Sun City Computer Club

Cyber Security SIG

June 21, 2023

Questions, Comments, Suggestions welcomed at any time

Even Now

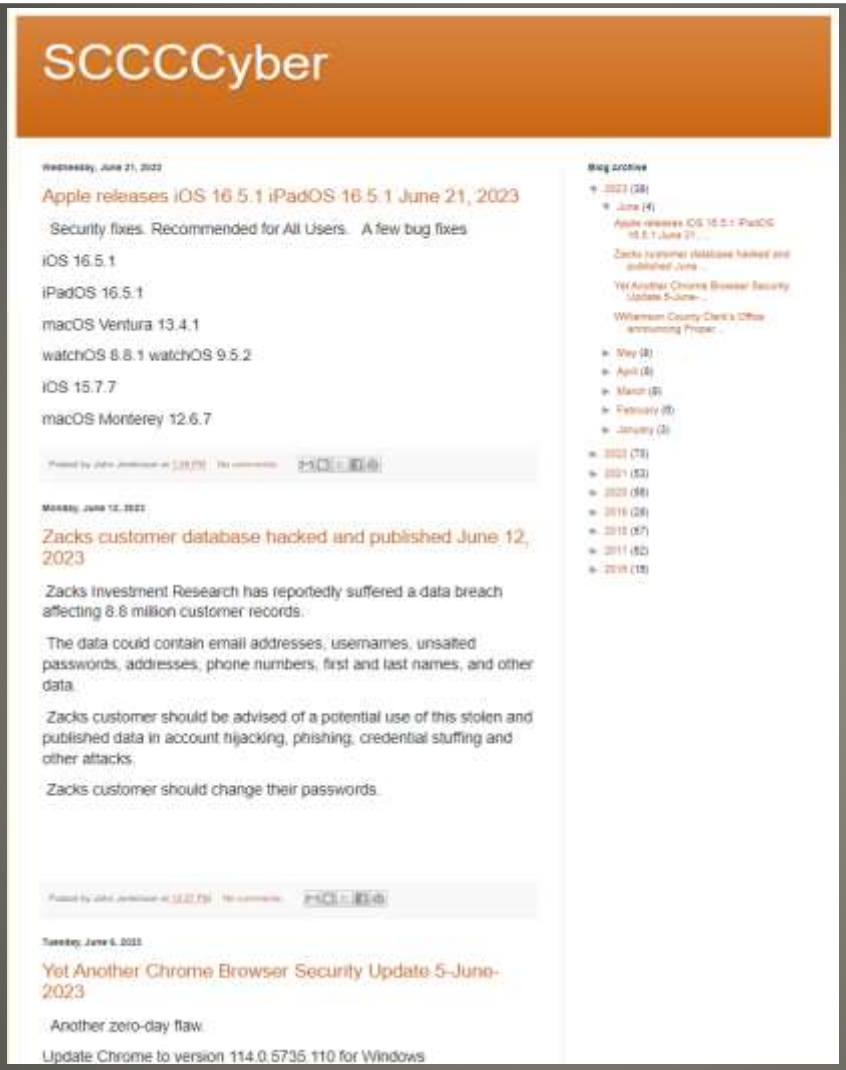
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

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

Special Edition

- Normal presentation: 15-June
- Special presentation due to:
- Apple Security fixes release June 21
- Our status: Home bound
- HEAT
- Vimeo advantages:
- Your schedule
- Adjust volume
- Adjust size
- Pause, rewind, replay, closed caption, exit early, …
- Presentation with our zoom attendance
- Others



SCCCCyber

Wednesday, June 21, 2023

Apple releases iOS 16.5.1 iPadOS 16.5.1 June 21, 2023

Security fixes. Recommended for All Users. A few bug fixes

iOS 16.5.1

iPadOS 16.5.1

macOS Ventura 13.4.1

watchOS 8.8.1 watchOS 9.5.2

iOS 15.7.7

macOS Monterey 12.6.7

Monday, June 12, 2023

Zacks customer database hacked and published June 12, 2023

Zacks Investment Research has reportedly suffered a data breach affecting 8.8 million customer records.

The data could contain email addresses, usernames, unsalted passwords, addresses, phone numbers, first and last names, and other data.

Zacks customer should be advised of a potential use of this stolen and published data in account hijacking, phishing, credential stuffing and other attacks.

Zacks customer should change their passwords.

