

# Sun City Computer Club

Cyber Security SIG  
November 16, 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**

- Recent Club Event
- *Foundations of Scam and Fraud Prevention*  
<https://vimeo.com/883616696?share=copy>
- Former FBI and CIA director PSA  
<https://youtu.be/BNIPQvdRf1E>
- Questions & Concerns

Do Not Answer – Contacts SIM Swap Stolen Phone

Gift Card Numbers gift card sell online

F12

Lock icon

Multiple CC Bank accounts eMail Browsers Identities

Bank routing numbers Checks Informed Delivery

Credit Card requirements & fees

Mobile Banking

# Scams

- Several recordings

<https://vimeo.com/832429457?share=copy>

<https://vimeo.com/804336768?share=copy>

- Only answer if in Contacts

Contacts smart device stolen Safer

- Prepare Now

Inventory

Digital Life

Multi Factor Authentication methods Multiple phone numbers

Recovery Methods

AppleID

3-2-1 Backup Encryption

Paper

Play like your phone can not be used for authentication

Device only password manager

Authenticator app

Loss, damaged, stolen

My smart device is locked down very well Helpful <-> Harmful

Backup to device (PC MAC Linux Chromebook) backup that device

Find My Wipe My

Share location Helpful <-> Harmful

Web based password Manager

Password reset procedures

Passcode

Inventory, Document, Test

# Smart Devices

# Privacy Badger      uBlock Origin

- Conflict?
- Privacy Badger 9 blocks
- uBlock Origin 10 blocks
- Datadoghq-browser-agent  
Collects events & metrics  
Sends to Datadog  
You can monitor  
Anyone can monitor?  
Data collected value  
Sold?



A screenshot of the Privacy Badger extension interface. It displays a list of domains with corresponding progress bars indicating their privacy status. The domains and their status are:

| Domain                        | Status           |
|-------------------------------|------------------|
| js-cdn.music.apple.com        | Blocked (Yellow) |
| amp-api.podcasts.apple.com    | Blocked (Yellow) |
| embed.podcasts.apple.com      | Blocked (Yellow) |
| www.apple.com                 | Blocked (Yellow) |
| static.cloudflareinsights.com | Blocked (Red)    |
| www.googletagmanager.com      | Blocked (Yellow) |
| fonts.gstatic.com             | Blocked (Yellow) |
| open.spotify.com              | Blocked (Red)    |
| www.tiktok.com                | Blocked (Red)    |

## Browser Extensions

- November 14
- Copilot to Windows 10

**Microsoft Patch Tuesday**

- iOS 17
- Bluetooth low energy alerts
- Flipper Zero
  - sub-1GHz, RFID, NFC, infrared, Bluetooth
- \$160

**Flipper Zero can crash iPhones**

- Russia reshipping service  
SWAT USA Drop exposed  
1200 US residents exposed  
Work from home  
until first payday  
Large stolen merchandise laundering  
Hacked and exposed  
Reship expensive consumer goods  
Sold on black markets  
Stolen credit card information  
Rival service steals and publishes site's data

**SWAT USA Drop**

https://swatship.club/stuffer/rules.php

1 BTC = 533117 Hello, [username]

Total paid: [amount]  
Total packages: [amount]  
My drops: [amount]  
Balance: [amount]

Request payment

Packages  
Archive  
News  
Stuff list  
Rules of service  
Couriers  
Mail  
Profile  
Дополнение баланса

### Rules of service

ПРАВИЛА

RULES EGN

By sending stuff to our couriers you automatically agree to the rules below. No complaints are accepted. Ignorance of the rules is not an excuse!  
Couriers' statuses:  
NEW / TEST- The courier successfully passed the interview and signed a contract. (Packages that go to such couriers are not compensated, claims are not accepted)

READY- Actively working courier. (If the courier loses the delivered package or if courier cheats, we offer a compensation or forwarding the package for approximately the same cost, provided that the courier did not die due to a call from the shop or the police.)

GOING TO DIE- Automatic status that includes all couriers 5 days before the end of the term of work. (Compensation for lost stuff with these couriers is not provided)

PROBLEM - any kind of problems, see description

SUSPICIOUS - did not go into the panel for more than 2 days or there are some other problems. Compensation is not provided, it is better to wait for the working status.

DELAYING - the courier receives this status when he delays sending packages. Do not send to these couriers. Wait for the working status.

