Sun City Computer Club

Cyber Security SIG
December 21, 2023

Questions, Comments, Suggestions welcomed at any time

Even Now

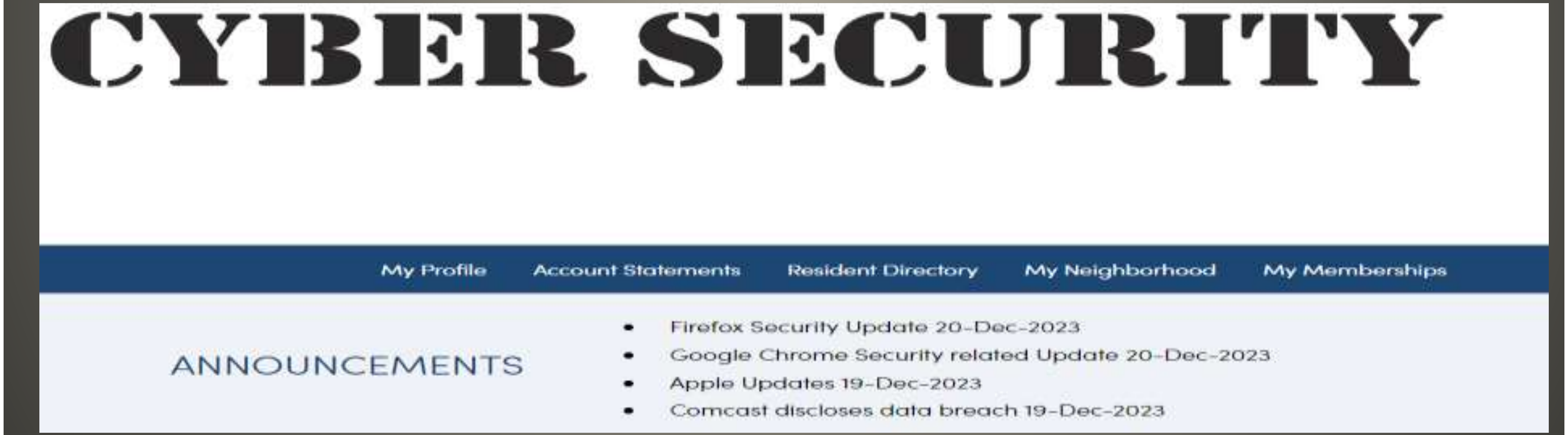
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

- Apple-commissioned Study MIT
- 2.6 billion personal records data breaches
- Apple Study PDF
- Apple Advanced Data Protection for iCloud
- End-to-End encryption
- Beeper
- Blue bubbles Green bubbles

- Computer club resources
- Cyber Security SIG, News blog, Vimeo recordings
- Scams and Computer Safety Vimeo recordings
- Facebook SCTX Computer Club Group, Sun City I
- Computer Club Wiki
- Computer Club Announcements
- SIG Announcements



ANNOUNCEMENTS

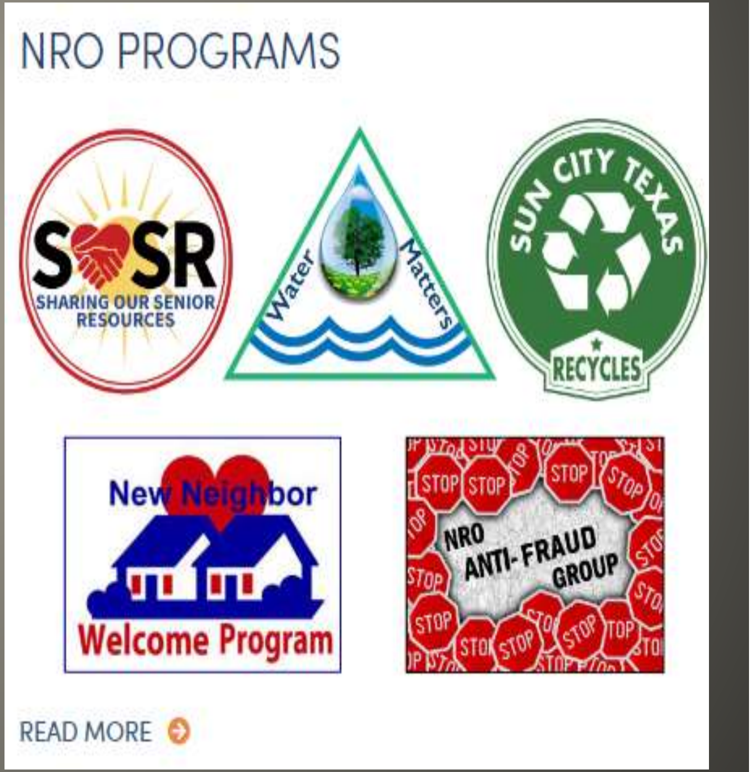
- Firefox Security Update 20-Dec-2023
- Google Chrome Security related Update 20-Dec-2023
- Apple Updates 19-Dec-2023
- Comcast discloses data breach 19-Dec-2023

Pause

- Not One More Sun City Resident
- Awareness, Preparedness, Understanding
- Consider:

  Spread the word

- NRO Anti-Fraud Group



NRO PROGRAMS

READ MORE

Pause

- HAVE YOU BEEN SCAMMED? TELL WILLIAMSON COUNTY DEPUTY SHERIFF DETECTIVE AND U.S. SECRET SERVICE TASK OFFICER SCOTT DUBIELAK ABOUT IT IN PERSON!

- The NRO's Anti-Fraud Group is delighted to announce a new, convenient way for SC residents to report scams and fraud to law enforcement.

- Williamson County Sheriff Mike Gleason has graciously agreed to allow Deputy Sheriff Detective and Task Force Officer Scott Dubielak to join us in SC once a month to take reports of scams and frauds directly from residents. Deputy Sheriff Dubielak will be available to discuss fraud schemes that took place in the last five years, even if you were not a victim or are not sure whether you were a victim. Also, as a Task Force Officer with the U.S. Secret Service, Deputy Sheriff Dubielak has the power to accept criminal complaints even if the criminals are located outside of Williamson County.

- Deputy Sheriff Dubielak plans to be at the Activities Center (1 Texas Drive) and available to meet with SC residents the first Wednesday of each month from 9:00 AM to noon, beginning Wednesday, January 3, 2024. No appointment is necessary. Although the Anti-Fraud Group does not have law enforcement powers, members of the Anti-Fraud Group will also be available to answer questions.

- Deputy Sheriff Dubielak specializes in fraud investigations. In addition to being a Wilco Deputy Sheriff and Detective and U.S. Secret Service Task Force Officer, he is a Certified Fraud Examiner and a Certified Financial Crime Investigator.

- Please note that it is often important to report a fraud or scam to law enforcement promptly, and we encourage residents to do so. By reporting an incident to the police or other authorities promptly, you may increase the chance that law enforcement will be able to catch the perpetrator, and you may help prevent others from being scammed.

- Also please understand that Deputy Sheriff Dubielak will be taking reports of scams and frauds, but not of other types of crimes.