Tuesday, June 6, 2023

Yet Another Chrome Browser Security Update 5-June-2023

Another zero-day flaw

Update Chrome to version 114.0.5735.110 for Windows

Blog Archive

Cyber Security Archive News

SCCCCyber

Wednesday, June 21, 2023

Apple releases iOS 16.5.1 iPadOS 16.5.1 June 21, 2023

Security fixes. Recommended for All Users. A few bug fixes

iOS 16.5.1

iPadOS 16.5.1

macOS Ventura 13.4.1

watchOS 8.8.1 watchOS 9.5.2

iOS 15.7.7

macOS Monterey 12.6.7

Posted by John Jenkinson at 1:39 PM

ANNOUNCEMENTS

- Apple releases iOS 16.5.1 iPadOS 16.5.1 June 21, 2023

« ALL CLUBS
« COMPUTER CLUB
CYBERSECURITY
MEETING NOTES

CYBERSECURITY

MEETINGS

Note: All meetings are now audio recorded

Next Presentation with audio

July 6, 2023

3:00 pm - 4:00 pm

Zoom

- Ever want to be a presenter??

- Apple Users Group SIG
- Join Now
- First meeting September 8

- Until then, iDevices topics in Mac Users Group

Presenter???

Operation Triangulation

- Kaspersky employees iPhones with malware
- No click
- iMessage
- Then infecting message deleted
- Transmits personal information:
  microphone, camera, geolocation, and more
- Russian FSB blames NSA and Apple
- iOS 15.7 and earlier

- The following reports came from the Georgetown Police Chief:

- "We are fraud detectives from Amazon. We need you to buy gift cards to remove hackers from your account." – Successful
- "There has been a loan made on your Paypal account and your Bank of America has issues as well. Send $13,000 to this bitcoin account to clear it up." – Successful
- "Computer notification from Microsoft that says computer is compromised. Insert bank account information and buy gift cards" – Mostly Successful
- "Email and phone call from a personal friend who says they need money because of a banking issue. Credit card information emailed to the friend." – Successful
- "Your money is in danger in your account. Transfer all $34,000 into my account to protect it" – Successful
- "You owe between $21,000 and $23,000 in credit. We can close all that out for $7,000." Later sent another $3,000 because of issues." - Successful
- "The Social Security Administration is giving out bonuses to those who collect retirement. Get Apple gift cards. Also send money via CashApp to see if it works." – Successful
- "Email from PayPal saying money charged. Call to dispute. PayPal rep takes over computer and takes $4,500 from bank account. Claims it was a mistake. Asks for gift cards in that amount to offset. Now out $9,000." – Successful

- Now imagine the incidents not reported.
- PLEASE report incidents.

- Utilize the NRO Anti-Fraud group's resources.

- Become more cyber aware.

- Not one more financial loss to our residents.

