Sun City Computer Club

Cyber Security SIG

April 21, 2022

Questions, Comments, Suggestions welcomed at any time

Even Now

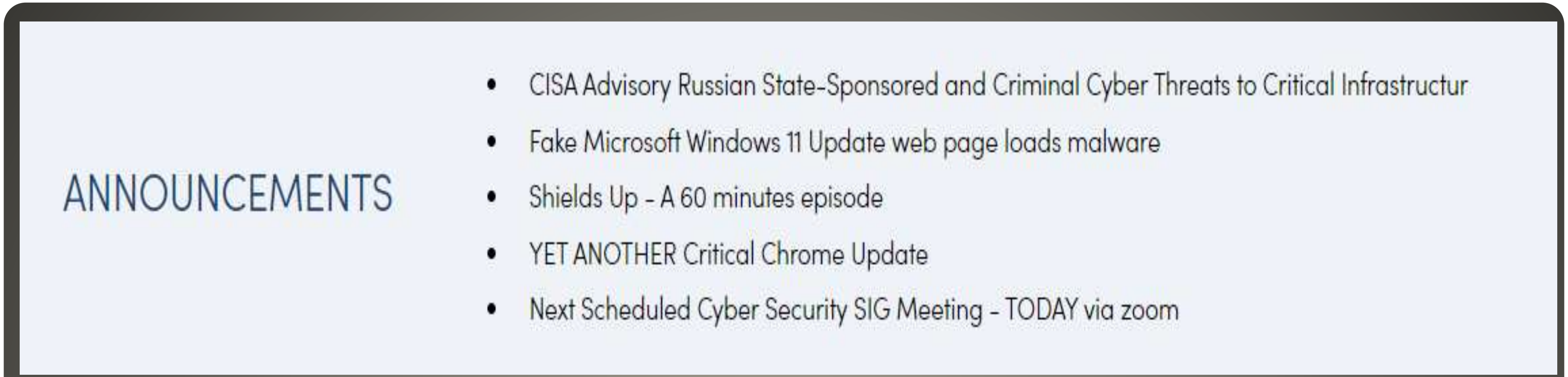
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

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

- Ever want to be a presenter??

Presenter???



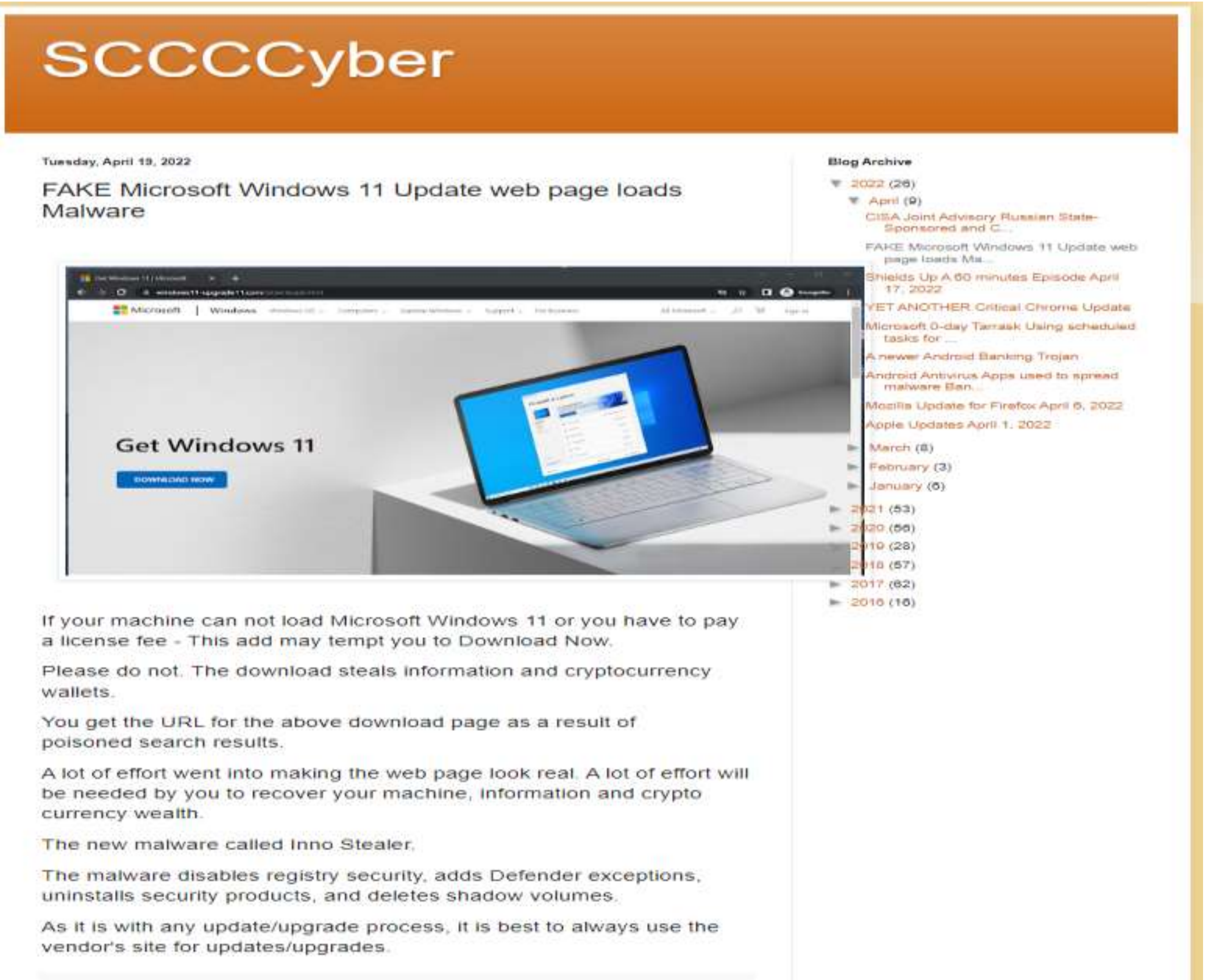
ANNOUNCEMENTS

- CISA Advisory Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructur
- Fake Microsoft Windows 11 Update web page loads malware
- Shields Up - A 60 minutes episode
- YET ANOTHER Critical Chrome Update
- Next Scheduled Cyber Security SIG Meeting - TODAY via zoom

FAKE MICROSOFT WINDOWS 11 UPDATE WEB PAGE LOADS MALWARE

https://scccyber.blogspot.com/2022/04/fake-microsoft-windows-11-update-web.html

SIG Announcements



SCCCyber

Tuesday, April 19, 2022

FAKE Microsoft Windows 11 Update web page loads Malware

If your machine can not load Microsoft Windows 11 or you have to pay a license fee - This add may tempt you to Download Now.

Please do not. The download steals information and cryptocurrency wallets.

You get the URL for the above download page as a result of poisoned search results.

A lot of effort went into making the web page look real. A lot of effort will be needed by you to recover your machine, information and crypto currency wealth.

