Sun City Computer Club

Cyber Security SIG

November 17, 2022

Questions, Comments, Suggestions welcomed at any time

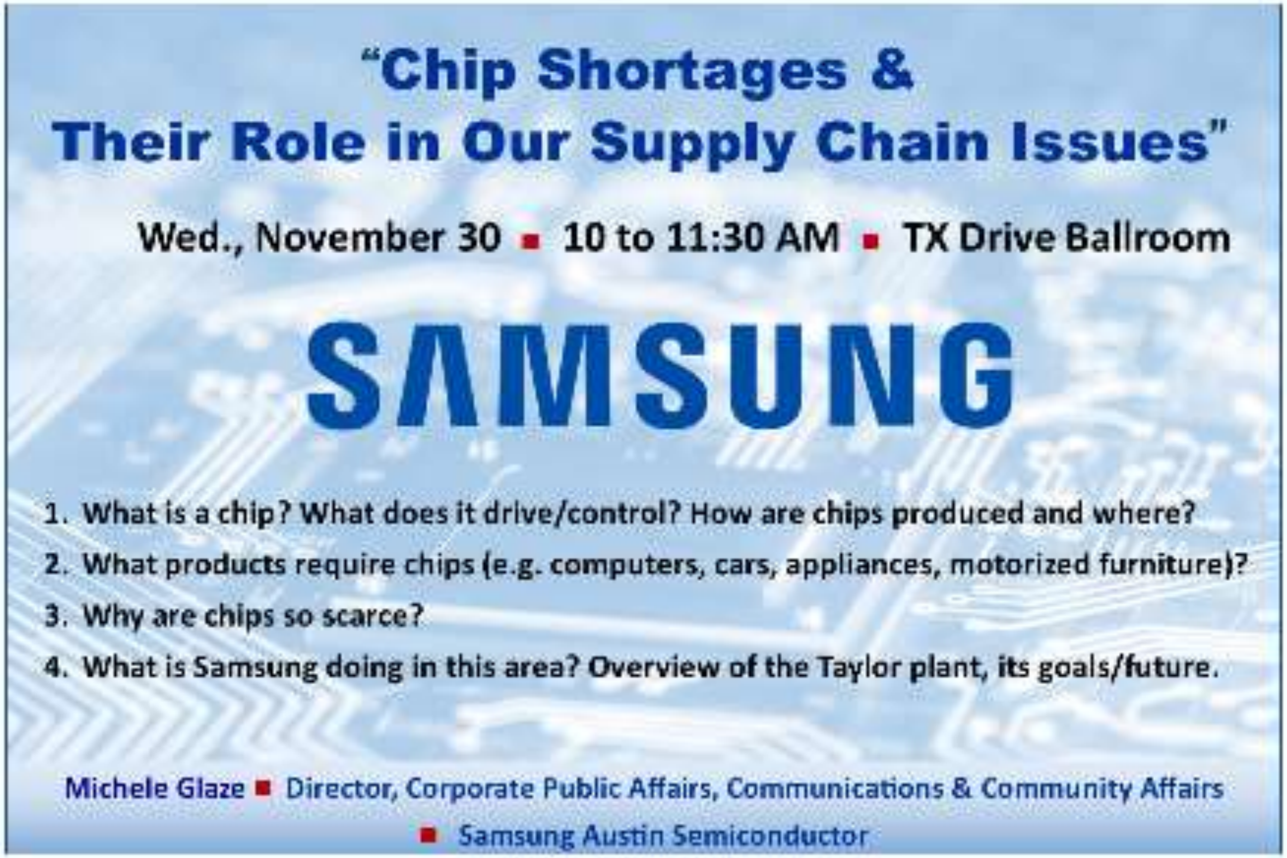
Even Now

- 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