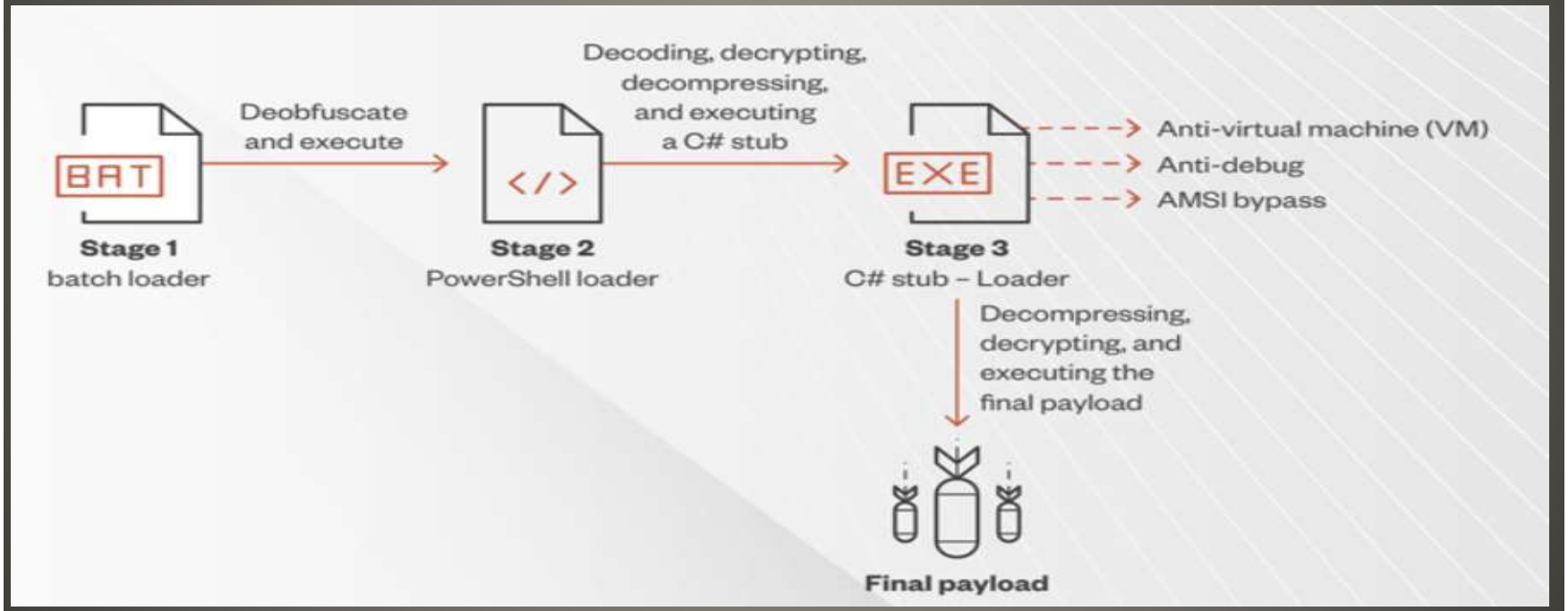
Facebook Post

Zacks

- Zacks Investment Research has reportedly suffered a data breach affecting 8.8 million customer records.
- The data could contain email addresses, usernames, unsalted passwords, addresses, phone numbers, first and last names, and other data.
- Zacks customer should be advised of a potential use of this stolen and published data in account hijacking, phishing, credential stuffing and other attacks.
- Zacks customer should change their passwords.

Zacks Customer Data example

- BatCloak
- Fully undetectable malware obfuscation engine
- Undetectable across ALL security solutions



BatCloak

- New campaign
- Legitimate trusted sites
- Inject and hide credit card stealing scripts
- Most victim sites unaware
- No need for attackers to create & maintain
- So many sites with critical vulnerabilities
- Sites: security updates/settings
  Protect web site admin accounts
- Us: electronic payment methods
  Virtual cards
  Charge limits

Hackers hijack legitimate sites Host credit card stealing scripts

Current Issues

- Consumer Financial Protection Bureau
  Warning storing funds in payment apps
- Other Toyota misconfigured database servers
- Google Drive
  Attacker revokes paid license
  Google quits logging
  Attacker steals files with no trace
- Horabot botnet .rar archive
  Hijack email accounts - WARNING Trust
- Windows Enterprise to require SMB signing
  Limit NTLM attacks
- MOVEit vulnerability
  BBC, British Air

SEC Actions

- Binance
  web of deception
- Coinbase
  middleman crypto transactions
  No disclosure requirements to protect consumers
- SEC jurisdiction
- Tokens not Securities

- Unlock Bitwarden vault with biometrics
- FaceID, fingerprint
- Credential stuffing
- Android FaceID phone
  fingerprint for secure apps
- Device(s) with biometric capability enabled
- Bitwarden Master password (look both ways)
- Settings > Security

Bitwarden now with biometrics

Recover Facebook Account

- 160 million hacked accounts per day
- Credential stuffing
- Changes to email, password, profile
- Friend requests you did not make
- Messages you did not write

- Change your password
- Use MFA
- Check which devices are logged in
  Password and Security
  "Where You're Logged In"
  Click on suspicious login
  Secure Account
- Notify Facebook
  Password and Security
  "Get Help"
- Report crime

Recover Facebook Account

- Facebook.com/hacked

- Strengthen password
- Use Multi factor authentication
- Disable connected apps
- Password and Security

  3-5 trusted friends - receive links & codes
- Limit info you share

Trend Micro Warning Signs

- Friends and family say they are getting spam messages from your account
- Your computer and browser's performance has slowed down
- Your computer has started acting erratic
- Your saved or commonly used passwords no longer word
- Your IP address has changed
- You have received an unrequested password change/recovery email
- Money is missing from an online account
- There are unusual changes in your network's traffic activity
- You have received a ransomware messages
- You have received a falsified antivirus alert
- You have spotted unwanted toolbars in your browser

iPhone protection

- Screen Time setting
- Apple Watch automation
- Must Be Quick
- Create Focus on iPhone

  Settings > Focus

  + Lock Screen

  Shortcuts App > Automation

  Create Personal Automation

Tap Lock Screen
When Turning On
Next
Add Action
Lock Screen
Airplane Mode Off
Set Mobile Data On
Set Bluetooth On
Set Wi-Fi On
Set Low Power Mode on
Show Notification
"This is a stolen Phone ….."
Next
Disable Ask Before Running
Done

iPhone Protection

- Apple Watch
  Control Center
  Lock Screen
  On

iPhone Protection

- Adds biometrics on desktops
  PCs & Macs
  Facial Recognition and/or Fingerprint
- Add notes
- Import