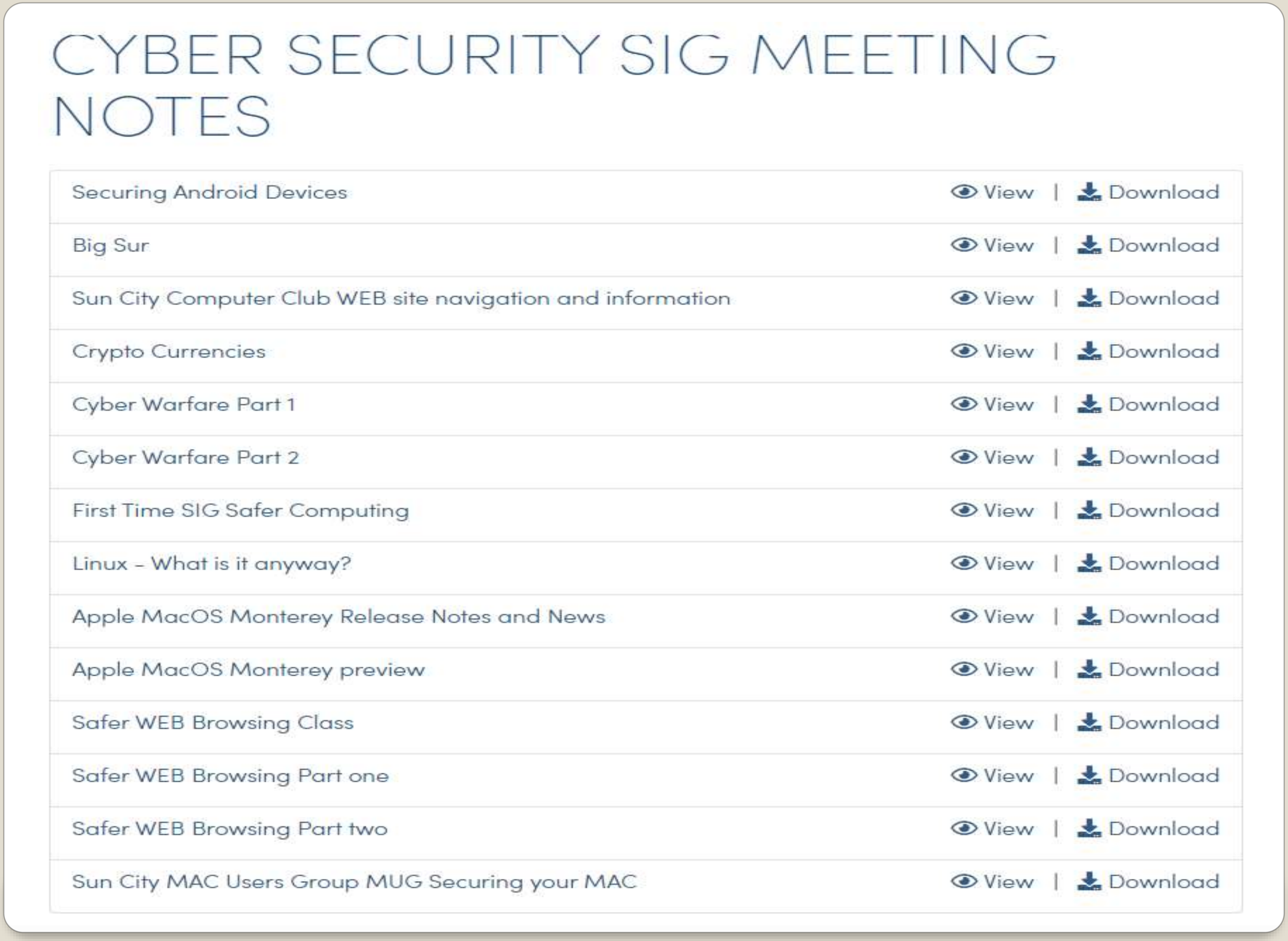
The new malware called Inno Stealer.

The malware disables registry security, adds Defender exceptions, uninstalls security products, and deletes shadow volumes.

As it is with any update/upgrade process, it is best to always use the vendor's site for updates/upgrades.

