School's in session: 7 considerations to secure your system

By: Jennifer Leach, Associate Director, Division of Consumer & Business Education, FTC | Aug 28, 2020 1:39PM

If you have kids in school, there's a good chance they're kicking off their school year . . . in your living room. All the while, you're connecting with clients, taking meetings, and making sales from a carved out corner at home. The start of a new school year is a good time to double-check your online set-up to make sure the kids can take their classes while you take care of business. Here are a few things to check or consider.

- **Secure your router.** Does it still have the same default name and password that it came with? You'll want to change that, and be sure you've turned off remote management. Then log out as the administrator once the router is set up.
- **Update your software.** That means updating your browsers, operating systems, and apps. Then, set them to update automatically.
- **Use strong passwords and two-factor authentication (when available).** And while you're teaching your kids about the importance of a strong password, remind them NOT TO SHARE their password with their friends.
- **Update and protect your phone.** Make sure your phone's security is up to date and you have your data backed up. (Backing up is good advice for your computer, too.)
- **Remind your family why they shouldn't watch pirated content.** Hackers are using illegal pirated content as a way in to your devices and wireless network. So If you have content-hungry kids at home who have found free ways to stream content, learn more about what the pirates look like, what the hackers can do, and what you can do to stop them.
- **Make use of privacy and security tools.** If you're hosting a video conference, or just participating in one, check out the privacy and security options your platform provides, including ways to keep unwanted visitors out of your conference.
- **Don't open unexpected video conferencing invitations or click on links.** It might look real, but is it? Check with whoever invited you to be sure (and not by replying to that message). Scammers are using fake invitations to load malware onto your computer or phone.

You're probably facing way bigger headaches right now, but taking a few minutes to check your systems can save you – and your business – from even bigger headaches later on.