CHIP SHORTAGES AND THEIR ROLE IN OUR SUPPLY CHAIN ISSUES



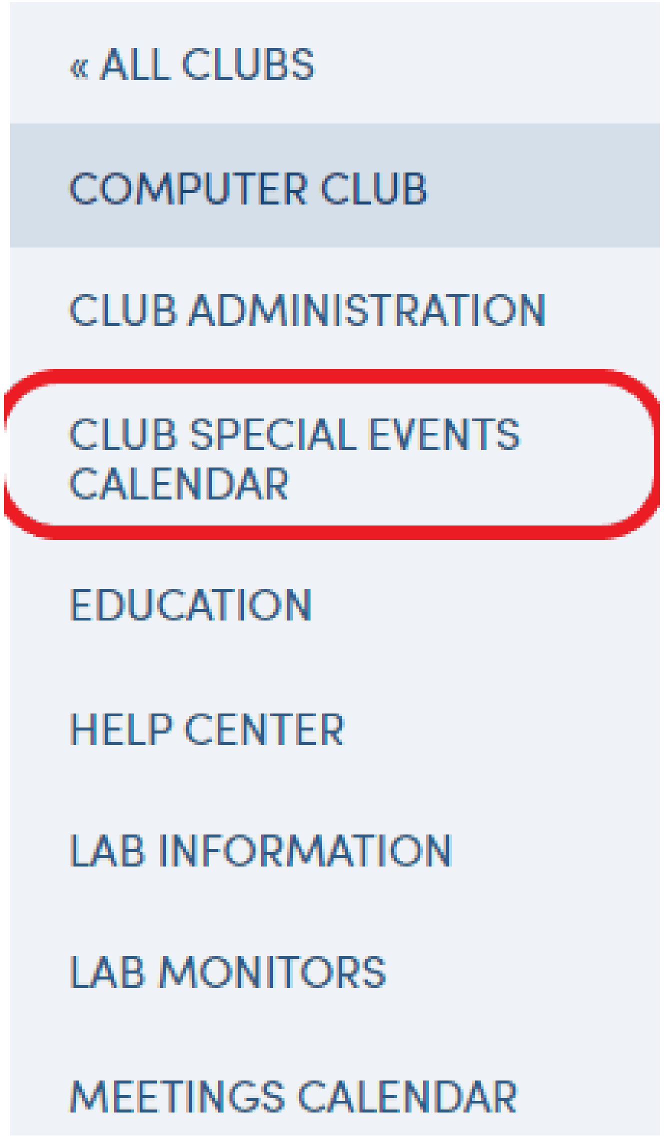
"Chip Shortages & Their Role in Our Supply Chain Issues"

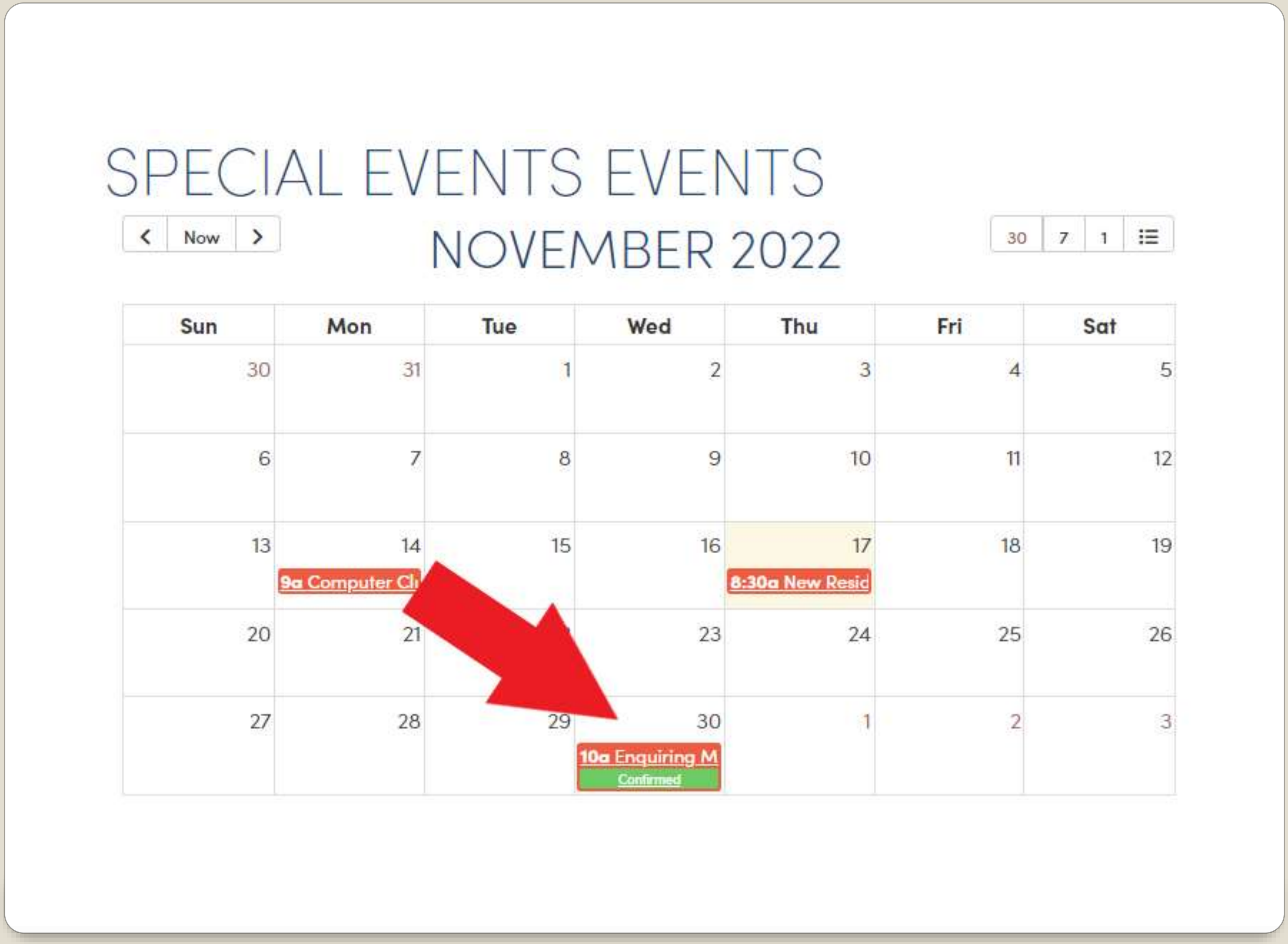
Wed., November 30 ▪ 10 to 11:30 AM ▪ TX Drive Ballroom