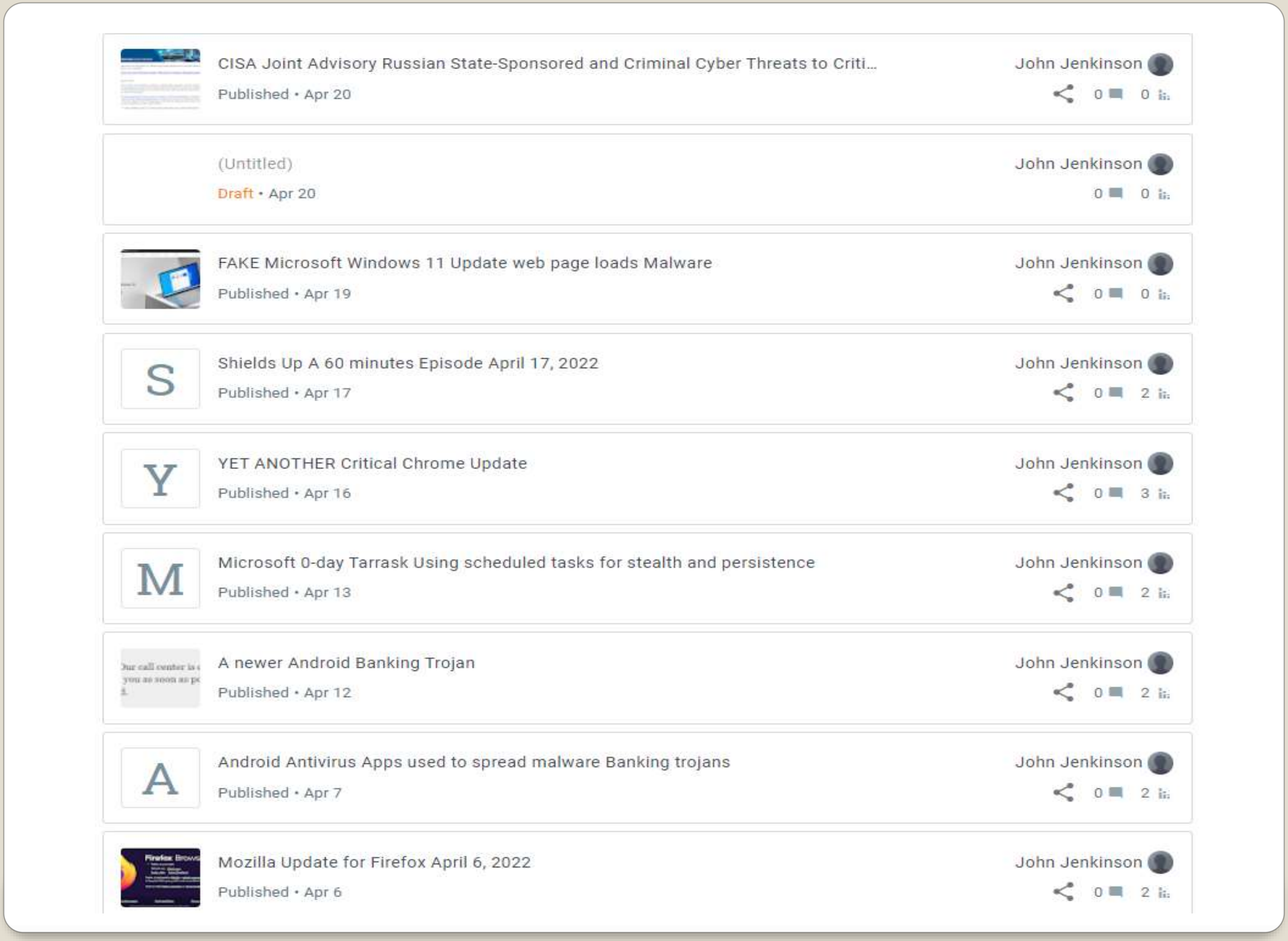
Blog Archive

- ▼ 2022 (26)
  - ▼ April (9)
    - CISA Joint Advisory Russian State-Sponsored and C...
    - FAKE Microsoft Windows 11 Update web page loads Ma...
    - Shields Up A 60 minutes Episode April 17, 2022
    - YET ANOTHER Critical Chrome Update
    - Microsoft 0-day Tarrask Using scheduled tasks for ...
    - A newer Android Banking Trojan
    - Android Antivirus Apps used to spread malware Ban...
    - Mozilla Update for Firefox April 6, 2022
    - Apple Updates April 1, 2022
  - ► March (8)
  - ► February (3)
  - ► January (6)
- ► 2021 (53)
- ► 2020 (56)
- ► 2019 (28)
- ► 2018 (57)
- ► 2017 (62)
- ► 2016 (16)



CYBER SECURITY SIG MEETING NOTES

Securing Android Devices	View	Download
Big Sur	View	Download
Sun City Computer Club WEB site navigation and information	View	Download
Crypto Currencies	View	Download
Cyber Warfare Part 1	View	Download
Cyber Warfare Part 2	View	Download
First Time SIG Safer Computing	View	Download
Linux – What is it anyway?	View	Download
Apple MacOS Monterey Release Notes and News	View	Download
Apple MacOS Monterey preview	View	Download
Safer WEB Browsing Class	View	Download
Safer WEB Browsing Part one	View	Download
Safer WEB Browsing Part two	View	Download
Sun City MAC Users Group MUG Securing your MAC	View	Download



CISA Joint Advisory Russian State-Sponsored and Criminal Cyber Threats to Criti…	Published • Apr 20	John Jenkinson	0	0
(Untitled)	Draft • Apr 20	John Jenkinson	0	0
FAKE Microsoft Windows 11 Update web page loads Malware	Published • Apr 19	John Jenkinson	0	0
Shields Up A 60 minutes Episode April 17, 2022	Published • Apr 17	John Jenkinson	0	2
YET ANOTHER Critical Chrome Update	Published • Apr 16	John Jenkinson	0	3
Microsoft 0-day Tarrask Using scheduled tasks for stealth and persistence	Published • Apr 13	John Jenkinson	0	2
A newer Android Banking Trojan	Published • Apr 12	John Jenkinson	0	2
Android Antivirus Apps used to spread malware Banking trojans	Published • Apr 7	John Jenkinson	0	2
Mozilla Update for Firefox April 6, 2022	Published • Apr 6	John Jenkinson	0	2

