Sun City Computer Club

Cyber Security SIG

April 15, 2021

Questions, Comments, Suggestions welcomed at any time

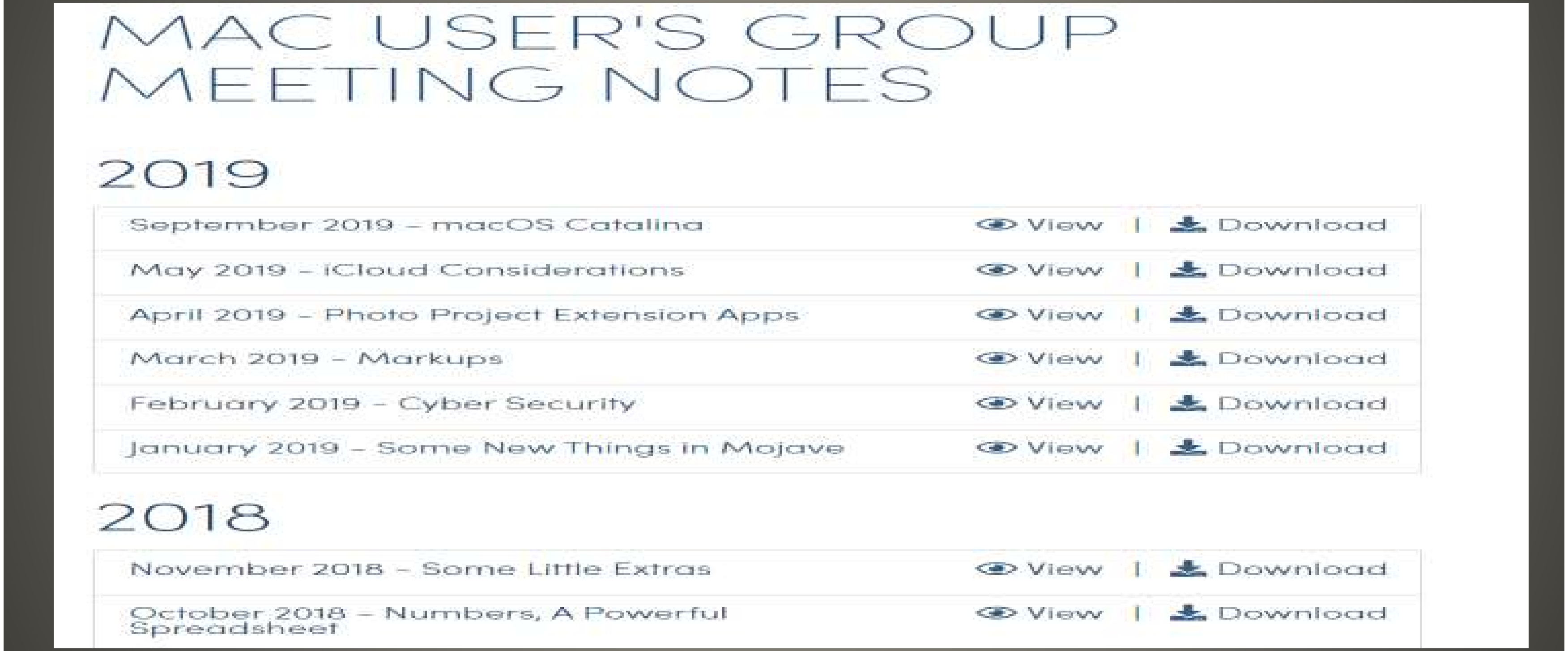
Even Now

- 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

Sun City Texas Community Association File Library Mac User's Group Meeting Notes (sctexas.org)



MAC USER'S GROUP MEETING NOTES

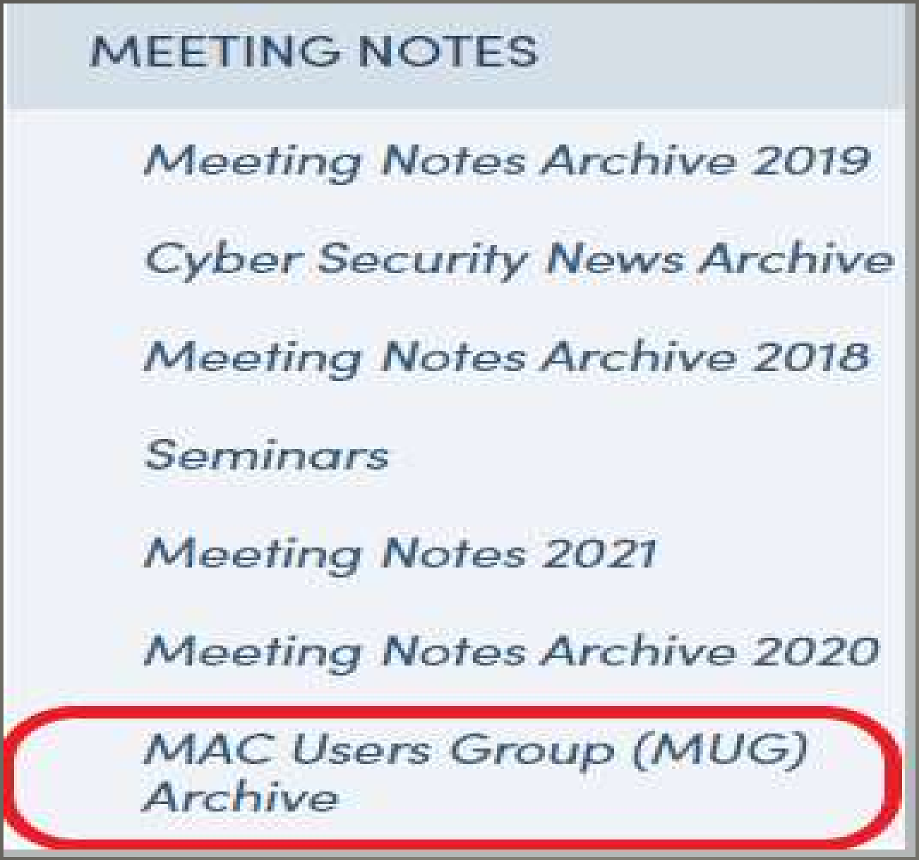
2019

September 2019 – macOS Catalina	View	Download
May 2019 – iCloud Considerations	View	Download
April 2019 – Photo Project Extension Apps	View	Download
March 2019 – Markups	View	Download
February 2019 – Cyber Security	View	Download
January 2019 – Some New Things in Mojave	View	Download

2018

November 2018 – Some Little Extras	View	Download
October 2018 – Numbers, A Powerful Spreadsheet	View	Download

MAC Users Group (MUG)



MEETING NOTES

Meeting Notes Archive 2019

Cyber Security News Archive

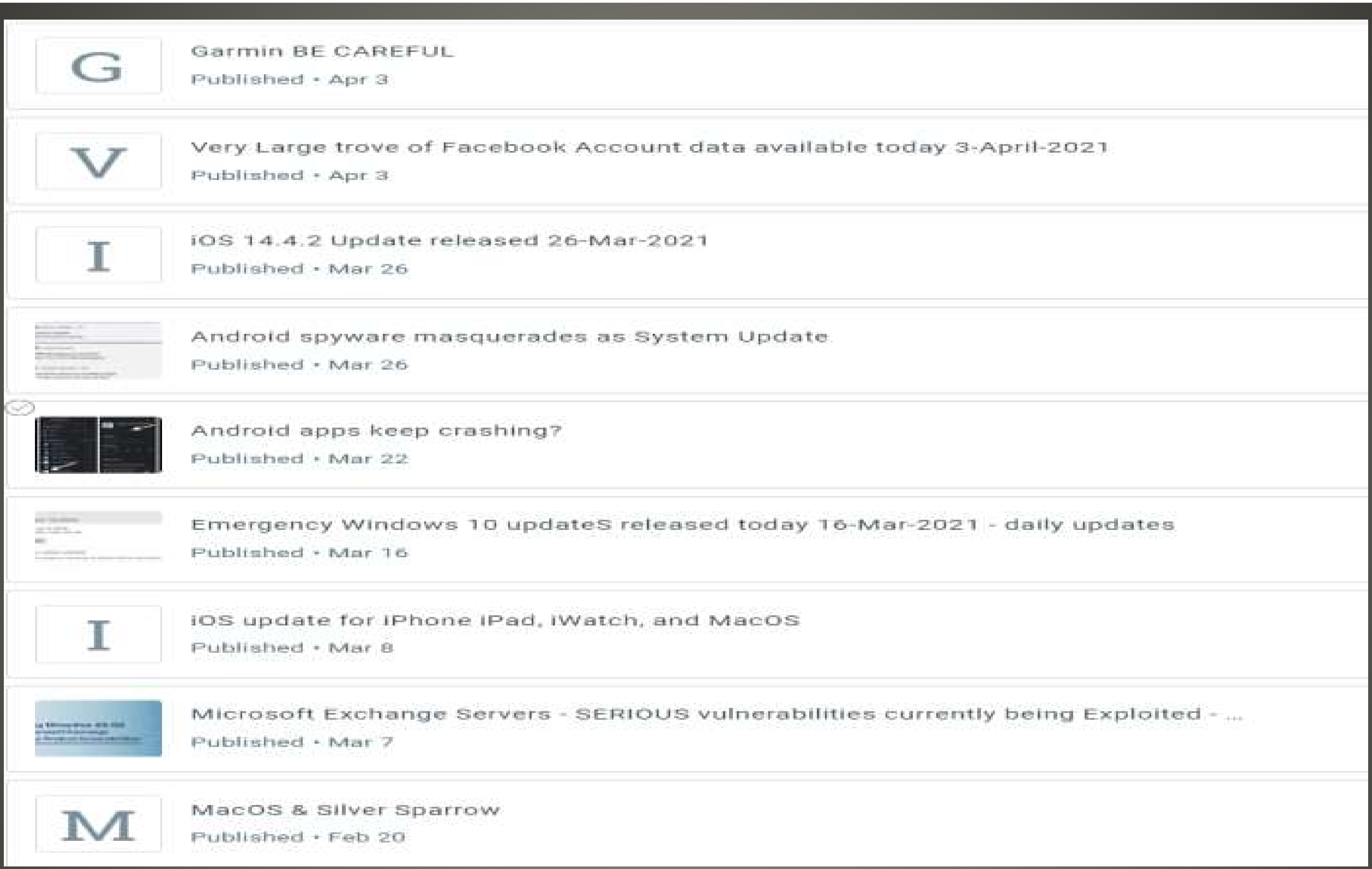
Meeting Notes Archive 2018

Seminars

Meeting Notes 2021

Meeting Notes Archive 2020

MAC Users Group (MUG) Archive



Garmin BE CAREFUL
Published • Apr 3

Very Large trove of Facebook Account data available today 3-April-2021
Published • Apr 3

iOS 14.4.2 Update released 26-Mar-2021
Published • Mar 26

Android spyware masquerades as System Update
Published • Mar 26

Android apps keep crashing?
Published • Mar 22

Emergency Windows 10 updateS released today 16-Mar-2021 - daily updates
Published • Mar 16

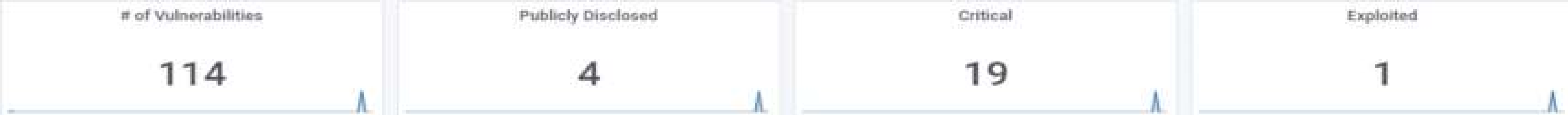
iOS update for iPhone iPad, iWatch, and MacOS
Published • Mar 8

Microsoft Exchange Servers - SERIOUS vulnerabilities currently being Exploited - ...
Published • Mar 7

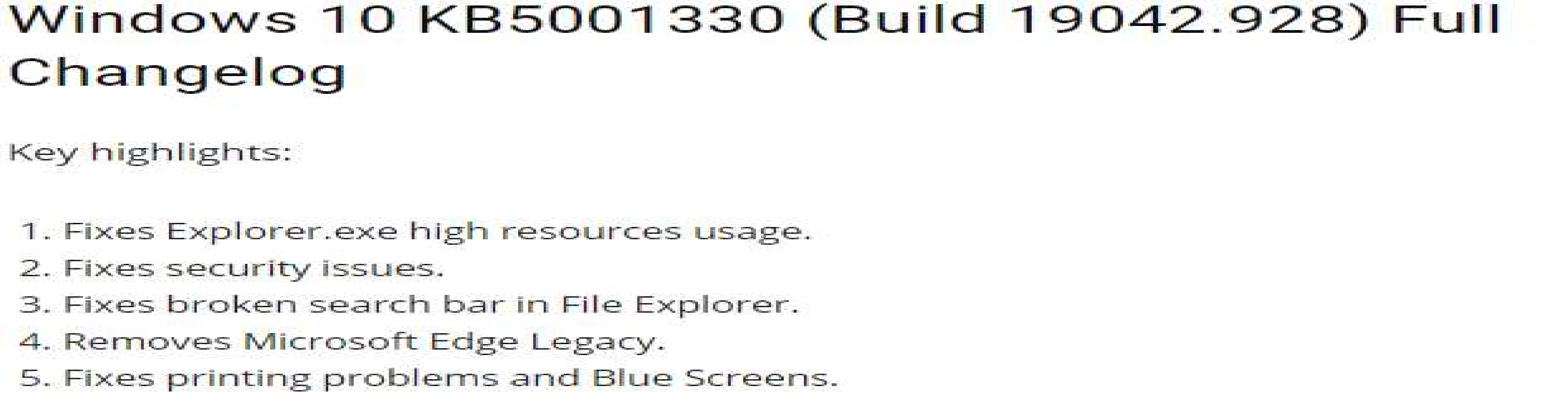
MacOS & Silver Sparrow
Published • Feb 20

Cyber Security SIG News Archive

- At time of this writing NO info at Microsoft on Purpose?
- US-CERT Advisory to patch



# of Vulnerabilities	Publicly Disclosed	Critical	Exploited
114	4	19	1



Windows 10 KB5001330 (Build 19042.928) Full Changelog

Key highlights:

1. Fixes Explorer.exe high resources usage.
2. Fixes security issues.
3. Fixes broken search bar in File Explorer.
4. Removes Microsoft Edge Legacy.
5. Fixes printing problems and Blue Screens.

