Security Tips When Learning From Home

If you're adjusting your routine to learn remotely, it's more important than ever to ensure your network and devices are safeguarded from cyberattacks. No matter where you are in your learn-from-home journey, know that we're in this together.

With more than 65% of our global team working in a flexible capacity, we're here with security tips to help you stay safely productive from anywhere. Learn about some of the actions we take to boost our online security below.

5 Quick Ways to Boost Online Security

1. Start With Education

Educating yourself about the tactics that hackers use to intercept data is key to staying one step ahead of dangerous online forces. Take a few moments to brush up on ways cybercriminals can infiltrate your systems, such as through phishing emails and weak passwords so that you can stay alert to their tricks.

2. Install Antivirus Software

A great way to shield your technology from hackers and scammers is by installing antivirus software, like McAfee, to the devices you use. Being able to rely on a program that automatically spots and eliminates online threats is crucial to keep you safely learning from home. If you have questions about which software is ideal for your unique needs, reach out to one of our product experts for guidance.

3. Turn on Two-Factor Authentication

Another efficient way to boost your online security is by enabling two-factor authentication on sites, programs and applications that allow it. Doing this means that in the unfortunate event that your password ever becomes compromised, hackers will have another barrier to overcome to be able to log in to your accounts.

After a quick set up, your new login process will consist of two steps. Upon entering your usual password, you'll be sent a secondary request to your personal device and asked to enter a time-sensitive password or specific identifier. This additional barrier greatly increases your chances of stopping an online attack with one quick and easy action.

4. Use Advanced Passwords

Sometimes upping online security is as simple as making your passwords more complicated. Stay ahead of cyberattacks by creating advanced passwords that hackers can't guess.

Coming up with advanced passwords is easy. Choose a password that uses lowercase, uppercase, punctuation, numbers and special characters. A few password best practices to keep in mind: Do not keep a physical or digital record of any online password, ever. Don't include words or phrases that can be personally tied to you, like birthdays or nicknames. Refrain from using the same password across sites. And be unique – the more unique, the better!
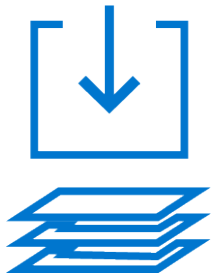
5. Backup Important Data

From cyberattacks to accidents, there are many ways that your data can become compromised. Backing up important files allows you to safely store away what you need in a separate location, so you can always be prepared.

We advise having at least one backup of essential files in another location, whether that's an external hard drive or the cloud, in case one ever becomes compromised or corrupted.

How can we help?
If you have questions about online security, we're here for you.
Contact our experts for one-on-one guidance to help you learn securely from anywhere.

SPEAK WITH A PRODUCT EXPERT TODAY
877-BUY-DELL

DELL