Sun City Computer Club

Cyber Security SIG

August 4, 2022

Questions, Comments, Suggestions welcomed at any time

Even Now

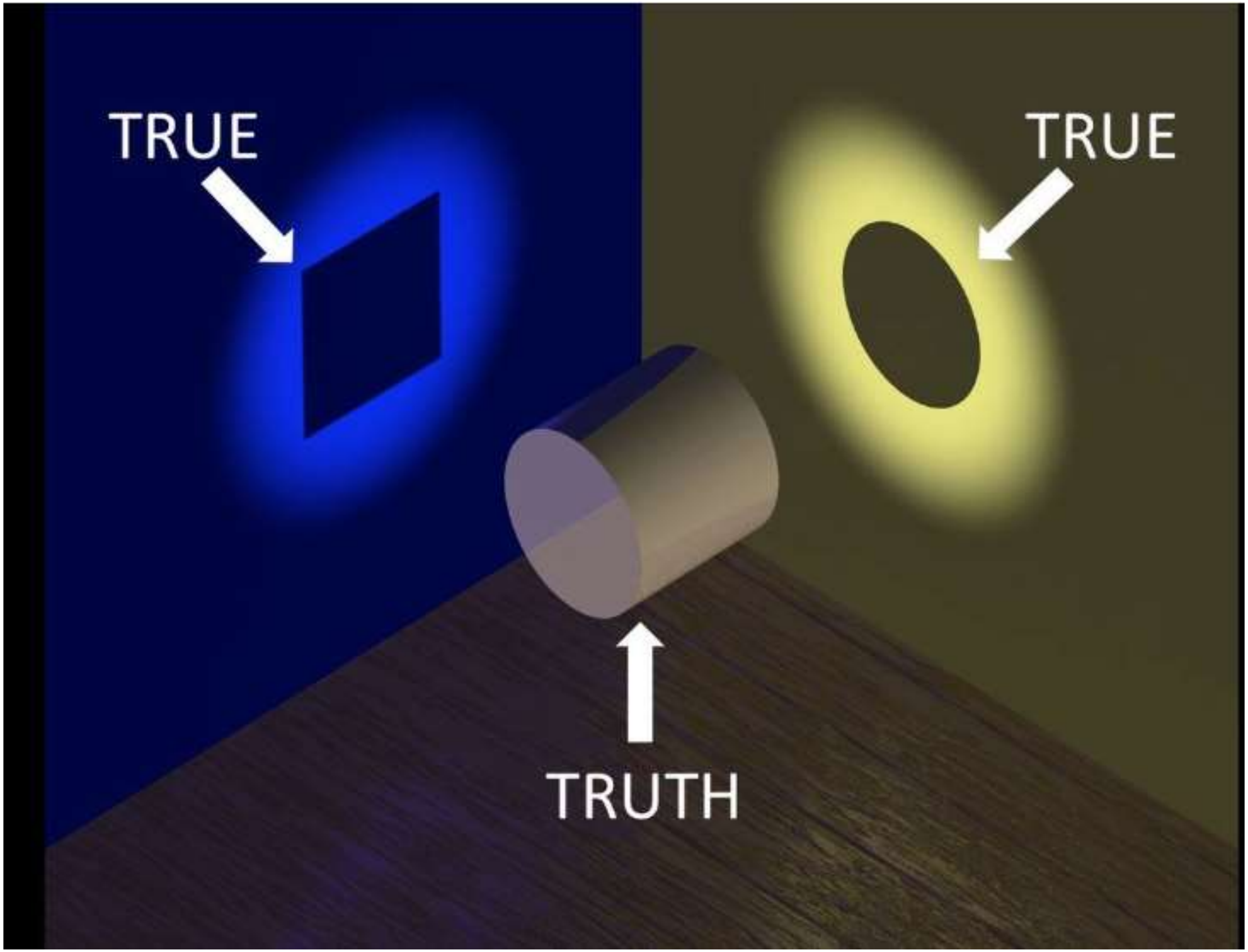
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

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???


TRUE
TRUE
TRUTH

- Kia and Hyundai vehicle thefts

  Using USB charger cable

  Kia 2011 – 2021

  Hyundai 2015 – 2021

  Cyber Security SIG News Archive
- Amazon drive loses support December 2023
- Google Pixel 6a any fingerprint to unlock

  June security patch?
- US Court system Breach

  US House Judiciary hearing 2020
- OMB requirements to protect Federal Data Center
- Equifax incorrect scores “coding error”

Current Issues

BEC

- Business Email Compromise (BEC)
  Number 1 more than ransomware!
  Not usually reported as cyber crime
  Social engineering
  CFO reports – funny frantic frightening
  spoofed account
  account take over
  easy information to gather
  Shame & embarrassment
  Clients, customers, business partners

BEC

- Easy to carry out
- Difficult to stop or detect or reverse
- Multi Factor authentication
- Multi Party authorization
- Guess who pays?