Rules of service  
Payment is made when courier ships the package. (Package receives status "ship") Compensation: 10% of the cost of the item or shipping of similar item. The service has the right to refuse cooperation without explanation. Before ordering anything, check the stuff list in the administration panel or coordinate the product with the support if there is no such a product in the stuff list. Inconsistent / non-list item is not paid or

https://swatship.club/stuffer/widgets.php/widget=usps ebay for selling

- Privacy Notice
- "Acts of God" exemption

# SWAT USA Drop

|                               |   |   |         |              |     |             |   |
|-------------------------------|---|---|---------|--------------|-----|-------------|---|
| <input type="checkbox"/> 3866 | <div style="background-color: #f0f0f0; padding: 2px;">[Redacted]</div> (United States)<br>Time: 11:01 AM<br><div style="background-color: #f0f0f0; padding: 2px;">New package</div> | <div style="background-color: #f0f0f0; padding: 2px;">[Redacted]</div> CHICAGO IL , 60628, United States <div style="background-color: #f0f0f0; padding: 2px;">[Redacted]</div>    | 0/0/0/3 | Going to die | all | Nov-04-2023 | <div style="background-color: #f0f0f0; padding: 2px;">Notes</div> |
| <input type="checkbox"/> 3936 | <div style="background-color: #f0f0f0; padding: 2px;">[Redacted]</div> (United States)<br>Time: 11:01 AM<br><div style="background-color: #f0f0f0; padding: 2px;">New package</div> | <div style="background-color: #f0f0f0; padding: 2px;">[Redacted]</div> CHICAGO IL , 60620, United States <div style="background-color: #f0f0f0; padding: 2px;">[Redacted]</div>    | 0/0/0/2 | Ready        | all | Nov-06-2023 | <div style="background-color: #f0f0f0; padding: 2px;">Notes</div> |
| <input type="checkbox"/> 4054 | <div style="background-color: #f0f0f0; padding: 2px;">[Redacted]</div> (United States)<br>Time: 11:01 AM<br><div style="background-color: #f0f0f0; padding: 2px;">New package</div> | <div style="background-color: #f0f0f0; padding: 2px;">[Redacted]</div> CHICAGO IL , 60616, United States <div style="background-color: #f0f0f0; padding: 2px;">[Redacted]</div>  | 0/0/0/5 | Ready        | all | Nov-10-2023 | <div style="background-color: #f0f0f0; padding: 2px;">Notes</div> |

- You too can signup
- NOT ADVISED
- a LOT of personal information required  
With proof DL and/or Passport image
- Large number of similar sites
- Allows non-payment to mules
- Average cost per CC victim \$1,156.93
- 1.6 million credit cards
- \$1.8 billion in losses

**SWAT USA Drop**

- USPS Informed Delivery
  - Register first
  - Publicly available information to register
  - USPS has scanned images of all US Mail
  - Notifications to users
  - Unencrypted email
    - email stored on users device(s)
  - Web site
- The Clearing House
  - Manual human error
  - November 1-3
  - Chase, Bank of America, Wells Fargo

## **Current Issues**

- Privacy Search  
Private Information Retrieval  
Cryptography
- Personal assistant search result poisoning
- Okta single employee  
Personal device & email account
- Google to remove millions of Gmail accounts
- Tutanota mail > Tuta
- Signal Phone Number -> Usernames
- WhatsApp "protect IP Address in calls"
- Microsoft Authenticator "risky" notifications
- Zhefengle ecommerce store  
Millions of citizens data exposed
- GPT detect tool
- Microsoft temporarily blocks employee's ChatGPT access

## Current Issues

- Cyberattack world's biggest bank  
China ICBC  
Disruption of treasury markets  
USB stick and bicycle  
What If?
- Australia shipping port  
Nationally significant cyber attack
- SysAid 0-day flaw used in ransomware  
IT Services management platform  
Data theft
- CVSS Common Vulnerability Scoring System  
Version 4

## Current Issues

Confidential email from [REDACTED]

Yahoo/Inbox ☆



[REDACTED]@tutanota.com [REDACTED]



Wed, Nov 8 at 11:53 AM ☆

To: j [REDACTED] m

Hello,

You have just received a confidential email via Tutanota (<https://tuta.com>). Tutanota encrypts emails automatically end-to-end, including all attachments. You can reach your encrypted mailbox and also reply with an encrypted email with the following link:

[Show encrypted email](#)

Or paste this link into your browser:

