Security Tips When Working Remotely

As more people rely on their personal WiFi networks, it's more important than ever to ensure every network is safeguarded from frequent online threats. If you're seeking solutions to help protect your data and maintain productivity, know that we're in this together.

More than 65% of our global team works in a flexible capacity, giving us advanced insight in all areas of online security. Explore some of the methods and end-to-end security solutions our teams use to keep our personal and company data safe.

7 Ways to Boost Online Security

1. Start With Education

If you or your employees are making the shift to working remotely, education is key to ensuring they have the tools that empower them to work securely.

This means training your team about common ways cybercriminals can infiltrate your systems, like phishing emails and weak passwords. Teaching how to recognize the signs of a security breach will let employees respond quickly if a threat does occur, so they can take the right steps to keep data safe and out of the hands of online attackers.

2. Install Antivirus Software

Additionally, safeguard your network by installing antivirus software, like McAfee, to the devices you use for remote work. Having a program that automatically spots online threats and eliminates them is invaluable to help you safely stay productive. If you have questions about what software is right for you, contact a Dell Technologies Advisor for expert guidance to keep your team working securely.

3. Set Up Two-Factor Authentication

One of the easiest ways to boost your security is to turn on two-factor authentication on sites and applications that allow it. This quick action will stop hackers from being able to log in to your accounts if a password has been compromised.

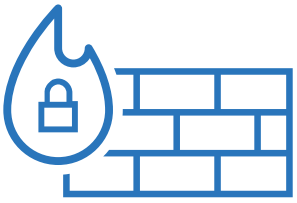
After setting up two-factor authentication, users will be sent a secondary request to their personal device and will be asked to enter a time-sensitive password or specific identifier, such as a fingerprint or retina scan, to gain access to the company network. This ensures that in the unfortunate event that your password ever gets stolen, additional barriers are put in place to stop attackers before they can reach your data.

DELL Technologies

4. Create Advanced Passwords

Hackers and online threats grow stronger every day. It's crucial to stay ahead of their tactics, and one of the most efficient ways to stop attackers is by having advanced passwords.

Creating advanced passwords doesn't have to be complicated. Simply choose a password that uses lowercase, uppercase, punctuation, numbers and special characters. Password best practices to keep in mind: Refrain from keeping a physical or digital record of any online password. Don't use words or phrases that can be personally tied to you, such as nicknames or birthdays. And lastly, create a unique password for each site. The more unique, the better!

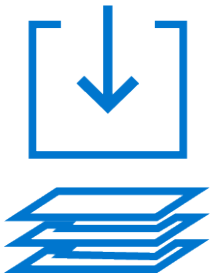


5. Start Using a Firewall

If working from home is a new reality for you or your business, relying on a firewall like SonicWall will provide high-performance intrusion prevention, malware blocking, content/URL filtering and application control. This can defend your team against online threats, no matter how big or small. A firewall will also provide secure mobile access, so employees can access files safely from anywhere, right from their personal devices.

6. Backup Your Data

From cyberattacks to simple human error, there are many ways your data could get compromised. Backing up files and data gives you additional security in the chance that your files are unable to be accessed. Using a hybrid-cloud solution, with both cloud applications and your own server, will allow you to reliably store your company's online assets in a safe place, away from hackers and scammers.



7. Set Up a VPN (Virtual Private Network)

If you're setting your team up to work remotely, having a Virtual Private Network is vital to keep your company data secure while allowing individual employees to access company email, files and other systems.

The process works by connecting you to a group of servers through your internet provider, or ISP. Once you've established a connection with your VPN (a system known as "tunneling"), these servers act as your newly secure home online, restricting access to entities outside of the tunnel. As you surf the web, all the data you send and receive is then encrypted, letting you work from home without the threat of malevolent online forces.

Start by choosing a VPN provider, weighing the cost versus security you'll get from each. Depending on your needs and what types of files and content you'll be accessing, you may need a more robust security package. If you have questions about which security option is right for you, we're here to help. Reach out to our experts for one-on-one guidance to help you work securely from anywhere.

SPEAK WITH AN ADVISOR TODAY

877-BUY-DELL

DELL Technologies