Lesson 10: Rapid Research - Cybercrime

Adapted from code.org curriculum

Objectives: You will be able too…

 Explain the characteristics of a phishing attack

 Explain how a DDoS attack works

 Describe how one computer virus works

 Research and describe a cyber attack found in the news

 Reason about the threats posed by, and methods of recourse for, various types of cyber attacks

Video: Cybersecurity and Crime

 To conclude our thinking about encryption and security we're going to focus for a day on the bad guys, and take a look at cybercrime, how it's conducted, what to look out for and how to protect yourself.

 Video: https://youtu.be/AuYNXgO_f3Y

 We will fill out the "Cybersecurity and Crime Video Worksheet"

Types of attacks:

ঙ DDoS Attacks (and Bot Nets)

ঙ Cyber warfare

ঙ Viruses and Anti Virus Software

ঙ Phishing Scams

ঙ Credit Card theft

ঙ Types of people who commit cybercrimes

Activity: Rapid Research - Cybercrime

 We will use the "Guide: Rapid Research – Cybersecurity and Crime – Activity Guide"

 You can work in pairs, just follow the steps on the guide

 Please do not use Wikipedia as a source (you may look at the references cited at the bottom of Wikipedia to start)

Wrap-up: Review Cybersecurity Terms

 Implementing cybersecurity has software, hardware, and human components.

 This is a theme for the whole lesson

 Vulnerabilities in hardware and software can be compromised as part of an attack.

 But, as mentioned in the video, a large percentage of cybersecurity vulnerabilities are human-related, such as choosing bad passwords, (unintentionally) installing viruses, or giving personal information away.

Wrap-up: Review Cybersecurity Terms

 Sockets layer/transport layer security (SSL/TLS)

 An encryption layer of HTTP. When you see the little lock icon and https it means that you are visiting a website over HTTP but the data going back and forth bewtween you and the server is encrypted.

 SSL (secure sockets layer) and TLS (transport layer security) use public key cryptography to establish a secure connection.

Wrap-up: Review Cybersecurity Terms

 Cyber warfare and cyber crime have widespread and potentially devastating effects.

 This is especially true in the case of warfare which (fortunately) we have not experienced much of on a global scale. But using cyber attacks to cripple basic infrastructure (power, water) and communication could be devastating.

 Distributed denial of service attacks (DDoS)

 Typically a virus installed on many computers (thousands) activate at the same time and flood a target with traffic to the point the server becomes overwhelmed – doing this can render web services like DNS, or routers, or certain websites useless and unresponsive.

Wrap-up: Review Cybersecurity Terms

 Phishing scams

 Typically a thief trying to trick you into sending them sensitive information. Typically these include emails about system updates asking you send your username and password, social security number or other things.

 More sophisticated scams can make websites and email look very similar to the real thing.

Wrap-up: Review Cybersecurity Terms

 Viruses / Antivirus software and firewalls

- A virus is program that runs on a computer to do something the owner of the computer does not intend. Viruses can be used as a Bot Net to trigger a DDoS-style attack, or they can spy on your computer activity, such as capturing all the keystrokes you make at the computer, or websites you visit, etc.

- Antivirus software usually keeps big lists of known viruses and scans your computer looking for the virus programs in order to get rid of them.

- A "firewall" is simply software that runs on servers (often routers) that only allows traffic through according to some set of security rules.

Now…

Go ahead and answer the questions on Code Studio