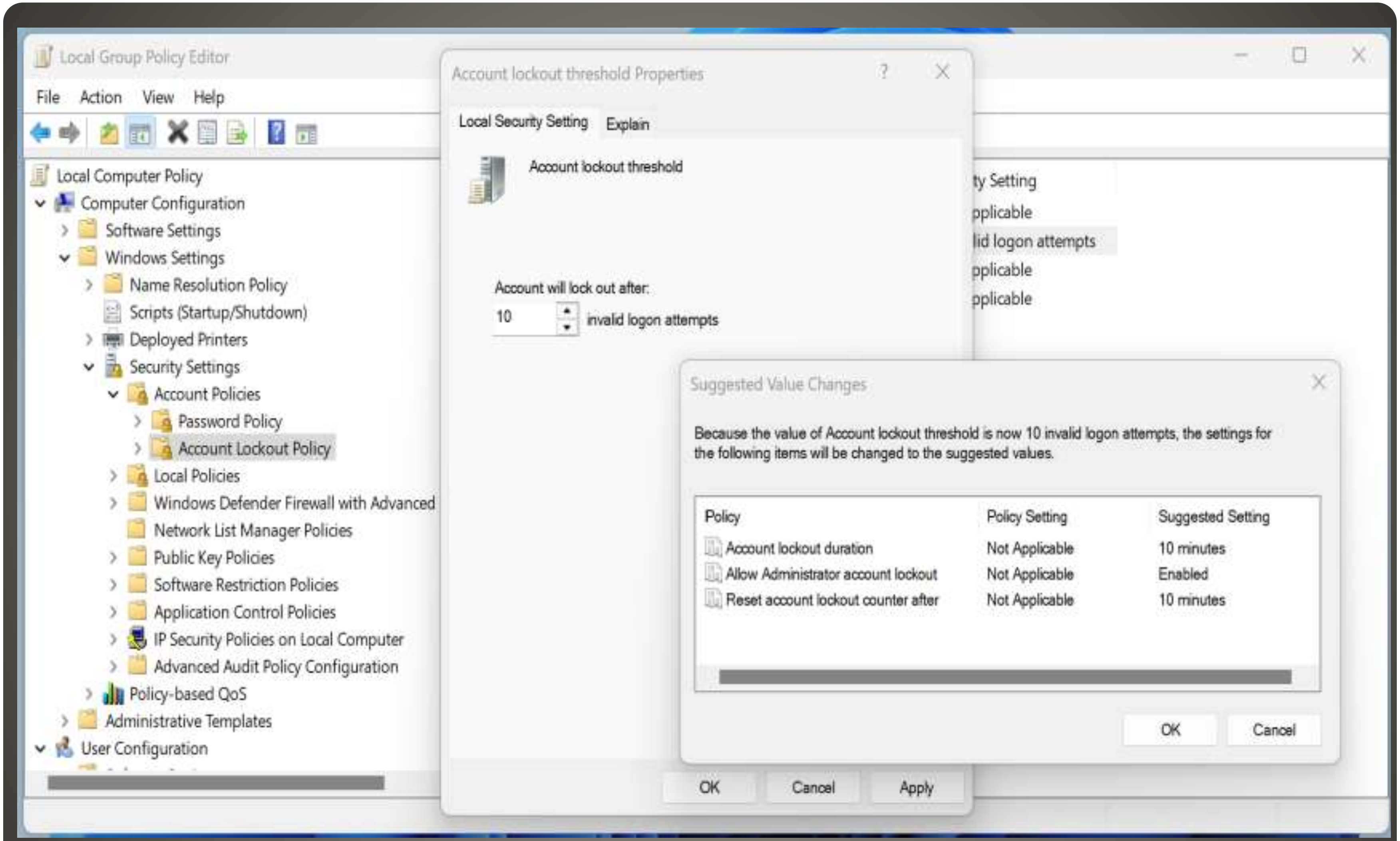
- Open House Intelligence Committee hearing
- NSO Group Pegasus
- Only sold for fighting terrorism and crime
- BUT

  Reports of unnamed country on US ambassador teenaged son of CNN journalist
- US company L3Harris to purchase NSO
- FBI purchased but never used
- Legislation State Dept to compile list of spyware

Congress battles foreign spyware

Current Issues

- Port of Los Angeles calls FBI
  Number of foreign attacks double
  Cyber Resilience Center
- T-Mobile $350M massive data breach(es)
- Phishing attack
  HTML > password protected zip
  2 DLLs and calc.exe
- Apple traffic touted through Russia
  12 hours July 26-27
  BGP hijacking
  AS714 APPLE-ENGINEERING, US
- SHARPEXT Gmail read as user reads



Account lockout threshold

Account will lock out after:

10 invalid logon attempts

Because the value of Account lockout threshold is now 10 invalid logon attempts, the settings for the following items will be changed to the suggested values.

Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Applicable	10 minutes
Allow Administrator account lockout	Not Applicable	Enabled
Reset account lockout counter after	Not Applicable	10 minutes

RDP Account Lockout

- “We’re resuming the rollout of this change in Current Channel. Based on our review of customer feedback, we’ve made updates to both our end user and our IT admin documentation to make clearer what options you have for different scenarios.”

