

Sun City Computer Club

Cyber Security SIG

June 16, 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???

SCCCCyber

Monday, June 13, 2022

Williamson County Officials reporting jury scam calls

Williamson county district clerk's office reports that residents of Williamson county are receiving calls informing them they have failed to report for jury duty and must pay a fine to avoid arrest. The call tells the called party to report to district clerk Lisa David at the justice center to remove the warrants.

The Williamson district clerk has indicated no authority to make such calls are authorized.

If you receive such calls, the Williamson county sheriff's office requests reporting the incident at 512-943-1300.

Posted by John Jenkinson at 2:23 PM No comments:



Saturday, June 11, 2022

Chromium Based Browser Updates about June 10

Almost every Chromium based browser has security updates available.

Chrome, Brave, Opera, Vivaldi, Tor, Edge, Torch, ...

Security Updates. Not much in media on the vulnerability. Which is usually a sign to update with urgency.

Blog Archive

- ▼ 2022 (41)
 - ▼ June (2)
 - Williamson County Officials reporting jury scam calls
 - Chromium Based Browser Updates about June 10
 - May (7)
 - April (15)
 - March (8)
 - February (3)
 - January (6)
- 2021 (53)
- 2020 (56)
- 2019 (28)
- 2018 (57)
- 2017 (62)
- 2016 (16)

- Follina patch
- 60 vulnerabilities
- 9.8

Microsoft Patch Tuesday

- May 13 Enquiring Minds recording Georgetown Police Department warning Square devices



Enquiring Minds Square warning

- Hack
 - Disable encryption
 - Do not use authentic Square reader app
 - “oops, use this one” switch device
- Express Transit
- Relay
- Capture, Store, Attack

Square Reader Caution

- Counterfeit \$100 bill under windshield wiper
- Wine Delivery \$3.50
- Garmin storage card swap
- Telalaska
- NRO Anti-Fraud group
- Self Defense club Self & Home Security SIG
- Williamson County Jury duty

Recent scams



100

ONE HUNDRED DOLLARS

100

D₃
THIS IS NOT A LEGAL TENDER

FOR
MOTION PICTURE
USE ONLY

DB 66688803Z

THIS IS NOT LEGAL IT IS TO
BE USED FOR MOTION PROPS

C4 COPY



July 4, 1776



Prof movie money
Secretary
Suzanne
Treasurer

DB 66688803Z

SERIES
2017
A

100

100

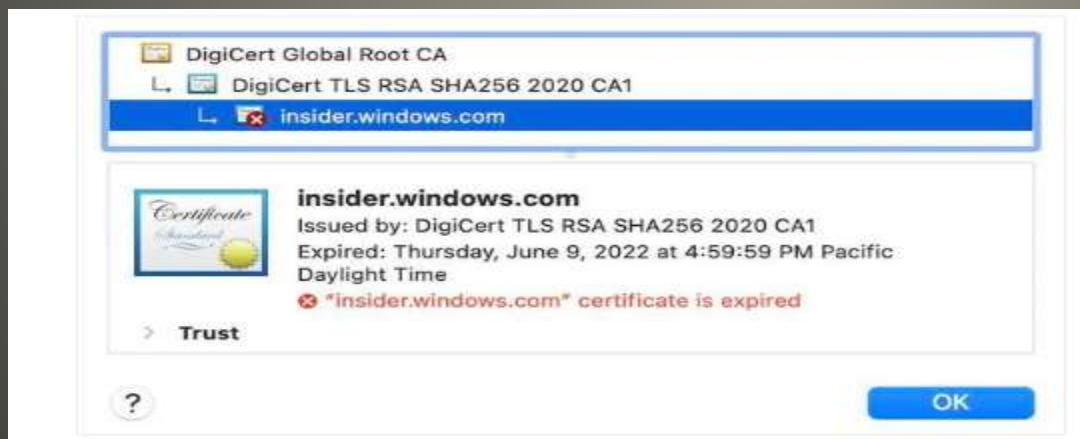
- India law
 - store user data for at least 5 years
 - ExpressVPN to remove servers from India
- Google Account > Security > Your Devices
- Fraud/scam Flags
 - Urgency, any ole link, truthful, over share, open profiles, free apps, history too full, older installs, Multi Factor Authentication, Update, Update everything, public Wi-Fi, check financials often, new financial protections

