Sun City Computer Club

Cyber Security SIG

April 7, 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???

Current Issues

- Microsoft & Okta investigating attack from Lapsus$
- FBI investigating 5 US energy firm scans
- Apple service Outage 3/21/2022
- Google Maps outage 3/18/2022
- Altered software for selected attacks – geopolitical
- OpenSSL infinite loop
- MicroTik routers C&C proxies
- Russia state actors
  exploit PrintNightmare & default MFA
- Ransomware speed 100,000 files
  LockBit – 4 minutes 9 seconds
  Babuk - 6 minutes 34 seconds
  . . . .
  Maze - 1 hour 54 minutes
- Kaspersky Labs security
- FinFisher shuts down

- Security Updates
- Settings > General > VPN & Device Management
- iOS Beta (or similar)
- Remove *that* profile
- Restart
- Update

Apple Beta

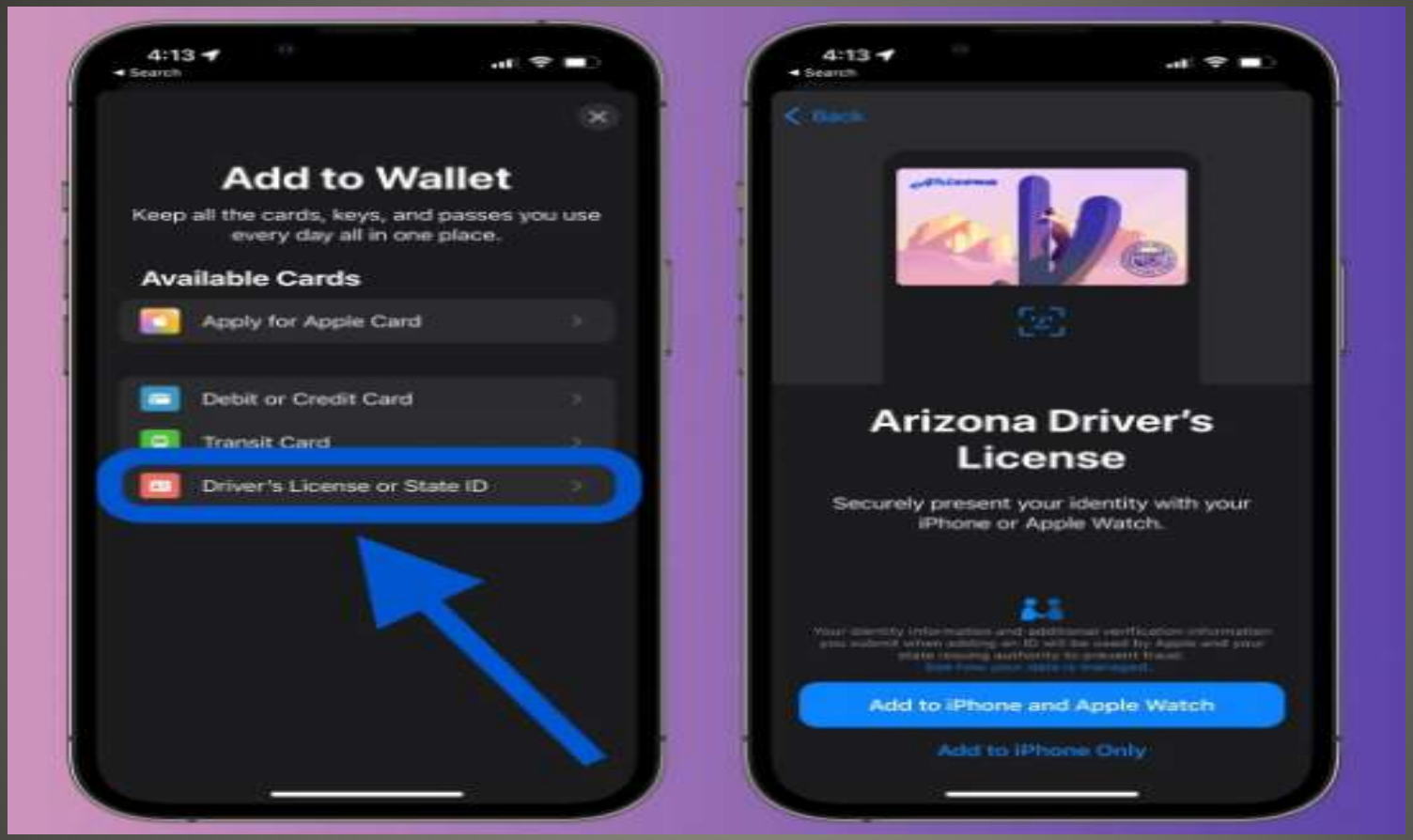
Apple digital IDs

- Security & privacy
  Over physical IDs
- Arizona
- Soon? Colorado
- Connecticut
- Georgia
- Hawaii
- Iowa
- Kentucky
- Maryland
- Mississippi
- Ohio
- Oklahoma
- Territory of Puerto Rico
- Utah