Microsoft disable remotely received VBA Macros

August

- August 6-11 Black Hat
- August 11-14 DefCon

DefCon

No online registration

No credit card payments Cash

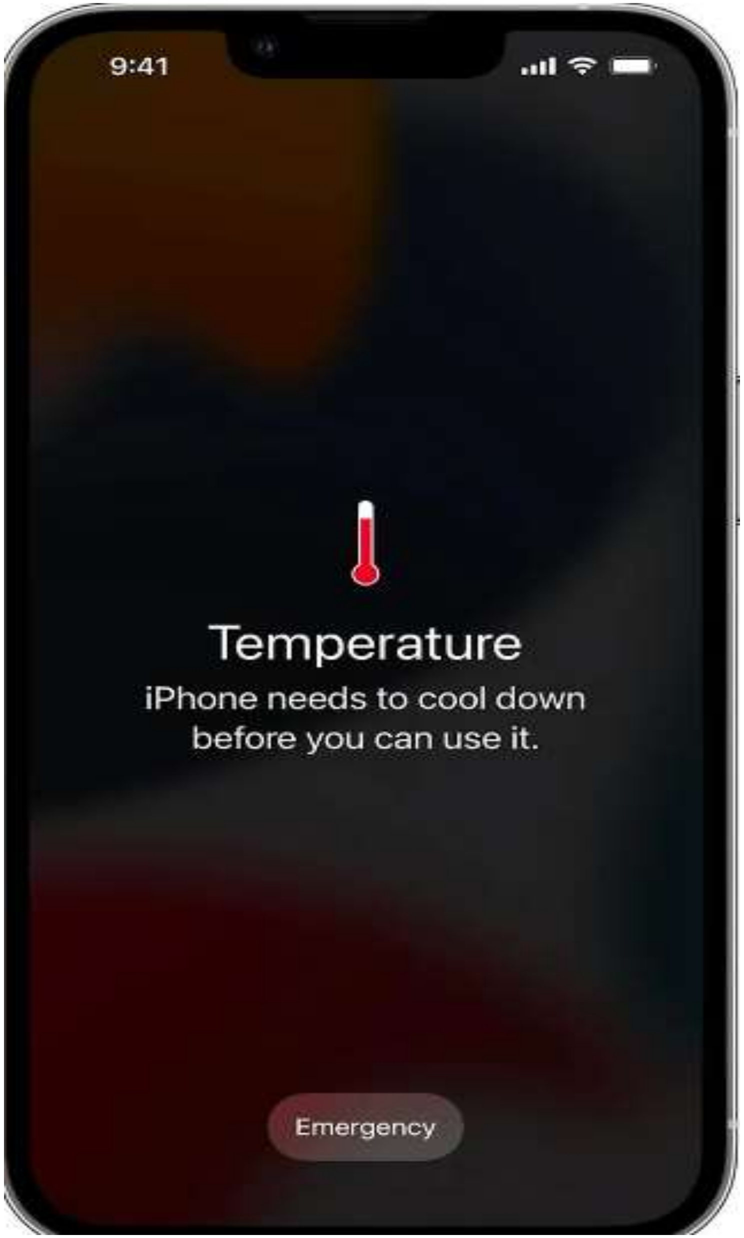
No ID required Generic badge

Easy to Hide
MV720, looks like a relay, but is actually a locator.

MV720

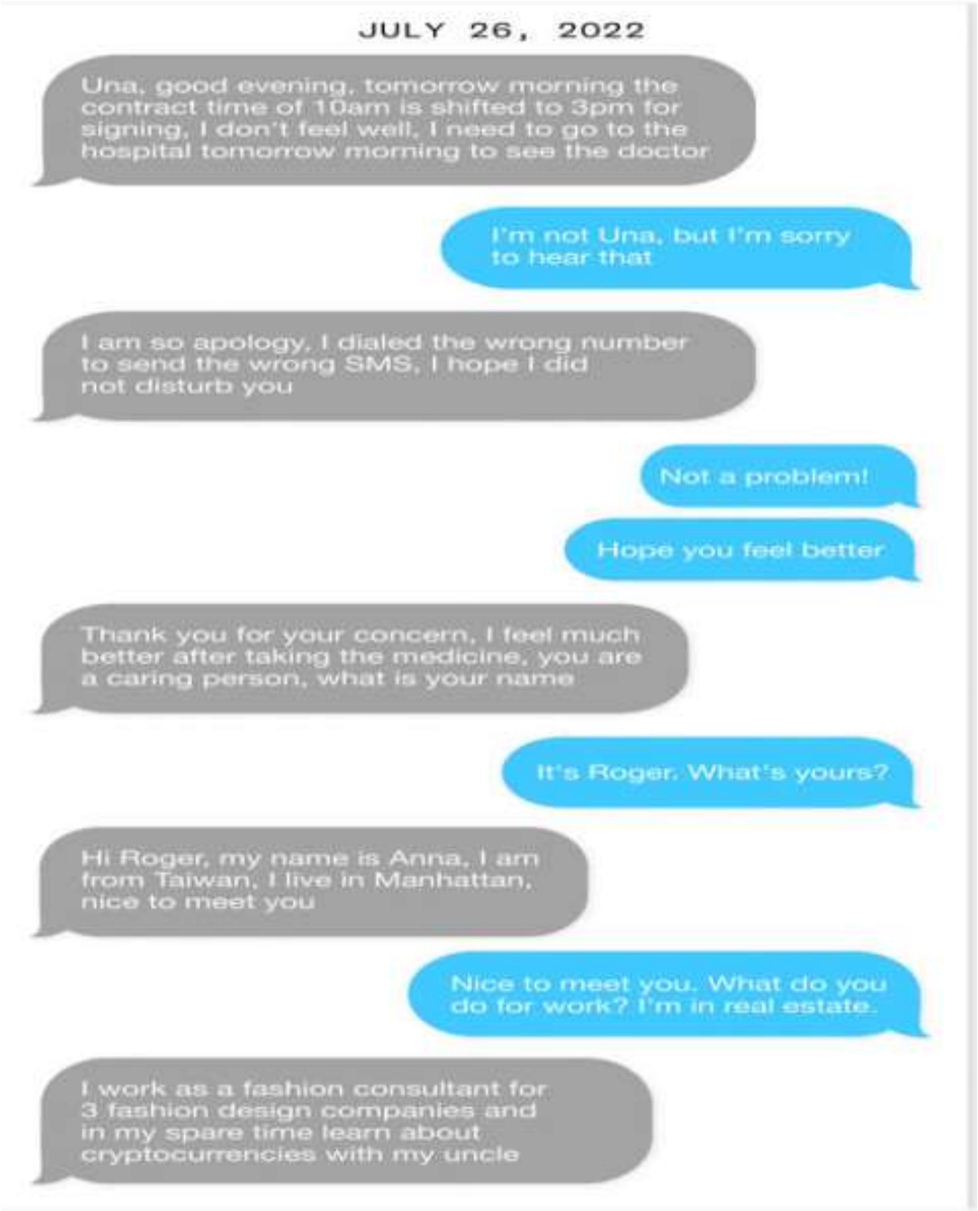
- $20
- Monitor and track location & speed
- Remotely shutdown flow of fuel
- Micodus China based manufacturer
- Cellular-enabled GPS tracker
- Transmit data to supporting servers
- RECEIVE commands via SMS
- RECEIVE commands via SMS anyone
- Geofencing
- 1.5 million devices   so far   169 countries
- Single server unencrypted protocol single port
- 555 fuel off   666 fuel on