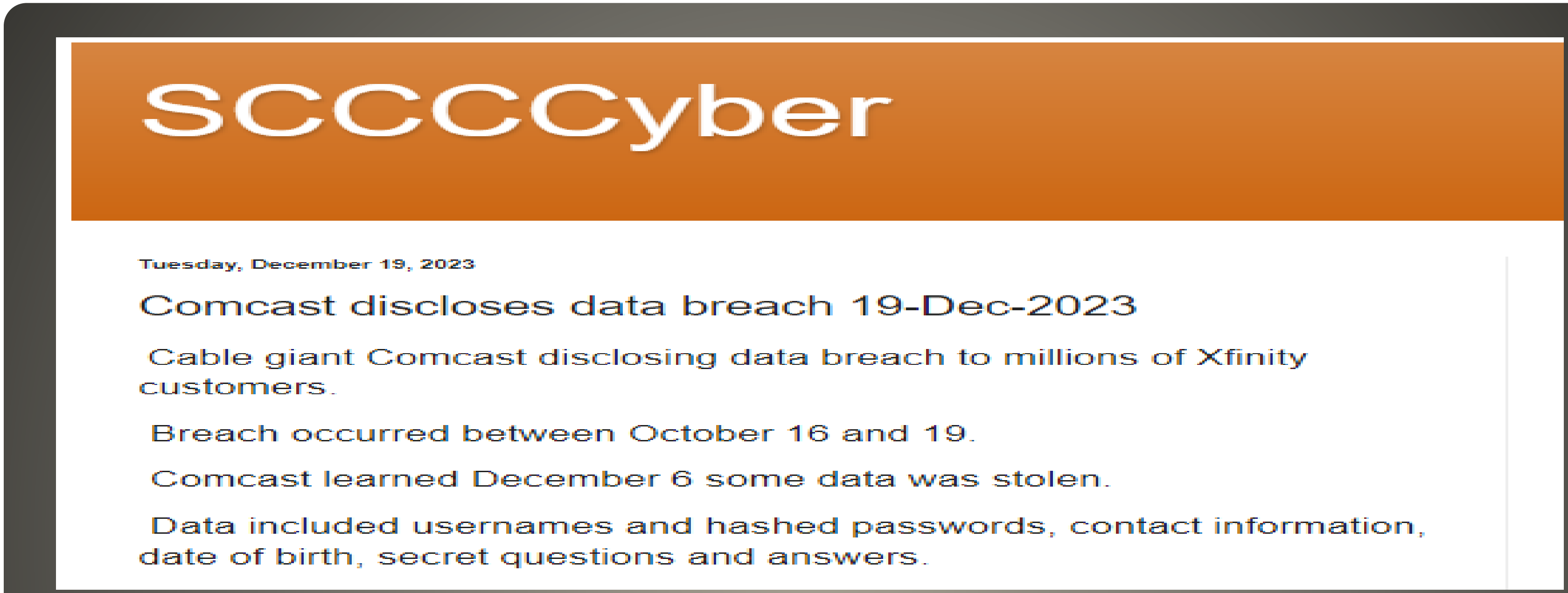
- In related news, the Anti-Fraud Group will hold its 2nd annual Elder Fraud Town Hall in the ballroom the morning of May 6, 2024. Please make a note in your calendar and watch for additional information about this Town Hall.

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

- Zoom Session?

  Ability to provide input anonymously

PAUSE



SCCCyber

Tuesday, December 19, 2023

Comcast discloses data breach 19-Dec-2023

Cable giant Comcast disclosing data breach to millions of Xfinity customers.

Breach occurred between October 16 and 19.

Comcast learned December 6 some data was stolen.

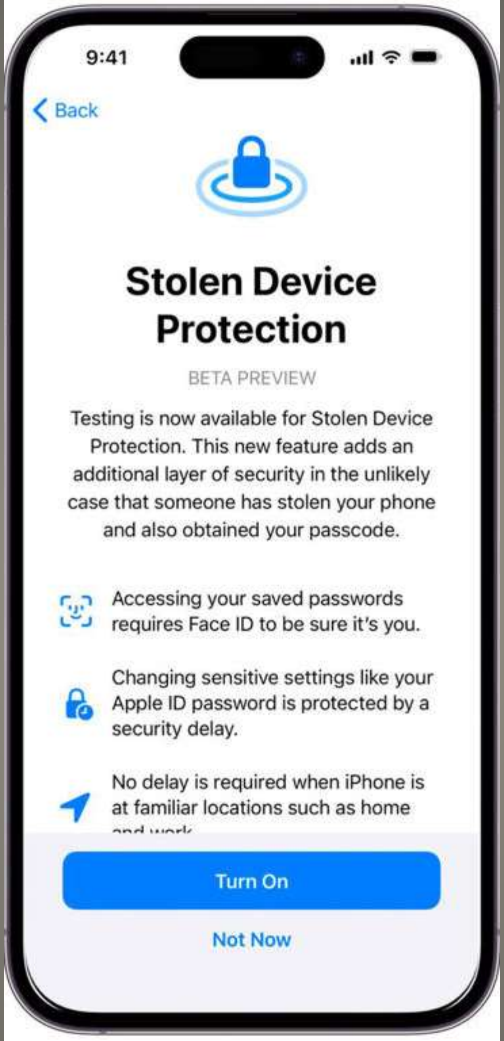
Data included usernames and hashed passwords, contact information, date of birth, secret questions and answers.

- Cell carrier forcing root CA
- Current customers notified 60 days later
- Prior customers
- Credential stuffing
- Credit monitoring breach?
- Leverage contact trusts - your safer, your contacts safer?

Comcast Xfinity

- Stolen Device Protection setting
- Beta

Apple iDevices



Stolen Device Protection

BETA PREVIEW

Testing is now available for Stolen Device Protection. This new feature adds an additional layer of security in the unlikely case that someone has stolen your phone and also obtained your passcode.

Accessing your saved passwords requires Face ID to be sure it's you.

Changing sensitive settings like your Apple ID password is protected by a security delay.

No delay is required when iPhone is at familiar locations such as home and work

Apple Stolen Device Protection

- Opt-in
- 4 to 6 digits   Face ID Touch ID fallback
- Stolen iDevice unlocked
- Restrict certain settings when NOT in familiar location
- Thefts often reset settings in known locations
  Or can find and visit known locations

- Stolen Device Protection enabled
  Turn off Stolen Device Protection
  Change AppleID password
  Recovery Code
  Trusted Phone number

Face ID or Touch ID
Hour wait
Face ID or Touch ID

Apple Stolen Device Protection

Apple Stolen Device Protection

- Keychain access Biometrics only

- Apps can be accessed
- Apple Pay can be used

- Protect passcode
- Custom Alphanumeric code
- Custom iDevice lock
- MFA for apps

- Binance DOJ settlement
  Entire database access for DOJ
- St Andrews University UK
  Banned email niceties
  Exposed Russia state actors
  "I hope this finds you well"
- Ring employees spy on videos
  Now limited circumstances
- Sierra Wireless cellular routers
  Un patchable vulnerabilities
- US federal agencies missed cyber requirements deadlines
  GAO report
- 246 *known* ransomware incidents K-12 this year
- Ukraine main mobile network cyber attack
  Russia claims credit   Ukraine – servers & data NOT destroyed

Current Issues

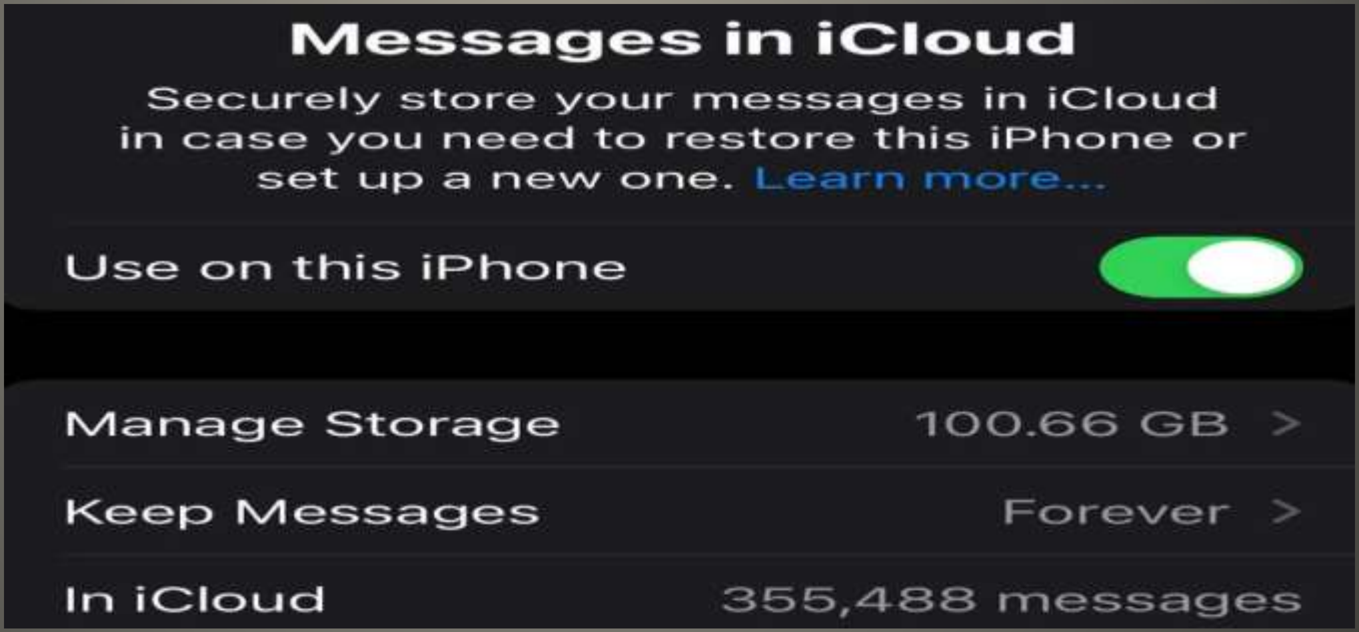
- China’s Peoples Liberation Army
- Volt Typhoon
- Mask activity – access home routers
- Company credentials
- Public Utility Commission of Texas PUC
- Electric Reliability Council of Texas ERCOT
- ERCOT statement:
- “ERCOT prepares year-round for any type of threat to the electric system. Whether the threat is cyber or physical, ERCOT continually invests in trained staff and resources to help keep the electric grid safe. From system redundancies to controlled access, ERCOT has multiple layers of protective measures to safeguard its critical infrastructure. This layered cyber and physical security approach is known as a defense -in-depth strategy.
- “ERCOT does not comment on specific operations. Please view cybersecurity one pager for more information.”

