1. Mark your confusion.
2. Show evidence of a close reading.
3. Write a 1+ page reflection.

The Very First Thing Hackers Do as Criminals

Learn the steps they use every day

Source: Kurt Knutsson, FoxNews.com, September 4, 2023

Have you ever wondered what goes on in the mind of a cybercriminal? How do they plan and execute their attacks on unsuspecting victims? What are the tools and techniques they use to break into computers and networks and steal data?

Knowing these answers could help get you off a hacker's target list. Cybercrime is a serious and growing threat that affects millions of people and businesses around the globe – not to mention that cybercriminals are consistently finding new ways to attack us.

Just so you are aware of what you are up against, let me lay out the four steps that a cybercriminal will often take when plotting a cyberattack. Then, you'll become more powerful with some important tips on how to protect yourself from becoming their next target.

Cybercriminals' steps when plotting a cyberattack

These are the 4 steps that a cybercriminal will always take when plotting a cyberattack.

1. Finding their target

A cybercriminal has to find a specific person or organization to attack before they can do anything else. They use various ways to do this; however, they typically will aim for whoever seems to be the easiest and most vulnerable target. Here are some of the ways they can target an individual or business.

Social media: Cybercriminals can use social media platforms like Facebook, Instagram, Twitter, or Threads to find personal info, such as location, occupation, hobbies, interests, etc., that can help them tailor their attacks or scams.

The dark web: Cybercriminals can also use the dark web to buy or sell stolen data such as credit card numbers, passwords, usernames, etc., that can be used to access online accounts or commit identity theft.

Information brokers: Cyberswindlers use information brokers to obtain data that is collected from public sources, such as motor vehicle records, court reports and voter registration lists. This deeply intimate information can reveal personal details, such as your full name, address and phone number, that can be used to target or impersonate you.

Network scanning: Cybercrooks use network scanning tools to comb the internet for devices or systems that have vulnerabilities or weak security. They exploit these vulnerabilities to gain access or launch attacks.

This first step is perhaps the most important of a hacker's manipulation game, because it makes or breaks a hacker's game. You see, without a target, there's no crime to commit.

2. Researching their target

After finding a potential target, a cybercriminal will likely do some research to gather as much information as possible in order to steal your credentials. They'll tap into various tools and techniques to do this, such as:

Reconnaissance tools: They can deploy reconnaissance tools to scan the target's network and discover their IP address, open ports, operating system, services, etc. This can help them identify any vulnerabilities to exploit later.

Social engineering: This is used to trick the target into revealing sensitive info, such as passwords, security questions, or personal details. They do this by impersonating something or someone the target trusts, such as a friend, a colleague or a customer service rep from a familiar organization. These tools include phishing emails or phone calls to lure the target into clicking on malicious links or attachments or downloading dangerous malware.

Keyloggers: This popular sneaky technique is used by cybercriminals to secretly record the keystrokes of the target and capture login credentials, messages and emails. They often install keyloggers on the target's device by using malware or physical access to continue spying for extended periods of time scooping up account numbers, credit cards and any valuable data.

By researching their target, a cybercriminal can gain a better understanding of their habits, preferences and vulnerabilities. This can help them plan and execute a more effective and customized attack.

3. Breaking into the network

This is when the hacker really begins to be creative. The most widely deployed way that a hacker will break into a network is with phishing.

Phishing emails & websites

This could be a phishing email scam with malicious links attached or even a phishing website that is designed to look like a legit company so that the victim falls for it and hands over their information.

This is one of the most popular attacks now that hackers are using phishing-as-a-service tools that basically do all the dirty work for them. By giving these hackers a bulletproof template that could trick anyone, they just have to sit back and allow the victim to fall for the trick.

Other clever tools a hacker might use include a creepy way of displaying a digitized human hair follicle on a victim's phone or tablet screen so that when they go to brush it away, malware is downloaded immediately.

Hackers might use fake ads and post them on social media sites like Facebook, hoping that the victim will fall for them. Instead of it going to a real company, it leads you and me straight into the grasp of criminals. The possibilities are truly endless for a good hacker.

4. Taking control of the network

This is the final stage of the hacker's attack and the most rewarding one for them. After gaining access to a system, they exfiltrate any valuable information they can grab as quickly as possible with the help of post-exploitation tools, such as AdFind and Cobalt Strike, which are designed to collect and transfer data from compromised networks. They will either disappear with the stolen data or use it to extort money from their victims, depending on the target and the motive of the attack.

What can I do to protect myself from these hackers?

Invest in removal services. A hacker cannot easily use you as a target if they cannot find your information on the internet. Data broker sites run by scammers get fed with the personal data a hacker steals from you including email addresses, Social Security numbers and more. They do this so that they can sell the information to third parties and make a profit.

While no service promises to remove all your data from the internet, subscribing to a good removal service is the most effective way to constantly monitor and automate the process of deleting your information from hundreds of sites continuously.

Have good antivirus software. Having strong antivirus software installed can help keep hackers out of your phone, tablet and computer. This will also prevent you from clicking malicious links intending to install malware, allowing hackers to gain access to your personal information.

Use identity theft protection. Identity theft companies can monitor personal information like your home title, Social Security number, phone number and email address and alert you when they are being sold on the dark web or being used to open an account in your name. They can also assist you in freezing your bank and credit card accounts to prevent further unauthorized use by criminals.

The great part of some identity theft companies is that they often include identity theft insurance of up to $1 million to cover losses and legal fees and a white glove fraud resolution team, when a U.S.-based case manager helps you recover any losses.

Key takeaways

Cybercriminals typically follow a four-step process when plotting a cyberattack, which includes finding a target, researching their target, breaking into the network and taking control. To protect yourself, I strongly suggest you erase personal information from the internet, have good antivirus software and use identity theft protection services.

Possible Response Questions

- What are your thoughts about protecting yourself from hackers ? Explain.
- Did something in the article surprise you? Discuss.
- Pick a word/line/passage from the article and respond to it.
- Discuss a "move" made by the writer in this piece that you think is good/interesting. Explain.