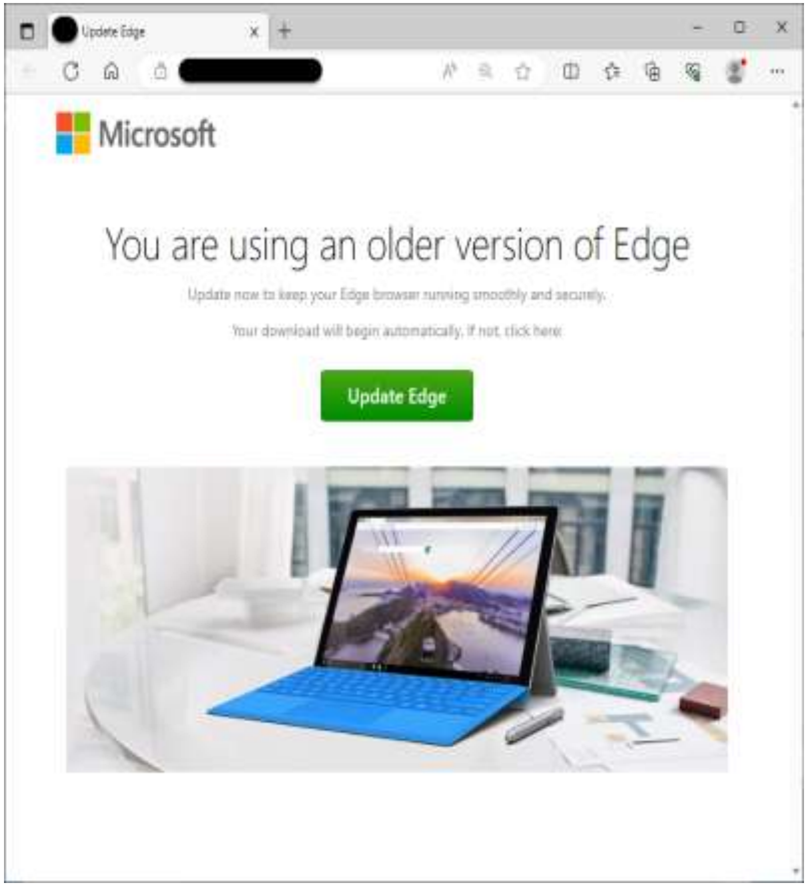
Your Payments
View all transactions, manage payment methods and settings

Digital Services and Device Support
Troubleshoot device issues

Your Messages
View messages to and from Amazon, sellers, and buyers

Current Issues

- Cisco IOS XE devices
  Actively exploited   Full network control
  Severity 10
- SpyNote Android banking trojan
  Die Hard services
  Factory reset to remove
- Browser “updates” iff from Browser vendor
- WinRAR vulnerability version 6.24 to resolve
- Google Drive drop requirement for 3rd party cookies   2024



Update Edge [redacted]

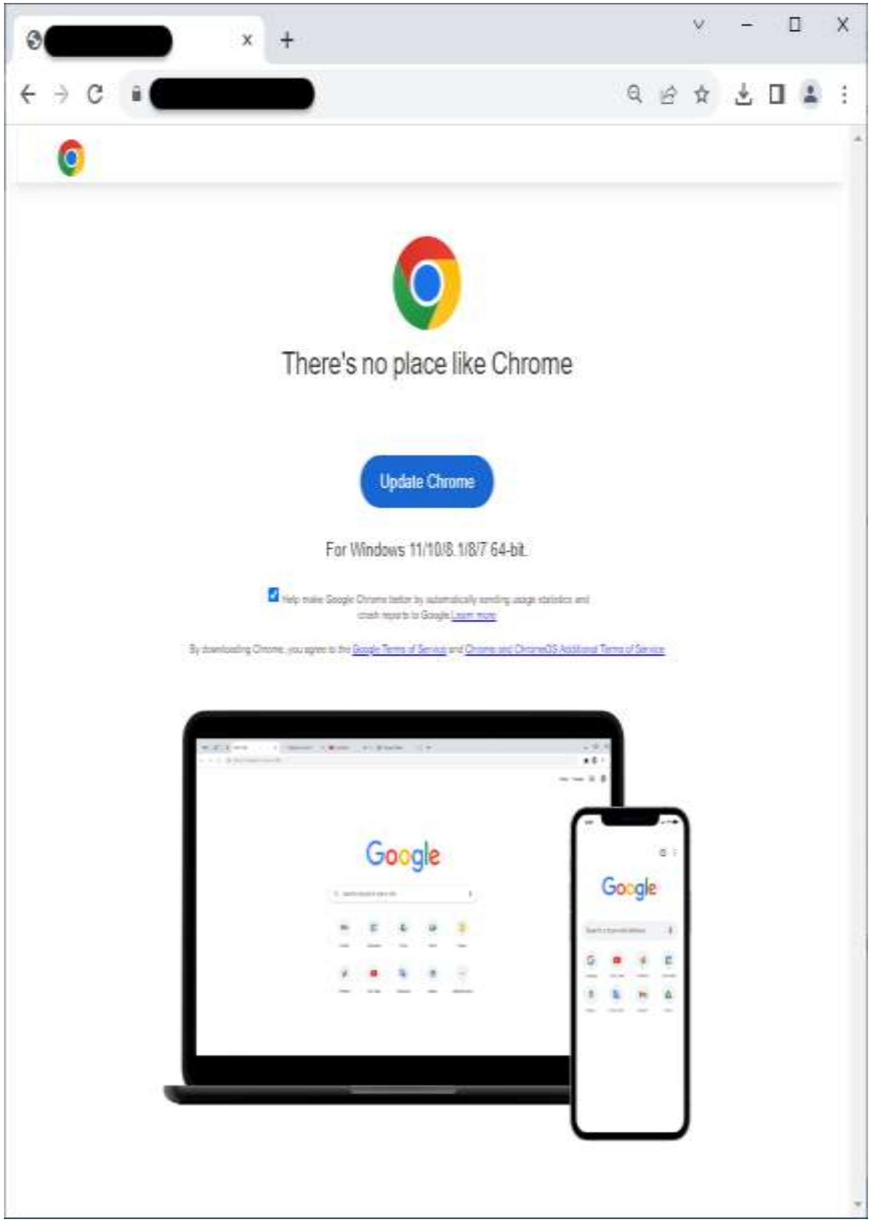
[redacted]

Microsoft

You are using an older version of Edge

Update now to keep your Edge browser running smoothly and securely.