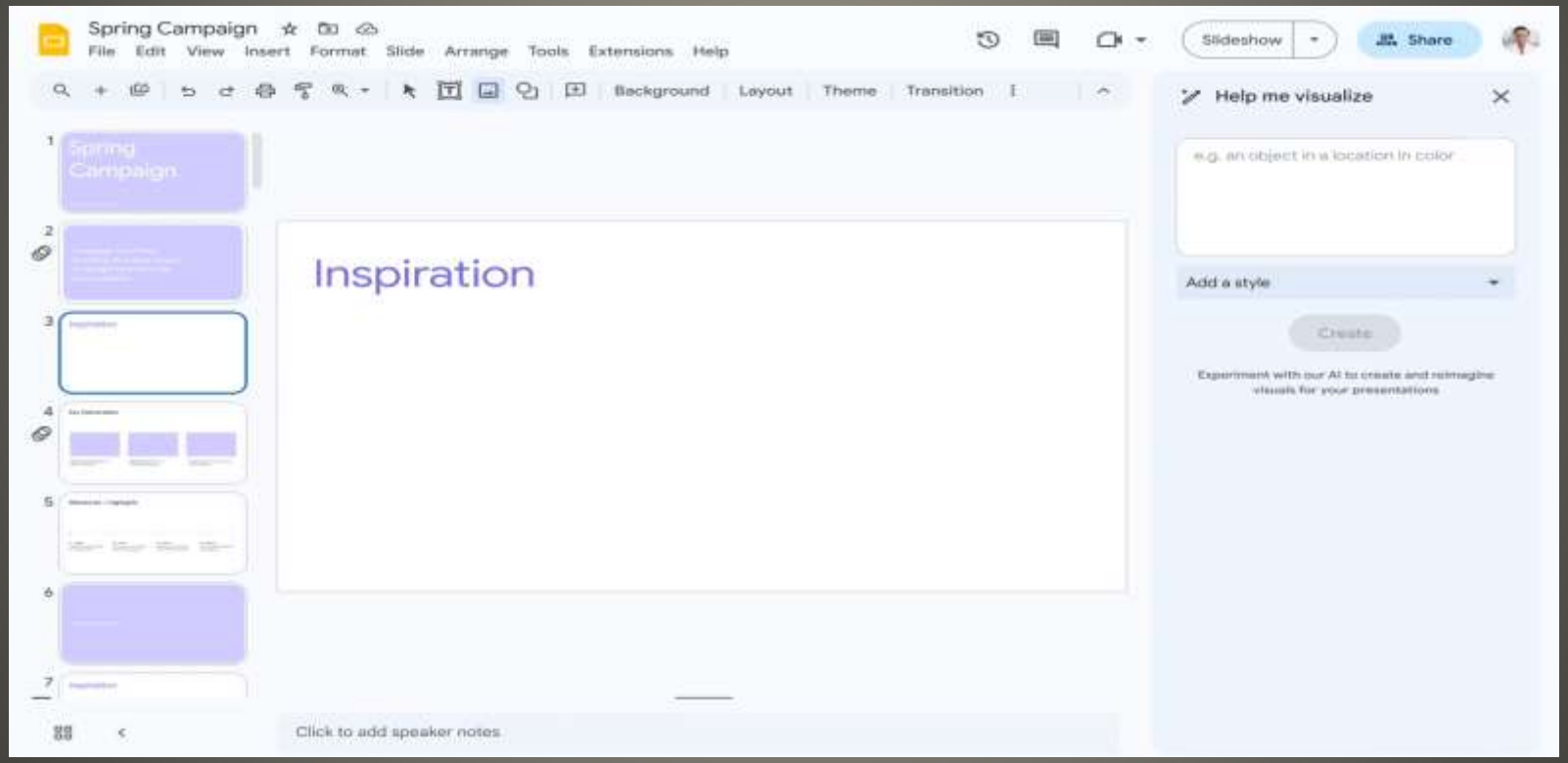
Google Chrome Password Manager

Devices

- Only way to get unlocked device

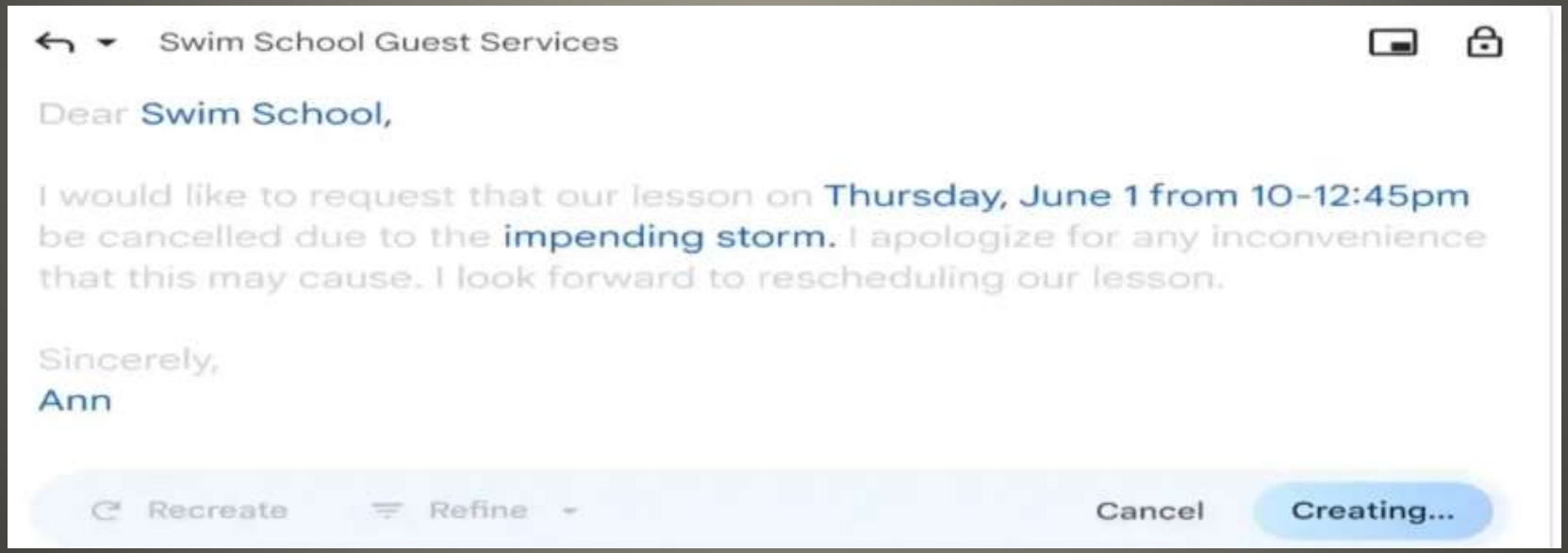
iPhone iPad Direct from Apple

- Google March Generative AI