Washington Post 11-Dec-23

- First Party Fraud

  "I got it" & "I like it" "I want a refund"
- iOS 17.2 iMessages on iCloud

  Settings > your AppleID> iCloud > Messages



Messages in iCloud

Securely store your messages in iCloud in case you need to restore this iPhone or set up a new one. Learn more...

Use on this iPhone ●

Manage Storage 100.66 GB >

Keep Messages Forever >

In iCloud 355,488 messages

Current Issues

- Drive-Thru AI creepy – famous voices
- PLC with password 1111

  4 more water treatment plants

  Aquarium
- Ukraine hack Russia federal tax service

  "Complete destruction" of databases

  Russia used wiper malware prior to invasion
- Mr. Cooper hack 14 million customers

  Sensitive personal information

  Current and former customers
- Rite Aid facial recognition ban 5 years
- Hackers hide malware in Microsoft Azure security logs

Current Issues

Shopping Apps

- eBay
- Amazon Shopping
- Afterpay
- Lowes
- iHerb
- Vinted
- Home Depot
- Alibaba
- Poshmark
- Nike

Shopping Apps

- Share information with 3-rd parties

  Name, eMail, phone number, home address
- Share device ID with 3-rd parties
- Share financial data

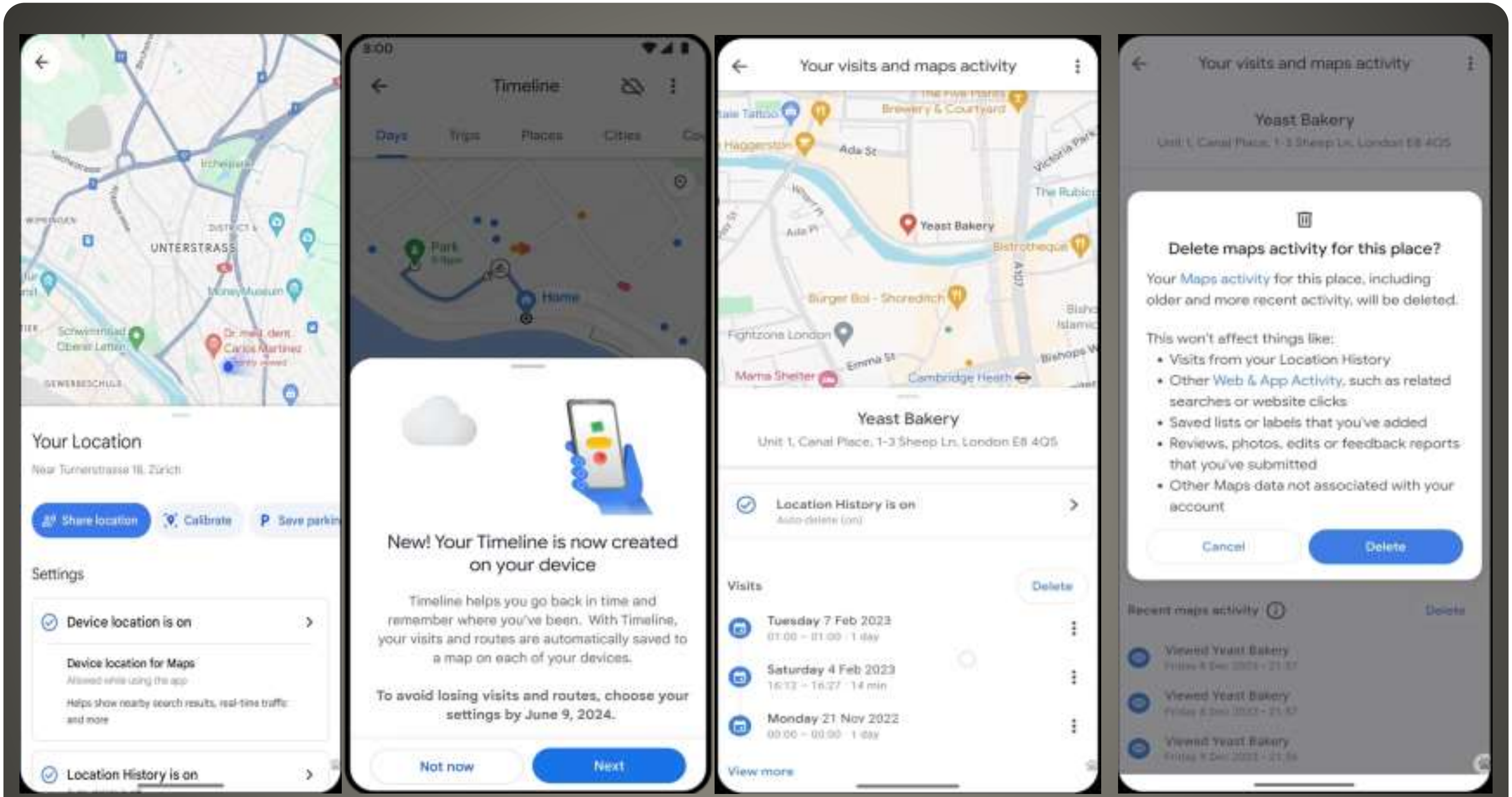
  purchase history, payment information
- Amazon:

"We collect, process, and share customers' personal information to provide a great shopping experience, and use it only as described in our Privacy Notice. We are not in the business of selling our customers' personal information to others."

Shopping Apps

- Research app before download
- Do not download untrustworthy apps

  That’s you, TEMU
- (Re)Review app permissions
- Consider VPN
- Clear cache & cookies
- Strong & UNIQUE password/passphrase
- Multi-Factor authentication
- Opt-out personalized ads



Your Location

Near Turnerstrasse 18, Zürich

Share location · Calibrate · Save parking

Settings

Device location is on

Device location for Maps

Allowed while using the app

Helps show nearby search results, real-time traffic and more

Location History is on

9:00

Timeline

Days · Trips · Places · Cities · Co

New! Your Timeline is now created on your device

Timeline helps you go back in time and remember where you've been. With Timeline, your visits and routes are automatically saved to a map on each of your devices.

To avoid losing visits and routes, choose your settings by June 9, 2024.

Not now · Next

Your visits and maps activity

Yeast Bakery

Unit 1, Canal Place, 1-3 Sheep Ln, London E8 4QS

Location History is on

Auto-delete (on)

Visits · Delete

Tuesday 7 Feb 2023
01:00 – 01:00 · 1 day

Saturday 4 Feb 2023
16:13 – 16:27 · 14 min

Monday 21 Nov 2022
00:00 – 00:00 · 1 day

View more

Your visits and maps activity

Yeast Bakery

Unit 1, Canal Place, 1-3 Sheep Ln, London E8 4QS

Delete maps activity for this place?

Your Maps activity for this place, including older and more recent activity, will be deleted.

