

Sun City Computer Club

Cyber Security SIG
January 18, 2024

**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**

- NRO Anti-Fraud Group
- Williamson County Deputy Sheriff
Report Fraud
- Work-from-home scams
- [NRO Anti-Fraud Group](#)
- Scams and Computer Safety SIG

- For the good of our community
Report scams

Sun City NRO Bulletin Jan 17, 2024

SCCCyber

Wednesday, January 17, 2024

Google Chrome 0-day vulnerability 17-Jan-2024

Google released Chrome updates today. CVE-2024-0519.

Updates to Chrome browser are encouraged

Chrome version 120.0.6099.224/225 for Windows.

macOS version 120.0.6099.234

120.0.6099.224 for Linux

ChromeOS 120.0.6099.235

Posted by John Jenkinson at 2:31 PM No comments: 

Friday, January 5, 2024

Google Session cookies a proposed mitigation?

In the Cyber Security presentation 4-Jan-2024 the new attack targeting Google session cookie reuse was cited.

Session cookies, if re-validated, allow attackers to logon to Google services without re supplying the password/authentication.

Not Good!

A just proposed mitigation: power cycle the device. A further step, sign-out of any/all browser profiles. Even more secure, reset your passphrase and sign-in again.

Posted by John Jenkinson at 9:47 AM No comments: 

SCCCyber


Thursday, January 18, 2024

Very Very Large password database just released

This slide from the Cyber Security SIG presentation 18-Jan-2024.

- Jan 17, 2024
- Circulating on Internet at least 4 months
- Password dump
 - 319 files totaling 104GB
 - 70,840,771 unique email addresses
 - 427,308 individual HIBP subscribers impacted
 - 65.03 percent of addresses already in HIBP (based on a 1,000 random sample set)
- So, 1/3 never seen before
- Facebook, Roblox, Coinbase, Yammer, Yahoo
- Checked for accuracy
- Passwords Harvested in the Clear!!
- <https://haveibeenpwned.com/>

Have I Been Pwned

Posted by John Jenkinson at 9:52 AM No comments: 

Wednesday, January 17, 2024

Google Chrome 0-day vulnerability 17-Jan-2024

Google released Chrome updates today. CVE-2024-0519.

Updates to Chrome browser are encouraged

Chrome version 120.0.6099.224/225 for Windows.

macOS version 120.0.6099.234

120.0.6099.224 for Linux

ChromeOS 120.0.6099.235

Posted by John Jenkinson at 9:51 PM No comments: 

Friday, January 5, 2024

Google Session cookies a proposed mitigation?

In the Cyber Security presentation 4-Jan-2024 the new attack targeting Google session cookie reuse was cited.

Session cookies, if re-validated, allow attackers to logon to Google services without re supplying the password/authentication.

Cyber Security News

- Jan 17, 2024
- Circulating on Internet at least 4 months
- Password dump
 - 319 files totaling 104GB
 - 70,840,771 unique email addresses
 - 427,308 individual HIBP subscribers impacted
 - 65.03 percent of addresses already in HIBP (based on a 1,000 random sample set)
- So, 1/3 never seen before
- Facebook, Roblox, Coinbase, Yammer, Yahoo
- Checked for accuracy
- Passwords Harvested in the Clear!!
- <https://haveibeenpwned.com/>

Have I Been Pwned

```
1 https://www.trionworlds.com/glyph/register/en [REDACTED]@gmail.com:91215155156lol!↓
2 https://account.wizbii.com/sign-in/email [REDACTED]@gmail.com:Cestmoi1@↓
3 https://casino.bangbet.com.ng/share/df3577b2-fba6-440d-afe2-[REDACTED]/ng_bonus.htmls
4 http://status.szu.edu.cn/szulxs/stuzs/stuLogin.action [REDACTED]@gmail.com:Ichi12022↓
5 https://www.neobux.com/m/1 [REDACTED] CoummosFab0rAc4↓
6 https://new.edmodo.com/student-signup [REDACTED]:_svCiC*fBeSsCz5↓
7 https://id.g2a.com/password/reset/confirm/w4b76sw1lamcufgvdsuxsqfsoqv5ghod[REDACTED]v4f
8 https://rollinscwp.b2clogin.com/rollinscwp.onmicrosoft.com/b2c_1_signup/oauth2/v2.0/auth
9 https://www.videoscribe.co/en/sign-up [REDACTED]@gmail.com:Computacion2021↓
10 https://kiwiirc.com/client [REDACTED]:jasonjason↓
11 https://geozno.dp.ua/cabinet [REDACTED]:xaw1234r↓
12 https://www.gsuplementos.com.br/checkout/aceso [REDACTED]:8524561997pd↓
13 https://www.ebay.co.uk/ws/ebayisapi.dll [REDACTED]:Jeremy02↓
14 https://www.mycommerce.com/vendor-login.html [REDACTED]:yb932062↓
15 https://login.yahoo.com/account/challenge/password [REDACTED]@yahoo.co.id:ryshakA@@00↓
16 https://www.coinbase.com [REDACTED]@hotmail.com:Ioamolol22123↓
17 https://www.facebook.com [REDACTED]@gmail.com:arjuna19↓
18 https://www.roblox.com/newlogin [REDACTED]:kian0208↓
19 https://www.yammer.com/login [REDACTED]@companeo.com:jdc+8173MK↓
20 https://www.racedepartment.com/login/login [REDACTED]@hotmail.com:22667755↓
```

- Assume your password is known
- Enable MFA
- Passkeys
- Hardware tokens
- Password history
- Shared secret
- Public/Private key cryptography
- Private key requires private
- Passkeys biometric access
- Passkeys vendor vaults
- Passkeys private vaults MULTIPLE private vaults
- Recovery codes