SAMSUNG

1. What is a chip? What does it drive/control? How are chips produced and where?
2. What products require chips (e.g. computers, cars, appliances, motorized furniture)?
3. Why are chips so scarce?
4. What is Samsung doing in this area? Overview of the Taylor plant, its goals/future.

Michele Glaze ▪ Director, Corporate Public Affairs, Communications & Community Affairs ▪ Samsung Austin Semiconductor


« ALL CLUBS
COMPUTER CLUB
CLUB ADMINISTRATION
CLUB SPECIAL EVENTS CALENDAR
EDUCATION
HELP CENTER
LAB INFORMATION
LAB MONITORS
MEETINGS CALENDAR



SPECIAL EVENTS EVENTS

NOVEMBER 2022

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14 9a Computer Cl	15	16	17 8:30a New Resid	18	19
20	21	22	23	24	25	26
27	28	29	30 10a Enquiring M Confirmed	1	2	3

SIG News

- In Person meetings
- Last Member Survey 15% desired
- Help Center 2023 12:00 – 3:00
- SIG 3:30 – 4:30 if In Person
- Topic Suggestions
- https://vimeo.com/user96981772

  172

  NO Login nor Join necessary

  Search 🔍

Presenter???

- Ever want to be a presenter??

- FTX implosion

  Filed for bankruptcy

  FTX based in Bahamas
- Digital Dollar 12-week trial

Cyber Finance

- Official Cop27 App

  Climate talks in Egypt

  App captures and sends:

  Photos, locations, emails & messages

  Loading requires: Name, email, mobile number, nationality, passport number
- Egypt surveilled nation state
- UK vulnerability

  scanningscanner.scanning.service.ncsc.gov.uk

  18.171.7.246   33.177.10.231

  Don’t scan me

  Help fix me
- KeePassXC memory strings
- wifite Wi-Fi attack tool

Current Issues

- Dropbox & pHishing attack surface

No one does anything alone any more

SolarWinds Managed Services Providers

- OpenSSL vulnerability patched
- FTC sues Chegg

Chegg educational products

Rent textbooks, scholarship search, tutoring,

40 million customers

High school & college & life learners

religion, heritage, dob, sexual orientation, disabilities, house income, …

stored in plain text No MFA,

SEVERE incidents

Current Issues

Current Issues

- Basic Security Training

  It only takes one

  It only takes one
- Awareness
- Life, Liberty, Pursuit of happiness

- Inflation

Reported ransomware payments 2021

Financial institutions

FinCEN Bank Secrecy Act

$1.2 Billion

Current Issue

- Phishing toolkits > Phishing > Breaches
- Information given

  cumulative

  NO indication of being stolen

  Initial Access Brokers IAB

Victim of a victim

Bad actors are suffering from inflation too

3rd quarter report

570 network access listings

$1500 per

- North Korea Nuclear & missile programs
  US & Europe
  Asia & Latin America
  Africa

Map, Coordinate, coordinated attack
Money mules

Banking Cyber Heist

- Russia -> Linux
- China -> Develop own
  Geopolitical implications
  0-day reporting

Accurate? If so, how so?

Red Cross
Attacks any/everyone

- IAB access CPA & Tax accountants
  Create CPA & Tax accountant firms
  File fake tax returns

Current Issues

Twitter

- Blue Check
  Blue Check charge
  No Blue check charge

  Subscribers leaving
  Mastodon alternative
  230,000 new subscribers last week

- Unlock Android phone WITHOUT password
- Locked Android phone/tablet
- Passcode, Face Scan, or Fingerprint
- Google Pixel 5 & 6
- Passcode required after reboot
- *Except*
- Insert attacker's SIM
- Wrong PIN 3 times
- Enter attacker's SIM PUK
- (Personal Unlock Code)
- APPLY November 2022 Android Update

