In this presentation, we're going to show you how to think like a cybercriminal. We're going to explain what they do before, during, and after stealing your data. Before we move forward, we must mention this disclaimer: the information we're about to give you is for educational purposes only.

We do not condone or encourage you to use this information for nefarious purposes, especially cyber attacks. We are also not responsible for any malicious actions you take as a result. With that out of the way, let's get into the presentation. So, let's get started.

## Before the Attack

Before an attack occurs, a cybercriminal will perform extensive research on their target. What they'll do here is gather as much information as possible regarding vulnerabilities, online presence, and security measures. This is also known as reconnaissance. During this period, an attacker will create a strategy to exploit weaknesses and maximize the effectiveness of their attack.

Once they identify these vulnerabilities, they will carefully plan the attack accordingly. The vulnerabilities they may be looking for include outdated systems, unpatched software, or human error such as social engineering, weak passwords, or poor security practices.

Once vulnerabilities are identified, they will start piecing the puzzle together and prepare to carry out the attack.

## During the Attack

During the attack, a cybercriminal will exploit the identified vulnerabilities. They will gain unauthorized access using methods such as malware, phishing emails, or other techniques. Once they successfully gain access to servers, networks, or other parts of a computer, they can install backdoors and other tools to ensure they can return to the target computer as much as they please.

Finally, they will begin the data extraction process from the infected computer system. They will copy sensitive files, intercept communication, and exfiltrate data to external servers. Their goal is to steal as much data as possible while remaining undetected.

## After the Attack

Once the attack is complete, they will work to cover their tracks and erase any evidence of their presence. This includes removing installed malware, deleting logs, and covering up their activities to avoid detection. After this, they will have the opportunity to monetize the stolen data.

Most of the time, they will sell it on the dark web and use it for identity theft or fraud. They may also demand ransom from the target in exchange for the safe return of personal data. After this, it's rinse and repeat for cybercriminals, who will carry out the process over and over again to as many victims as they like.

## Conclusion

We hope this presentation has given you an idea of how a cybercriminal behaves. Now that you have a behind-the-scenes look at how they work, it is important to take the necessary steps to protect yourself so you do not become a victim. This presentation is designed to help you become aware of what a cybercriminal can do to your data.

Please stay safe and always be on the lookout for any suspicious links or attachments, as they may be part of a cyber attack that a criminal hopes you fall victim to. Do not click on or download anything unless you have proper verification. Thank you for checking out this presentation. Have a wonderful day.