Passwords/Passphrases

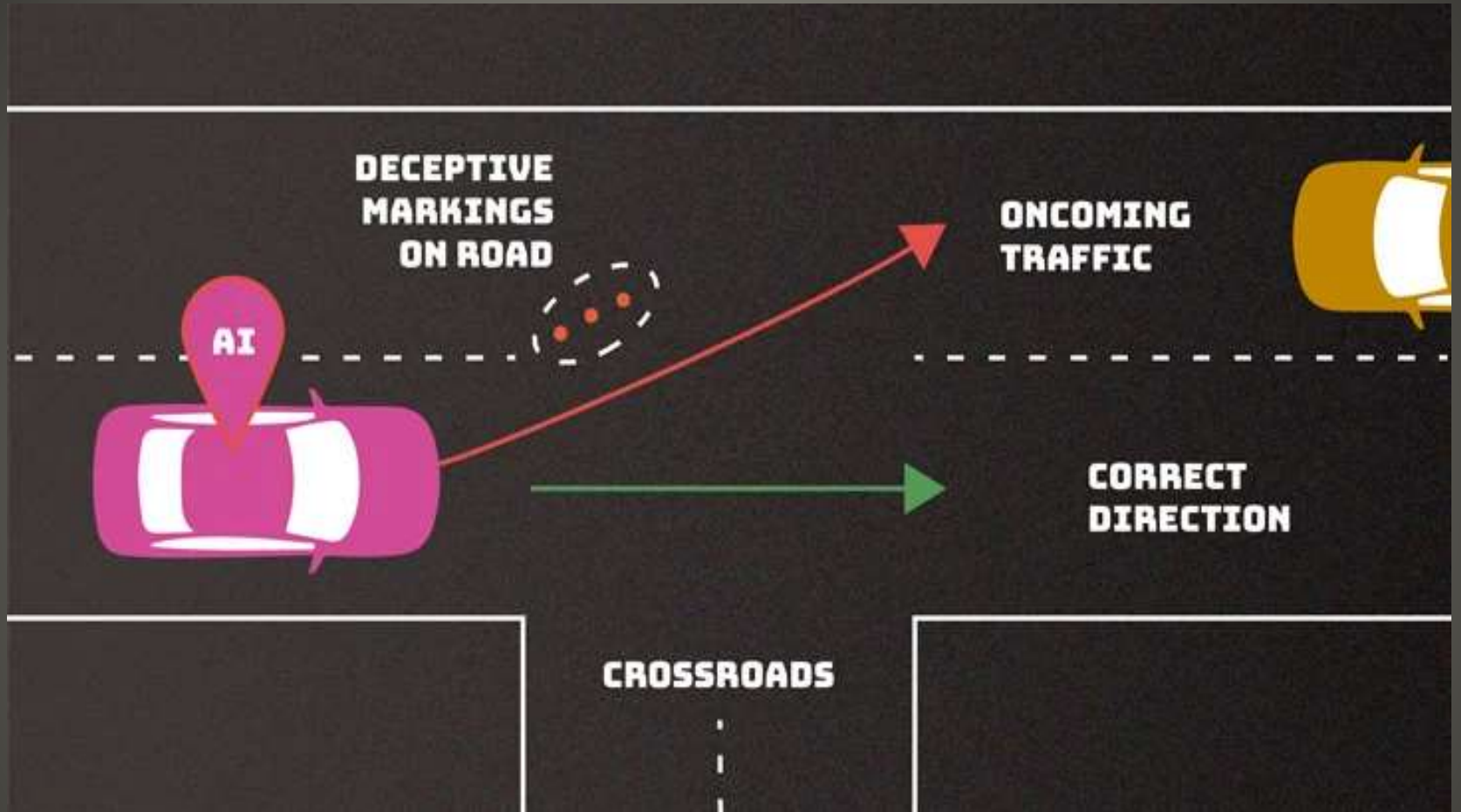
- One of the few communities with our resources
- Available to the home bound, employed, ...
- Inform your friends, neighbors, clubs, ...
- Awareness

- Not One More Resident
scammed
defrauded
impacted
Due to lack of awareness

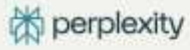
Spread the Word

- Evasion attacks, which aim to generate adversarial output after a model is deployed
- Poisoning attacks, which target the training phase of the algorithm by introducing corrupted data
- Privacy attacks, which aim to glean sensitive information about the system or the data it was trained on by posing questions that circumvent existing guardrails
- Abuse attacks, which aim to compromise legitimate sources of information, such as a web page with incorrect pieces of information, to repurpose the system's intended use

AI threats NIST



Autonomous driving



New Thread **Ctrl** **I**

Q Home

🔍 Discover

📖 Library

👤 Sign In

Sign Up

Where knowledge begins

Ask anything...

☰ Focus 📎 Attach


🔍 Copilot →

→ Try asking 🔥 How high can a kangaroo jump? 📖 Why do birds sing in the morning?
📖 How was the UN formed? 🍜 Ramen toppings Ideas

Try Pro
Upgrade for image upload,
smarter AI, and more
Copilot.
[Learn More](#)

Download ✕ 🗨️
<https://www.perplexity.ai>

[Try Pro](#) [Careers](#) [Playground](#) [Blog](#)

✕

Sign in or create an account

See your history, upload files, and use the latest AI models.

[Continue with Google](#)

[Continue with Apple](#)

[Continue with Email](#)

Perplexity AI

- Answers with links

Why is the sky blue?

Sources

Why Is the Sky Blue?

nasa · 1

Why is the sky blue?

rmg · 2

Why Is the Sky Blue?

scijinks · 3



View 2 more

Answer

The sky appears blue due to a phenomenon called Rayleigh scattering. When sunlight reaches the Earth's atmosphere, it is scattered in all directions by the gases and particles in the air. Blue light is scattered more than other colors because it travels as shorter, smaller waves, making it the most dominant color we see. This is why we see a blue sky most of the time. During sunrise and sunset, the sunlight must travel through a thicker chunk of the atmosphere to reach our eyes, causing the blue light to be scattered completely out of our field of vision, which is why the sky appears red or orange at those times.

Share Rewrite

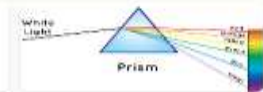


Related

- why does the sky turn red during sunrise and sunset +
- what causes the sky to turn black during a thunderstorm +
- why does the sky turn green during a volcanic eruption +

Ask follow-up...

Copilot



Search Videos



Generate Image



Perplexity AI

- Chinese authorities identify senders
- TLS
- Bluetooth & Wi-Fi
- Device logs
- Rainbow tables
- Public Security
- Case solving, spread of inappropriate remarks, bad influences
- Check each end has each in address book
- Limited in China November 2022
- Everyone limit 10 minutes

