

Cybersecurity Presentation



Hacks, Tips & Tools



2020 ICA - CyberCon V



Blake Griffin - CNE IT Solutions



blake@cne-it.com

What is the first thing most of us do when traveling?

(Lets just pretend that we traveled to this conference)



There is Open / Public WiFi everywhere!



plug into
free Wi-Fi*
during your stay.

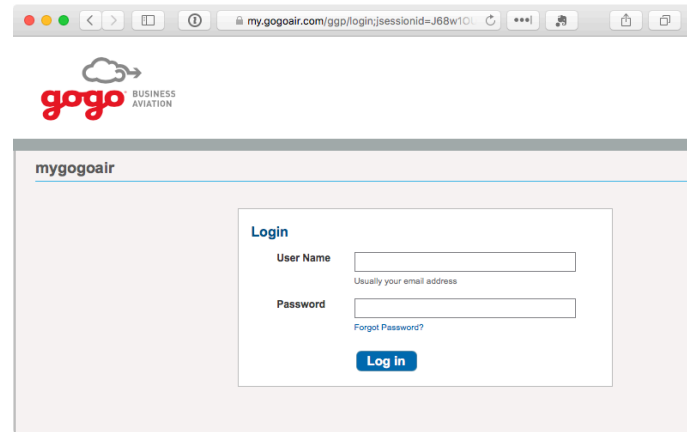
Stay connected at any of our hotels with free Wi-Fi, including Courtyard®, Fairfield Inn & Suites®, SpringHill Suites®, Residence Inn® or TownePlace Suites location. It's the best way to stay in touch without spending a dime!

book now!

Plug into a great value.

*Free Wi-Fi available in North and Central America

COURTYARD®
Fairfield
Fairfield Inn & Suites®
SpringHill Suites®
Residence Inn
TownePlace Suites®
Marriott



mygogoair

Login

User Name
Usually your email address

Password
Forgot Password?

Log in



I'm Feeling Lucky

Google

SINCE 1971

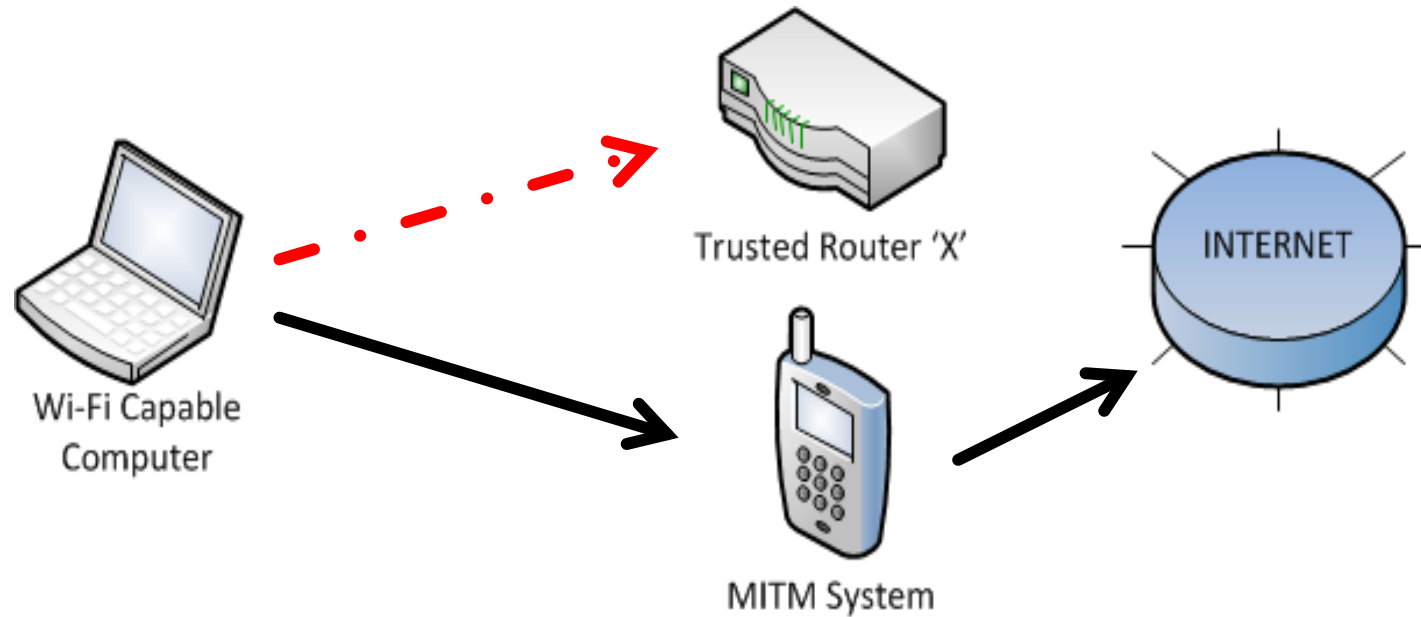
Free WiFi
From our friends at Google

Accept & Connect

I agree to the Terms of Service and have reviewed the Google Privacy Policy
Need help? 855-446-2374

Google

Perfect opportunity for hackers and a Man-in-the-Middle attack



WiFi Pineapple

- ▶ Cheap, portable device used typically for penetration testing.
- ▶ Can be used maliciously for a MiTm attack
- ▶ Easy to use
 - ▶ Multiple modules to download to initiate attacks.
- ▶ Demo of some examples of what can be done.



