

How to Prioritize Online Security While Working From Home

Opinions expressed by *Entrepreneur* contributors are their own.

Everyone seems to be concerned about cybersecurity these days. Recent polling data from The Pearson Institute and The Associated Press-NORC Center for Public Affairs Research shows that around 90% of people are concerned about protecting themselves online. Yet many people don't know about all the sneaky ways that cyber criminals can gather information. This leaves them wide open for attack.

Employees who work remotely in particular seem to be lacking in cybersecurity awareness. Why? They feel comfortable and safe in their personal environments. Usually, they password-protect devices like smartphones, tablets and laptops. They don't tend to worry about all the other avenues cyber thieves can use to steal everything from IDs to bank account numbers. Consequently, they open the door to a cybersecurity nightmare.

Wondering how you can make your castle more secure? Consider the following ways to protect yourself, and your company, while working from home.

Related: Top 5 Security Strategies for Home-Based Entrepreneurs from IoT Cyber Threats

1. Update and secure your

entertainment devices

Do you enjoy smarter digital entertainment? Research from Plume, a SaaS experience platform for Communications Service Providers, shows that the highest increase in home cyber threats doesn't come from where you might assume. It comes from advanced entertainment devices like streaming devices and smart TVs. In fact, smart TV cyber threats increased 433% between late 2019 and early 2021.

In other words, while you're gaming with the family or binge-watching your favorite shows, a cyberattacker could be hard at work. To keep yourself out of that unwanted position, install updates immediately, upgrade your devices to later-generation models, and invest in a smart network security system.

2. Keep private information separate from company information

Three-quarters of executive leaders told McKinsey's researchers in 2021 they wanted employees back in the office at least a few days a week. However, they were generally fine with them working elsewhere the rest of the time. While this opens many opportunities for professionals whose jobs can be done practically anywhere, it also presents opportunities for risk in workers' homes.

Consider this scenario: You're working on your personal computer at home. You log into your company's network. At this point, you may have exposed everything on your computer – such as prior year's tax documents and healthcare statements – to a cyberattack that starts at your company's location. Instead of putting yourself in this kind of situation, talk to your employer about ways to shelter your private information. One answer could be to ask to work from a laptop purchased and owned by the company so that you don't have to use your own

device.

Related: 3 Reasons Your Company Should Prioritize Data-Privacy Compliance and Safety Issues

3. Install home security systems with caution

You feel great because you finally purchased a home security system to monitor access points. Have you just given criminals one more way to find out information about you and your family? Perhaps. If you had your security system installed and handled by a third party, your device may be susceptible to hacking. Certainly, some hackers may be more voyeuristic and just watch your family come and go. To them, that's entertainment. It's also creepy and disturbing.

Avoid this issue by working with reputable technicians who've been sent by your home security provider. Or, if you buy a home security system and put it in yourself, stay current with all device updates. The video will then be encrypted properly and less open to hacking. Next, report any inkling of problems immediately to the appropriate customer support team. They should be able to help you maintain tighter control.

4. Monitor and secure your kids' devices

The U.S. Census Bureau's Household Pulse Survey showed more than nine out of 10 kids underwent cyberschooling during the pandemic. Though that number has gone down as children have returned to physical classrooms, some institutions still offer remote lessons. Every time your child logs into any kind of online learning platform, your home becomes a bigger cybercrime target.

You can't depend upon schools to have the tightest cybersecurity measures. Many are still figuring out how to keep information out of the hands of cyberattackers. Children and teens also don't always make the best decisions when it comes to sharing sensitive data. They may unintentionally give out passwords or reveal family information online. You need to stay on your toes and monitor your child's remote schooling habits from an online standpoint.

Related: How to Help Employees Work From Home With Kids

Our world continues to move closer and closer to a true "metaverse" as people become more interconnected through digital means every day. Nevertheless, you aren't obligated to give everyone on the planet full access to your home and private data. This year, make stronger home cybersecurity one of your family's collective resolutions.

<https://www.entrepreneur.com/article/420969>