Apple Air Drop

- Virtual Desks shelf button

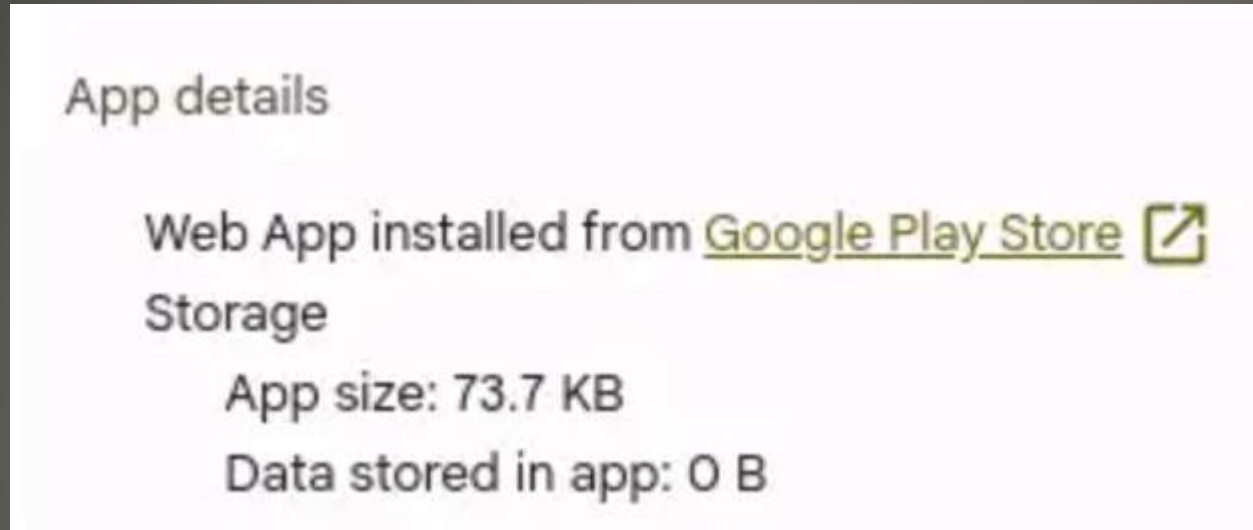


- Self Share via Nearby share



ChromeOS 120

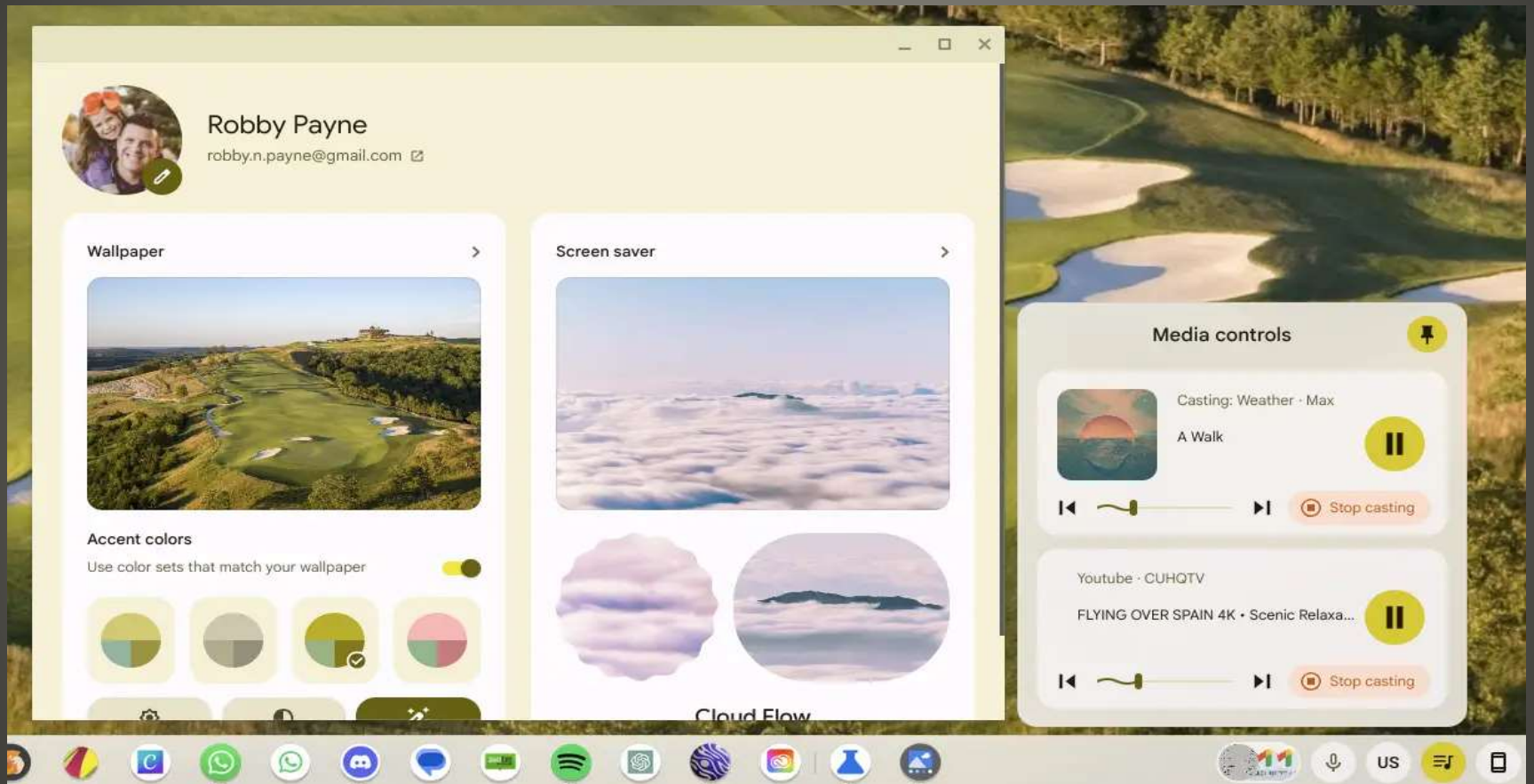
- App details in App Manager



- New keyboard shortcuts and options
- Pinch-zoom for PIP windows

ChromeOS 120

• New Media Controls



ChromeOS 120

- Biometric Identity Fraud
- Anti-Surveillance innovations
- AI tools
- Abundance of face & voice data
- Digital doppelgängers for the masses
- Fashion religious & medical face coverings
- Eye ware lenses to distort

News not

- Possible data leak
- Publicly available data
- Full names, dob, sex, CPF numbers
Cadastro de Pessoas Físicas (CPF)
223 million records

Entire Brazilian population

- 23 terabytes 1 billion Chinese nationals
- Billions of Shanghai police records

And

- Large Action Model
- Rabbit R1
Rabbit OS
Use existing apps




'Hey, first of all, go to a software called Photoshop. Open it. Grab your photos here. Make a lasso on the watermark and click click click click. This is how you remove watermark.'" It takes 30 seconds for Rabbit OS to process and then it can automatically remove all your watermarks going forward.

Rabbit R1

- SEC X (Twitter) account takeover
Bitcoin ETF
Takeover of phone number?
- Apple Magic keyboard firmware update
Bluetooth pairing vulnerability
Firmware update version 2.0.6
Check version
System settings > Bluetooth
"I" icon Magic Keyboard
- NoaBot Linux worm crypto miner
- Google Play Store remove purchases
No notification Paid for Gone
- Google Chrome \$5B incognito mode
- Apple Triangulation – lack of press coverage
- Fingerprints "similar" same person – different fingers
- New secretive court Data Protection Review Court
EU regulatory 8 judges
- Bluetooth flaw iOS, Android, Linux, macOS

Current Issues

 **U.S. Securities and Exchange Commission**  @SECGov · 29m

Today the SEC grants approval for #Bitcoin  ETFs for listing on all registered national securities exchanges.

The approved Bitcoin ETFs will be subject to ongoing surveillance and compliance measures to ensure continued investor protection.



U.S. SECURITIES AND EXCHANGE COMMISSION

Today's approval enhances market transparency and provides investors with efficient access to digital asset investments within a regulated framework.

Chair, Gary Gensler

- Mandiant X account
Team transition (Google purchase)
SMS 2FA
- Know Your Customer checks
AI generated/altered selfies
Passport/State Drivers License photos
- Cert.PL scan Polish websites for flaws
- U.K. Post Office scandal
Screw-up Cover-up
Prosecuting subpostmasters
Then find the flaws in machines

[Report](#)

Current Issues

- US Supreme Court rejects X (Twitter) transparency bid
2014 disclose national security requests
- LoanDepot hack
Mr. Cooper First American Fidelity National Financial
- Stress text hardware security keys [Report](#)

Current Issues

- <https://venturebeat.com/ai/new-study-from-anthropic-exposes-deceptive-sleeper-agents-lurking-in-ais-core/>
- AI SIG
- Copilot Windows 10

AI



Watch as a mouse

- Edge close

System - 3 results

Startup **boost**



Get to browsing quickly. When this is on, it helps Microsoft Edge open faster when you start your device. [Learn more](#)

Startup **boost** is turned off as the current profile is using one or more extensions that are conflicting. Turning on startup **boost** anyway may not work as expected. [Learn more](#)



[Avast Online Security & Privacy](#)