Patch Tuesday

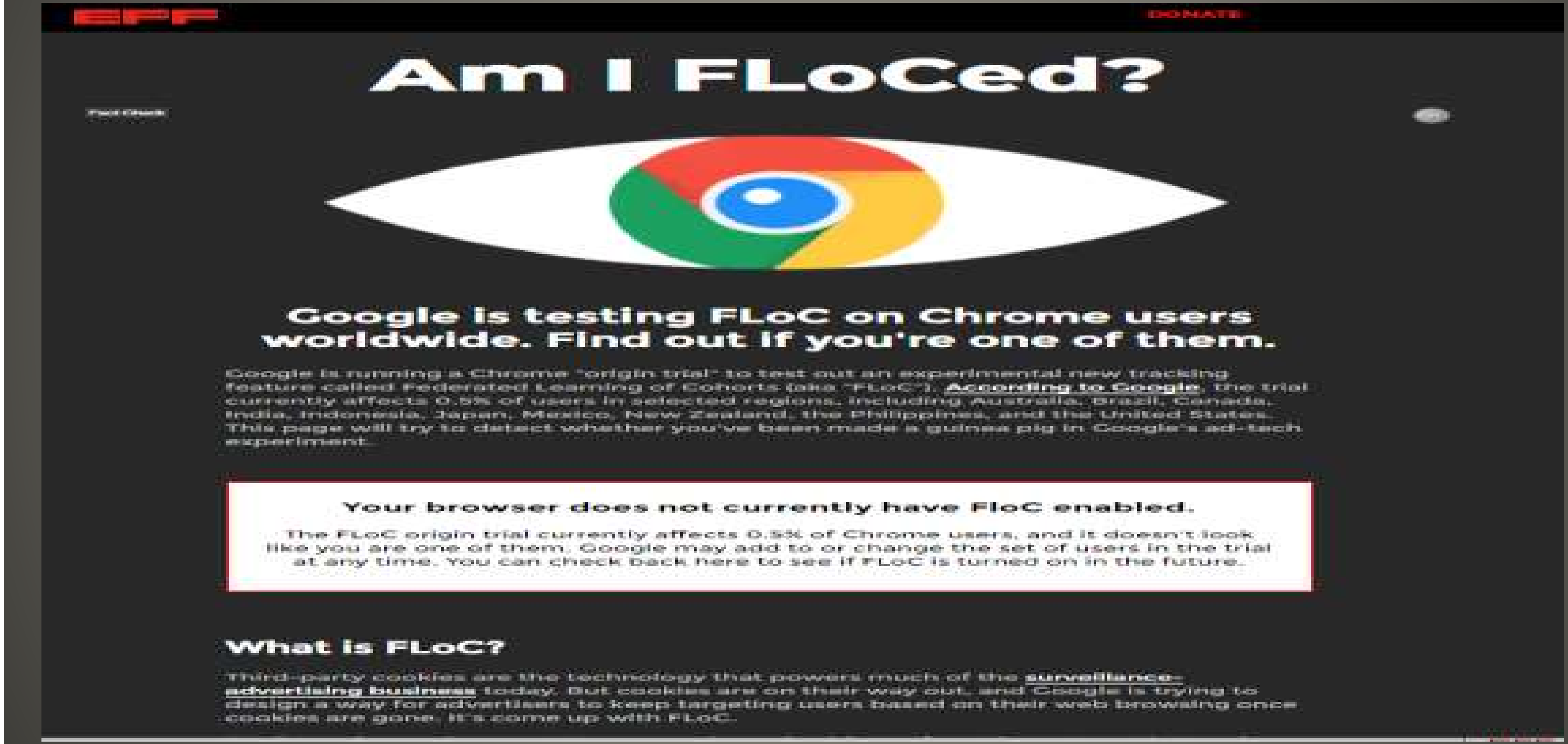
Google FLoC

- *Federated Learning of Cohorts*
- *Gmail 1.5Billion Outlook 400Million*
- *SPAM control – not bad*
- *Creepy line*
- *Apple IDFA ID for Advertisers*
- *Apple ATT App Tracking Transparency*
- *99% say NO*
- *China Anonymization ID (CAID)*

- Trial underway
- DuckDuckGo browser extension?

- EFF site

https://amifloced.org/



Am I FLoCed?

Google is testing FLoC on Chrome users worldwide. Find out if you're one of them.

Google is running a Chrome "origin trial" to test out an experimental new tracking feature called Federated Learning of Cohorts (aka "FLoC"). According to Google, the trial currently affects 0.5% of users in selected regions, including Australia, Brazil, Canada, India, Indonesia, Japan, Mexico, New Zealand, the Philippines, and the United States. This page will try to detect whether you've been made a guinea pig in Google's ad-tech experiment.

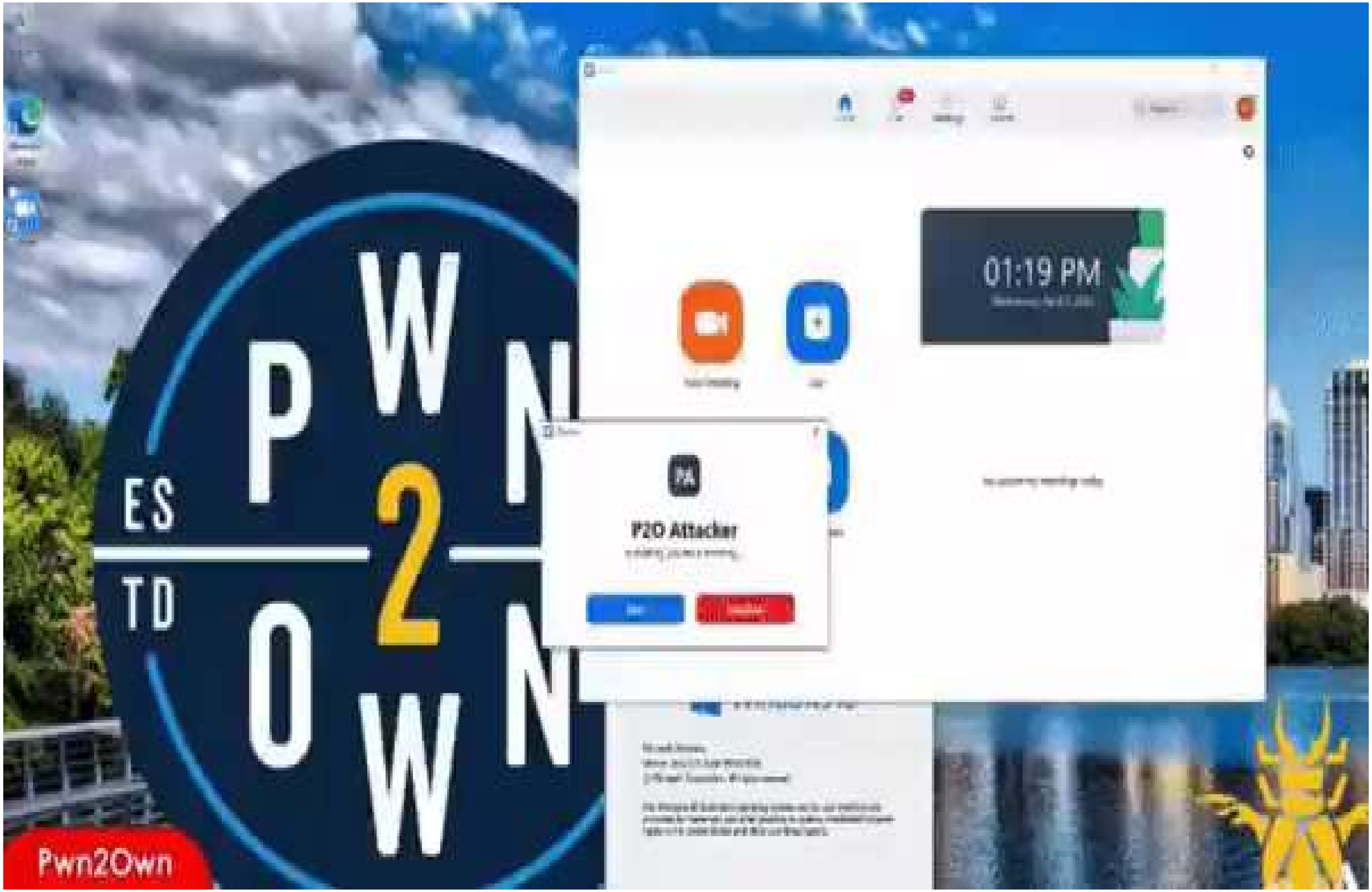
Your browser does not currently have FloC enabled.

The FLoC origin trial currently affects 0.5% of Chrome users, and it doesn't look like you are one of them. Google may add to or change the set of users in the trial at any time. You can check back here to see if FLoC is turned on in the future.

What is FLoC?

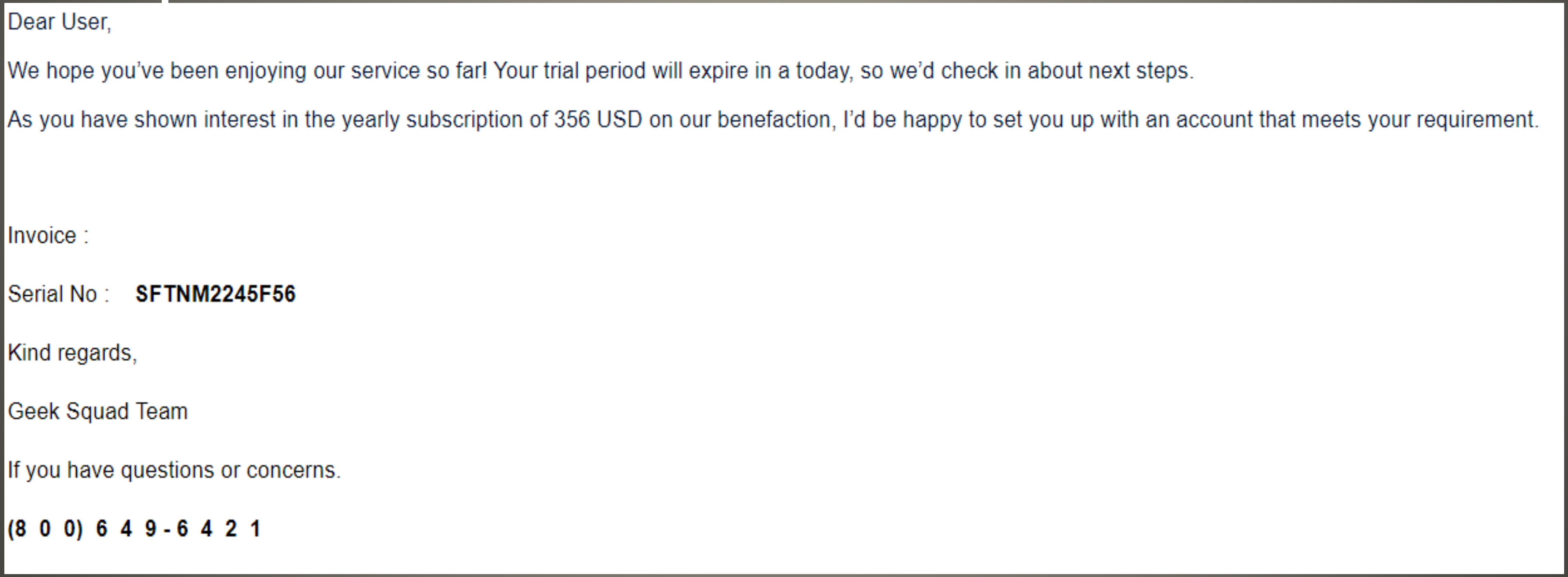
Third-party cookies are the technology that powers much of the surveillance-advertising business today. But cookies are on their way out, and Google is trying to design a way for advertisers to keep targeting users based on their web browsing once cookies are gone. It's come up with FLoC.

Am I FLoCed?



PWN 2 OWN
ES
TD
Pwn2Own
01:19 PM
P2O Attacker

- Bad grammar
- Unique serial number/invoice/ID/etc.
- Compromised email sender
- Dispute with bank



Dear User,

We hope you’ve been enjoying our service so far! Your trial period will expire in a today, so we’d check in about next steps.

As you have shown interest in the yearly subscription of 356 USD on our benefaction, I’d be happy to set you up with an account that meets your requirement.

Invoice :

Serial No : **SFTNM2245F56**

Kind regards,

Geek Squad Team

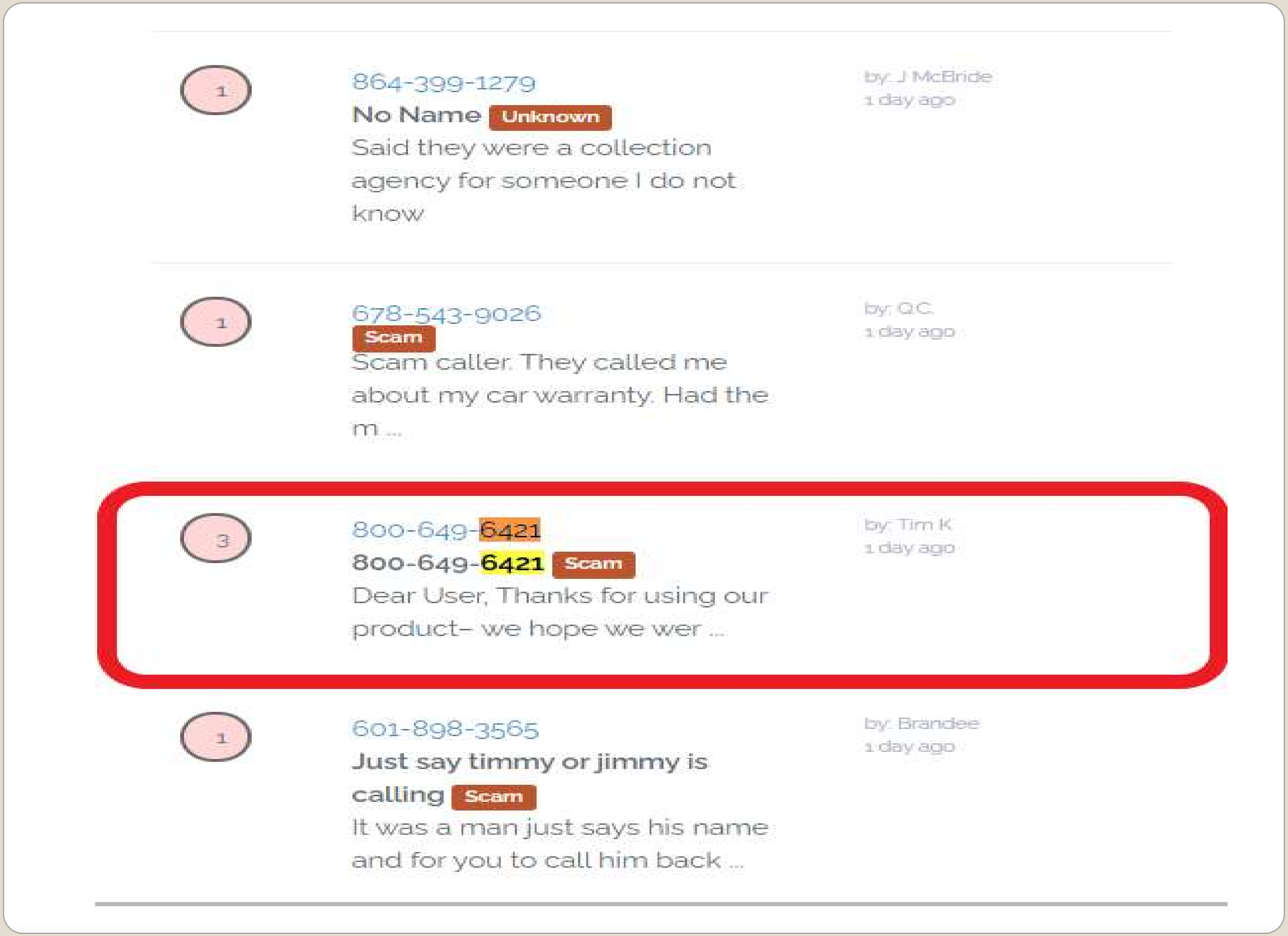
If you have questions or concerns.