- “Go to beach house and crash”
- Do No Harm   -   delete No



Temperature

iPhone needs to cool down before you can use it.



JULY 26, 2022

Una, good evening, tomorrow morning the contract time of 10am is shifted to 3pm for signing, I don't feel well, I need to go to the hospital tomorrow morning to see the doctor

I'm not Una, but I'm sorry to hear that

I am so apology, I dialed the wrong number to send the wrong SMS, I hope I did not disturb you

Not a problem!

Hope you feel better

Thank you for your concern, I feel much better after taking the medicine, you are a caring person, what is your name

It's Roger. What's yours?

Hi Roger, my name is Anna, I am from Taiwan, I live in Manhattan, nice to meet you

Nice to meet you. What do you do for work? I'm in real estate.

I work as a fashion consultant for 3 fashion design companies and in my spare time learn about cryptocurrencies with my uncle

- 28 Apps

  wallpaper apps, keyboards, photo editors, video editors, cache cleaners, varies system maintenance apps

  "System App" to discourage removal

  Push Ads, enroll premium services

  Unnecessary permissions

  Removed from Play Store

  NOT removed from your device

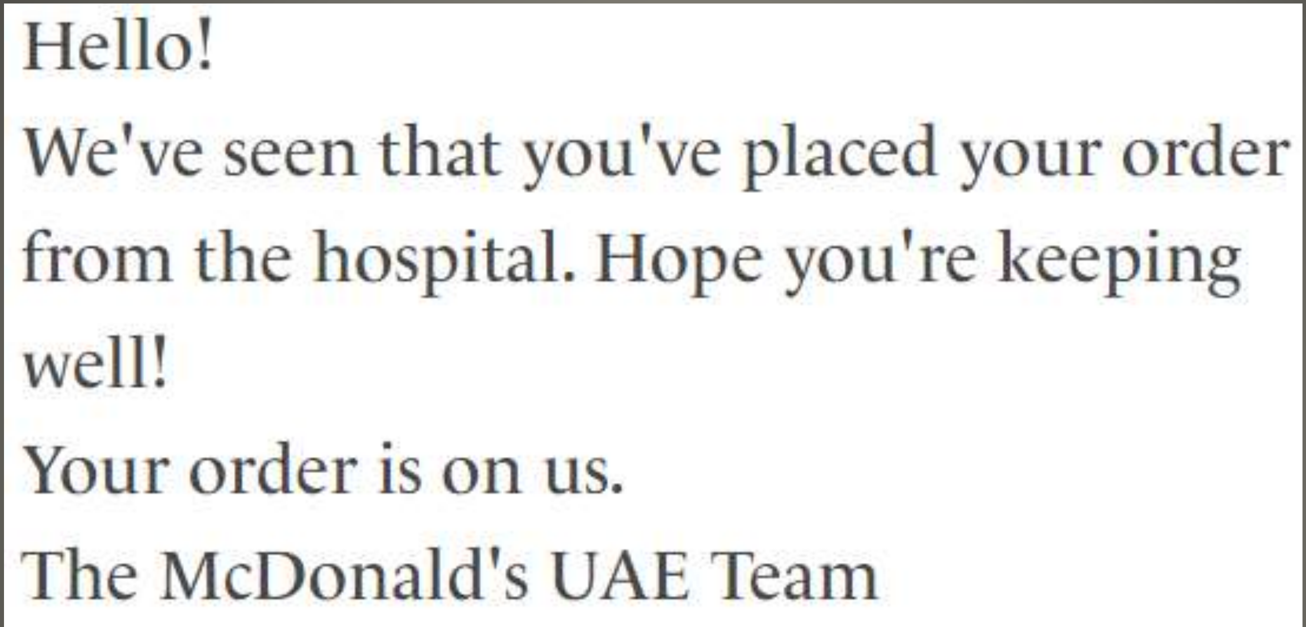
Android wallet draining malware

- Photo Editor: Beauty Filter (gb.artfilter.tenvarnist)
- Photo Editor: Retouch & Cutout (de.nineergysh.quickarttwo)
- Photo Editor: Art Filters (gb.painnt.moonlightingnine)
- Photo Editor - Design Maker (gb.twentynine.redaktoridea)
- Photo Editor & Background Eraser (de.photoground.twentysixshot)
