Cyber Hygiene: Home Office Cybersecurity

It is easy to control security precautions when everyone was in the office. Working from home requires every employee to defend the company and stay safe from cyber crime. Here are some cyber safety habits and cyber breach signals to remember.

Home cybersecurity safety habits:

Separate work and personal

Best practice is to use your company provided device for work, keeping personal use separate. Since many remote workers are having to use their personal devise for work, stay safe by using a separate profile for work and personal. When you are "at work", log on under the work profile, switching profiles when you handle personal matters.

Lockdown your devices

Even though you feel safe in your home, you still need to protect the work on your physical device. Set a unique password for your device and lock it every time you walk away. This is good practice for after the quarantine as well.

Be wary of add-ons and downloads

There are many add-ons and extensions that promise to make something run faster, smoother and better. Be cautious of downloading these onto your device. Many contain malware that could lead back to your company network when you connect.

Use company approved sharing sites

With everyone working remotely, there is a greater need to communicate digitally. While it's easy to use what you're used to, make sure you send private data only through company approved sharing sites.

Cyber breach signals & solutions:

Increase in unwanted pop-ups

Pop-ups are a widely seen by-product of malware. You may have fallen prey to a phishing email or clicked a link while searching the web.

Processing slows down

Is it taking longer than usual for your computer to load? If there is a significant lag in your computer processing time, you might have a virus. They tend to slow your whole system because they are working on the back end of your computer.

New programs appear

Computers do not add content on their own. If a new program, app or internet add-on appears on your computer, you may have a virus that inserted content onto your computer.

How to handle a potential breach

1. Report it! - Inform your IT department of what you are experiencing, with screen shots of pop-ups and unwanted content.
2. Don't click - Never click on suspicious content. Malware is the gateway for a virus. Do not give them access!
3. Scan with anti-virus software - Company devices should be equipped with anti-virus software. If you are using a personal device, get with your IT department about having it installed on the computer you're using for work.
4. Don't access private data - Until the issue is resolved, do not attempt to access your company network or work on private data.

CyberCompass® SECURITY

CyberCompass navigates businesses to cyber resilience across their business ecosystem of their people, processes, technology and vendors. We are a one-stop solution for a cybersecurity, compliance and privacy program.