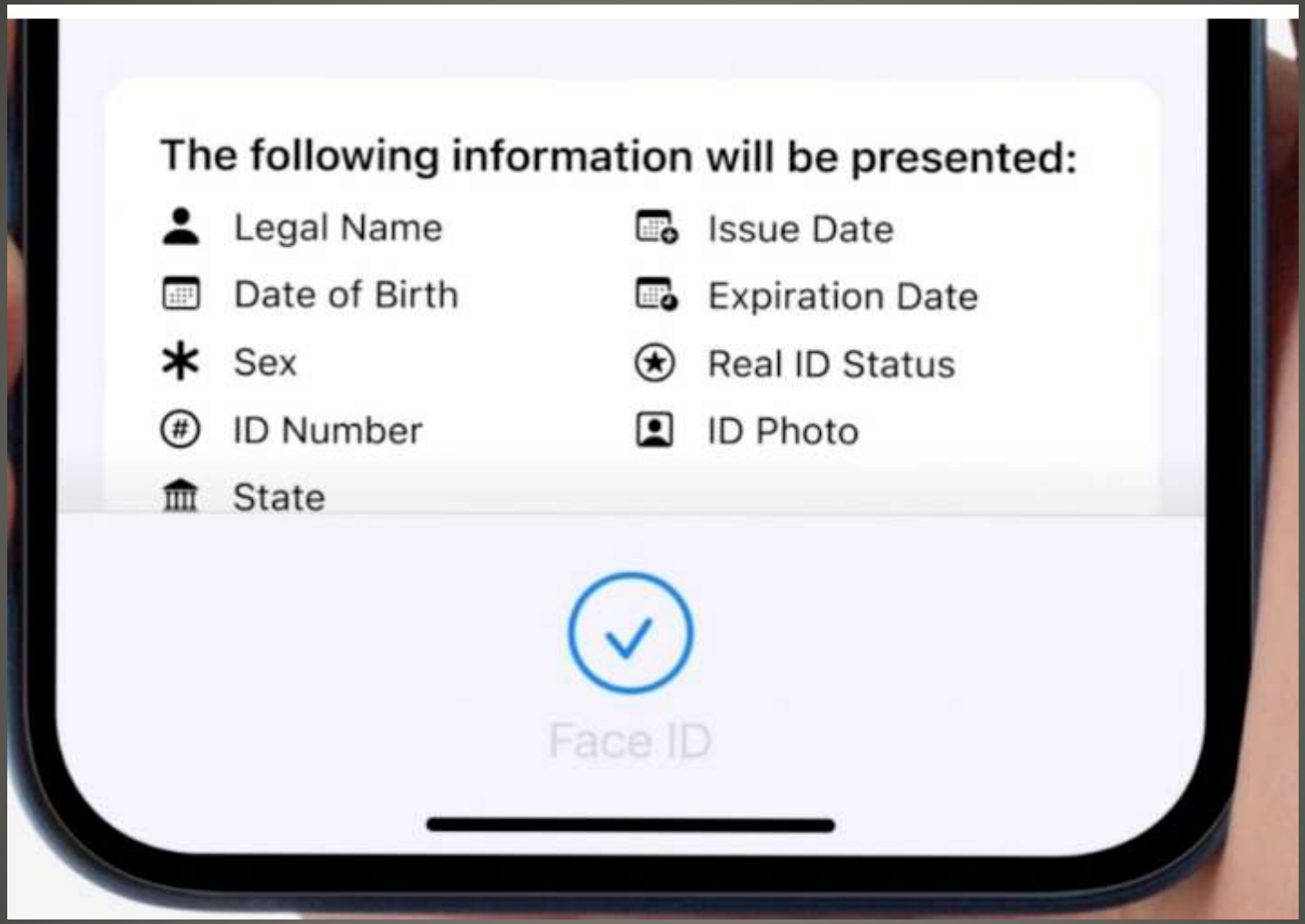
Apple digital IDs

Apple digital IDs

- iPhone 8 or later iOS 15.4
- Apple watch series 4 or later watchOS 8.4
- Wallet App
  Drivers License or State ID
  Add to iPhone and Apple Watch
  Add to iPhone
  Logon to state DMV to authorize
  Take selfie Scan Front & Back
  Secure transfer to state agency
  State defined head or other movements
- TSA using NFC readers
- NOT a substitute for having license in owners' possession



