Internet Security When You Work From Home

10 Tips for Success

Don't take a break from good internet security practices when you are working away from the office. Use these tips and questions to stay secure and find success when your organization provides the option to work remotely. Your IT staff can provide further guidance as needed.

Getting Ready to Work from Home

TIP 1

Start preparing to work from home as soon as possible.

If you wait until the day you need to work from home to start this process, you have waited too long. Make sure to ask these types of questions:

- What do I need to do to start this process today?
- If I run into problems along the way, who should I contact for help?

TIP 2

Identify any technology you will need.

Some organizations provide everything you will need, and others expect you to use your own technology.

- Who provides the needed equipment (system, monitors, printers, storage) and are there any specific requirements?
- Is my internet connection fast and stable – can it handle what my job requires?

TIP 3

Identify the software you will need.

Having the right device to use is great, but without the proper software, there isn't a lot you can do.

- Is there special software, like communication software to chat or host virtual meetings, that I will need?
- What's the process to have software installed? Does IT handle this task, or will I need to do it?

Securing Your Workspace

TIP 4

Identify and secure your physical workspace.

Find a space that allows you to maximize your productivity. It should be comfortable and have minimal distractions.

- Am I using a clean-desk policy where I secure work-related items like printed material or devices when not in use?
- Can I shred important documents I no longer need?

TIP 5

Keep your work and personal life separate.

This is easier said than done when you are working from home, especially if it's because of an unexpected event. However, from a security standpoint, the more you can do this, the better.

- Am I making sure my work device isn't used for personal activities?
- If I have to use my personal device for work, have I tried to keep things separate?

TIP 6

Make sure your devices are secured.

The bad guys often gain access to a system because it wasn't properly secured.

- Am I using unique passwords for everything and not ones that are similar to or the same as those I've used before?
- Do I make sure to secure my device when I step away, even for just a second?
- Have all the latest security updates been installed on my device?

TIP 7

Make sure your internet connection is secure.

One of the biggest security holes in your home is the internet connection.

- Have I changed the default password and enabled the security settings on my router (the device from my internet provider that allows me to connect to the internet)?
- Am I using virtual private network (VPN) technology, which creates a safe internet connection that shields my online activity from the bad guys every time I am connected to the network?
- Am I using multi-factor authentication (MFA), which is a way of confirming my identity using two or more security mechanisms (like fingerprint and username and password), when available?

Best Practices for Staying Secure

TIP 8

Always be cautious of hackers' tricks.

Hackers want to trick you into taking an action that grants them access to your device and your organization's network. Remember to stop, look, and think before taking any sort of action.

- Does this information I'm about to share really need to be shared?
- Am I suspicious of all unexpected messages and social media connection requests?
- Is this email real or a phishing attack? Phishing emails are disguised to look like they are from familiar contacts or organizations and try to trick you into taking an action like opening an infected attachment or clicking a malicious link.

TIP 9

Stay secure when working remotely from public places.

The security threats around you are much greater when you are away from your home or the office. Stay alert to your surroundings and don't take any unnecessary risks.

- Do I keep confidential information private by not discussing or working on it out in the open?
- Am I turning my internet connection off when I don't need to be online and using the VPN when I am online?
- Did I connect to the correct Wi-Fi network, not a fake one the bad guys created to trick me?

TIP 10

Know your organization's policies and procedures.

Beyond the first nine tips, making sure you know your organization's expectations when working from home is critical.

- Have I reviewed all of the appropriate policies and procedures my organization has in place related to working remotely?
- Do I know who to ask for assistance or clarification of these guidelines?

KnowBe4
Human error. Conquered.