Current Issues

- Was extension -
ability to add comments to web sites
then browser fork from Brave
free speech goal
now abandoned
searchers now get “driver updates” offer

Dissenter browser

- LastPass mobile app no master password required
- Countries shutting down Internet
During student exams
- Windows Defender Endpoint “contain”
unmanaged devices
- Microsoft insider.windows.com cert expired



Current Issues

- Digital License Plates
Arizona, California, Michigan,
Monthly subscription fee



Current Issues

- Meeting Owl
Exposure: names, email, IP, geo locations
Online database
IPC exposure
Bluetooth access - NO passcode
Wireless access point mode protections
Whiteboard images easily available
- Linux Symbiote
Remote access to any account
Evades discovery
LD_PRELOAD
Filters library loads
Filters monitoring captures

Current Issues



Meeting Owl

- Drop support for Manifest v2 January 2023
- Manifest V3
- uBlock Origin, Privacy Badger, etc.
- Limits innovation
- Caps capabilities
Helpful <-> Harmful

Chromium Extensions

- Machine Learning 2.5 times better
- Gmail spam, web notifications, Maps, etc.
- Data never leaves Chromebook, tablet, phone

Google Chrome

- Data infiltrated using music sheets
- AlphaBay revived
- Bitcoin decline Celsius Network freeze withdrawals
- DOJ using court orders to remove malware from users' computers
Fourth amendment
Lisa Monaco
last resort & potential harm

Current Issues

- *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Fourth Amendment text

- *persons, houses, papers, and effects*

Then the cloud

Fourth Amendment

- Joint advisory
- NSA, FBI, CISA
Cybersecurity & Infrastructure Security Agency
- Foothold -> Critical users & infrastructure
- SQL databases, routers, firewalls, logs
- THE KEYS

Chinese hackers US Telco years

- Not Printers Computers that can print and Fax, And copy And scan
Scanned documents stored for later
- Firmware Updates every 6 months
Via network Via printer app
- Limit access
- Off network always most of the time
- Strong passphrase change often
- Monitor logs settings consumables
- Avoid consumables subscriptions

Secure Printer



Hi [REDACTED],

We'd like to extend an invitation to our Anchorage residents.

Please see the link shown below for details and contact us with any other questions.

[Access our newest incentives for \[REDACTED\]](#).

Thank you,

[REDACTED]

SunCity | P.O. Box 534, Austin, TX 78767

To stop receiving our mail, please [unsubscribe](#)



"I don't get it... we keep changing the password and we still have a leak!"

- VPN

Java functions

`Intl.DateTimeFormat().resolvedOptions()`

Timezone

`Date().toLocaleString()`

Local time

The screenshot shows a web browser window with the URL `vytal.io`. The page features the Vytal logo and navigation buttons for "Download Extension" and "Source Code". The main content area displays scan results for two functions: `Intl.DateTimeFormat().resolvedOptions().locale` and `Intl.DateTimeFormat().resolvedOptions().timeZone`. Each function's results are presented in a table with columns for the execution context (Top Window, Initial Load, Frame, Web worker), the detected value, and a status indicator (green checkmark for no tampering, red X for tampered data).