Android unlock

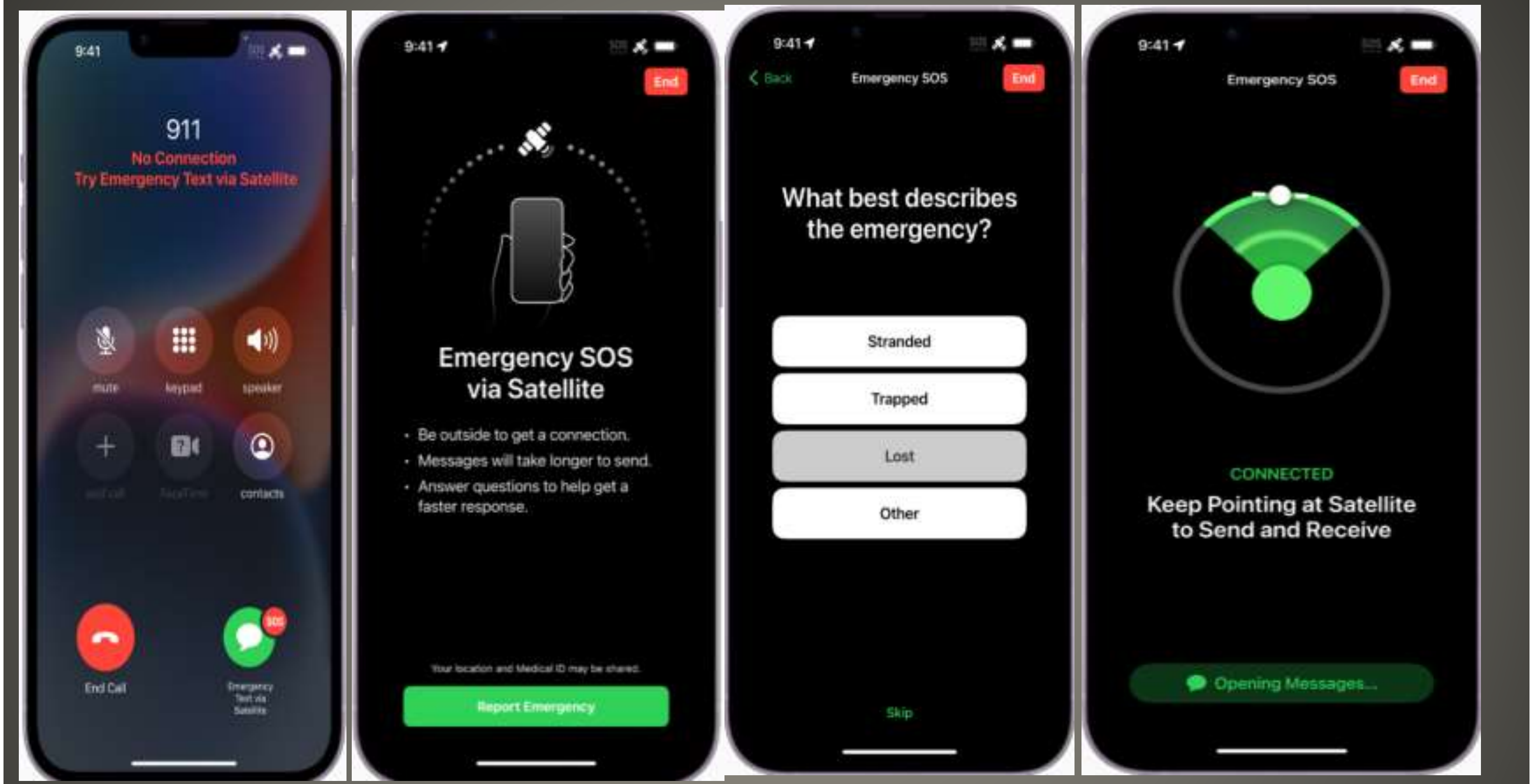
- Over-permissioned apps are a threat. The Ehteraz app asks users to allow remote access to pictures and videos, make unprompted calls, and read or modify device data while the Hayya app asks for full network access and unrestricted access to personal data. It also prevents the device from going into sleep mode and views the phone’s network connections. Both need location data to operate, which is expected. This is an excellent time to take a loaner/burner device which has _MINIMAL_ data. Also at the event are 15,000 surveillance cameras with facial recognition capabilities, ostensibly to keep people safe.
- NOT Just Qatar

Qatar & World Cup

- Zimbra Collaboration Suite
  CISA & MS-ISAC
  US Cybersecurity and Infrastructure Security Agency
  Multi-State Information Sharing and Analysis Center
- Microsoft Windows Kerberos authentication issues
- K-12 Cybersecurity concerns
- First there was Pushwoosh, then there was not
- Apple Emergency SOS-via-satellite service
  Launch 11/15/2022
  iPhone 14
  Questionnaire plus
  Location (and altitude), iPhone battery charge, MedicalID
  Globalstar

Current Issues

"Your Fitness Tracker just texted me. You haven't been exercising or eating right like you claim. It's not a traitor, it's your friend."



9:41

911

No Connection

Try Emergency Text via Satellite

9:41

Emergency SOS via Satellite

- Be outside to get a connection.
- Messages will take longer to send.
- Answer questions to help get a faster response.

Your location and Medical ID may be shared.