(800) 649-6421

Yet another scam

Yet another scam

- DO NOT Call phone number
- DO NOT provide unique serial number, etc.
- https://www.whoisthatnumber.com/allreports
- <CRTL>/F Search last 4 digits?



1

864-399-1279

No Name Unknown

Said they were a collection agency for someone I do not know

by: J McBride
1 day ago

1

678-543-9026

Scam

Scam caller. They called me about my car warranty. Had the m ...

by: Q.C.
1 day ago

3

800-649-6421

800-649-6421 Scam

Dear User, Thanks for using our product– we hope we wer ...

by: Tim K
1 day ago

1

601-898-3565

Just say timmy or jimmy is calling Scam

It was a man just says his name and for you to call him back ...

by: Brandee
1 day ago

- Facebook breach
  Your phone number?
  Irish Data Protection Commission
- Garmin
- Android spyware as system update
- Auto emissions testing disrupted
- LinkedIn phishing
- Microsoft Azure outage
- .gov domain
  GOTGOV Online Trust in Government Act
  Government Services Administration
  Cybersecurity and Infrastructure Security Agency
- SAP attacks
- San Bernardino cell phone unlock

Current Issues

San Bernardino cell phone

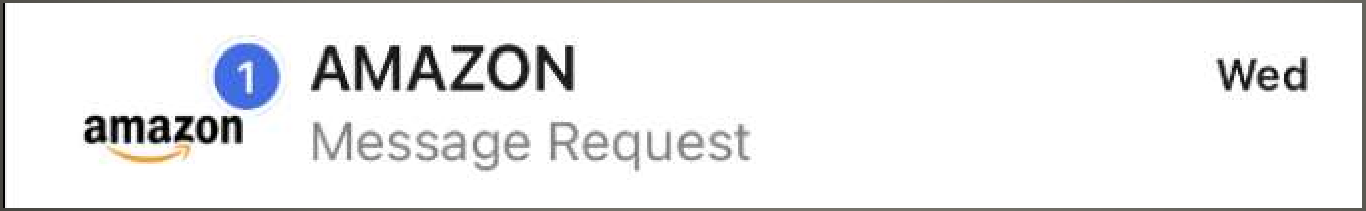
- December 2015 attack
- His company issued 5C iPhone iOS9
- If only FBI acted more quickly …
- Court order sought, then dropped
- Debate - still
- $900,000
- Virtual iPhone Apple suing

Current Issues

- FBI-CISA joint advisory Fortinet Fort iOS
- CISA Industrial Control Systems
- Ubiquiti breach – coverup?
- Ubiquiti cloud login required
- Oldsmar, Florida
  Ellsworth County Kansas
  water treatment compromise
- Supreme Court ruling
  Google vs. Oracle
  Google use of Java API “fair use”
- Google Play Store FlixOnline
- Early news Iranian enrichment cyber attack
- CISA-FBI joint advisory Russian SVR scans
- US – Russia sanctions due to past events

Current Issues

- Android API
  getInstalledPackages
  getInstalledApplications
  effective Summer 2021
- Call of Duty: Warzone cheats
- QNAP NAS "complete device takeover"
- Yahoo Answers May 4, 2021
- Signal Message Request



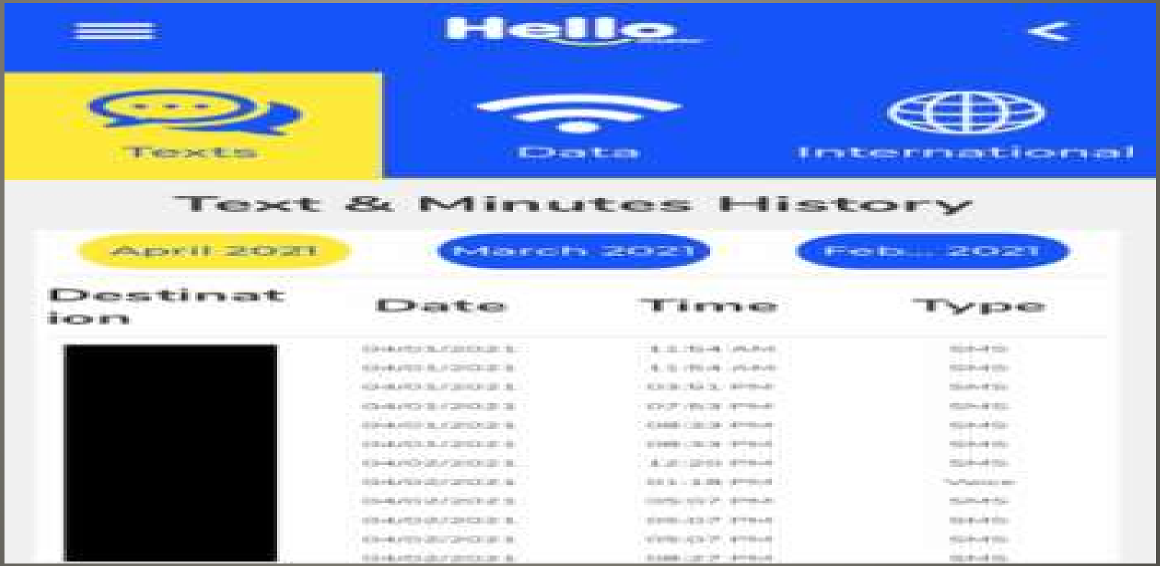
AMAZON
Message Request
Wed

Current Issues

- Q Link wireless

  know a phone number?

  get full name, home address, call history, text history, email address, last 4 payment card



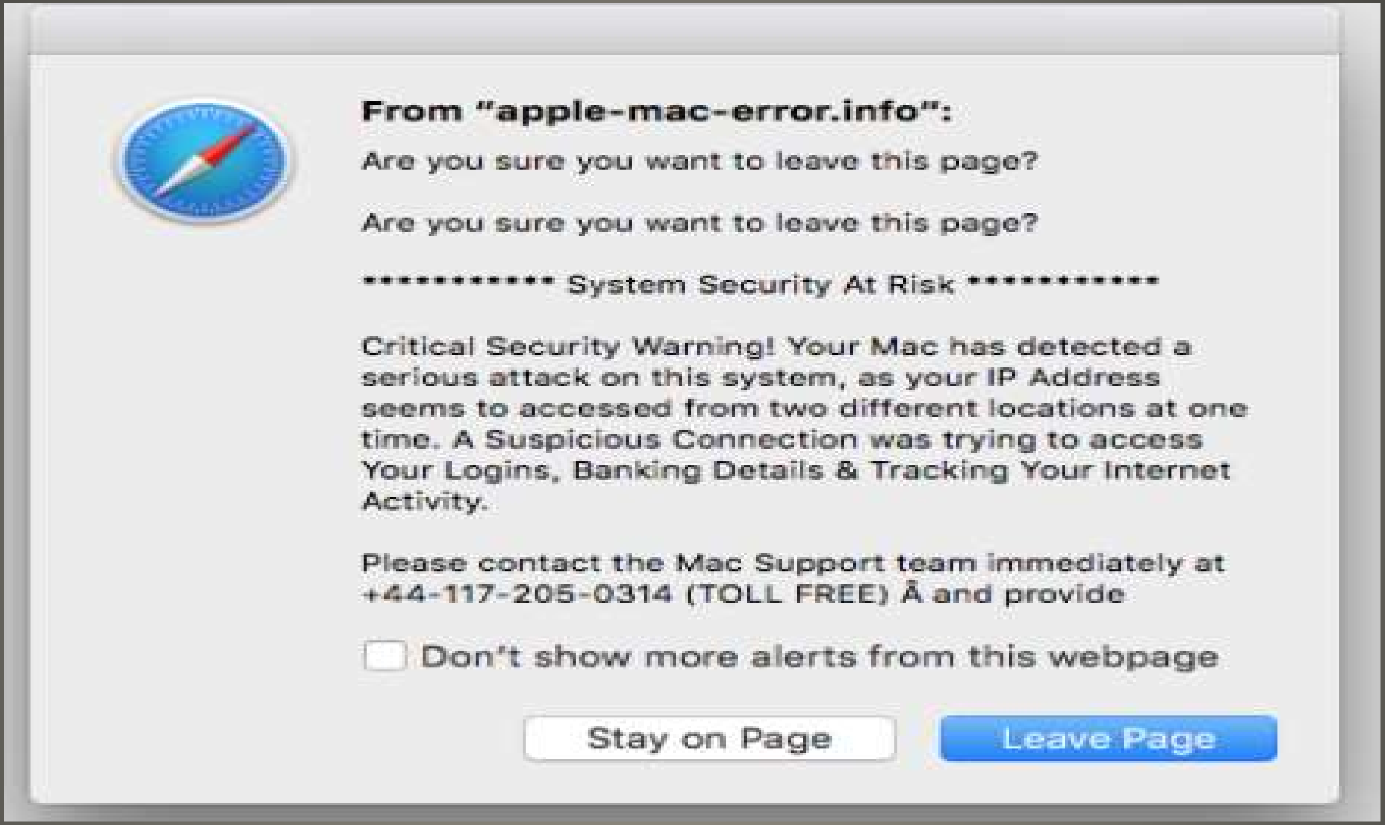
Text & Minutes History

April 2021 | March 2021 | Feb... 2021

Destination	Date	Time	Type
[redacted]	04/01/2021	11:54 AM	SMS
[redacted]	04/01/2021	11:54 AM	SMS
[redacted]	04/01/2021	03:51 PM	SMS
[redacted]	04/01/2021	07:53 PM	SMS
[redacted]	04/01/2021	08:33 PM	SMS
[redacted]	04/01/2021	08:33 PM	SMS
[redacted]	04/02/2021	12:20 PM	SMS
[redacted]	04/02/2021	01:18 PM	Voice
[redacted]	04/02/2021	05:07 PM	SMS
[redacted]	04/02/2021	05:07 PM	SMS
[redacted]	04/02/2021	05:07 PM	SMS
[redacted]	04/02/2021	08:27 PM	SMS

- FBI – court authorized operation
  remove malicious web shells sites in US
  Without owner’s permission
  Helpful – unaware & unprepared
  Harmful – critical file removed
- IoT bugs in DNS allowing cache poisoning
- Outbound port blocking in browser
  Combat NAT slipstreaming
  10080
- Windows 10 1909 end of support May 11, 2021
- Cisco SOHO routers not to be fixed
- Browser updates abound

Current Issues



From "apple-mac-error.info":

Are you sure you want to leave this page?

Are you sure you want to leave this page?

*********** System Security At Risk ***********

Critical Security Warning! Your Mac has detected a serious attack on this system, as your IP Address seems to accessed from two different locations at one time. A Suspicious Connection was trying to access Your Logins, Banking Details & Tracking Your Internet Activity.

Please contact the Mac Support team immediately at +44-117-205-0314 (TOLL FREE) Â and provide

□ Don't show more alerts from this webpage

- Annual Threat Assessment of the US Intelligence Community

https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Director of National Intelligence

- 21 Million records

Email addresses, date of birth, phone numbers, license plate numbers, hashed passwords, postal mail address

- Customer notice
- Details on the selling sites

ParkMobile

- Indian stock trading company
- Know-Your-Customer data
- Names, contact info, date of birth, bank account information, Photo IS, passport, utility bills, …
- Fight money laundering

Upstox

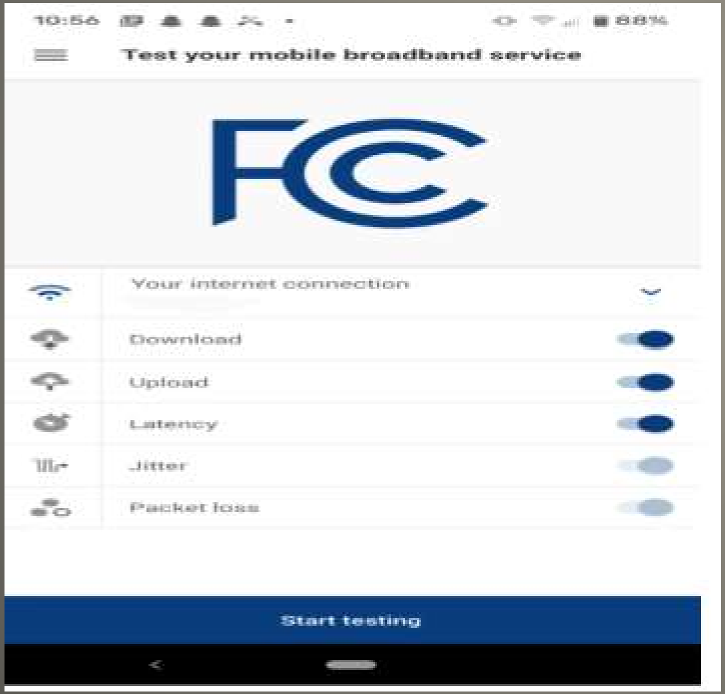
Lessons ?