This won't affect things like:

- Visits from your Location History
- Other Web & App Activity, such as related searches or website clicks
- Saved lists or labels that you've added
- Reviews, photos, edits or feedback reports that you've submitted
- Other Maps data not associated with your account

Cancel · Delete

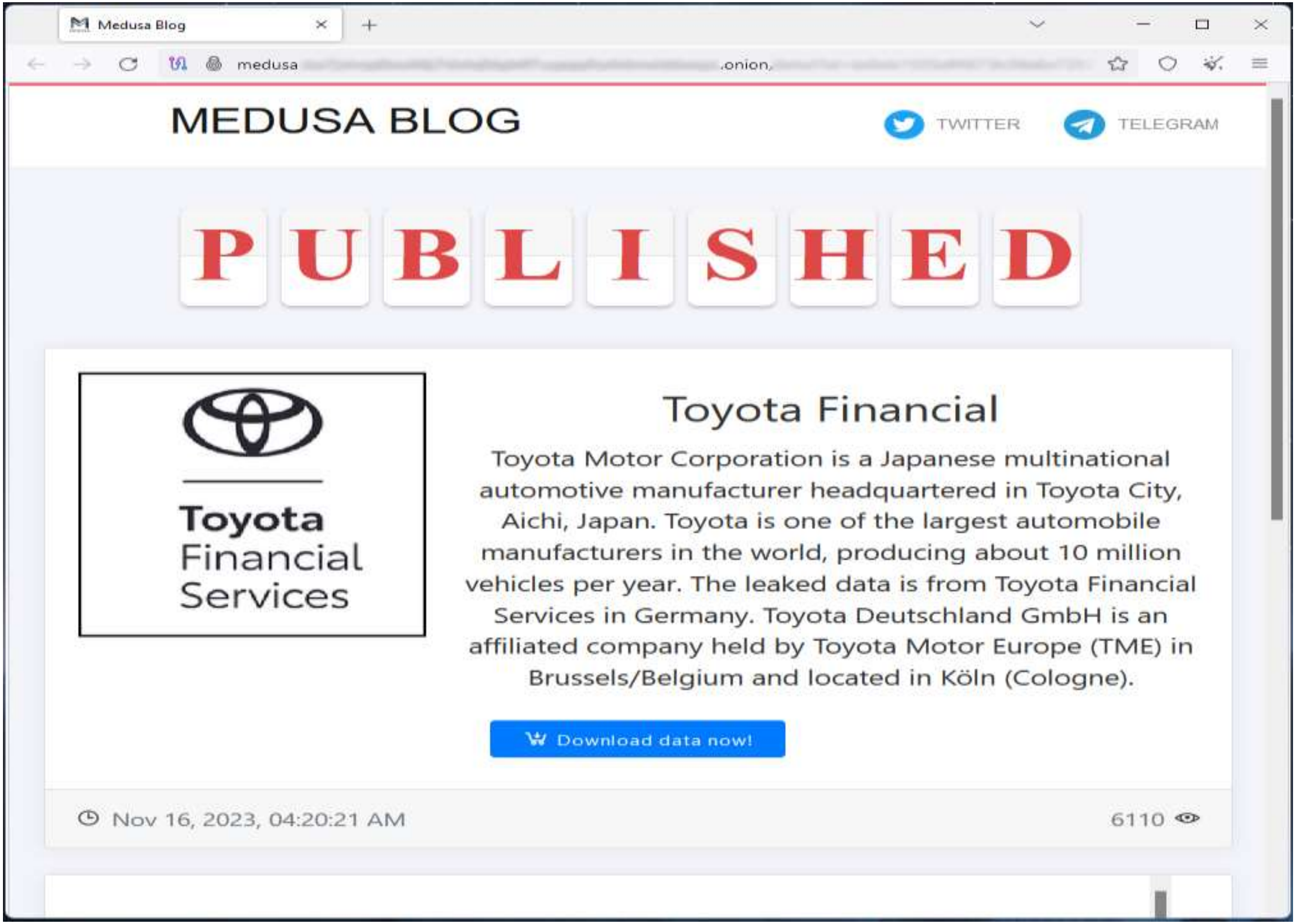
Recent maps activity · Delete

Viewed Yeast Bakery

Viewed Yeast Bakery

Viewed Yeast Bakery

Google Maps Blue Dot Privacy



MEDUSA BLOG

PUBLISHED

Toyota Financial

Toyota Motor Corporation is a Japanese multinational automotive manufacturer headquartered in Toyota City, Aichi, Japan. Toyota is one of the largest automobile manufacturers in the world, producing about 10 million vehicles per year. The leaked data is from Toyota Financial Services in Germany. Toyota Deutschland GmbH is an affiliated company held by Toyota Motor Europe (TME) in Brussels/Belgium and located in Köln (Cologne).

Nov 16, 2023, 04:20:21 AM

6110

A problem has be
to your computer

- Surveil smartphone users via push notifications
- Senator Ron Wyden letter to DOJ
- Repeal / modify policies hindering public discussions
- Then Apple
- "In this case, the federal government prohibited us from sharing any information," the company said in a statement. "Now that this method has become public we are updating our transparency reporting to detail these kinds of requests.�begin
- Which governments and how long?
- Encryption of notification message, BUT metadata
- Apple now requiring warrant or court order
- Section 702 expire end Dec?

  Now pushed till April 2024

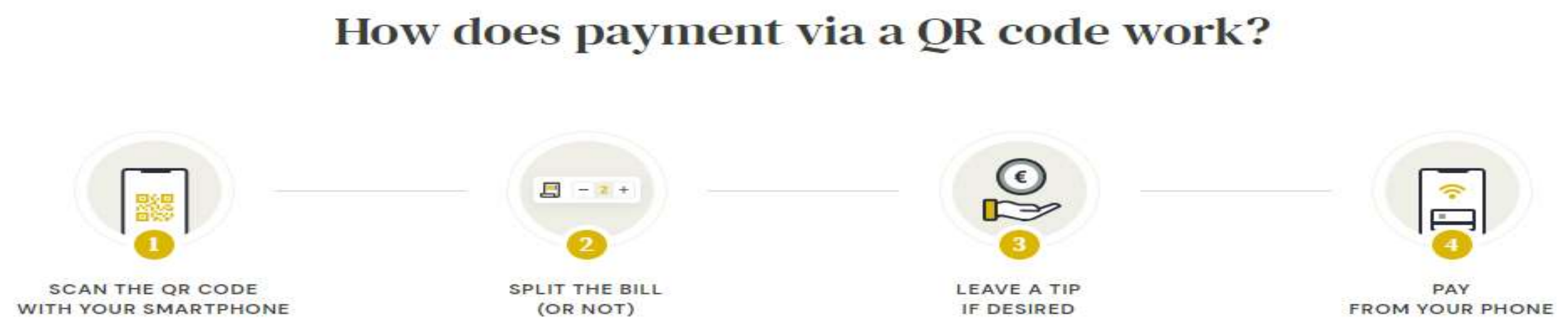
  Annual FISA certification
- Major pharmacies data to LE “on the spot”

Push Notifications

Geofence data

- Google location data on-device “soon”
- Apple location data on device now
- Reverse location warrants
- Information on innocents
- Past data?

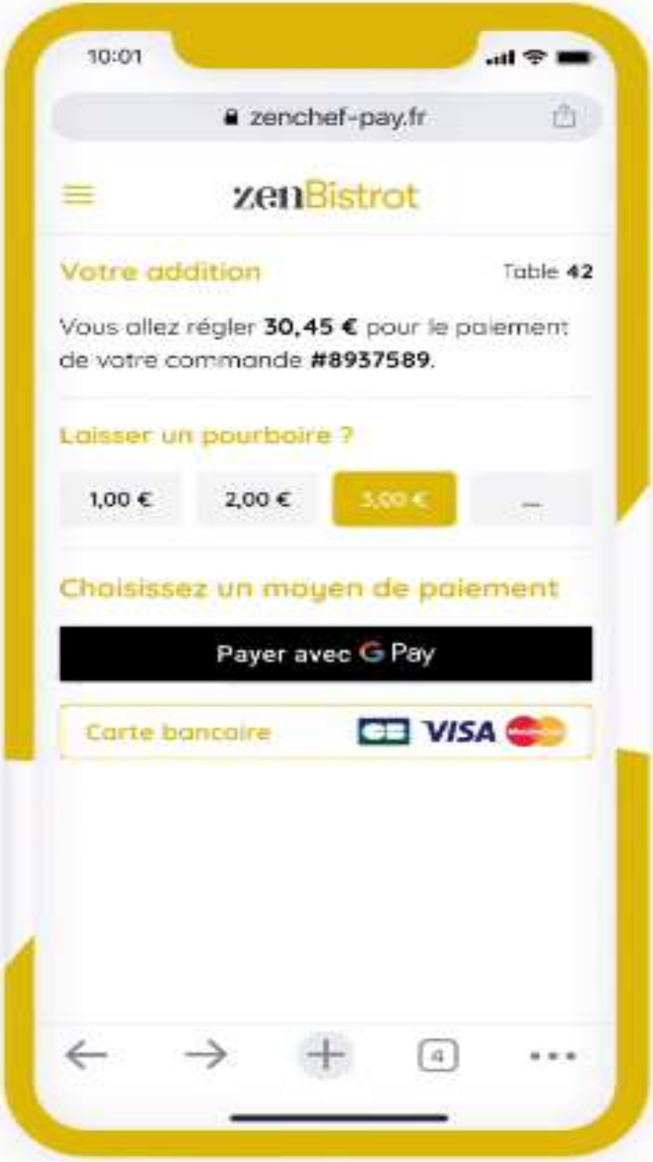
- Reverse keyword warrants



How does payment via a QR code work?