<https://mail.tutanota.com/#mail/M3x290n----2CZ0xCfxRRY8XL13B5G3tAg>

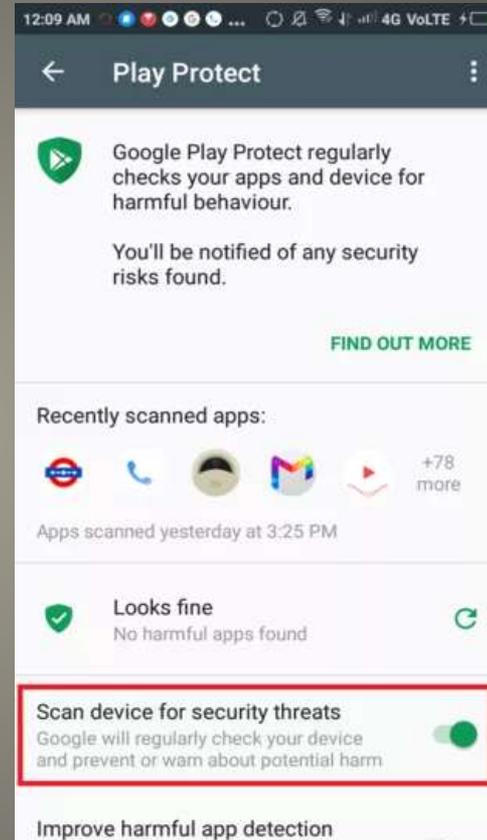
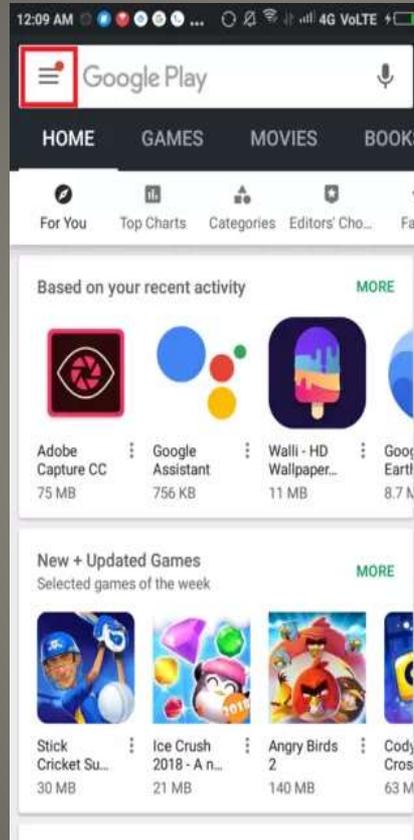
This email was automatically generated for sending the link. The link stays valid until you receive a new confidential email from me.

Kind regards,

[REDACTED]

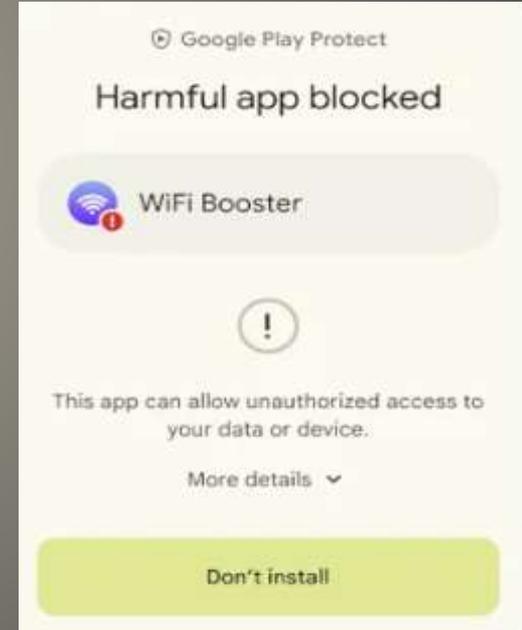
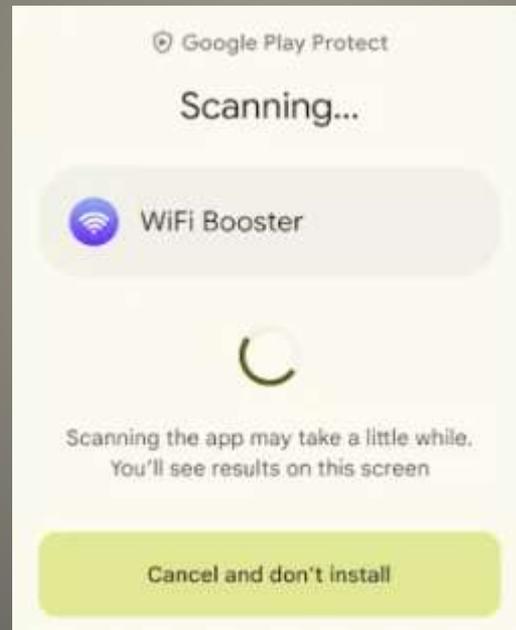
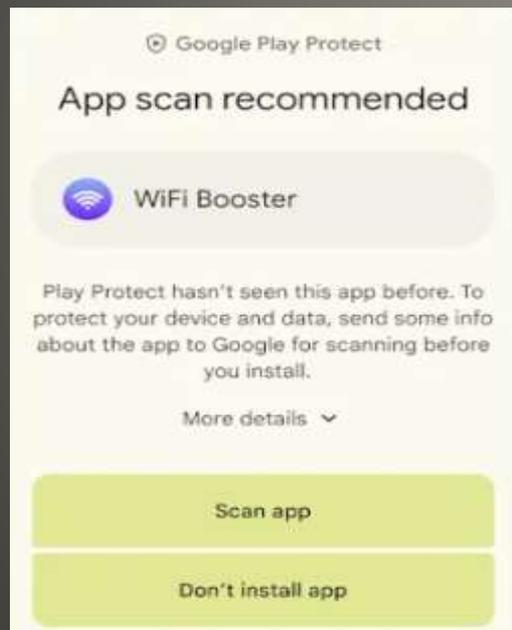
# Tuta mail

