February 2023

# SecurityAwarenessNews

the security awareness newsletter for security aware people

## *Understanding the Insider Threat*

Navigating the Threat Landscape

Types of Insider Threats

Becoming an Insider Asset

# Navigating the Threat Landscape

Information security presents an ongoing challenge for every organization in every industry. Meeting that challenge requires sound strategies and processes to help navigate the sprawling landscape of threats that put data, systems, and people at risk.

As you might expect, most security efforts primarily focus on external threats — those that come from outside the organization. Here are just a few examples:

- ***Social Engineers:*** scammers who use psychological manipulation to mislead people
- ***Phishing Attacks:*** emails that contain malicious links or attachments
- ***Smishing Attacks:*** text messages that urge the recipient to click on a link
- ***Distributed Denial-of-Service:*** cyberattacks that can knock services and websites offline
- ***Advanced Persistent Threats:*** highly coordinated groups of cybercriminals who infiltrate networks and can go undetected for months or even years

Unfortunately, an organization's concerns aren't limited to external threats. There's also the insider threat — anyone who knowingly or unknowingly exposes sensitive data, or otherwise undermines security and privacy efforts. Insiders can include employees, contractors, business associates, third-party vendors, and others. You might be an insider if you:

- ***Have been given a badge or key to access secured areas***
- ***Use work-issued devices and accounts***
- ***Develop and manage products or services***
- ***Have inside information about your organization's core strategies***
- ***Have been granted access to confidential data***

There's a good chance that you, like most members of an organization, fit these criteria. As such, it's vital to understand a fundamental concept of security: Mitigating threats goes well beyond avoiding common attacks like phishing. It also involves every member of an organization treating the access they're granted with the utmost respect.

Whether it be highly confidential information, work-related online accounts, or physical clearance to secured areas, the very nature of having access makes someone a threat to it. That's the reality of the modern threat landscape.

# Types of Insider Threats

*Insider threats generally fit into three categories:*

- **Malicious:** *someone who intentionally harms an organization*
- **Negligent:** *someone whose carelessness harms an organization*
- **Accidental:** *someone whose mistake harms an organization*

**Gaining an understanding of the different types of threats offers an opportunity to learn more about your role in protecting information.**

## The Malicious Insider

Malicious insiders are often disgruntled individuals or those that seek to profit by stealing from their organizations. For example, trade secrets (like a recipe or blueprint) carry a massive amount of value. Divulging those secrets to competitors could irreparably destroy an organization's competitive edge. Personal gain aside, some malicious insiders simply want to cause great harm by destroying or intentionally leaking confidential data.

## The Negligent Insider

Insider threats don't always have malicious intentions. Imagine, for example, an employee breaking policy by downloading confidential data to a personal computer, or leaving a work-issued device in an unsecured area where a thief could easily steal it. Even if that person had no intention of causing harm, their lapse in judgment and disregard for policy creates just as much risk as malicious insider threats.

## The Accidental Insider

We're all human. We all make mistakes. Unfortunately, sometimes those mistakes yield major consequences. Accidentally emailing sensitive information to the wrong party, misconfiguring server settings that leave a door open for cybercriminals, and misplacing sensitive documents that contain confidential data are just a few examples of how small mistakes could cause huge problems. In fact, human error is one of the leading causes of security incidents.

**So what does this mean for you and your role? First, it's important to recognize that the entire concept of insider threats comes down to access: Attackers want it; insiders have it and must protect it. Most people wouldn't intentionally abuse that access for malicious purposes, but mistakes can and do happen.**

**For that matter, the goal of many external threats is to steal your access. They want you to make mistakes, like clicking on a phishing link or plugging in a random USB flash drive. Both actions could infect systems with malware.**

**Thus, it's everyone's duty to stay alert, know and follow policies, and take every precaution to separate the "insider" from the "threat."**

# Becoming an Insider Asset

The challenge of mitigating threats requires a nuanced combination of people and technology. In theory, modern security technologies can help lower the chances of a phishing email finding your inbox, for example. In reality, even the latest and greatest versions of software or hardware are only as effective as the people that use them.

That's why it's vital every member of an organization learns how to become an insider asset — the final and most valuable link in the security chain. Here's how:

## *Always follow policy.*

Everything starts with following an organization's policies, which were designed to keep cybercriminals from gaining unauthorized access while also giving employees specific guidelines for protecting information. Failure to follow policy, intentionally or unintentionally, undermines security efforts and could lead to major consequences like data breaches.

## *Learn to identify social engineering attacks.*

Social engineers use psychological manipulation to convince their victims to click on a malicious link or divulge confidential information. Learn how to spot phishing emails and other attacks carried out by these scammers. Never assume someone is who they claim to be, and treat requests for sensitive information with skepticism.

## *Report security incidents immediately.*

A phishing attack, a secured door left open, an unfamiliar person in a secured area — anything and everything that seems suspicious must be reported immediately. The sooner you report it, the better the chances of mitigating damage and preventing future events. If you see something or hear something, please say something!

## *Understand the risks.*

Think about data protection from a personal perspective. What would happen if your sensitive information, such as your home address, banking information, national ID number, etc., ended up in the wrong hands? No one wants that to happen to them. Consider the ramifications of intentionally, accidentally, or carelessly mishandling data.

## *Respect privileged access.*

Privileged access refers to both the physical and digital clearance provided to members of an organization. Respecting access refers to the process of ensuring your access is not obtained by unauthorized parties for any reason. That includes never sharing login credentials, keys, or badges; utilizing strong, unique passwords for every account; and always locking systems when not in use.