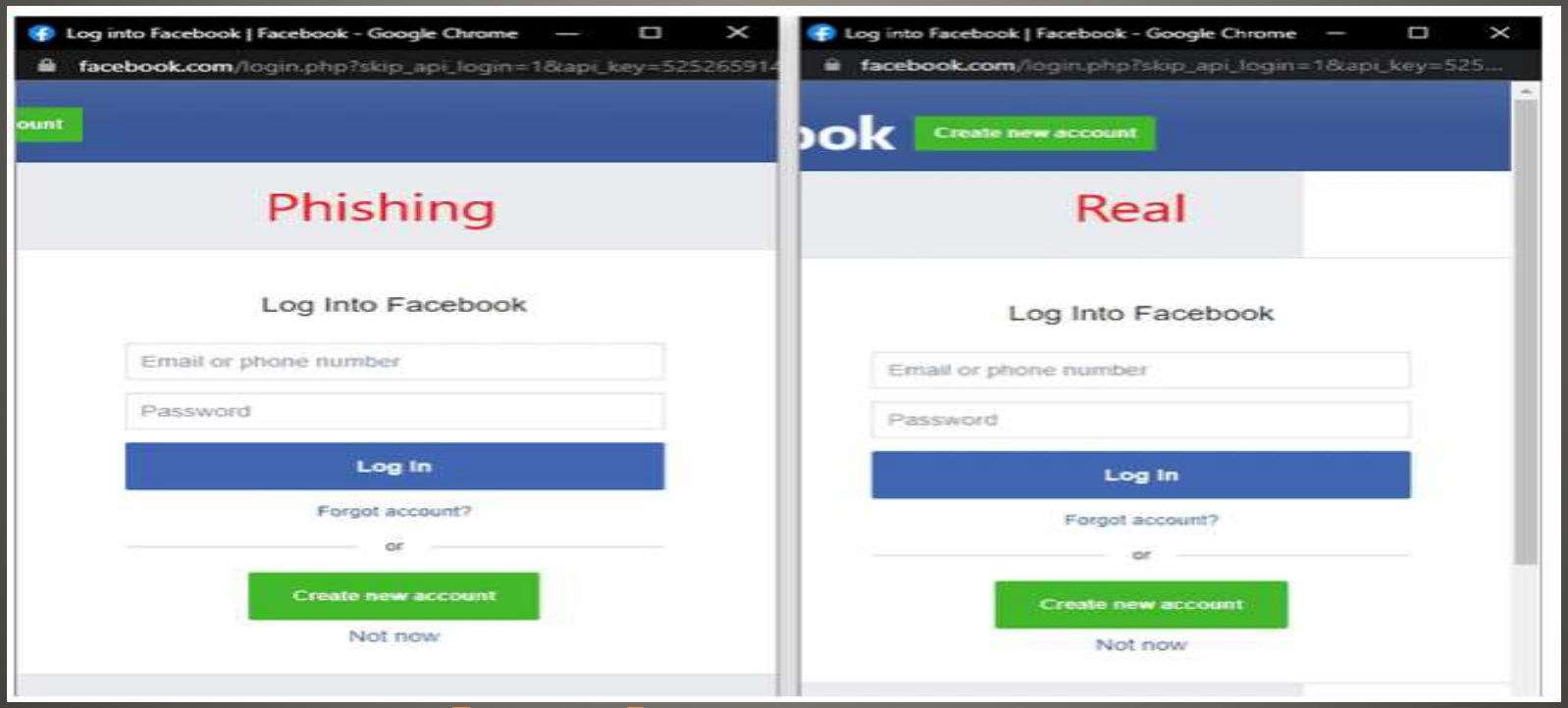
Apple digital ID



Apple digital ID

- Perfect? Convincing?
  simulate Single Sign On

  Sign in with {Google | Facebook | Apple| Microsoft }



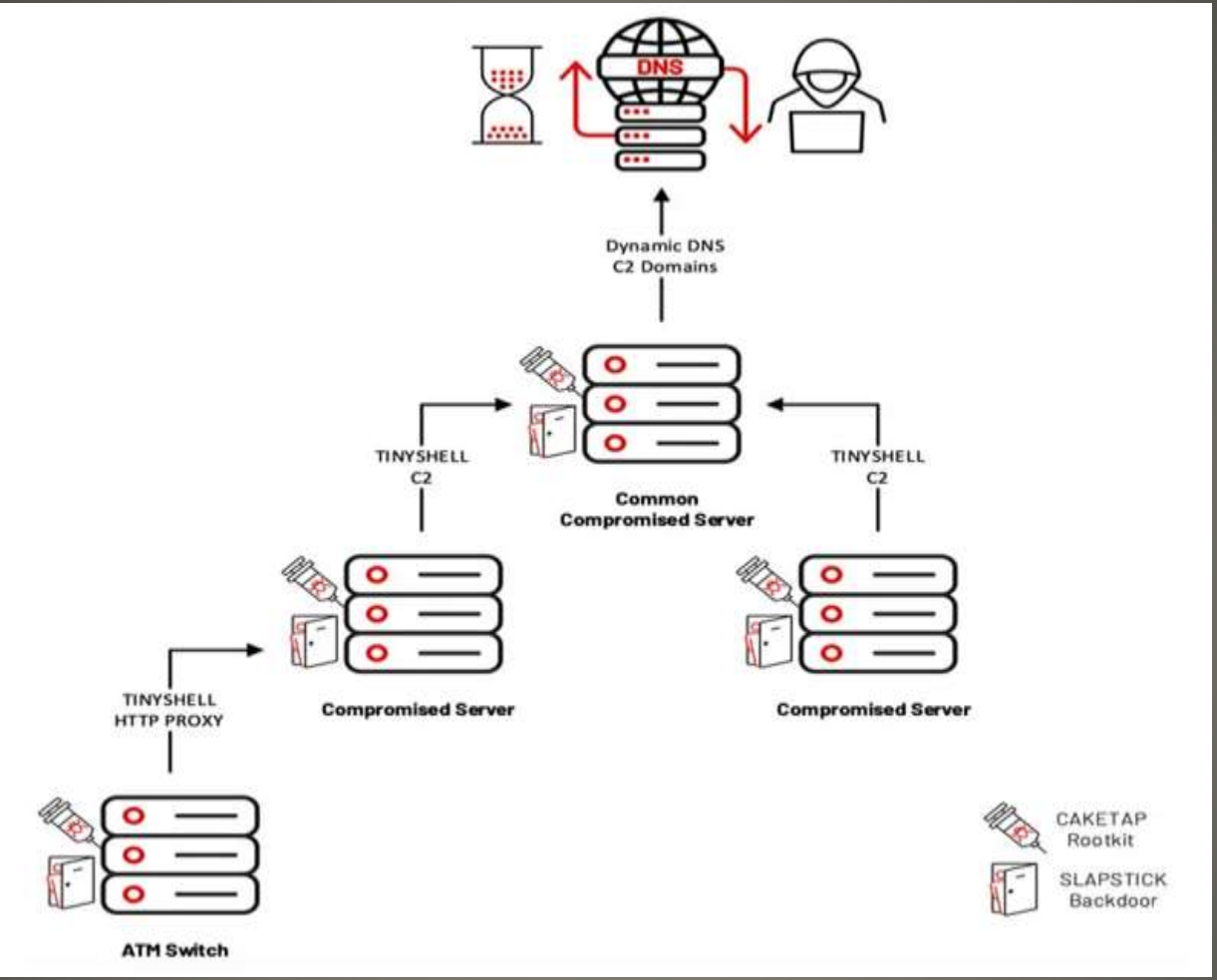
Browser in the Browser

- Exact & correct domain name
- Right site? Check
- Check URL? Check
- Check for look-a-like characters? Check

- Ready to use templates

- 10 days to in-the-wild detect

Browser in the Browser



ATM Switch Attack

- US Critical Infrastructure
  Bill passed 3/10/2022
  "substantial cyber incident" 3 days
  ransom paid 24 hours
- "Strengthening America Cybersecurity Act"
- Removed from defense policy bill
- Then passed with unanimous vote
- *What do they know?*
- CISA has 2 years to publish rules in Federal Register
- Goal Whole of government response

Critical Infrastructure

- Presidential Policy Directive 21, section 2242, subsection b
- Chemical, Commercial facilities, Communications, Critical manufacturing, Dams, Defense industrial base, Emergency services, Energy, Financial services, Food and agriculture, Government facilities, Healthcare and public health, Information technology, Nuclear reactors, Materials and waste, Transportation systems, Water and wastewater
- Subpoena power
- Civil or Criminal penalty?

Current Issues

- Dell Bios bugs
  5 security weaknesses
- Insyde software's InsydeH20
- HP Unified Extensible Firmware Interface
  UEFI

CVE-2022-14415
CVE-2022-24416
CVE-2022-24419
CVE-2022-24420
CVE-2022-24421
CVE rating 8.2
Persistent firmware implants
NOT detected by TPM

Current Issues

- AcidRain malware wipes Viasat satellite modems
- GPS jammers disrupting commercial airliners and others
- Facebook Messenger
- Microsoft Power Toys v0.57.0
- Hackers using EDRs
  Emergency Data Requests
  sans judge's signature
- Ukrtelecom cyber attack
- Chrome OS 100.0.4896.75
- Hydra shutdown
  Largest darknet marketplace
  US & German joint operation
- Elon Musk Twitter "deal" 241 words
- Wyze internet connected web cams

- BitDefender attempts 3 years
- Helpful <-> Harmful
- YOU – shared secret key
  send ID 0x2710 client to camera
  crypto magic
  client sends result as ID 0x2712
  encrypted channel
- THEM – just send 0x2712

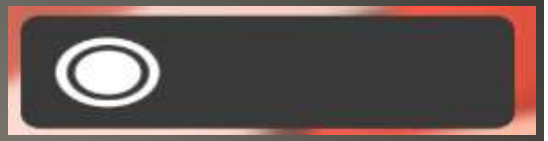
- AND SD card contents simple XOR
- Got one? Got 1st gen?

