5 Tips to Secure Your Home Office Network

You may be a busy, travelling executive, a telecommuter or multi-tasking parent. More than likely you have multiple devices that connect to your home Wi-Fi. With cyber-criminals getting more sophisticated and attacks more frequent, you may want to do more to secure your home office network.

If you are concerned about identity theft and the security of your accounts and personal information, here are our top five recommendations to secure your home office network:

1. Use 2FA for Bank Accounts, Social Media and System Access

Cyber-criminals now use a variety of methods to guess or steal passwords. Simply put, a password-protected account is not protected enough.

> *We recommend that you implement two-factor authentication (2FA) on all your devices, accounts and social media. Consider this a requirement to secure your accounts and identity.*

In addition to your bank accounts, enable two-factor authentication for Facebook, LinkedIn, Twitter, Microsoft, Apple and Google. Furthermore, use 2FA to protect any other accounts that contain personal or sensitive business information.

What is 2FA?

2FA requires the user to supply two out of three possible types of credentials to gain access to an account. In addition to user name and password, it creates an additional hurdle for cyber-criminals to clear. Thus, your account becomes a much less attractive target.

The three types of 2FA credentials:

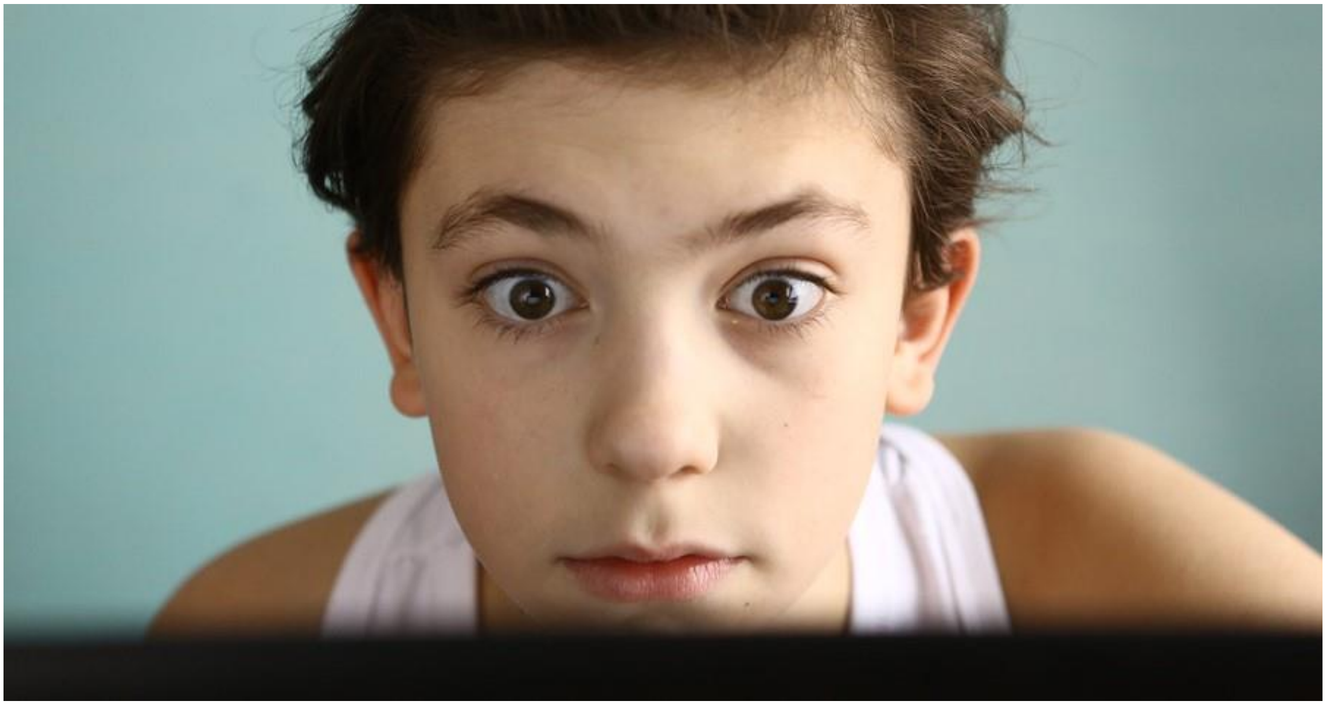
- Something you know – Such as a PIN, password or zip code
- Something you have – Such as a smart card, smartphone or QR Code
- Something you are – A biometric like your face, fingerprint or voice print

When you use your credit card and must enter your PIN to approve a charge, that's an example of 2FA in action. You have provided something you have—the card, and a something you know—the PIN.

Easy to Use

> *Many users think that 2FA will be expensive or hard to use, but often find that not to be the case. Hence, 2FA is catching on quite rapidly.*

One of the great features of 2FA apps is that you no longer need to remember passwords. The 2FA app remembers them for you. In addition, you can have the login pages auto-complete on your behalf. Several affordable 2FA solutions are available.



2. Monitor Network Traffic

If you are concerned about how others in your household use the network or the websites they access, you can monitor your network traffic with a cloud security service.

