Cyber Security at Work

Five Basic Steps to Secure Computing at Work

1) Always Lock Your Computer:

When you step out of your work area, if only for a minute, lock your computer. If you lock your computer, you can ensure that no one has accessed your email and other work files while you were away.

2) Do Not Share Your Passwords:

Never give your password out to anyone, including your IT staff. Your IT staff should not need your password to assist you. If you give your password out, you are giving someone complete access to your account. Depending on the account type, they will have access to your email, work files, and other personal data. In addition, do not write down your passwords and place them on or around your workspace. If you must write down your passwords, keep them in a secure location.

3) Encrypt Sensitive Information:

If you have information that needs to be protected, encrypt it. Applications that "zip" files usually offer the option of adding a password. If you use a laptop, external hard drive, or USB flash drive, make sure that encryption is being used. Lastly, if you need to send sensitive information, ensure that the transmission is encrypted. Many email programs and FTP applications offer methods of encrypting the information as it is being transferred.

4) Use Caution When Sending Sensitive Information:

Before you send sensitive information to someone, make sure that you understand the risks involved. Ensure that the recipient is a trusted individual and that you have encrypted the sensitive information prior to sending it.

5) Make Frequent Backups of Important Files:

At work, you are more than likely have access to a networked drive containing a folder just for your files. Use this drive for all of your files so that in the event your desktop computer fails, your files will be safe and sound.