Mildred Suriel

Intro Info Tech

April 17th, 2019

Week 11 – Security

Security

1. Briefly describe how you avoid becoming a phishing victim.

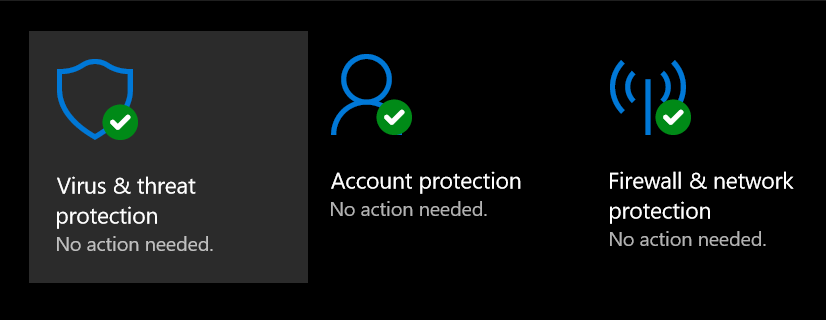
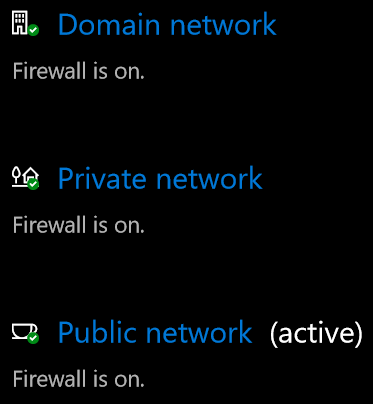
* Keep yourself up to date on the latest phishing trends
* Be cautions before clicking on unknown links
* Verify a site before inputting payment information
* Keep tabs on all online accounts as often as possible
* Make sure you have the latest version of your software
* Be mindful before clicking on a popup on websites

2. Find a news article involving computer security. Briefly describe the news item.

**Article:** The Importance of Securing Sensitive Data in a 5G World by Scott Sykes and Samuel Visner

Once 5G capabilities is truly made accessible to the majority of consumers the need for security will become crucial at many levels. It will be the tasks of the operators to secure the various types of data such as; customer, transaction and network data. Securing data becomes increasingly difficult due to 5G enabling network slicing.

3. Add a screen shot of the security settings from the windows control panel (security center) showing whether there is a firewall on.



4. Answer all the questions in the above portion of the lab.

* What anti-virus software is installed (lab and home)? When was it last updated? When was the last scan?

Windows defender. Update:4/17/19 Scan:4/16/19

* What Anti-spyware software are you using? When was it last updated? When was the last scan?

I do not have anti-spyware software on my pc.

* Do you have a firewall running?

Yes

5. What programs are installed? Are any viruses? Spyware? Toolbars for your browsers? If you have any of those make sure you uninstall them.

I recognized all installed programs on my pc

6. When was your computer last updated? What updates have been installed since you've had it?

My pc was last updated on 4/10/19

Quality, Driver, and Definition updates.

7. Phishing is a type of Social engineering. Describe a different social engineering attack, how it works, why it might be used and how to protect yourself.

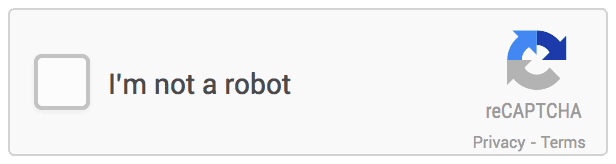
Pretexting: Disguising oneself or passing as someone else to collect private information.

This form of social engineering is most successful when trust is gained from the victim.

I used to see this form of phishing a lot within law firms, the hacker would either hack the lawyer or buyers’ email and change the account information the down payment or mortgage payoff should be wired into and have it wired into their own account. We always strongly suggested the lawyer call the person on a phone number on file to verify all bank account information.

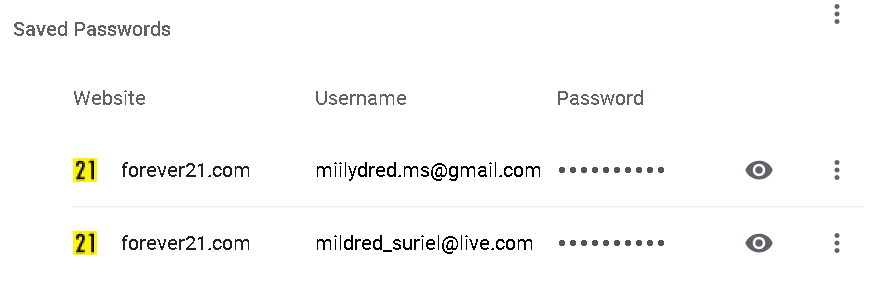
8. Explain what a captcha is and why it is used in your own words. Include a picture of one.

A system that allows a computer to differentiate when it’s a human utilizing the program or another computer or machine.



9. Research a password manager. What are the pros and cons to using a password manager? Which one did you pick and why? Pick a free password manager and try it for a week. Which one did you pick and why? Take a screenshot to show you've installed one on your home machine (NOT with visible passwords!)

I use two type of password managers, both already integrated to my pc and my smart phone. I use the google chrome password manager and the one on my iPhone. I use these because they are already into my devices and it makes it easy for me to access al my passwords across multiple platforms and websites. The risk to this is that at times I can open a web page and it will already have my password pre filled and give me the option to view t which makes me cautions if I were ever to allow someone to temporarily use my device. Also if either program was ever hacked all the passwords for my financial institutions would be at risk.



10. What is 2 factor authentication? Why do you use it? If you don't already have it enabled on your email/social networking/etc pick one of those, and enable it. How hard was it to use and enable?

A way of confirming a user’s identity using two different factors. (i.e. password and a code being texted to a cell phone number associated with the account in question.)

I use it to make sure if my device was every stolen it would be\ increasingly more complicated for someone to get a hold of my personal data.