Home Network Security

What Is Network Security?

Network security is protecting the integrity, usability and availability of network data, including both software and hardware technologies. Effective network security provides access to the network, targets and neutralizes a variety of threats, and prevents them from spreading. This may involve applying various network security tools and techniques to reduce the security concern.

Network security comprises software, hardware, and procedures that are designed to enhance network defense against external and internal threats to an threats to computer systems computer systems. There are multiple layers of software and hardware that prevent numerous threats from penetrating, damaging, and spreading through the network.

Using the Internet for both business and personal reasons has become a necessity. However, it also increases the risk of exposure to security threats and scams.

Your internet router is the link between the devices you use on your home network and the outside world. It can also potentially be exploited by hackers.

Don't think that your home system is safe or too small for the bad guys to target. Since 2016, the US Department of Homeland Security has been warning us that hackers were attacking routers and firewalls.

Setting up a secure home network is a necessity to protect your identity and data. There is no way to be 100% secure. However, there are several preventative measures you can take with your network security to make yourself a more difficult target to attack.

Make Sure Your Network Security is Enabled

Most homes have multiple devices connected to their network, such as smartphones, gaming systems, TVs, computers, wearable devices, and tablets. Each connected device must have the latest operating system, security software, and web browsers.

Malicious code (malware/Virus) or hackers that gain access to one Internet-enabled device may have the ability to infect or steal private information from any other device connected to the same network.

Secure Your Router

When you purchased Internet connectivity, your provider installed a modem and router (or a combination) to connect your home to the Internet. A modem receives information from your Internet Service Provider (ISP) such as Comcast, Verizon, AT&T or your Local telephone or Cable company through the phone lines, optical fiber, or coaxial cable in your home (depending on your service provider) and converts it into a digital signal. A router is a device that communicates between the internet and the devices in your home that connect to the internet.

As its name implies, it "routes" traffic between the devices and the internet. If your provider doesn't give you access to their router, ensure that you have them change the default password when they install the router. Hackers can gain access to your router model with a simple Google search because the default password for most common routers are well known. Once they have access, they can reset your password, change any configurations from the available options and potentially access your data.

Atos

Secure Your Wireless Connectivity (Wi-Fi)

More than three-quarters of households in North America use Wi-Fi as their primary connection to the Internet. If the Internet Connection installed by your provider includes Wireless connectivity (Wi-Fi), you should ensure that the provider changes the network name and the network security key.

Follow the steps below to improve your wireless network security:

Change your Service Set Identifier (SSID)

This is the name assigned to your Wi-Fi network. Make it more difficult for hackers to identify the type of router you have and exploit it for any known vulnerabilities. Don't use a name that includes any personal information or any other identifiable data that is easy to interpret. Use a name that is unique to you and difficult to guess.

Change the Wi Fi security Key

Each Wi-Fi network comes with a default security key. This is the security key that connects you to the wireless network. Use a strong Security Key that is at least 12 characters long.

Create a Password for Guests

If you have frequent guests to your home, create a separate network for them to use. Most current wireless access points can support a guest network. Your Provider/Installer can assist with this if needed.

Keep Your Network Software Updated

Network Software is updated frequently to include security fixes and critical patches for newly discovered vulnerabilities and threats. One of the most effective steps you can take to improve security for your network is to ensure your network installer configures your device to automatically install software updates.

Cover Your Camera

We have all heard the quasi-joke that **Big Brother is Watching You.** Unfortunately, it isn't a joke anymore. Many hackers will steal access to your computer's microphone and webcam. To make sure that no one has access to your webcam, cover your camera. Many cameras both built in and external come with the ability to close the camera lens when not in use. This allows you to open the lens when you need to use the camera for Zoom, Facetime, Telehealth visit etc., then you can cover the camera when you are finished. If your camera does not have a built in cover you can use a post it note or paper to temporarily cover the camera.

HopeTech provides educational life empowerment programs for adults.

The mission of Atos HopeTech is to provide a toolkit of resources that will comprise "TechASYST", enabling Atos employees to provide educational life empowerment programs through technology, with special focus on reaching communities that are underserved by technology currently (with focus on senior adults).

For More Information on HopeTech please email: nahopetech@atos.net