Your download will begin automatically. If not, click here.



[redacted]

[redacted]

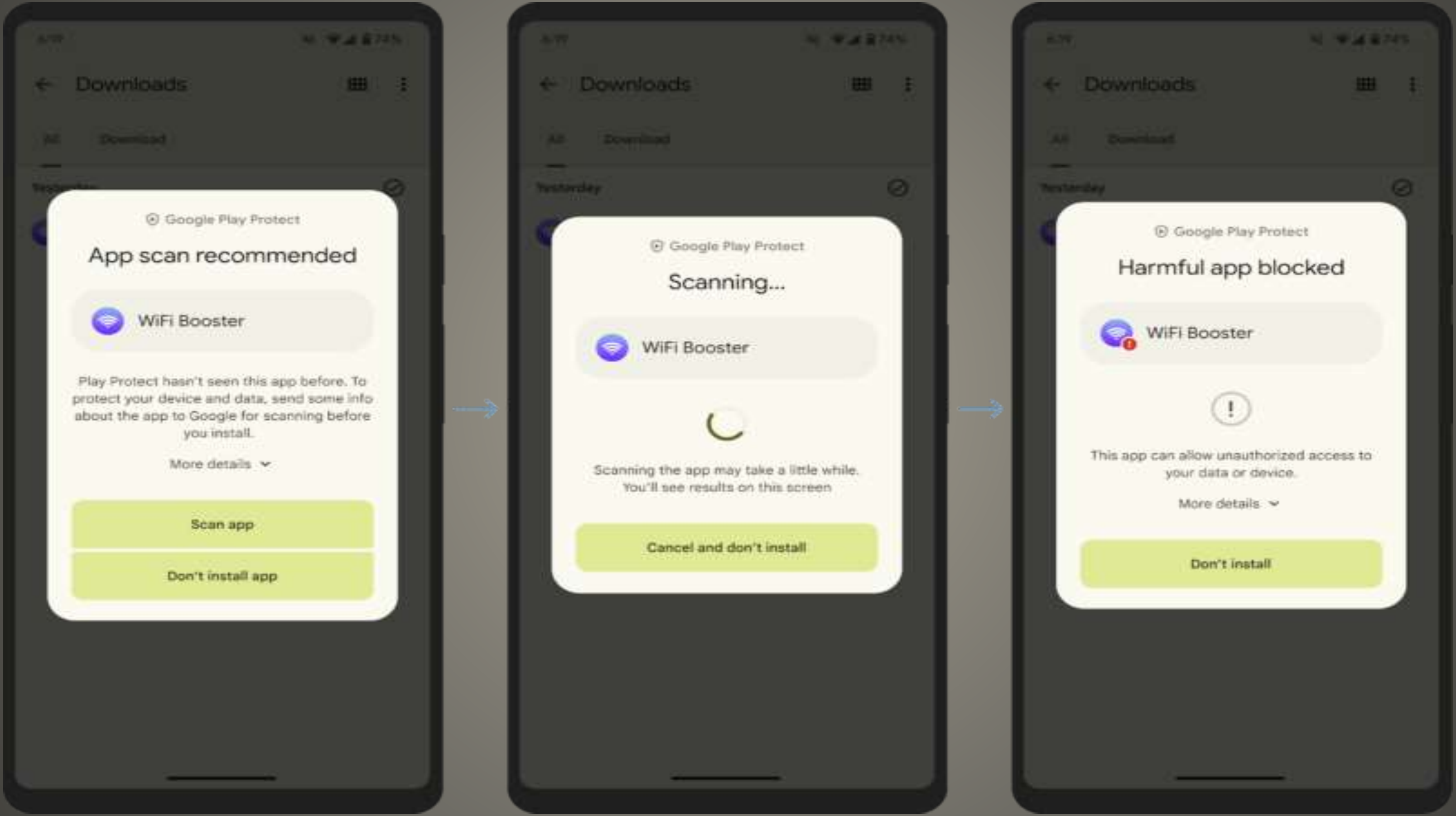
There's no place like Chrome

For Windows 11/10/8.1/8/7 64-bit.

☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. Learn more

By downloading Chrome, you agree to the Google Terms of Service and Chrome and ChromeOS Additional Terms of Service

- Sent to Google for analysis



App scan recommended

WiFi Booster

Play Protect hasn't seen this app before. To protect your device and data, send some info about the app to Google for scanning before you install.

Scanning...