Turn off

Continue running background extensions and apps when Microsoft Edge is closed



Use hardware acceleration when available



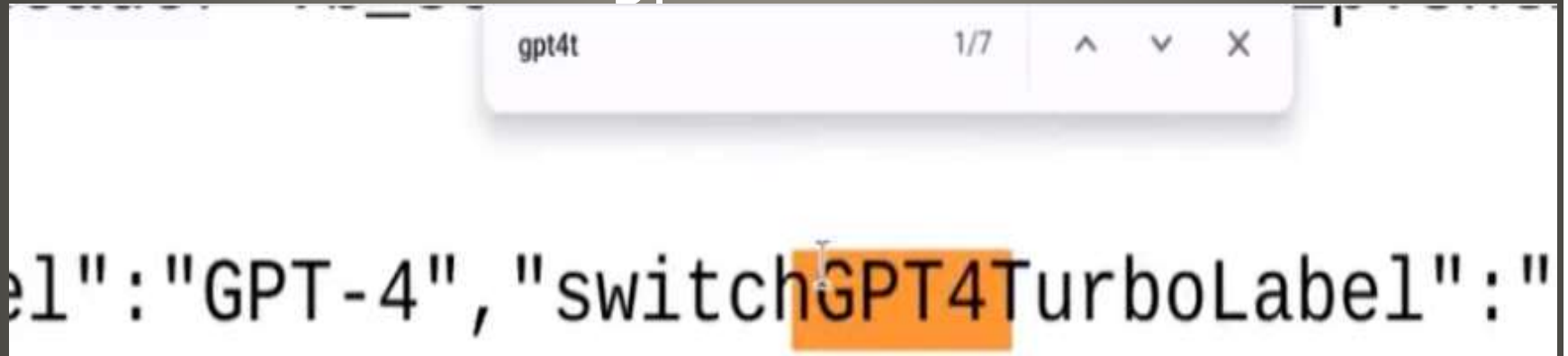
Open your computer's proxy settings



- <https://www.investopedia.com/how-to-freeze-and-unfreeze-your-credit-5075527>

Current Issues

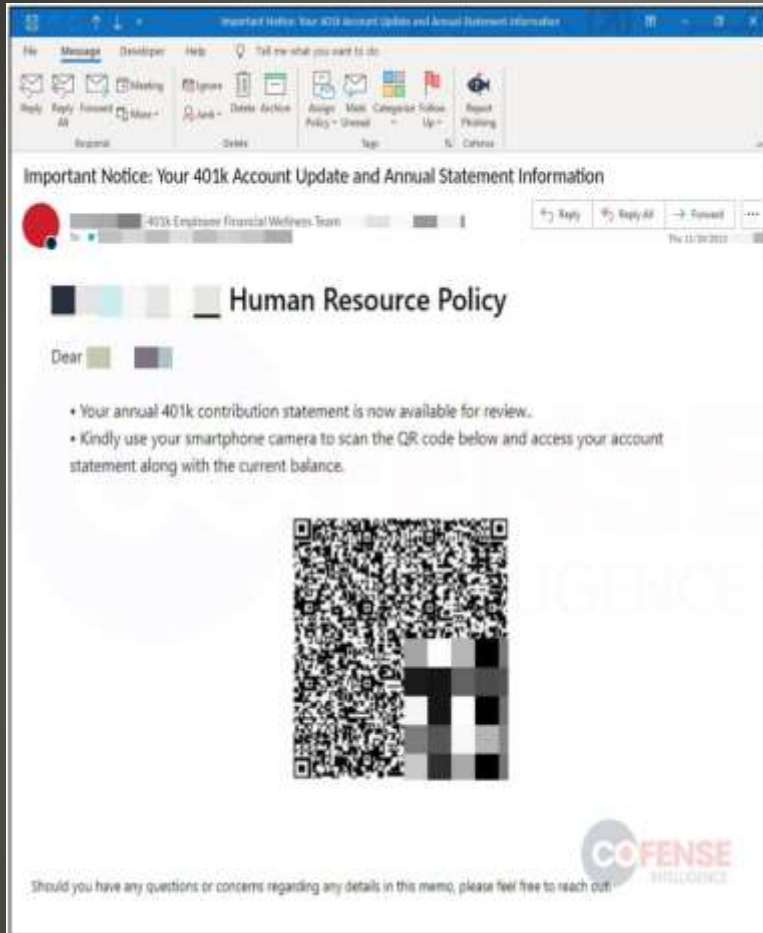
- Copilot.microsoft.com
Ctrl+U display page code
- Ctrl+F search "gpt4t"



The image shows a browser search interface. At the top, there is a search bar with the text "gpt4t" and a "1/7" indicator. Below the search bar, a search result snippet is visible, containing the text: "e1": "GPT-4", "switchGPT4TurboLabel": "

- A \$20/mo value
- On Windows 10 also
- Windows SIG 14-Nov 12-Dec 9-Jan

Copilot Version



Bogus Notices from your company or their partners

- U.S. Cybersecurity and Infrastructure Security Agency
CISA

Known Exploited Vulnerabilities

6 new flaws

CVE-2023-38203 (CVSS score: 9.8) - Adobe ColdFusion Deserialization of Untrusted Data Vulnerability

CVE-2023-29300 (CVSS score: 9.8) - Adobe ColdFusion Deserialization of Untrusted Data Vulnerability

CVE-2023-41990 (CVSS score: 7.8) - Apple Multiple Products Code Execution Vulnerability

CVE-2016-20017 (CVSS score: 9.8) - D-Link DSL-2750B Devices Command Injection Vulnerability

CVE-2023-23752 (CVSS score: 5.3) - Joomla! Improper Access Control Vulnerability

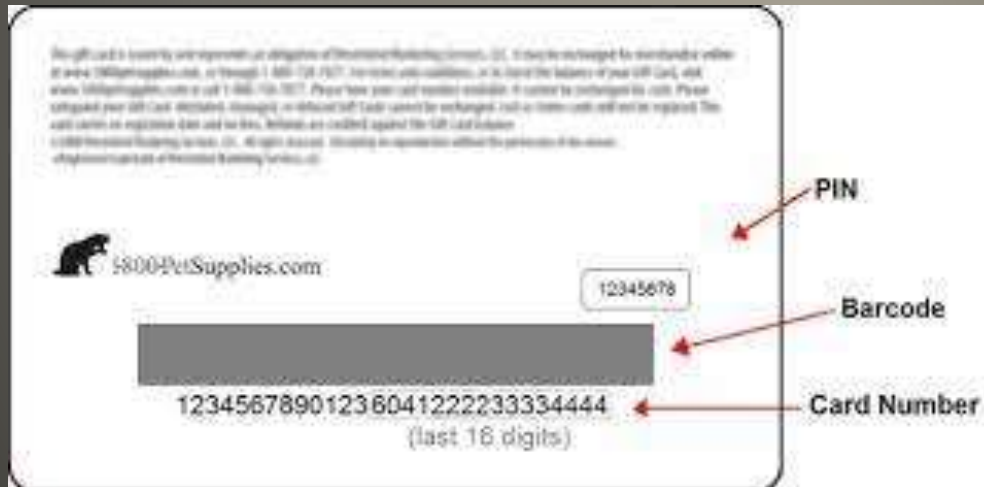
CVE-2023-27524 (CVSS score: 8.9), a high-severity vulnerability impacting the Apache Superset open-source data visualization software

