[Ten steps to secure networking | Computerworld](https://www.computerworld.com/article/2559866/ten-steps-to-secure-networking.html" \l ":~:text=1%20Ten%20steps%20to%20secure%20networking.%202%20Use,zones%20and%20user%20roles.%20Use%20firewall%2C%20filter%20)

**Secure networking layers**

Secure networking involves securing the application traffic as it traverses the network. It should encompass these areas:

* *Perimeter security* protects the network applications from outside attack, through technologies such as firewall and intrusion detection.
* *Communications security* provides data confidentiality, integrity and nonrepudiation, typically through the use of Secure Sockets Layer or IPsec virtual private networks (VPN).

Secure networking extends this by protecting the underlying infrastructure from attack.

* *Platform security* ensures that each device is available to perform its intended function and doesn't become the network's single point of failure. The network security plan should include antivirus checking and host-based intrusion detection, along with endpoint compliance, to ensure that security policies check user devices for required security software.

**Standards for secure networking**

To ensure a consistent set of requirements, lower training costs and speed the introduction of new security capabilities, IT managers should use these 10 security techniques across their networks.

**1. Use a layered defense.** Employ multiple complementary approaches to security enforcement at various points in the network, therefore removing single points of security failure.

**2. Incorporate people and processes in network security planning.** Employing effective processes, such as security policies, security awareness training and policy enforcement, makes your program stronger. Having the people who use the network (employees, partners and even customers) understand and adhere to these security policies is critical.

**3. Clearly define security zones and user roles.** Use firewall, filter and access control capabilities to enforce network access policies between these zones using the least privileged concept. Require strong passwords to prevent guessing and/or machine cracking attacks, as well as other strong forms of authentication.

**4. Maintain the integrity of your network, servers and clients.** The operating system of every network device and element management system should be hardened against attack by disabling unused services. Patches should be applied as soon as they become available, and system software should be regularly tested for viruses, worms and spyware.

**5. Control device network admission through endpoint compliance.** Account for all user device types -- wired and wireless. Don't forget devices such as smart phones and handhelds, which can store significant intellectual property and are easier for employees to misplace or have stolen.

**6. Protect the network management information.** Ensure that virtual LANs (VLAN) and other security mechanisms (IPsec, SNMPv3, SSH, TLS) are used to protect network devices and element management systems so only authorized personnel have access. Establish a backup process for device configurations, and implement a change management process for tracking.

**7. Protect user information.**WLAN/Wi-Fi or Wireless Mesh communications should use VPNs or 802.11i with Temporal Key Integrity Protocol for security purposes. VLANs should separate traffic between departments within the same network and separate regular users from guests.

**8. Gain awareness** of your network traffic, threats and vulnerabilities for each security zone, presuming both internal and external threats. Use antispoofing, bogon blocking and denial-of-service prevention capabilities at security zone perimeters to block invalid traffic.

**9. Use security tools to protect from threats**and guarantee performance of critical applications. Ensure firewalls support new multimedia applications and protocols, including SIP and H.323.

**10. Log, correlate and manage security and audit event information.** Aggregate and standardize security event information to provide a high-level consolidated view of security events on your network. This allows correlation of distributed attacks and a networkwide awareness of security status and threat activity.

[Network Security Best Practices - A 12 Step Guide (coxblue.com)](https://www.coxblue.com/how-to-secure-your-business-network-a-12-step-guide-to-network-security/)

**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:**

* Possible security vulnerabilities
* Unused or unnecessary applications running in the background
* Open ports
* Overall strength of your firewall
* 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.

**2. Disable File Sharing**

File sharing might seem like a great and convenient collaborative method, but it can also put your business’ 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.

**3. Update Your Anti-Virus/Anti-Malware Software**

In many cases, businesses will purchases 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.

**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 also 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. Installing a WAF will help protect all your stored data

**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.

**6. Secure Your Router**

[Securing your router](https://www.coxblue.com/10-steps-to-take-right-now-to-secure-your-business-wifi-network/) 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.

**7. Update Router Information Periodically**

In addition to moving your router to a more secure location, 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 something a password manager, such as LastPass or CloudCracker to securely store and share your passwords.

**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.

**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.

**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

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.

**11. Create a Network Security-Centered Culture**

In addition to taking specific network 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 and risks of lack network security, and what they can do to help.

**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.