- Assume your information is “out there”
- Change passphrases *often*
- Use Multi Factor Authentication
- Set up alerts
- Increase awareness
- Increase preparedness
- Increase understanding

- Machine speed
- Network speed
- Algorithm speed
- Algorithm tunning
- Moving regulations
- Money Bots

Rapid Traders

- FCC Speed Test App
- Apple Store Google Play
- Fact check provider provided test results



Test your mobile broadband service

Your internet connection

Download ●

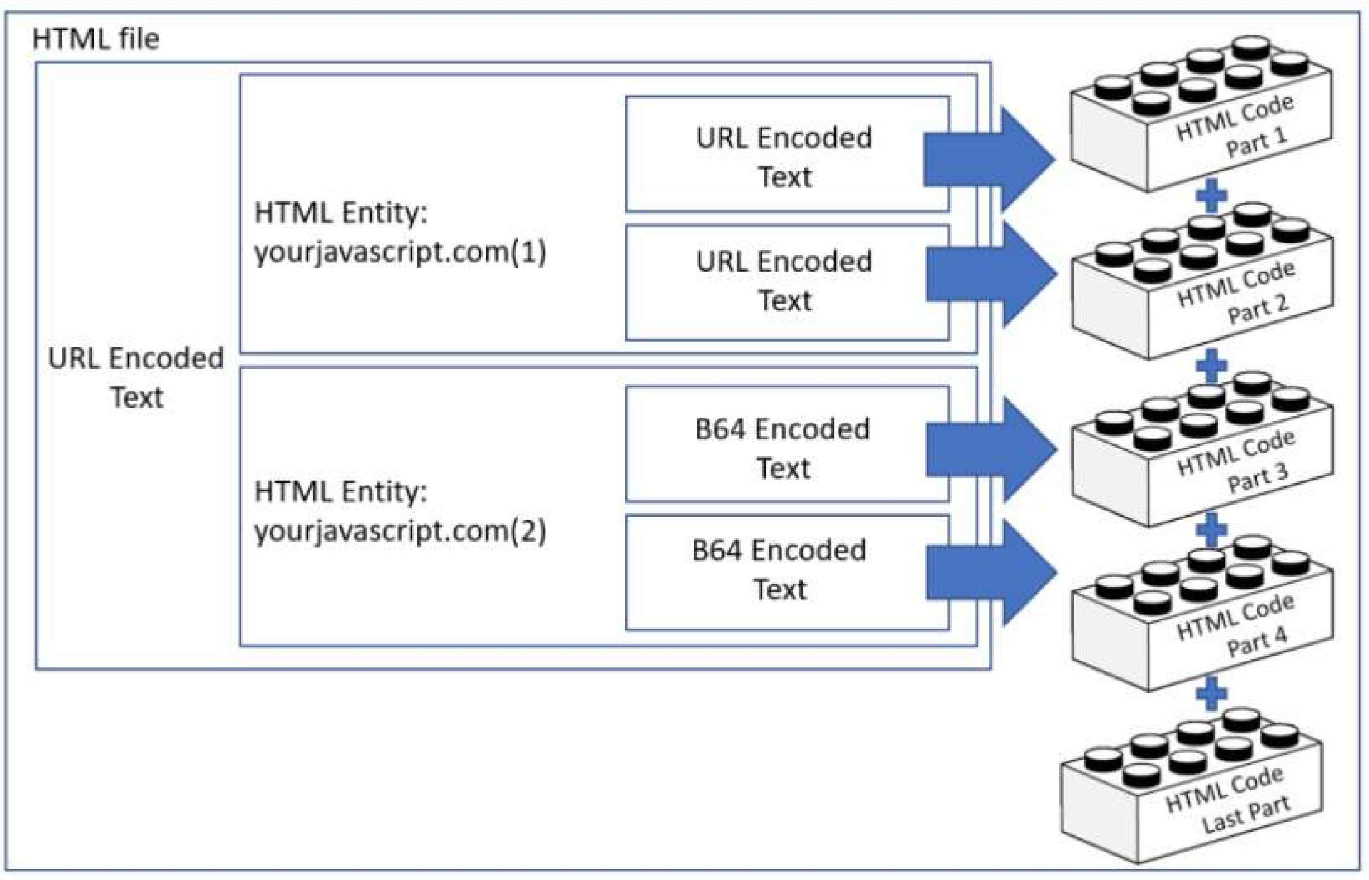
Upload ●

Latency ●

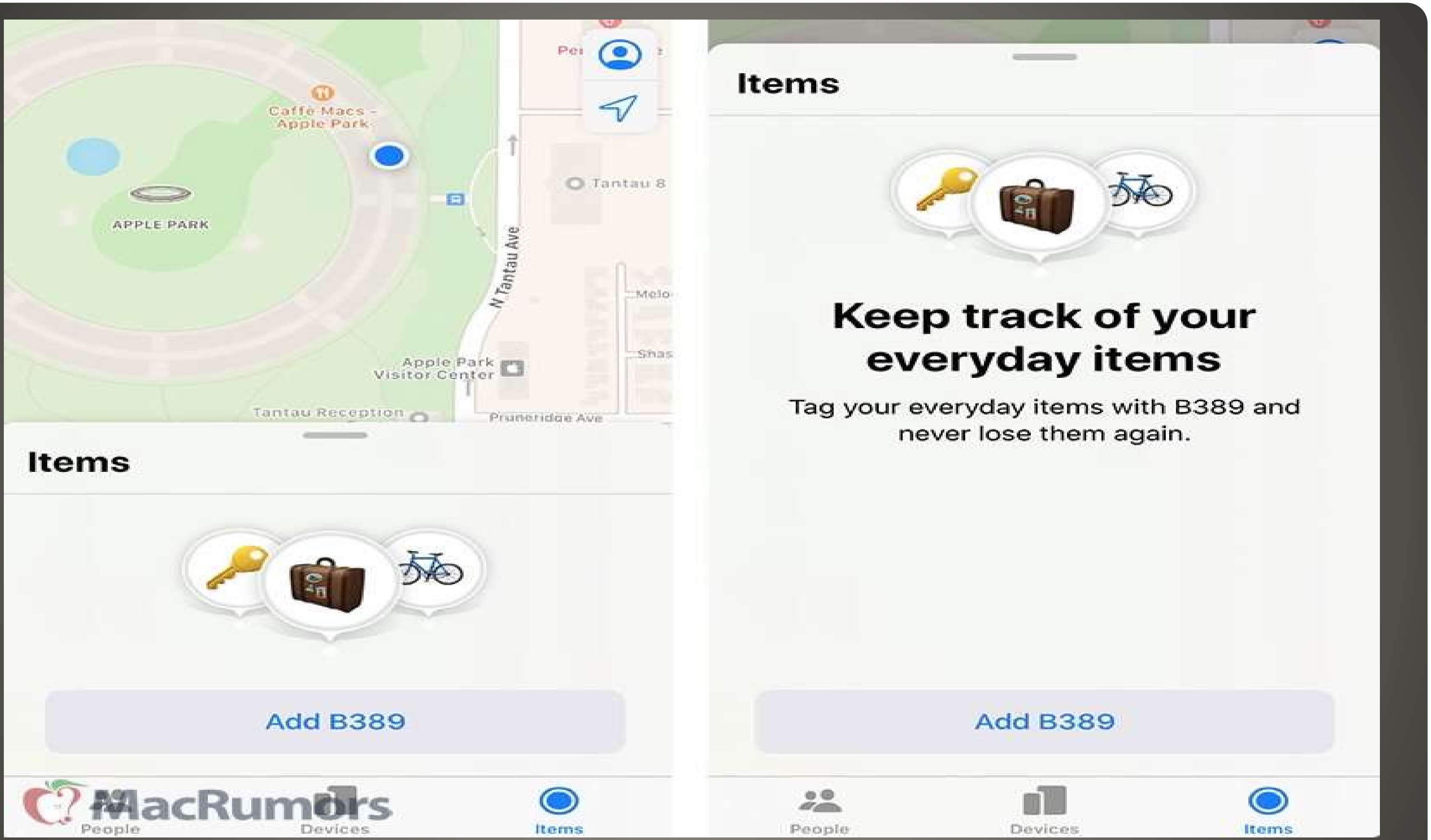
Jitter ○

Packet loss ○

FCC WANTS your speed test results



Build the exploit on your machine



Items

Add B389

Items

Keep track of your everyday items

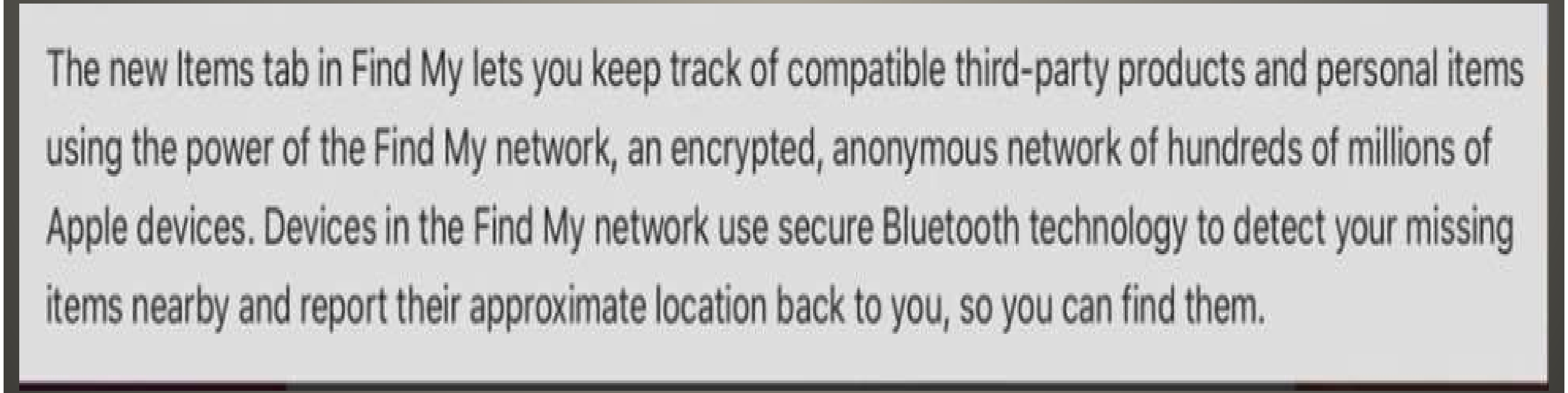
Tag your everyday items with B389 and never lose them again.

Add B389

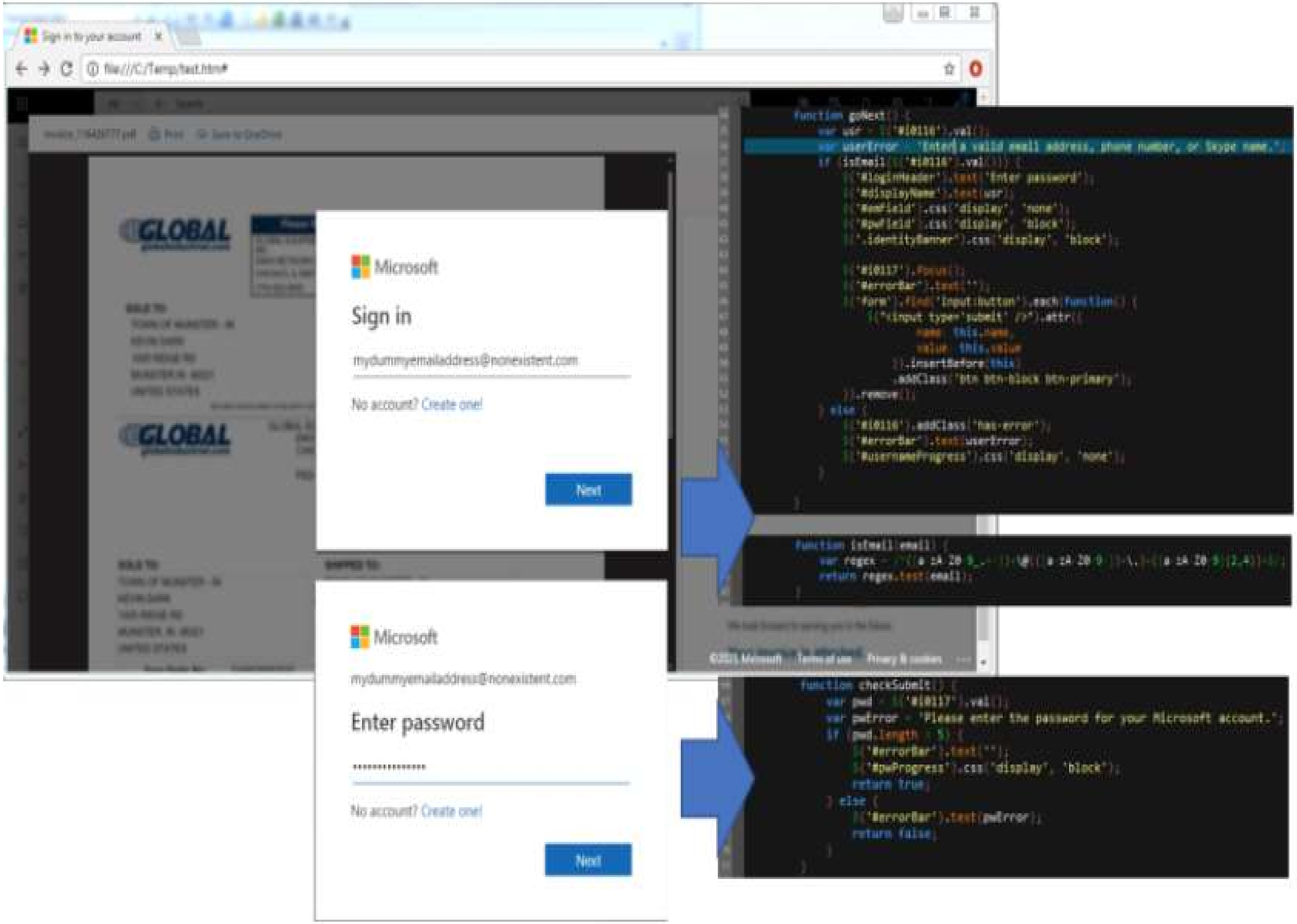
Apple *Find My*

Apple *Find My*

- Apple ID
- Signed into iCloud with Find My enabled
- Permit Find My access to Location data
- Location Services enabled
- Air Tags



The new Items tab in Find My lets you keep track of compatible third-party products and personal items using the power of the Find My network, an encrypted, anonymous network of hundreds of millions of Apple devices. Devices in the Find My network use secure Bluetooth technology to detect your missing items nearby and report their approximate location back to you, so you can find them.


