

Tips on Notebook and Wireless Security

- Always keep track of your notebook computer. If possible, try keeping it in sight at all times or locking it up.
- Encrypt your data. This way even if your computer is lost or stolen, encrypted data cannot be accessed.
 - Resources:*
 - Windows Encryption Tools
 - Pretty Good Privacy Website (www.pgp.com)
- Backup your data. Many things can cause the loss of data, it is much easier to go out of your way slightly right now than to lose all of your necessary data (family pictures, important documents, emails, etc.) and not have it elsewhere.
 - Suggestions to Backup Data:*
 - Use your MP3 player to store some of your data. Many music players have enough space to backup information from your computer as well as hold songs.
 - A USB flash drive usually holds a similar amount of data as the average MP3 player and is smaller/more convenient to transport.
 - Internet Email will often provide an external server to store your data, which is accessible anywhere there is an internet connection.
 - Purchase an external hard drive. If you have a lot of files you need to backup an external hard drive may be a good choice. Some hold as much as 300 Gigabyte (twice as large as the average hard drive of a notebook).
- Label your computer by physically engraving your name in it.
- Purchasing a tracking program will also aid in the retrieval of a lost or stolen computer by essentially “calling home” when accessing the internet. Tracing programs include zTrace (www.ztrace.com), CyberAngel (www.sentryinc.com) and ComputracePlus (www.computrace.com).
- You can also set your computer to ask for a password at start up, however, be sure to remember what it is as this is an important password.
- When purchasing your notebook computer you may also want to purchase insurance along with it. This may seem like just an added cost at the time, but it will be worth it if your computer is ever stolen.
- Set up a firewall on your computer to better protect it when accessing a WiFi network in public places such as a coffee shop, airport, or hotel.
- When using a public WiFi hot spot, be sure to check with the privacy policy found at the network’s web site, if they don’t have one, you want to rethink connecting.
- While connected to a public WiFi, be extra cautious when using passwords and/or credit card numbers, as hackers are sometimes able to view this information.
- When you are not on the internet, be sure to turn off the wireless function, ensuring that no malicious hackers are able to access your computer.

Sources:

<http://www.microsoft.com/athome/security/privacy/wirelessnetwork.mspx>

http://www.microsoft.com/smallbusiness/resources/technology/security/how_to_protect_your_laptop_from_thieves.mspx