**Lesson 2: Cyber Threats**

A lesson on data breaches, its types and examples, and the consequences of cyberattacks.

In the introduction, we briefly talked about cyberthreats, including its relation to cybersecurity, current importance, and scale. In this article, we will cover cyberattacks more in depth, touching on topics such as its causes and consequences, how to recognize threats, and examples of attacks. Remember, learning about cyberthreats and increasing awareness about potential data breaches is necessary for ensuring user-based cybersecurity protection.

A **cyberattack** is the electronic theft of data; similarly, a **data breach** is an incident where data is taken without permission and occurs when an unauthorized program or individual accesses your network.

A screen with text on it

Description automatically generated

**Vulnerability Categories**

Most cyberattacks are caused by a vulnerability in a security system that is taken advantage of by cybercriminals looking to gain access of someone's data. The types of vulnerabilities include:

* **Technical**: A weakness in a computer and device system or network
* **Physical**: A weakness in the physical protections surrounding devices
* **Social**: The most notable weakness, these are human vulnerabilities that cause cyberattacks. An example of this is a phishing attack, which is a fraudulent message (designed to look legitimate) that tricks a user to expose sensitive information or deploys malicious software on the user's system. We'll discuss phishing further in a different article.

**Types of Breaches**

The following are common data breaches to look out for and learn how to recognize:

* **Ransomware attacks**: In this type of attack, a malicious actor encrypts their victim's files and steals their data until a ransom is paid. To recognize if your system has been infected by a ransomware attack, check to see if your files have been encrypted by looking for extensions like .micro, .encrypted, .locky, .aaa, .ttt, .xyz, .zzz, .crypt, or .vault. Also, keep your eyes open for any new, suspicious files that might contain a message from the attacker.
* **Malware attacks**: These attacks occur when malicious software and code (such as viruses, files, worms) infiltrates a user's system, allowing cybercriminals to gain access of or destroy data. Telltale signs that you might have malware on your system is if your device crashes or slows down, you have unexpected pop-up ads, you lose a mysterious amount of disk space, or your browser settings strangely change.
* **Companies** using our data in ways we don't approve of: Although this technically does not classify as a data breach, it still counts as a cyberthreat for us consumers. We will explore this topic in a future article, but for now, know that cyber risks include when businesses might use our data in an unauthorized manner.

A computer screen with a skull symbol

Description automatically generated

**Effects and Next Steps**

The consequences of cyberattacks can be severe for the victim whose data was stolen. In addition to sensitive, private data becoming compromised, data breaches can lead to identity theft. **Identity theft** is when a criminal uses a victim's personal information without permission to commit fraud and other crimes (making purchases, borrowing money, etc.). Victims of cyberattacks are forced to constantly monitor their accounts, enact credit freezes, change passwords/usernames/other account information, and other hassles that require time and energy.

But the practice of cybersecurity is all about handling and preventing cyber risks including cyberattacks and other threats. Moving forward, this curriculum will continue to teach you how to take steps to protect yourself and your data from breaches and malicious cybercriminals.