Sign in to your account
file:///C:/Temp/test.htm#
GLOBAL
©2021 Microsoft Terms of use Privacy & cookies

Microsoft

Sign in

mydummyemailaddress@nonexistent.com

No account? Create one!

```
function goNext() {
    var usr = $('#i0116').val();
    var userError = 'Enter a valid email address, phone number, or Skype name.';
    if (isEmail($('#i0116').val())) {
        $('#loginHeader').text('Enter password');
        $('#displayName').text(usr);
        $('#emField').css('display', 'none');
        $('#pwField').css('display', 'block');
        $('.identityBanner').css('display', 'block');

        $('#i0117').focus();
        $('#errorBar').text("");
        $('form').find('input:button').each(function() {
            $("<input type='submit' />").attr({
                    name: this.name,
                    value: this.value
                }).insertBefore(this)
                .addClass('btn btn-block btn-primary');
        }).remove();
    } else {
        $('#i0116').addClass('has-error');
        $('#errorBar').text(userError);
        $('#usernameProgress').css('display', 'none');
    }

}
```

```
function isEmail(email) {
    var regex = /^([a-zA-Z0-9_.+-])+\@(([a-zA-Z0-9-])+\.)+([a-zA-Z0-9]{2,4})+$/;
    return regex.test(email);
}
```

Microsoft

mydummyemailaddress@nonexistent.com

Enter password

••••••••••••••••

No account? Create one!

```
function checkSubmit() {
    var pwd = $('#i0117').val();
    var pwError = 'Please enter the password for your Microsoft account.';
    if (pwd.length > 5) {
        $('#errorBar').text("");
        $('#pwProgress').css('display', 'block');
        return true;
    } else {
        $('#errorBar').text(pwError);
        return false;
    }
}
```

- Security Now Podcast – Steve Gibson
- Research Trinity College Dublin, Ireland

iOS shares with Apple

Android shares with Google Pixel phones

Average 4.5 minutes

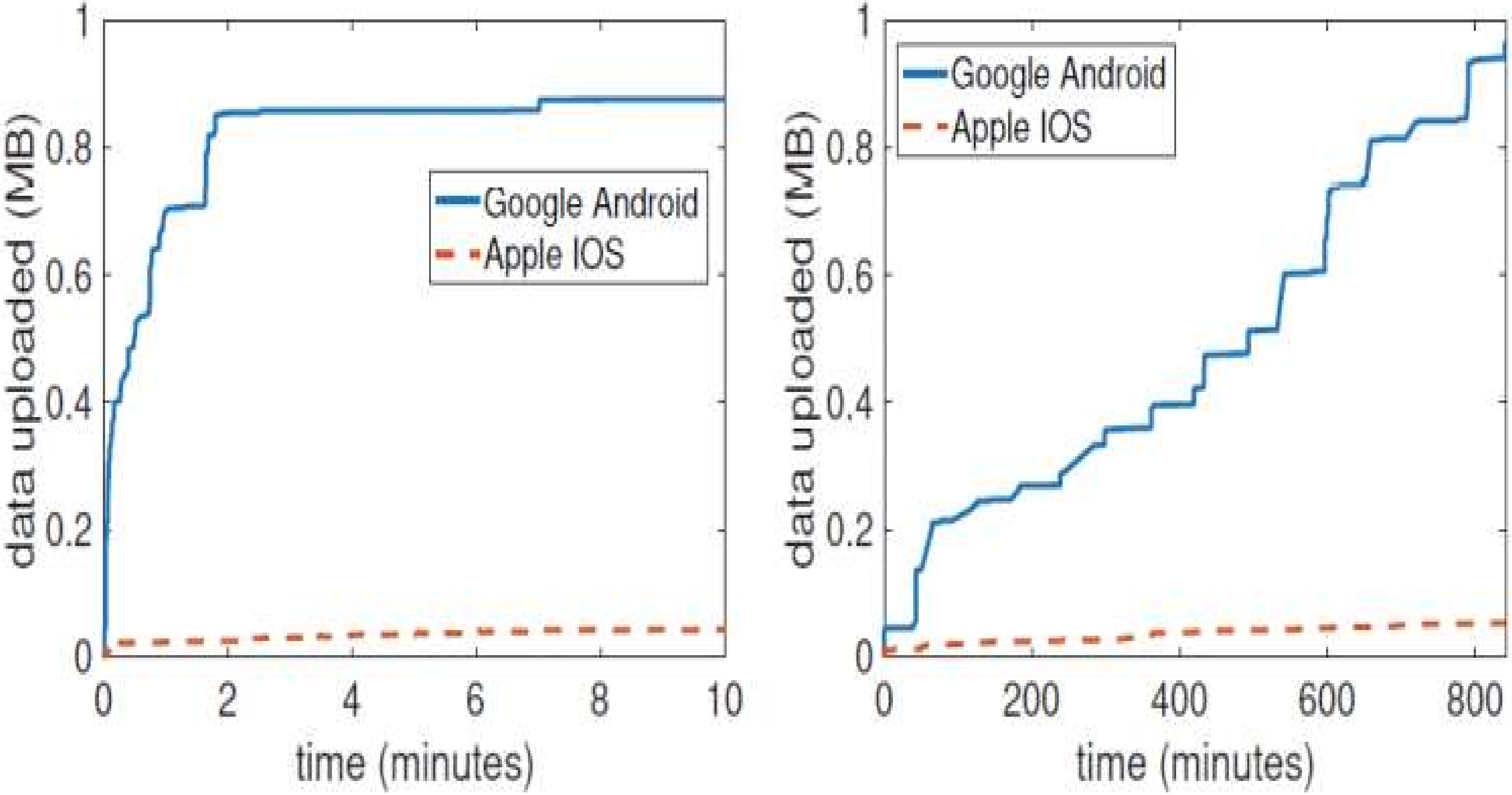
Phone IMEI, hardware serial number, SIM serial number and IMSI, phone number,

iOS sends MAC addresses of all nearby devices and gateway, GPS location

NO opt out

https://www.scss.tcd.ie/doug.leith/apple_google.pdf

Spy in our pocket



(a) Startup

(b) Idle

Spy in our pocket

- Pre-installed apps/services

  Apple - Siri, Safari, iCloud

  Google – YouTube, Chrome, Google Docs, Safetyhub, Google Messaging, clock, Google Search bar
- Linked to personal data Name, eMail, credit card, other personal devices, browsing history, etc.
- Law enforcement can’t get inside phone
- Apple/Google can “see” all around phones

SIM Swap Protections

- Smart Device trust
- BE AWARE

  Facebook breach

  Any and all breaches

  Information gives no indication of being stolen

  Our cellular number is EVERYWHERE

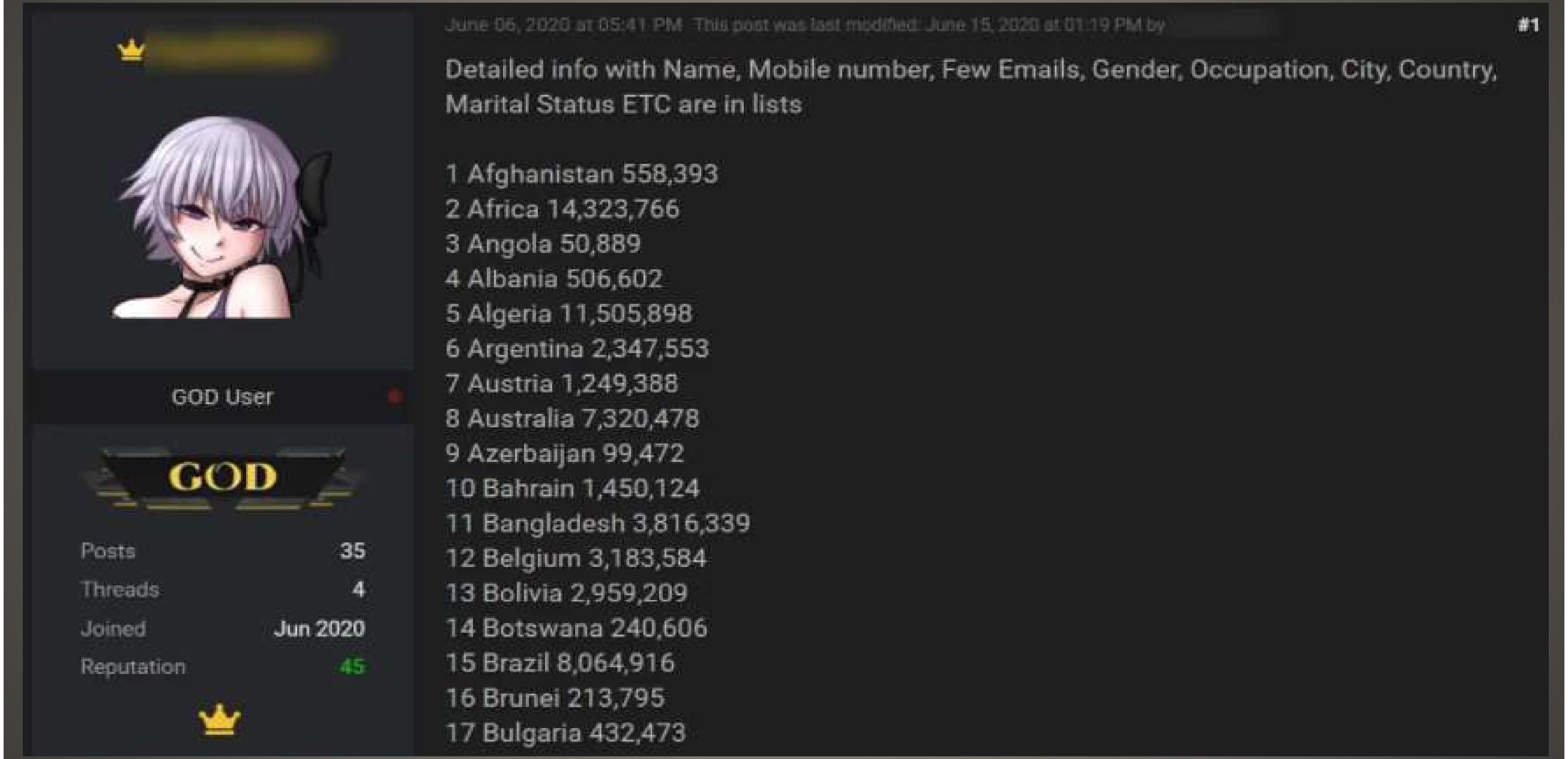
  Authenticator App

  Security Key

  Have I been Pwned eMail Phone number?

  Use sites that claim to report on phone numbers?
- Service providers are aware
- Service providers are aware
- Attacking as a service
- Robocalls advantage?

- 2019 breach – release



[redacted]

GOD User

Posts 35
Threads 4
Joined Jun 2020
Reputation 45

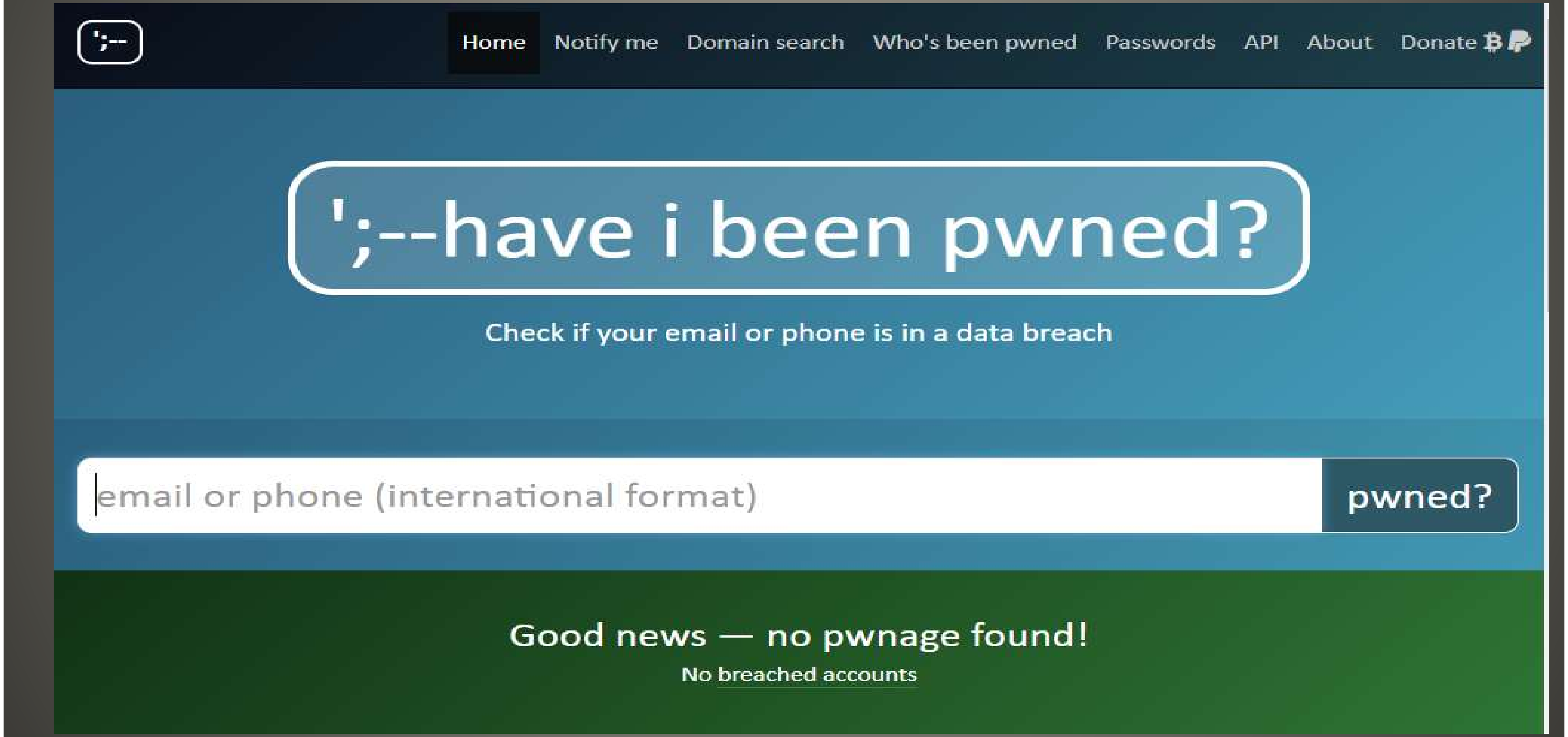
June 06, 2020 at 05:41 PM This post was last modified: June 15, 2020 at 01:19 PM by [redacted] #1

Detailed info with Name, Mobile number, Few Emails, Gender, Occupation, City, Country, Marital Status ETC are in lists

1 Afghanistan 558,393
2 Africa 14,323,766
3 Angola 50,889
4 Albania 506,602
5 Algeria 11,505,898
6 Argentina 2,347,553
7 Austria 1,249,388
8 Australia 7,320,478
9 Azerbaijan 99,472
10 Bahrain 1,450,124
11 Bangladesh 3,816,339
12 Belgium 3,183,584
13 Bolivia 2,959,209
14 Botswana 240,606
15 Brazil 8,064,916
16 Brunei 213,795
17 Bulgaria 432,473

Facebook

- Have I Been Pwned
- Phone lookup added 6-Apr-2021



';--have i been pwned?