Wyze Internet connected web cams

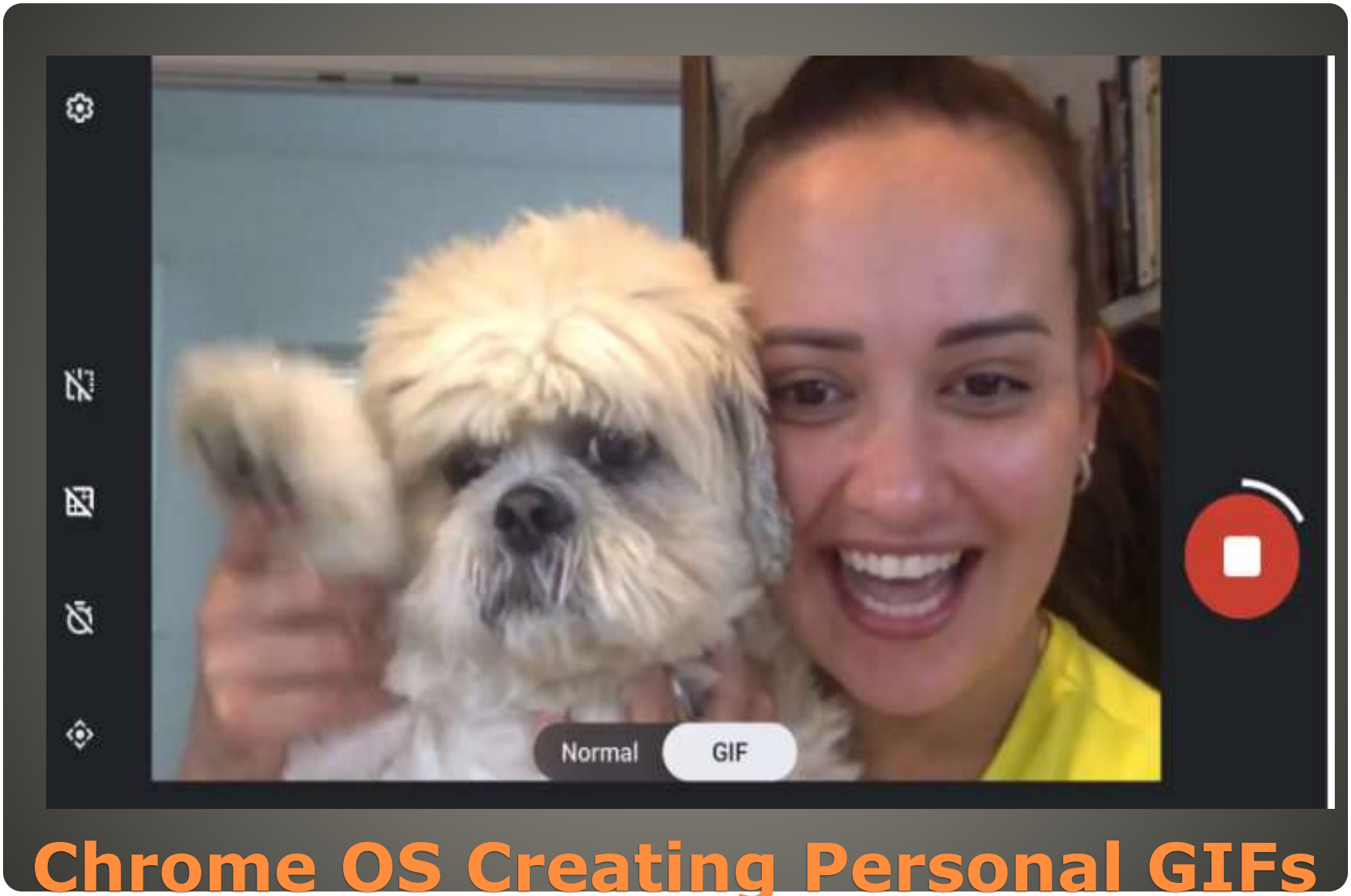
- New App launcher

Chrome OS Version 100

- Editing with Voice Dictation
  After Dictation activation
  Everything key + D
- Create personal GIFs
- Updated Android Container
  Android Runtime for Chrome (ARC)
  to
  Android Runtime for Chrome VM



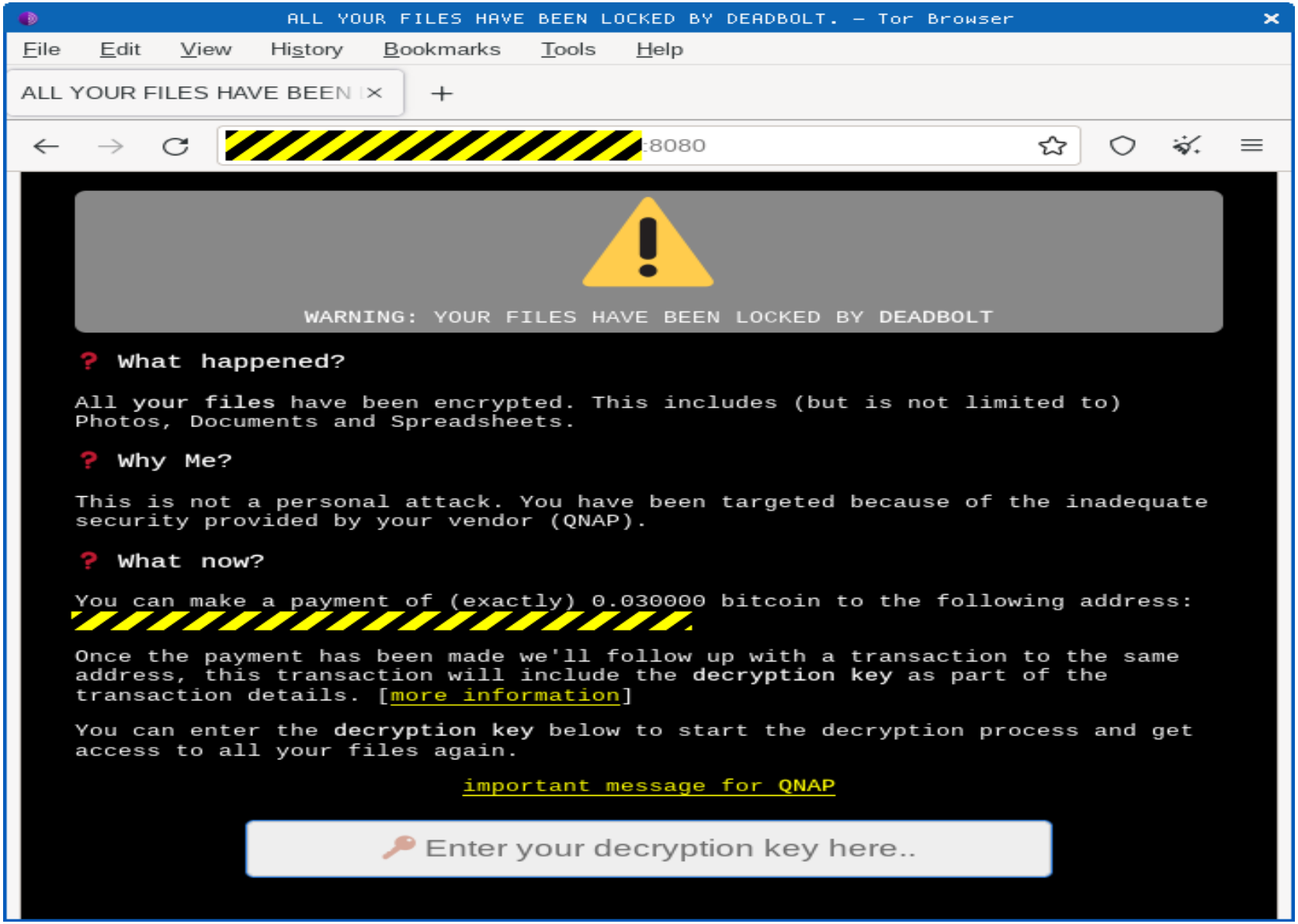
Chrome OS version 100



Chrome OS Creating Personal GIFs

- DeadBolt ransomware
  Seeks backup first

Current Issues


ALL YOUR FILES HAVE BEEN LOCKED BY DEADBOLT. — Tor Browser
File Edit View History Bookmarks Tools Help
ALL YOUR FILES HAVE BEEN
:8080
WARNING: YOUR FILES HAVE BEEN LOCKED BY DEADBOLT
? What happened?
All your files have been encrypted. This includes (but is not limited to) Photos, Documents and Spreadsheets.
? Why Me?
This is not a personal attack. You have been targeted because of the inadequate security provided by your vendor (QNAP).
? What now?
You can make a payment of (exactly) 0.030000 bitcoin to the following address:
Once the payment has been made we'll follow up with a transaction to the same address, this transaction will include the decryption key as part of the transaction details. [more information]
You can enter the decryption key below to start the decryption process and get access to all your files again.
important message for QNAP
Enter your decryption key here..

ALL YOUR FILES HAVE BEEN LOCKED BY DEADBOLT. — Tor Browser

File Edit View History Bookmarks Tools Help

ALL YOUR FILES HAVE BEEN

:8080

Obtaining Decryption Key

Our decryption key delivery process is **100% transparent and honest.**

The decryption key will be delivered to the bitcoin blockchain inside the **OP_RETURN** field. You can retrieve it by monitoring the address you made your payment to for new transactions containing the **OP_RETURN** field. An easy way to do this is using a public blockchain explorer like blockchain.com.

