Hack the Human: End-user Training and Tips to Combat Social Engineering

We like to think we can trust our co-workers to do the right thing. Unfortunately, this is not always the case. Some people become insider threats; that is, they use their authorized access to systems to harm their organization. For example, someone may sell information from a database to a third party.

There are three types of insider threats:

1. **Unintentional** – This person does not intend to cause a threat, but they do so through carelessness. They may misplace their laptop or flash drive, fail to update software, or ignore instructions when setting up software or cloud storage. Their attention to detail may be poor and they can make mistakes that damage the organization, such as causing a breach by emailing data to the wrong person.
2. **Intentional** – This person intends to harm their organization and is often called a “malicious insider”. They may be in it for financial gain, to get revenge for some perceived slight, or for some other motivation. They may leak information to third parties for money or political beliefs, steal information to advance a side business, or destroy data to sabotage the organization.
3. **Collusive or Third-party** – *Collusive threats* occur when an insider collaborates with an outsider to compromise an organization. The outsider may recruit an insider to obtain information to commit fraud, intellectual property theft, espionage, or some other crime. Some insiders may be manipulated into becoming a threat and may not recognize that what they are doing is harmful. *Third-party threats* occur when the insider works for a contractor or vendor who has access to the organization’s network or facilities.

Some of the indicators of an intentional insider threat include:

- Life changes, such as financial, relationship, family, or work problems.
- Behavioral changes, such as signs of depression, anger, or possible drug or alcohol addiction. However, a colleague who seeks help is showing good judgment.
- Changes in work habits such as working through lunch, accessing or asking questions about information or systems not part of the scope of the colleague’s employment, or a disregard for security policies and practices.

Many unintentional insiders are:

- Poorly trained in cyber hygiene, either because the organization does not train staff or because they do not pay attention.
- Disorganized; loses laptops or flash drives.
- Unfamiliar with technology or thinks they know more than they do and do not follow instructions when installing new software or setting up cloud storage.

We all make mistakes, but many unintentional insiders simply do not pay attention to what they are doing. The lack of attention to detail puts their organization at risk for breaches and malware.

To reduce the likelihood of an insider threat, organizations should develop a comprehensive program that includes knowing the people within the organization, identifying the assets and prioritizing the risks, and establishing the proven operational approach of detect and identify – assess – manage. Organizations should take extra steps to vet third party service providers to ensure they can access only necessary systems and areas of the building.

The Cybersecurity and Infrastructure Security Agency (CISA) has more information about insider threat mitigation at https://www.cisa.gov/insider-threat-mitigation.

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.