Questions, Issues,

Concerns, Suggestions

Welcome at any time

Even Now

Sun City Computer Club

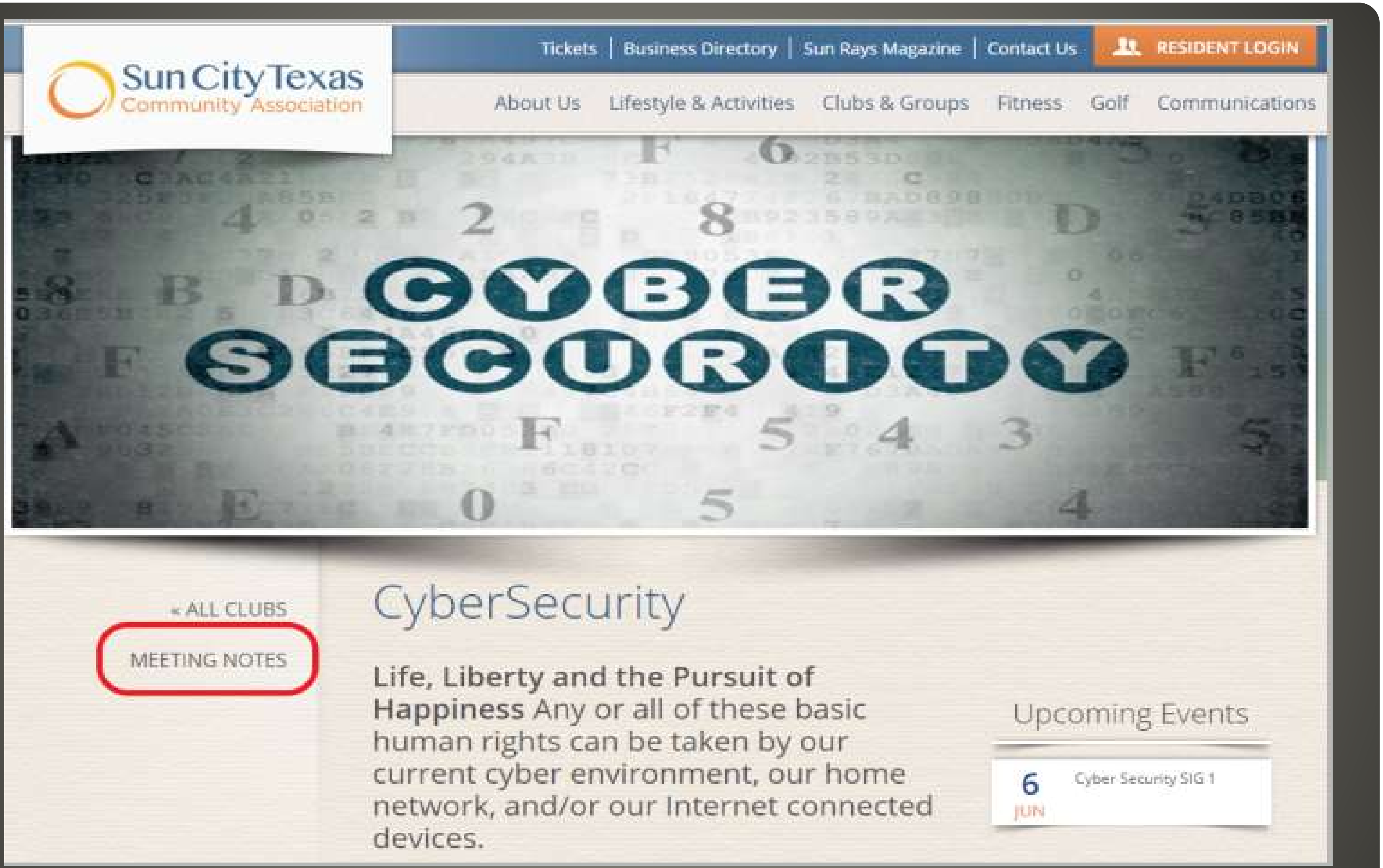
Cyber Security SIG

June 6, 2019

- Audio Recording of this session

- Audio Recording in Progress

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



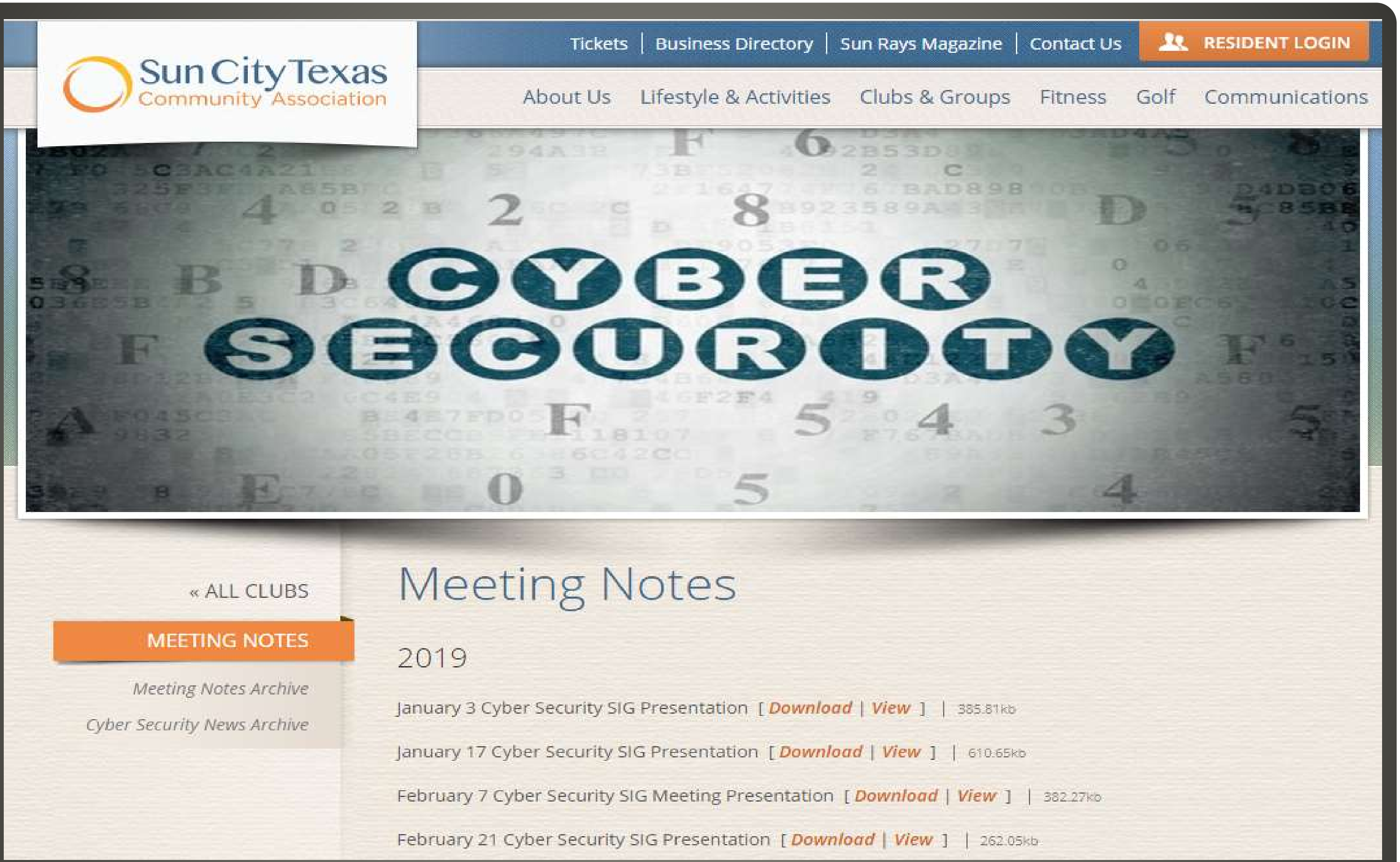
CyberSecurity

