

Working from Home - Staying Secure



Many people are enjoying the advantages of working from home. They can enjoy the much shorter no-stress morning and evening commutes, flexible working hours, a more relaxed working environment, and studies have shown a rise in productivity for these workers. These are all good things, but with these advantages and a more relaxed atmosphere, there is the possibility that cybersecurity and privacy may not be the priority

they should be. After all, you only need an internet connection to work and communicate with co-workers, and we are safe and sound in our own homes, but this is not the whole story.

First, consider your physical security.

It's still important, just like cybersecurity. Yes, you are in your own home where no one can see or access your files, computer or mobile devices like in an office. But unless you live alone, and no one ever comes to see you or comes

into your home for needed repairs, then there are other eyes and ears and possible access – husbands, wives, kids, friends, etc.

In that case, you need to protect sensitive files, computers and mobile devices like you would in the office. Don't leave your computer on and logged in while you run to the store. Always lock it when you step away and keep it off and secured when not using it. Don't let someone use your work computer to check their email or look something up on the internet. Sensitive files can't be left on the coffee table where you were reading them last night or on the printer where others can

continued on next page

SAFE: Security Awareness For Everyone

All information provided by WEST, a Williston Financial Group company

Provided by WFG National Title Corporate Marketing Department

west 
<protectSM

continued from previous page

read them. Any sensitive files should be secured when you are not working with them. You need to follow your organization's policies and processes at home to keep sensitive information protected and private, just like you would in the office.

Next, you should also think about who is listening.

Working in an office, we are aware that others are around and can hear what we say. We talk more quietly, or find an office or conference room or go outside to hold private conversations. At home, it's not a problem, right? But what about your always-listening devices (Google's Assistant, Apple's Siri, Amazon's Alexa, Microsoft's Cortana, and Facebook's Portal)? All of these devices are always listening to you. They have to, because they are waiting to hear their "wake word," like "Hey Google" or "Alexa," to let them know to start recording what they hear and send

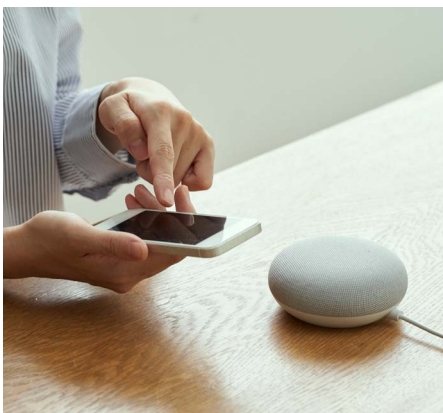


it to their servers (and the employees who are monitoring) so it can find out how to respond to you.

How many times have you, or someone you know, had the various devices answer you or respond to something else it has heard in the room, like the TV or a conversation you were having with someone else? Every time you get a response, it was listening, then recording and responding to what was being said. This is something to keep in mind while working from home. During phone calls and meetings, or any personal conversations you want to have, consider what will be discussed and what should remain private. Then

turn those services off that use a microphone, or disconnect them during your conversation or working hours. You can also view - or listen to - then delete past conversations that have been recorded in some of these apps, like Alexa and Google Assistant. You can easily find instructions for how to do this for all types of devices by searching online.

These are things to consider while working from home, including some actions you can take to be more secure while working but still enjoy all the benefits of those always-listening devices.



SAFE: Security Awareness For Everyone

All information provided by WEST, a Williston Financial Group company

Provided by WFG National Title Corporate Marketing Department

SAFE: Security Awareness For Everyone

The goal of any security awareness program is to provide people with information on threats they might not be aware of and the actionable steps they can take to recognize and react to them.

Cybersecurity threats are everywhere: scams, malicious software, intercepted emails, etc. This is what businesses like ours face every single day. Companies are targeted because of the valuable information they handle. Technology and processes are important, but they're not enough. Research shows that people are the weakest link and often the prime targets.

The SAFE program was launched - almost two years ago - to keep you informed, raise awareness, change behavior and provide the tools to defend against these threats. Your actions matter. Secure habits practiced daily can significantly strengthen your security, so spreading awareness and knowledge are key.

To this end, we will continue providing Tip Sheets monthly, the Advisor Newsletter quarterly, and Alert! notifications on urgent, important topics and news as they are needed. We also continue to celebrate Data Privacy Day every January and champion Cyber Security Awareness Month during October.

Let's make 2021 the most secure year yet for our work and personal lives. As we continue to provide you with the SAFE monthly and quarterly content, we encourage you to share these with anyone you feel could benefit from the tips, articles or alerts.

Happy Holidays!



SAFE: Security Awareness For Everyone

All information provided by WEST, a Williston Financial Group company

Provided by WFG National Title Corporate Marketing Department