WiFi Booster

Scanning the app may take a little while. You'll see results on this screen

Harmful app blocked

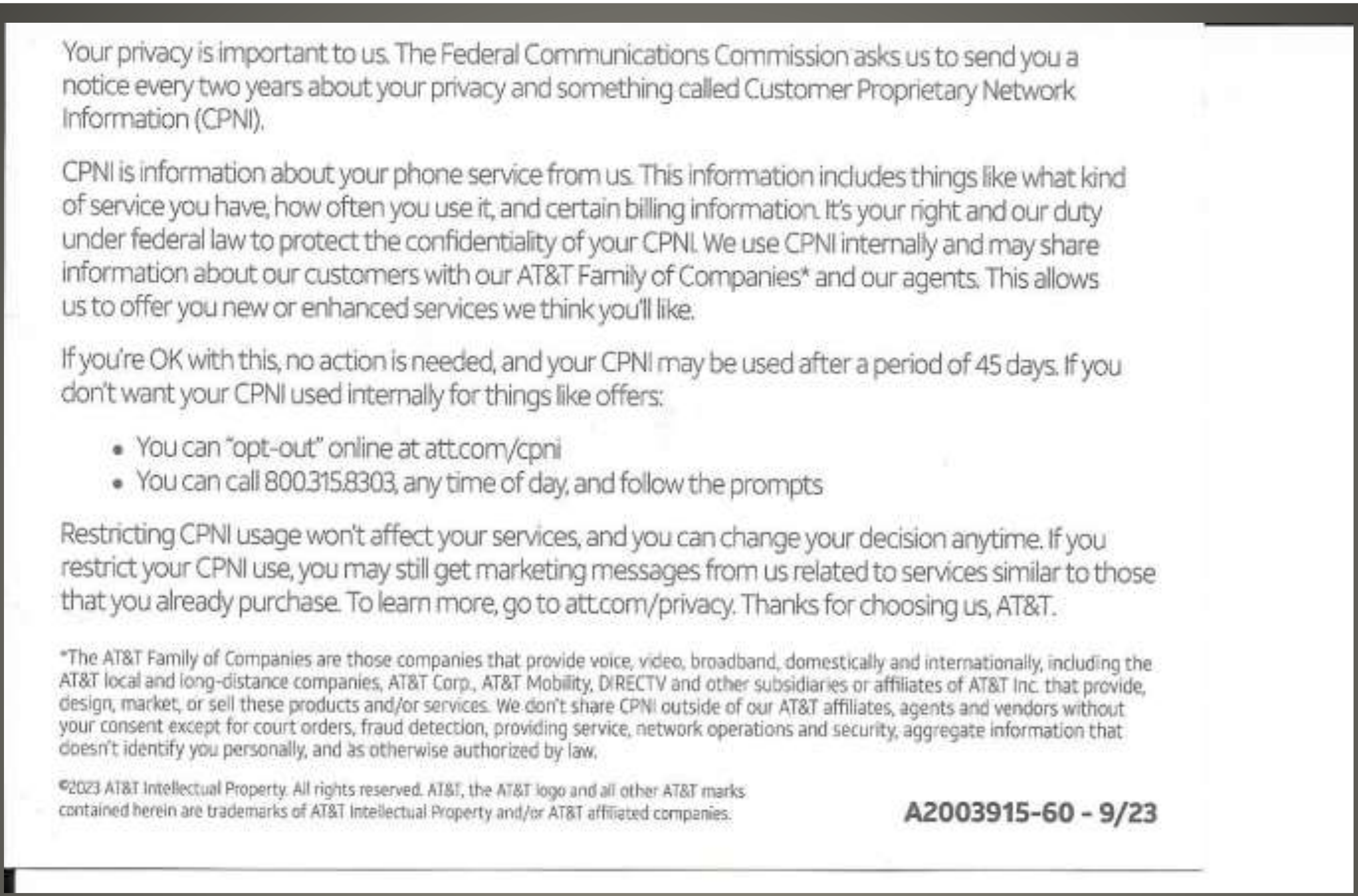
WiFi Booster

This app can allow unauthorized access to your data or device.

Android scan sideloaded apps

Google Android Play Protect

- Update to protect against polymorphic malware



Your privacy is important to us. The Federal Communications Commission asks us to send you a notice every two years about your privacy and something called Customer Proprietary Network Information (CPNI).

CPNI is information about your phone service from us. This information includes things like what kind of service you have, how often you use it, and certain billing information. It's your right and our duty under federal law to protect the confidentiality of your CPNI. We use CPNI internally and may share information about our customers with our AT&T Family of Companies* and our agents. This allows us to offer you new or enhanced services we think you'll like.

If you're OK with this, no action is needed, and your CPNI may be used after a period of 45 days. If you don't want your CPNI used internally for things like offers:

- You can "opt-out" online at att.com/cpni
- You can call 800.315.8303, any time of day, and follow the prompts

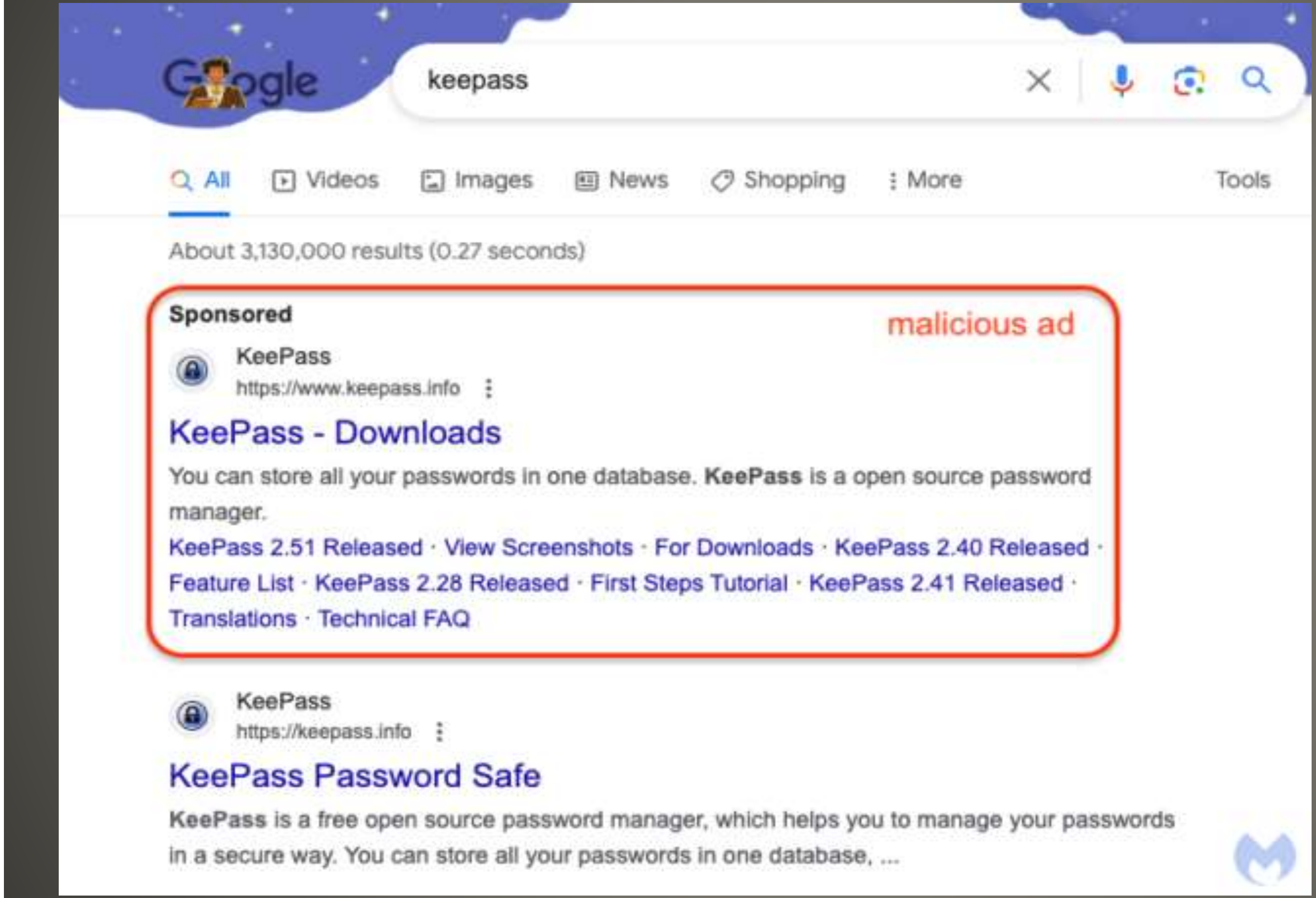
Restricting CPNI usage won't affect your services, and you can change your decision anytime. If you restrict your CPNI use, you may still get marketing messages from us related to services similar to those that you already purchase. To learn more, go to att.com/privacy. Thanks for choosing us, AT&T.