# • Google Play Protect



# Google Play Protect

- Sideloaded
- Morph appearance
- Use AI to cloak
- Predatory loan apps



# Google Play Protect



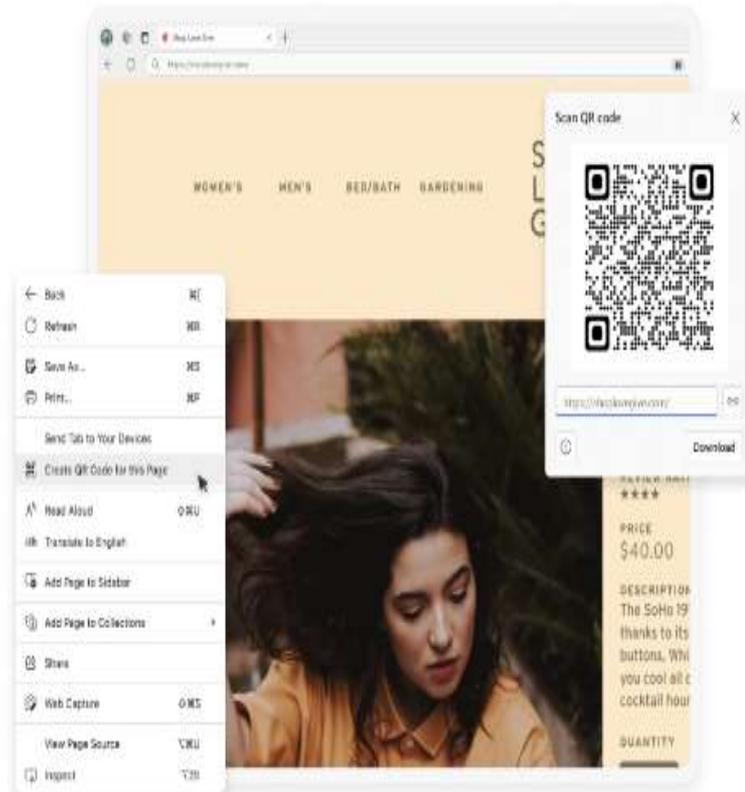
NEW

# Create a QR code for any webpage in seconds

Share your webpage with others using a unique QR code. To generate the QR code, open your webpage in Microsoft Edge, right-click on the page and choose **Create QR code for this page**.

[Learn more](#)

Next



 Here's what's new in Microsoft Edge

▼ QR code

Search the web



- Duke University researchers  
Thousands of records of US military  
Members and veterans  
Families, acquaintances  
Full names, physical & email addresses  
Health and financial information  
Ethnicity, religious practices, political affiliation  
Own or rent  
Married? Children?  
Children's sex and age  
45,000 records  
\$0.12 to \$0.32 per record  
5,000 friends & family  
1.5 million records \$0.01

<https://www.axios.com/2023/11/06/military-data-sold-for-cents-cheap-privacy>

- Atlassian Confluence - mass exploitation
- Entire state of Maine resident's data stolen  
MOVEit

## Current Issues

- Add to all Maine residents
  - Louisiana Department of Motor Vehicles
  - Colorado Department of Health Care Policy
  - Oregon Department of Transportation
- British Columbia search & rescue
  - Hikers following non-existent trail
  - Google Maps Removed Nov 6
- Stolen Boeing data leaked – ransom non-payment
- NSA warning Chinese hackers in US critical infrastructure
- Ethereum address poisoning
  - Two step forward first test transfer abscond with second
- Amazon replaces Android on Echo Show Fire TV?