9:41

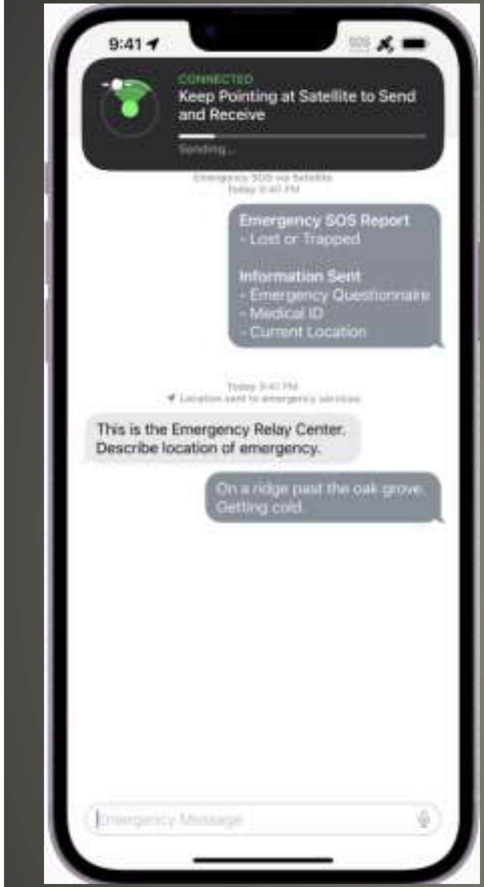
What best describes the emergency?

9:41

CONNECTED

Keep Pointing at Satellite to Send and Receive

Apple Emergency SOS-via-satellite service



9:41

CONNECTED

Keep Pointing at Satellite to Send and Receive

Sending...

Emergency SOS via Satellite
Today 9:40 PM

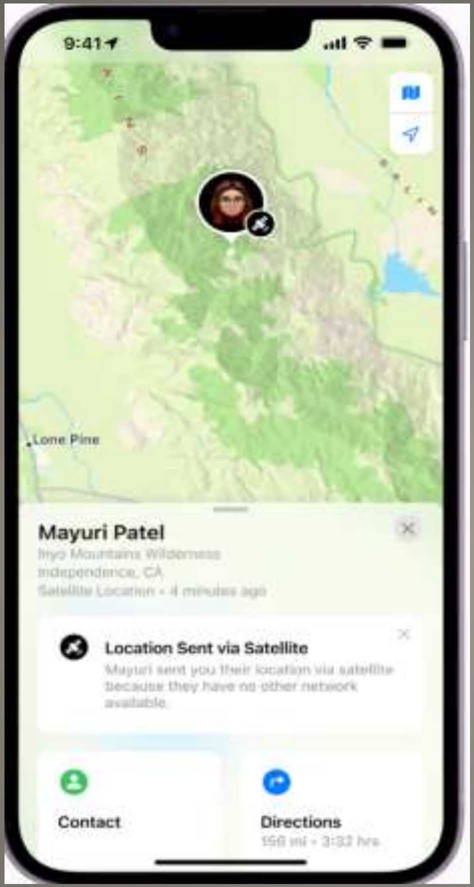
Emergency SOS Report
- Lost or Trapped

Information Sent
- Emergency Questionnaire
- Medical ID
- Current Location

Today 9:41 PM
Location sent to emergency services

This is the Emergency Relay Center. Describe location of emergency.

On a ridge past the oak grove. Getting cold.



