Working from home makes you vulnerable to hackers. Here's how to stay safe

At home, it's less likely you're protected by the corporate software that can scan every link you click and every file you download for signs of danger.

Working at home can leave you open to hackers, even in normal times, and these aren't normal times. With one in four people in the US under orders to stay home to slow the spread of the novel coronavirus, many more people are now working in their personal space, sometimes on their personal computers or phones. That makes a much wider target for hackers, cybersecurity experts say.

At home, it's less likely you're protected by the corporate software that can scan every link you click and every file you download for signs of danger. Additionally, your brain might be fried with worries about the spread of a disease that's threatening to overwhelm health care systems around the country, and by all the logistical problems that staying inside presents.

"I don't think there are many people alive who have gone through something of this magnitude," said Eva Velazquez, president and CEO of the Identity Theft Resource Center, who added that current events are so distracting, we're more vulnerable to scams.

There are simple steps you can take to limit the risk, though. That's good, because cybersecurity firms say it appears hackers have become more active lately. Researchers at Zscaler say that since January, they've seen a 15% to 20% increase each month in overall hacking incidents and a spike in hacking threats that use terms like "coronavirus" or "COVID-19" to trick users into handing over sensitive information or installing malicious software.

According to Microsoft, 91% of hacking attacks begin with a malicious email, in what's called a phishing attack. Limiting these hacks could help prevent headaches at work, and they could also stop hackers from stealing data that your company is holding on to. And since your personal and professional life are all mixed up at the moment, you can stop yourself from handing over your own sensitive information to hackers at the same time.

Here's what you can do to work from home more safely.

Update your software

Because you aren't in your office, your company could have a harder time keeping your software updated automatically. And you might not realize it, but professionals whose job it is to stop hackers say that keeping your software up to date is one of the most important things you can do.

When software companies release updates that fix security flaws, they're essentially handing hackers a key that helps them access devices running the older version of the software. If you update your software, you're changing the locks, and it'll be a lot harder for hackers to get in.

Of course, there are potential drawbacks. Software updates themselves can sometimes cause problems on your device, breaking programs that are essential to your job or making your device unusable. These problems, however, typically get noticed and addressed quickly. So if you must wait to make sure there aren't any surprise problems with the update, go ahead, but don't wait too long.

Use two-factor authentication

If hackers do manage to infiltrate your system, they might be able to steal your usernames and passwords. That sounds scary, but there's something you can do to make that information much less useful for hackers. It's called two-factor authentication, and it requires you to enter a one-time code or use a hardware token to finish logging in after you enter your login credentials.

When you have this feature enabled, stealing your password isn't enough for a hacker to log in to your personal bank account -- or your company's payroll system. It's an extra step, but it's one of the most effective ways to stop hackers. The security settings in Microsoft and Google cloud services used by many small businesses let you turn on two-factor authentication and review other options for keeping your accounts secure.

Avoid phishing scams

Just as you need to be on the alert for scams and bogus information about COVID-19, the disease caused by the coronavirus, you should keep your guard up against suspicious messages that could come from hackers and scammers.

According to Microsoft, 91% of hacking attacks begin with a malicious email, in what's called a phishing attack. The emails can take all forms. Some might promise you vital information about the spread of the coronavirus in your region, but in fact contain a malicious file that can infect your computer. Others will use spoofing to look like they're coming from your boss, asking you to wire him or her some money in a hurry.

While you're working from home, you can't walk down the hall and ask your boss for more details about an odd request for funds, but you can still check in on the phone, said Chris Hallenbeck, chief information security officer at cybersecurity firm Tanium.

That way, he said, you won't "suddenly wire $200,000 to someplace you didn't intend to."

Beef up your personal security

For people using a work computer at home, corporate antivirus software and other security tools are often running by default. If you have access to a corporate VPN, you can use it to access your company network, where your employer can better protect you from afar.

This won't work for all companies, which might not be prepared to have their entire workforce use the VPN at once, so it's worth checking in with your employer about this one. You can also use a personal VPN, but that's mostly to protect your own privacy, as these services aren't meant to protect you from malicious software and apps.

If you're using your own computer and can't access your company's internal network, you can still install consumer products that scan for malicious software that can steal information, spy on you and spam your contacts, as well as potentially unwanted programs like adware. If you run these programs and keep these other tips in mind, you'll be in good shape to defend yourself from hackers.

Plus, there might be a silver lining, Hallenbech said. If you can't access your employer's network, then hackers can't use your computer to access it either.