- Slides **Help me visualize**



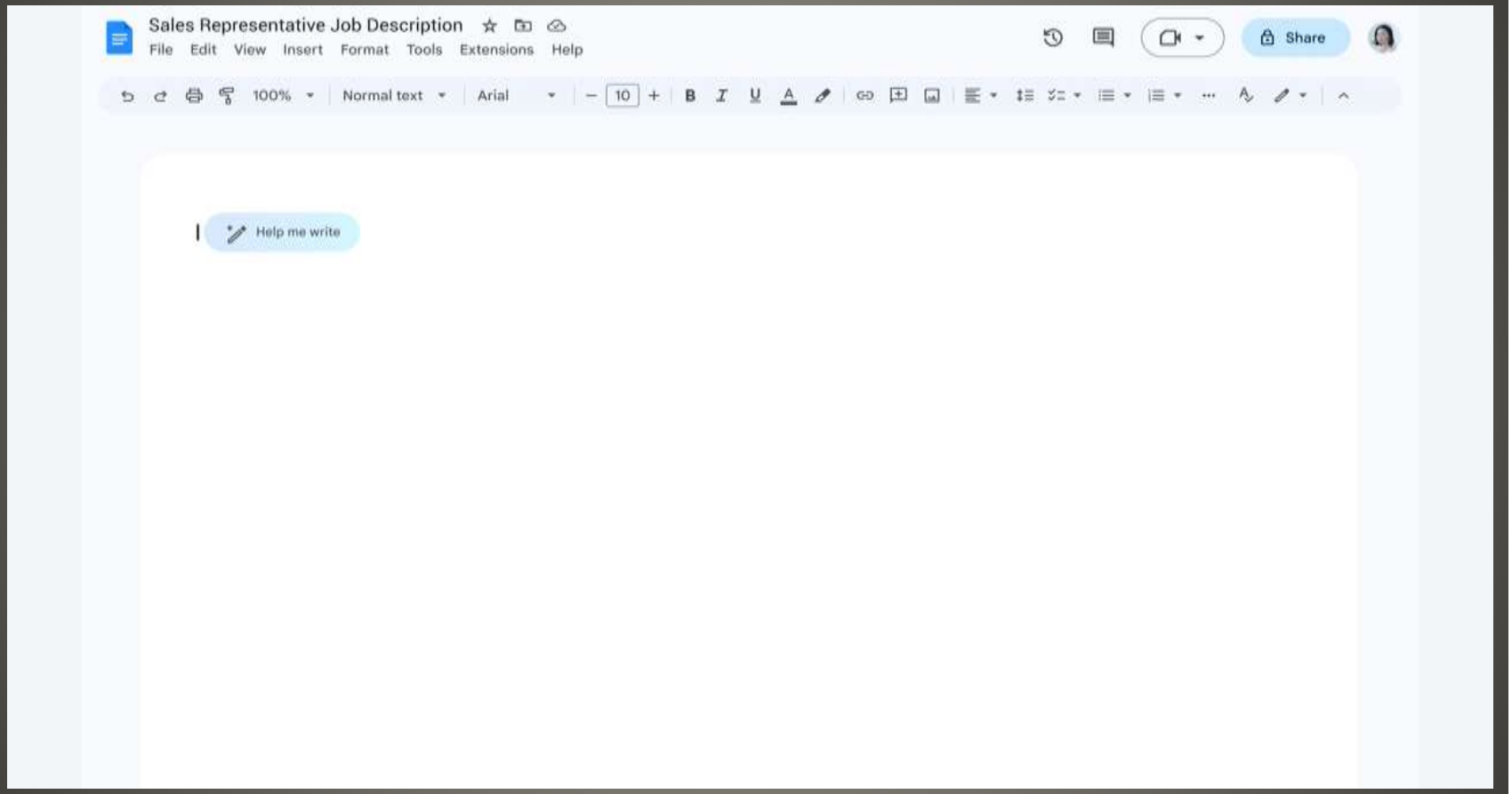
Google Docs, Slides, Gmail AI

- Gmail **Help me write**
- Older emails in thread contextual assistance



Google Docs, Slides, Gmail AI