9:41

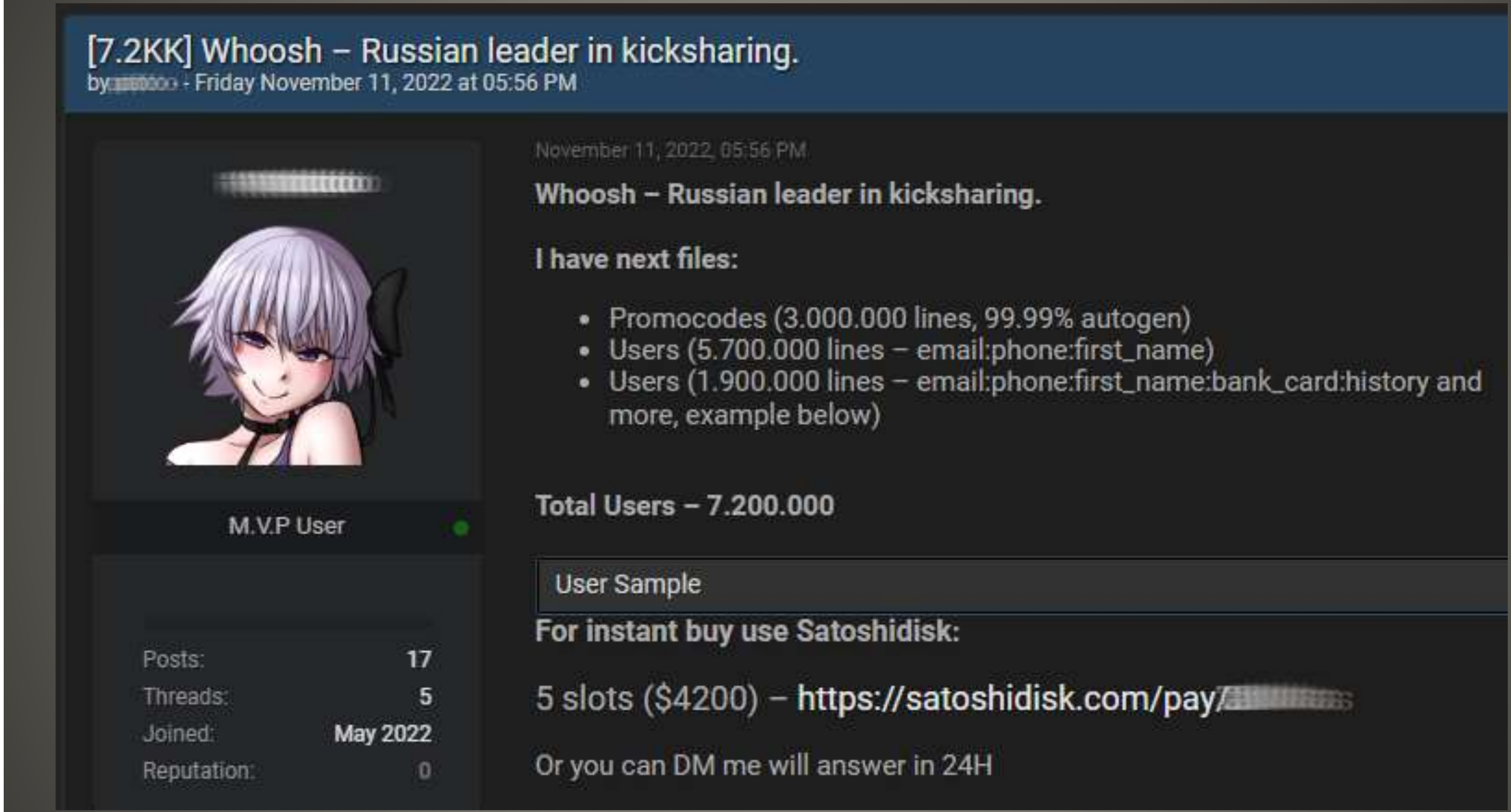
Mayuri Patel

Inyo Mountains Wilderness
Independence, CA
Satellite Location • 4 minutes ago

Location Sent via Satellite

Mayuri sent you their location via satellite because they have no other network available.

- Whoosh 7.2 million customer records stolen & sold



[7.2KK] Whoosh – Russian leader in kicksharing.
by[redacted] - Friday November 11, 2022 at 05:56 PM

[redacted]

M.V.P User

Posts: 17
Threads: 5
Joined: May 2022
Reputation: 0

November 11, 2022, 05:56 PM

Whoosh – Russian leader in kicksharing.

I have next files:

- Promocodes (3.000.000 lines, 99.99% autogen)
- Users (5.700.000 lines – email:phone:first_name)
- Users (1.900.000 lines – email:phone:first_name:bank_card:history and more, example below)

Total Users – 7.200.000

User Sample

For instant buy use Satoshidisk:

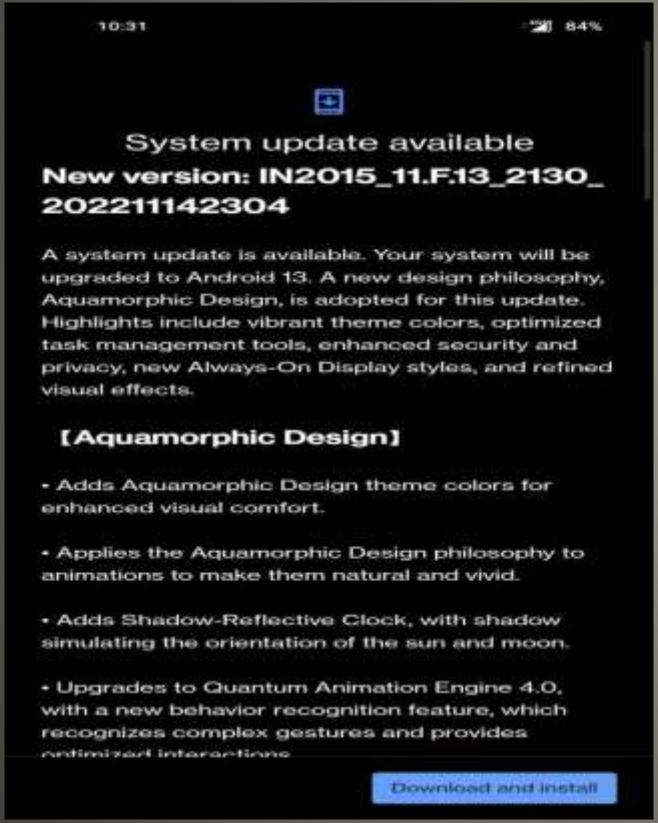
5 slots ($4200) – https://satoshidisk.com/pay/[redacted]