- Driverless car pulled over (no lights)
- But I have a VPN

  You – ISP – Internet

  You – VPN – Internet

Evading censorship

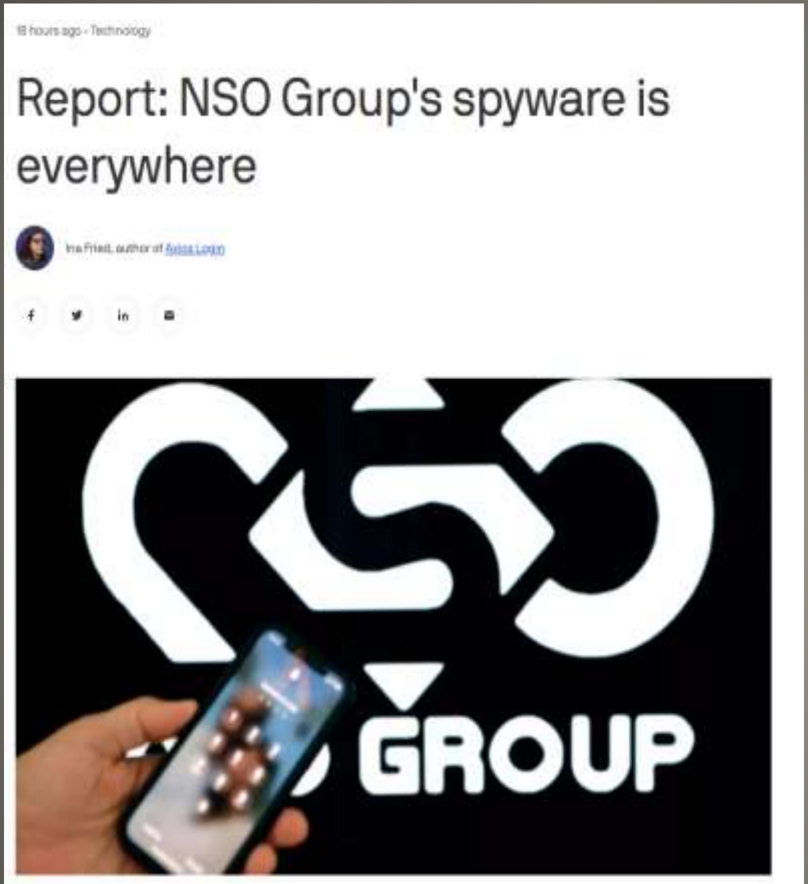
Surveillance – tracking

Torrenting

Streaming

Public Wi-Fi

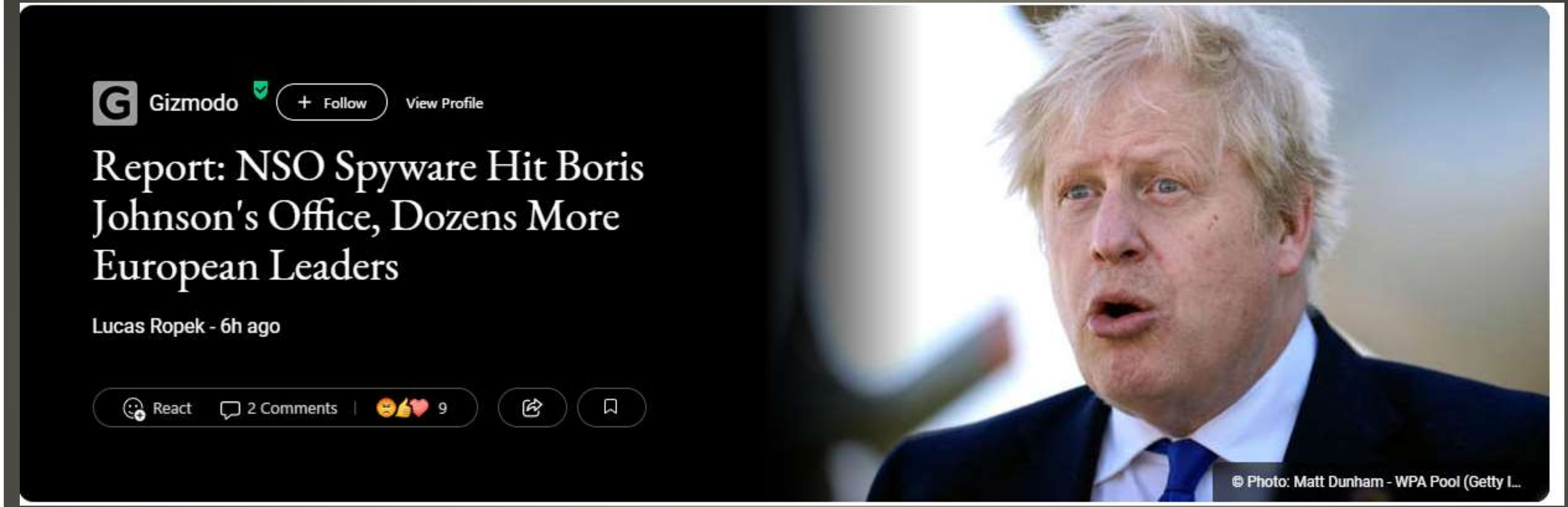
Current Issues



18 hours ago · Technology

Report: NSO Group's spyware is everywhere

Ina Fried, author of Axios Login



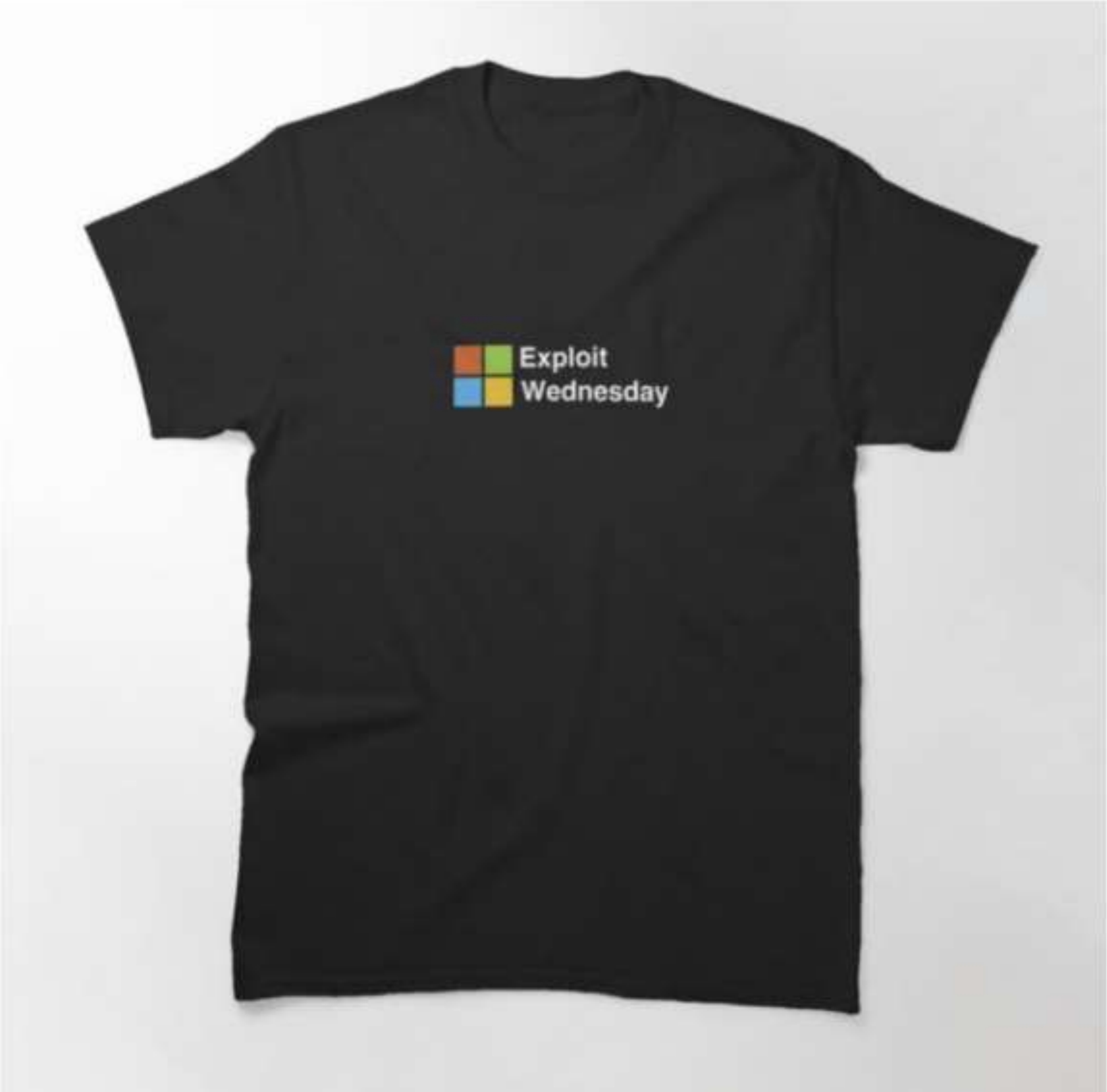
Report: NSO Spyware Hit Boris Johnson's Office, Dozens More European Leaders

Lucas Ropek - 6h ago

© Photo: Matt Dunham - WPA Pool (Getty I...

And Catalan politicians

What Follows "Patch Tuesday" ???



Current Issues

- Tarrask zero day
  hidden scheduled tasks
  subsequent actions to hide
  maintain persistence

https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/

https://sccccyber.blogspot.com/2022/04/microsoft-0-day-tarrask-using-scheduled.html

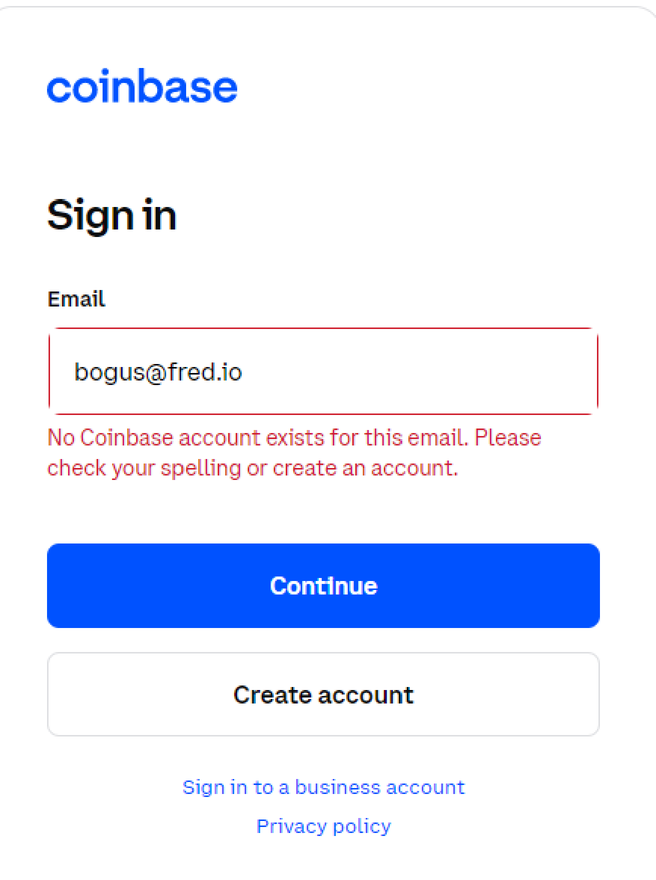
Current Issues

- NGINX web server 0-day
- Microsoft autopatch

  Rings: Test, First, Fast, Broad

  Halt & rollback
- Russia protest in JavaScript repository
- May 2022 end of service

  Windows 10 20H2   Windows 10 1909
- Port knocking defenses
- Spring4Shell
- Just Walk Out Minute Maid Park



coinbase

Sign in

Email

bogus@fred.io

No Coinbase account exists for this email. Please check your spelling or create an account.

