NEED TO KNOW NEWSLETTER JANUARY 2021

New year, new home office security strategy

Make security your New Year's resolution

Home may feel like the safest place on the planet these days, but your personal network might not be. This year, step up your home office security strategy and dedicate 2021 to protecting yourself and your organization online.

5 tips to kick off the new year

Get a head start on securing your home office with these 5 tips.

1. Avoid unsecure public networks

Free Wi-Fi at your favorite coffee shop may tempt you to set up there during working hours, but these hotspots also attract hackers.

Unsecured public networks let cybercriminals sneak in between you and the connection point, which means they could intercept your emails, credit card information and business account credentials.

No matter where virtual work takes you, use a VPN (virtual private network) to prevent hackers from stealing your personal and business information. And above all, **never trust public Wi-Fi.**

2. Protect personal devices from people and pets

Never leave your personal devices unsecured and unsupervised. Guests and roommates can snoop around and steal personal info – and you'd probably never suspect it. Prevent this by password-protecting computers, tablets, phones and important files, and lock them away somewhere safe when you're not home.

Kids and pets, on the other hand, can accidentally share or delete important data in just one click. In addition to locking your devices, you can also pet- and kid-proof your computer by encrypting files, setting up parental controls and installing detector software that monitors reckless keyboard activity.

3. Shred sensitive documents

Buying a shredder may seem unnecessary but here's the truth: **people who want to steal your identity are willing to dumpster-dive for it.**

Protect your personal information by destroying documents that contain your name, address, phone number, identity number and banking information. That also includes last month's electric bill, old airline tickets and ATM receipts, as well as expired credit cards, IDs and passports.

4. Avoid using personal devices for work

Working remotely can blur the boundaries between work and home, especially when you've got all your devices within reach. But each device serves its own purpose for a good reason.

Using your work computer for shopping, social media and banking can give hackers access to your accounts and credit card info in the event of a data breach. And on the flip side, accessing sensitive documents from your phone or personal laptop can give cybercriminals the opportunity to steal data from your organization. Keep work and personal matters separate to mitigate risk.

Signs of compromise

A burglar is easy to spot, but catching a hacker who's hijacking your Wi-Fi can be harder. Monitor your network for these signs of compromise and get familiar with your company's incident reporting and response procedures.

1. Your computer is behaving strangely (and without your input).
2. Family and friends receive messages from you that you didn't send.
3. You get ransomware messages and phishing emails.
4. Passwords have been changed and settings have been reset.
5. Devices crash, reboot and lose power quickly.

5. Ask your IT team to help you configure connected devices

If you haven't already, now's the perfect time to become best buddies with your IT support team. As work-from-home policies and procedures evolve, IT can help you make sure you stay safe and connected.

For example, you can reach out to IT for assistance with setting up your printer. They can make sure it's properly secured and configured to your company's services.

Real horror stories of Wi-Fi hacking

Barb Angelova awoke one morning to a startling letter from her internet provider. Not only were they threatening to suspend her service, but the Motion Picture Association of America **wanted to sue her.** Why? For illegally downloading Man of Tai Chi, a movie she'd never even heard of.

After some investigation, Barb put the pieces together. Her frozen laptop and poor internet connection had been telltale signs that someone hijacked her Wi-Fi. Once she knew what to look for, she wouldn't be framed for a cybercriminal's pirating scheme again.