How to Secure Your Business Network:

A 12 STEP GUIDE TO NETWORK SECURITY

by Chelsea Segal

How to Secure Your Business Network

Businesses today are facing more threats than ever and can't afford to take network security lightly; the risks are far too great. With the increasing number of devices, applications and platforms being used in the workplace, vulnerability to a security breach has increased exponentially. So, how can you secure your business network without breaking the bank? Follow this 12 step guide, "How to Secure Your Business Network".

In this guide, we will provide 12 steps on how to secure your business network starting today.

STEP 1: PERFORM A NETWORK AUDIT

You can't very well tighten and improve network security without first knowing your weaknesses. Therefore, the first step we recommend is to perform a thorough audit of your network.

The goal of the audit is to identify and assess:

- Any possible security vulnerabilities
- Any unused or unnecessary applications running in the background
- Any open ports
- The overall strength of your firewall
- The anti-virus/anti-malware software
- The overall health of servers, software, and applications
- Backups

The output from a network security audit is a detailed report for you to review with your IT administrator and make improvements where necessary.

STEP 2: DISABLE FILE SHARING

File sharing might seem like a great and convenient collaborative method, but it can also put your network security at risk. However, file sharing means that any user that is accessing the same public network can access your files. Therefore, it's a good idea to disable file sharing on all employee devices, except on your independent, private servers.

STEP 3: UPDATE YOUR ANTI-VIRUS/ANTI-MALWARE SOFTWARE

In many cases, businesses will purchase desktop computers for their offices or laptops with the latest version of anti-virus and anti-malware software. However, over time, that software becomes outdated. In many cases, users never update their software again! By taking the time to ensure that your anti-virus and anti-malware is up to date, you are also ensuring that your devices are running software with the most recent bug fixes and security updates.

STEP 4: SET UP A FIREWALL

If you don't currently have a firewall, then make this a priority. Not only should you install firewalls on your devices, but it's also a good idea to set up a web application firewall (WAF). This is especially important if you are an eCommerce business and sell products online and store customers' confidential information, such as their credit card numbers and addresses. Installing a WAF will help protect all your stored data.

STEP 5: INVEST IN A VPN

A Virtual Private Network (VPN) encrypts your network to ensure online privacy for all your users. A VPN blocks your activities, data, browsing history, communications and other personal information from hackers. It also protects your files and information while using a public WiFi network.

If your employees frequently travel or work remotely, then a VPN is a good investment for your business.

STEP 6: SECURE YOUR ROUTER

Securing your router is essential.

Believe it or not, a security breach or other security event can occur by simply hitting the reset button on your network router. Therefore, if your router is in an open or common location in your office, consider moving it to a more secure location, such as in a locked room or closet.

You can also take security one step further and investing in video surveillance equipment and installing it in your server or network router room.

STEP 7: UPDATE ROUTER INFORMATION PERIODICALLY

In addition to moving your router to a more secure location in your office, you can take security a step further and update the login information on a semi-regular basis. Most routers are initially set up with a default username and password, such as "admin". If you are considering leaving your username and password as "admin" because it's easy, think again. There is actually a list of usernames and passwords that are easiest to hack, and "admin" tops the list.

Therefore, set a complex password combination that contains at least 15 characters, a number, and a special symbol. Be sure to also schedule a reminder to change the router information once a month, or once a quarter, whatever you think might be appropriate.

You can also use a password manager, such as LastPass or CloudCracker to securely store and share your passwords.

STEP 8: UPDATE THE NAME OF YOUR NETWORK

Again, similar to updating your network router's username and password on a regular basis, you might also want to update your network name on a regular basis—and keep your router's make and model confidential.

For example, many default network names are "Linksys", "Netgear", or the name of your provider. This tells a potential hacker that you don't follow best network security practices, which makes your business a prime target.

STEP 9: USE A PRIVATE IP ADDRESS

In order to prevent unauthorized users or devices to access your network, consider assigning private IP addresses to specific devices on your network. Therefore, when you or your IT administrator check your router logs, you will see any and all attempts of unauthorized users or devices connecting to your network or any other suspicious activity.

STEP 10: ESTABLISH A NETWORK SECURITY MAINTENANCE SYSTEM

Depending on the size of your business, you may have an in-house IT team, or you might be a DIY solopreneur.

Regardless of size, network security is still important. Therefore, take the time to establish a network security maintenance system that involves processes such as:

- Performing regular backups
- Running activity reports
- Keeping software up to date
- Setting up a schedule for changing your network name and passwords

Again, depending on the size and complexity of your business, your network security maintenance system may involve additional or fewer steps. The overarching goal here is to be proactive and establish a process for monitoring and maintaining network security.

Once you have established a network security maintenance system with the necessary steps that make sense to your business, document it and circulate it to your team.

STEP 11: CREATE A NETWORK SECURITY-CENTERED CULTURE

In addition to taking specific security measures and adopting a network security protocol, the other steps involve educating and training your staff on the importance of network security and how they can do their part.

By creating a culture devoted to network security, you can ensure that your team will better understand the implications of network security, and what they can do to help.

STEP 12: TRAIN EMPLOYEES ON NETWORK SECURITY PRACTICES

Even though you have put thought, effort, and time into documenting your network security practices and process, unfortunately, most team members and employees will skim through your documentation.

In an effort to build a network security-centered culture, it is also important to follow up with a network security training session for your employees. For example, in addition to educating team members on good versus poor network security practices, you can also engage them with interactive activities, such as having them identify phishing emails, quality versus unsecured password combinations, and what to do if they notice any suspicious activity on any of their devices.

KEEP YOUR BUSINESS SAFE WITH QUALITY NETWORK SECURITY

All in all, the truth is that the majority of network security events occur because many businesses don’t cover even the fundamental security basics, which leaves them susceptible to crippling attacks.

Your network security is more important than ever. Therefore, it is always worth the investment to adopt and implement best network security practices in your business to keep you, your business, your clients, and your team members safe online.