Coinbase

Current Issues

- US House launch investigation ID.me

  Facial recognition concerns

  Privacy, Failure rate, etc.

  IRS to require ID.me to delete selfies and face scans

  Issues with older and poorer - no camera
- Deflating SUV tires
- Incontroller newly discovered malware

  Industrial control systems

  NOT financially motivated
- Insteon down?
- Doxxing

Doxxing

- Do NOT Hack back
- Contact Law Enforcement
- Use protections MFA, strong passphrase, unique passphrases
- Google Alerts
- Limit and review social media postings

- Hand your iPhone around?
- Notification previews

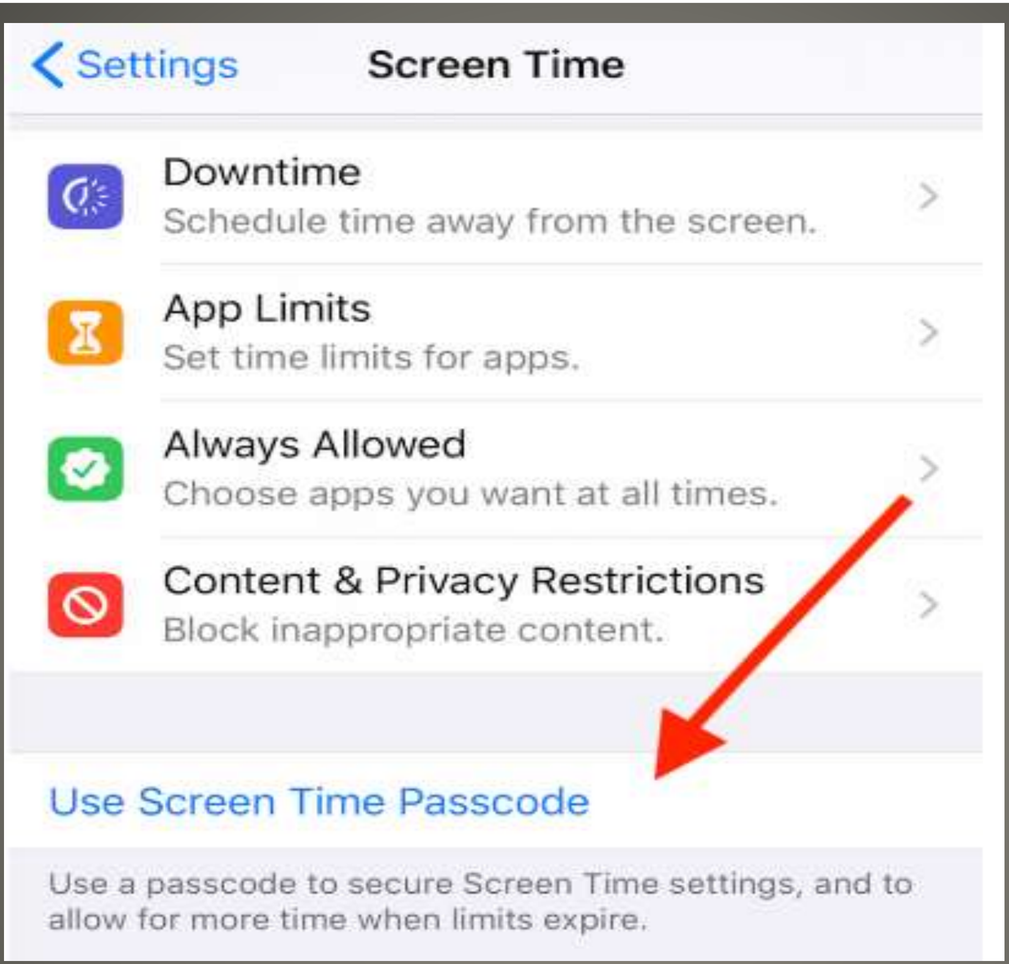
  Settings > Notifications > Show Previews
- FindMy
- Screen Time   Passcode

  Set and remember passcode

  App Limits 1 minute?

  use passcode to bypass limits

Handy iPhone



Screen Time

Downtime
Schedule time away from the screen.

App Limits
Set time limits for apps.

Always Allowed
Choose apps you want at all times.

Content & Privacy Restrictions
Block inappropriate content.

