October 2007

Physical Security Tips

Secure it, protect it...It’s all about the data

When thinking of physical security, most people think of security guards, cameras, and locked doors. Many of us fail to realize our responsibility to keep information safe from physical attackers. Let’s review a few physical information security scenarios common to most of us.

Are you the only person with access to your office?

I highly doubt that you are the only one. I’m sure that you have visitors or hold meetings in your office area. Also, custodial and maintenance staff have keys to many offices in order to perform their job duties. Remember it’s your responsibility to keep the data secure!

Do you have any documents with sensitive data in plain view?

I know that you need to be able to see the documents to work with them, so of course they are in plain view at some point. However, when someone comes in your office or when you are absent, these documents need to be securely stored away to prevent theft or copy. With miniature cameras like those in cell phones widely and easily available, it is simple for anyone to photo documents without being noticed... even when you are standing right there!

When you print documents, do you pick them up immediately, or do they sit on an office printer for some time? How about fax documents? The fax machine should be located in a physically secure area with sensitive data accessible only to authorized personnel. These are other areas where caution needs to be taken.

When you dispose of documents with sensitive information, a shredder or Shred-it bin must always be used. People may legally dig through trash (called “dumpster diving”), and take whatever they find. Many people even treat this as a hobby and rummage regularly.

Do you have any removable media (floppy disks, CDs, Flash drives, etc) with sensitive information?

How often have you misplaced a CD or a flash drive? If you placed one on your desk before leaving work, would you notice that it is missing the next day or would it take some time? Removable media is very compact, which is convenient for both you and any thieves so be sure to store them securely and encrypt any sensitive data on them.

Before disposing of removable media, be sure to either physically destroy it, overwrite the data using a software utility such as killdisk or dispose of it in the Shred-it bin to prevent unauthorized access to the data. Just deleting the contents is not enough. Recovering deleted files is a time-consuming task, but is fairly easy to do with the assortment of tools that are widely available on the market today.
**Do you use a laptop, PDA, etc?**

The same safety measures for removable media apply to portable devices as well. These devices can hold even larger amounts of data, so physically protecting the device and encrypting sensitive information is critical.

**Do you either lock your screen or log out of your computer every time you leave your office?**

An attacker only needs a minute or so to send themselves documents, send someone threats, etc. Your account is the one being used, so you would be investigated should an incident occur. Locking your screen only takes a second, and unlocking it only requires that you type your password. It’s a simple habit to learn that protects both you and the information.

To lock your screen in Windows, you press and hold the Windows key and press the L key. The Windows key is located in between the Ctrl and Alt keys on the lower left side of your keyboard.

**Is your password written down anywhere? Is it a strong password?**

I’m sure you’ve heard it before, but I have to say it again, do NOT write your password down anywhere. If your password is written down, someone else probably knows it already. The most common “hiding places” are under your keyboard or in a desk drawer. If it is stuck to the front of your monitor, it isn’t even hidden!! YES, even though it’s hard to believe, we still find this occurring in our environment. Also, use strong passwords. If your password isn’t strong (e.g. ‘password’, your dog’s name, your birthday), someone may know it or be able to guess it. If someone else has your password, they have the “keys to the kingdom” which defeats all of the other security measures you have in place.

**Secure it, protect it…It’s all about the data**

Be aware that you are responsible for protecting sensitive information. Unauthorized use or release of sensitive information may subject the violator to personal, civil, and/or criminal liability and legal penalties. Violations may constitute grounds for corrective action up to and including termination of employment or student status, loss of UNC Health Care and UNC School of Medicine privileges or contractual or affiliation rights in accordance with applicable UNC Health Care procedures.