Sun City Computer Club

Cyber Security SIG Special Alert

May 3 , 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

Recent Events

- SolarWinds
- US Intelligence services attribute Russia
- “inside” for 4 months
- May NEVER be completely cleared
- US government, Fortune 500, Google, Microsoft, etc.
- Other foreign actors used same vulnerabilities?
- It was news, then it was not
- Sanctions with blended reasons

Recent Events

- Microsoft Exchange Server vulnerability
- Attribution not strong
- Even more widespread
- Webroot
- FBI authorized to seek and destroy *known* Webroot scripts
- Online merchants in cloud
- Cloud co-hosting

Recent Events

- Pulse Secure VPN
- MacOS 11.3 Big Sur
- Facebook Phone numbers leaked
- Have I Been Pwned
  https://haveibeenpwned.com/
- Pandemic
- Economy
- WFH
- Divisiveness
- Hacking tools metasploit
- Shodan

https://www.shodan.io/search?query=title%3A"Outlook+Web+Access"+%21port%3A443%2C80

Shodan Developers Book View All...

SHODAN title:"Outlook Web Access" !port:443,80 Explore Downloads Reports Contact Us

Exploits Maps Download Results Create Report

TOP COUNTRIES

Poland	11
China	2
United States	1
Russian Federation	1
Pakistan	1

TOP SERVICES

HTTPS (8443)	13
HTTP (8080)	3
444	3
HTTP (81)	1

Showing results 1 - 9 of 20

Microsoft Outlook Web Access

89.174.250.104
GTS Poland Sp. z o.o.
Added on 2015-12-06 16:08:43 GMT
Poland
Details

SSL Certificate

Issued By:
|- Common Name: **bizi.support-online.pl**
|- Organization: **Support Online Sp. z o.o.**

Issued To:
|- Common Name: **wsrv.soundtrade.pl**
|- Organization: **Soundtrade**

Supported SSL Versions
SSLv2, SSLv3, TLSv1

Microsoft Outlook Web Access

24.212.47.131
tap.ambulancesabitemis.ca
Cablevision du Nord de Quebec
Added on 2015-12-05 09:41:29 GMT
Canada, Val-d'or
Details

SSL Certificate

Issued By:
|- Common Name: **StartCom Class 1 Primary Intermediate Server CA**
|- Organization: **StartCom Ltd.**

Recent Events

- COMB
  Combination of Many Breaches
  4 BILLION account logins
- Hacking as a service
- Identity theft is misnomer
- Information gives no indication of being stolen
- eMail account takeover & forward
- Supply chain attacks to increase

- Cyber criminals use HUGE resources to “spray” Internet with stolen credentials with Artificial Intelligence aids
- Large numbers of friends already compromised

Credential Stuffing

Take aways

- *They* are not after me
  They are after any/everyone
- Passphrases
  Strong
  Unique
  Inventory
  Separation
  Consider NOT storing in browsers
  Use hints
- Multi Factor Authentication

Take aways

- Be aware, prepare, understand
- Set up alerts
- Think, Investigate IFF then click
- Keep updating

  Operating system, Applications, Browsers, Browser extensions, router firmware, security suites and signatures, …
- Raise suspicion

  eMail, Text, Messages, Phone calls, Social media posts, pop-ups, Ads, …

Take Aways

- 3-2-1 backups
- Encryption
- Inventory
- Financial

Re-consider credit/debit card management

Use cellular tether and live Linux

Report the Abuse

- Your friend (sender) may NOT get your warning
- Report abuse to provider
  Facebook, Gmail, Yahoo, AOL, etc.
- Account takeover
- Spoofing
- Same name, new account
- Scam, Spam, fraud, Identity theft,

- An advantage of Spam & robocalls?

- We reviewed the profile your friend reported and found that it isn't pretending to be you and doesn't go against our Community Standards. Note: If you see something on someone's profile that shouldn't be on Facebook, be sure to report the content (ex: a photo or video), not the entire profile.

  Thanks,
  The Facebook Team

Spot the Difference?

maybank2u.com is not the same as
maybɑnk2u.com

citibank.com is not the same as
citibɑnk.com
(the first one is correct, the second one is from hackers)

The "a" in the later url is a cyrillic alphabet.