- Photo & Exif Editor (de.xnano.photoexifeditornine)
- Photo Editor - Filters Effects (de.hitopgop.sixtyeightgx)
- Photo Filters & Effects (de.sixtyonecollice.cameraroll)
- Photo Editor : Blur Image (de.instgang.fiftyggfife)
- Photo Editor : Cut, Paste (de.fiftyninecamera.rollredactor)
- Emoji Keyboard: Stickers & GIF (gb.crazykey.sevenboard)
- Neon Theme Keyboard (com.neonthemekeyboard.app)
- Neon Theme - Android Keyboard (com.androidneonkeyboard.app)
- Cashe Cleaner (com.cachecleanereasytool.app)
- Fancy Charging (com.fancyanimatedbattery.app)
- FastCleaner: Cashe Cleaner (com.fastcleanercashecleaner.app)
- Call Skins - Caller Themes (com.rockskinthemes.app)
- Funny Caller (com.funnycallercustomtheme.app)
- CallMe Phone Themes (com.callercallwallpaper.app)
- InCall: Contact Background (com.mycallcustomcallscrean.app)
- MyCall - Call Personalization (com.mycallcallpersonalization.app)
- Caller Theme (com.caller.theme.slow)
- Caller Theme (com.callertheme.firstref)
- Funny Wallpapers - Live Screen (com.funnywallpapaerslive.app)
- 4K Wallpapers Auto Changer (de.andromo.ssfiftylivesixcc)
- NewScrean: 4D Wallpapers (com.newscrean4dwallpapers.app)
- Stock Wallpapers & Backgrounds (de.stockeighty.onewallpapers)
- Notes - reminders and lists (com.notesreminderslists.app)

The list As of July 29

- Portland General Electric
- Volunteer program 100,000 subscribers
- Dozens of other utilities
- Credit on electric bill

Smart Smart Thermostats



Hello!

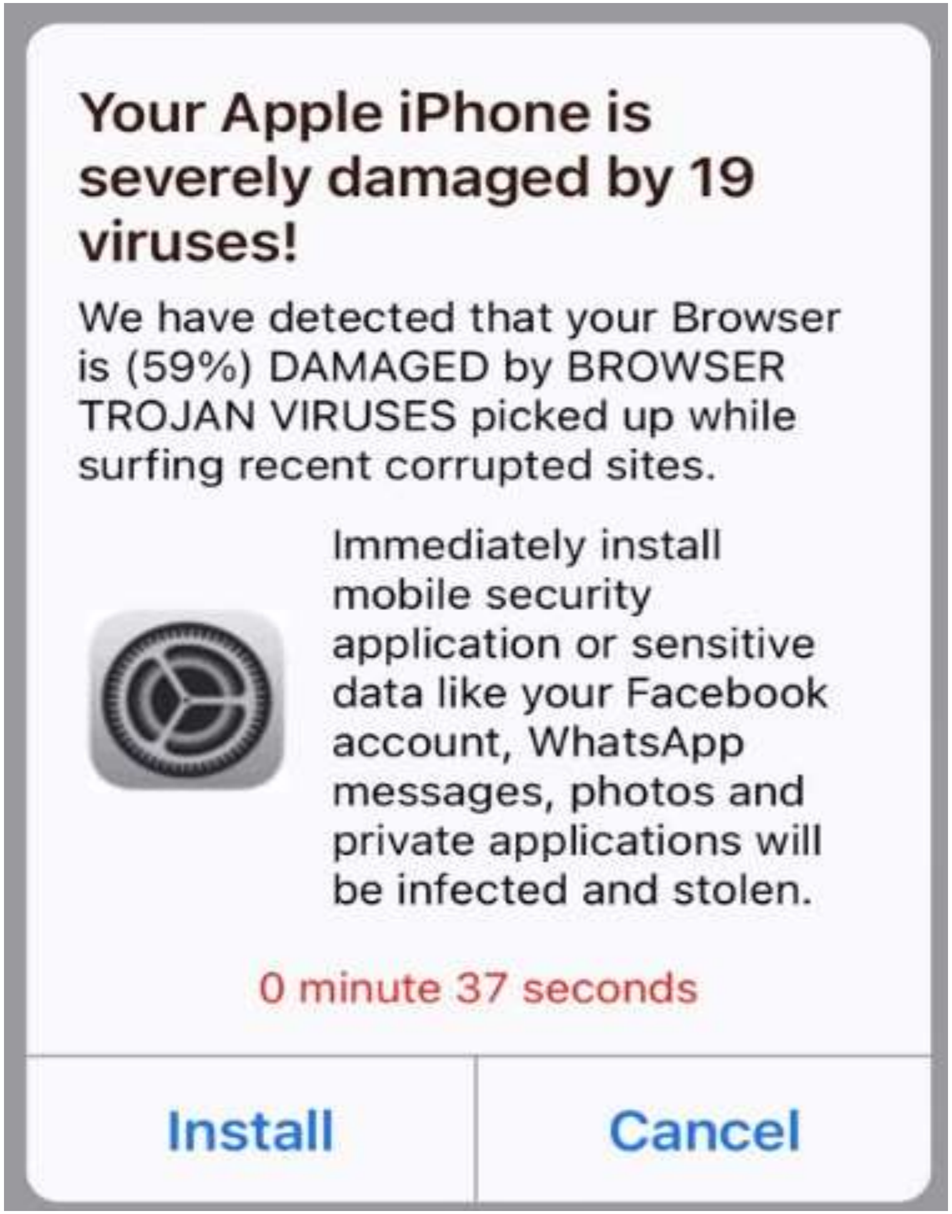
We've seen that you've placed your order from the hospital. Hope you're keeping well!