Life, Liberty and the Pursuit of Happiness Any or all of these basic human rights can be taken by our current cyber environment, our home network, and/or our Internet connected devices.

Upcoming Events

6 JUN Cyber Security SIG 1

Cyber Security SIG News



Meeting Notes

2019

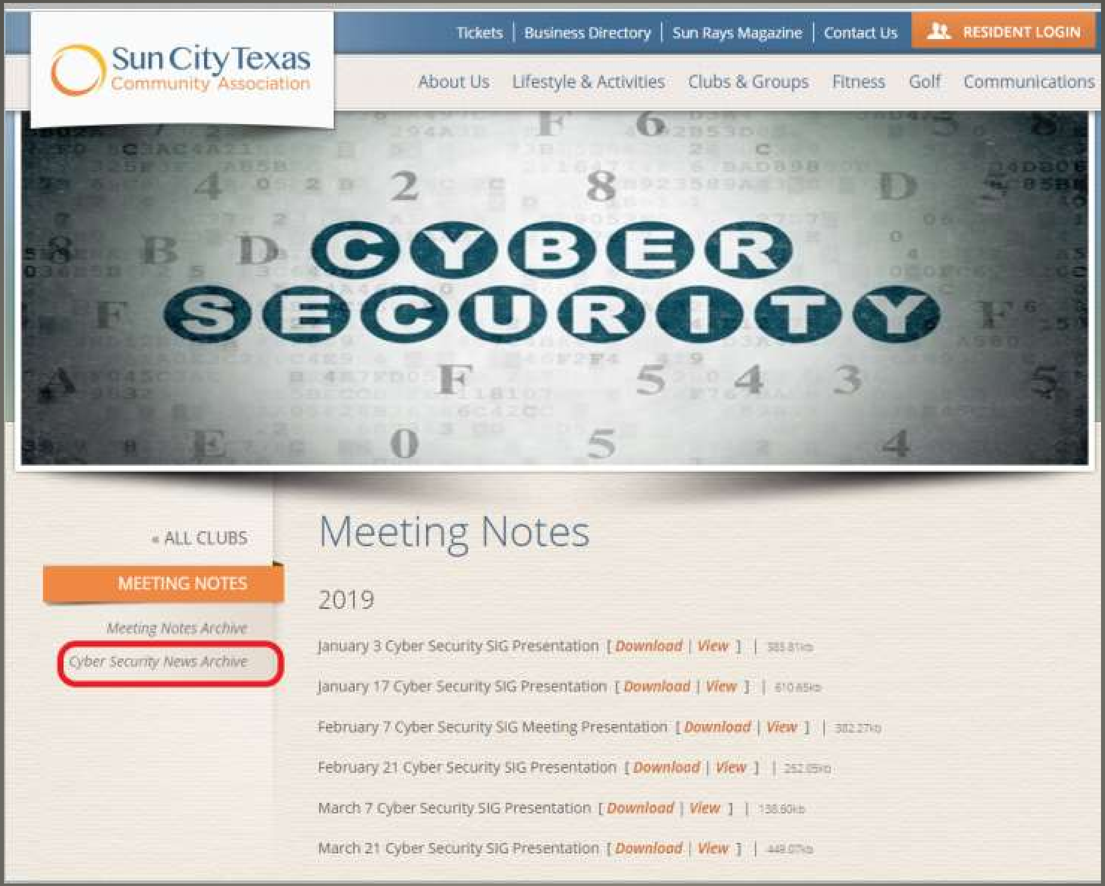
January 3 Cyber Security SIG Presentation [Download | View] | 385.81kb