0 hours, 5 minutes

UPTIME

100% CPU USAGE

2

CLIENTS CONNECTED

14

SSIDS IN POOL

14 SSIDS ADDED THIS SESSION

Clients

MAC Address	IP Address	SSID	Hostname	Kick Client
<input type="checkbox"/> 40:4E:36:8D:DE:D3	No IP	No SSID	No Hostname	<button>Kick</button>
<input type="checkbox"/> B0:6F:E0:11:31:2A	172.16.42.130	<input type="checkbox"/> fg123e	Galaxy-Tab-A-8	<button>Kick</button>
<input type="checkbox"/> A8:51:5B:55:E3:0E	172.16.42.196	<input type="checkbox"/> Sheraton Guest	Galaxy-J3-Orbit	<button>Kick</button>

68

SSIDS IN POOL

0 SSIDS ADDED THIS SESSION

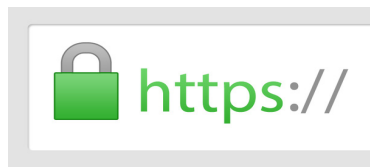
SSID Pool

Refresh

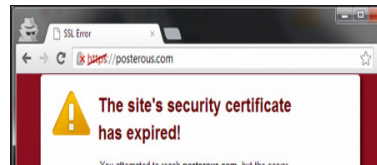
Cneit
shgw
Broncos iPhone
Heyisthisournetwork?
LD Cellular
Airport Extreme
fg123e
0A344ABB
7SROCKS
sheero
srgwifi
XCI_GUEST
Peaksunset
ADTRAN_2.4GHZ_2054
Guest-LaPerla
ATT4MCu2HA_EXT

How to avoid Public WiFi Pitfalls

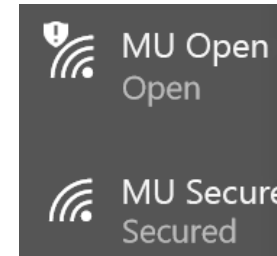
- ▶ Don't connect to open networks
 - ▶ Corporations can control with Group Policies or MDM
 - ▶ Turn off WiFi when not using.
- ▶ Use VPN if possible.
 - ▶ Third party provider or corporate VPN
- ▶ Use your phone WiFi Hotspot instead
- ▶ Avoid using website where there is personal info
- ▶ Avoid using unsecure websites



Good



Bad



Bad

Good

LastPass....|

Password Related Suggestions



- ▶ Use of 20+ character passphrases
- ▶ Use of a password manager such as LastPass.
- ▶ Enable 2FA wherever possible
- ▶ Don't Reuse Passwords
 - ▶ Keep work passwords different from personal passwords.
- ▶ TRAINING!



What is Vishing?



- ▶ Voice (or VoIP) phishing
- ▶ Tactic in which an individual is tricked into providing financial or sensitive information over the phone.
- ▶ Doesn't always occur over the internet and is carried out over voice technologies.
- ▶ Traditionally the target receives a call and is told suspicious activity has occurred.
 - ▶ Caller ID spoofing
- ▶ Target is then told to call in and verify their information.



Vishing Man-in-the-Middle Demonstration

FreePBX Setup

Log File Settings

General Settings

Log Files

Rectangular Snip

Logfile Help

Field	Information
File Name	Name of file, relative to Asterisk logpath. Use absolute path for a different location
Debug	Messages used for debugging. Do not report these as error's unless you have a specific issue that you are attempting to debug. Also note that Debug messages are also very verbose and can and do fill up logfiles (and disk storage) quickly.
DTMF	Keypresses as understood by asterisk. Usefull for debugging IVR and VM issues.
Error	Critical errors and issues
Fax	Transmition and receiving of faxes
Notice	Messages of specific actions, such as a phone registration or call completion
Verbose	Step-by-step messages of every step of a call flow. Always enable and review if calls dont flow as expected
Warning	Possible issues with dialplan syntax or call flow, but not critical.