Outputs

Index	0
Address	
Pkscript	OP_RETURN 9025a8c9946f9ecc651879e49ff42a6e

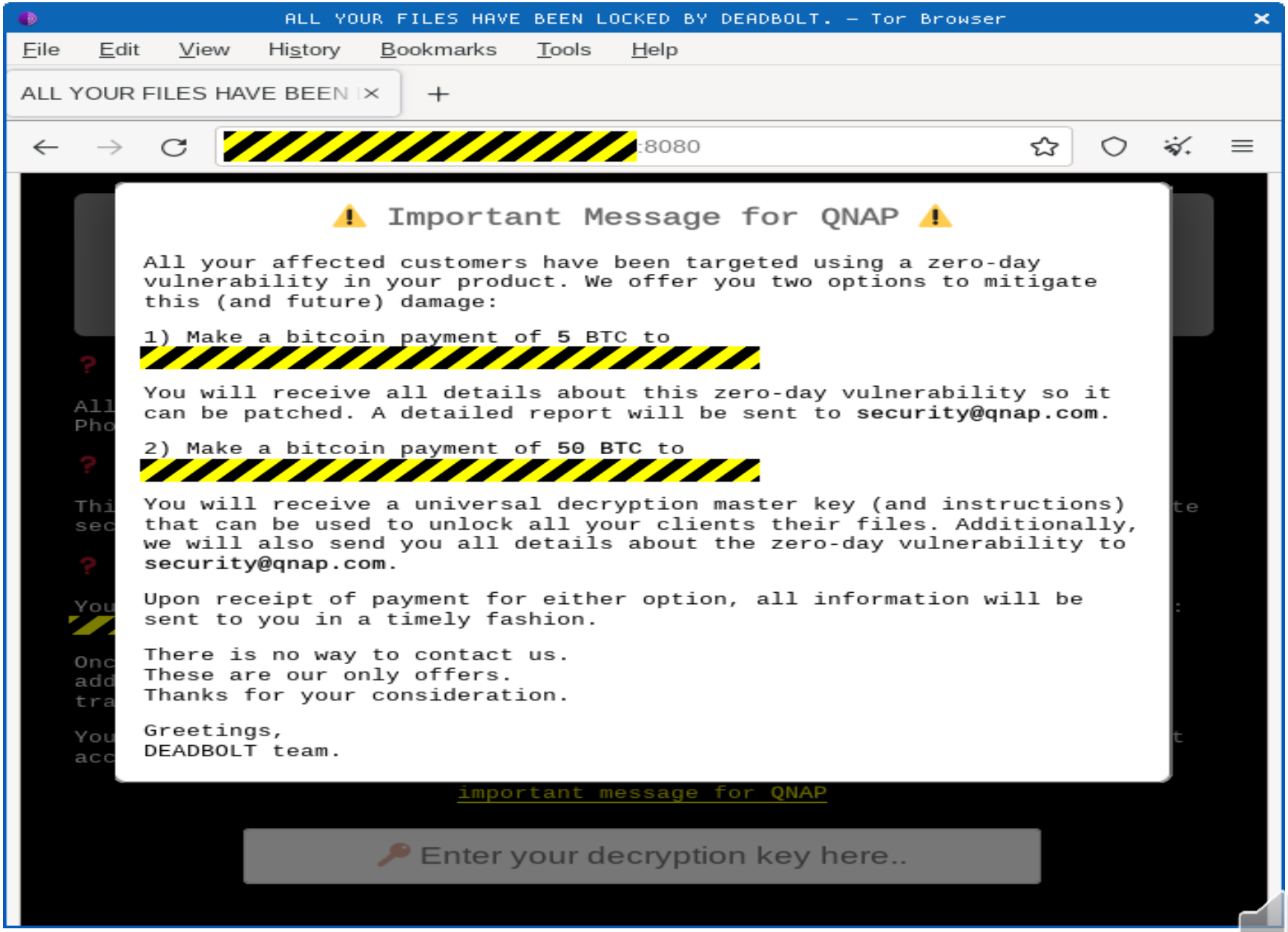
example of decryption key as found on **blockchain.com** explorer.

The decryption key always has an exact length of **32 characters.**

Entering the **wrong** decryption key **will not** harm your files. This page will tell you if the entered key is invalid.

After the decryption has finished successfully, this page will disappear and you can access the management interface again. However, it is **strongly advised** to migrate all your data to a more secure platform.

If you struggle with this process, please contact an IT professional to help you.


ALL YOUR FILES HAVE BEEN LOCKED BY DEADBOLT. – Tor Browser
File Edit View History Bookmarks Tools Help
ALL YOUR FILES HAVE BEEN
:8080
Important Message for QNAP
All your affected customers have been targeted using a zero-day vulnerability in your product. We offer you two options to mitigate this (and future) damage:
1) Make a bitcoin payment of 5 BTC to
You will receive all details about this zero-day vulnerability so it can be patched. A detailed report will be sent to security@qnap.com.
2) Make a bitcoin payment of 50 BTC to
You will receive a universal decryption master key (and instructions) that can be used to unlock all your clients their files. Additionally, we will also send you all details about the zero-day vulnerability to security@qnap.com.
Upon receipt of payment for either option, all information will be sent to you in a timely fashion.
There is no way to contact us.
These are our only offers.
Thanks for your consideration.
Greetings,
DEADBOLT team.
important message for QNAP
Enter your decryption key here..

- Delete everything …

  Settings > Alexa Privacy > Manage Your Alexa Data

  Enable deletion by voice

  "Alexa, delete what I just said"

  "Alexa, delete everything I said today"

  Helpful <-> Harmful

- Alexa, drop in

  Device name - All devices

  Confirmation tone

  OTHER HOMES

Alexa?

- Alexa App
  Devices > Echo & Alexa > Drop In
  Enable
  Allow Drop In
- Alexa Calling & Messaging
- BOTH parties must setup

Alexa Drop In setup

- Video Calling
- Hands Free
- “announce I am on my way home”
- “Call for help” Emergency Contacts
- Captioning
- Whisper mode
- Pair with Bluetooth
- Beer Goggles
- Skills

Smart Speakers

- Remote Access Trojan (RAT)
- Spyware
- Ransomware
- Builder, feature modules, server certificate
- DDoS
- Record audio & video
- Take control mouse and/or keyboard
- Screen captures
- Modify system settings
- Stealing and/or deleting files Modification
- Reverse proxy
- Browser manipulations

Borat RAT malware


Borat~RAT
#1 Remote Administration Tool

FEATURES

Remote hVNC

- ✓ Hidden Desktop
- ✓ Hidden Browsers
- ✓ Hidden Chrome
- ✓ Hidden Firefox
- ✓ Hidden Edge
- ✓ Hidden Internet Explorer
- ✓ Hidden Pale Moon
- ✓ Hidden Pale Waterfox
- ✓ Hidden Explorer

Remote Fun

- ✓ Monitor on/off
- ✓ Open/close CD
- ✓ Show/Hide taskbar
- ✓ Show/Hide Start Button
- ✓ Show/Hide Explorer
- ✓ Show/Hide Clock
- ✓ Show/Hide Tray
- ✓ Show/Hide Mouse
- ✓ Enable/Disable TaskMgr
- ✓ Enable/Disable Regedit
- ✓ Disable UAC
- ✓ much more...