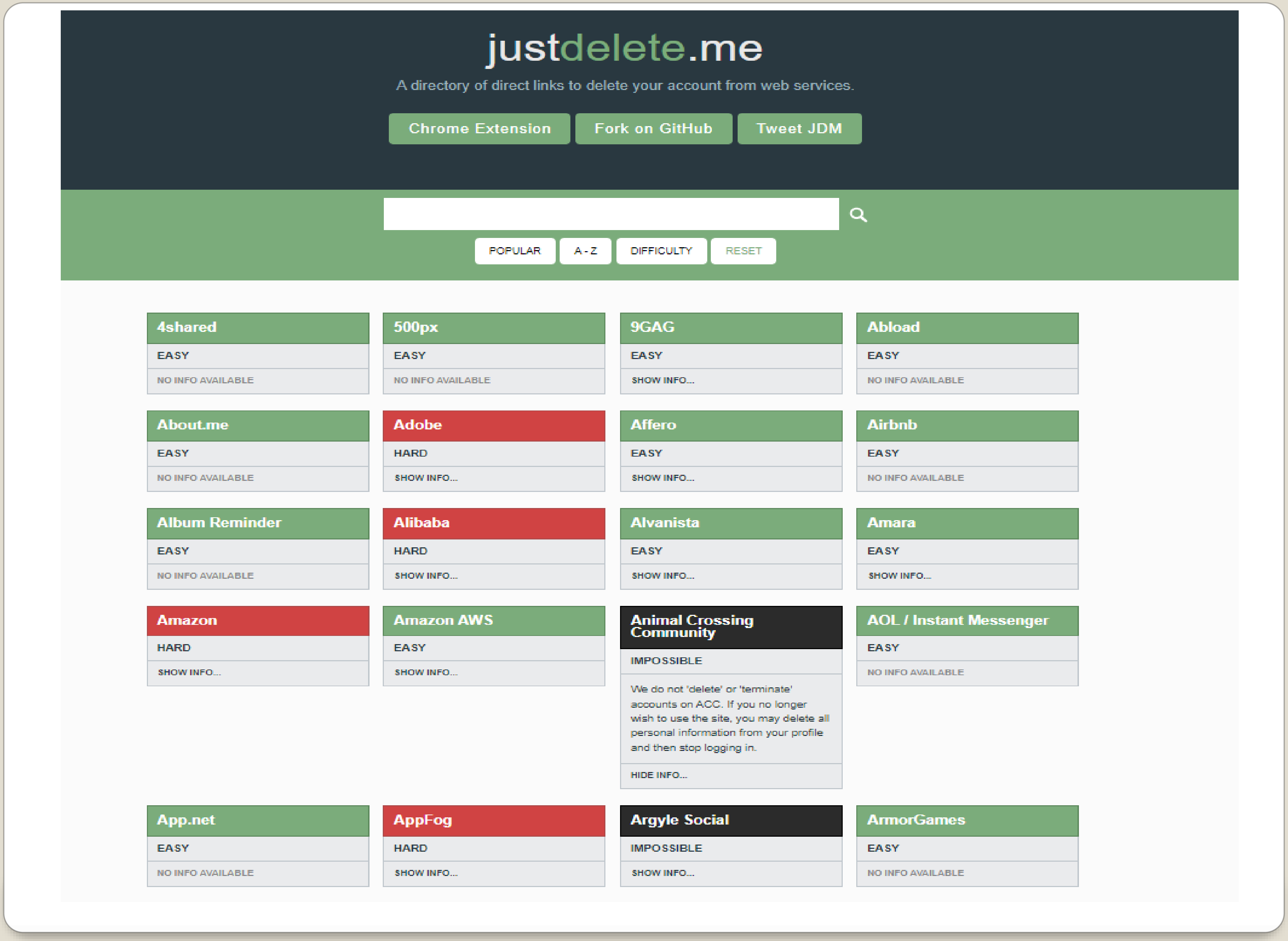
Use Screen Time Passcode

Use a passcode to secure Screen Time settings, and to allow for more time when limits expire.

Screen Time iPhone iPad

- Directory of direct links to delete you account
- Green – easy
- Red – difficult
- Black - impossible

Justdelete.me



justdelete.me

A directory of direct links to delete your account from web services.

Chrome Extension | Fork on GitHub | Tweet JDM

POPULAR | A - Z | DIFFICULTY | RESET

4shared	EASY	NO INFO AVAILABLE
500px	EASY	NO INFO AVAILABLE
9GAG	EASY	SHOW INFO...
Abload	EASY	NO INFO AVAILABLE
About.me	EASY	NO INFO AVAILABLE
Adobe	HARD	SHOW INFO...
Affero	EASY	SHOW INFO...
Airbnb	EASY	NO INFO AVAILABLE
Album Reminder	EASY	NO INFO AVAILABLE
Alibaba	HARD	SHOW INFO...
Alvanista	EASY	SHOW INFO...
Amara	EASY	SHOW INFO...
Amazon	HARD	SHOW INFO...
Amazon AWS	EASY	SHOW INFO...
Animal Crossing Community	IMPOSSIBLE	We do not 'delete' or 'terminate' accounts on ACC. If you no longer wish to use the site, you may delete all personal information from your profile and then stop logging in. HIDE INFO...
AOL / Instant Messenger	EASY	NO INFO AVAILABLE
App.net	EASY	NO INFO AVAILABLE
AppFog	HARD	SHOW INFO...
Argyle Social	IMPOSSIBLE	SHOW INFO...
ArmorGames	EASY	NO INFO AVAILABLE

- There are services
- Remember you provide your info
- Helpful <-> Harmful

Justdelete.me

- ASRock motherboard driver
  Joint advisory
  DOE, FBI, CISA, NSA
- Owe IRS? Pay with cash:
  Family Dollar, CVS, Walgreens,7-Eleven,
- VPNs installing root certificates
  Surfshark, TurboVPN, VyprVPN
- Lenovo UEFI vulnerability
- Brave browser bypass Google AMP pages
  Accelerated Mobile Pages
- 7-zip Elevated privilege vulnerability
  version 21.07 and previous
- MetaMask seeds stored in iCloud

Current Issues

Cell Phone number

- Better for life hacking than SSN

  sites WhoEasy, White pages, Fast People Search
- SIM swapping

  Forgot my password
- Texting scams
- Google Voice
- 2 lines

Current Issues

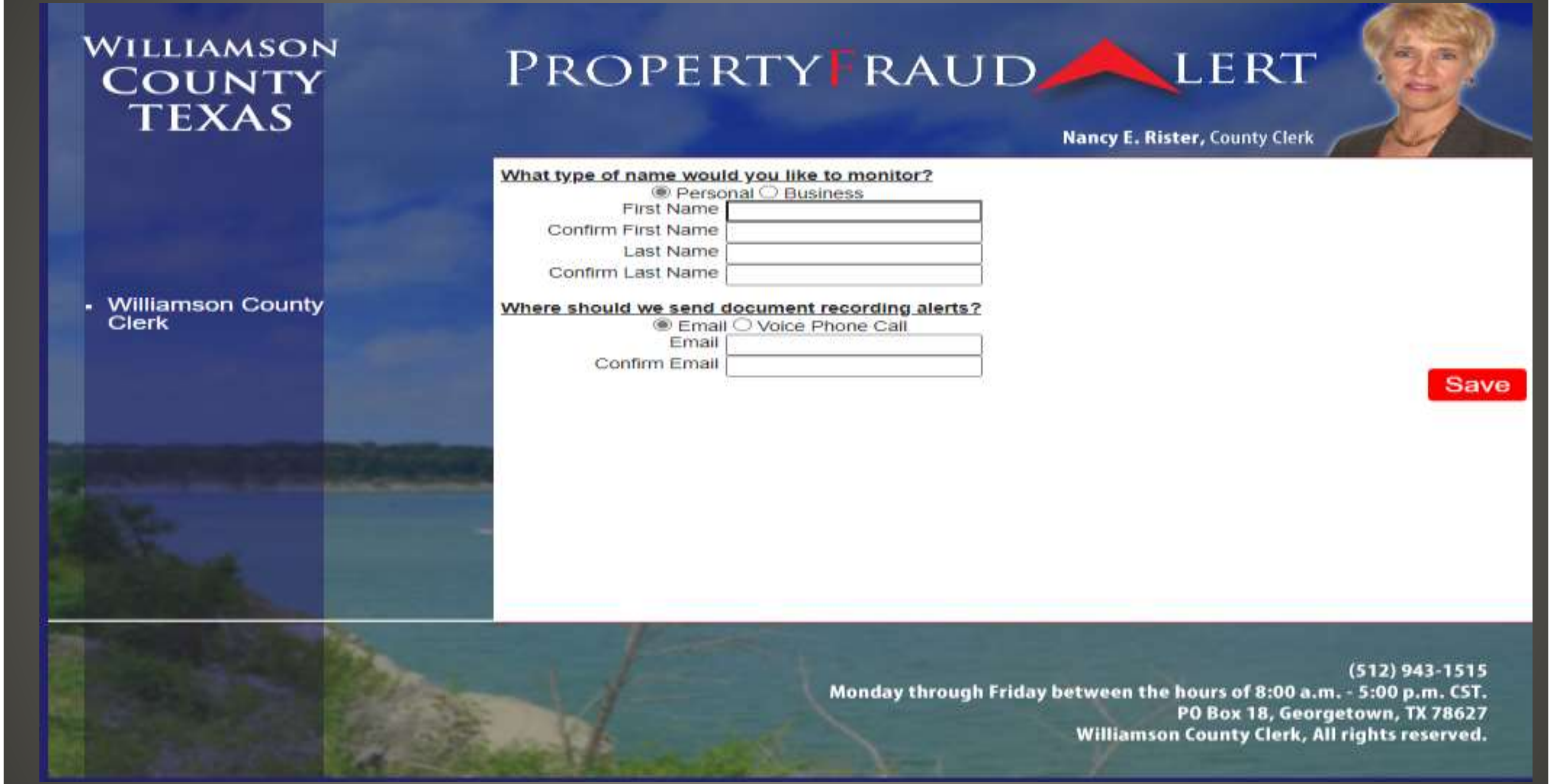
- SMB1 disabled Windows 11 insider
- Google adds “badges” to chrome extensions

