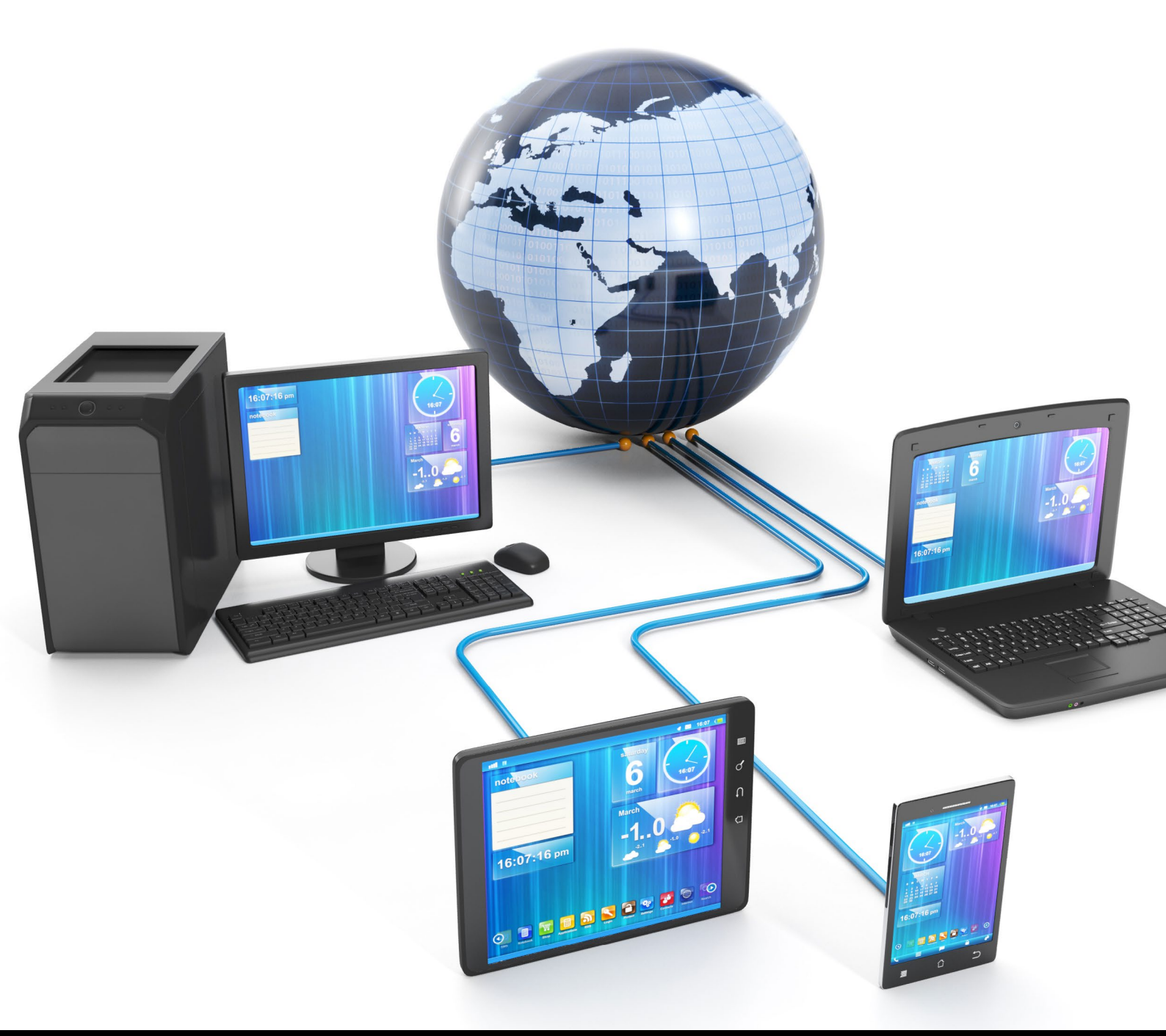
COGNOSCAPE LLC



8 Steps for Network Security Protection

8 Steps for Network Security Protection

Many small and medium sized businesses make the mistake of thinking they won't be the target of hackers because of their smaller size. Unfortunately, there are automated techniques used by hacker groups that don't discriminate based on company size – they are simply programmed to look for a lack of network security that will allow them to get in the door. Here are 8 steps you can take for network security protection that will help minimize your risks for attack:

1) Get a Network Firewall

When automated scanners or hackers seek out websites to attack, they're looking for open ports. Ports are the path between your business network and the internet and if you leave the 'door open', you're basically putting out a welcome mat for an attack. Configuring a network firewall will lock all of the doors that do not need to be opened to the outside world and minimize your risks for attack.

You can lock down the IP address through the router/ firewall and assign IP addresses to specific users.

Don't forget to change the default password on your firewall. It is very easy for hackers to figure out what network equipment you're using and find the default username and password.

2) Lock Your IP Address

The majority of routers used by small businesses use DHCP, a system that automatically allocates IP addresses to computers connecting to the business network. While DHCP makes it convenient for employees to connect to your network, it also makes it easier for attackers to connect to your network. For businesses that do not have too many guests using the network, you can lock down the IP address through the router/ firewall and assign IP addresses to specific users.

3) Block Pings

Many hackers send a "ping request" to a network to see if they get a response. If the

network device responds, the hacker can do some exploring and probably exploit your network. Set up your firewall or network router to block pings.

4) Update Router Firmware

Keep your router up to date for bug and security fixes. From the router's administration menu, there is probably an option to check for new firmware versions. If not, look in the administration screen for your router and visit your router vendor's support site to make sure you have the most up to date version.

5) Get an IPS

Most network traffic out of your business to the internet will go over Port 80. It has to be left open in order to use the internet, which means you are still at risks from any hacker that targets Port 80. In addition to your firewall, you can install IPS technology to monitor your ports and traffic

flow to indicate any potentially malicious activities that need to be investigated or stopped.

6) Scan your Network

One way to see whether you are vulnerable to hackers is to scan your network the same way a hacker would with a network scanning tool. These tools will take a look at your network to find any open ports that don't need to be opened, and will make the changes to your firewall to close them.

7) Use a Virtual Private Network

When people connect remotely to your network, they need to be going through an encrypted tunnel. A VPN will shield your remote employees with the same firewall tools that your local employees are protected with, and will prevent other users with mobile devices from connecting.

8) Set Up a VLAN

A Virtual LAN (VLAN) lets you divide your network based on the access needs of each group. For example, your finance department may need one set of access while your human resources may require access to different areas of the network, and outside guests or contract workers may need access to a separate area. When setting up VLAN for your employees, you can mitigate risk by providing access only to the network resources each group of people require and restrict access

to the data they do not need to do their job.

Secure Your Network and Minimize Risks

Setting up a secure network can prevent most hacker attacks from accessing confidential data or causing problems for your business operations. Many of the network security tasks can be fulfilled on your own, but for ongoing monitoring and security, Cognoscape's experts can provide an additional layer of protection you just can't get on your own.

COGNOSCAPE LLC

16479 Dallas Parkway #230
Addison, TX 75001

(214) 377 4884

info@cognoscape.com
cognoscape.com