Why Is Cyber Security So Important?

Almost everything happens online today (not that that’s a bad thing): Business, banking, communication, and entertainment. This means that there is a lot of information going back and forth between your computer, your internet service provider, and servers for websites. If someone tried to gather information on you, they are likely to be able to find quite a bit, and while it is not possible to eliminate this entirely, you can take preventative measures to reduce the harm that someone could do. Such harm may include financial theft or identity theft.
Password Security

Passwords are used to keep your information private, they should be kept secure and only to you. Use difficult passwords that cannot be ‘brute force hacked’.

Password generators and managers are helpful and allow you to use more complicated passwords that computers can’t guess.
Password Security

This password generator: [http://correcthorsebatterystaple.net/](http://correcthorsebatterystaple.net/) is based off of a webcomic called xkcd (next slide)

It creates between 2-10 random words that can be separated by a character ((),/?><,etc) and allows you to memorize your password easier, especially while using a password manager.

“Aunt-Bribe-Pair-Compare-8” - easy to remember, hard for computers and people to guess.
Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
Keeping Your Information Private

When interacting on the internet, make sure to remember that once you post something it is there forever. Anyone can look at your social media accounts and see everything that you ever said. This can be used to gather information about you, things that you necessarily wouldn’t want everyone to know.

Examples: If you post a picture on the street you live on, make sure the numbers of houses aren’t visible. Don’t give your email, phone number, address, or any other telling information about yourself.
Keeping Your Information Private

Identity theft comes in several different forms:

Medical ID Theft (when someone steals your medical information to make claims, and has work done in your name), Tax ID Theft (when someone uses your information to file taxes with the IRS), and most relevant, Social ID Theft (when someone gets information from your social media and uses it to create false profiles or to use for other reasons).

Identity theft can largely be avoided with some internet smarts and common sense.
Keeping Your Information Private

How to avoid identity theft on the internet:

● Keep accounts private on social media
● Do not accept requests from unknown people
● Post wisely, information can be used against you in ways you didn’t intend (announcing vacations, address, phone number, etc.)
● Do not give your password to anyone, especially online
● Avoid participating in online quizzes, especially if they request lots of personal information
● Use security software on your computers
● Be very wary of downloads on any website
● USE COMMON SENSE - if it looks suspicious, it probably is
Privacy And Anonymity

In today’s world, it is hard to be truly private but there are some things you can do to limit the amount of infringement.

You can:

- Install a firewall/malware defense
- Make sure your internet browser is not storing too much information about you using tools such as BrowserLeaks.com and Ghostery extension to see what trackers can see
- Use a VPN to scramble your traffic and IP
Examples Of Significant Hacks

WannaCry - In May of 2017, a ransomware called WannaCry was spread, affecting more than 100,000 computers. It got into the computers in the hospitals of the UK, which delayed procedures and incited chaos. The hackers earned about $130,000 from the victims.

Equifax Breach - In September of 2017, the credit report company Equifax was breached through a flaw in their security software (Apache Struts). This led to the availability of up to 145 million Americans’ credit card information and identity information.
About the Program

Over summer, I went to a camp at Dartmouth College called Gen-Cyber, which aims to teach teens about cyber security with labs, lectures, and small field trips. The goal of the program is to generate more interest in cyber security and provide insight on security issues. The program is funded by the National Science Foundation and the National Security Agency.

http://www.ists.dartmouth.edu/events/gencyber2017.html
Works Cited

https://www.teamsid.com/the-importance-of-having-a-secure-password-infographic/
http://correcthorsebatterystaple.net/
https://www.usa.gov/identity-theft
http://www.idtheftcenter.org/Fact-Sheets/fs-138.html
https://www.pcmag.com/article2/0,2817,2363302,00.asp