Your order is on us.

The McDonald's UAE Team

- “we’ve seen”
- Transparency
- Customer data to benefit the customer *and McDonalds*
- Used data immediately - not at next refresh
- Individual – not audience

McDonalds



Your Apple iPhone is severely damaged by 19 viruses!

We have detected that your Browser is (59%) DAMAGED by BROWSER TROJAN VIRUSES picked up while surfing recent corrupted sites.

Immediately install mobile security application or sensitive data like your Facebook account, WhatsApp messages, photos and private applications will be infected and stolen.

0 minute 37 seconds

QR Codes

- 2-dimensional barcode
- 4K characters
- Static or Dynamic
- Rapid method:

  Contact details

  Virtual business card VCD

  Add to contact lists

  Phone

  Caller-ID

  Toll calls

SMS
 send to anyone else
Text
eMail
GPS location
URL
Calendar event
Social media follow or …
Wi-Fi credentials
Store purchase / subscriptions

QR Codes

- Dynamic

  Change at anytime

  Perform tasks

For more information:

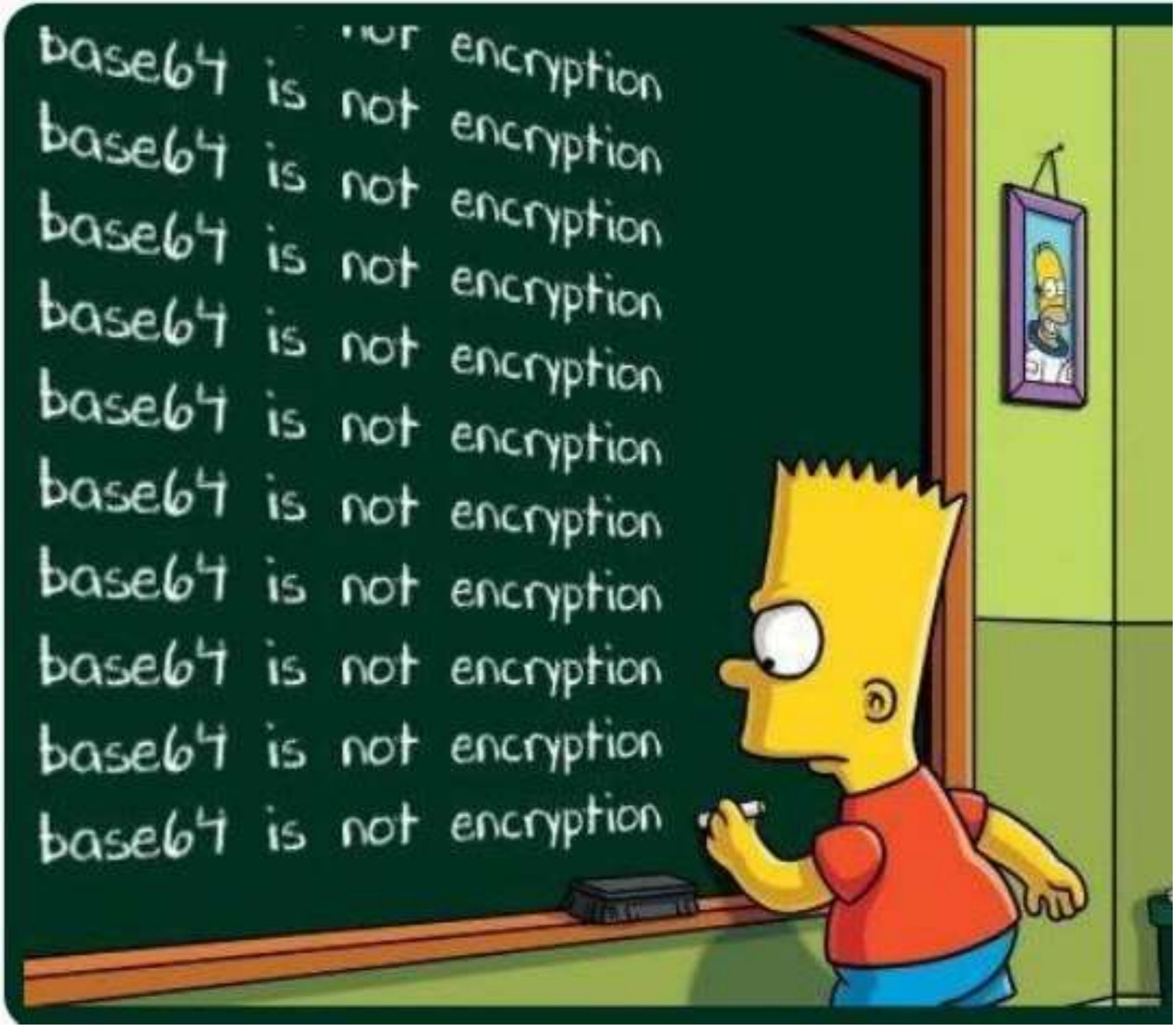
https://www.forbes.com/sites/forbestechcouncil/2020/06/01/i-dont-scan-qr-codes-and-neither-should-you/?sh=7a98e6dc51d1