CISA KEV Catalog

- Victim loss \$100,000 sim swap
- Traced value to wallet
- Civil suit Federal court
- Notice to defendant
- Defendant thief or government?
- “meaningful and timely communication”
- Recent notifications via email
- \$100 bitcoin to wallet with OP RETURN
- Recovery via courts not law enforcement
- Romance scams, LastPass, ...
- 2013 loss, 2020 response

Here's some Bitcoin, you've been served

- Physical gift cards
- Online gift cards
- Closed-loop
- Open-loop
- Third-parties involved



Gift Cards

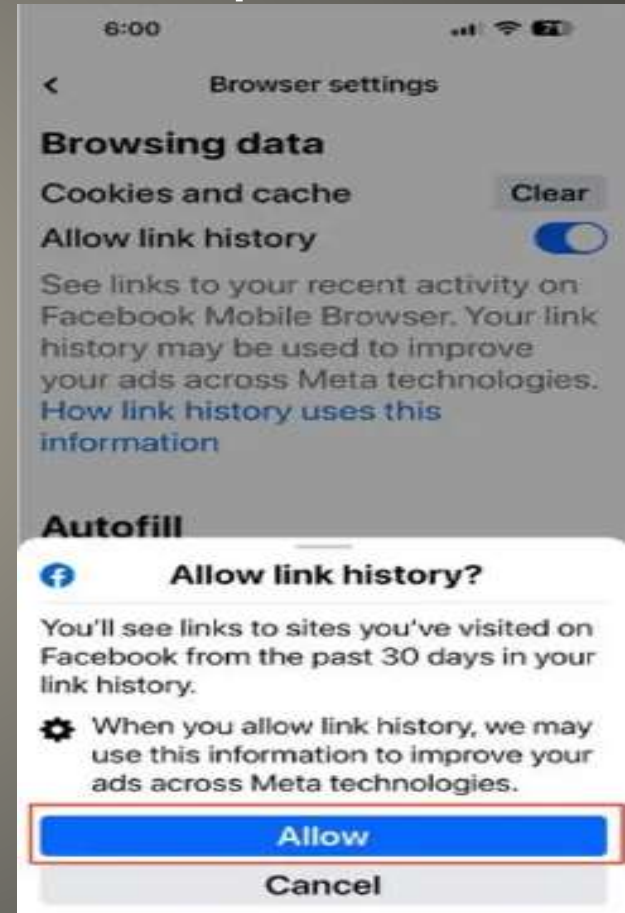
- Expiration date & fees
- Neiman Marcus 1994
- Mobile – phones
- Virtual email/text
- Gift Card collectors
- Social aspects gift exchange
- US jurisdictions limit or prohibit fees
- Value not spent
- Unsecured debt
- Underspend Overspend
- Secondary gift card market
- Brute force card information
- Monitor gift card balance, past & used numbers, ...

Gift Cards

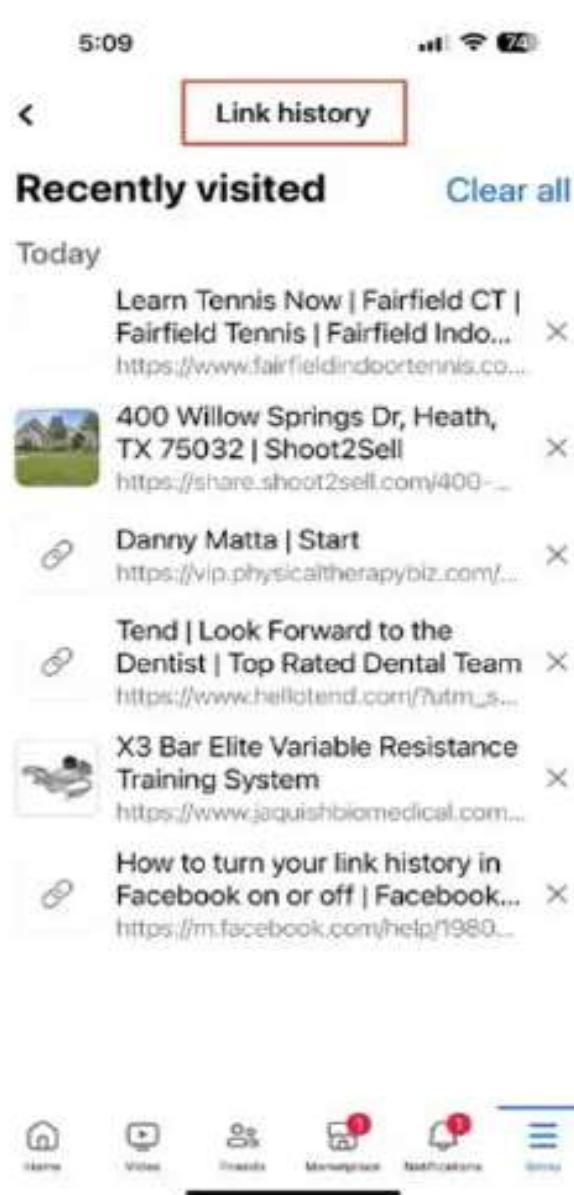
- Seldom blocked by corporate networks
- Familiarity to coders
- No fees
- No domain to maintain
- Reliable
- Little new account vetting
- Living-off-trusted-sites

GitHub

- Facebook App iDevice & Android
- All your browser history in one place
- Facebook Mobile browser
- Off by default
- 30-day history
- Meta tracking



Meta Link History





Social Security



Date: March 03rd, 2023

Case ID: SSA903-138J

Due to fraudulent activity, your Social Security Number (SSN) will be suspended within the next 24 hours.

We are writing to notify you that your Social Security Number is being suspended due to FTC's discovery of illegal activity using your identity in the state of TEXAS.

Your case is referred to the Department of Justice for prosecution under the Criminal Code Act 1950, and other criminal offenses in the state of TX, including the Proceeds of Crime Act 2002 for:

1. Count 1 (Drug Trafficking Act 2008 Section 2)
2. Count 2 (Money Laundering Act of 1996)
3. Count 3 (Theft by deception Texas Business Court Code conduct 1986)

As of today, we have received a legal charge against you. In accordance with our standard operating procedures, law enforcement agencies have uncovered 25 bank accounts that were opened using your Social Security number to perpetrate a \$14 million fraud. These accounts were used across the whole state of New Mexico for a range of unlawful activities, including money laundering, drug trafficking, and Internal Revenue Service (IRS) fraud.

The Department attempted to serve legal process at your most recent known address, but US Marshals who paid a visit found the house deserted.

If you've received this by email, it's because we've exhausted all other means of contacting you. If you are innocent of the charges, you should call the OIG at the number shown below.

To plead yourself, you can contact the Office of Inspector General (Social Security Administration) at 1-888-909-7667.

Ka. Pouton



PEABODY MA 01960-3511

Date: August 30, 2021

The Social Security Administration would like to inform you that there will be an increase of \$240.10 to your monthly benefits due to an increase in the cost of living. Please go ahead and give us a call at [REDACTED] to start receiving this increase immediately.

If you don't wish to receive this increase, instructions on how to unenroll from these payments will be available by end of September.

