# PROPERTY EDUCATION IN THE LAND OF ENCHANTMENT


# Stan Hall
# Cyber Security

PROPERTY
EDUCATION
IN THE LAND OF
ENCHANTMENT

# Cyber Security and Property Management

PROPERTY EDUCATION IN THE LAND OF ENCHANTMENT

## Why Cyber Security? I am a Property Professional!

Cyber Security “Protects” the assets. Property Professional’s “Manage” the assets.

From the Cyber Security WiKi site:

Cyber Security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

From the NPMA web site:

NPMA is the leading membership association for personal property and fixed-asset professionals.

Personal property professionals are responsible for the effective and efficient management of hundreds of billions of dollars of fixed-assets at leading corporations, at federal, state and local government agencies, and at healthcare and educational institutions.

Companies and organizations around the world benefit from the strategic role of fixed-asset and personal property professionals who are poised to be strong, integral parts of all organizational processes and contribute greatly to the bottom line.

Why? Because effective, efficient asset management results in cost savings and cost avoidance throughout the property life cycle, from determination of requirements, through acquisition, utilization and disposition.

# Cyber Security and Property Management



## Why Cyber Security? I am a Property Professional! -Continued

- If you can't use the device, you essentially have lost the device
- If you need to purchase a replacement, this impacts the bottom line
- If you receive counterfeit hardware, the equipment cannot be used
- A (successful) cyber attack will result in lost work, reputation and costly repairs
- A (successful) cyber attack will impact all members of the workforce for the company at work and possibly at home
- A (successful) cyber attack will most likely be the gift that keeps on giving for all members of the workforce

# Phishing

Sometimes they are Random, other times they are specific

- They prey on catching you off guard.
  - “PAY THIS INVOICE NOW!”
  - Click here to report Fraudulent activity
  - Email - Stan, this is Daniel (Friend) I need help with this site (Web link)
  - Email - Stan, This is Monica (Coworker) we have a problem with this document

The adversary will study you and your company. First from External sources and Internally if they get in.

End goal is to make money

# Vishing – (Voice Phishing)

Like Phishing, sometimes they are Random, other times they are specific

- They prey on catching you off guard.
  - Vm-The is Steve, I need you to PAY THIS INVOICE NOW!
  - Stan, This is Monica (Coworker) I need you to call me back to verify some information
  - The always favorite. I'm calling about your Car Warranty. (It does work)
  - Another favorite. We are calling because your computer is hacked. (Just tell them it is an iPad. They will hang up) (This one works also)

End goal is still to make money

# Smishing - Mobile Phishing



Same as the other two “ishings”, but with text messages or phone calls

- This device has been hacked, Click here to get help
- Stan, This is Monica (Coworker) I need you to call me to verify some information

Mobile carriers are getting better at flagging fraudulent calls and preventing text messages from getting delivered for the Random spray attacks. Targeted calls and messages will still get through

End goal is to make any money

# Ransomware

They will try all of the “ishings” in order to get to this stage.

They will look for unpatched systems

They will use Zero-day exploits

- Vulnerabilities that are unknown to the vendor and/or have no patch

They will use other bad guys services as a service to help out

Ransomware of old, would get in, encrypt your data and try to collect money

# Ransomware - Continued

Ransomware of new, will get in, **“study you in detail”**, steal your data, encrypt your data and try to collect money from many avenues

- The offer the decrypt key for a price
- They know how much you can pay
- They threaten to release all of your data unless you pay
- The call your employees or customers and have them pay to keep their data safe (PII, Credit Card info, other data)
- They use the employee or customer data for identity fraud

End goal is to make as much money as they can

# What can I do?

Think before you click on that link

Be mindful both at work and at home

Keep your software current

-Operating system

-Application that are used

Remember that free is never really free. You are giving up something

Question yourself on any thing. Remember “In god we trust” all others we validate

Keep in mind that Amazon will never call to report a fraudulent charge. They will just stop it and make you verify it. Or if it does make it through, give you the option to report and get a refund

I can’t even ship to my kids without verifying everything and logging in again

# What else can I do?

Keep in mind that Amazon will NEVER call to report a fraudulent charge

- You can't event get a live person when you need to

Microsoft will never know that it is your machine that is infected with malware or a virus.  (There are Billions of devices out there and they do not know you from me)

Apple will never know that your machine is infected with malware or a virus

If you get a fraudulent charge on your credit card. You call the credit card company yourself and report the issue. They do not call you. They will block it if it is too suspicious

Never, never, never let some one help you over the phone. Especially is they CALLED YOU ←

Set up text message notifications for Credit card or Bank card transactions

Keep a current AntiVirus app on your system

Add a pop-up blocker

Add Malware protection

# What can I do at work?

Verify the property that was delivered was what was ordered and from the source you expected

Remember that the advisory will do homework on you and your company if you are targeted

If you are still using password at your company, ask why they have not implemented a Multi-Factor authentication solution (Smart Card)

Passwords have been and still are major fails for any company.

Remember, They are only in it to make a buck.

# Notable headlines to talk about

- Hackers Capitalizing On Recently Passed U.S. Infrastructure Bill
- Cyber Expert: Be Leery Of Social Media Friend Requests
- Hackers Releasing Stolen Children PII On The Dark Web
- Cyber Task Force Member: “Cybercrime Growth Is Unbelievable”
- CISA Issues Ransomware Fact Sheet
  - (https://www.cisa.gov/sites/default/files/publications/Fact%20sheet_Ransomware%20Awareness%20Campaign_20210119_508.pdf)
  - cisa.gov good site to review – Cybersecurity & Infrastructure Security Agency
- Why 2-Factor Authentication Is More Important Than Ever
- FBI: Americans Suckered Out Of $8 Million
- Ransomware Hackers Continue Upping Their Game
- FBI Issues Warning Of A New Ransomware Group
- Federal Trade Commission Issues Text Message Warning
- Hi - I'm Calling From Tech Support to Scam You out of Your Money

# CISA, FBI, NSA warn of increased attacks involving Conti ransomware

Conti often gains initial access to systems through spearphishing campaigns or malicious downloads posing as real software. It then uses that access to scan for credentials to get higher privileges. A Conti playbook leaked by a disgruntled affiliate earlier this month showed that the group has targeted multiple Microsoft vulnerabilities as access points.

From Cyberscoop.com -– dated 9/23/2021