- Docs



Google Docs, Slides, Gmail AI

Limit Blue Light iPhone

- Night Shift
- Schedule Night Shift

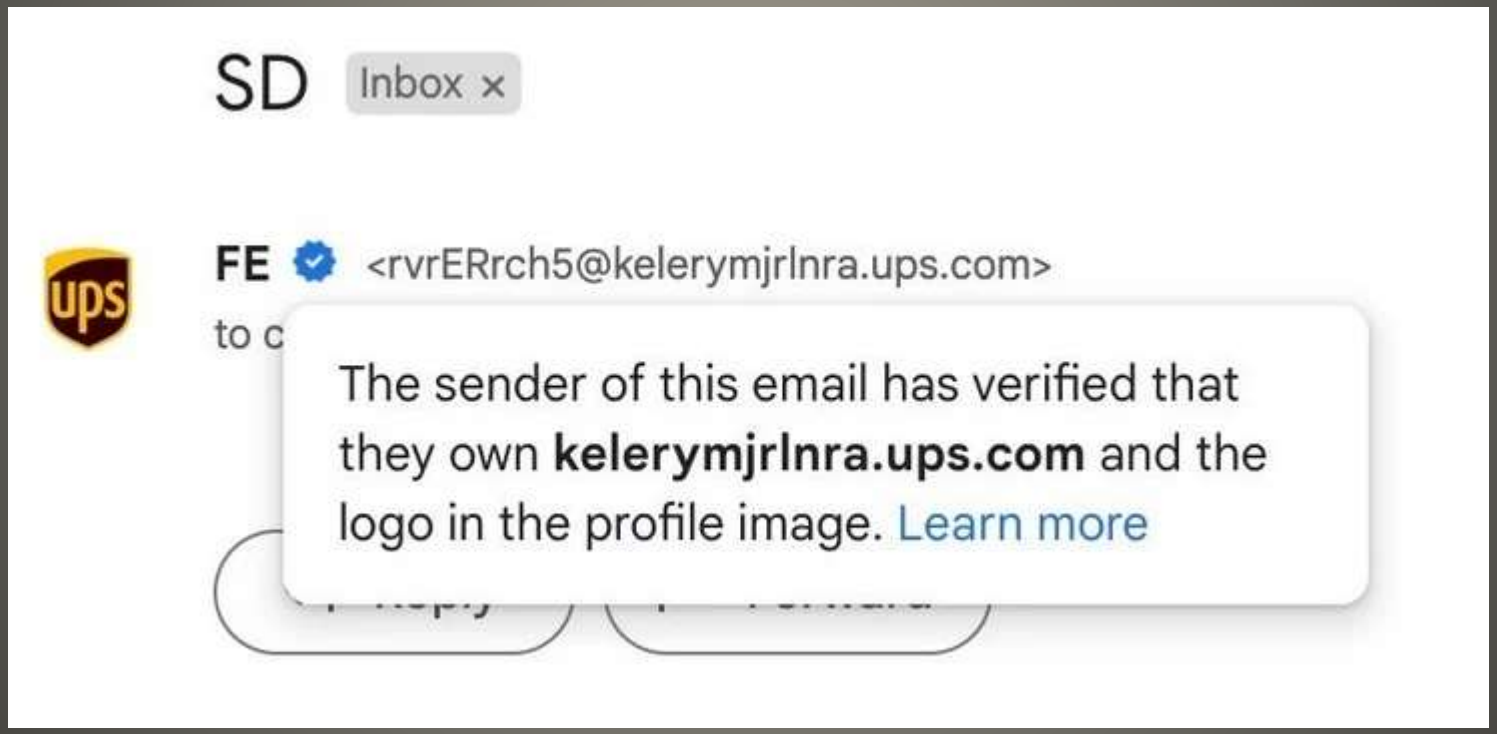
  Settings > Display & Brightness > Night Shift