Regards,

Commissioner Of Social Security

[Signature]

FAKED DOCUMENT

- Data sold Dark Web did not pay ransom
- Multi-extortion strategy
- 74 organizations
- Living-off-the-land
- Media-savvy Media team
- Ransomware against ransomware

Medusa Ransomware

- SEC
- Mandiant
- X formerly Twitter change to MFA with SMS
- Organizations team change

X Formerly Twitter **Account**

- Peer-to-Peer payment service
- Registered in 32 states
- "revolutionize 2024"
- Elon Musk PayPal co-founder

X as Everything App

- Actively exploited
- JSON Web token
- CVE-2023-24955

CISA

Critical Microsoft SharePoint Bug

- Chinese manufactured drones
- Use in US Critical Infrastructure
- Capture data

CISA & FBI Warning

- And Android streamers
- Hijacked to use in botnet
- 170,000 bots
- Malicious site browsing Smartphone
Push app to SmartTV
- Botnet & cyber crime
- Political & terrorist broadcasts
- AI generated video broadcasts
- Register seized DNS domains
- Then they Attack Back

Android Based SmartTVs

- Critical RCE Juniper SRX firewalls & EX switches
- Lithium metal ion battery research
 - More efficient, more affordable, more recyclability, more cycles, less explodey
- LG washing machine



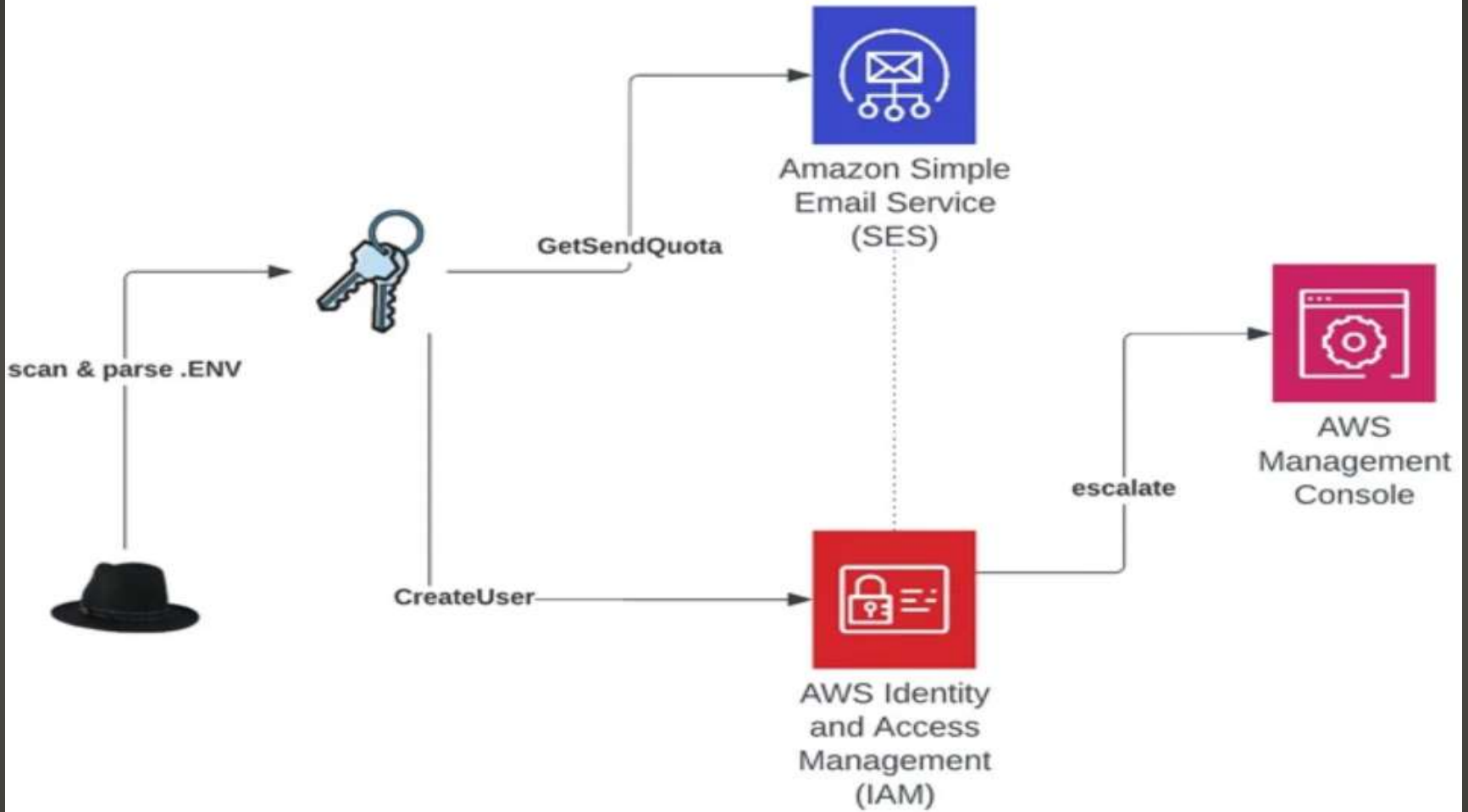
Current Issues

- GitLab zero-click account hijack vulnerability
Community & Enterprise editions
CVE-2023-7028 Critical 10/10
- Chrome API low impact claim
Re constitute authentication cookies
- Cerabyte low cost, high resilient storage
unlimited lifespan Ceramic nanolayers
- YouTube vs Ad Blockers – scam ads
Adblock Adblock Plus version 1.1.2
- Danish energy organizations cyber attacks
May 11 May 22-31 Zyxel firewall
- Samsung Galaxy January security patches
Android 11 – 14
- Wine bottle scams
- British Library – not paying ransom
Readers PII
- Google email rules next month – bulk mailers

Current Issues

- X-Mode banned – selling phone location data
FTC first of its kind fail to place safeguards
location data from Muslim prayer apps, ...
Apple & Google banned in earlier days
FTC action
- NSA director – AI helping/hurting critical infrastructure
- SonicWall Firewalls exposures 178,000
CVE-2022-22274 9.4
CVE-2023-0656 7.5
- US tops list access Origin Wukong quantum computer
- Equifax data breach settlement
2017 140 million customers claim deadline passed
Apply compensation for expenses
- Secret Service – fake antivirus renewal subscription emails
- PixieFail vulnerabilities PXE boot
- CISA & FBI warning
AndroxGh0st malware
Credential stealing Azure, AWS, Twilio, Office 365, ...

Current Issues



AndroXGh0st

- Character.AI

Historical figures

Helpers

Assistants

Fun & games

- Splash

Song based on your input

- Volley Games

20 question game


- AWS AI for developers

Alexa AI skills

- EU popup

Inbox ★

Choose your ads layout



We and 772 third parties process data to: store and/or access information on your device, develop and improve products, personalise ads and content, measure ads and content, derive audience insights, obtain precise geolocation data, and identify users through device scanning. Some third parties may process your data on the basis of their legitimate interest. You may exercise your right to consent or object at any time by selecting the Manage preferences link below, or through Outlook settings. By clicking the Accept all button, you agree to the use of these technologies and the processing of your data for these purposes while using Outlook. [Privacy Statement](#)

Manage preferences Reject all Accept all

Banner Mailbox (Recommended)

Microsoft Outlook App

- The agreement allows these entities to do the following:
- Store and/or access information on the user's device.
- Develop and improve products
- Personalize ads and content
- Measure ads and content
- Derive audience insights
- Obtain precise geolocation data
- Identify users through device scanning