*The AT&T Family of Companies are those companies that provide voice, video, broadband, domestically and internationally, including the AT&T local and long-distance companies, AT&T Corp., AT&T Mobility, DIRECTV and other subsidiaries or affiliates of AT&T Inc. that provide, design, market, or sell these products and/or services. We don't share CPNI outside of our AT&T affiliates, agents and vendors without your consent except for court orders, fraud detection, providing service, network operations and security, aggregate information that doesn't identify you personally, and as otherwise authorized by law.

A2003915-60 - 9/23

AT&T Customer Proprietary Network Information

- Hosted on Google



keepass

About 3,130,000 results (0.27 seconds)

Sponsored

malicious ad

KeePass
https://www.keepass.info

KeePass - Downloads

You can store all your passwords in one database. **KeePass** is a open source password manager.

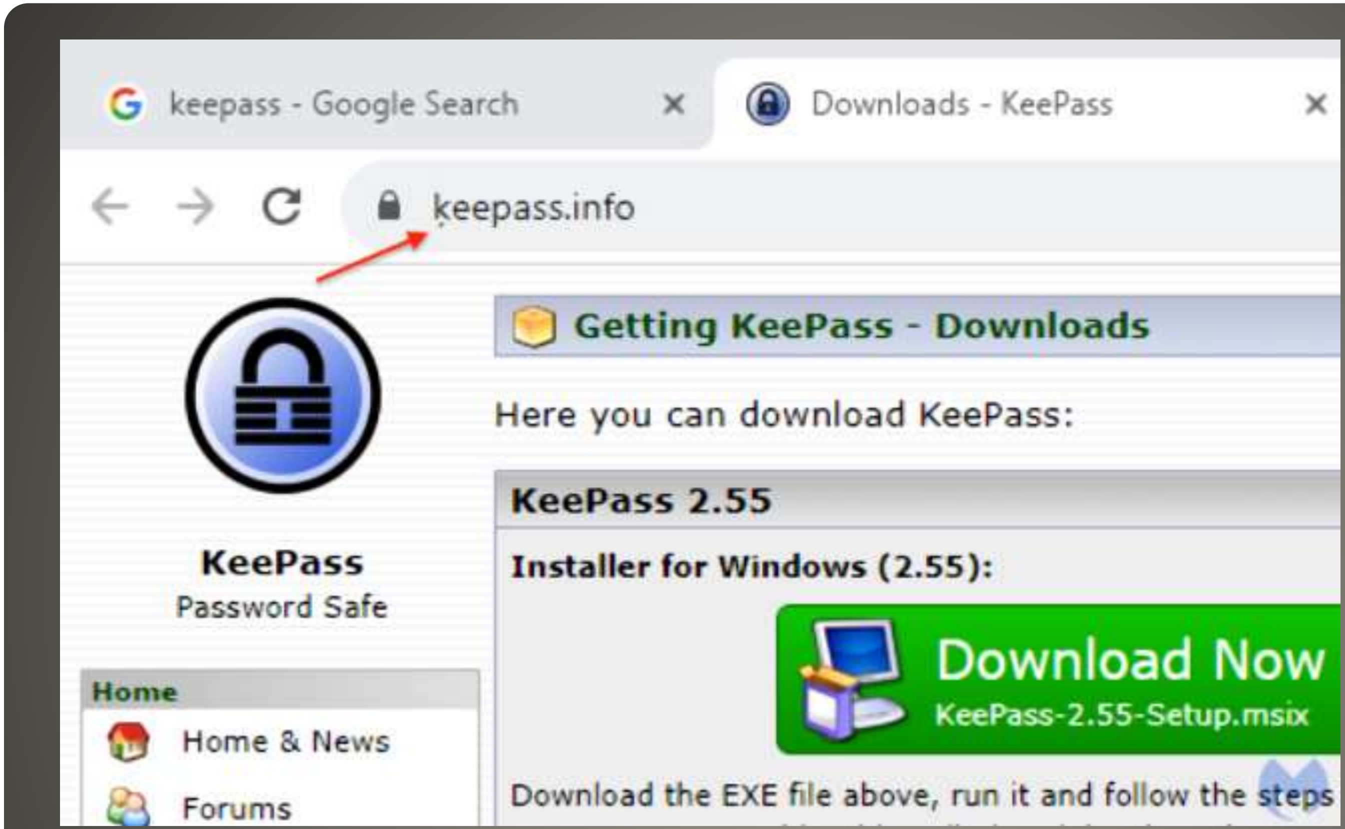
KeePass 2.51 Released · View Screenshots · For Downloads · KeePass 2.40 Released · Feature List · KeePass 2.28 Released · First Steps Tutorial · KeePass 2.41 Released · Translations · Technical FAQ

KeePass
https://keepass.info

KeePass Password Safe

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. You can store all your passwords in one database, ...