January 17 Cyber Security SIG Presentation [Download | View] | 610.65kb

February 7 Cyber Security SIG Meeting Presentation [Download | View] | 382.27kb

February 21 Cyber Security SIG Presentation [Download | View] | 262.05kb

Cyber Security SIG News



Meeting Notes

2019

January 3 Cyber Security SIG Presentation [Download | View] | 385.81kb

January 17 Cyber Security SIG Presentation [Download | View] | 610.65kb

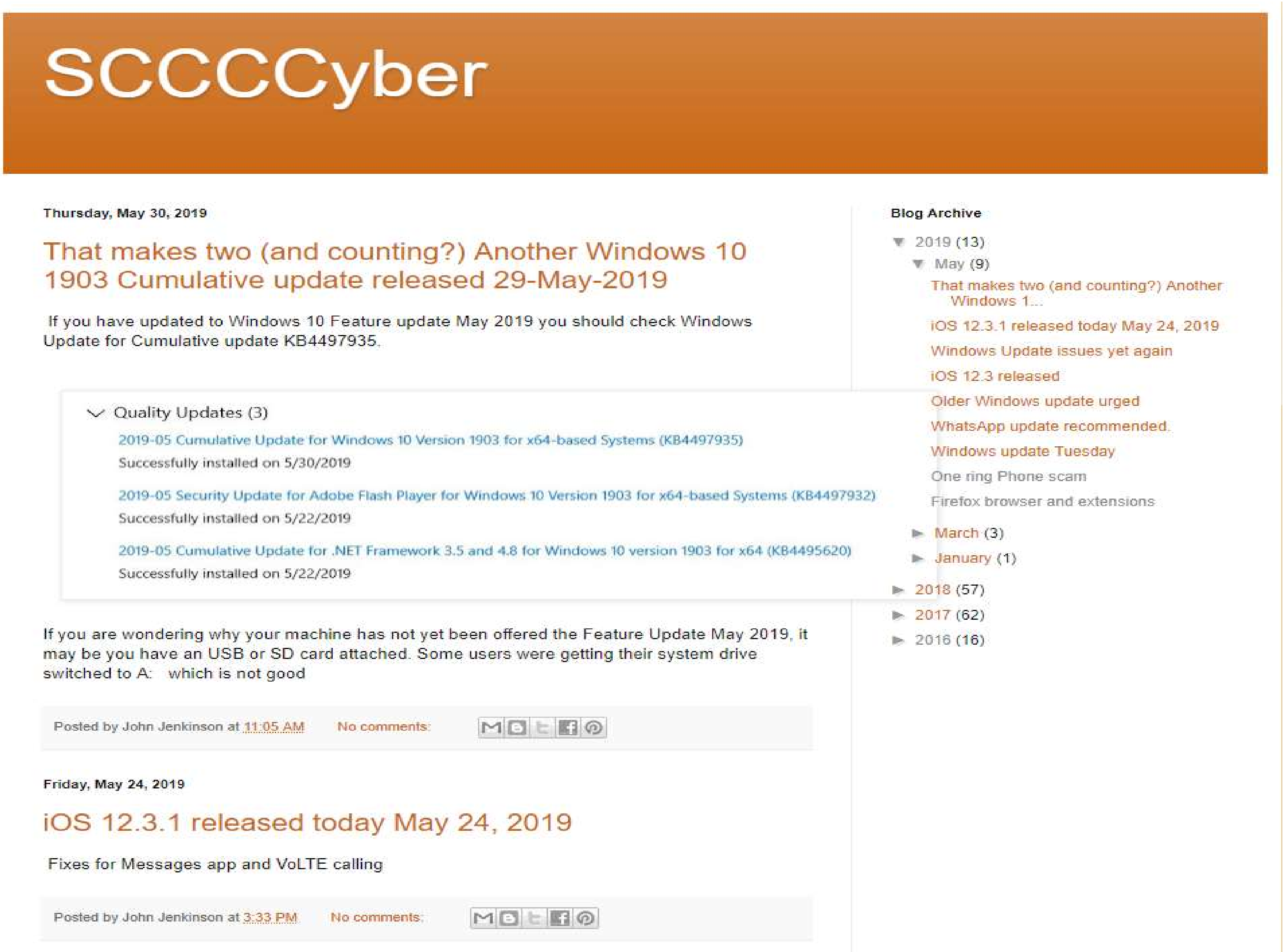
February 7 Cyber Security SIG Meeting Presentation [Download | View] | 382.27kb

February 21 Cyber Security SIG Presentation [Download | View] | 252.05kb

March 7 Cyber Security SIG Presentation [Download | View] | 138.60kb

March 21 Cyber Security SIG Presentation [Download | View] | 448.07kb

Cyber Security SIG News



SCCCyber

Thursday, May 30, 2019

That makes two (and counting?) Another Windows 10 1903 Cumulative update released 29-May-2019

If you have updated to Windows 10 Feature update May 2019 you should check Windows Update for Cumulative update KB4497935.

Quality Updates (3)

2019-05 Cumulative Update for Windows 10 Version 1903 for x64-based Systems (KB4497935)
Successfully installed on 5/30/2019

2019-05 Security Update for Adobe Flash Player for Windows 10 Version 1903 for x64-based Systems (KB4497932)
Successfully installed on 5/22/2019

2019-05 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 version 1903 for x64 (KB4495620)
Successfully installed on 5/22/2019

If you are wondering why your machine has not yet been offered the Feature Update May 2019, it may be you have an USB or SD card attached. Some users were getting their system drive switched to A: which is not good

Posted by John Jenkinson at 11:05 AM   No comments:

Friday, May 24, 2019

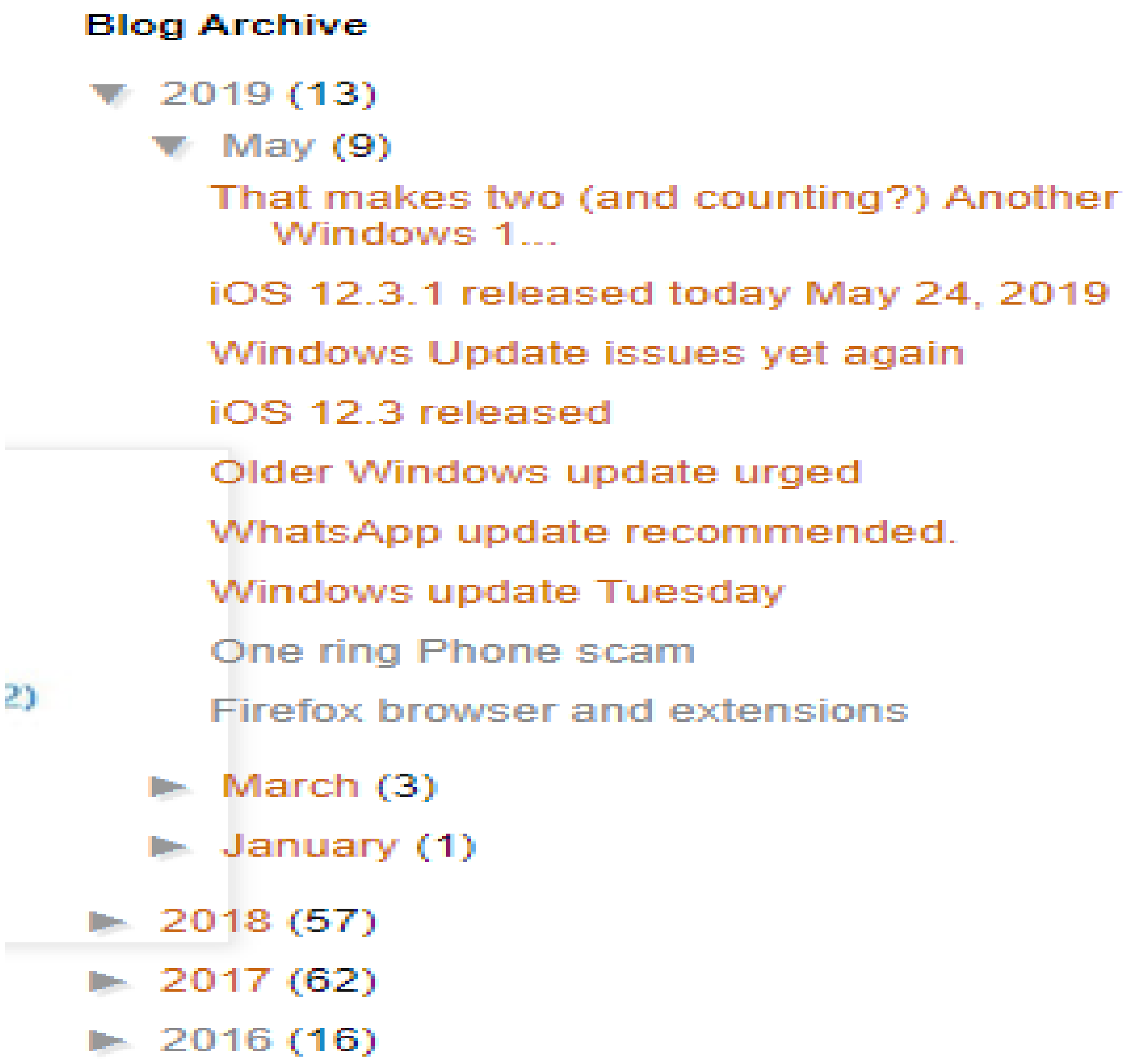
iOS 12.3.1 released today May 24, 2019

Fixes for Messages app and VoLTE calling

Posted by John Jenkinson at 3:33 PM   No comments:

Blog Archive

- ▼ 2019 (13)
  - ▼ May (9)
    - That makes two (and counting?) Another Windows 1...
    - iOS 12.3.1 released today May 24, 2019
    - Windows Update issues yet again
    - iOS 12.3 released
    - Older Windows update urged
    - WhatsApp update recommended.
    - Windows update Tuesday
    - One ring Phone scam
    - Firefox browser and extensions
  - ► March (3)
  - ► January (1)
- ► 2018 (57)
- ► 2017 (62)
- ► 2016 (16)



Blog Archive

- ▼ 2019 (13)
  - ▼ May (9)
    - That makes two (and counting?) Another Windows 1...
    - iOS 12.3.1 released today May 24, 2019
    - Windows Update issues yet again
    - iOS 12.3 released
    - Older Windows update urged
    - WhatsApp update recommended.
    - Windows update Tuesday
    - One ring Phone scam
    - Firefox browser and extensions
  - ► March (3)
  - ► January (1)
- ► 2018 (57)
- ► 2017 (62)
- ► 2016 (16)

- No Meeting June 20
- Sign in clarification
- Cyber Security SIG 1   first meeting of month first Thursday
- Cyber Security SIG 2   second meeting of month third Thursday
- Google cloud outage 6/2/2019
- Quest Diagnostic breach

