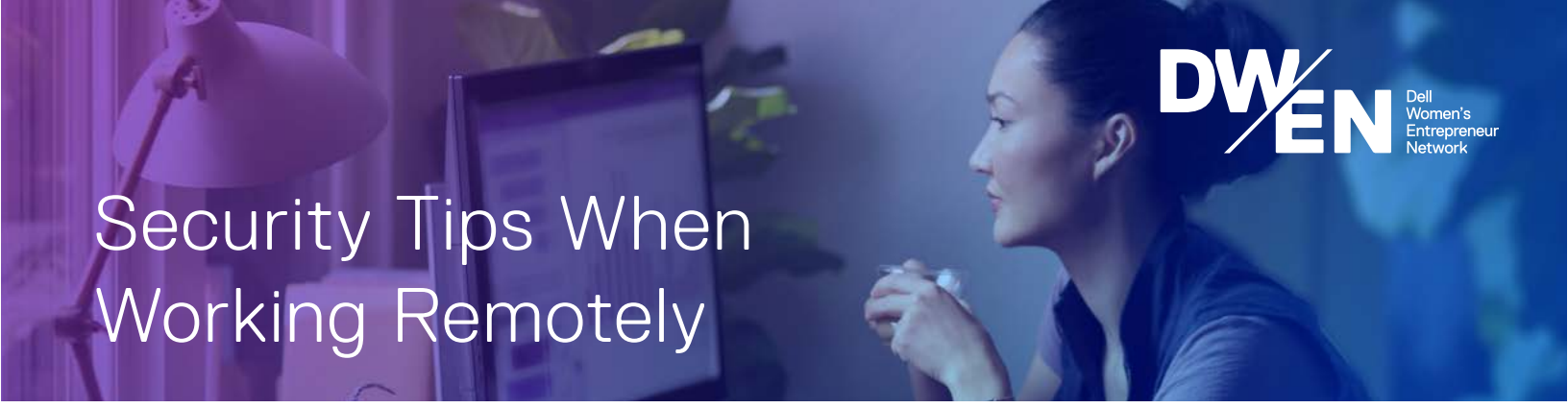


Security Tips When Working Remotely

As more of us begin working from or running businesses from home, sensitive material is passed over personal networks. It's important to make sure your data is safeguarded from common online threats.

Small businesses in particular can be at risk. In fact, 1 in 5 small businesses were the target of a ransomware attack and experienced a shutdown due to the attack. It's critical to create safe, remote access to software applications and files so small business owners and their employees can focus on keeping the business productive.

There are several easy ways you can boost your online security, including the following.

1. Start with education

Make sure you have the tools that empower secure work from home. 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.

2. Install antivirus software

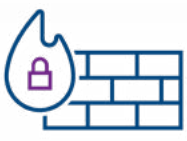
Safeguard your network by installing antivirus software like McAfee to the devices you use for remote work. Having a program that automatically spots online threats and eliminates them is invaluable to help you maintain productivity and security.

3. Set up two-factor authentication

One of the easiest ways to boost your security is to enable two-factor authentication on sites and applications that allow it. With two-factor authentication, users will be sent a secondary request to their personal device with a time-sensitive identifier in order to gain access to the company network. This quick action will stop hackers from logging in to your accounts if a password has been compromised.

4. Create advanced passwords

An advanced password uses lowercase, uppercase, punctuation, numbers and special characters. A few good password rules 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 a nickname or birthday. And lastly, create a unique password for each site. The more unique, the better!



5. Start using a firewall

If remote work 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 to defend your team against online threats both big and small. A firewall will also provide secure mobile access so employees can access files safely from anywhere.

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 primary files become inaccessible. Using a cloud-based system 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 getting your team set up to work remotely, having a VPN is vital to keep your company data secure while allowing individual employees to access company email, files and other systems. A VPN connects you with a remote group of servers through a process known as "tunneling." Once you have linked up to that, the servers act as your secure home online, restricting access to anyone outside of the tunnel. As you navigate the web, all the data you send and receive is encrypted, letting you work from home without fear of malevolent outside forces.

For more information and one-on-one dedicated support to help guide you with tailored tech solutions, contact a Dell Technologies Advisor today.

SPEAK WITH AN ADVISOR TODAY
877-BUY-DELL