7 Best Practices for Keeping Your Home Network Safe

One PPG Place, Suite 1700
Pittsburgh, PA 15222
(412) 697-5200
www.schneiderdowns.com

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

7 Best Practices for Keeping Your Home Network Safe

One of the primary pillars of cybersecurity is having a defense in depth strategy, which means layering defensive security measures to protect your assets from digital intruders.

With a defense in depth strategy, even if a digital intruder gets through one layer, they are met with another, and another, and another... until the digital intruder simply loses interest and moves on to a new, more vulnerable target. Defense in depth is not about being perfect, it's about making it difficult for digital intruders to gain access to your assets.

While many people think about multi-faceted security strategies from an organizational perspective, it's also important to think about the personal security of our home networks. We prioritize our physical safety at home, from frequently checking windows, locking our doors and installing security systems, but we need to approach and prevent digital intruders with the same vigor.

To have the best chance of preventing digital intruders' attacks, home networking equipment needs to be configured properly and updated on a regular basis. Here are seven best practices for improving your home network security:

1 Responsible Network and Password Security

Managing a home network might sound daunting, but the truth is, it is quite simple with the proper guidance.

What many consumers don't realize is that they interact with modern home networking equipment by using graphical user interfaces (GUIs) that allow point-and-click configuration and maintenance. All of the following can be configured using GUIs: the administrator account password, USB and cloud settings, configuration from inside the network, wired administrator connection, segmentation, updates, and resources.

Home networking equipment includes an administrator account to configure your home networking equipment. Out of the box, that administrator account uses a default password, and in most cases, you are forced to change the administrator account password for security reasons. If you are not forced to change the default administrator password, make sure you change it anyway.

When changing your administrator account password, never re-use the default password or any easy-to-guess passwords, such as your physical street address or last name. If a digital intruder discovers the make/model of your home networking equipment, they can find the default password by performing a simple Internet search.

If you're wondering how someone could discover the name of your home networking equipment, use your phone or laptop to search for wireless networks around you. You should notice that the default name for home networks usually includes the make and model of the network device.

2 Secure USB Devices and Connectivity

Modern home networking equipment usually includes USB connection capabilities that allow you

to connect a USB device to the home networking equipment. These USB devices usually include printers or flash drives but can also include external hard drives and other digital asset repositories used to store private information.

Before plugging in, remember that once connected to the networking equipment, the information contained on the USB device is available to all users on your network – including malicious ones loaded with malware. Also, if a digital intruder gets access to your network, they will have access to those USB-based assets.

From a security perspective, the ability to plug a USB device into your home networking equipment is like an open window in your house. This is why I recommend disabling the USB device connectivity from your home network if possible.

3 Secure Cloud Services and Connectivity

The same risks associated with USB devices connected to your network apply to cloud storage.

Cloud services allow you to store files on “the cloud” and are usually offered by the manufacturer of the home networking equipment or can be bought from a third party, such as Google or Microsoft.

While cloud services have many upsides, the fact is that “cloud” is just another name for somebody else’s computer. This means anything you store on the cloud is only as secure as the service provider, and unfortunately, cloud service providers continue to experience security issues that impact their users.

Remember, any service on your home networking equipment that connects directly to a third-party service, such as cloud services, is another entry point for a digital intruder to access your network.

4 Restrict Administrator Rights

Another best practice for improving home network security is to restrict the administration rights to only being used inside your network.

Nearly all modern home networking equipment has a setting that allows you to limit the connection type when performing administrative duties. Make sure your home networking equipment can only be administered from inside the network.

This means you can’t be on the road or in a hotel somewhere and connect back to your home networking equipment to configure it. It also means digital intruders can’t configure your home networking equipment from outside your network.

Also, consider only performing administrator tasks while using a wired connection. Performing administrative tasks on networking equipment using a wireless connection allows for the potential of a digital intruder to capture that traffic over the air. Typically, manufacturers of modern home networking equipment include cables in the box. If you need a cable, they are usually available at your local big box store or favorite online shopping outlet.

5 Implement Network Segregation

Another best practice for securing home networks is to create multiple wireless networks, also known as network segmentation. Network segmentation involves creating separate networks for separate purposes. These networks can include televisions, smart devices, computers, phones, and guest networks.

For those working from home, it’s a good idea to have a separate network just for work equipment. Imagine visiting a hotel or restaurant and observing their network traffic for payments. If you work from home, the same thought should be applied. Nobody

should be able to observe network traffic related to your work.

Guest networks are especially important due to the fact you have no idea how others use their devices. If their device is infected, the potential exists for that infection to spread to your networks. Additionally, guests should never have access to your networks due to the potential risk of visitors losing their devices or accidentally revealing your network password to others.

If a guest were to lose their device or reveal your guest network password, and you have proper network segmentation, there's less potential for harm. Segmentation is the same reason public establishments don't provide you with their network password, just their guest network password. Preventing networks from seeing each other provides traffic and access segmentation, which can prevent network segmentation-caused breaches, such as the **attack on Target** many years ago.

Take the time to review your networking needs and develop your own list of networks. If your home networking equipment provides an option that prevents networks from seeing each other, be sure to activate it.

6 Continually Update Home Network Equipment

The final best practice is to continually update your home networking equipment. Just like computers and phones, networking equipment receives updates, which provide critical security fixes, security enhancements, and new features.

If you can't set up automatic updates, simply set a calendar reminder or opt-in to your network provider's notifications to make sure your equipment is running at its best and most secure state. If you are purchasing used equipment or prefer a more manual process, you can reference your home network equipment firmware and

manually check the manufacturer's website for updates.

Remember to warn other users of your home network before launching the firmware update as these updates usually drop connections while they install the new firmware and reboot.

7 Contact the Manufacturer

If you are experiencing issues with your home network, you can always reach out to the manufacturer if you want to avoid restarting or restoring the network to its default settings.

With the rise of remote work and cloud-based storage and applications, it's vital to keep your household network and all the information in it secure – and view it as important as locking your doors at night.

How Can Schneider Downs Help?

Schneider Downs can help your organization to be better prepared. We offer a comprehensive set of information technology security services, including network penetration assessments, network vulnerability assessments, web application security testing and IT security maturity assessments. Our team of network security specialists, application configuration specialists, implementation consultants and certified information system auditors provide a growing slate of services dedicated to keeping organizations secure, including:

- Cybersecurity-as-a-Service
- Digital Forensics and Incident Response
- Enterprise Information Security Program Review and Consultation
- External Footprint Analysis Firewall Configuration Review
- Forensic Analysis
- Incident Response Plan Development, Testing and Training
- Indicator of Compromise Assessment
- Information Security Program Maturity Assessments
- Infrastructure Assessments
- Intrusion Prevention/Detection Review
- MS Office 365 Security Assessments
- Penetration Testing
- Phishing Simulation Exercises
- Purple Team Assessments
- Ransomware Security Service
- Recovery and Remediation
- Vulnerability Assessment
- Web Application Penetration Testing

Breached?

Our **Digital Forensics and Incident Response Team** is available 24x7x365 at 1-800-993-8937 if you suspect or are experiencing a network incident of any kind.

Contact Us

cybersecurity@schneiderdowns.com
www.schneiderdowns.com/cybersecurity

Want to be in the know? Subscribe to our bi-weekly cybersecurity newsletter at www.schneiderdowns.com/subscribe.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com