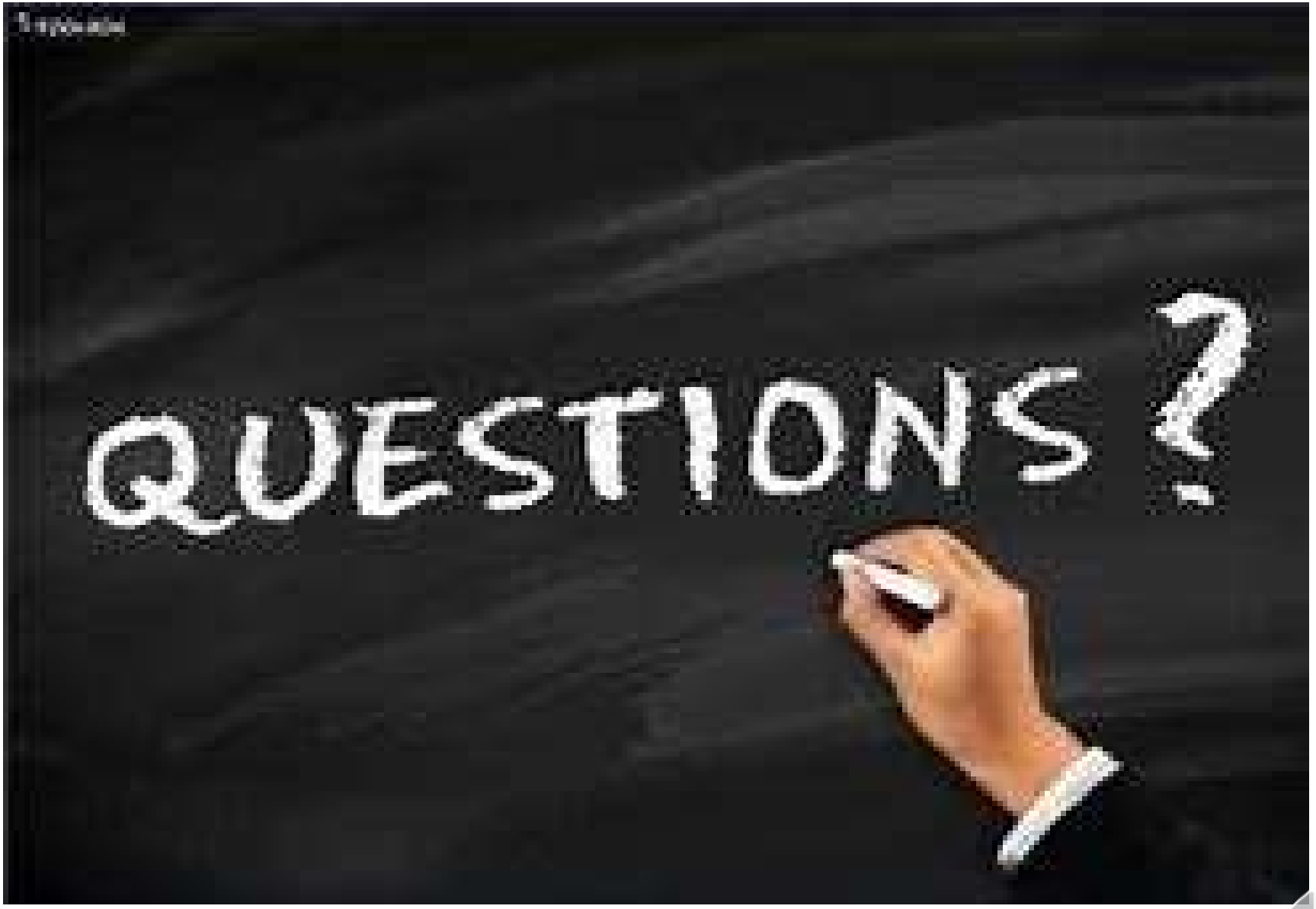
- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet
Education classes:
Using a Password Manager
Computer and Information Security

Garmin

- Questions, suggestions, comments?

SCCCCyber@gmail.com


QUESTIONS?