Microsoft Outlook App

- View list of advertising partners
- Toggle for each advertising partner

Microsoft Outlook App

• Mail Telemetry

- Name and contact data
- Passwords
- Demographic data
- Payment data
- Subscription and licensing data
- Search queries
- Device and usage data
- Error reports and performance data
- Voice data
- Text, inking, and typing data
- Images
- Location data
- Content
- Feedback and ratings
- Traffic data

Microsoft Outlook App

- Yeah, Mac too
- Synch with Gmail, Yahoo, etc.
- Passwords required Plain text
- Proton Report

Microsoft Outlook App

- Copilot for
- MAC, Linux, Android, iDevices
- Useful Creepy

Microsoft

- Businesses Copilot Windows 365
- Removed 300-seat minimum
- Copilot Pro – consumers \$20/mo
- Per User Family Plan

	For Individuals		For Organizations
	Copilot	Copilot Pro	Copilot for Microsoft 365
	Free	\$20	\$30
Foundational Capabilities	•	•	•
Web Grounding	•	•	•
Commercial Data Protection	•	•	•
Priority Model Access		•	•
Copilot in Outlook, Word, Excel, PowerPoint, and OneNote		•	•
Copilot in Teams			•
Microsoft Graph Grounding			•
Enterprise-Grade Data Protection			•
Customization		Copilot GPT Builder	Copilot Studio

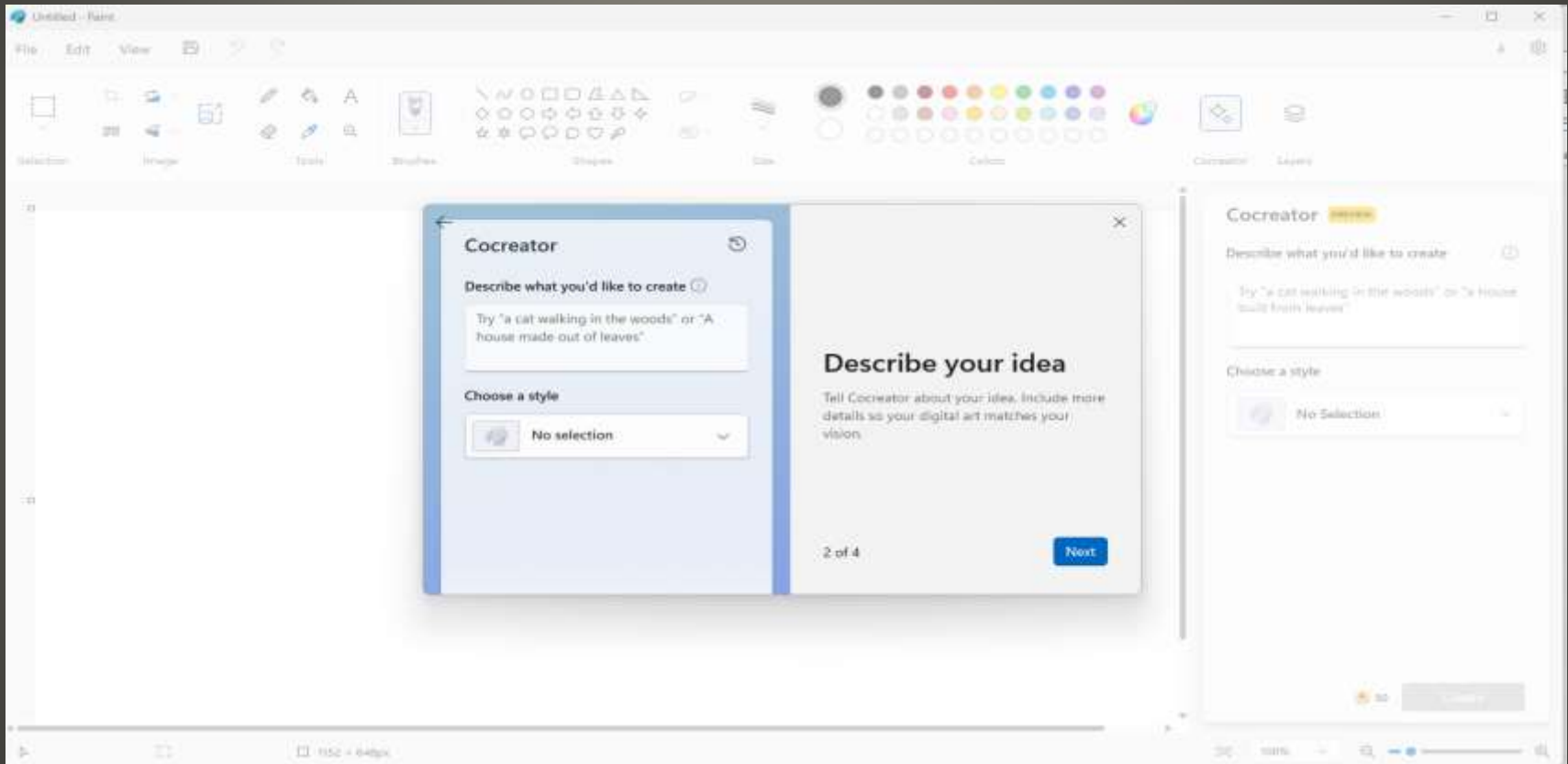
For Copilot Pro, access to Copilot in Word, Excel, PowerPoint, Outlook, and OneNote requires a Microsoft 365 Personal or Family subscription. Commercial Data Protection applies when users are signed into their work account using their organization's Entra ID.