Intl.DateTimeFormat().resolvedOptions().locale

| | | |
|--------------|-------|---|
| Top Window | en-US | ✓ |
| Initial Load | en-US | ✓ |
| Frame | en-US | ✓ |
| Web worker | en-US | ✓ |

Intl.DateTimeFormat().resolvedOptions().timeZone

| | | |
|--------------|------------------|---|
| Top Window | America/New_York | ✓ |
| Initial Load | America/New_York | ✓ |
| Frame | America/New_York | ✓ |
| Web worker | America/New_York | ✓ |

new Date().getTimezoneOffset()

| | | |
|--------------|-----|---|
| Top Window | 240 | ✓ |
| Initial Load | 240 | ✓ |
| Frame | 240 | ✓ |
| Web worker | 240 | ✓ |

New York User using VPN - London

- Identity theft is misnomer
- Identity cloning?
- Services
 - Monitoring
 - Alerts
 - Recovery Insurance element
 - email advice
 - Providers: LifeLock, ID Watchdog, Identity Force, Credit Karma

To enroll you provide your IDentity

Identity Theft protection?

- Monitor credit reports
- Alert on changes
- Insurance protections to varying degrees
- Check if medical care using your identity
- Most cited services are free

Credit Monitoring

- Freeze free
- Lock paid
- Three credit bureaus (more actually)
- Freeze and Unfreeze

- Fraud Alerts
- Initial - one year
- Active Duty - military on deployment
- Extended - 7 years

Credit Freeze vs Credit Lock

- The major players

Apple, Microsoft, Google

May 5 Password Day

passphrase, please

committed to build passwordless authentication

Phones or smart devices

PIN, drawing pattern, fingerprint, facial ID, etc.

Simplicity & security

Password capture

Yeahbut lose THE device ...

Passkey May cyber security presentation

- W3C consortium approval
- BUT refit will be needed/required
- Web server with public key
generates a random nonce
sends to browser
signs and returns nonce to server
server checks with the public key

WebAuthn






- Google
google.com/devices

**Who Else is using your Gmail,
Facebook, Netflix accounts?**

← Your devices

Where you're signed in

You're currently signed in to your Google Account on these devices. [Learn more](#)

| | | |
|---|---|---|
|  Windows California, USA This device More details | New  Galaxy A12 United States 51 minutes ago More details |  iPad United States Jan 29 More details |
|  Nexus 5X California, USA Jan 3 More details |  Home Helpful home devices kitchen and 6 more devices More details | |

Where you've signed out

You've signed out of your Google Account on these devices in the last 28 days

Note: If you've given third-party apps on these devices access to your Google Account, some apps might still have account access. [Manage app access](#)

| | | |
|--|--|---|
|  iPad United States Last activity: Jan 27 Signed out More details |  Moto g(7) white United States Last activity: Jan 21 Signed out More details |  Mac United States Last activity: Dec 11, 2021 Signed out More details |
|--|--|---|

- Facebook

Sign in > Settings & Privacy > Settings
Security and Login

**Who Else is using your Gmail,
Facebook, Netflix accounts?**

General

Security and Login

Your Facebook Information

Privacy

Timeline and Tagging

Stories

Location

Blocking

Language and Region

Face Recognition

Notifications

Mobile

Public Posts

Apps and Websites

Instant Games

Business Integrations

Ads

Payments

Support Inbox

Videos

Security and Login

Where You're Logged In



Windows PC · [blurred]

Firefox · Active now



Samsung Galaxy Note 10+ · [blurred]

Messenger · 3 hours ago



Windows PC · [blurred]

Firefox · 15 hours ago



Samsung Galaxy Note 10+ · [blurred]

Facebook app · 16 hours ago



Windows PC · [blurred]

Firefox · October 10 at 10:44 AM



Samsung Galaxy Note 8 · [blurred]

Messenger · September 4 at 9:43 AM



Samsung Galaxy Note 8 · [blurred]