Or you can DM me will answer in 24H

Current Issues

- Android 13 update

Some Pixel devices, Some Samsung, some OnePlus



10:31 84%

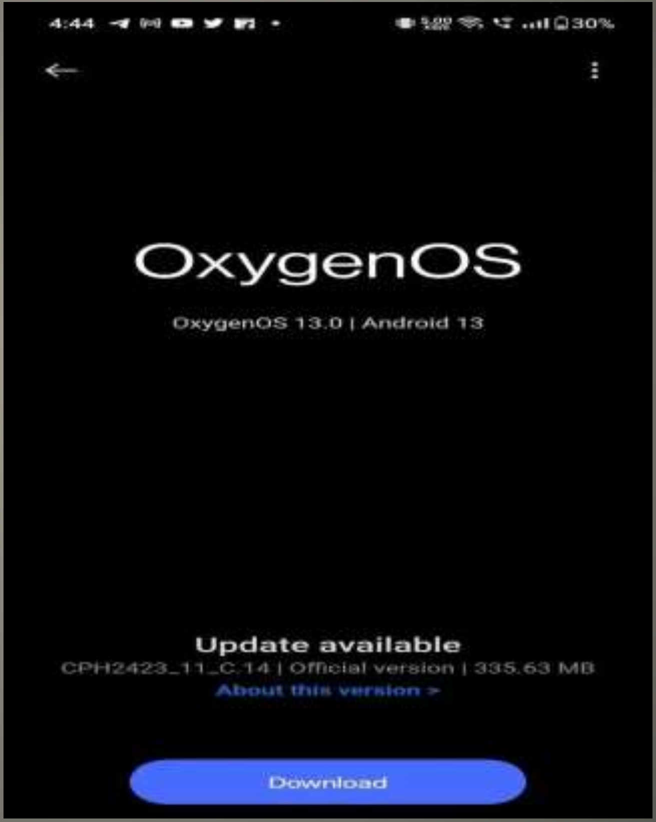
System update available

New version: IN2015_11.F.13_2130_202211142304

A system update is available. Your system will be upgraded to Android 13. A new design philosophy, Aquamorphic Design, is adopted for this update. Highlights include vibrant theme colors, optimized task management tools, enhanced security and privacy, new Always-On Display styles, and refined visual effects.

[Aquamorphic Design]

- Adds Aquamorphic Design theme colors for enhanced visual comfort.
- Applies the Aquamorphic Design philosophy to animations to make them natural and vivid.
- Adds Shadow-Reflective Clock, with shadow simulating the orientation of the sun and moon.
- Upgrades to Quantum Animation Engine 4.0, with a new behavior recognition feature, which recognizes complex gestures and provides optimized interactions



4:44 30%

OxygenOS

OxygenOS 13.0 | Android 13

Update available

CPH2423_11_C.14 | Official version | 335.63 MB

Current Issues

- Optus – telecommunications
- Medibank – insurance
- Millions of customers
- US SolarWinds & Colonial Pipeline
- Traditional tools, law enforcement, diplomatic tools ineffective
- Regain cryptocurrency, take down servers
- Pros and CONS

Australia Hacks Back

- https://lifehacker.com/the-best-firefox-extensions-everyone-should-use-1849784170
- uBlock Origin
- 600% Sound Volume
- SponsorBlock
- Absolute Enable Right-Click & Copy
- Dark Reader
- Facebook Container
- Bypass Twitter Login
- LocalCDN
- Augmented Steam
- Everything Metric

Firefox Extensions

- November Patch Tuesday
  Adobe, SAP, Android, VMware, Citrix, …
- Automating host exploitation with AI
  Shennina Framework
  Hack-in-the-box $100,000
  Host Exploitation and/or malware evasion
  NMAP & Metasploit
- LightSpeed vulnerability
  webserver 1.9 million deployments
- Shufflecake Hide volumes
- iOS 16.1.1 "Share with Everyone" airdrop
  Time limit 10 minutes
  China
- Even more crypto heist Pando & DFX Finance
- NSA Cybersecurity Collaboration Center

Current Issues

- Virtual Credit Cards

  One time

  No Refund ability
- Digital Wallet

  PayPal, Apple Pay, Google Pay, etc.

