Computer security and privacy tips: Home computer networks

In conjunction with the Office of Administrative and Information Management Systems (AIMS), the DHS News is offering tips for using your computer safely and securely. DHS employees and contracted personnel are required to adhere to laws and regulations regarding confidentiality and Protected Health Information (PHI). These tips are designed to enhance knowledge on avoiding use that could compromise data. If you have additional questions, contact the DHS Service Desk at 412-350-4357, option 2.

How to secure your home computer network

Protecting your home network and connected devices allows you to securely connect your DHS-issued or personal devices to the DHS network remotely, while enabling your family to access the Internet safely and securely.

The first step to security is to "Keep a Clean Machine", meaning you should ensure all of your Internet-enabled devices have the latest operating systems, web browsers and anti-virus software. This includes mobile devices that access your wireless or Wi-Fi home network.

Also, unless your home internet router is secured, you're vulnerable to unauthorized people accessing sensitive information on your computer and connected internet devices, or using your Internet service for free and potentially using your network to commit cybercrimes.

Here are some ways to secure your internet router/wireless network:

- **Change the default name of your Wi-Fi network:** When you set up a wireless home network, you give it a name to distinguish it from other networks in your neighborhood. Service Set Identifier (**SSID)** is simply the technical term for a network name. You'll see this name when you connect your device to your wireless network. Change your Wi-Fi network SSID for your household member names or home address to a unique name that will not be easily guessed by others.

- **Change the pre-set password on your router:** When creating a new password, make sure it uses a mix of numbers, letters and symbols and is lengthy.

- **Review wireless security options:** When choosing your router's level of security, opt for WPA2, if available, or Wireless Protected Access (WPA). Wired Equivalent Privacy (WEP) option has been known to be a less secure and vulnerable encryption protocol.

- **Create a guest Wi-Fi password:** Some routers allow guests to use the network via a separate password. If you have many visitors to your home, it's a good idea to set up a separate guest wireless network.

- **Use a personal firewall:** While anti-virus software scans incoming email and files, a firewall acts as a protective guard, watching for attempts to access your system and blocking communications with sources you don't permit. Your operating system and/or security software likely comes with a pre-installed firewall, but make sure you enable this feature.
- **Exercise caution with web sites and emails:** Avoid malicious or suspicious internet sites or content downloads and take extreme caution in clicking emails/attachments from unknown or suspicious senders.
- **DHS network remote access:** Access the DHS network from your home using only mobile phones, tablets, laptops or other such devices that have been issued by DHS. Or, make sure that the devices you are using have the latest operating systems, internet browsers, screen saver, password/passcode options and security patches applied. Refrain from using public computers to access the DHS network. Do not share DHS-issued devices with others and promptly report lost or stolen devices to your supervisor.
- **Monitor your internet data usage trends:** Review your monthly internet usage from internet service provider invoices/reports for detecting any unusually higher internet bandwidth usage.

See more at https://staysafeonline.org/stay-safe-online/keep-a-clean-machine/securing-your-home-network