  Featured & Established Publishers
- Apple Beta updates

  Monterey 12.4

  iOS 15.5 iPadOS 15.5
- Chrome OS 100.0.4896.133
- Golden Knights event => Capitol evacuation
- DHS Thwarts cyber attack on undersea cable
- Ukraine defends power grid attack

- https://www.propertyfraudalert.com/TXWilliamson/Home/Disclaimer



What type of name would you like to monitor?

● Personal ○ Business

First Name

Confirm First Name

Last Name

Confirm Last Name

Where should we send document recording alerts?

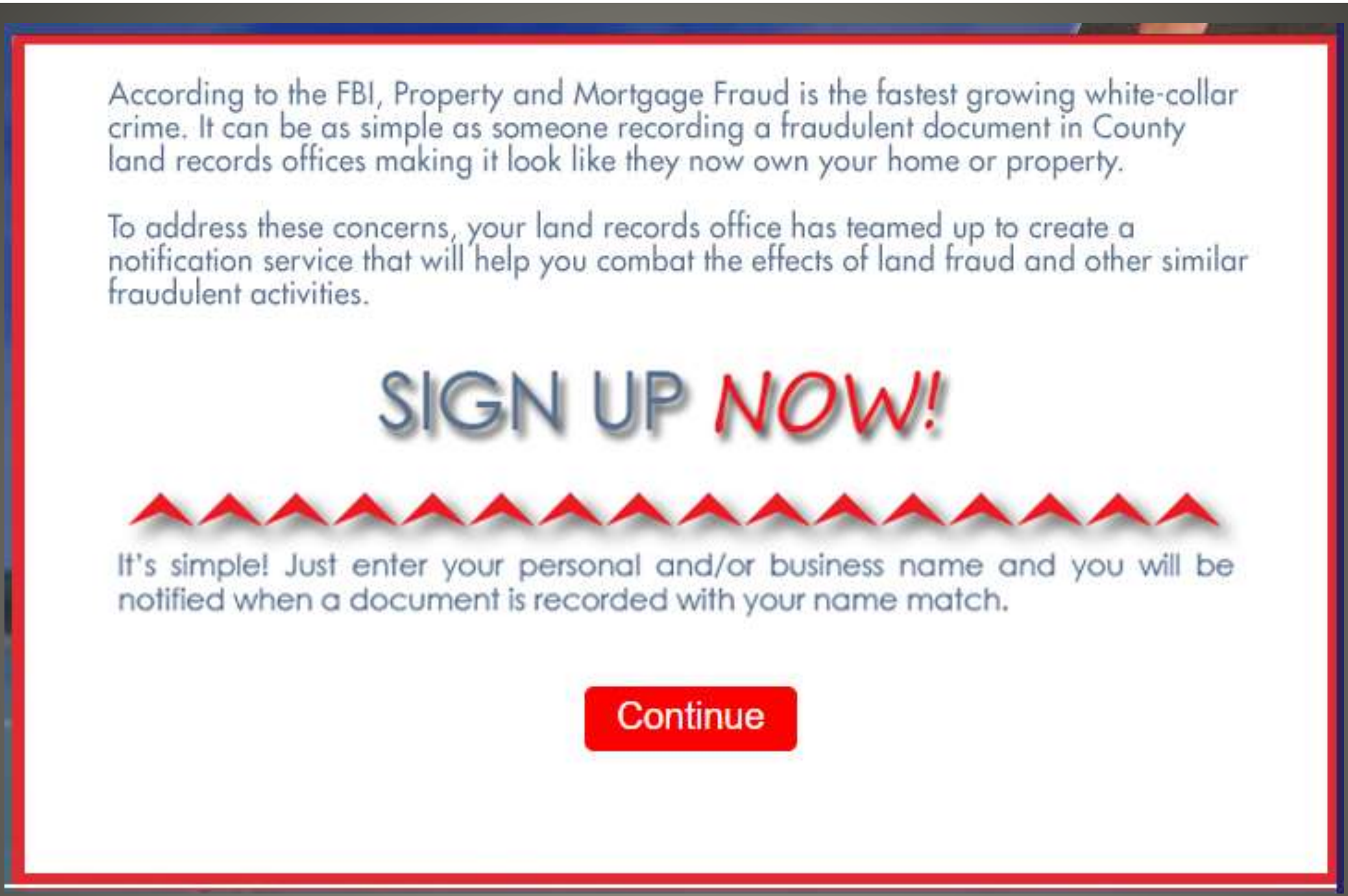
● Email ○ Voice Phone Call

Email

Confirm Email

(512) 943-1515
Monday through Friday between the hours of 8:00 a.m. - 5:00 p.m. CST.
PO Box 18, Georgetown, TX 78627
Williamson County Clerk, All rights reserved.

