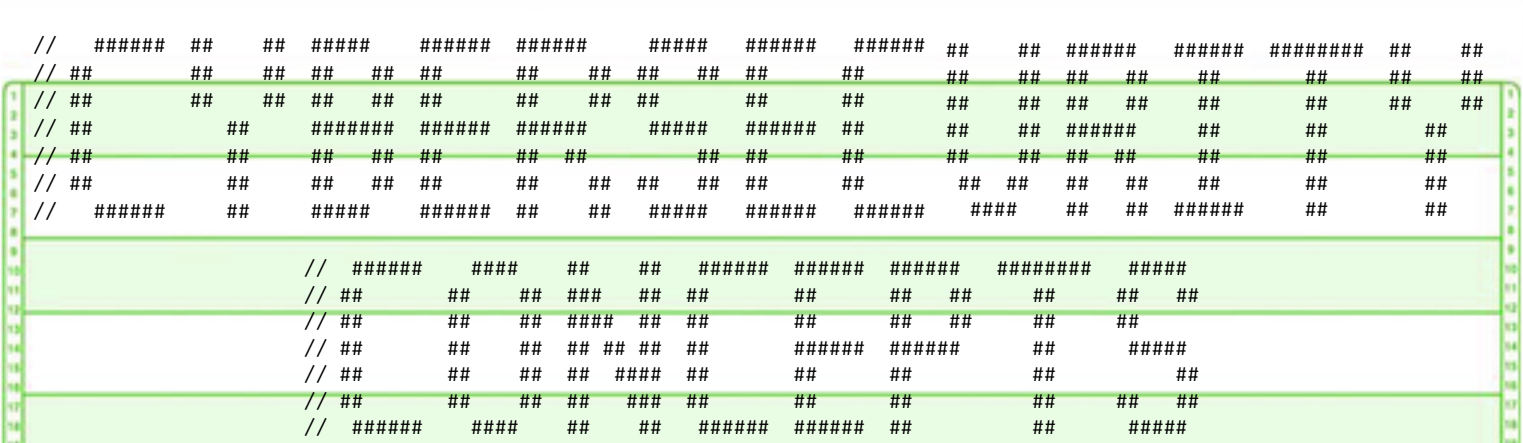

// Written by Kaitlyn J. Smith.

We should start very simply at what exactly “cybersecurity” is:

Cybersecurity is about protecting technology from digital attacks. Digital attacks come in many forms, but the goal is to damage technological systems by gaining unauthorized access. The entire world is connected through technology, and almost everybody uses some sort of computer or digital device on a daily basis. This technology usually holds important information relevant to our lives. How would you feel if a person entered into your devices without permission and tried to do bad things? I don’t think anybody would appreciate that! At a larger scale, these digital attacks can lead to unauthorized disclosure of information critical to national security and extreme physical damage such as infrastructure damage, power outages, or even loss of life. This is why we need cybersecurity and people who know cybersecurity: they keep us, our devices, and our information protected.

// ######## Below are some of the cybersecurity concepts I am currently focused on ########

Malware: malware is software on your computer that wants to do something bad or harmful to you or your system. It comes in many different forms. Common ones include:

- **Viruses** - malware that copies itself and spreads throughout systems to damage them.
- **Ransomware** - malware that locks you out of your system until you pay a ransom. It encrypts (changes the information so you can’t understand it) your files and will not let you regain access until you give the attacker what they want. It can be extremely expensive to deal with and have costed organizations millions to BILLIONS of dollars.
- **Trojans** - similar in concept to the popular Greek Trojan Horse story, a Trojan Horse is a type of malware that disguises itself as an innocent program, but in reality is evil and will do bad things once inside your system. It may look legitimate, but once it gets onto your device…Boom! Bad stuff happens. Not fun!
- **Spyware** - just like a spy, spyware hides on your device and spies on you. It will monitor your activity and steal sensitive information (like passwords), and you will be completely oblivious that this is even happening!

The above only scratches the surface of the different types of malware that exist. There are many, many more.

Bug: not the insect! In this context, a bug is a defect in a computer system or program.

Exploitation: any method of taking advantage of a bug to get some type of task accomplished. This task is usually malicious. An example of exploitation would be a person taking advantage of a bug so they can put malware in your computer. However, not all bugs are exploitable.

Vulnerabilities: Exploitable bugs are VULNERABILITIES - weaknesses in your system that can open your system up to being attacked and exploited. They need to be fixed!

Intrusion detection system: a system that monitors devices and keeps an eye out for malicious activity. If any suspicious activity is detected on any of the devices, it will notify someone who can respond appropriately.

Internet of Things (IoT): any device connected to the Internet that communicates data with other devices.

Smart homes are one of many examples of IoT.
Your smart home may include:

- air conditioning
- lights
- thermostats
- televisions
- doorbells
- security cameras
- stoves
- refrigerators

All of these smart home devices are connected to your phone and you can control all of them remotely. You can change the temperature on your thermostat, look out of your doorbell camera, turn the air conditioner on or off, and dim the lights ALL FROM YOUR PHONE. Isn't that so cool and convenient?!
BUT IoT devices can have bugs. Attackers can find these bugs, exploit the vulnerabilities, and gain unauthorized access to any of your IoT devices. For example, someone can spy on you through any of your house cameras, change the temperature in your house, make your lights turn on and off, and much more. Attacks like these are merely the tip of the iceberg of cyber attacks that unfold on a daily basis - attacks come in countless more forms and have humongous negative impacts on our lives. This is very real and pressing stuff that happens to thousands of people and businesses every day.

// ##

While technology brings profit, efficiency, and convenience to people, businesses, nations, and the world, it also subjects them to the dangers of digital attacks. These attacks have resulted in huge financial losses, the compromise of millions of people's personal information, and significant real-world consequences. It is CRITICAL to ensure there are proper security measures in place to prevent these attacks from happening. Cybersecurity is not just a choice; it's a necessity in our technology-driven modern world.