## Current Issues

- Truepill / Postmeds data breach  
2.3 million persons data
- Google Titan Security Keys  
Passkeys storage
- Hackers snitch to SEC Meridian Link  
digital solutions for banks, credit unions, ...
- Bangladesh agency  
National Telecommunications Monitoring Center  
Data collection Extensive data collection  
Published unsecured database  
Then stolen by hackers

## Current Issues

- Pause / Wait
- Search
- Num Lock
- Caps Lock
- Keyboard battery
- Microsoft Account?
  - Recover your account page
- Local Account?
  - Security Questions?
  - Reset password
  - PIN? Forgot just PIN Key icon



**Windows access forgotten password**

- Use Computer Club Help Center
- Linux tools

**Windows access forgotten password**

██████████ • Facebook

## Trust frequently used devices

Any devices you've frequently used Facebook on in the past 2 years will be automatically trusted.

If other people have access to any of your devices, it's best to opt out of this by Nov 12.

Trust frequently used devices



Opt out



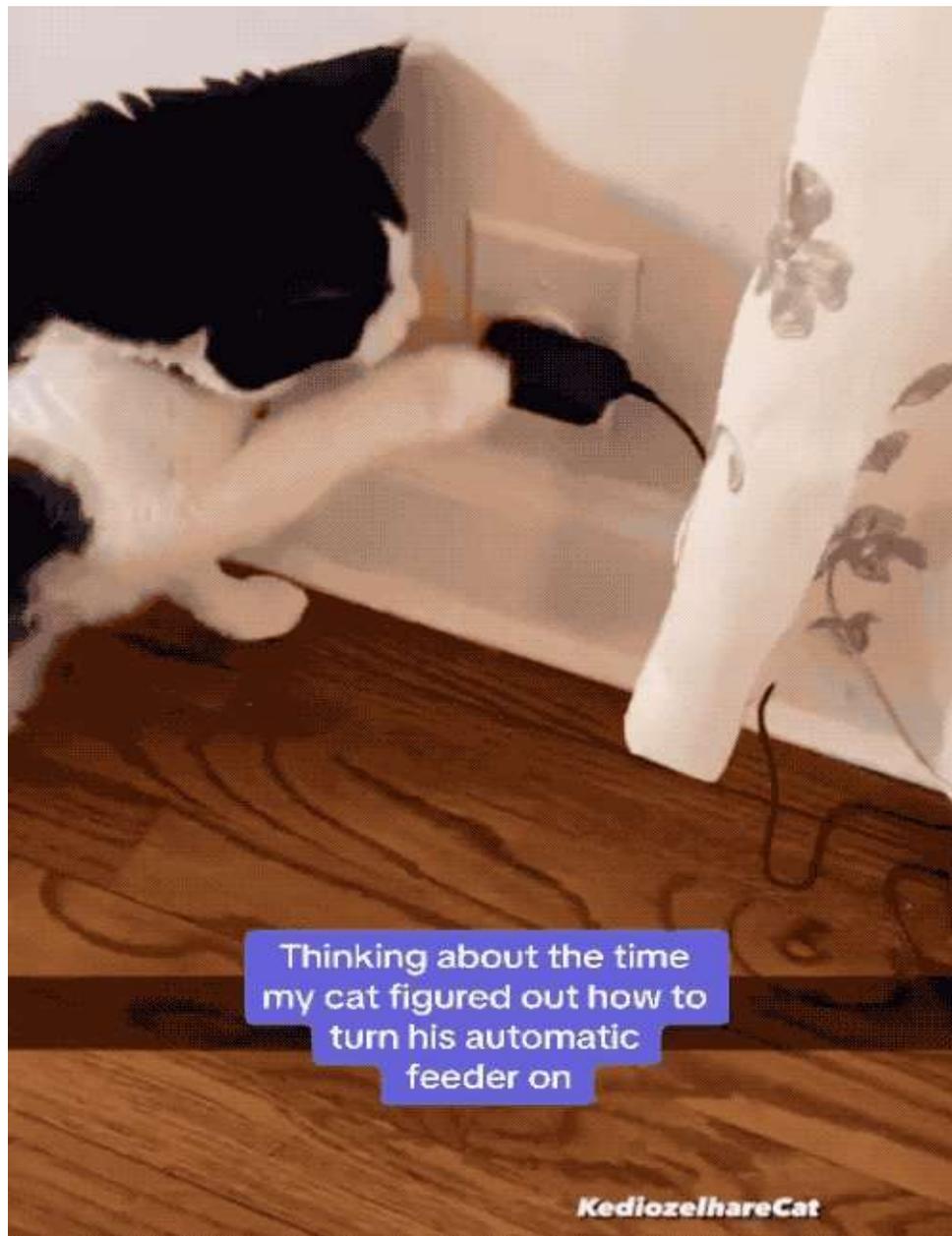
**Facebook (Meta) MFA Opt-out**

- Anyone can become You at Experian
- Summer 2022 reported
- Vulnerability still exists
- Account take over?
- Re create account
- ALL personal information
- Account re-created
- Notification to old email address
- BUT credentials have changed
- PIN changed recovery questions changed
- Only option re-takeover your account
- MFA to account takeover's phone number
- Account still frozen? Or Re-frozen?

**Experian**

- 2022: Class Action Targets Experian Over Account Security
- 2017: Experian Site Can Give Anyone Your Credit Freeze PIN
- 2015: Experian Breach Affects 15 Million Customers
- 2015: Experian Breach Tied to NY-NJ ID Theft Ring
- 2015: At Experian, Security Attrition Amid Acquisitions
- 2015: Experian Hit With Class Action Over ID Theft Service
- 2014: Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records
- 2013: Experian Sold Consumer Data to ID Theft Service
  
- SEC suit

**Experian**



Thinking about the time  
my cat figured out how to  
turn his automatic  
feeder on

**KediozelhareCat**



## Ed Gerck, PhD, PhD

Founder Planalto Research, Chief Scientist, ZSentry architect.

+ Follow

View full profile



## Ed Gerck, PhD, PhD • 3rd+

Founder Planalto Research, Chief Scientist, ...  
2d • Edited •

+ Follow ...

Today, we could announce it. Quantum computing (QC) has become a reality. We broke the RSA -2048 key. Ron Rivest is a dear friend, but that was needed to advance.