Cyber Security SIG News

Current Issues

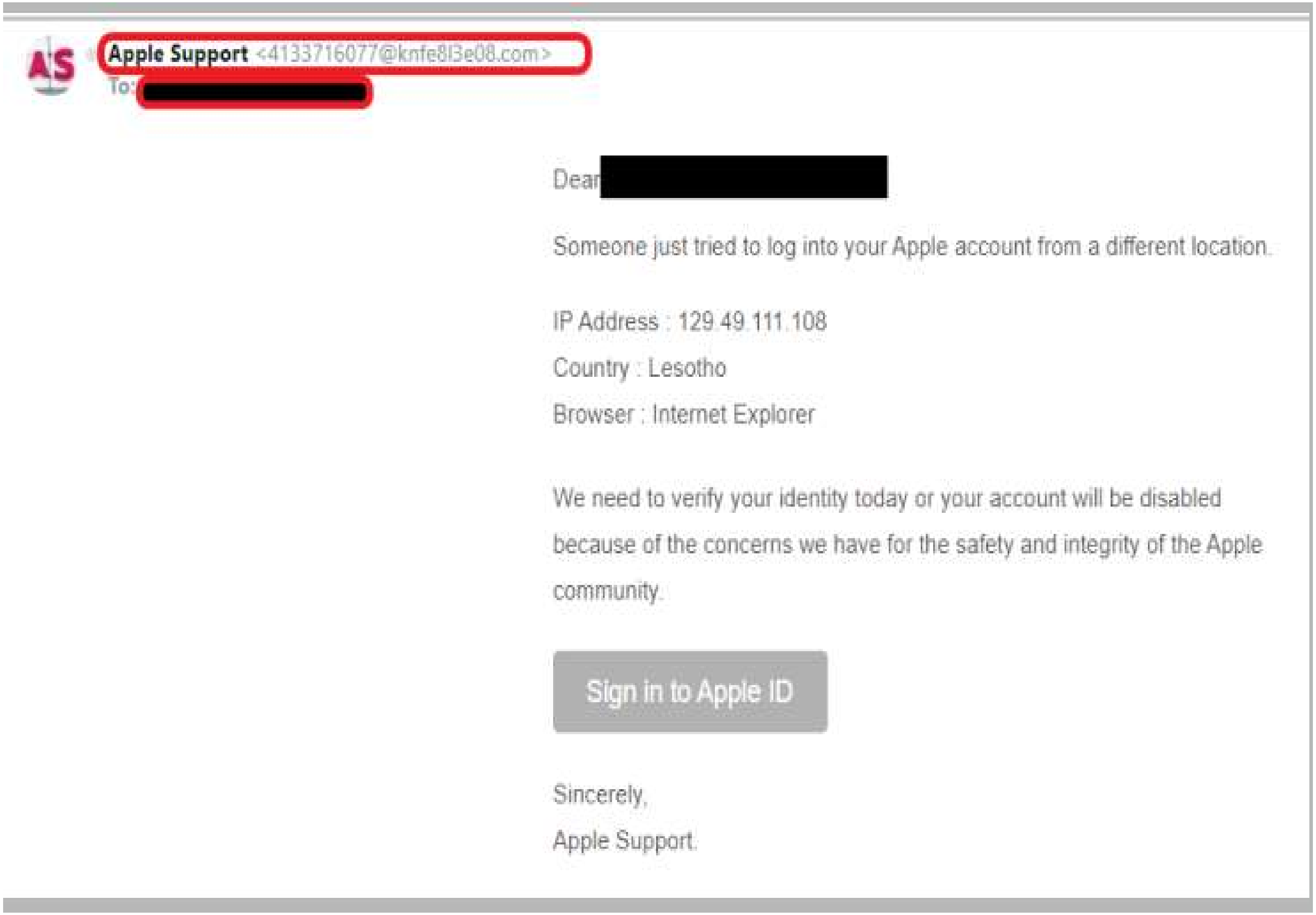
- Conscription of Cyber talent
- 5G vs. weather forecasting
- BlueKeep
- Robocall

Telephone Robocall Abuse Criminal Enforcement and Deterrence Act

TRACED

SHAKEN STIR

- Russian & Chinese move from MS



Apple Support <4133716077@knfe8l3e08.com>
To: [redacted]

Dear [redacted]

Someone just tried to log into your Apple account from a different location.

IP Address : 129.49.111.108

Country : Lesotho

Browser : Internet Explorer

We need to verify your identity today or your account will be disabled because of the concerns we have for the safety and integrity of the Apple community.

Sign in to Apple ID

Sincerely,

Apple Support.

Securing Smart Devices Part 1

- Smart phones
- Smart tablets
- Smart doorbells Security Cameras
- Smart speakers Echo, Google Home, Homepod, Cortana
- Smart power meters
- …………

Passphrases

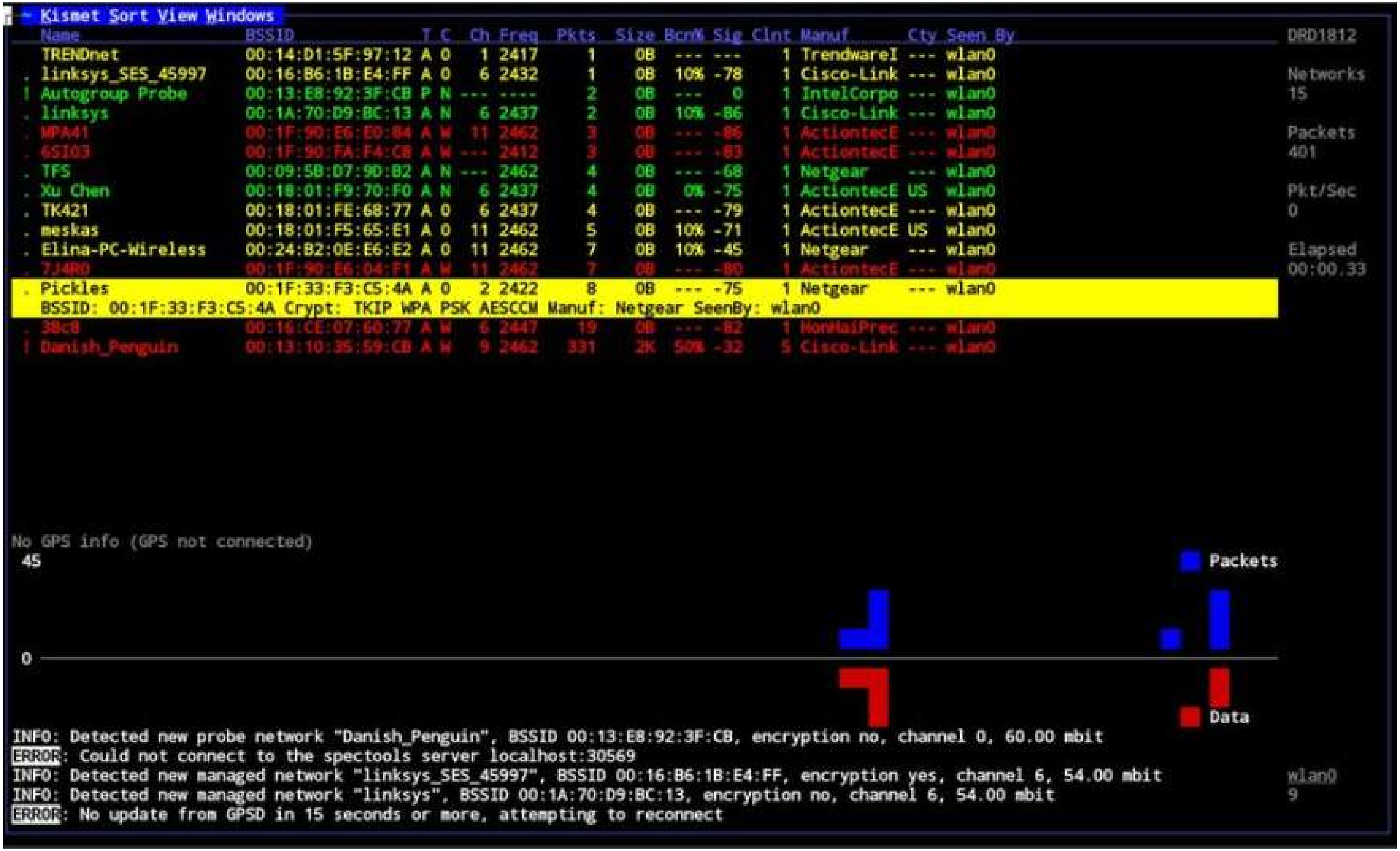
- NOT factory default
- Check passphrases often
- More than one passphrase (apps)
- After passphrase or settings change
  SAVE

