Seven Tips for Work IT Security

Research shows that over 50% of security breaches are a result of end-user error, oversight and ignorance; so training your employees to follow processes and protocol is the place to start.

1.) Working with the IT Department: Install all of the patches and updates that your IT department asks you to do. There are continually updates that need to be installed for Windows and Office programs as well as security software to protect your individual computer. In addition, if you have a remote session through your server you want to make sure that your home computer has a firewall or security installed to protect you in remote locations. Making these regular updates will keep your computer and your company's network as secure as possible.

2.) Don't Use the Save Password Option: It's easy to hit "Remember Me on This Computer" but you should make it mandatory to enter your password on all operating systems or application settings. This will protect your computer from someone else easily accessing your data. And, remember to use a variety of passwords on all of your logins. It's easy to use the same one, but that makes it easy for anyone to figure out how to access your information; whether personal or data from the organization.

3.) Never Open Questionable Emails: Hackers and virus perpetrators have become very sophisticated at tricking people into opening innocent or official looking emails. If anything looks fishy at all, don't open it. Send it to your IT department so they can check it out and then alert everyone in the company about the potential danger. And never open anything that looks suspect regarding financial information. You should never be asked for your Social Security number from any source.

4.) Install only Licensed Software: Your company should have a license for all software installed on your computer. Unlicensed software can create legal problems so don't install software that's been given to you by someone other than your IT department. Additionally, software that's been purchased for home use may not be compatible with what's on your work computer and may cause problems down the line with upgrades and other applications.

5.) Don't Rely on Your Expertise: Many times employees try to fix things themselves and end up creating bigger problems for their computer as well as the network. It's best to ask your IT department immediately rather than hoping something will clear up on its own. Typically things will just get worse, especially if you have a virus on your desktop from that email you weren't supposed to open!

6.) Don't Download Programs from Sites You Don't Know: Downloading programs from sites you don't know may jeopardize the entire network. It may seem innocent enough to download a harmless app or program, but you should remember that your work computer is not your personal device and should only be used for work related activities.

7.) When in Doubt, Ask: Things are happening so fast in the IT world that you may not have the most current information about a program. Ask your IT Department whenever things may seem questionable. It's better to give IT the opportunity to research and evaluate an option then to risk taking your entire network down.

Change your passwords on a regular basis to ensure security for your company and your personal identity.

Disclaimer