The QC version used here has simultaneous multiple-states logic (following 'all states at once'), with more than a googol of possible states.

We show that the equivalence of QC techniques (with IBM, Google and others compared with our version of QC) has been hidden for about 2,500 years – since Pythagoras.

All our QC computations were done in a commercial cellphone, or a commercial Linux desktop, as our QC devices -- opening the user market to many industries. No cryogenics or special materials were used.

A post-quantum, HIPAA compliant, end-to-end, patent-free, export-free, secure online solution, is being created, based on ZSentry as used from 2004 to 2014, to replace RSA. One needs a quantum-resistant algorithm, because all existing public-key encryption can be broken.

The U.S. NIST needs to deprecate RSA today! Otherwise, SNDL continues.

- Bugs
- Improved performance

**Apple Pause on development**

- Advance security engineering

**Microsoft Secure Future Initiative**

- Really Bad
- Widely user
- Hard to patch

**Cisco & Citrix**

- For illegal activity
- Make you anonymous
- Free just as good as paid
- Speeds up Internet connection
- Bypass geo-restrictions
- Complex to use
- Protections from malware

## VPN Myths

- Almost paperless
- Refund Tracker
- Improved phone assistance
- Reopening Taxpayer Assistance Centers

**IRS Tax 2023**

- Bard suit scammers fake Bard download

*Google AI, AIGoogle, AiGoogle, AIGooglePlus, AIGoogleBard FB  
And others*

- Google Ads network

Fake Windows News

Trojan CPU-Z

RedLine Stealer

- Gmail mass delete December 1, 2023

**Google**

- EU political regulation drama
- Crypto Money software few understand
- [iotaseed.io](https://iotaseed.io) generate seed phrases guess what happened
- Downfall Intel CPU vulnerability
  - Intel 6th generation – Intel 11th generation
  - microcode update up to 50% performance hit
  - speculative code execution
- OpenVPN security Updates - no problem in Russia

## Current Issues



**Windshield Barnacle**

- Law enforcement
- To remove
  - Pay fine & Pay device deposit
  - Remove device
  - Return device to regain deposit
- GPS detects movement
- Traffic boot requires 2 visits
- Jeep vehicle with folding windshield

## **Windshield Barnacle**

I finally realized it!



People are prisoners  
of their phones.  
That's Why they are  
called cell phones!

- Danish Cybersecurity details attacks  
Critical Infrastructure May, 2023  
“What, we need to monitor & update?”