1. SCAN THE QR CODE WITH YOUR SMARTPHONE
2. SPLIT THE BILL (OR NOT)
3. LEAVE A TIP IF DESIRED
4. PAY FROM YOUR PHONE

QR code payment



Votre addition Table 42

Vous allez régler **30,45 €** pour le paiement de votre commande **#8937589**.

Laisser un pourboire ?

Choisissez un moyen de paiement

Beeper Mini

- Android messaging app
- Blocked by Apple “security & privacy concerns”
- Apple & Beeper cyber fight
- Now requires Mac Machine access

Blue bubbles on Android

Why was the blueberry sad?

Because all his friends

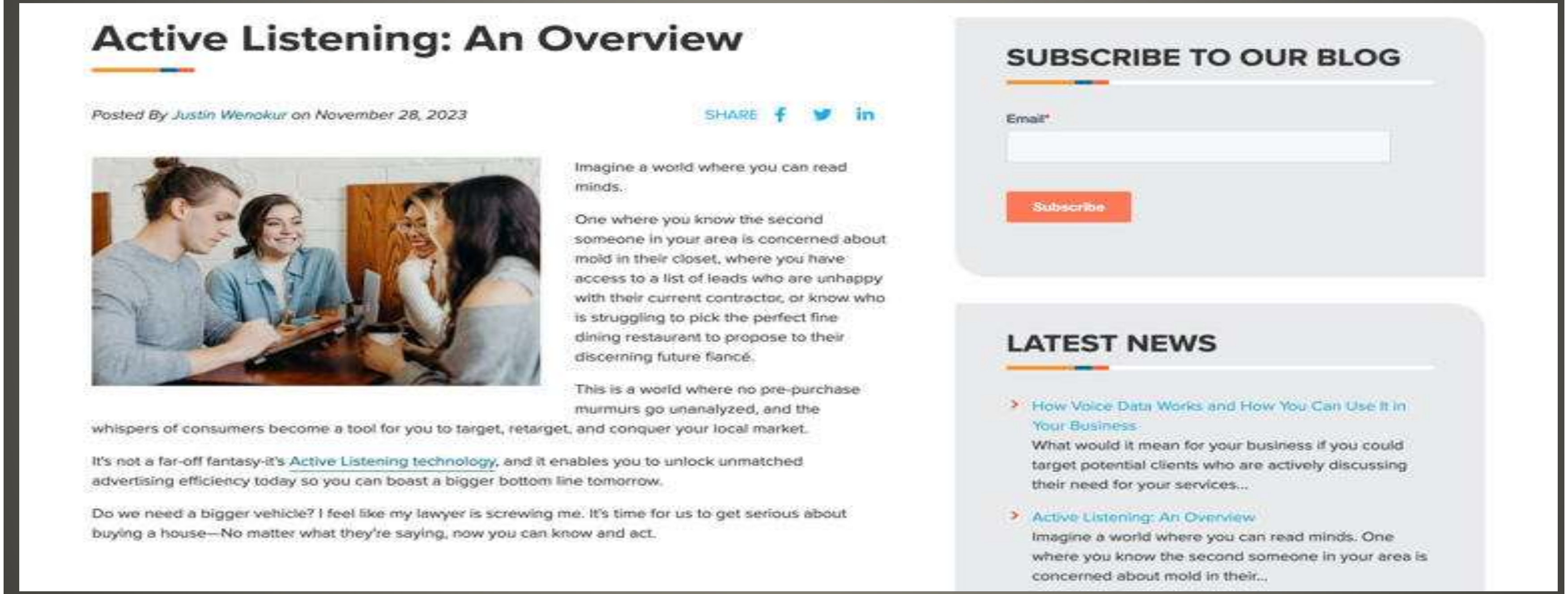
...were in a jam.

Get in the jam

- Among the new rules include regulations that "make it unequivocally clear" that lead generators and online shopping sites can no longer robocall or robotext consumers without their explicit consent.
- "Comparison shopping websites and lead generators must obtain consumer consent to receive robocalls and robotexts one seller at a time – rather than have a single consent apply to multiple telemarketers at once”
- Increase scope of federal Do-Not-Call registry
- Yeahbut NOT political campaign nor polling companies

New FCC rules

- Target Privacy?
- Cox Media Group   “Active Listening”
- Smart devices with microphone



Active Listening: An Overview

Posted By Justin Wenokur on November 28, 2023

Imagine a world where you can read minds.

One where you know the second someone in your area is concerned about mold in their closet, where you have access to a list of leads who are unhappy with their current contractor, or know who is struggling to pick the perfect fine dining restaurant to propose to their discerning future fiancé.

This is a world where no pre-purchase murmurs go unanalyzed, and the whispers of consumers become a tool for you to target, retarget, and conquer your local market.

It's not a far-off fantasy-it's Active Listening technology, and it enables you to unlock unmatched advertising efficiency today so you can boast a bigger bottom line tomorrow.

Do we need a bigger vehicle? I feel like my lawyer is screwing me. It's time for us to get serious about buying a house—No matter what they're saying, now you can know and act.