- More than one Wireless Access Point
- Use tethered Cellular data for sensitive data
- Hardwired if possible   USB printer
- Devices are never “off”
- IPv6
- Chromecast
- shoden

Network Segmentation

- RADIO
- WEP WPA WPA-2 WPA-3
- Data portion ONLY

Wi-Fi Bluetooth ZigBee etc.



```
~ Kismet Sort View Windows
  Name                 BSSID             T C  Ch Freq  Pkts  Size Bcn% Sig Clnt Manuf      Cty Seen By       DRD1812
  TRENDnet             00:14:D1:5F:97:12 A O   1 2417     1    0B  --- ---    1 TrendwareI --- wlan0
. linksys_SES_45997    00:16:B6:1B:E4:FF A O   6 2432     1    0B  10% -78    1 Cisco-Link --- wlan0         Networks
! Autogroup Probe      00:13:E8:92:3F:CB P N --- ----     2    0B  ---   0    1 IntelCorpo --- wlan0         15
. linksys              00:1A:70:D9:BC:13 A N   6 2437     2    0B  10% -86    1 Cisco-Link --- wlan0
. MPA41                00:1F:90:E6:E0:84 A W  11 2462     3    0B  --- -86    1 ActiontecE --- wlan0         Packets
. 6SI03                00:1F:90:FA:F4:C8 A W --- 2412     3    0B  --- -83    1 ActiontecE --- wlan0         401
. TFS                  00:09:5B:D7:9D:B2 A N --- 2462     4    0B  --- -68    1 Netgear    --- wlan0
. Xu Chen              00:18:01:F9:70:F0 A N   6 2437     4    0B   0% -75    1 ActiontecE US  wlan0         Pkt/Sec
. TK421                00:18:01:FE:68:77 A O   6 2437     4    0B  --- -79    1 ActiontecE --- wlan0         0
. meskas               00:18:01:F5:65:E1 A O  11 2462     5    0B  10% -71    1 ActiontecE US  wlan0
. Elina-PC-Wireless    00:24:B2:0E:E6:E2 A O  11 2462     7    0B  10% -45    1 Netgear    --- wlan0         Elapsed
. 7J4R0                00:1F:90:E6:04:F1 A W  11 2462     7    0B  --- -80    1 ActiontecE --- wlan0         00:00.33
. Pickles              00:1F:33:F3:C5:4A A O   2 2422     8    0B  --- -75    1 Netgear    --- wlan0
  BSSID: 00:1F:33:F3:C5:4A Crypt: TKIP WPA PSK AESCCM Manuf: Netgear SeenBy: wlan0
. 38c8                 00:16:CE:07:60:77 A W   6 2447    19    0B  --- -82    1 HonHaiPrec --- wlan0
! Danish_Penguin       00:13:10:35:59:CB A W   9 2462   331    2K  50% -32    5 Cisco-Link --- wlan0

No GPS info (GPS not connected)
 45                                                                                            Packets

 0

                                                                                               Data
INFO: Detected new probe network "Danish_Penguin", BSSID 00:13:E8:92:3F:CB, encryption no, channel 0, 60.00 mbit
ERROR: Could not connect to the spectools server localhost:30569
INFO: Detected new managed network "linksys_SES_45997", BSSID 00:16:B6:1B:E4:FF, encryption yes, channel 6, 54.00 mbit   wlan0
INFO: Detected new managed network "linksys", BSSID 00:1A:70:D9:BC:13, encryption no, channel 6, 54.00 mbit             9
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
```

Router - Wireless Access Point

- THE key
- Into and out from your networks
- Not usually monitored
- Enable maximum logging

  Forensics

  Discard benign, investigate the rest

SmartTV

- Voice control
- Never “off”
- Ability to *know* your content

- OFF if unneeded
- Tape for camera
- Dummy plug for microphones
- Turn down gain
- Disable

