1. Update Your Devices

One of the easiest and most effective ways to protect the security of your computers and mobile devices is to keep the software up to date, says Maria Roerich, senior director of product testing at Consumer Reports. Updates help manufacturers patch security vulnerabilities quickly. Just this month, for example, Apple released a patch for a bug that allowed eavesdropping on FaceTime conversations. Though phone and computer manufacturers are usually vigilant about informing you of updates and even offering you the chance to automatically update your devices—a smart option— that's not always the case with devices such as routers, security cameras, and baby monitors. So, take a moment every few months to check for software and firmware updates for those items. Any device that is connected to a network can and has allowed hackers into the network.

1. Use Two-Factor Authentication

What if you could find a way to make your password all but useless to a hacker? That's what two-factor authentication does. Instead of relying solely on a password, user accounts secured by two-factor authentication require an additional level of proof of ID before granting access.

When you log in to an account on a new laptop or smartphone, you'll be asked for your password, but once you enter it, you won't immediately get access to your account. Instead, the website will ask for a one-time code sent by text to your phone. The second "factor" is your phone; without it and the password, you'll be denied access.

1. Use a VPN or a remote access software whenever you're online

A Virtual Private Network is not as mysterious or secretive as it sounds. With a VPN account turned on, your Internet activity is tunneled through a hacker-proof, spy proof network. Hackers can't steal and/or read your data transmissions when it's in transit over the Internet. Remote access software allows easy, encrypted secure access to practice resources from anywhere went set up properly.

1. Close unused accounts and uninstall unused programs

Think about all of the online accounts you’ve opened over time. Now, consider which ones are still open, but that you never use. If there’s a breach involving one of those entities, hackers may have access to whatever personal information is tied to that account. An old email account, for instance, could be holding any number of past bank statements and healthcare forms. As a tech I often find remote software installed, a huge security threat. You should look at all programs installed on your computer and uninstall the ones you don’t use.

1. Have Multiple backups.

Backups have also evolved. Running your backup on a single hard drive that you take home each night is no longer the safest or most secure method. Today, if your practice is the victim of ransomware or otherwise gets hacked, you need a copy of the data that’s stored remotely. You should have multiple backups, including offsite backups that rely on secure cloud-based technology and encryption. Often ransomware gets in from emails claiming to be from the CDC or WHO. Use sites like coronavirus.gov and usa.gov/coronavirus to get the latest information. And don’t click on links from sources you don’t know.

For more information go to [Https://sandiegohit.com/7protections](https://sandiegohit.com/7protections). During this crisis I have a limited number of free remote support licenses for members during this crisis. In addition, I also want to offer any free remote support or any other technical issues you are struggling with. This is just a tiny way I can help dentists during this  crisis.