SUBSCRIBE TO OUR BLOG

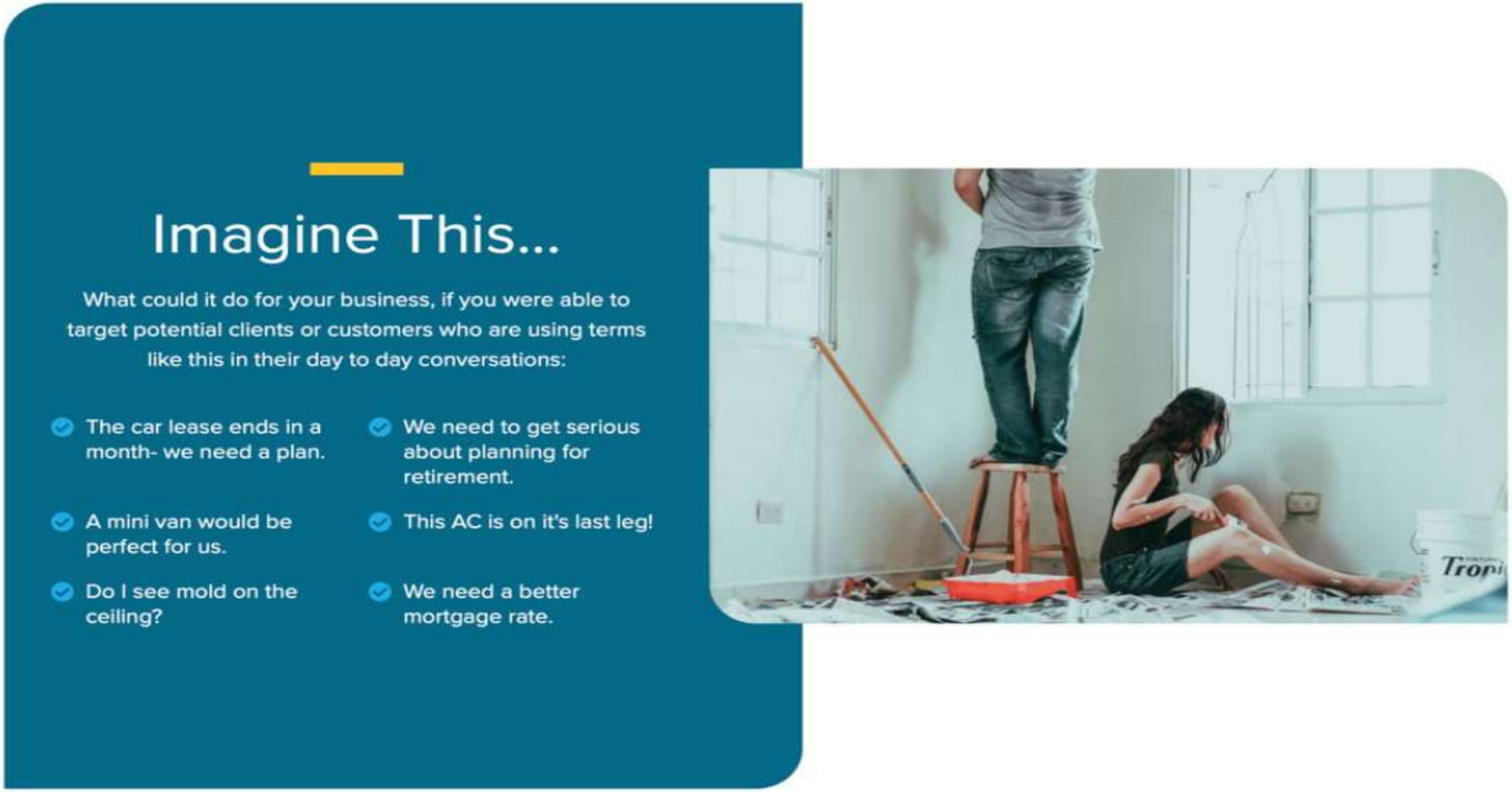
Email*

Subscribe

LATEST NEWS

- How Voice Data Works and How You Can Use It in Your Business
  What would it mean for your business if you could target potential clients who are actively discussing their need for your services...
- Active Listening: An Overview
  Imagine a world where you can read minds. One where you know the second someone in your area is concerned about mold in their...

Marketing Company
Listen to whispers   Targeted Ads



Imagine This...

What could it do for your business, if you were able to target potential clients or customers who are using terms like this in their day to day conversations:

- ✓ The car lease ends in a month- we need a plan.
- ✓ A mini van would be perfect for us.
- ✓ Do I see mold on the ceiling?
- ✓ We need to get serious about planning for retirement.
- ✓ This AC is on it's last leg!
- ✓ We need a better mortgage rate.

- The car lease ends in a month—we need a plan.
- A mini van would be perfect for us.
- Do I see mold on the ceiling?
- We need to get serious about planning for retirement.
- This AC is on its last leg!
- We need a better mortgage r

Marketing Company
Listen to whispers Targeted Ads

- Ad posted then deleted

"a world where no pre-purchased murmurs go unanalyzed,“
"the whispers of consumers become a tool for you to target.“

"We know what you're thinking. Is this even legal?“

"It is legal for phones and devices to listen to you. When a new app download or update prompts consumers with a multi-page term of use agreement somewhere in the fine print, Active Listening is often included."

"With this unprecedented understanding of consumer behavior, we can deliver personalized ads that make your target audience think: wow, they must be a mind reader,"

- Turn on keywords

- App access to microphone
- Voice Memos

- Micro electronics Rare earth
- Always On microphones
- Listening for keywords
- Listening
- Smart Phones Smart tablets PCs Macs Smart TVs Smart Remotes Smart Speakers Smart Cars Smart GPS Smart Drive Thru

Cox Media Group’s surveillance capabilities

Brave New World

- December 2013
- Tech Talk
- Bob Frost
- Page 97
- Is your smart phone listening to your conversations?

Sun City Sunrays Article

- “Keeping Children safe no longer possible”
  - Law Enforcement

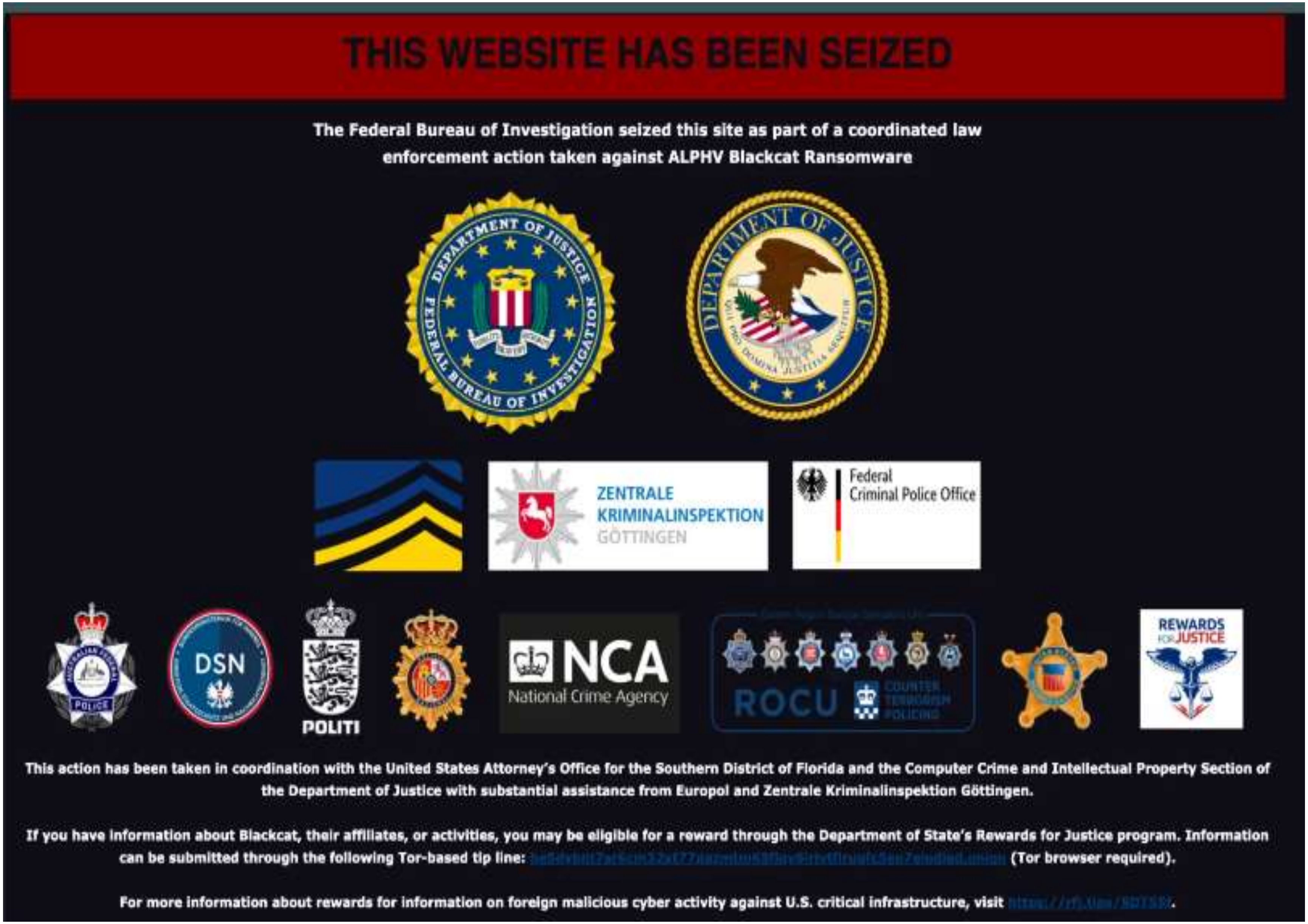
  Meta law enforcement requests hundreds of thousands for user data

  56% legitimate
- Meta to use Signal protocol

Meta end-to-end encryption

- Google shuttering Play Movies & TV app
  Jan 17 Moved to Android TV & YouTube
- Making guard railed chatbots talk – using AI
- Samsung Internet – browser
- Android Lock Screen vulnerability
  Android 13 Android 14
  Reported May
  Google Maps Driving Mode enabled
- Proton Mail Desktop App Windows & macOS
  Beta
- Poland railroad manufacturer Newag
  Third-party repair disable
  Manufacturer accusing hackers of slander