**Current Issues**

**Artificial Intelligence  
Machine Learning  
Large Language Models**

- OpenAI pauses new ChatGPT Plus Subscriptions
- EU political regulation drama
- Crypto Money software few understand
- [iotaseed.io](https://iotaseed.io) generate seed phrases guess what happened
- Downfall Intel CPU vulnerability  
Intel 6<sup>th</sup> generation – Intel 11<sup>th</sup> generation  
microcode update up to 50% performance hit  
speculative code execution
- OpenVPN security Updates - no problem in Russia

## Current Issues

- Two Chatbots playing 20 questions
- Not playing by rules
- Apology

**ChatBots playing 20 Questions**

- OpenAI DevDay
- GPT-4 Turbo
- 100 million weekly visitors
- April 2023
- Limit 3,000 words -> 300 pages
- DALL-E 3
- Text to Speech 6 voices
- Personalized chatbot builder
- Open AI App store
- All tools in one place
- Copyright shield

**ChatGPT**



### Announcing Grok!

Grok is an AI modeled after the Hitchhiker's Guide to the Galaxy, so intended to answer almost anything and, far harder, even suggest what questions to ask!

Grok is designed to answer questions with a bit of wit and has a rebellious streak, so please don't use it if you hate humor!

A unique and fundamental advantage of Grok is that it has real-time knowledge of the world via the X platform. It will also answer spicy questions that are rejected by most other AI systems.

Grok is still a very early beta product – the best we could do with 2 months of training – so expect it to improve rapidly with each passing week with your help.

Thank you,  
the xAI Team

[x.ai](https://x.ai)

3:51 PM · Nov 5, 2023 · 40.8M Views

# Elon's Grok

- AI Completely changes how we use computers
- <https://www.gatesnotes.com/AI-agents>

**Bill Gates**

- Anonymous and secure AI chatbot
- Leo
- Brave browser 1.60
- Built into Brave Browser
- Chats Not used for training
- Noone can view chats

**Brave**

## Table of Contents

### BROWSER

# Try Brave Leo on desktop

Introducing Brave Leo, the smart AI assistant built right into the browser. Whether you're looking for information, trying to solve a problem, or asking for video transcripts or interactive article summaries, Leo can help.

Chats in Leo aren't used for training purposes, and no one can review your conversations. With Leo, you get a seamless AI experience *and* unparalleled privacy.

Ready to try Leo? Just start typing in the Brave address bar and choose "ask Leo" from the suggestions. Or open the sidebar and click

- Anonymous and secure AI chatbot
- Leo
- Brave browser 1.60
- Built into Brave Browser
- Chats Not used for training
- Noone can view chats
- speedreader
  - remove nonessential elements
- Block cookie consent notices
  - `brave://settings/shields/filters`
  - EasyList-Cookie List*

**Brave**

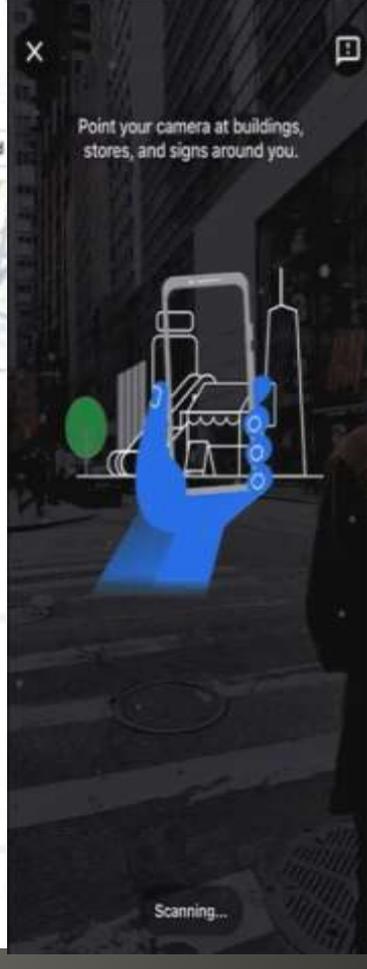
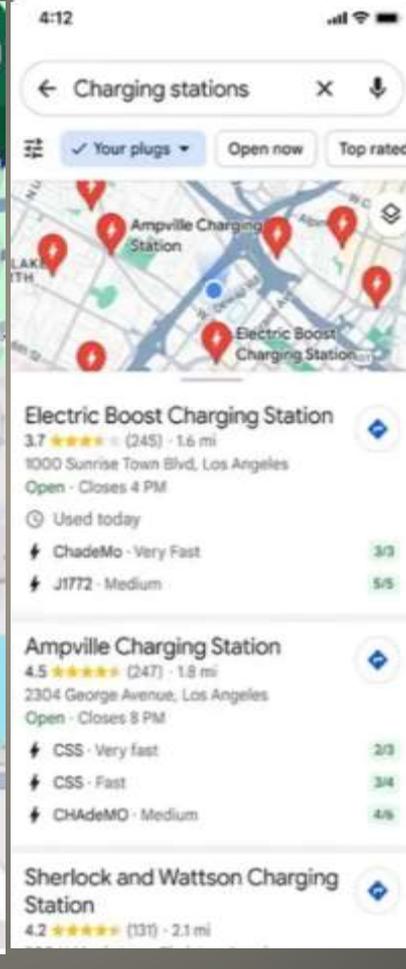
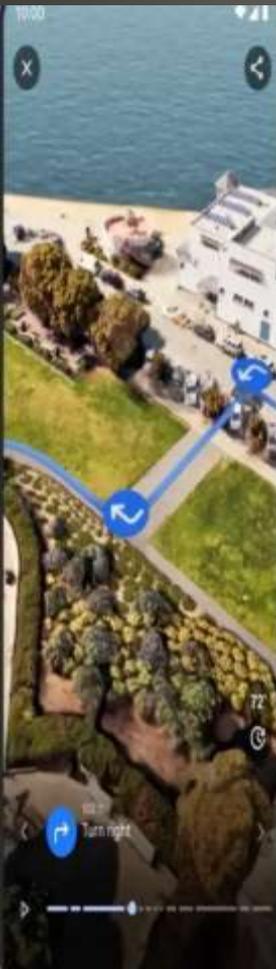
Immersive