- Austin parking meters
- Super Bowl Ad

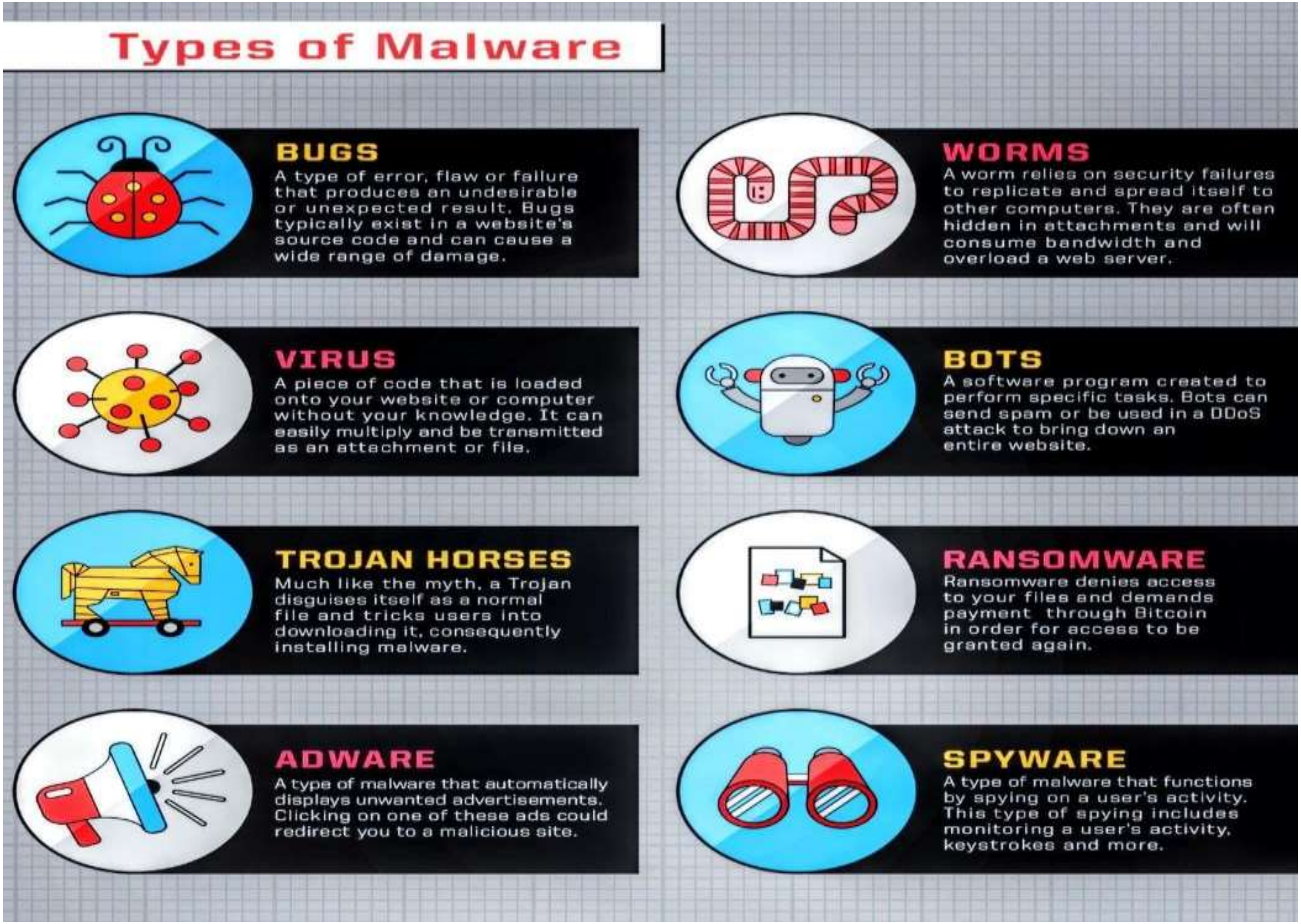
QR Codes

QR Codes

- When in doubt, don’t
- Pasted over
- Shortened code
- Use secure browser to follow URL
- Security Suite’s QR scanner
- Check QR scanner logs



base64 is not encryption
base64 is not encryption
base64 is not encryption
base64 is not encryption
base64 is not encryption
base64 is not encryption
base64 is not encryption
base64 is not encryption
base64 is not encryption
base64 is not encryption
base64 is not encryption



Types of Malware

BUGS

A type of error, flaw or failure that produces an undesirable or unexpected result. Bugs typically exist in a website's source code and can cause a wide range of damage.

WORMS

A worm relies on security failures to replicate and spread itself to other computers. They are often hidden in attachments and will consume bandwidth and overload a web server.

VIRUS

A piece of code that is loaded onto your website or computer without your knowledge. It can easily multiply and be transmitted as an attachment or file.

BOTS

A software program created to perform specific tasks. Bots can send spam or be used in a DDoS attack to bring down an entire website.

TROJAN HORSES

Much like the myth, a Trojan disguises itself as a normal file and tricks users into downloading it, consequently installing malware.