KeePass



keepass - Google Search ×

Downloads - KeePass ×

ķeepass.info

KeePass
Password Safe

Home

Home & News

Forums

Getting KeePass - Downloads

Here you can download KeePass:

KeePass 2.55

Installer for Windows (2.55):

Download Now
KeePass-2.55-Setup.msix

Download the EXE file above, run it and follow the steps

, ķeepass[.]info–

xn--eepass-vbb[.]info,

KeePass punnycode

- Check the Digital Certificate

Check the Digital Certificate

SMS

- Short Message Service
- Not encrypted

Provider(s)

Warrant Court

Altered in transit

Metadata

Signal, WhatsApp, Telegram

False Signal, WhatsApp, Telegram

Privacy

- Ride services
- Food delivery services
- Social media

CISA, NSA, FBI, MS-ISAC

- https://www.cisa.gov/news-events/news/cisa-nsa-fbi-ms-isac-publish-guide-preventing-phishing-intrusions

- https://www.cisa.gov/news-events/alerts/2023/10/19/cisa-nsa-fbi-and-ms-isac-release-update-stopransomware-guide

Passkeys gain traction

- Amazon – kinda
- Google account – default
- GitHub, Windows 11, TikTok, 1Password

Beeper

- Messaging:

  Messages, WhatsApp, Signal, Telegram, GroupMe, Google Chat, Discord, Slack, Messenger, Snapchat, LinkedIn, Instagram, X, Reddit, TikTok
- Now Chat

- Got one of these plans?

One, Simple Choice, Magenta, Magenta 55 Plus

Expect price increase in November

T-Mobile customer support
1-800-TMOBILE
1-800-2453

T-Mobile

Artificial Intllegence
Machine Learning
Large Language Models

- 60 minutes Holocaust story
- 55,000 survivors interviewed
- 20 camera sphere 3D hologram
- 2000 questions

- HereAfter AI

HereAfter AI

AI PIN

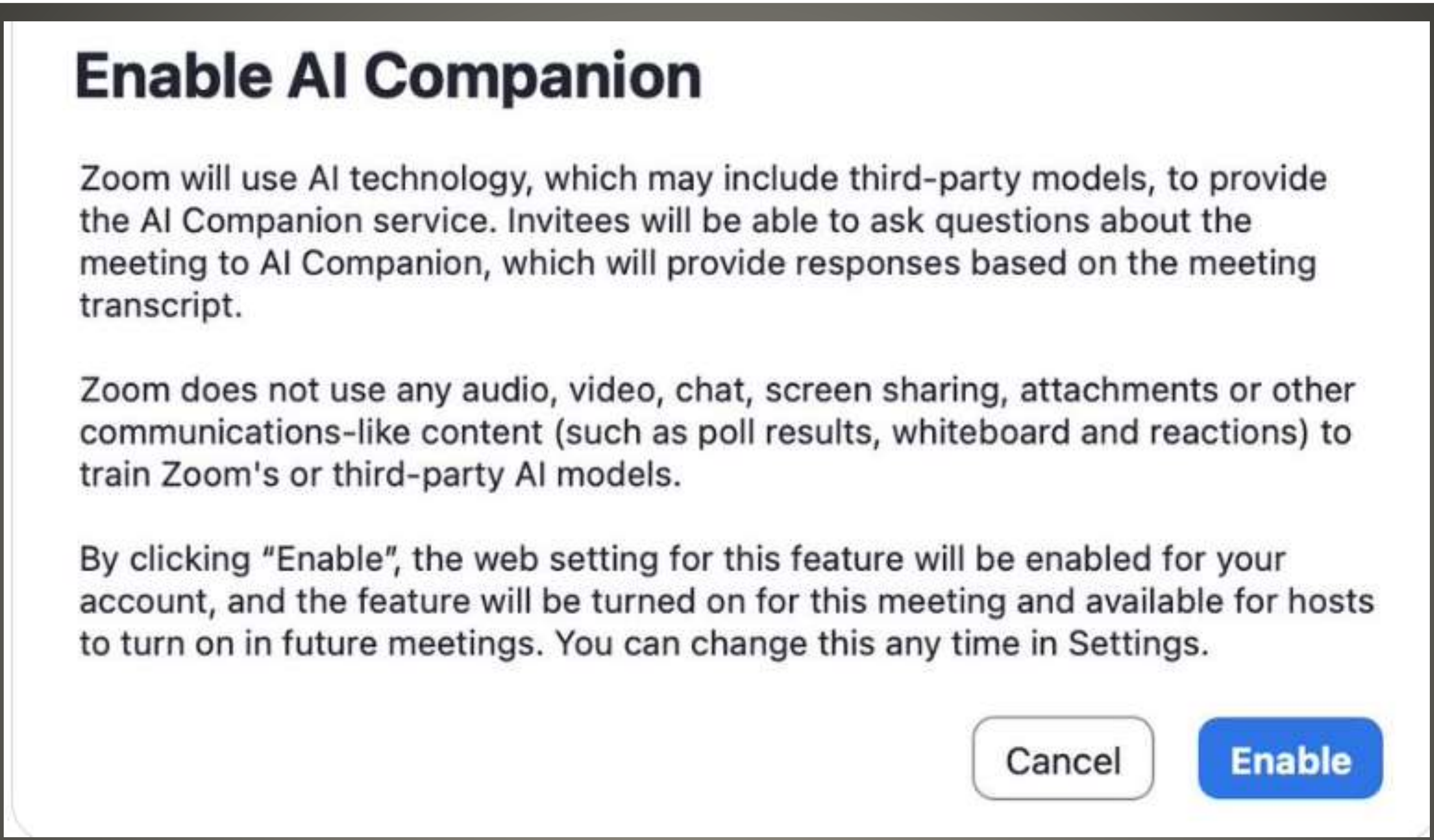
AI PIN

- Seamless, Screenless, Sensing
- Standalone
- AI to “learn about you”
- Capture toddler’s first steps w/o phone between you
- Hold object, identify and question about it
- Concerts filmed without crowd’s hands
- Instant translations
- Speak translation in owner’s voice
- Capture and sort personal data
- “Catch me up”

- https://www.ted.com/talks/imran_chaudhri_the_disappearing_computer_and_a_world_where_you_can_take_ai_everywhere

- US, UK, select countries in Asia & South America
- Temporary unavailable in Europe – privacy laws
- “In the European Economic Area (EEA), Windows will now require consent to share data between Windows and other signed-in Microsoft services. You will see some Windows features start to check for consent now, with more being added in future builds.”

