CYBERSECURITY TIPS FOR REMOTE WORK

As a result of the pandemic, many employees are now working remotely or in hybrid settings, which can create more security risks. Just like in a corporate office, employees working remotely need a set of cybersecurity standards. These guidelines can help keep remote work secure.

1 USE STRONG PASSWORDS.

Your password is the first line of defense. The weaker the password, the easier it is for intruders to gain access. Ensure strong, hard-to-crack passwords by using a reliable password manager tool or checking a website like Dashlane's How Secure Is My Password? tool.

2 AVOID PUBLIC NETWORKS.

When working from a public location, avoid using public WiFi. In many cases, these public networks may come with little or no security, allowing customers—and cybercriminals—easy access. If you must use one, check to see if the network is using WPA or WPA2 authentication (i.e., a password-protected network in which the encryption key constantly changes). Be careful with your home WiFi, too. Check online or the manufacturer's steps to secure your home's router.

3 USE A VPN.

If an intruder finds a way to gain access to your device, shielding any information from prying eyes will be paramount. That's where a virtual private network (VPN) comes in handy. VPNs encrypt your browsing history, making it virtually unreadable to cybercriminals and even your internet service provider. If you aren't already using a VPN on all computers, make it the new standard.

4 FOLLOW SECURITY PROTOCOLS.

Measures like firewalls, antivirus software, and email encryption are easy to take for granted, and consequently easy to forget. Most companies have strict protocols regarding the software that can be placed on your work devices. That is why it is imperative that you only use the tools that are provided or approved by your employer. This helps to safeguard company files and secure confidential information for clients and employees.

5 WATCH FOR PHISHING SCAMS.

Many bad actors use phishing emails or text messages to trick you into clicking a link or opening an attachment. They continually change their methods, so you must be vigilant. Look carefully to confirm the request is legitimate before you click or download.

6 KEEP WORK DEVICE SEPARATE.

Always use separate devices for personal and work tasks. This helps avoid compromising sensitive business data. Since employers are probably more aware of threats, they take more precautions than you would on a personal device. Plus, you are more likely to visit sites that are targeted by cybercriminals (e.g., social media and Netflix).

STAY VIGILANT!

*The most important factor in cybersecurity is **you**.*
If you don't follow best practices, all other measures are moot.

Balanced Equation is brought to you by
ACS Member Insurance
Protecting Life's Elements

THE BALANCED EQUATION
PRACTICAL ADVICE FOR A WELL-ROUNDED LIFE