Property Fraud



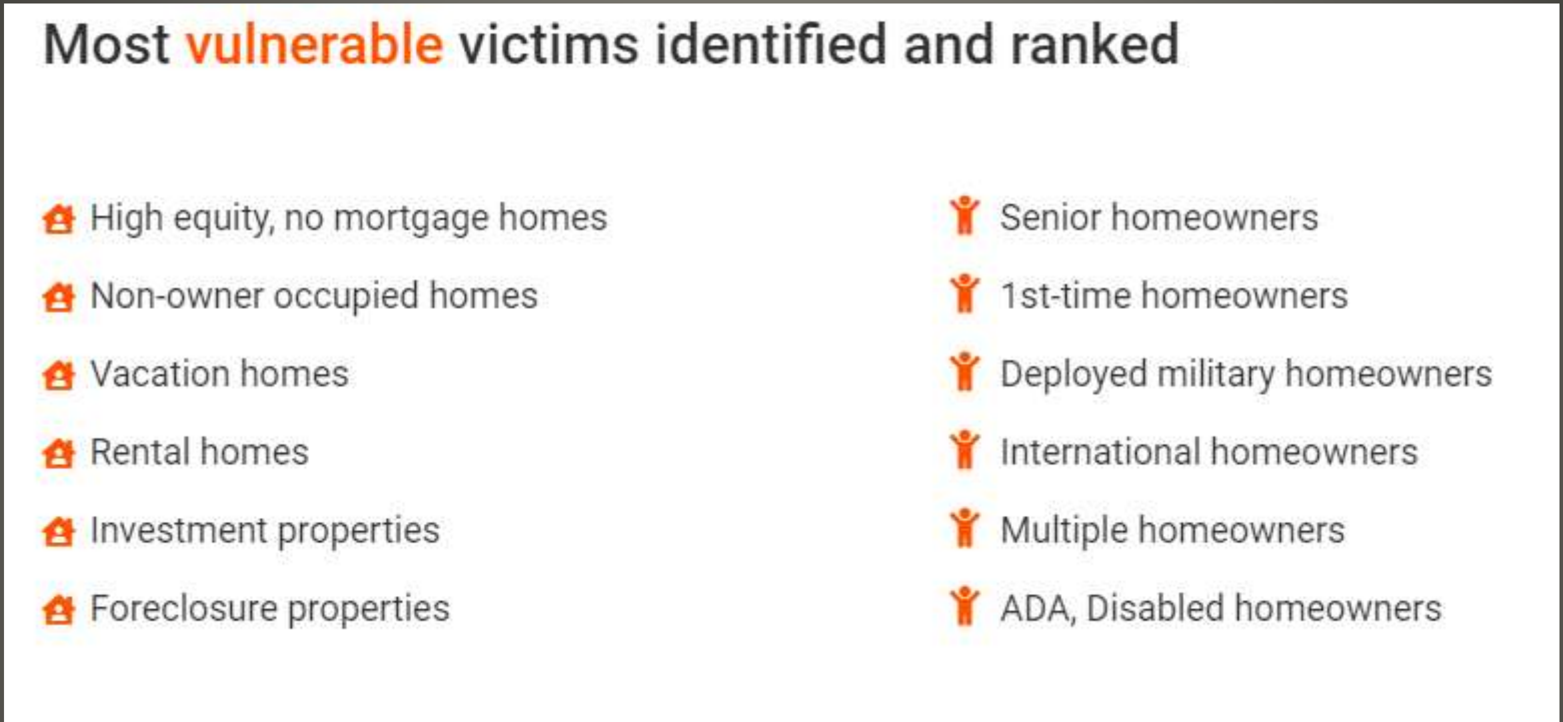
According to the FBI, Property and Mortgage Fraud is the fastest growing white-collar crime. It can be as simple as someone recording a fraudulent document in County land records offices making it look like they now own your home or property.

To address these concerns, your land records office has teamed up to create a notification service that will help you combat the effects of land fraud and other similar fraudulent activities.

SIGN UP NOW!

It's simple! Just enter your personal and/or business name and you will be notified when a document is recorded with your name match.

Property Fraud



Most vulnerable victims identified and ranked

- High equity, no mortgage homes
- Non-owner occupied homes
- Vacation homes
- Rental homes
- Investment properties
- Foreclosure properties

- Senior homeowners
- 1st-time homeowners
- Deployed military homeowners
- International homeowners
- Multiple homeowners
- ADA, Disabled homeowners

Property Fraud

Property Fraud

- To prevent property fraud

  just provide this website with every PII to commit property fraud
- Today many entities will easy cash any property

- And devices along for the ride
- Insurance monitors

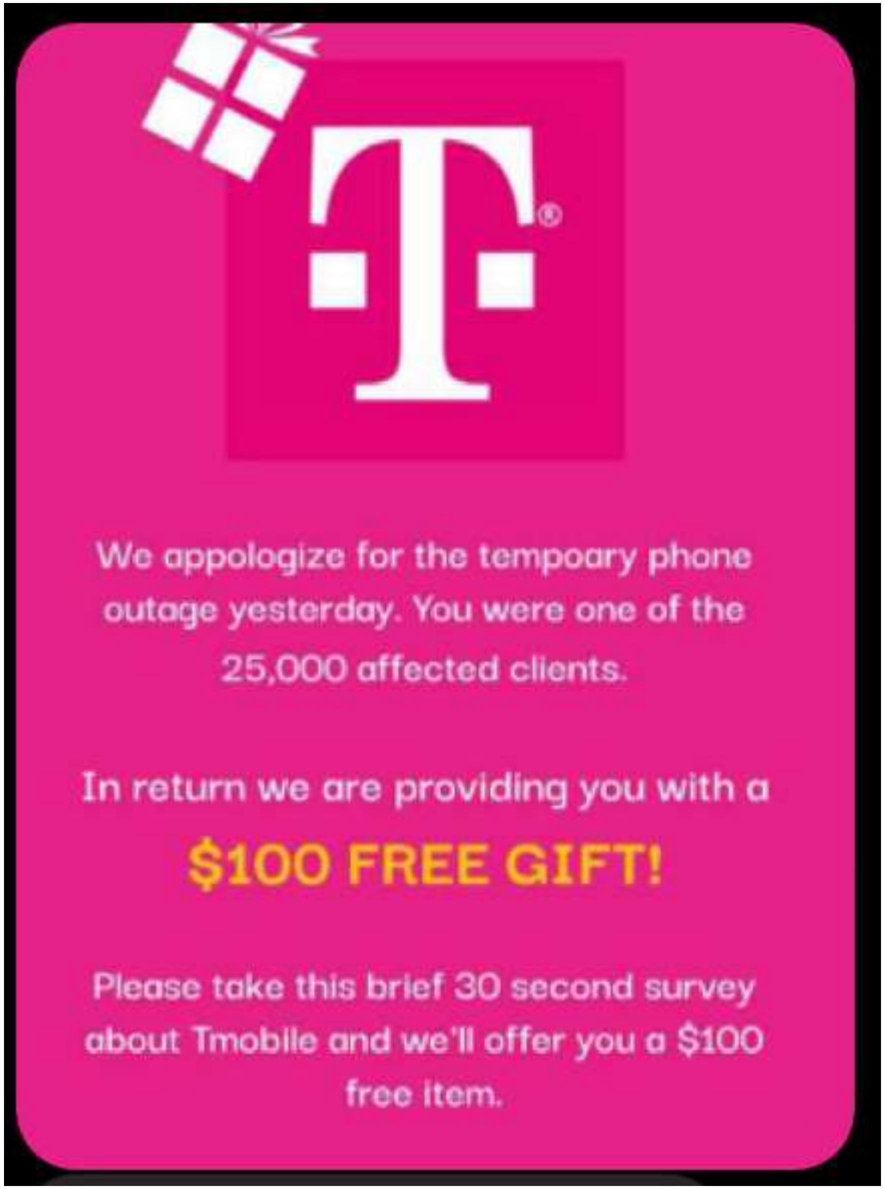
  Save $ iff you never ever …

  Otherwise
- Smart devices phones, tablets, game consoles
- Garmin camera, microphone, SD card

- 1 – 2 Terabytes/day
- Not wiped

  dealership, auto shop, wrecking yard

Automobile data collection



We appologize for the tempoary phone outage yesterday. You were one of the 25,000 affected clients.

In return we are providing you with a

$100 FREE GIFT!

Please take this brief 30 second survey about Tmobile and we'll offer you a $100 free item.

- 7 data breaches in past 4 years
- Ask if T-Mobile in your area?
- Group texts thus unable to block

T-Mobile

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com