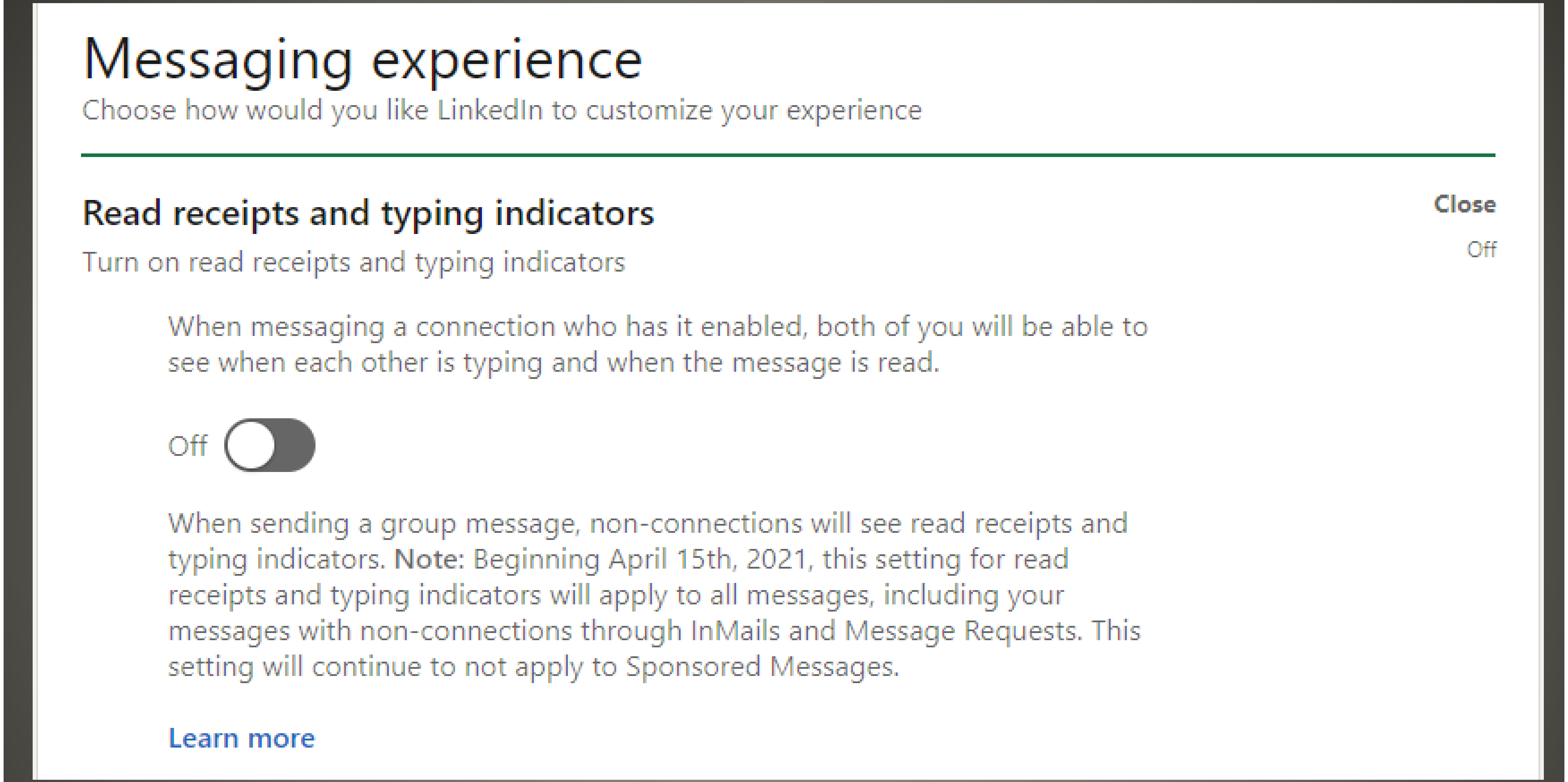
Check if your email or phone is in a data breach

Good news — no pwnage found!

No breached accounts

- Yet another data breach?
- User IDs, eMail addresses, Phone numbers, gender, professional titles, social media profiles,
- LinkedIn - not us
- Yeahbut

LinkedIn



Messaging experience

Choose how would you like LinkedIn to customize your experience

Read receipts and typing indicators

Close

Off

Turn on read receipts and typing indicators

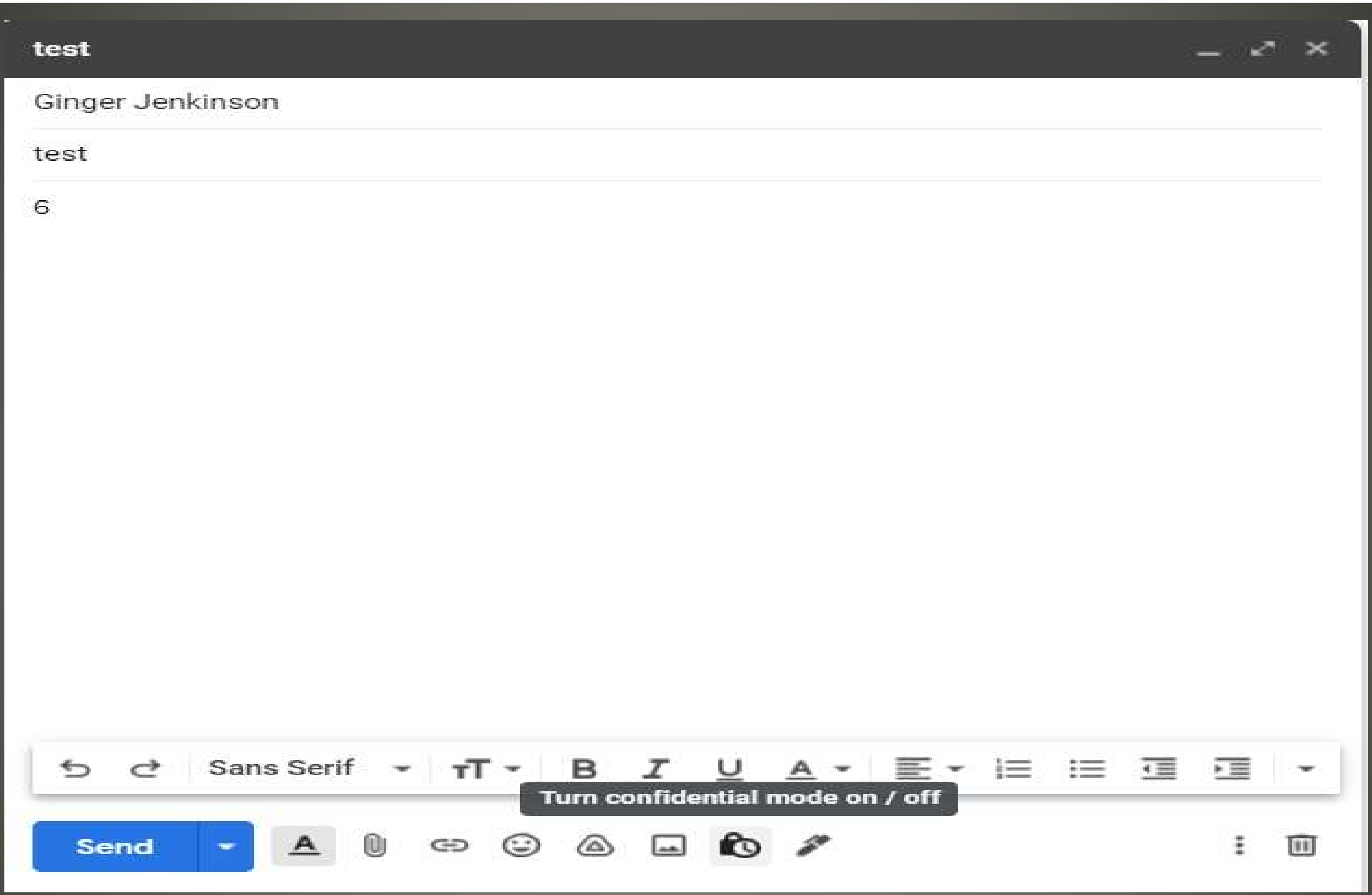
When messaging a connection who has it enabled, both of you will be able to see when each other is typing and when the message is read.

Off

When sending a group message, non-connections will see read receipts and typing indicators. **Note:** Beginning April 15th, 2021, this setting for read receipts and typing indicators will apply to all messages, including your messages with non-connections through InMails and Message Requests. This setting will continue to not apply to Sponsored Messages.

Learn more

Change 15-Apr-2021



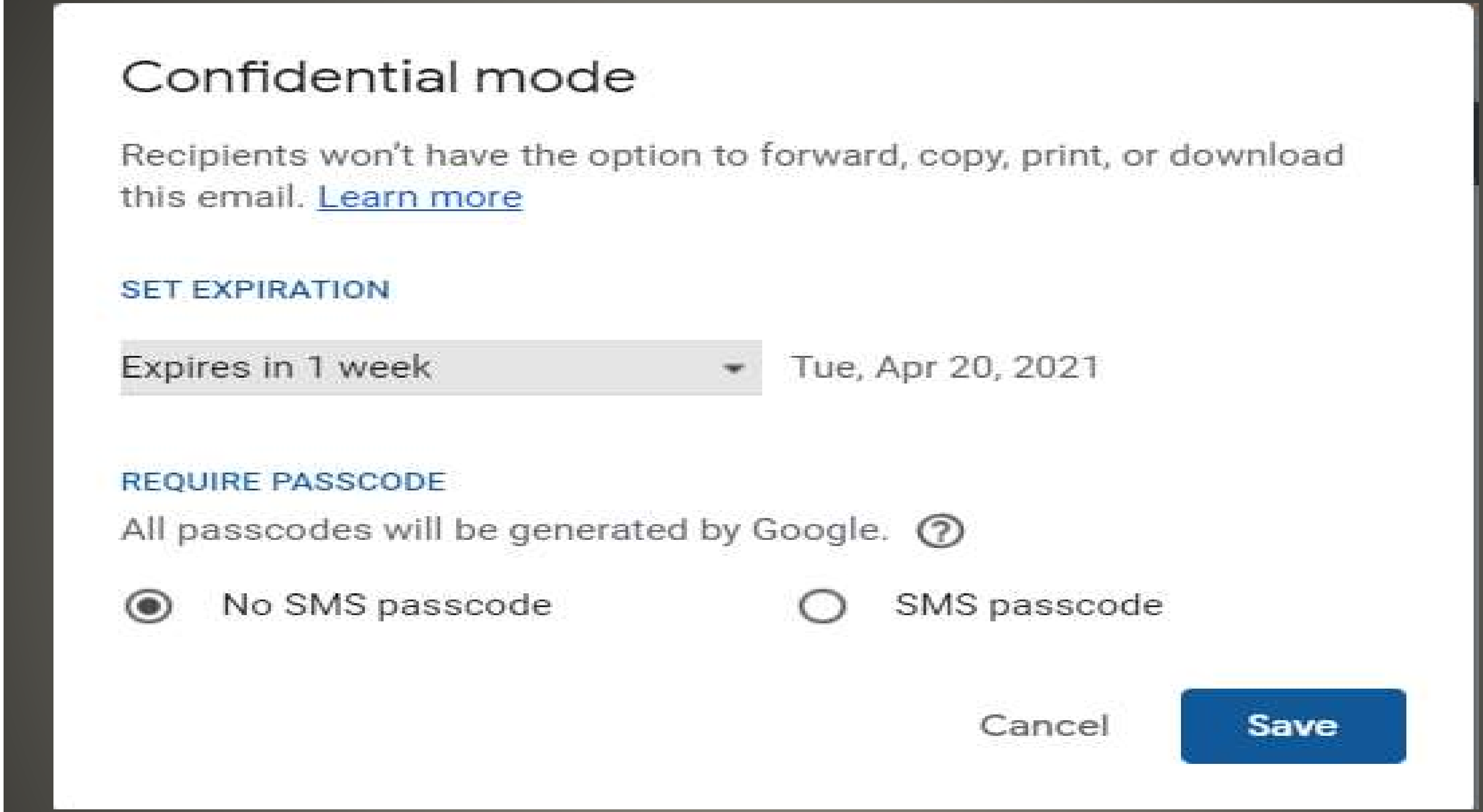
test

Ginger Jenkinson

test

6

Confidential Gmail



Confidential mode

Recipients won't have the option to forward, copy, print, or download this email. Learn more