File Name	Debug	DTMF	Error	Fax	Notice	Verbose	Warning	Security	Delete
full	On	Off	On	Off	On	On	On	Off	
console	On	Off	On	Off	On	On	On	Off	
DTMF	Off	On	Off	Off	Off	Off	Off	Off	

FreePBX Setup

Extension: 215

General

Voicemail

Find Me/Follow Me

Advanced

Pin Sets

Zulu

Other

General Settings

Enabled ?

Yes

No

Enable Calendar Matching ?

Yes

No

Calendar ?

--Not Calendar Controlled--

Calendar Group ?

--Not Calendar Group Controlled--

Calendar Match Inverse ?

Yes

No

Initial Ring Time ?

1

Ring Strategy ?

ringallv2-prim

Ring Time ?

20

Follow-Me List ?

8008722657#

Quick Select

Announcement ?

None

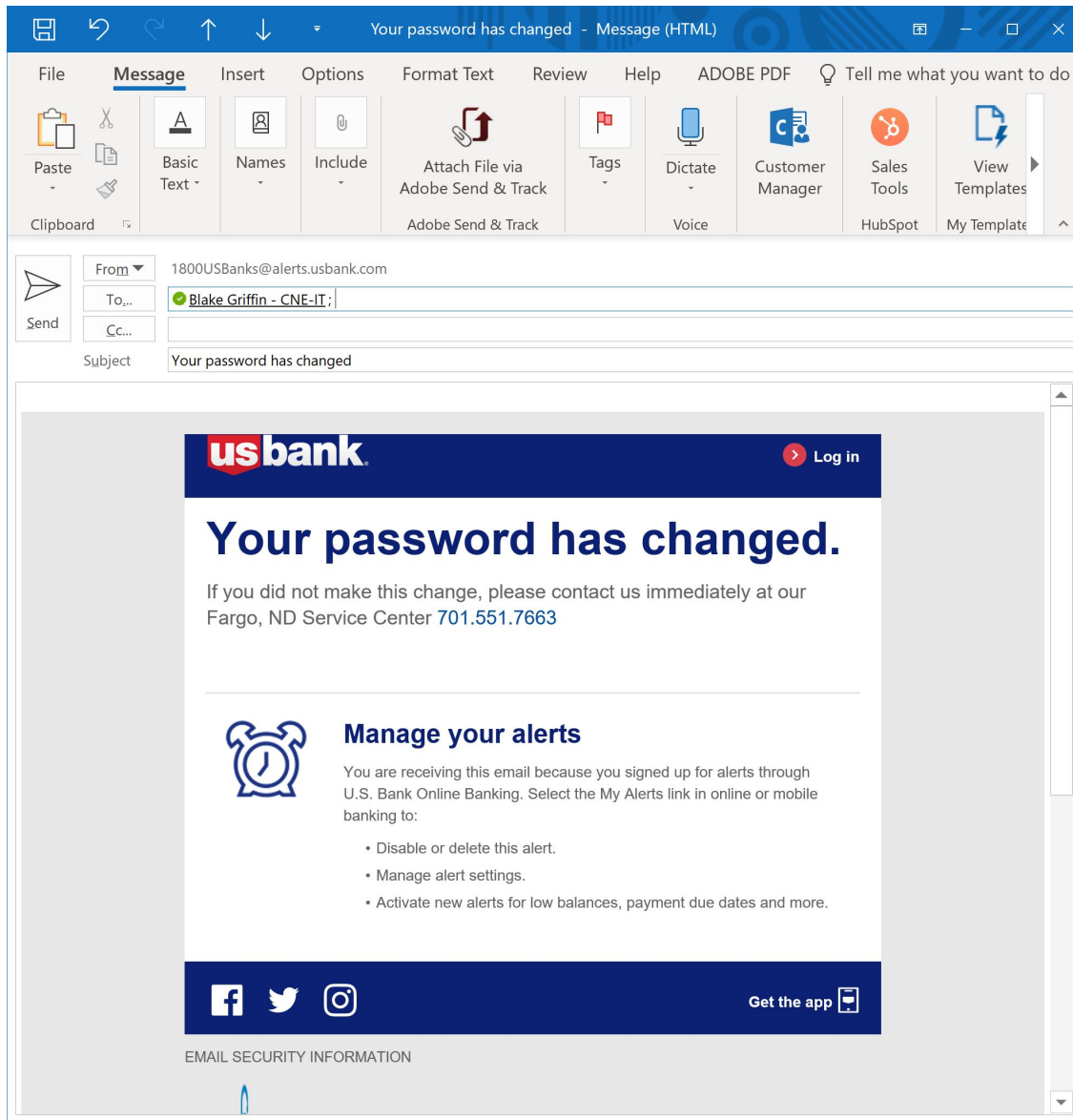
Play Music On Hold ?