Windows Copilot restrictions



Enable AI Companion

Zoom will use AI technology, which may include third-party models, to provide the AI Companion service. Invitees will be able to ask questions about the meeting to AI Companion, which will provide responses based on the meeting transcript.

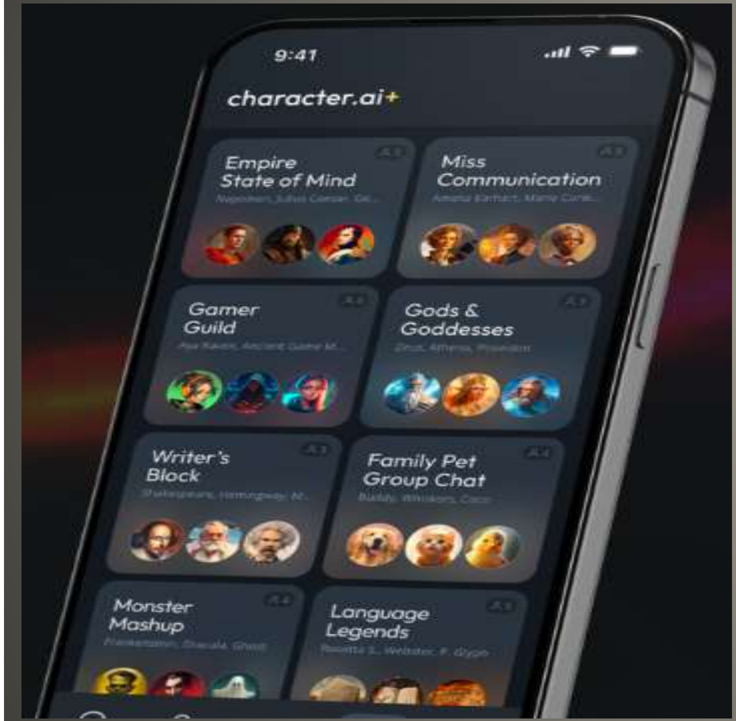
Zoom does not use any audio, video, chat, screen sharing, attachments or other communications-like content (such as poll results, whiteboard and reactions) to train Zoom's or third-party AI models.

By clicking "Enable", the web setting for this feature will be enabled for your account, and the feature will be turned on for this meeting and available for hosts to turn on in future meetings. You can change this any time in Settings.

Zoom

- Character.AI

  Group chats with multiple AI can talk



Character.AI Group Chat

More Characters.

More Humans.

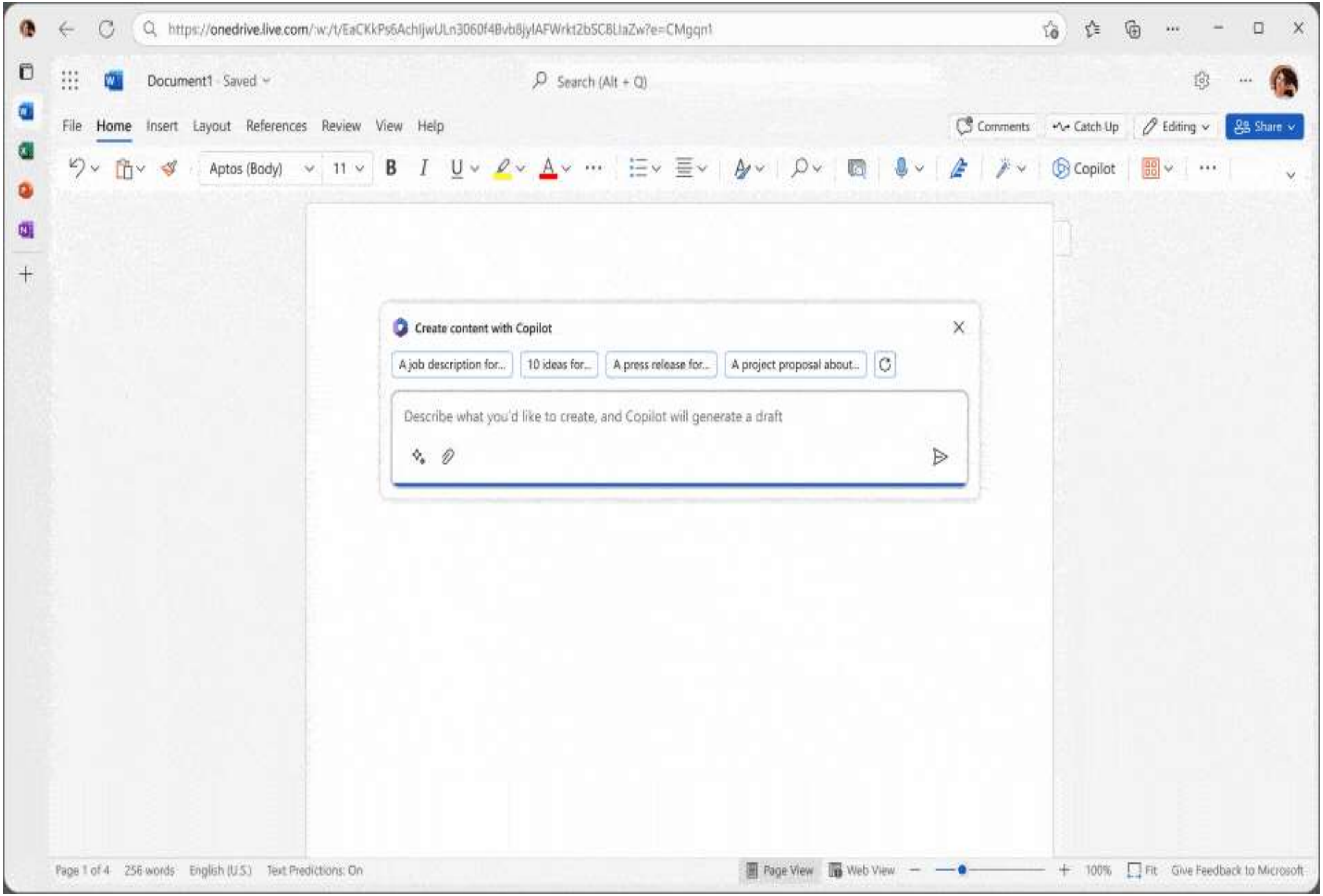
More Fun.