SET EXPIRATION

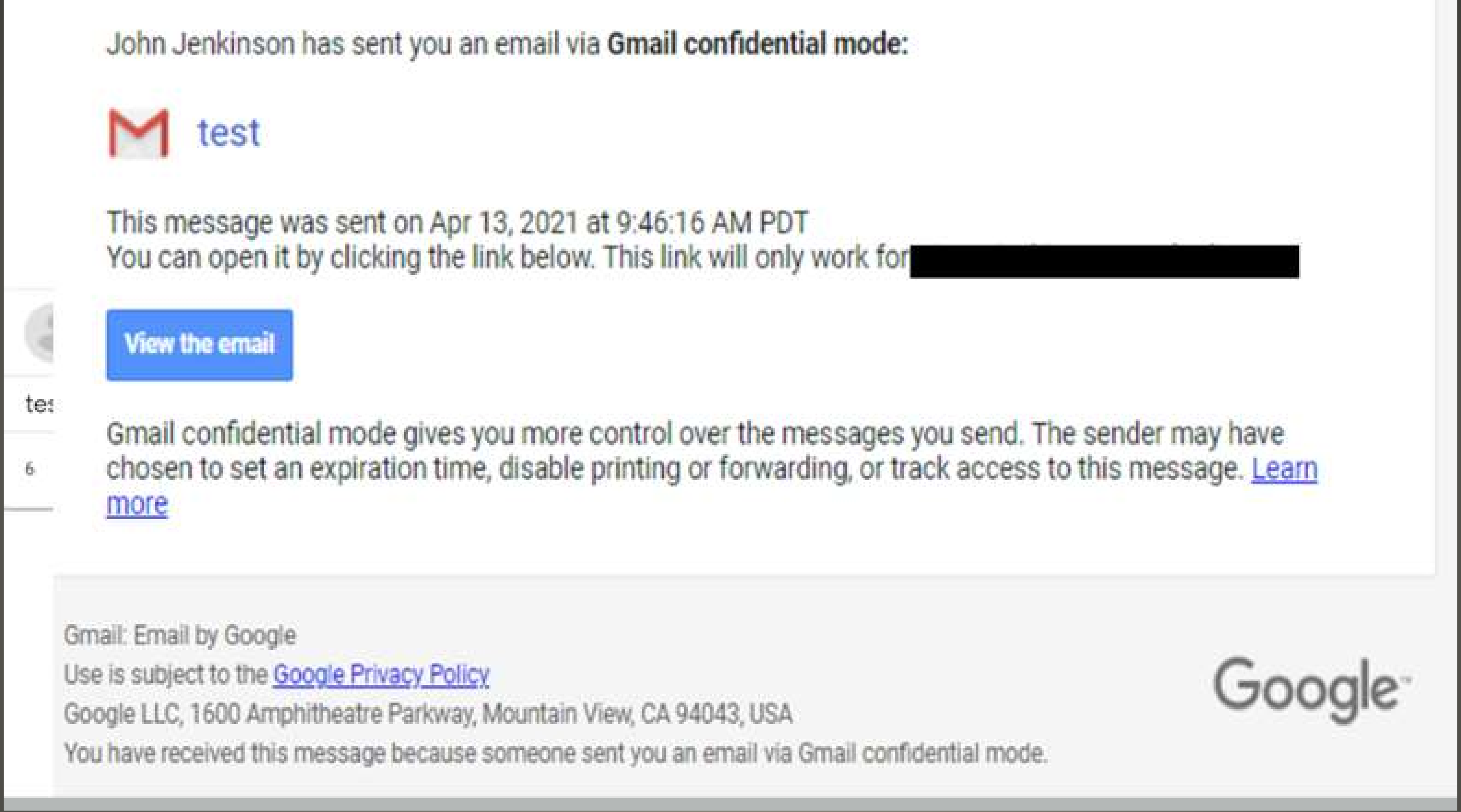
Expires in 1 week ▾ Tue, Apr 20, 2021

REQUIRE PASSCODE

All passcodes will be generated by Google. ⓘ

● No SMS passcode ○ SMS passcode

Confidential Gmail



John Jenkinson has sent you an email via **Gmail confidential mode:**

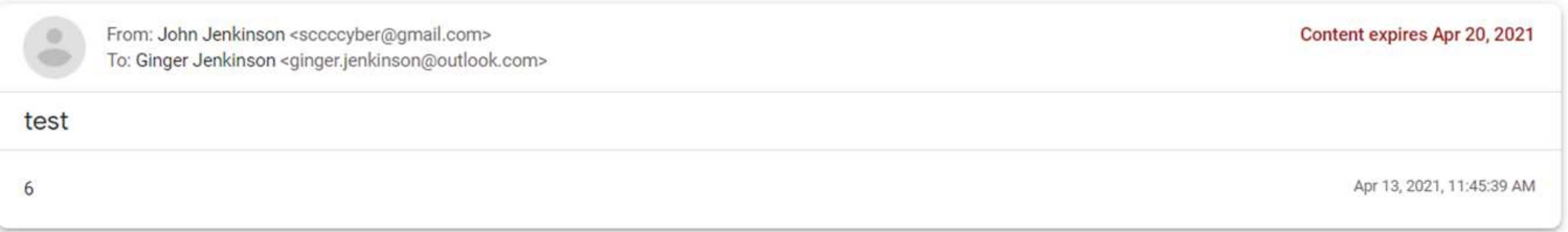
test

This message was sent on Apr 13, 2021 at 9:46:16 AM PDT
You can open it by clicking the link below. This link will only work for [redacted]

Gmail confidential mode gives you more control over the messages you send. The sender may have chosen to set an expiration time, disable printing or forwarding, or track access to this message. Learn more

Gmail: Email by Google
Use is subject to the Google Privacy Policy
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
You have received this message because someone sent you an email via Gmail confidential mode.

Confidential Gmail



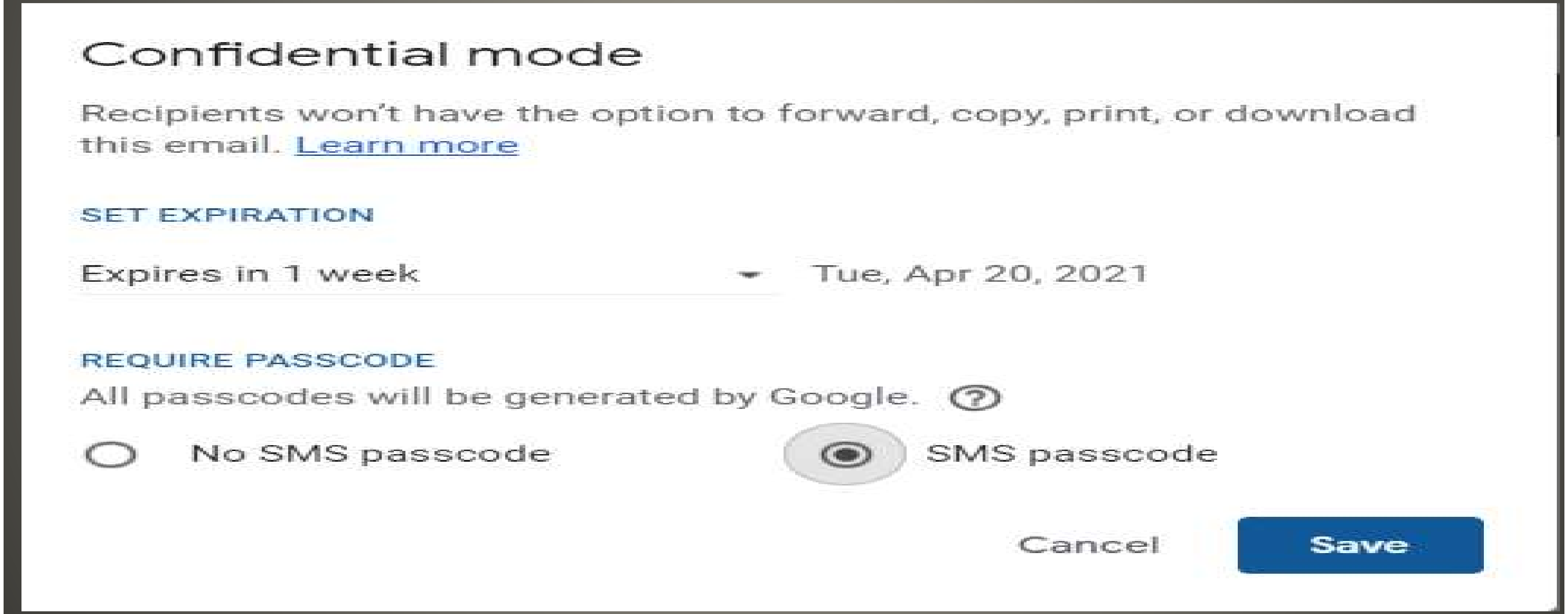
From: John Jenkinson <scccyber@gmail.com>
To: Ginger Jenkinson <ginger.jenkinson@outlook.com>

Content expires Apr 20, 2021

test

6

Apr 13, 2021, 11:45:39 AM



Confidential mode

Recipients won't have the option to forward, copy, print, or download this email. Learn more

SET EXPIRATION

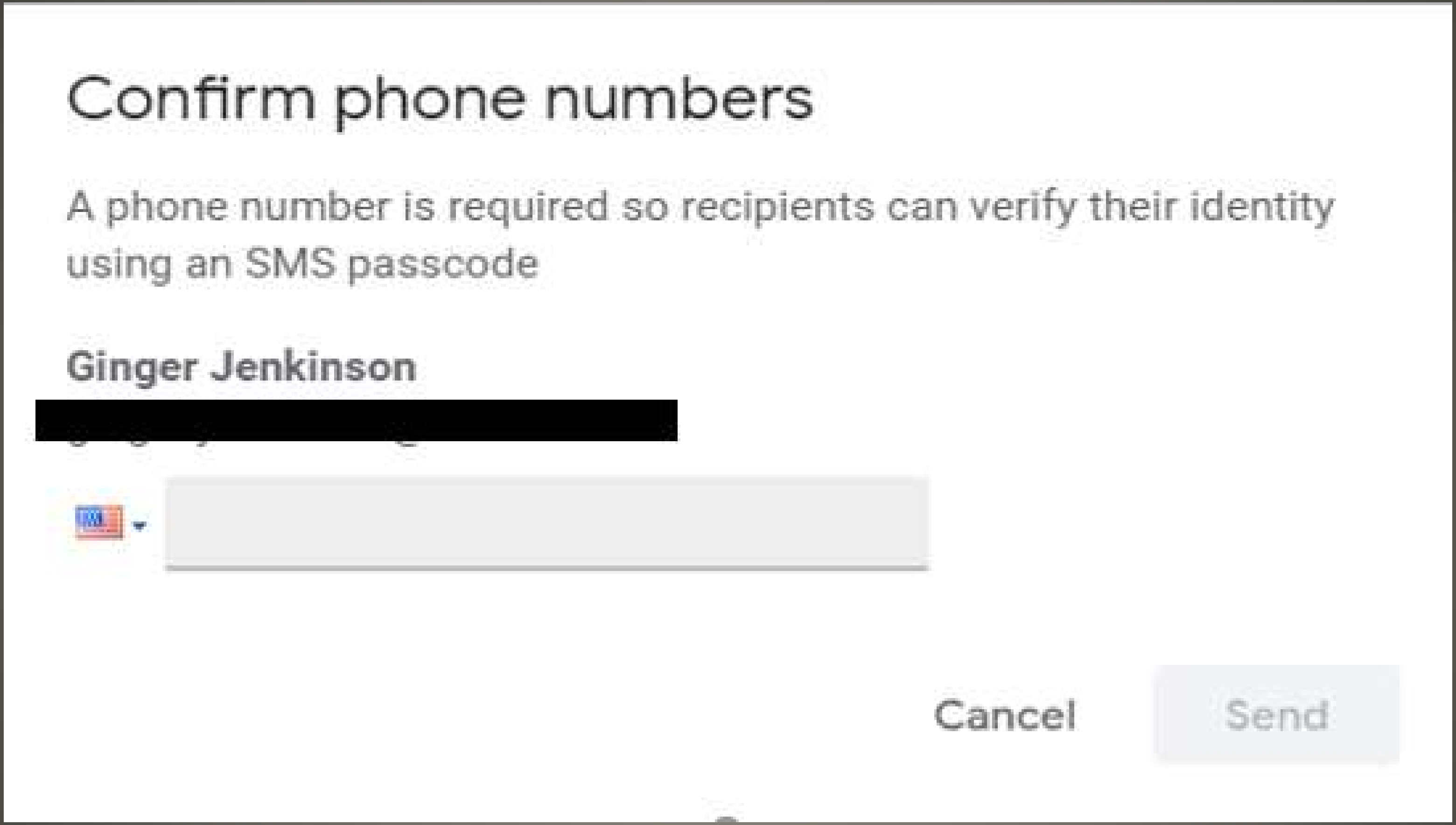
Expires in 1 week — Tue, Apr 20, 2021

REQUIRE PASSCODE

All passcodes will be generated by Google.

○ No SMS passcode ● SMS passcode

Confidential Gmail



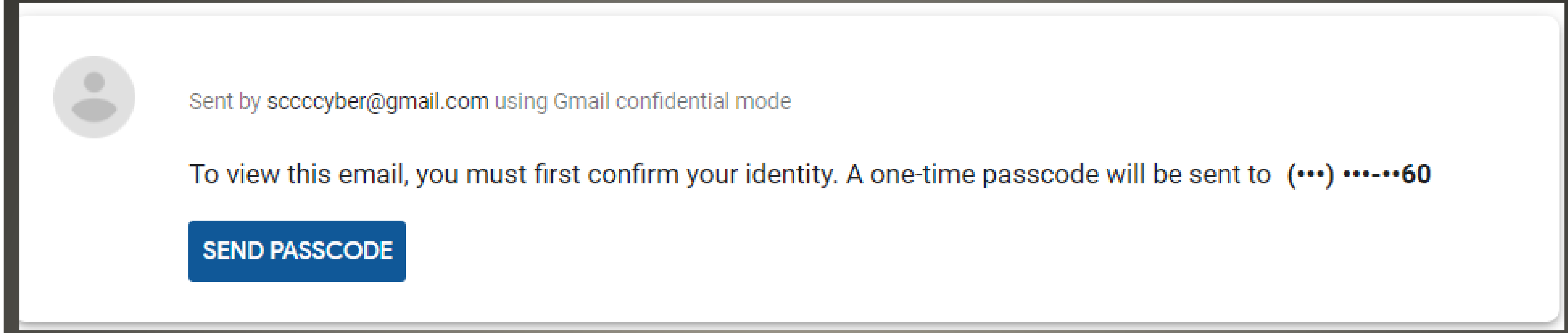
Confirm phone numbers

A phone number is required so recipients can verify their identity using an SMS passcode

Ginger Jenkinson

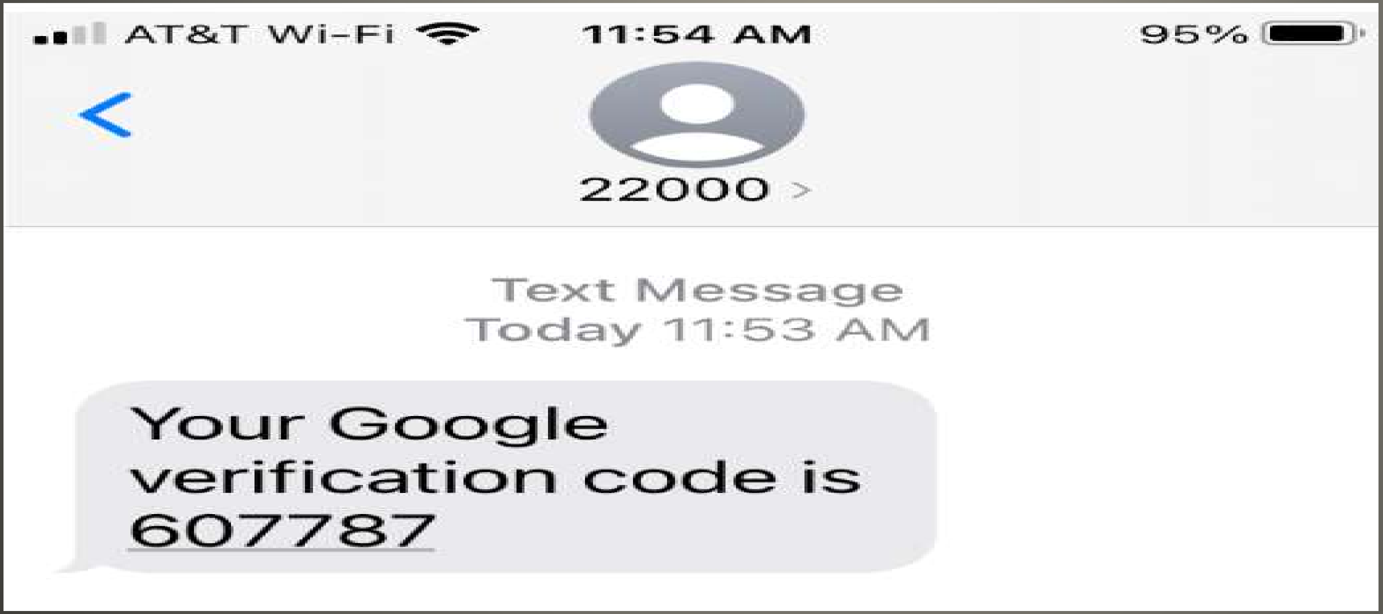
[redacted]

Confidential Gmail



Sent by scccyber@gmail.com using Gmail confidential mode

To view this email, you must first confirm your identity. A one-time passcode will be sent to (•••) •••-••60