Current Issues



THIS WEBSITE HAS BEEN SEIZED

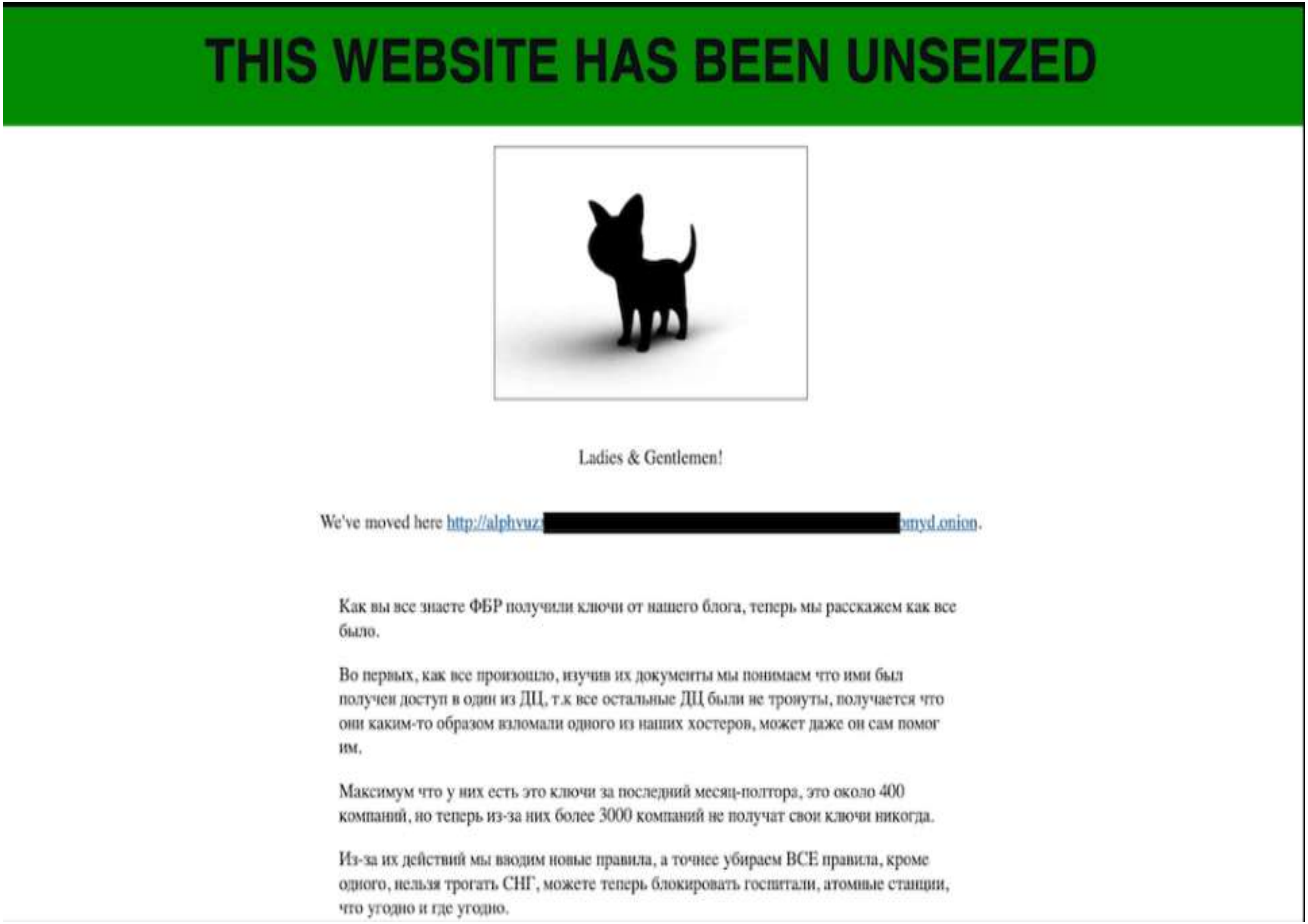
The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE
ZENTRALE KRIMINALINSPEKTION GÖTTINGEN
Federal Criminal Police Office
DSN
POLITI
NCA National Crime Agency
ROCU
COUNTER TERRORISM POLICING
REWARDS FOR JUSTICE

This action has been taken in coordination with the United States Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State's Rewards for Justice program. Information can be submitted through the following Tor-based tip line: [illegible] (Tor browser required).

For more information about rewards for information on foreign malicious cyber activity against U.S. critical infrastructure, visit https://rfj.tips/SDTSSI.



THIS WEBSITE HAS BEEN UNSEIZED

Ladies & Gentlemen!

We've moved here http://alphvuz[redacted]nnyd.onion.

Как вы все знаете ФБР получили ключи от нашего блога, теперь мы расскажем как все было.

Во первых, как все произошло, изучив их документы мы понимаем что ими был получен доступ в один из ДЦ, т.к все остальные ДЦ были не тронуты, получается что они каким-то образом взломали одного из наших хостеров, может даже он сам помог им.

Максимум что у них есть это ключи за последний месяц-полтора, это около 400 компаний, но теперь из-за них более 3000 компаний не получат свои ключи никогда.

Из-за их действий мы вводим новые правила, а точнее убираем ВСЕ правила, кроме одного, нельзя трогать СНГ, можете теперь блокировать госпитали, атомные станции, что угодно и где угодно.

BlackCat ransomware

- FBI seized site
- Releases decryption tool

- BlackCat unseized site
- Offered 90% commissions
- Open season on hospitals to nuclear power plants, but not CIS
  Commonwealth of Independent States
- Ransomware-as-a-service

LogoFAIL

- Constellation of vulnerabilities
- Unified Extensible Firmware Interface UEFI
- Rendering manufacturer’s Logo
- Bypass UEFI defenses Secure Boot, etc.
- Bootkit infections
- 29 security issues 15 arbitrary code execution
- Entirety of CPU ecosystem
- Apple devices not vulnerable
- Nor Dell
- LogoFAIL unstoppable Stop the infection
- Physical Control
- Firmware updates

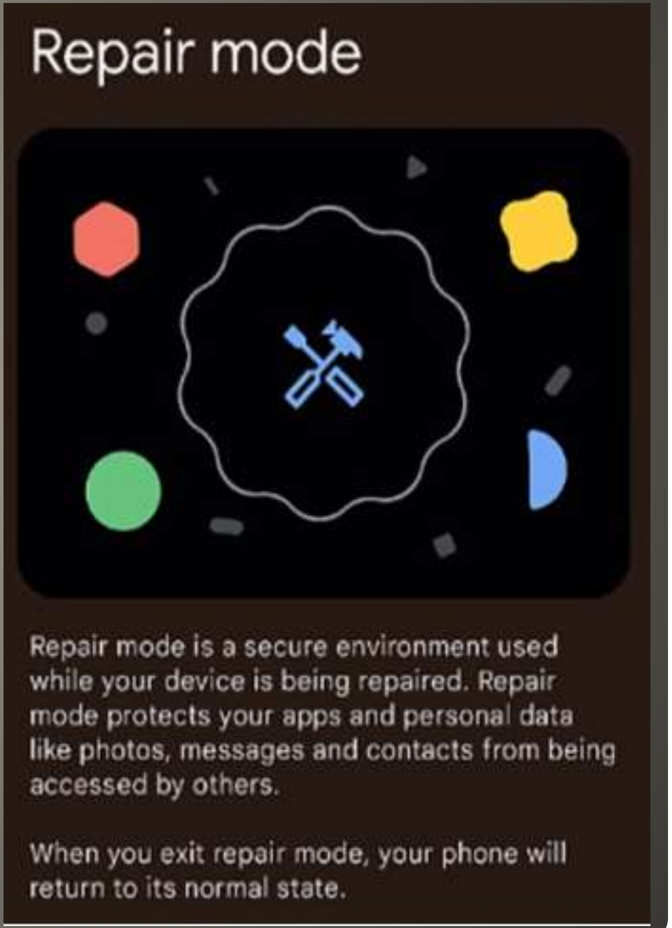
- Created to be multimodal
- Content, emotion, personality – converse
- Demo using canned information
- Project Ellman *Your life story teller*
- Search results, photo patterns, chatbot interactions
- Ellman Chat “we know you, what would you ask?”

