CYBER SECURITY newsletter

PHYSICAL SECURITY

Problem

To date, most of the risks we have discussed are cyber-based attacks. These types of attacks are committed by cyber criminals around the world. It has become very easy for them to automatically probe and attack millions of computers every hour, every day. However, we cannot forget the physical world. In some ways it is simpler for criminals to physically steal the information they need as we often forget to secure such information. 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. This is because for an organization like ours to operate there are many different people coming into and leaving our facilities, including people who are not employees. To help protect our organization against physical threats we need your help with the following.

1. Disposing of Confidential Information: One of the simplest ways for a criminal to find confidential information is to simply look for it in our garbage. Often people do not think about the information they throw out, such as sensitive documents, printouts, or photographs. They simply assume that once something is thrown in the garbage, it is safely disposed of. Unfortunately that is not the case.

Once you throw something out it goes through a long process. During each step of that process a criminal can find and recover your confidential information. In fact, this attack has become so common that there is even a term for 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 both yourself and our organization ensure that any confidential information you dispose of, such as printed documents, is shredded or physically destroyed.

Physical Security

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

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

The Repairman

In previous training we discussed Social Engineering. This is when cyber criminals use tricks to fool you, such as convincing you to give them your password or infect your computer for them. However these types of attacks have existed for thousands of years in the physical world; cyber criminals are simply applying them to the Internet.

Just like in the cyber world, 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, let's say a criminal wanted to break into our building and steal our information. One of the simplest ways to do this would not be break into the building at night but simply walk into it during the day. They can do this by pretending to be someone we trust, such as a repairman for the telephones or copier machines. These are people we expect to see and therefore trust. In fact, we may even be fooled into helping them, such as opening the door for them or answering any questions they ask.

Every person in the building should have a badge identifying them as an employee or a visitor, including repairmen. If they do not have a company badge, please be so kind as to 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, then simply walking into our building and stealing whatever they want. This is why we require anyone inside our building to wear a badge identifying themselves, regardless if they are an employee, contractor, or visitor. One of the simplest ways to protect ourselves is to always stop and ask individuals without a badge to identify themselves. If they do not have a badge, kindly escort them to the front desk so they can register with security.

3. Doors and Access Ways: If you open a door be sure to close the door behind you. This is especially true for doors that have locks, require badge access, or doors that lead outdoors. This ensures criminals cannot get in the building by a door left open by someone else. In addition, when you go through a door that requires an access card make sure anyone else that goes through that same door uses their access card also. A common attack for criminals is to simply follow you through the door behind you, pretending to be another employee. This attack is so common it is termed '*drafting*'.

4. Clean Desk: Unfortunately, our security team is unable to catch all threats, sometimes criminals bypass security and gain access to our building. In addition, at times we may have unethical contractors or employees that are looking for things they do not have authorization for.

To protect against these types of attacks, be sure to lock up any sensitive information or valuable items when you leave your desk. In addition, do not leave any passwords in an unsecured area. If you have any passwords written down, they must be secured in a locked cabinet.

Finally, if you are leaving your computer and it is left on, make sure the screen is locked and password-protected. Once again, this ensures that if anyone has gained unauthorized access to the building they cannot access your computer.

5. Your Laptop: Unfortunately, criminals do not have to break into to our buildings in order to steal our information; sometimes our information goes to them. One of the most common ways we have our computers and information stolen is when you leave the office with your laptop. When traveling with a company laptop make sure you always have it secured with you, especially in very public places such as in hotel lobbies, restaurants, or airports. In addition, whenever you leave your laptop make sure it is secured. For example, if you leave your laptop in your car, lock it in the trunk; do not visibly leave it on the car seat where criminals can easily see and then steal it.