RANSOMWARE

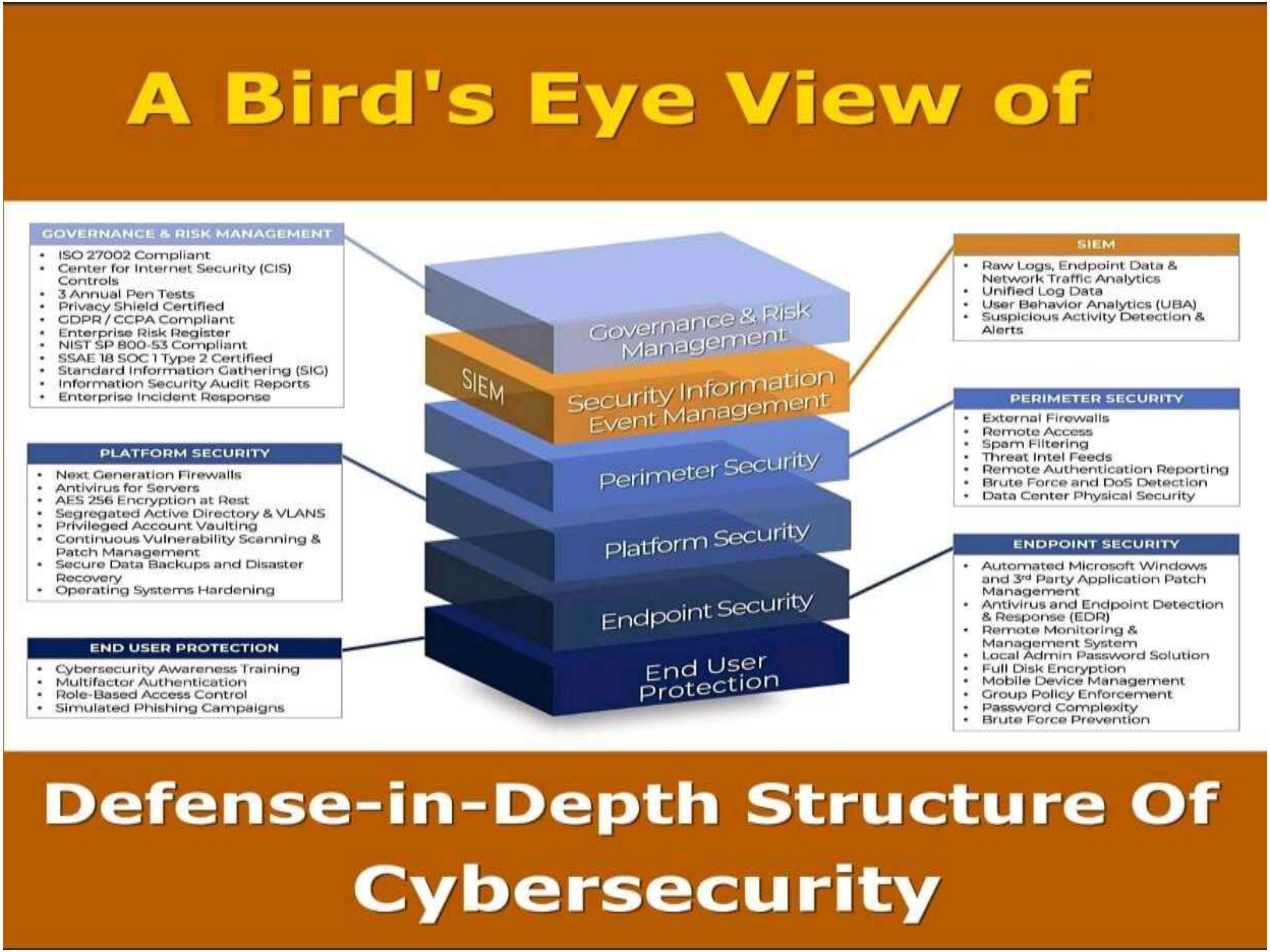
Ransomware denies access to your files and demands payment through Bitcoin in order for access to be granted again.

ADWARE

A type of malware that automatically displays unwanted advertisements. Clicking on one of these ads could redirect you to a malicious site.

SPYWARE

A type of malware that functions by spying on a user's activity. This type of spying includes monitoring a user's activity, keystrokes and more.



A Bird's Eye View of

GOVERNANCE & RISK MANAGEMENT

- ISO 27002 Compliant
- Center for Internet Security (CIS) Controls
- 3 Annual Pen Tests
- Privacy Shield Certified
- GDPR / CCPA Compliant
- Enterprise Risk Register
- NIST SP 800-53 Compliant
- SSAE 18 SOC 1 Type 2 Certified
- Standard Information Gathering (SIG)
- Information Security Audit Reports
- Enterprise Incident Response

PLATFORM SECURITY

- Next Generation Firewalls
- Antivirus for Servers
- AES 256 Encryption at Rest
- Segregated Active Directory & VLANS
- Privileged Account Vaulting
- Continuous Vulnerability Scanning & Patch Management
- Secure Data Backups and Disaster Recovery
- Operating Systems Hardening

END USER PROTECTION

- Cybersecurity Awareness Training
- Multifactor Authentication
- Role-Based Access Control
- Simulated Phishing Campaigns

SIEM

- Raw Logs, Endpoint Data & Network Traffic Analytics
- Unified Log Data
- User Behavior Analytics (UBA)
- Suspicious Activity Detection & Alerts

PERIMETER SECURITY

- External Firewalls
- Remote Access
- Spam Filtering
- Threat Intel Feeds
- Remote Authentication Reporting
- Brute Force and DoS Detection
- Data Center Physical Security

ENDPOINT SECURITY

- Automated Microsoft Windows and 3rd Party Application Patch Management
- Antivirus and Endpoint Detection & Response (EDR)
- Remote Monitoring & Management System
- Local Admin Password Solution
- Full Disk Encryption
- Mobile Device Management
- Group Policy Enforcement
- Password Complexity
- Brute Force Prevention

Defense-in-Depth Structure Of Cybersecurity

- 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