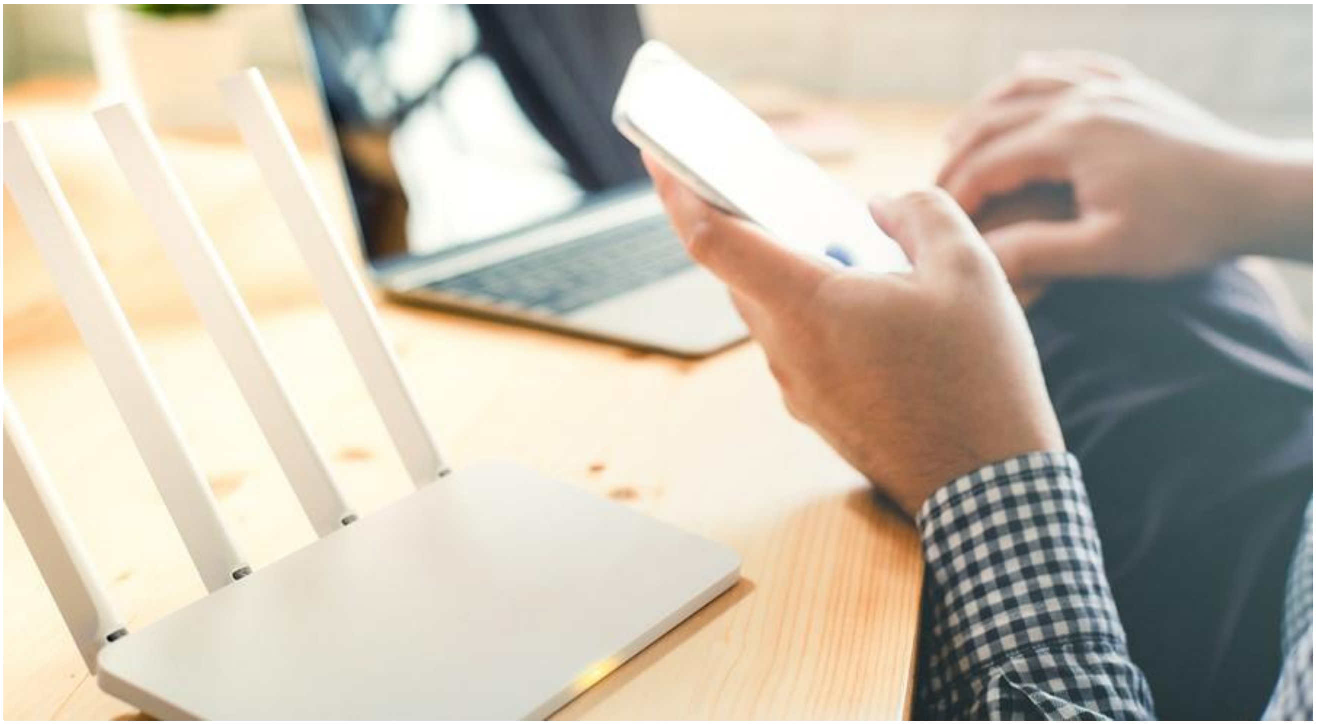
> *This type of service protects every device connected to your network—Desktops, smartphones, tablets, game consoles, DVRs, TVs, everything.*

With the increasing frequency of new malware and targeted attacks, you may also want to check outbound traffic with an **outbound firewall**. This additional layer of protection alerts you to programs attempting to connect out of the network. Use it to stop undetected malware or software that you don't want to be connecting to the Internet.

3. Current Updates

Keeping your computer operating systems such as Windows, iOS or Android updated is more important than ever. Operating system updates and security patches provide fixes to known vulnerabilities and the security features necessary to keep hackers at bay.

Apply this rule to every piece of equipment in your home network as well, such as your wireless router, extenders and access points. Current updates will protect your network against threats like last year's KRACK WPA vulnerability, which affects nearly all Wi-Fi networks.



4. Antivirus and Firewall

Be sure to install anti-virus and anti-malware software and regularly verify that the definitions are up-to-date. If you have Windows 10, you'll get the latest antivirus protection and automatic updates with Windows Defender.

Windows Defender also provides advanced firewall protection on Windows devices. Other firewall products may be used to supplement its capabilities. Alternatively, you may want to consider using a managed firewall service.

5. Device Encryption

Device encryption provides protection by encrypting the data on your hard drive. Only someone with the right encryption key (such as a password) can decrypt your files.

BitLocker, available on some versions of Windows 8.1 and Windows 10, provides easy-to-use and effective hard drive encryption with a minimal effect on performance. Device encryption is not available in Windows 10 Home.

IT Security Resources to Secure Your Home Office Network

Busy telecommuters and entrepreneurs working from home often engage IT security professionals to manage home networks and stay on top of the latest technology trends and threats. In any case, you should consult with security professionals to develop an IT security plan before implementing it.

When it comes to protecting home networks and sensitive information, experience and advanced technologies yield superior results. Residents that partner with IT security professionals for effective home network security solutions enjoy increased security, less downtime, and greater peace of mind.