August 2023

SecurityAwarenessNews

the security awareness newsletter for security aware people

Unmasking Cybercriminals

The Truth About Hackers

Spear Phishing: The Advanced Threat

Five Common Ways People Get Hacked

The Truth About Hackers

The people who commit cybercrime are often referred to as hackers or cybercriminals. To get a true sense of who those people are, it's important to first dispel a few myths about the concept of "hackers" and focus on four important facts.

Fact #1: Not all hackers are criminals.

A hacker is commonly defined as someone who uses advanced computing or networking skills to overcome technical obstacles. The term is often associated with cybercrime, but not all hackers are criminals. Penetration testers, for example, are hackers that organizations hire to attack their networks and identify security vulnerabilities before actual criminals find them.

Key takeaway: While there are plenty of criminal hackers in the world, there are also plenty of good hackers who leverage their skills to protect people and data.

Fact #2: Social engineering is the most common hacking method.

Social engineers are con artists who use deception to mislead people into doing something they shouldn't, like divulging login credentials. The main concept behind these attacks is they hack humans, not devices or technology. The attacks, therefore, are not advanced or technical in nature, which is partially why they're so common.

Key takeaway: The concept of hacking might be closely associated with technology, but most security incidents happen due to people falling for non-technical scams via social engineering.

Fact #3: Anyone can be a criminal hacker.

Possessing highly advanced hacking skills isn't always necessary to commit cybercrime, like infecting computers with malware (malicious software). Instead, someone could subscribe to a malware service. The service providers develop the malware and rent it out to people with instructions on deploying it, including on-demand tech support.

Key takeaway: Cybercrime continues to grow because it doesn't require advanced hacking knowledge. Someone can instead purchase a "hacking subscription" and use it to launch attacks.

Fact #4: Anyone can be a human firewall.

Hackers (the good kind) are constantly building new tools designed to keep organizations and people safe. Unfortunately, no security tool can be perfect. That's why the world needs human firewalls — people who represent the last line of defense. You become a human firewall by staying alert, remaining skeptical, and always following policies.

Key takeaway: New technologies will continue to emerge that allow criminals to bypass security controls. You can help fight cybercrime by becoming a human firewall both at work and at home.

Spear Phishing: The Advanced Threat

Phishing is a common scam that attackers use to steal data, spread malware, and defraud people of money. Most attacks involve a generic message sent to several people, often due to a database of contact information getting leaked online.

Spear phishing, however, is anything but generic. This dangerous attack targets specific people or organizations, often with custom-made emails or messages designed to avoid suspicion. Here's an example of how it works:

Gather Intelligence

Attackers may spend weeks or months researching an organization and gathering as much information as possible. During this initial stage, the goal is to gain access to employee directories, corporate email addresses and phone numbers, and any data that will help the scammer seem legitimate.

Identify Targets

With enough information the attacker identifies the employees of significant interest — those with authority to wire money or have high-level access to confidential information. Examples include human resources, executives, accounting, and IT personnel.

Gain Trust

Most spear phishing scams involve impersonation. The attacker will pose as someone the target knows, such as a co-worker or a legitimate business. The idea here is simple. When the target believes they are communicating with a trustworthy source, they are more likely to fall for the scam.

Steal Money or Data

Many of these attacks are financially motivated. For example, the attacker might pose as an executive and ask that executive's employees to wire money to a new account. Since the email comes from an authority figure, the target might not think twice about honoring the request. Impersonation is also how cybercriminals gain access to highly confidential information.

This is just one illustration of the many ways cybercriminals use spear phishing. Even if you're not in a position to, as an example, wire money, it's still vital to understand how these attacks work. Never assume someone is who they say they are, think before you click, and report anything suspicious immediately.

Five Common Ways People Get Hacked

While the intentions of cybercriminals vary, their approach to hacking people tends to follow a few general techniques. Let's review five of the most common ways people are targeted and how you can protect yourself and your organization.

Outdated Devices or Software

Failure to run updates equals failure to patch critical security vulnerabilities. Cybercriminals can use those vulnerabilities to steal valuable information or infect devices with malware. In your personal life, it's best to enable automatic updates whenever available so you never miss an important security patch. At work, follow policy for how and when to install updates.

Phishing Scams

Since phishing scams are the top way people get hacked, they should be your top priority in terms of security awareness. You can spot most attacks by looking for common warning signs. These include suspicious links or unexpected attachments in messages, random requests for confidential information, and threatening or urgent language. Think before you click!

Weak Passwords

Cybercriminals often use password-hacking software that can easily crack weak passwords in minutes, sometimes even seconds. This is how they get access to online accounts, which allows them to steal data or money or leverage social media profiles for malicious purposes. Don't let it happen to you. Ensure every password is several characters long and unique to each account.

Malicious Phone Apps

Popular app stores have implemented rigorous processes to identify and eliminate malicious applications. Unfortunately, it's still common for malicious apps to find their way to the public. Before installing anything, always do some research. Take a few minutes to review how many downloads an app has and ensure the developer is trustworthy. For work-issued devices, never install any software without explicit permission.

Social Engineering

Not every attack involves sophisticated, technological processes or software. Sometimes, the easiest way to hack someone is by simply misleading them. That's the main idea behind social engineering — the use of deception and psychological manipulation. Avoid this by staying alert, never assuming someone is who they claim to be, and treating any request for money or confidential information with skepticism.

Remember, people (like you) are the last line of defense. Be sure to report suspicious activity immediately, and always follow organizational policies.