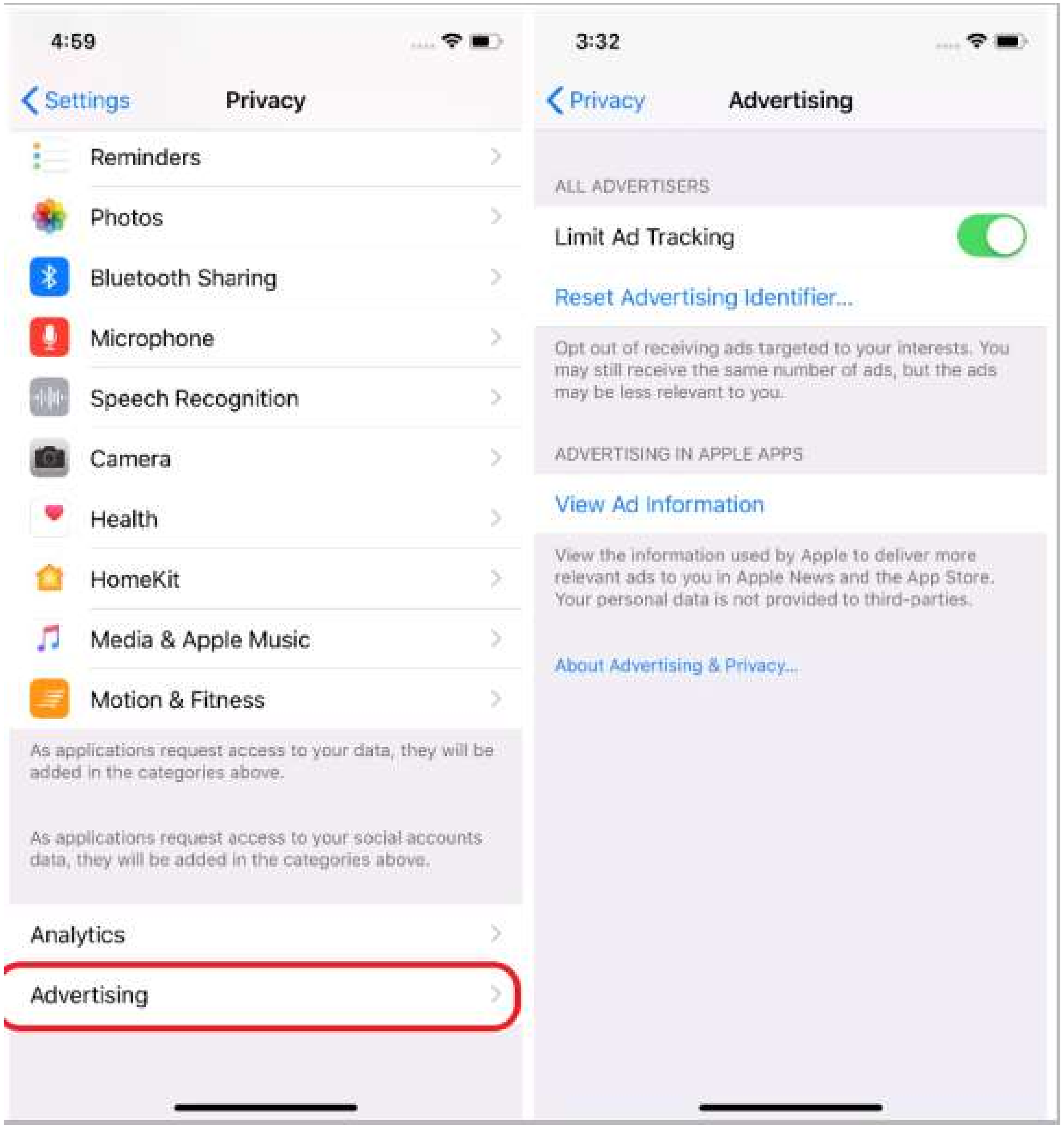
Cameras, Microphone, Speaker

- “call the sheriff”
- Law enforcement subpoena
- Keyword filters
- Other command sources (computer speakers, other home assistants)

Smart Home assistants

- Commodity devices
- Function over security
- Inability to update
- Ability to update
- Auto Update
- “backdoor”s
- Supply chain

Issues



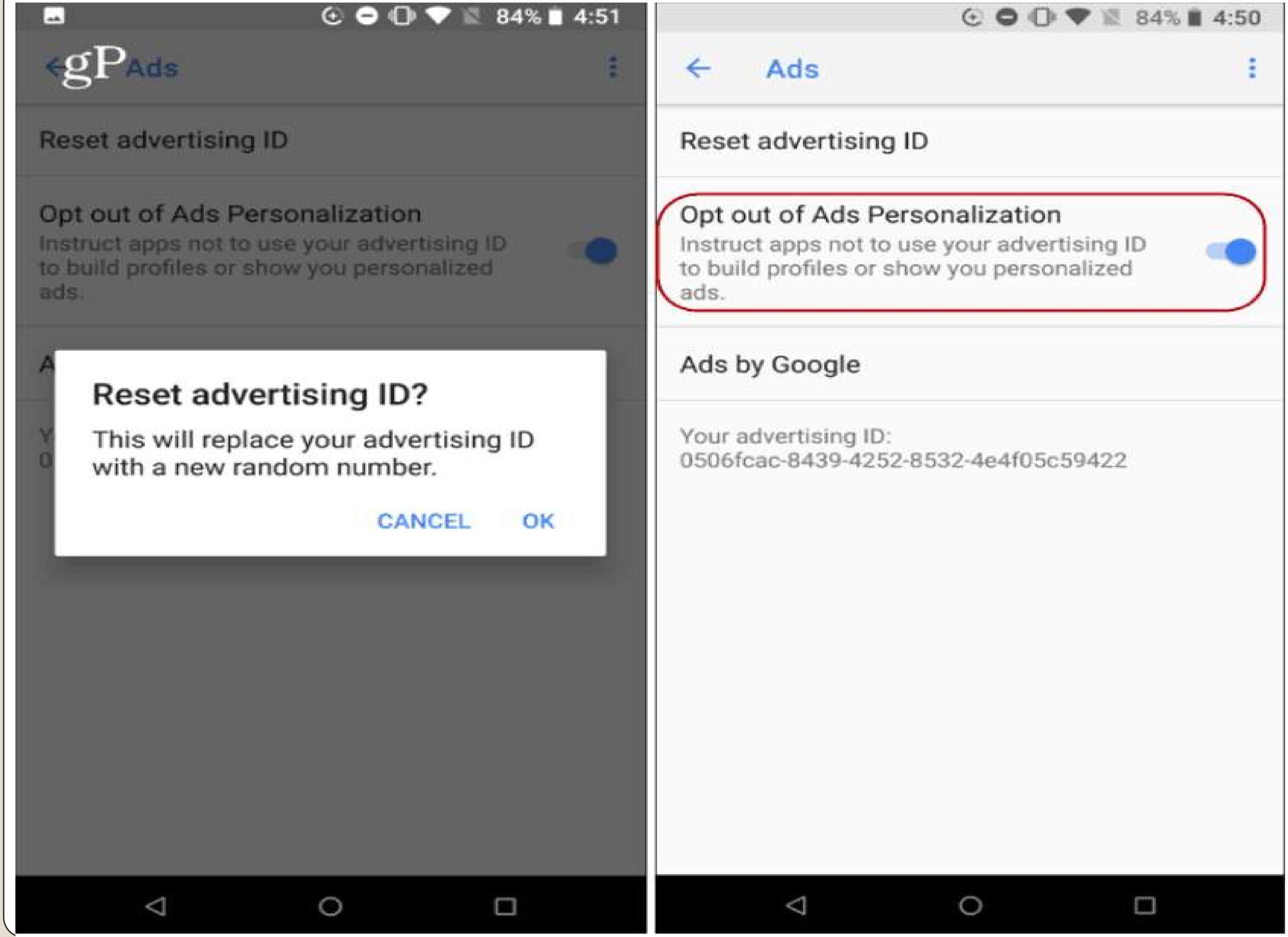
As applications request access to your data, they will be added in the categories above.