Remote System

- ✓ System Information
- ✓ File Manager
- ✓ Start Up Manager
- ✓ Task Manager
- ✓ Remote Shell
- ✓ TCP Connection
- ✓ Reverse Proxy
- ✓ Registry Editor
- ✓ UAC Exploit
- ✓ Disable WD
- ✓ Format All Drivers
- ✓ much more...

Car Key Fobs

- RollJam attack
- Yeahbut Honda still replay success
- why ?
  Little testing
  even less accountability or regulation

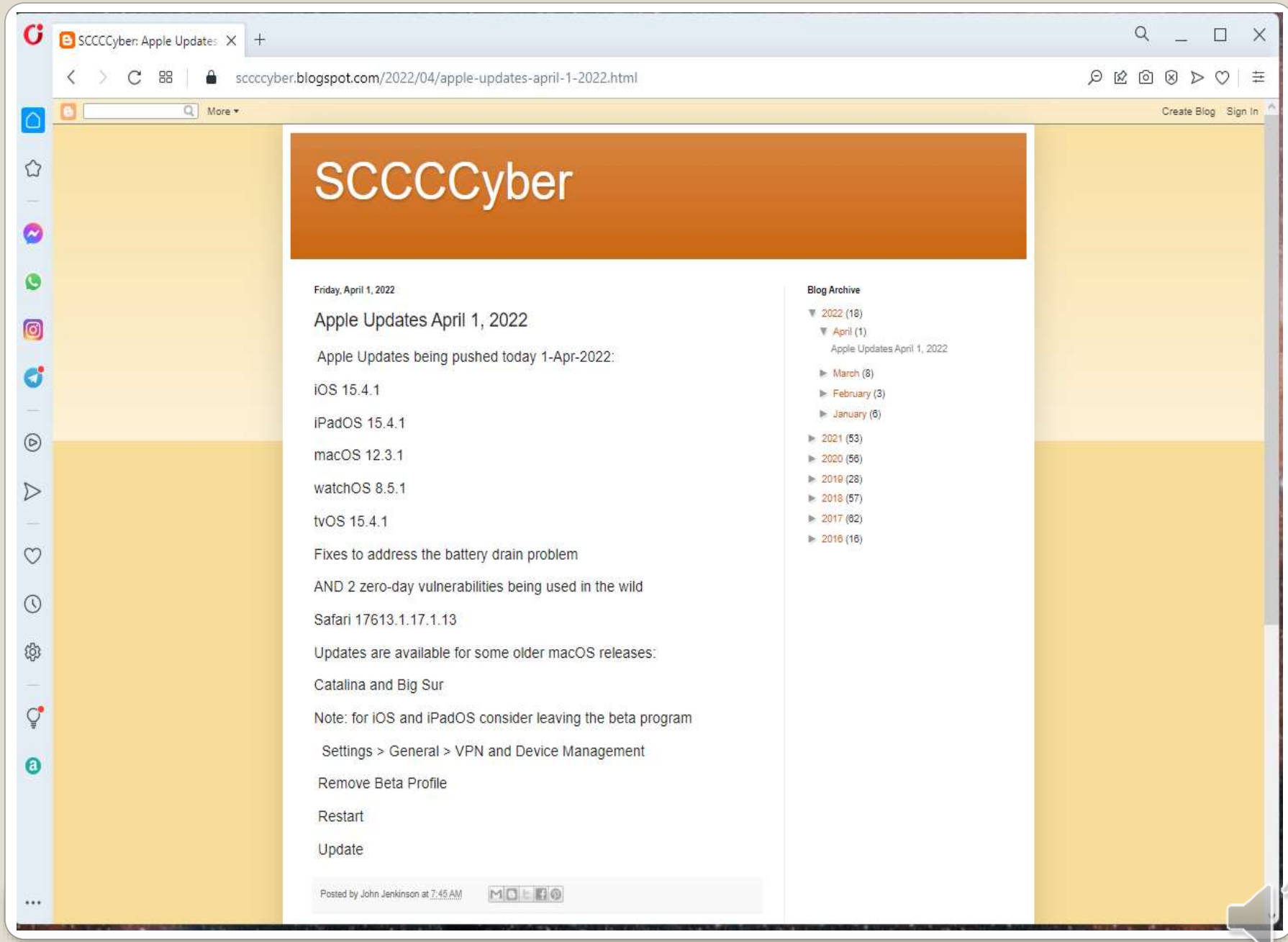
And garage doors
shift registers

- Cyber Security SIG web site to use ANNOUNCEMENTS

Cyber Security SIG updates

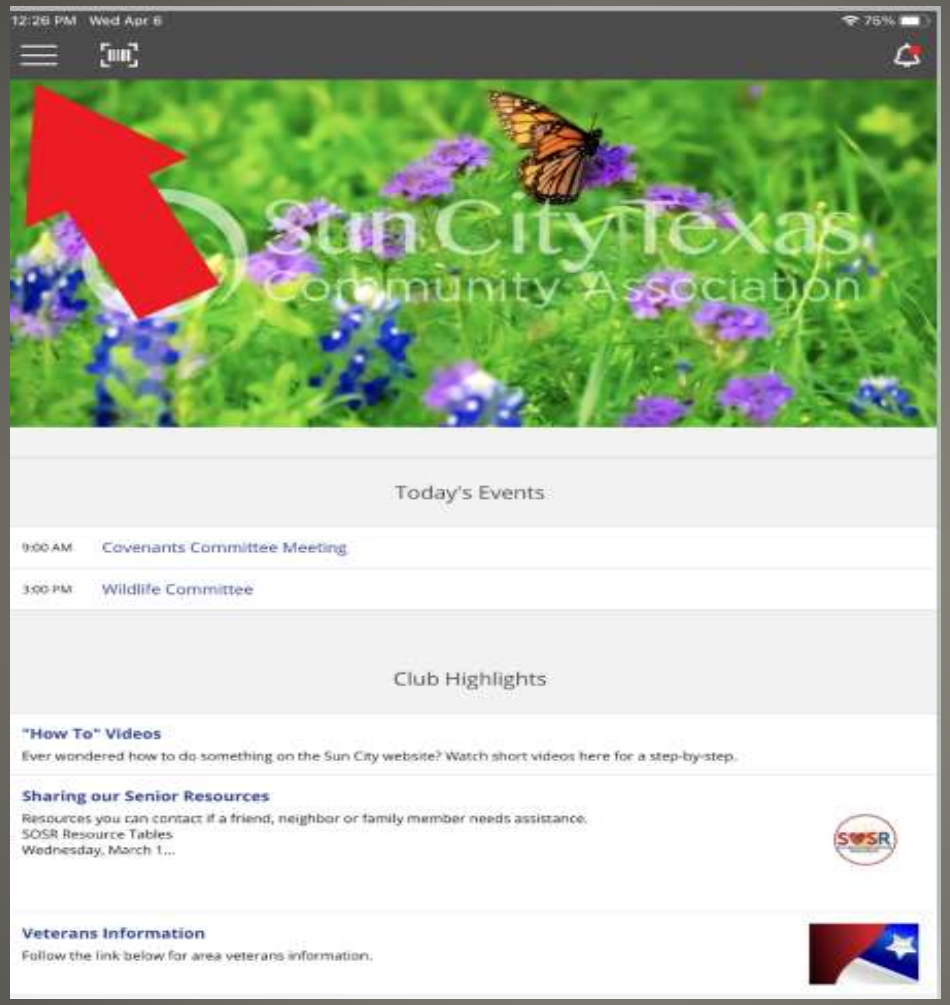
- Announcements will usually be links
- Click on link for more information
- Example:

Cyber Security SIG updates

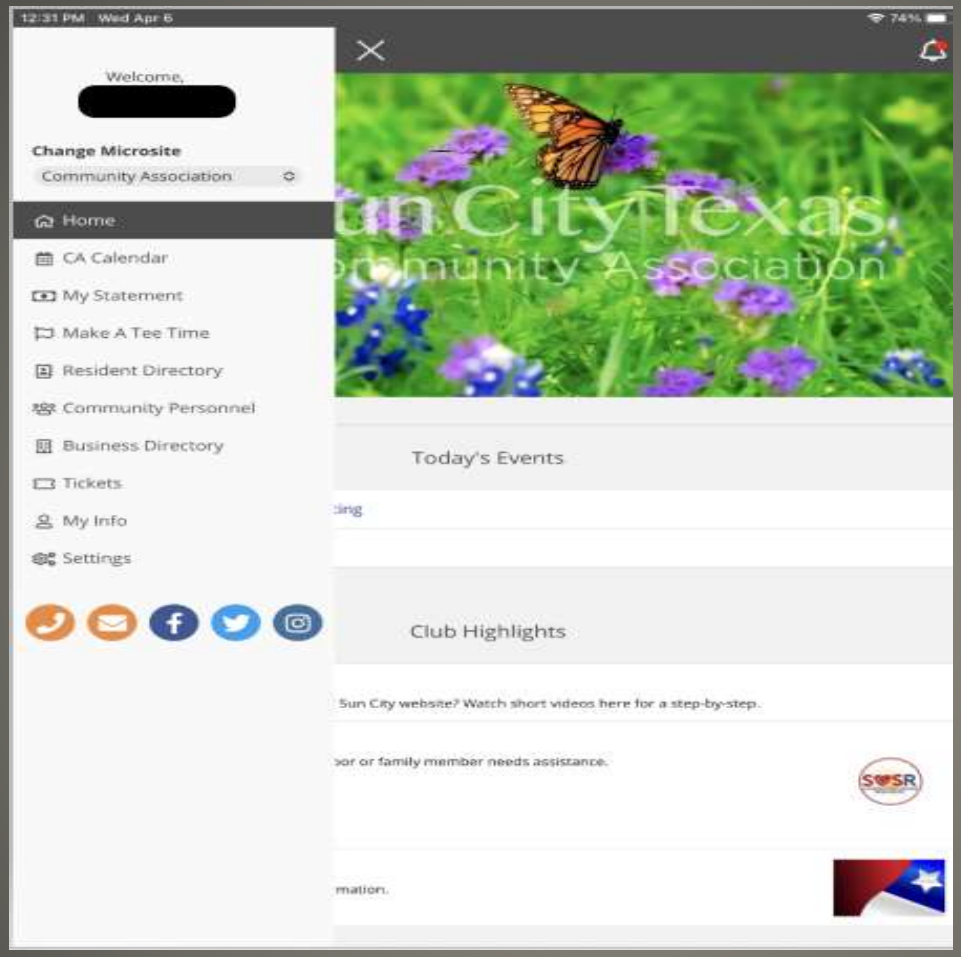

SCCCCyber: Apple Updates
sccccyber.blogspot.com/2022/04/apple-updates-april-1-2022.html
More
Create Blog
Sign In
SCCCCyber
Friday, April 1, 2022
Apple Updates April 1, 2022
Apple Updates being pushed today 1-Apr-2022:
iOS 15.4.1
iPadOS 15.4.1
macOS 12.3.1
watchOS 8.5.1
tvOS 15.4.1
Fixes to address the battery drain problem
AND 2 zero-day vulnerabilities being used in the wild
Safari 17613.1.17.1.13
Updates are available for some older macOS releases:
Catalina and Big Sur
Note: for iOS and iPadOS consider leaving the beta program
Settings > General > VPN and Device Management
Remove Beta Profile
Restart
Update
Posted by John Jenkinson at 7:45 AM
Blog Archive
2022 (18)
April (1)
Apple Updates April 1, 2022
March (8)
February (3)
January (6)
2021 (53)
2020 (56)
2019 (28)
2018 (57)
2017 (62)
2016 (16)

- From Apple Store and/or Google Play Store
- Search Sun City Community Association
- Open *Sun City Community Association* App
- Sign in with your Community Association credentials