Microsoft Copilot

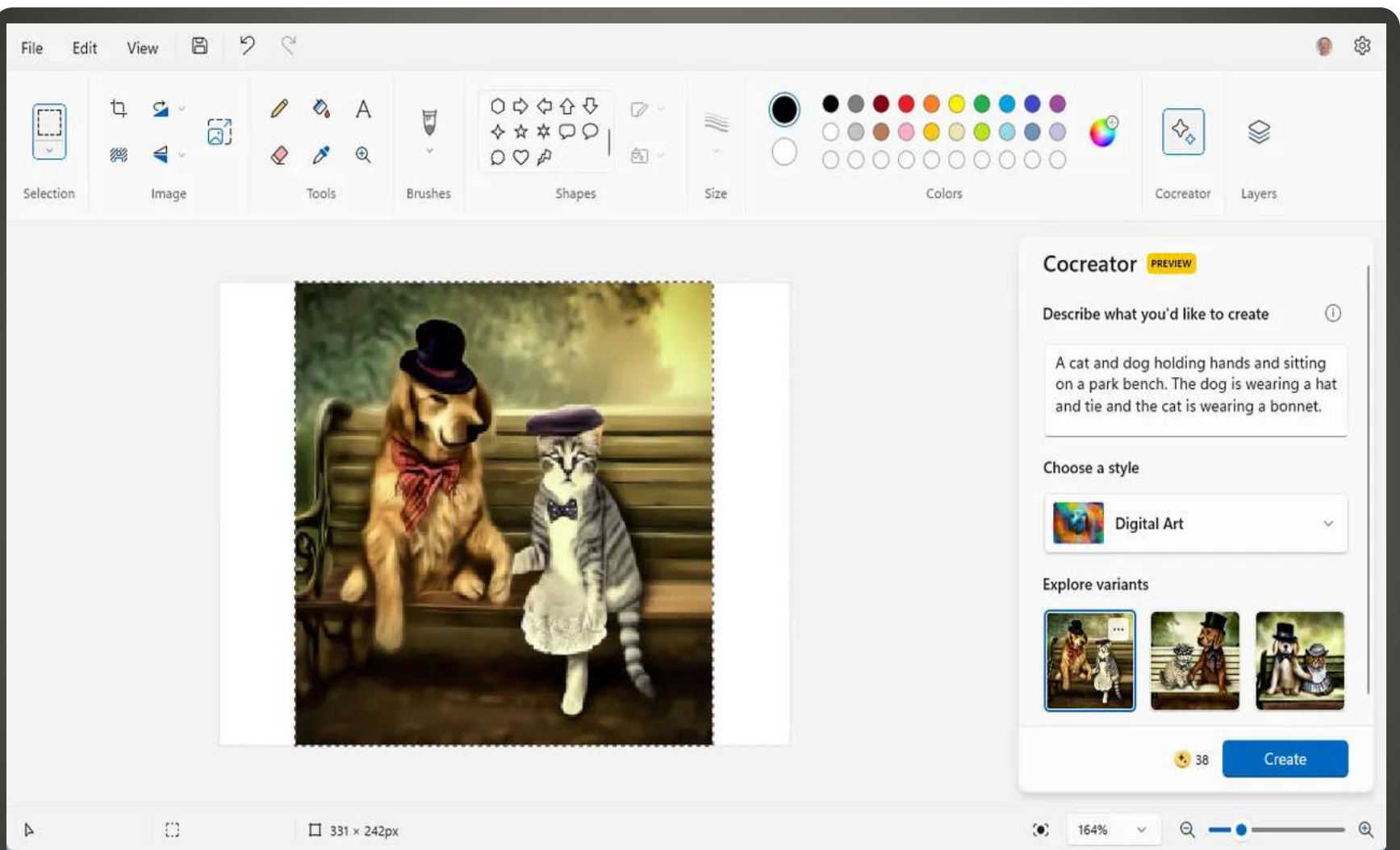
- Windows 11 Paint

About Paint

Paint 11.2311.29.0



AI Image Creation



Microsoft Paint AI Image creation

- Uber chief security officer
Convicted Federal court
- SolarWinds security chief charged
- New regulation
materially impactful data breach
4 business days public 8-K filing
Hackers call out victim company
- Remote work – more documentation

SEC CISO

- Brave ads for Brave products

Brave & similar

6:16

51%

 Assistant

Hi!
I'm **Assistant**
with Bard. I can
help you be
more creative
and productive.

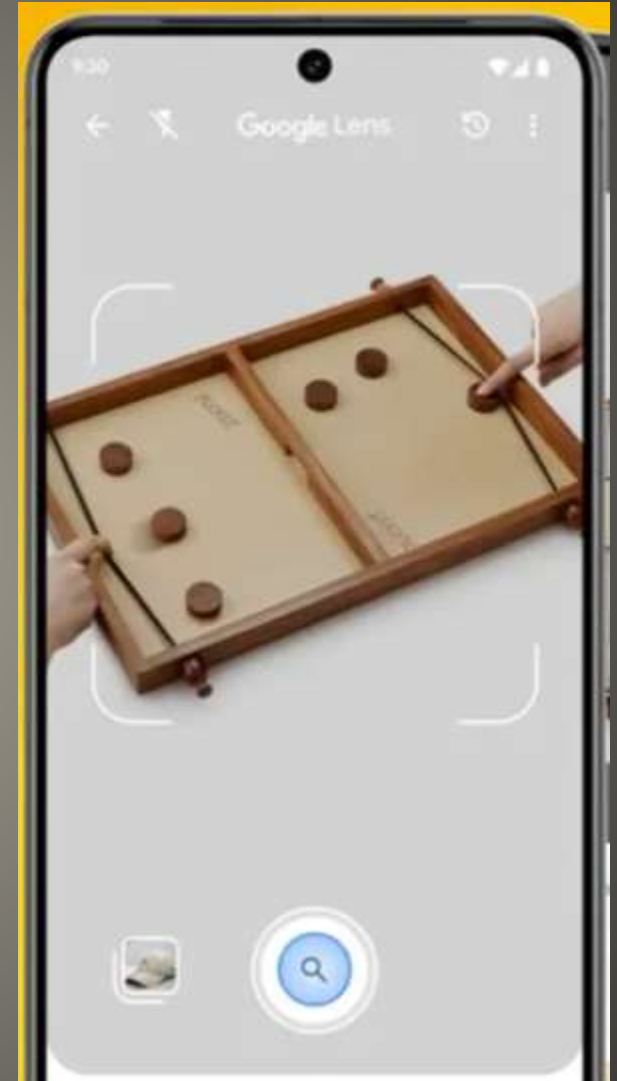
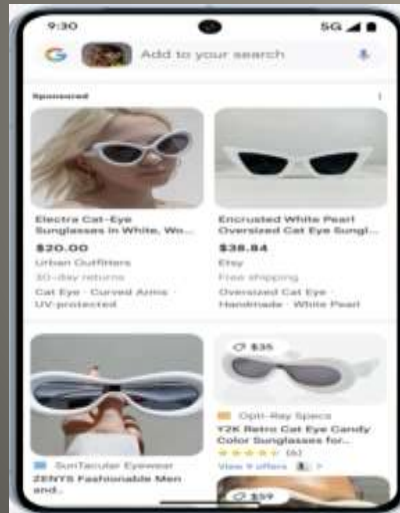
Get started

 Bard

Hi!
I'm **Bard**, a new
experimental AI
assistant on your
phone.
I can help you
write, plan,
learn, and more.

Get started

- Picture red shoes
Add "Blue"
- What is this game,
How is it played?
- Circle to search



Google Lens

- 45 billion attempts per day
- Double last years
- \$15B/year 62,000 technologists
- “more than Google or Amazon”
- Why?

“The fraudsters get smarter, savvier, quicker, more devious and more mischievous.”

- Russia sanctions, AI, Political climate
- Who pays that cost?

JPMorgan Chase Cyber battle

- Attempt to decouple Advertising & Privacy

- Chromium engine

Topics API Protected Audience API Attribution Reporting API

Related Website Sets API Private State Tokens API

Attribution Reporting API Shared Storage API CHIPS API

Fenced Frames API Federated Credential Management API

- TOPICS Protected Audience API

On-device ad auctions to serve remarketing and custom audiences, without cross-site third-party tracking.

Google Privacy Sandbox

- Short Message Service
cellular network
160-character limit
- Multimedia Message Service
image and video
Low limit -> compression
- Rich Communications Service
Wi-Fi and/or cellular
HD, read receipts, location sharing, group chat
- iMessage features Apple <-> Apple Blue bubbles
Apple <-> Android Green bubbles
Apple "Want blue?, buy iPhone"
iMessage has all RCS features
- EU regulations, customer demands
iMessage core service Digital Markets Act
- So, iMessage for Android -or- RCS for iPhone

SMS MMS RCS

- Galaxy S24 event
- New smartphones
- Galaxy AI
 - Live translate
 - Interpreter
 - Chat Assist
 - Note Assist
 - Transcript Assist
- Circle to Search
- 7 years of Software Updates
- Galaxy Ring

Samsung

- Intelligence is finite and has upper bound
- Calculators
- Easy -> less learned
- HUGE energy expense

- EMP

AI

- Recovery Seminar
- <https://vimeo.com/882272974?share=copy>
- NOW, Your input, experiences, ...

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com