As applications request access to your social accounts data, they will be added in the categories above.

Limit Ad Tracking: on

Opt out of receiving ads targeted to your interests. You may still receive the same number of ads, but the ads may be less relevant to you.

View the information used by Apple to deliver more relevant ads to you in Apple News and the App Store. Your personal data is not provided to third-parties.



Reset advertising ID

Opt out of Ads Personalization
Instruct apps not to use your advertising ID to build profiles or show you personalized ads.

Reset advertising ID?

This will replace your advertising ID with a new random number.

Reset advertising ID

Opt out of Ads Personalization
Instruct apps not to use your advertising ID to build profiles or show you personalized ads.

Ads by Google

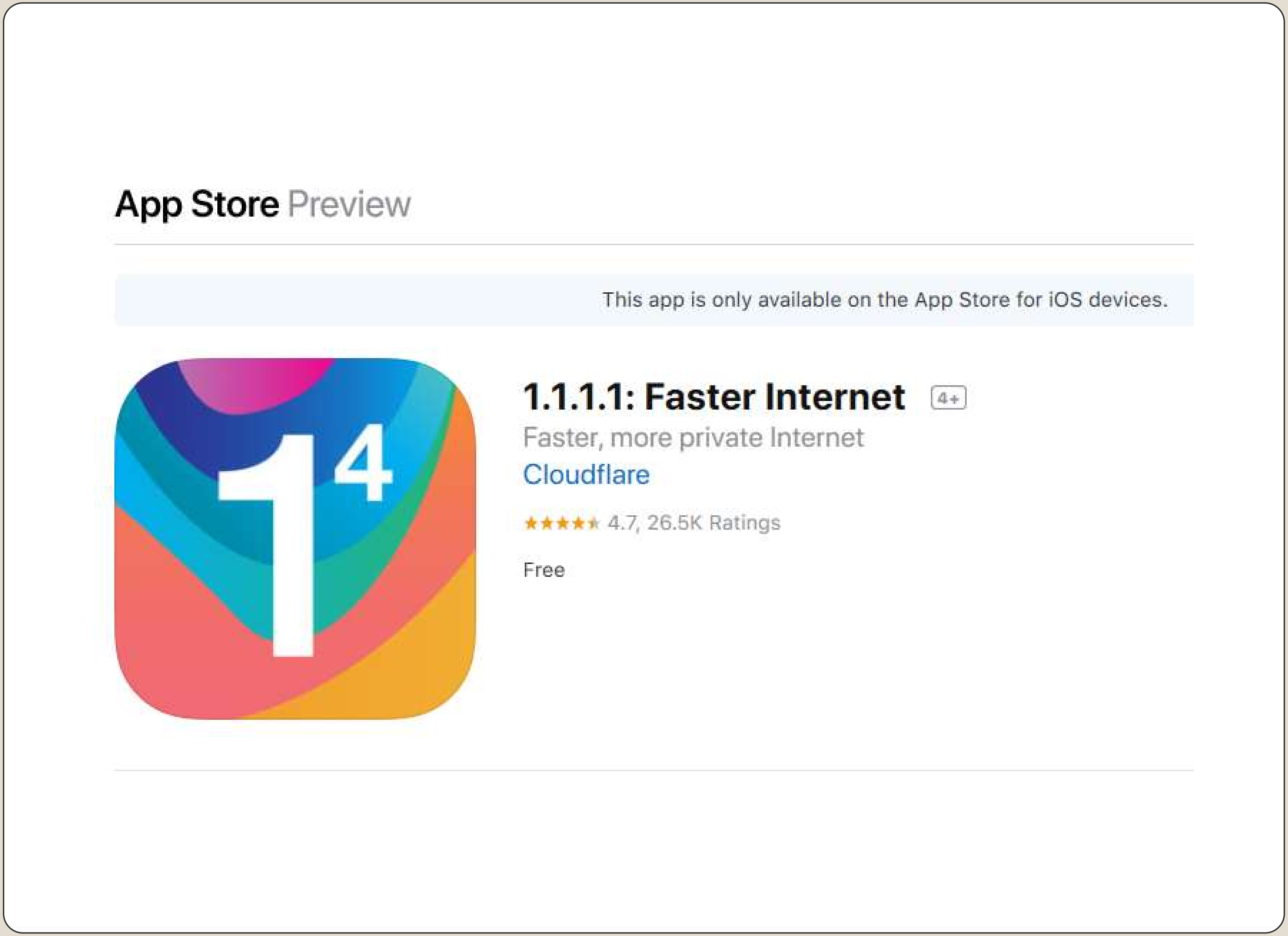
Your advertising ID:
0506fcac-8439-4252-8532-4e4f05c59422

Patching

- iOS
- Android
- Apps
- Settings

DNS

- Name resolution
- Easily spoofed
- 9.9.9.9 1.1.1.1



App Store Preview

This app is only available on the App Store for iOS devices.

1.1.1.1: Faster Internet 4+

Faster, more private Internet

Cloudflare

★★★★★ 4.7, 26.5K Ratings

Free

- Tortoise and Hare
- Chicken Little

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com

Questions?