Search

Navigation

EV station

AR



Google Maps

- Generative AI Foundations
- <https://www.youtube.com/playlist?list=PLhr1KZpdzukf-xb0lmiU3G89GJXaDbAIF>
- Introduction to Artificial Intelligence
- <https://explore.skillbuilder.aws/learn/course/external/view/elearning/1423/introduction-to-artificial-intelligence>
- Introduction to Machine Learning
- <https://explore.skillbuilder.aws/learn/course/external/view/elearning/11322/introduction-to-machine-learning-art-of-the-possible>
- Introduction to Generative AI
- <https://explore.skillbuilder.aws/learn/course/external/view/elearning/17176/introduction-to-generative-ai-art-of-the-possible>

**Amazon Free AI training**

- Generative AI for Executives
- <https://explore.skillbuilder.aws/learn/course/external/view/elearning/16666/generative-ai-for-executives>
- AWS DeepRacer (hands-on learning lab)
- <https://aws.amazon.com/deepracer/>
- Amazon Machine Learning University
- <https://aws.amazon.com/machine-learning/mlu/>
- Amazon CodeWhisperer – Getting Started
- <https://explore.skillbuilder.aws/learn/course/external/view/elearning/16405/amazon-codewhisperer-getting-started>
- Amazon Bedrock – Getting Started
- <https://explore.skillbuilder.aws/learn/course/external/view/elearning/17508/amazon-bedrock-getting-started>

## Amazon Free AI Training

- AWS Power Hour Intro Machine Learning for Developers
- <https://explore.skillbuilder.aws/learn/course/external/view/elearning/1854/twitch-series-aws-power-hour-introduction-to-machine-learning-for-developers>
- Generative AI with Large Language Models
- <https://www.coursera.org/learn/generative-ai-with-llms?>

**Amazon Free AI Training**

- Super Intelligent
- Artificial General Intelligence (AGI)
- Resources

**OpenAI GPT-5**



DEFEND TODAY, SECURE TOMORROW



Today, CISA released its [Roadmap for Artificial Intelligence](#)—in alignment with [White House Executive Order 14110: Safe, Secure, And Trustworthy Development and Use of Artificial Intelligence](#)—to outline a comprehensive set of actions CISA will take along five lines of effort:

1. Responsibly use AI to support our mission.
2. Assure AI systems.
3. Protect critical infrastructure from malicious use of AI.
4. Collaborate and communicate on key AI efforts with the interagency, international partners, and the public.
5. Expand AI expertise in our workforce.

Learn more about CISA's Roadmap for Artificial Intelligence at [cisa.gov/AI](https://cisa.gov/AI).

# CISA AI Roadmap

- \$700 + \$24/mo
- Apps -> Agents
- Docs app to read/write/edit docs
- Mail app to read/send/edit email
- Agents “Just do it, you (agent) figure out how”
- Cloud



**Humane AI Pin**

- 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**