Facebook app · September 4 at 9:43 AM

See Less

Log Out Of All Sessions

- Netflix
- Account > Settings > Recent device streaming activity

**Who Else is using your Gmail,
Facebook, Netflix accounts?**

Recent device streaming activity

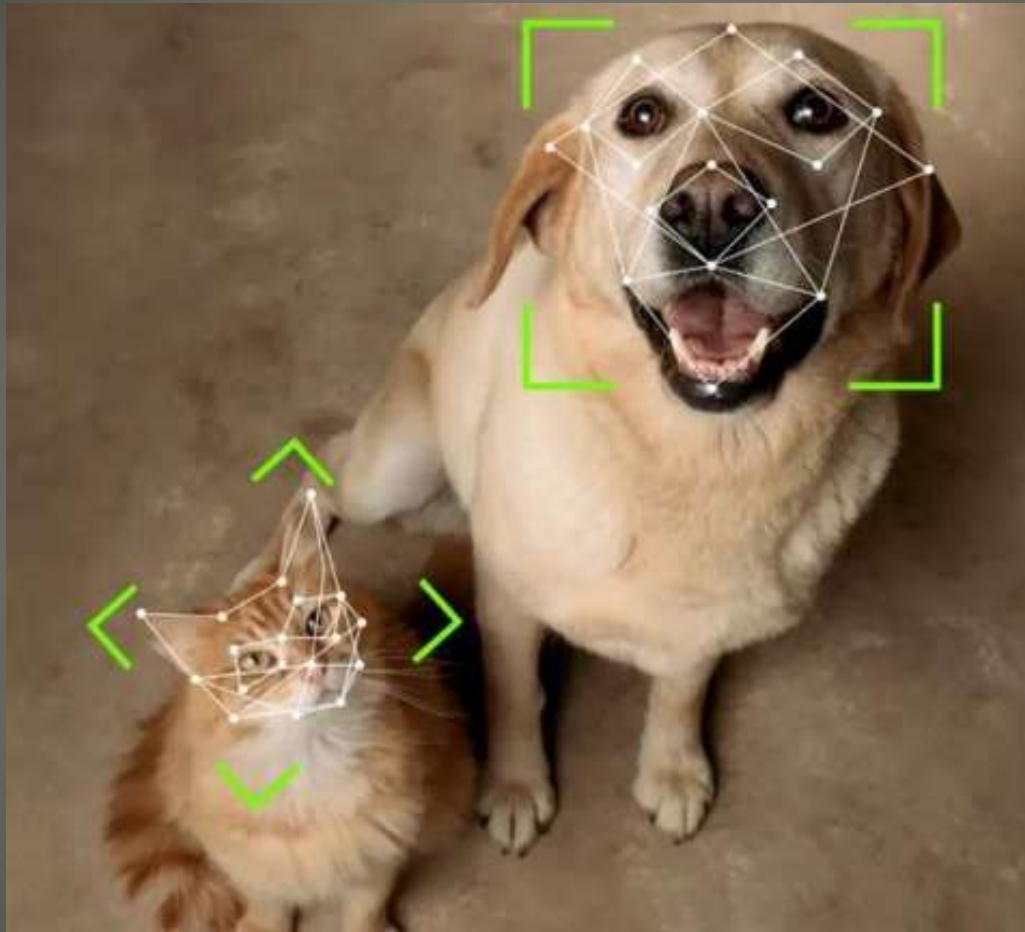
The most recently used devices and locations on your account.

Devices that were signed out of your account more than 60 days ago are not displayed.

| Last Used | Location | Device |
|---------------------------|-------------------------------------|----------|
| 1/20/19, 8:51:21 AM GMT-7 | United States (CO) 73.229.150.97 | Computer |
| 1/19/19, 5:15:08 PM GMT-7 | United States (CO) 73.229.150.97 | Apple TV |
| 1/18/19, 5:36:36 PM GMT-7 | United States (CO) 73.229.150.97 | Smart TV |
| 1/18/19, 5:33:51 PM GMT-7 | United States (CO) 73.229.150.97 | Computer |
| 1/18/19, 6:33:19 PM CST | United States (AR) 45.56.151.122 | Computer |
| 1/15/19, 8:30:00 PM GMT-7 | United States (CO) 73.95.132.178 | Computer |

- Capital One data case
- Microsoft Windows 10 & 11 update Tuesday
- Kali Linux Penetration Testing Courseware
<https://help.offensive-security.com/hc/en-us/articles/6702904332564>
- Tesla NFC unlock 130 seconds enrolling a new key

Current Issues



Smart Pet Door

- 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