  Schedule or manual
- Control Center

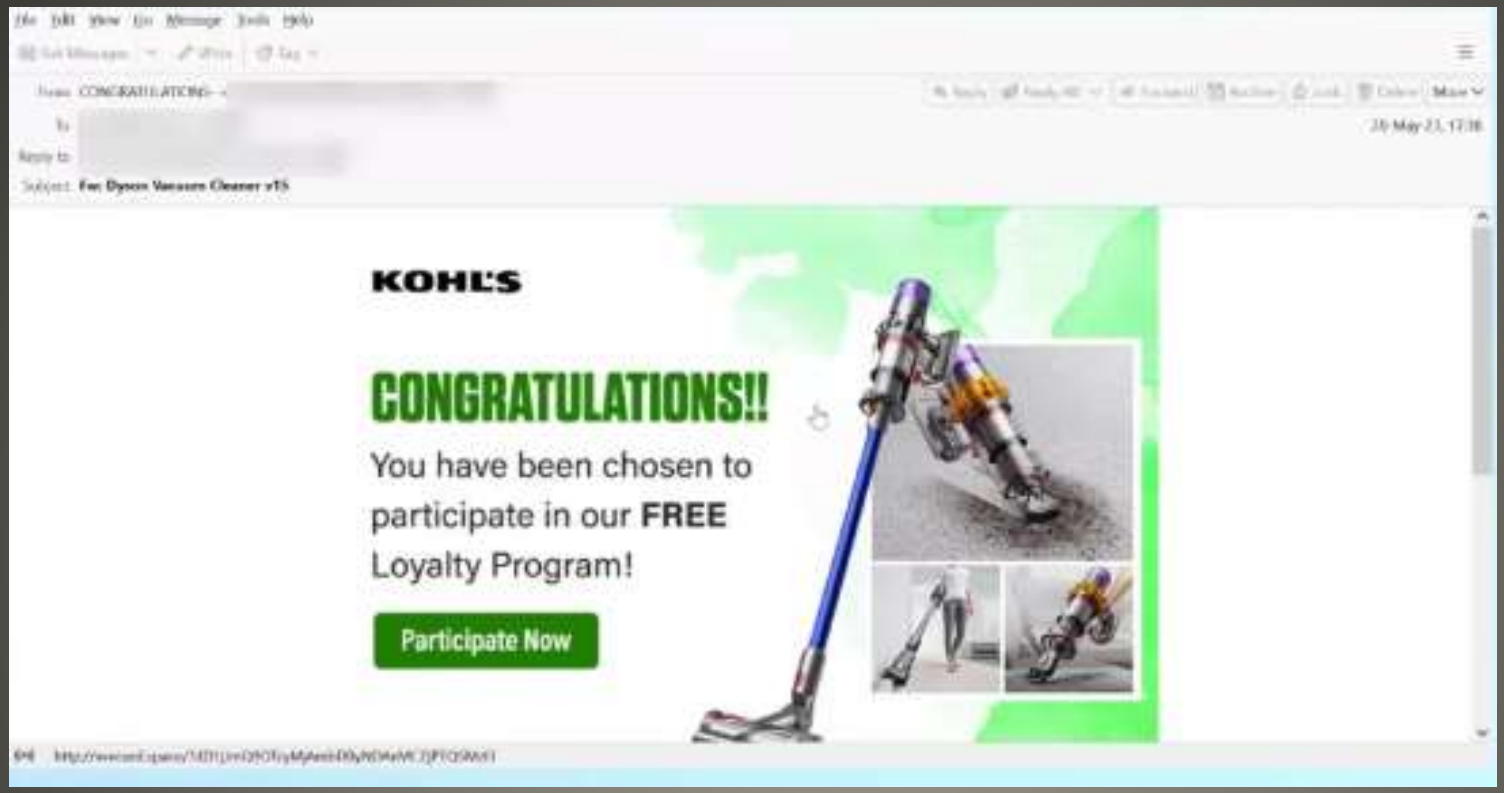
  Press and Hold Brightness icon

- Separate filter on display
- Special glasses

- Forbes article
- Blue check mark => safer
- Not an issue then a P1 problem



Gmail warning



- Messages - bad grammar
- Messages - phishing protections

Phishing Pictures

Current Issues

- Russia *Anti-Sanctions* PC
- MOVEit victims being extorted
- Cisco Secure Client vulnerability fixed
- Spear phishing
  - 0.1% but 66% success rate
  - hijacked contact list
  - social data collections
- Cuba to host Chinese spy facility
  - Many military and defense installations
  - Monitor US Navy
  - WSJ report

