Safety Tips for Wi-Fi Hotspots

Public Internet access portals provide many benefits such as flexibility in work locations and improved productivity, but there are also serious security risks. Here are some security tips to keep in mind when using them:

DO

Connect with caution – Before you connect, confirm the network name. Internet cafes, in particular, are favorite sites, where hackers routinely set up networks with names such as "Free Wi-Fi Hotspot". Avoid using public computers and public Wi-Fi connections to log into accounts or to access confidential or sensitive information.

Be aware - Take note of the types of information you might transmit over an unsecured network and assume that what you transmit will be read by a third party. Save logging into email, bank and credit card accounts, and making online purchases for times when you are on a known, secure network. Ensure any websites requesting the insertion of account credentials and those used to conduct transactions online are encrypted with a valid digital certificate to ensure your data is secure. These website addresses will have a green padlock displayed in the URL field and will begin with https.

Secure your folders – Computers have public folders, typically shared music, pictures and video locations, that are easily available to anyone on the same network. Don't keep anything personal in these folders. If another individual can access the same public computer you are using, do not log into your accounts or make online transactions. Public computers may contain malicious software that can make it easy for criminals to steal your confidential information. In addition, criminals can potentially recover information that was previously deleted from the computer. Try to keep all public computer activity as anonymous and general as possible.

Delete previous network searches – Your computer maintains a record of every network it connects to. Unfortunately, hackers can create networks with similar names that fool your computer into signing onto an unfriendly site. Ensure any websites requesting the insertion of account credentials and those used to conduct transactions online are encrypted with a valid digital certificate to ensure your data is secure. These website addresses will have a green padlock displayed in the URL field and will begin with https.

DON'T

Disable your firewall – Microsoft Windows has a built-in personal firewall and you can also install a third-party firewall from providers such as McAfee, Norton, Zone Labs and Kaspersky. Use a firewall and always run up-to-date antivirus software to detect and remove potential malware on your machine.

Spend too long in one place – The longer you are connected to an unsecured network, the greater the chance someone will notice your system. Sign on, do your work and get out as quickly as you can. Avoid using public computers and public Wi-Fi connections to log into accounts and access confidential or sensitive information. Sign out of accounts and shut down computers and mobile devices when not in use. Program systems and devices to automatically lock the active session after a set period of inactivity.

Let your security apps lapse – Keep your anti-virus and anti-spy-ware programs up to date. These protect you against many, but not all, cyber attacks. Always update the router's firmware. Always update operating systems and patch software. Use a firewall and always run up-to-date antivirus software to detect and remove potential malware on your machine. Remove outdated operating systems, software, or applications.

Let people see your screen - Face the crowd. It may sound like an old spy movie, but "shoulder surfers" still exist. Always be aware of who is watching you and don't turn your back in a crowded location.

NEW JERSEY DEPARTMENT OF CHILDREN AND FAMILIES