Google Gemini AI

- Pixel devices Android 14 2GB free space
- Settings > System > Repair Mode
- Diagnostic:
- #*#7287#*#

- For others?
  Suggest:
  Change your password/passcode
  Lie to repair person
  if/when they call you "I'll take it as it is"
  Change your password/passcode back

Google Pixel mode



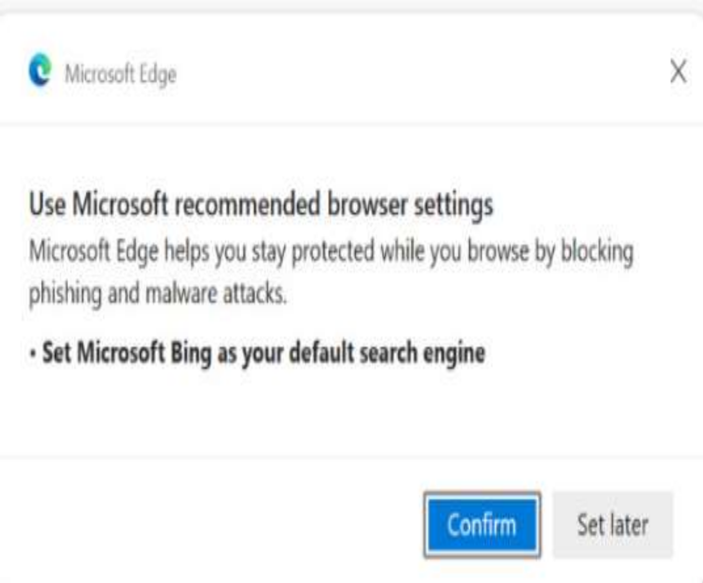
Repair mode

Repair mode is a secure environment used while your device is being repaired. Repair mode protects your apps and personal data like photos, messages and contacts from being accessed by others.

When you exit repair mode, your phone will return to its normal state.

- Edge

Windows 10

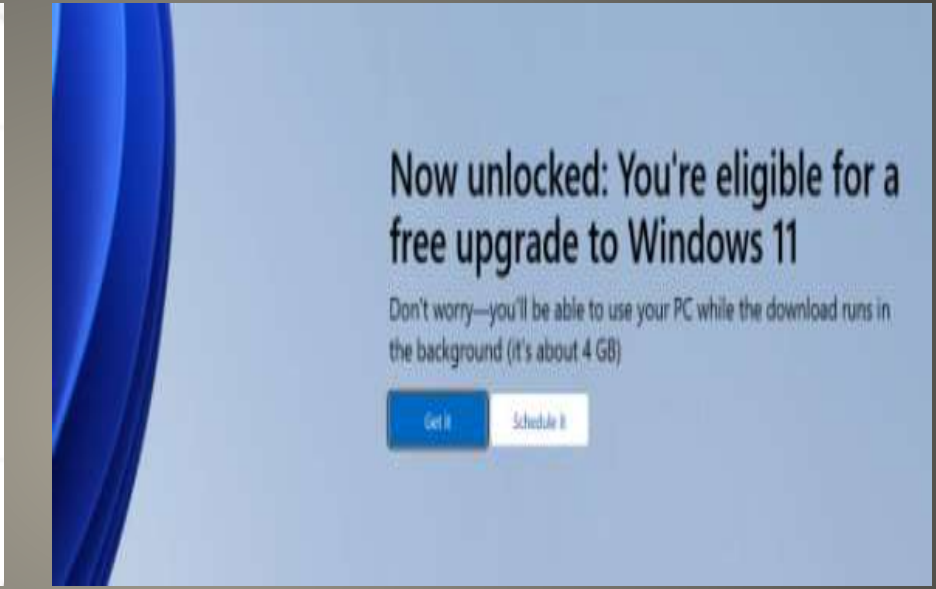


Microsoft Edge

Use Microsoft recommended browser settings

Microsoft Edge helps you stay protected while you browse by blocking phishing and malware attacks.

- Set Microsoft Bing as your default search engine



Now unlocked: You're eligible for a free upgrade to Windows 11

Don't worry—you'll be able to use your PC while the download runs in the background (it's about 4 GB)

Microsoft Where are my options?

- December 18, 2023
- Breach disclosure 4 days

  Hack will have a material impact

New SEC Cyber rules

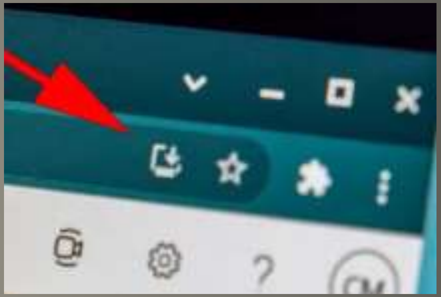
- Vulnerabilities more than 10 years old
- Critical scores
- CISA Known Exploited Vulnerabilities

  Remediate these as a priority
- Over developed - thus updates disabled

Cisco Talos annual cyber report

Current Issues

- Sony loses Quad 9 suit – Germany
- Quad 9 suit – Italy
- ChromeOS and Progressive Web Apps (PWA)
  Microsoft Office?

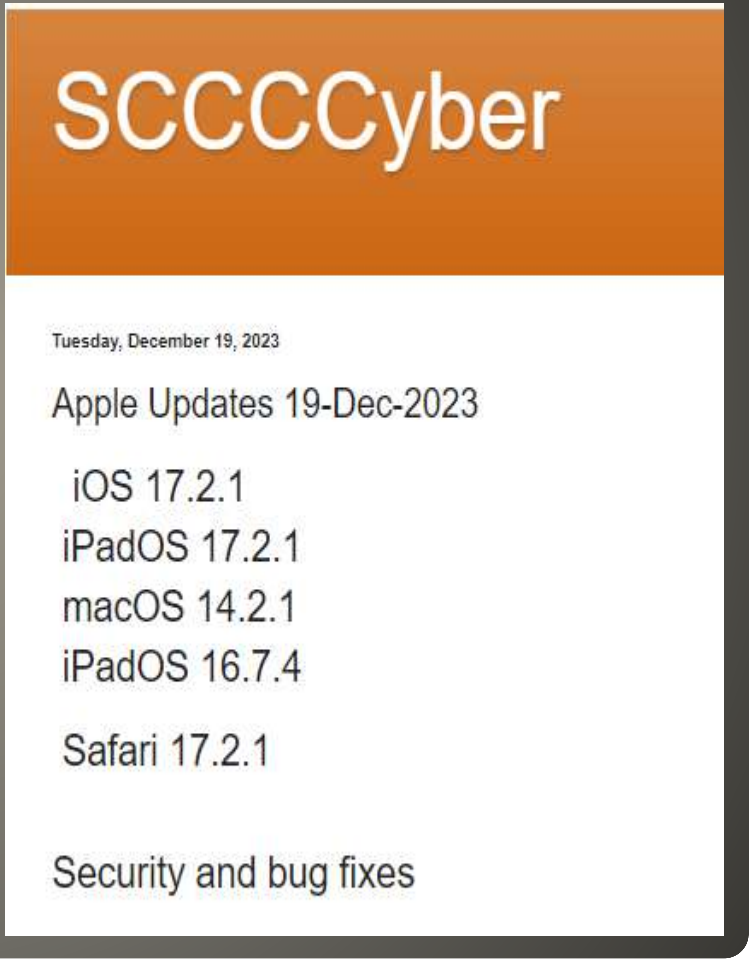


- Google Buzz 2010
  Automatically setup
  Friend network
  Email addresses
  FTC consent decree
  Comprehensive privacy program
- Telegram notifies users you have joined IF user had your phone number in contacts

- Security & bug fixes
- iPadOS 17.2.1
- Window manager
- Selected share window
- Apple stopped signing

  iOS 17.1.1

  iOS 17.1.2



SCCCCyber

Tuesday, December 19, 2023

Apple Updates 19-Dec-2023

iOS 17.2.1
iPadOS 17.2.1
macOS 14.2.1
iPadOS 16.7.4

Safari 17.2.1

Security and bug fixes

Apple Updates

- Overlay network
- TailScale
- ZeroTier

Reverse VPN

Apple Avatar

- 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