- Synthetic Humans

Chat Bots "talk" to each other

- AI assistant INSIDE Microsoft apps
  Office 365 and MORE
  Results can be sensitive

Microsoft Copilot



https://onedrive.live.com/:w:/t/EaCKkPs6AchIjwULn3060f4Bvb8jylAFWrkt2b5C8LIaZw?e=CMgqn1

Document1 · Saved

Create content with Copilot

A job description for... 10 ideas for... A press release for... A project proposal about...

Describe what you'd like to create, and Copilot will generate a draft

Page 1 of 4 256 words English (U.S.) Text Predictions: On

- Join Teams meetings

  summarize, action items, outstanding issues

- Outlook

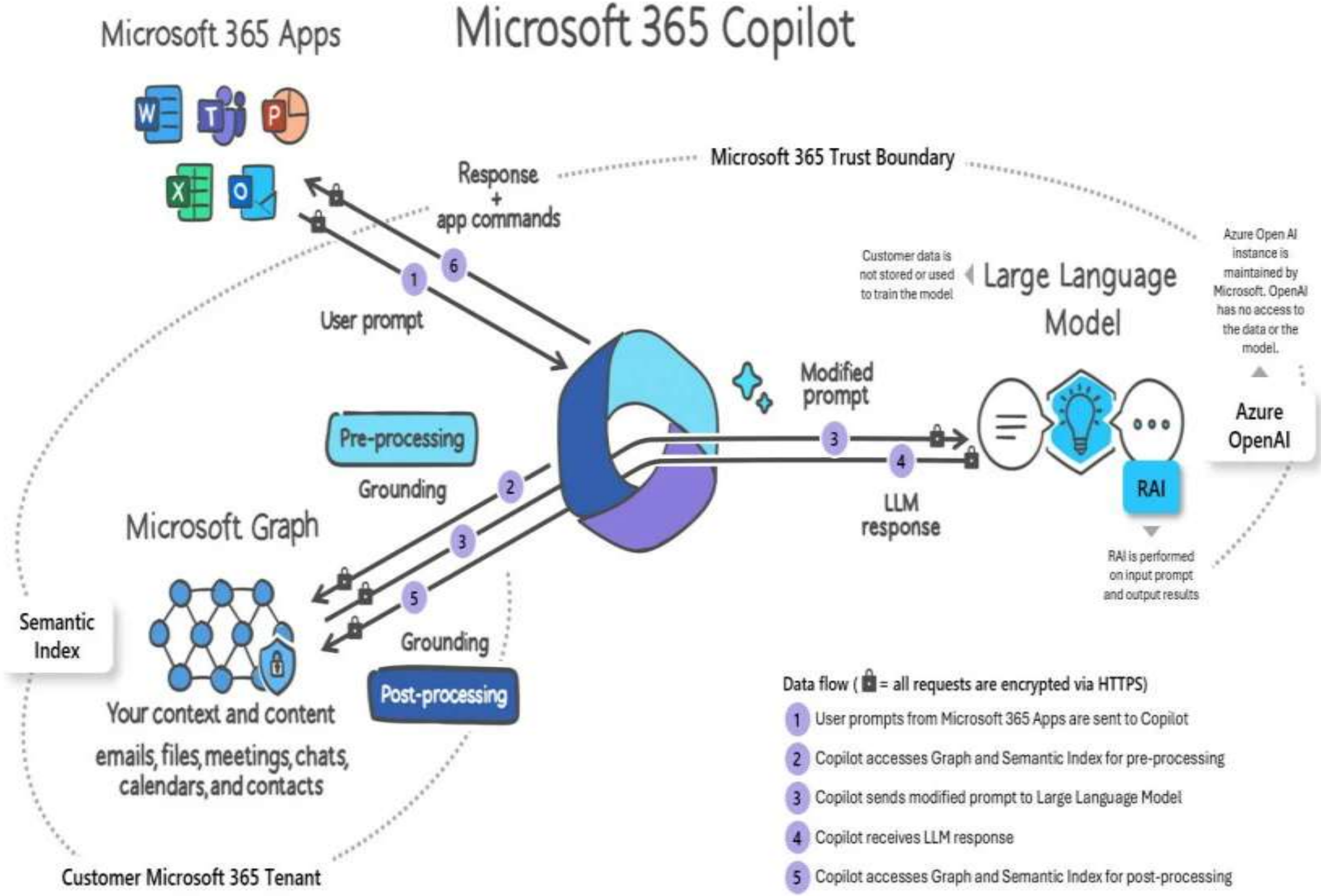
  triage inbox, summarize threads, generate replies

- Excel

  Analyze raw data, find trends

Microsoft Copilot

Microsoft 365 Copilot


Microsoft 365 Apps
Microsoft 365 Trust Boundary
Response
+
app commands
6
1
User prompt
Customer data is not stored or used to train the model
Large Language Model
Azure Open AI instance is maintained by Microsoft. OpenAI has no access to the data or the model.
Modified prompt
3
4
LLM response
Azure OpenAI
RAI
RAI is performed on input prompt and output results
Pre-processing
Grounding
2
3
5
Microsoft Graph
Semantic Index
Grounding
Post-processing
Your context and content
emails, files, meetings, chats, calendars, and contacts
Customer Microsoft 365 Tenant

Data flow (🔒 = all requests are encrypted via HTTPS)

1. User prompts from Microsoft 365 Apps are sent to Copilot
2. Copilot accesses Graph and Semantic Index for pre-processing
3. Copilot sends modified prompt to Large Language Model
4. Copilot receives LLM response
5. Copilot accesses Graph and Semantic Index for post-processing
6. Copilot sends the response, and app command back to Microsoft 365 Apps

- Tenant isolation. Copilot only uses data from the current user's M365 tenant. The AI tool will not surface data from other tenants that the user may be a guest, in nor any tenants that might be set up with cross-tenant sync.
- Training boundaries. Copilot does not use any of your business data to train the foundational LLMs that Copilot uses for all tenants. You shouldn't have to worry about your proprietary data showing up in responses to other users in other tenants.

