Computer Security Tips and Information

Strong passwords

This is something everyone hears all too often so you may be desensitized to it or think it doesn't apply to you. It is important to have strong passwords that can't be easily guessed. If a password can be easily guessed, it wouldn't take much for an user to gain access to your email, files, and other sensitive information. Try using a password that is a sentence that you'll remember (example: ThisPasswordIsStrong!). It is also good practice to have different passwords for different accounts and websites. If someone can guess a password to one site, chances are they'll try to use it for other sites as well. If you'd like to see how long it would take to guess your password, try checking for yourself: https://howsecureismypassword.net/

Do NOT share your password with others

I repeat, do NOT share your login information with others. Nor should you login with your account into a computer for someone else to use. Also you should not write your passwords down on sticky notes and leave them at your desk. If you must write them down, keep them with you at all times. You may think it is easier than calling the tech office to get the issue resolved even if the person just needs to get on a computer to print something quick. Giving out your login information means that person will have access to your email, files, campus and any other account that shares that username/password. They can send emails out or browse to unsafe websites and it will only be traced back to your name. Everyone should have their own network accounts. If they do not have a network account, it takes the tech office 5-10 minutes to create an account. Please contact the tech office.

Do NOT open email attachments from unknown sources

If you see an email with an attachment that you are not sure where it came from, do NOT open it. Scammers and hackers have become efficient at tricking users into opening email attachments that contain malware, ransomware, and other dangerous code that can be executed on your computer when the file is opened. The email may masquerade as a fake invoice for something they claim you ordered, or contain a link claiming to reset your password due to an update or some other reason. The tech office will never ask you to reset your password nor ask for your password information over email. If it seems suspicious, chances are it isn't trustworthy and should be deleted. Always feel free to call and ask the tech department if you're unsure of an email and we can help determine if it is legitimate or not.

Lock your computer when you are away

It is good practice to lock your computer when you step away from it. Think of it as locking your car door when you leave it parked and walk away. You would not want someone to have access to the things in your car, let alone the information on your computer. If you leave your computer unlocked and step away, all it takes is a couple minutes for someone to walk over and send an email, go to a bad site, view sensitive information, change grades, or steal your files. Locking your computer is a simple process and can be performed in one simple step: **Windows Key and L Key** pressed at the same time will lock your computer.