Working From Home?

5 Tips to Stay Secure

By Judith Bitterli, VP of Consumer Marketing at McAfee on Mar 12, 2020

According to OWL Labs, 52% of the employees work from home (WFH) at least one day a week. In the U.S., 4.7 million employees now work from home more than half the time, with the work-from-home population growing by 173% since 2005.

Working from home – a new reality

It's evident that working from home has become a new reality for many, as more and more companies are encouraging and even requesting that their staff work remotely. In fact, recent events have accelerated this WFH trend, or workforce transformation process, with companies restricting employee travel and many allocating more resources to enable virtual work. Major tech players, like Twitter and LinkedIn, have made even bigger moves by implementing policies that require all employees to work from home. Clearly, work from home is no longer just an initiative to harness global talent but also a way to protect workers from risk.

Increased security risks

At McAfee, we're keeping a close eye on this trend, observing huge increases in the number of personal devices connecting online. And while working from home owners benefits to employees, this upswing in personal devices connecting to enterprises can actually expose organizations and employees to security risks, such as malware attacks, identity theft, and ransomware. With the world now facing this new reality, the question remains–how can employers and employees equip themselves with the resources to work from home securely on a full-time or part-time basis?

Work from home securely

Employers must not only educate their employees on digital security best practices but also give them the tools to combat online threats that may stem from remote work. With many of us relying on emails and the web to work remotely, we need to be aware of the key giveaway signs that indicate a threat. From there, we can spot, flag, and report anything that looks suspicious. By sharing the responsibility and encouraging others to flag anything sketchy, we can all naturally raise awareness and help others avoid falling into similar traps. By staying open with one another, we can stay ahead of hackers.

Tips to protect both personal and corporate data

Want to ensure you work from home in a safe and secure way? Here are a five quick tips and tools you can use to protect both personal and corporate data:

Utilize a VPN

Many people use public Wi-Fi at coffee shops, airports, etc. in order to stay connected both professionally and personally. However, by using an unsecured Wi-Fi connection, you may be creating an easy gateway for hackers to access your personal information and data. Be sure to use a virtual private network (VPN), which is extremely important for establishing a secured connection to work files and personal photos saved in the cloud.

Be aware of phishing emails

We've seen hackers attempt to take advantage of people's fears by pretending to sell face masks online to trick unsuspecting people into giving away their credit card details. Do not open any email attachments or click on any links that seem suspicious.

Regularly change cloud passwords with two-factor authentication

Two-factor authentication is a more secure way to access work applications. In addition to a password/username combo, you will be asked to verify who you are with a device that you–and only you—own, such as a mobile phone. Put simply: it uses two factors to confirm an identity. Ultimately, getting access to something supposedly confidential isn't that hard for hackers nowadays. However, a second form of identification makes it so hackers are limited in what they can pull off.

Use strong, unique passwords

In the chance a hacker does gain access to one of your accounts, make sure to use complex passwords for each of your accounts, and never reuse your credentials across different platforms. It's also a good idea to update your passwords consistently to further protect your data. You can also use a password manager, or a security solution that includes a password manager, to keep track of all your unique passwords.

Browse with security protection

Ensure that you continue to update your security solutions across all devices. This will help protect devices against malware, phishing attacks, and other threats, as well as help identify malicious websites while browsing.

Stay up-to-date

To stay on top of McAfee news and the latest consumer and mobile security threats, be sure to follow @McAfee_Home on Twitter, listen to our podcast Hackable?, and 'Like' us on Facebook.

McAfee | Small Business Security