NOVUS INSIGHT

# Staying Cyber Safe When Working From Home

Very few organizations are prepared for all or most of their employees to abruptly have to begin working from home. There are a number of challenges associated with it, none perhaps bigger than technology readiness. Cyber criminals love this type of disruption because they can more easily take advantage of vulnerabilities that present themselves. With even heavier reliance on IT systems to keep the business operating as normally as possible, an emphasis on cybersecurity plays a critical role in keeping these systems up and running. Here are some things to keep in mind as you establish this different way of working.

**Securing Remote Access** - It is risky and almost never a good idea to install VPN software on an employee's home computer for remote access to the corporate network. Most malware needs administrative rights in order to infect a system. So unless employees establish a secondary account (which home users almost never do for convenience reasons), the one account they use has administrative rights. If this account is compromised, an attacker can then use it to more easily penetrate the corporate network. Therefore, remote access should be restricted to company-issued and maintained computers.

> **Technical Note** - VPNs should be configured with "split tunneling" disabled. This allows for all traffic to be tunneled to the office network from the work device. It isolates the corporate network from the home network and prevents anything infected on the home network from having a path to the corporate network.

**Password Hygiene** - Home routers, WiFi access points, video game consoles, thermostats, internet-connected TVs, baby monitors, security cameras, even your car. All of these come with default passwords that many people don't change, even when strongly recommended to do so. This point should be continually reinforced with employees. Changing default passwords adds another layer of protection between an employee's home network and your organization's network.

**Phishing/Social Engineering** - Employees now working from home will be spending more time than ever online, which increases exposure to phishing and other social engineering attacks. Cyber criminals are opportunistic by nature and thrive on taking advantage of compromised business processes that occur in situations like we're in. Now is the time to reinforce company policies related to online activity, expectations for proper online etiquette, and general tips for staying safe while online. Particularly important is making it easy for them to report suspicious e-mails or other online activity. The more that is reported, the more that can be shared with other employees, and the lower your risk will be of a security incident occurring.

**Two-Factor Authentication (2FA)** – 2FA is a user or internet-connected device providing a 2nd level of authenticity when connecting to a network, one step beyond the standard username/password sign-on. It should be implemented whenever feasible as an important additional layer of security that makes compromising an account much more difficult for an attacker.

**Standard Operating Procedures** – Make sure important tasks that are done for the office environment can be done remotely as well. One example is remote monitoring and management of devices connected to the corporate network. This is software installed on each device that simplifies proactive monitoring and maintenance. It is also good for getting issues resolved before users even notice them.

**Patching** - Unpatched systems remain one of the primary routes an attacker takes to infiltrate an organization. Patches are small pieces of code that upgrade, optimize or further secure software. From a cybersecurity standpoint, not installing them is analogous to leaving your front door unlocked. Being diligent when it comes to patching (combined with employee awareness training) will improve your cybersecurity strength considerably.

**Home Wireless Network** - Change default admin password to a strong password and enable WPA2 encryption.

**Employee Training** – Reinforce expected employee behavior by holding cybersecurity awareness training sessions with content tailored for working at home. Simple reminders like never allowing kids on the work computer can have a meaningful impact.

**Threat Management** – If you have one, your IT team should be equipped with tools to adequately detect, protect and respond to threats in this new distributed work environment. Traditional tools used in the office such as firewall monitors are ineffective when the workforce is remote. IT teams should instead be deploying solutions such as Defender ATP and Cisco Umbrella to collect user's machine data and network data, proactively block threats, and apply filtering to content and applications.