Copilot security Model – the good

- Permissions. Copilot surfaces all organizational data to which individual users have at least view permissions.
- Labels. Copilot-generated content will not inherit the MPIP labels of the files Copilot sourced its response from.
- Humans. Copilot's responses aren't guaranteed to be 100% factual or safe; humans must take responsibility for reviewing AI-generated content.

Copilot Security Model – the bad

- Assistant with Bard
- October 4 Made by Google
- Command execution -> Personalized allies
- Text, Voice, Images
- Integration with Google World
- “Draft my social media post”
- United States – U.S.A

Google

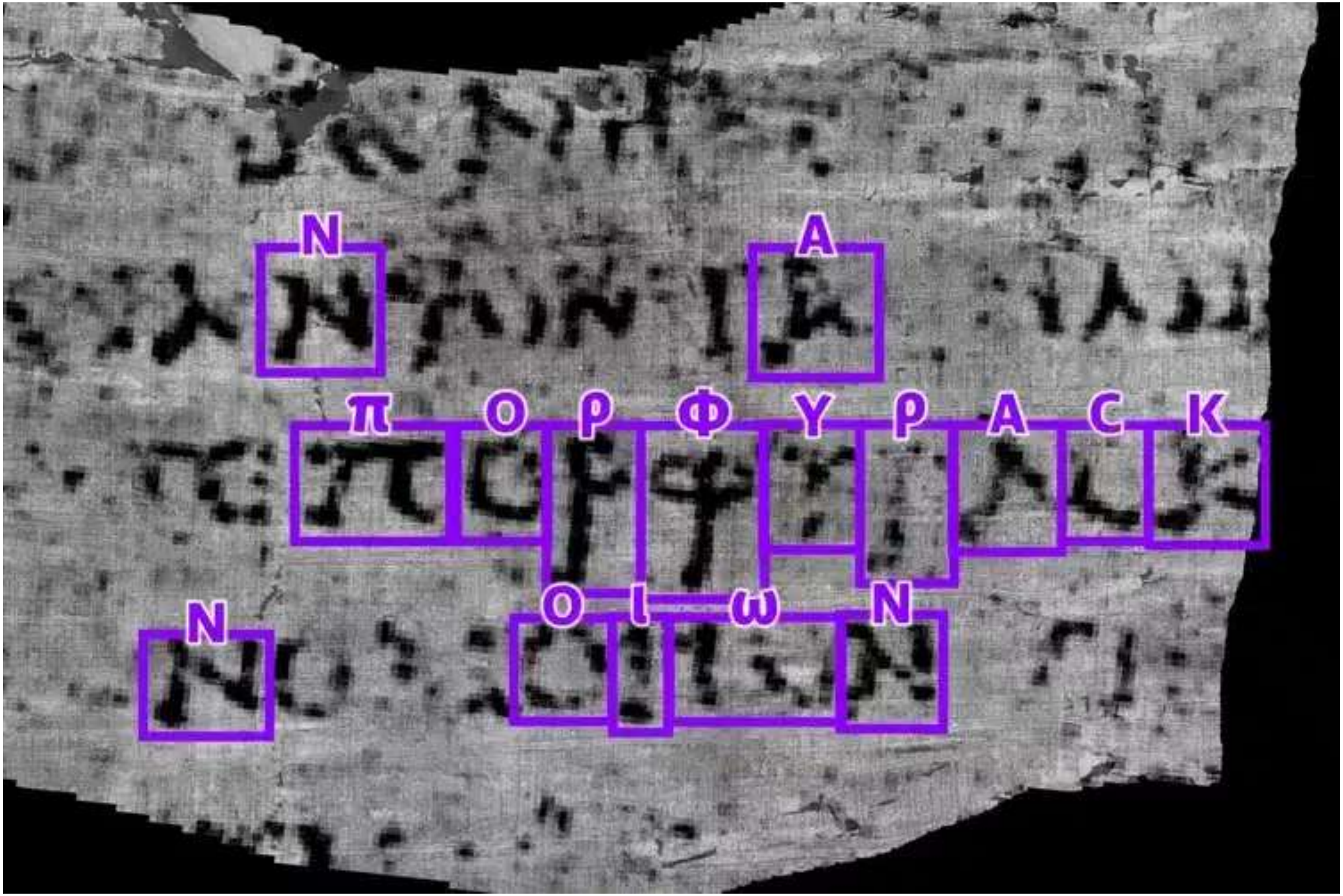
- ChatGPT words & sentences
- Basic science
- More and more specialized

Polymathic AI

- Microsoft will pay $15,000
  Get Bing AI to “go off the rails
- Face unlock Pixel 8 brothers
- California speeding drivers with cameras
- Apple *video reactions* video therapy sessions

Current Issues

AI reads ‘unreadable’ ancient scroll


N
A
π
O
ρ
Φ
Y
ρ
A
C
K
N
O
ι
ω
N

- 7 TB per glass sheet
- Data integrity 10,000 years
- Magnetic storage refresh 5 years
- Glass resistant to water, electronic pulses, temperatures, surface scratching, …
- Improved writing speeds

Microsoft Project Silica

- AI photo editors “do more, effortlessly”
- Photos ~~worth a thousand words~~

  worth a thousand fictions

None of our photos are real

- “Data Selfie”
- Chatbots “guess” PPI
  innocuous conversations based on training
  “caught morning tram”

- Harvard magazine reports:

“what transpired that day was a sobering glimpse of a not-too-distant future when AIs can find and exploit vulnerabilities with superhuman speed, scope, scale, and sophistication. These future AI hackers won’t be limited to computers. They will hack financial, political, and social systems in unimaginable ways — and people might not even notice until it’s too late.”

Cyber Grand Challenge

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com