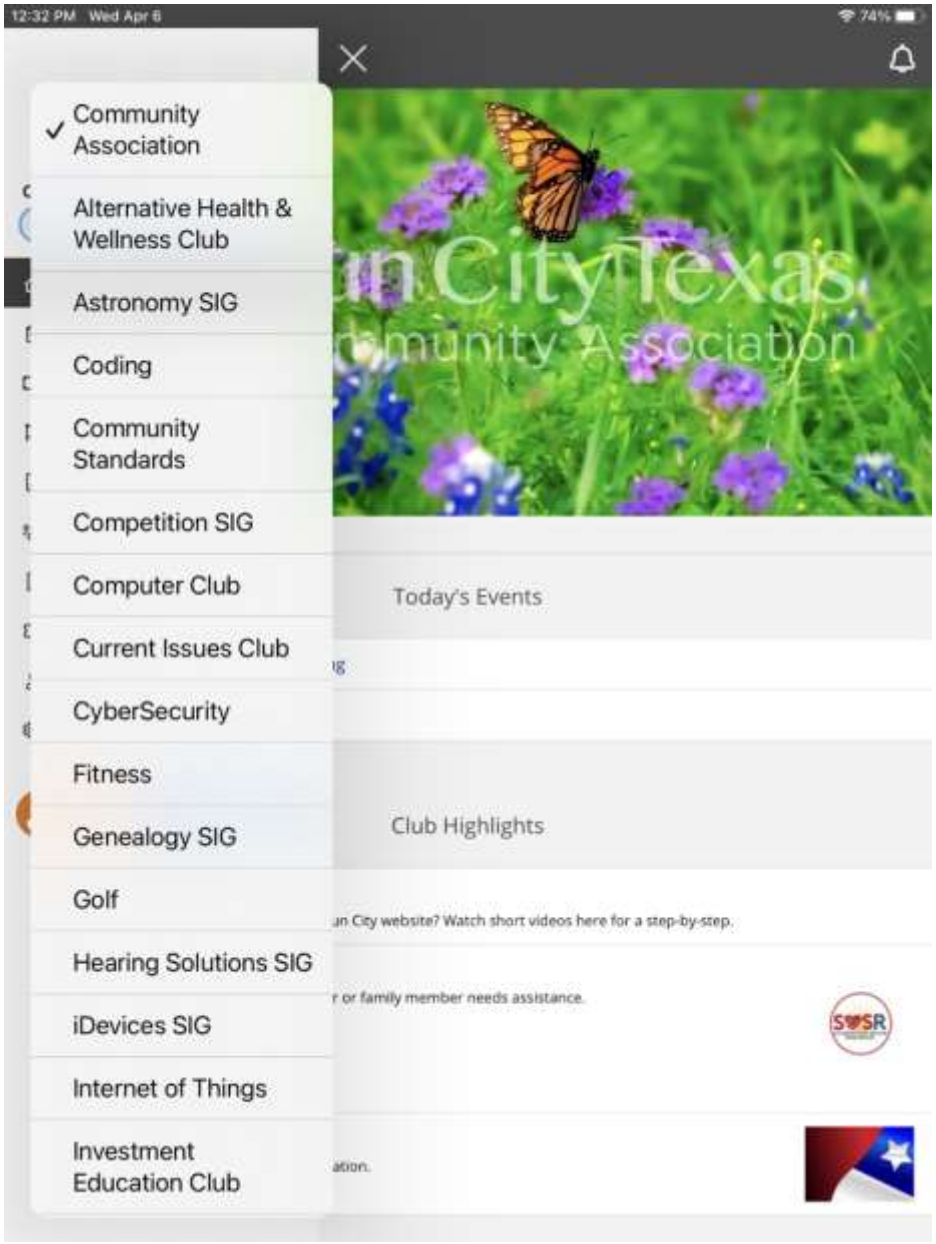
Mobile App Sun City CA



Open Menu button



Select the CA site


12:32 PM Wed Apr 6
74%
Community Association
Alternative Health & Wellness Club
Astronomy SIG
Coding
Community Standards
Competition SIG
Computer Club
Current Issues Club
CyberSecurity
Fitness
Genealogy SIG
Golf
Hearing Solutions SIG
iDevices SIG
Internet of Things
Investment Education Club
Today's Events
Club Highlights
SOSR

CyberSecurity

Announcements

Apple Updates

Next Meeting

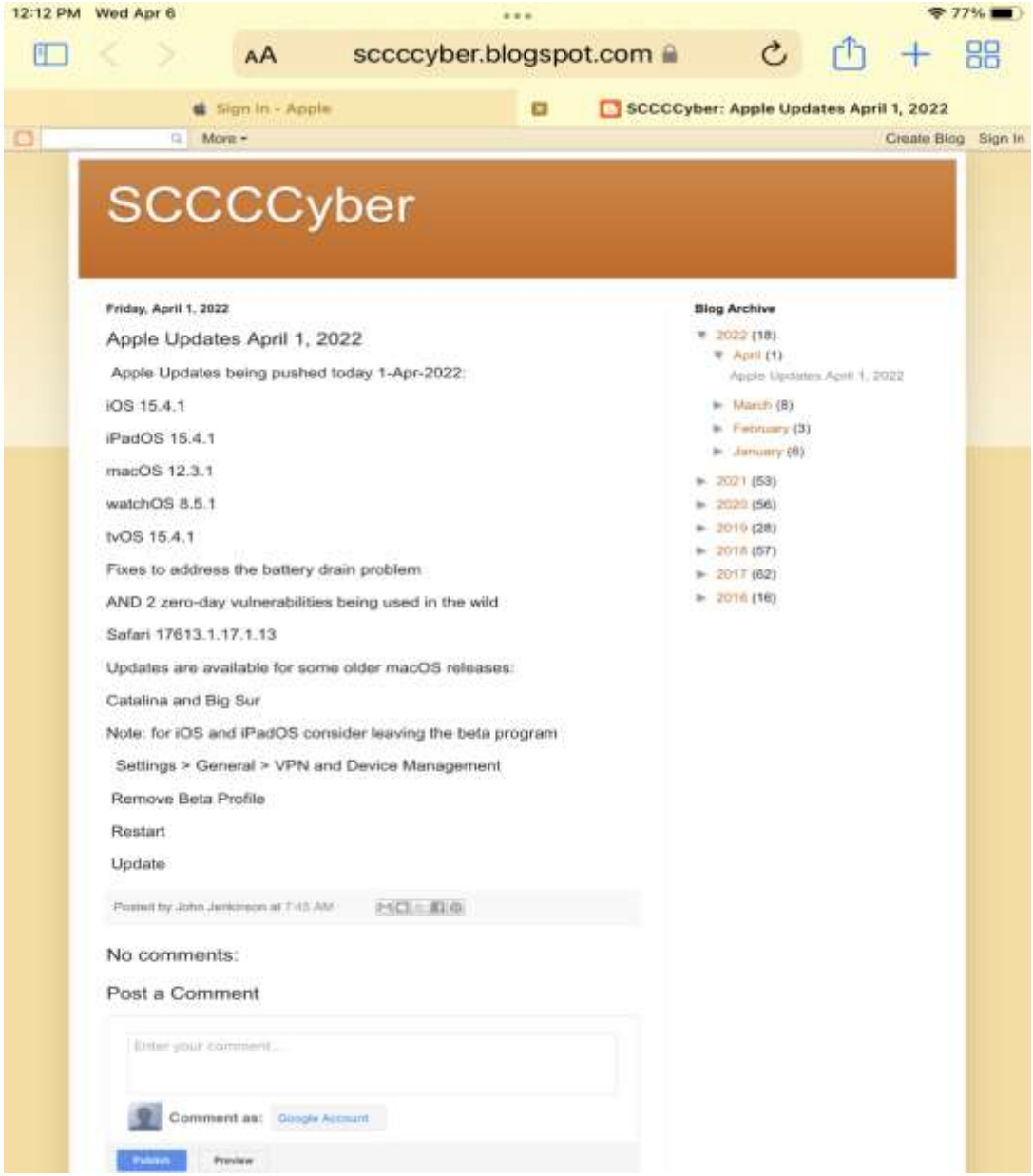
Club Highlights

Meetings

Note: All meetings are now audio recordedNext Presentation with audio April 7, 2022ZoomZoom Invitation: https://us02web.zoom.us/...

Overview

Current news articles are given in the Cyber Security News Archive link.Tutorials on computer topics are given in the Seminars l...


12:12 PM Wed Apr 6
77%
AA
sccccyber.blogspot.com
Sign In - Apple
SCCCCyber: Apple Updates April 1, 2022
More
Create Blog
Sign In
SCCCCyber
Friday, April 1, 2022
Apple Updates April 1, 2022
Apple Updates being pushed today 1-Apr-2022:
iOS 15.4.1
iPadOS 15.4.1
macOS 12.3.1
watchOS 8.5.1
tvOS 15.4.1
Fixes to address the battery drain problem
AND 2 zero-day vulnerabilities being used in the wild
Safari 17613.1.17.1.13
Updates are available for some older macOS releases:
Catalina and Big Sur
Note: for iOS and iPadOS consider leaving the beta program
Settings > General > VPN and Device Management
Remove Beta Profile
Restart
Update
Posted by John Jenkinson at 7:45 AM
No comments:
Post a Comment
Enter your comment...
Comment as:
Google Account
Publish
Preview
Blog Archive
2022 (18)
April (1)
Apple Updates April 1, 2022
March (8)
February (3)
January (6)
2021 (53)
2020 (56)
2019 (28)
2018 (57)
2017 (62)
2016 (16)

- MLB to use Pitch Calling system

Current Issues

- 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