  SECURE THE DEVICES
- Prepaid cards

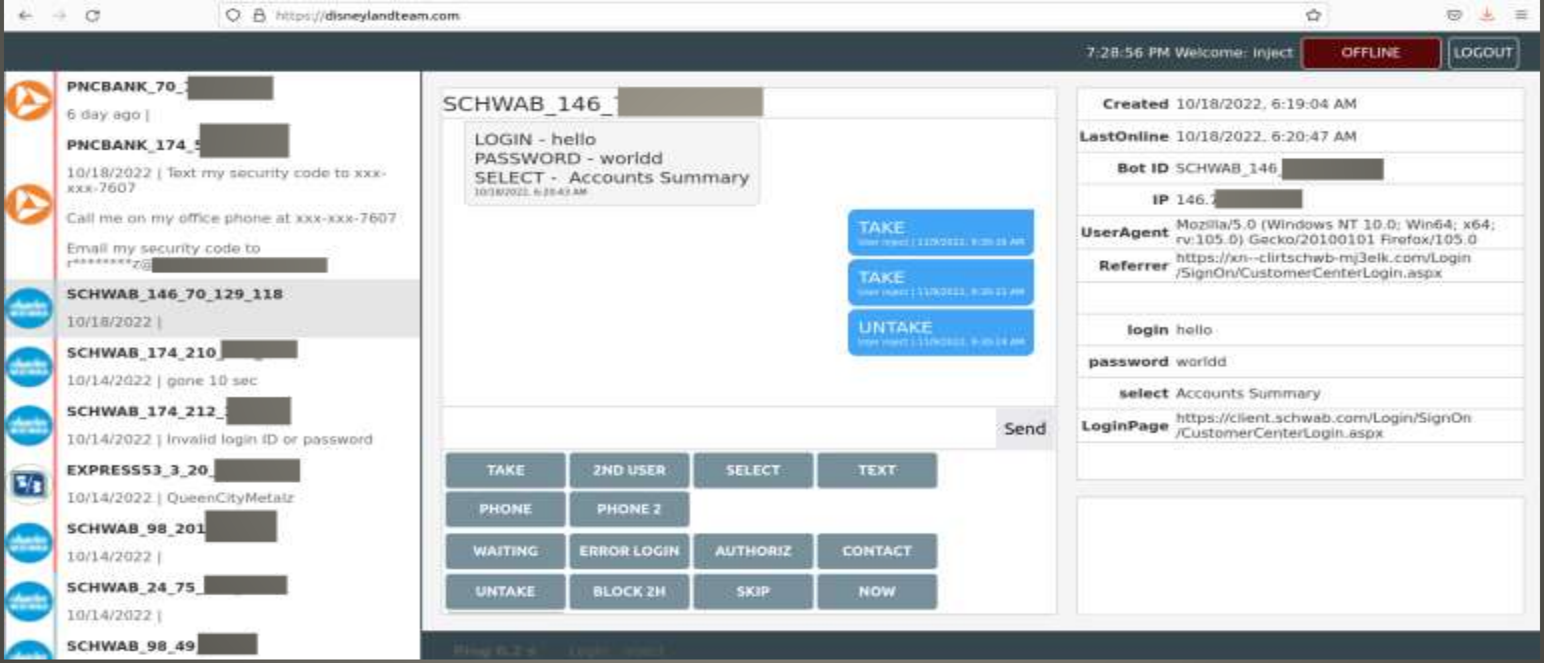
  Fees Loss of card
- Cryptocurrency

  Cold Wallet

  Secure digital crypto wallets

Safer OnLine Payment Methods

- Use of Punnycode
- ạmeripriseẹ[.]com.   NOT   ameriprise.com
- ushank[.]com



https://disneylandteam.com

7:28:56 PM Welcome: Inject

PNCBANK_70_1[redacted]
6 day ago |

PNCBANK_174_5[redacted]
10/18/2022 | Text my security code to xxx-xxx-7607

Call me on my office phone at xxx-xxx-7607

Email my security code to r********z@[redacted]

SCHWAB_146_70_129_118
10/18/2022 |

SCHWAB_174_210_[redacted]
10/14/2022 | gone 10 sec

SCHWAB_174_212_[redacted]
10/14/2022 | Invalid login ID or password

EXPRESS53_3_20_[redacted]
10/14/2022 | QueenCityMetalz

SCHWAB_98_201[redacted]
10/14/2022 |

SCHWAB_24_75_[redacted]
10/14/2022 |

SCHWAB_98_49[redacted]

SCHWAB_146_1[redacted]

LOGIN - hello
PASSWORD - worldd
SELECT - Accounts Summary
10/18/2022, 6:28:43 AM

Created	10/18/2022, 6:19:04 AM
LastOnline	10/18/2022, 6:20:47 AM
Bot ID	SCHWAB_146_[redacted]
IP	146.7[redacted]
UserAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
Referrer	https://xn--clirtschwb-mj3elk.com/Login/SignOn/CustomerCenterLogin.aspx
login	hello
password	worldd
select	Accounts Summary
LoginPage	https://client.schwab.com/Login/SignOn/CustomerCenterLogin.aspx

Punning

- 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