Ring

FreePBX Setup

— Recording Options

Inbound External Calls ?	Force	Yes	Don't Care	No	Never
Outbound External Calls ?	Force	Yes	Don't Care	No	Never
Inbound Internal Calls ?	Force	Yes	Don't Care	No	Never
Outbound Internal Calls ?	Force	Yes	Don't Care	No	Never
On Demand Recording ?	Disable	Enable	Override		
Record Priority Policy ?	10				



Sample Email

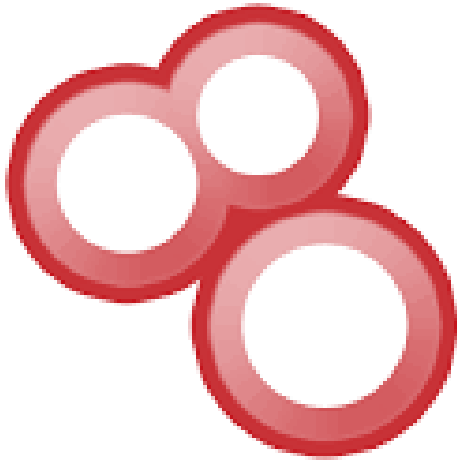
How to Avoid Vishing

- ▶ If you receive an email or voicemail from the “institution”, never call back the number that they give.
- ▶ Verify with your banks website the correct number to call.
- ▶ On all accounts, put all numbers that you will call from and only call from those numbers.
 - ▶ Full account number doesn't have to be entered that way for most banks and credit cards.
- ▶ **TRAINING!**



SHODAN

What is Shodan?



- ▶ Its like Google, but for everything “thing” connected to the Internet.
- ▶ Crawls the internet for connected devices.
- ▶ Finds open ports, systems with default passwords, etc.
- ▶ Port scanning is not illegal and doesn’t violate the Computer Fraud and Abuse Act
- ▶ What is done after that can be very illegal.
- ▶ Can be used for very bad things, especially when used with Metasploit / Autosploit
- ▶ Great thing.....You can use it to search your own network.




How do they get in?

▶ ABUSE LEGITIMATE PROCESSES



Careers Page / Apply Online

Friendly Person	
really@trustworthy.com	
(701) 555-1212	
1307 N. University Dr.	
Fargo	
ND	
58102	

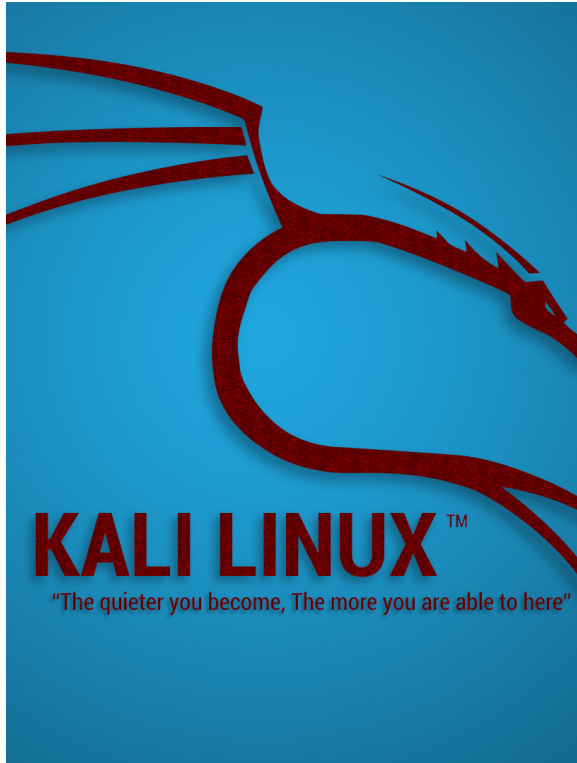
RESUME

Choose File

Resume_Spt_Specialist.docm

Hello ABA Team, please accept my attached resume for your Support Specialist opening. As you can see, I've been constantly improving my technical skills over the past two years and I'm ready to move into a more challenging role.

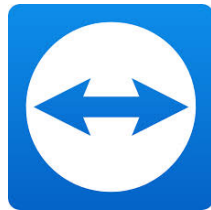
Thank you so much for your consideration!



Phishing Hacking Demo



Ransomware and Endpoint Detect & Respond (EDR) Demo



How to Avoid Ransomware Pitfalls



Implement a true layered security approach.

AV
Secure DNS
Strong Backup Regimen as rollbacks are not always guaranteed.
Checklist at the booth!



Endpoint Detect & Respond

24x7x365 SOC
Rollback Capabilities
Insurance Policy



TRAINING!

Contact me for this checklist!





TRAINING

Knowledge
useful abilities.
backbone of co
quired for a tr

Questions?

**BLAKE
GRIFFIN**

BLAKE@CNE-IT.COM

Contact Information
CNE IT Solutions
(701) 356-8955