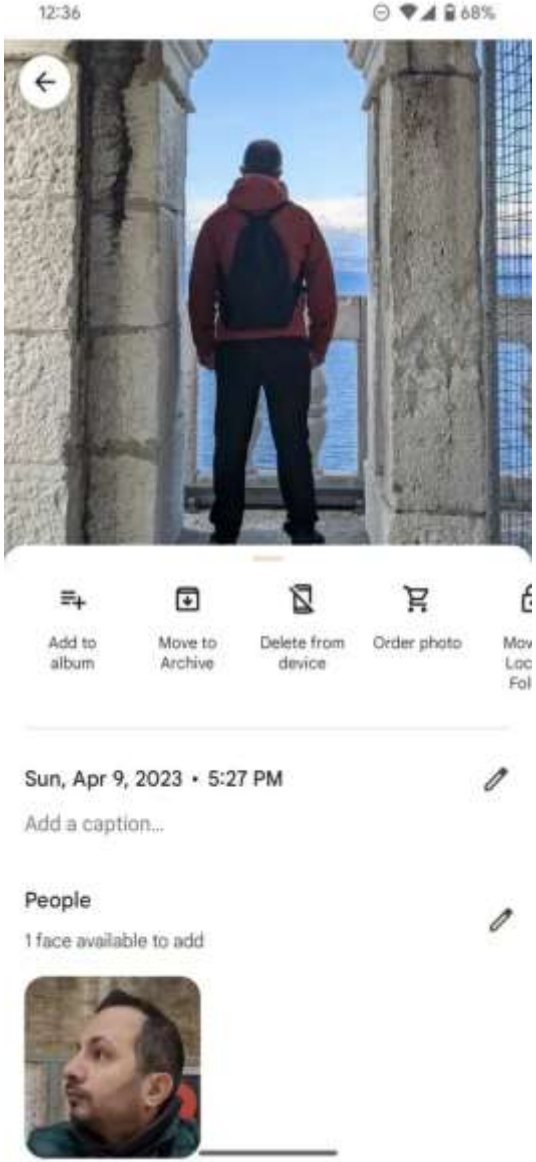
Current Issues

- IoT Sig
  - Email address for your house
  - Tailscale service
    - Access when not able to access
  - Document your home network
  - Look at your home network Wi-Fi
  - Other devices?
  - Correct channel or band?
- Anti-Fraud group NRO
  - Postal Annex
  - Town Hall Presentation

Current Issues

- Vivaldi spoofing Edge browser
  bypass Bing Chat restrictions
  browser fingerprinting
- ASUS multiple security releases firmware
- Apple Sherlock Our Tech
  voicemail, callerID, text messaging
  Alarm clocks
  Business cards

- Google Photos recognizing people from the back


12:36
68%
Add to album
Move to Archive
Delete from device
Order photo
Sun, Apr 9, 2023 • 5:27 PM
Add a caption...
People
1 face available to add


12:37
68%
Edit faces
Done
Available to add


12:37
68%
Add to album
Move to Archive
Delete from device
Order photo
Sat, Apr 22, 2023 • 2:38 PM
Add a caption...
People
1 face available to add

Reddit

- Reddit moderators lockout protest
- Protest charge for data access
- Hackers threaten to release 80GB of data

Phishing Clues

- Phishing emails often appear to come from legitimate companies, but the address you see masks the fake. Depending on the email program you use, you can hover your cursor over the address, or click on the header field of the email and ask for more info, and it will show you the real email address.

- Phishing emails often have subject lines that are urgent or that try to scare you into taking action. For example, the email might say that your account has been hacked or that your account will be blocked if you don't take action. Ignore, delete or report spam.
- Phishing emails often contain links or attachments that, if clicked on, will install malware on your computer. If you're not sure if a link or attachment is safe, you can hover your mouse over it to see the full URL. If the URL doesn't look like it's from the company the email claims to be from, don't click on it. Any attachment that has an .html extension is a link to an external site.
- Phishing emails often ask for personal information, like your password, credit card number, or PIN number. Never give out this information to someone you don't know and trust.
- The obvious message is, never click on a link that you do not trust 100%.

- Other general advice you will often come across, and should take, is:
- Keep your software and security applications up to date.
- Don't share your personal information, such as your password, credit card number, or ID number, with people you don't know and trust.
- Be suspicious of emails that ask for your personal information. If you're not sure, don't click on any links or open any attachments.

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com