CYBER SECURITY Newsletter

PHYSICAL SECURITY

Problem

So far, most of the risks we have discussed are cyber-based attacks which are committed by cyber criminals around the world. These attacks have become very simple for them to automatically probe and attack millions of computers every hour, every day. We also cannot forget the physical world. Frequently, it is simpler for criminals to physically steal information that is not secured. In addition, while physical attacks against our data are less common, when they do happen they can have far greater impact.

Solution

Physical security is often one of the most challenging risks to an organization because there are many people coming to and leaving our facilities, including those who are not employees. To help protect our organization against physical threats, we need your help with the following:

1. Correctly disposing our confidential information

One of the simplest ways for a criminal to locate confidential information is to find it in our garbage. Often, people do not think about information they dispose of. These items can be sensitive documents, photographs, legal and accounting documents, trade secrets, and proprietary information. Assuming these materials are safety disposed of once thrown out is a serious misconception.

During the various steps of the trash removal process, a criminal can find and recover your confidential information. In fact, this attack has become so common there is even a term used to describe it - ***dumpster diving***. This is when the criminal (often at night or pretending to be a janitor) will search through an organization's garbage looking for any sensitive documents or information. To protect yourself and our organization, ensure all confidential information you disposed of is shredded or physically destroyed.

Physical Security

Cyber attacks are the most common attack against your data and our organization. However, we must remember criminals also exist in the real world. While not as common, physical attacks against our information can have far greater impact.

Idaho State University

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

The Repairman

In previous training, we discussed Social Engineering. This is when cyber criminals use tricks to fool you, such as convincing you to provide your password or infect your computer for them. These types of attacks have existed before the age of the Internet; cyber criminals are now applying them to the Internet.

One of the simplest ways for a criminal to gain access in the physical world is to pretend to be something or someone you trust. For example, criminals can enter our building pretending to be someone we trust, such as a telephone or copier repairman. These are people we regularly expect to see and can even be fooled into helping them by opening a door or answering questions they may have.

Everyone in our building should have an identification badge identifying who they are (employee, visitor, or repairman). If they do not have am identification badge, please escort them to the front desk or security.

2. Identification Badges

A possible attack to our organization is a criminal pretending to be an employee, walking into our building, and stealing what they find. This is why we require everyone inside our building to wear identification badges designating their employment status (employee, contractor, or visitor). One additional way to protect ourselves is to always stop and ask individuals without an identification badge to identify who they are and kindly escort them to the front desk so they can register with security.

3. Doors and Access Ways

If you open a door that requires badge access, utilizes locks, or leads outdoors, always close the door behind you. This helps to ensure criminals cannot access our building due to someone else's mistake. In addition, when you enter a room that requires an access card, be sure anyone else entering also uses their access card. A common attack for criminals is to follow you, pretending to be another employee. This attack is so common it also has its own name: ***drafting***.

4. Have a clean desk

Unfortunately, our security team is unable to catch all threats; sometimes criminals bypass security and gain access to our building. At times, we may have unethical contractors or employees in our building looking for unauthorized articles. To protect against these types of attacks, lock any sensitive information or valuable items when you leave your desk and do not leave passwords in an unsecured area. If you have any passwords written down, they must be secured in a locked cabinet.

If you are leaving your computer, make sure the screen is locked and password-protected. Once again, this ensures all authorized and unauthorized individuals cannot access your computer.

5. Your Laptop

Unfortunately, criminals do not have to break into to our building to steal our information; sometimes they can access our information via stolen laptops. When traveling with a company provided laptop, always have it secured -- especially in very public places such as hotel lobbies, restaurants or airports. If you must leave your laptop, make sure it is secured. For example, always lock your laptop in the trunk of your car. Never leave your laptop visible where criminals can easily see it and be persuaded to steal it.