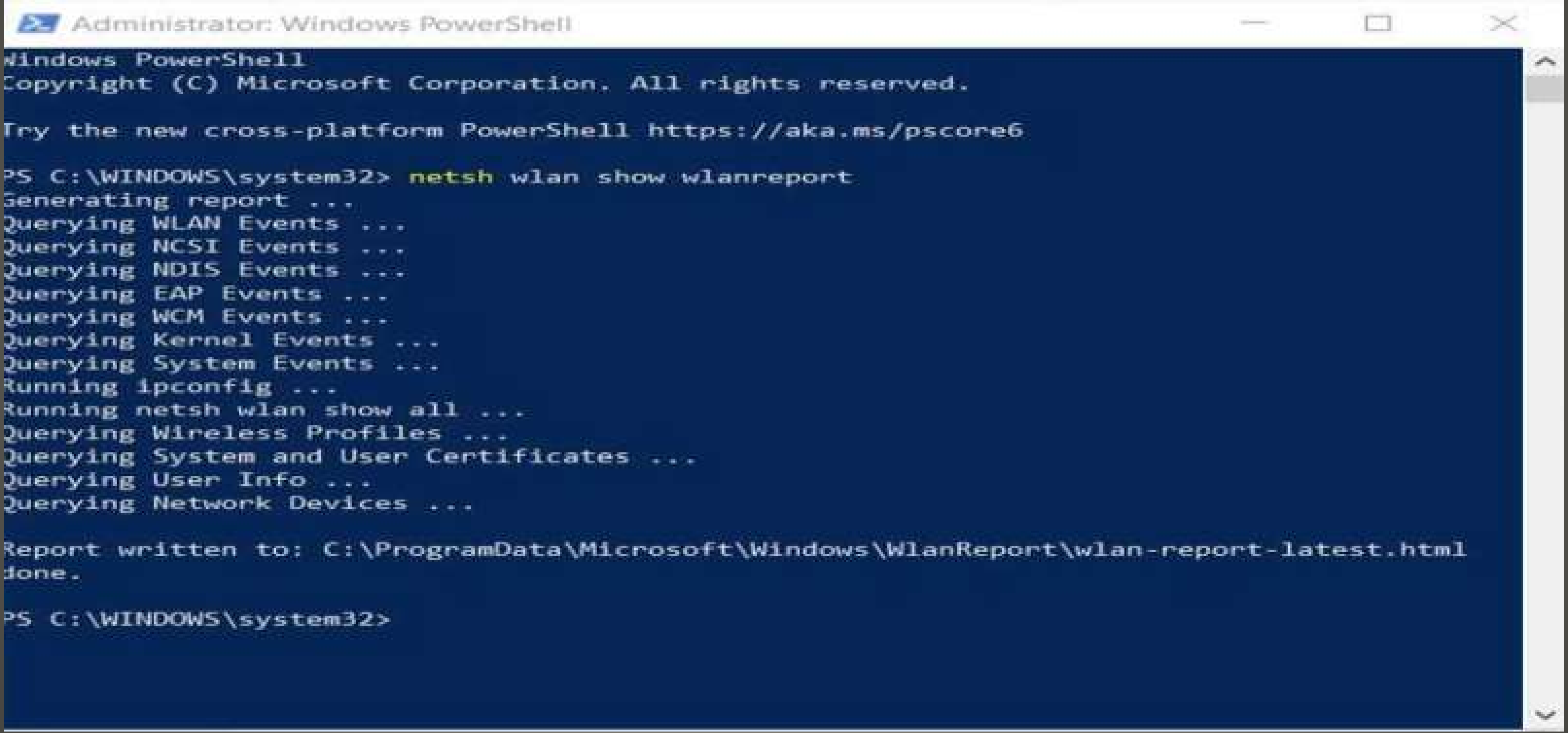
Your Google verification code is 607787

Confidential Gmail

- Confidential – just how so?
- Once viewed …
- Alternatives ?
- ProtonMail
- Tutanota

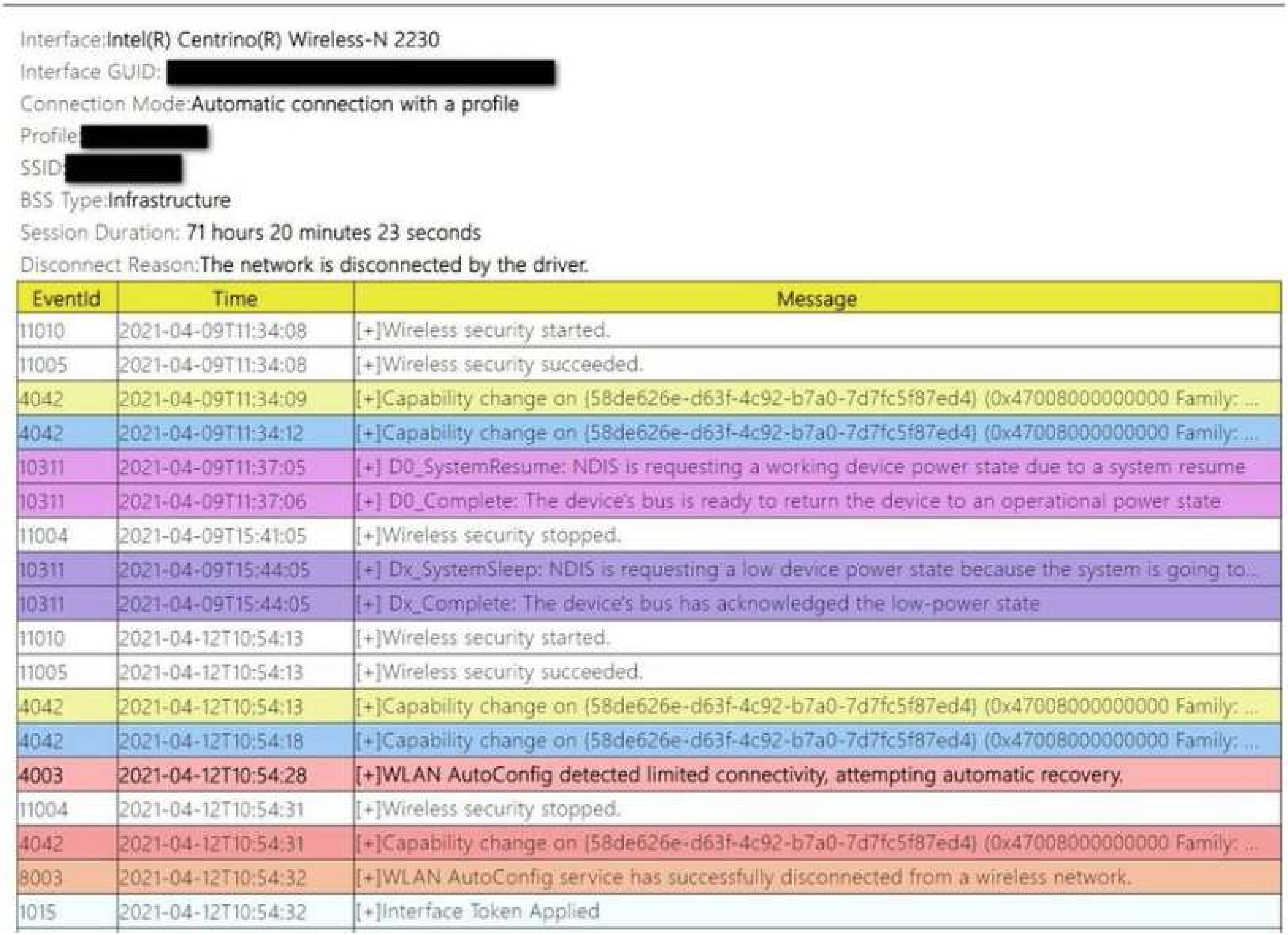
Confidential Gmail

- Troubleshooting
- Otherwise as well



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> netsh wlan show wlanreport
Generating report ...
Querying WLAN Events ...
Querying NCSI Events ...
Querying NDIS Events ...
Querying EAP Events ...
Querying WCM Events ...
Querying Kernel Events ...
Querying System Events ...
Running ipconfig ...
Running netsh wlan show all ...
Querying Wireless Profiles ...
Querying System and User Certificates ...
Querying User Info ...
Querying Network Devices ...

Report written to: C:\ProgramData\Microsoft\Windows\WlanReport\wlan-report-latest.html
done.

PS C:\WINDOWS\system32>
```

Network (wireless) report



Interface:Intel(R) Centrino(R) Wireless-N 2230

Interface GUID: [redacted]

Connection Mode:Automatic connection with a profile

Profile[redacted]

SSID[redacted]

BSS Type:Infrastructure

Session Duration: 71 hours 20 minutes 23 seconds

Disconnect Reason:The network is disconnected by the driver.

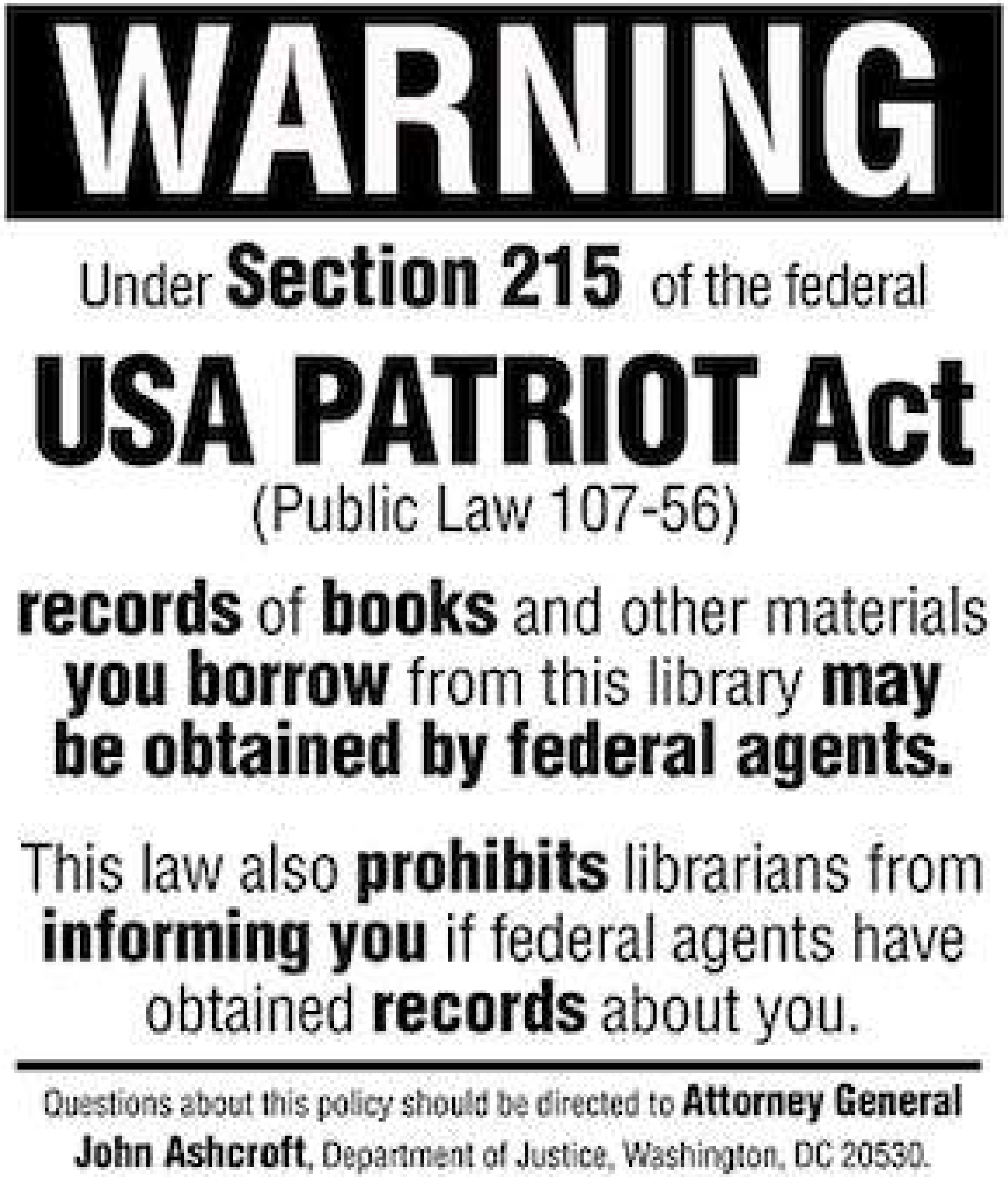
EventId	Time	Message
11010	2021-04-09T11:34:08	[+]Wireless security started.
11005	2021-04-09T11:34:08	[+]Wireless security succeeded.
4042	2021-04-09T11:34:09	[+]Capability change on {58de626e-d63f-4c92-b7a0-7d7fc5f87ed4} (0x47008000000000 Family: ...
4042	2021-04-09T11:34:12	[+]Capability change on {58de626e-d63f-4c92-b7a0-7d7fc5f87ed4} (0x47008000000000 Family: ...
10311	2021-04-09T11:37:05	[+] D0_SystemResume: NDIS is requesting a working device power state due to a system resume
10311	2021-04-09T11:37:06	[+] D0_Complete: The device's bus is ready to return the device to an operational power state
11004	2021-04-09T15:41:05	[+]Wireless security stopped.
10311	2021-04-09T15:44:05	[+] Dx_SystemSleep: NDIS is requesting a low device power state because the system is going to...
10311	2021-04-09T15:44:05	[+] Dx_Complete: The device's bus has acknowledged the low-power state
11010	2021-04-12T10:54:13	[+]Wireless security started.
11005	2021-04-12T10:54:13	[+]Wireless security succeeded.
4042	2021-04-12T10:54:13	[+]Capability change on {58de626e-d63f-4c92-b7a0-7d7fc5f87ed4} (0x47008000000000 Family: ...
4042	2021-04-12T10:54:18	[+]Capability change on {58de626e-d63f-4c92-b7a0-7d7fc5f87ed4} (0x47008000000000 Family: ...
4003	2021-04-12T10:54:28	[+]WLAN AutoConfig detected limited connectivity, attempting automatic recovery.
11004	2021-04-12T10:54:31	[+]Wireless security stopped.
4042	2021-04-12T10:54:31	[+]Capability change on {58de626e-d63f-4c92-b7a0-7d7fc5f87ed4} (0x47008000000000 Family: ...
8003	2021-04-12T10:54:32	[+]WLAN AutoConfig service has successfully disconnected from a wireless network.
1015	2021-04-12T10:54:32	[+]Interface Token Applied

- $1,210,00 awarded
- Safari, Microsoft Teams, Windows 10, Ubuntu, Chrome, Edge,
- Zoom partial fix server side

  No required user action

  5.6.1 ?

Pwn2Own



WARNING

Under **Section 215** of the federal

USA PATRIOT Act

(Public Law 107-56)

records of **books** and other materials **you borrow** from this library **may be obtained by federal agents.**

This law also **prohibits** librarians from **informing you** if federal agents have obtained **records** about you.

Questions about this policy should be directed to **Attorney General John Ashcroft**, Department of Justice, Washington, DC 20530.

- Ccleaner browser and browser extension

Questions

QUESTIONS ?

- 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