Keeping Work from Home (WFM) Environments Safe

Home network safety probably isn't a top-of-the-list concern for most business leaders. If your business has any remote or hybrid employees, it should be. 2020 saw a huge surge in the number of remote workers across the country. Many ill-prepared businesses are now suffering the consequences. Helping employees learn how to secure home networks is a key piece of the security puzzle.

Like many small businesses, individuals in their home carry the mindset, "I'm too small for a cyberattack." This type of thinking contributes to the steadily rising numbers of individuals and businesses impacted by cybercrime every year. It is up to the company to ensure cybersecurity policies are in place that mitigate risks. It may also be necessary to provide your workforce with information and tips on how to comply with these policies. Help your employees learn how to secure home networks so their homes aren't a threat to your business.

How to Secure Home Networks

1. Install and Use a *Reputable* Antivirus Software

Every computer on the network should be utilizing AV software. There's an old wives' tale, maybe an old engineer's tale, about how Macs don't get viruses. It's both prolific and potentially harmful when believed. Macs require AV software built for the Mac OS. Be sure you're providing the right software to your workforce.

2. VPNs or Virtual Desktops Help Create a Sandbox Environment

Working from a VPN or virtual desktop creates what is known as a sandbox environment. These are not impenetrable, but they are a great security layer. Provide remote employees with one of these options and limit tool access outside of the office network to VPN or virtual desktop only.

3. Update Software Regularly

Those pesky Windows and Mac updates bring vital patches to operating systems which help secure vulnerabilities before threat actors penetrate the weak spots. Employees should be made to make sure their home based systems used as vehicles to attach to the office systems are ALWAYS patched – both AV and OS.

4. Don't Use Devices Past End of Service Life

Using devices that are no longer supported and patched by their manufacturer poses a huge risk to both business and personal data. Understanding threats facing end of life devices is vital to every company's cybersecurity effort. A good asset management plan will assist in this area.

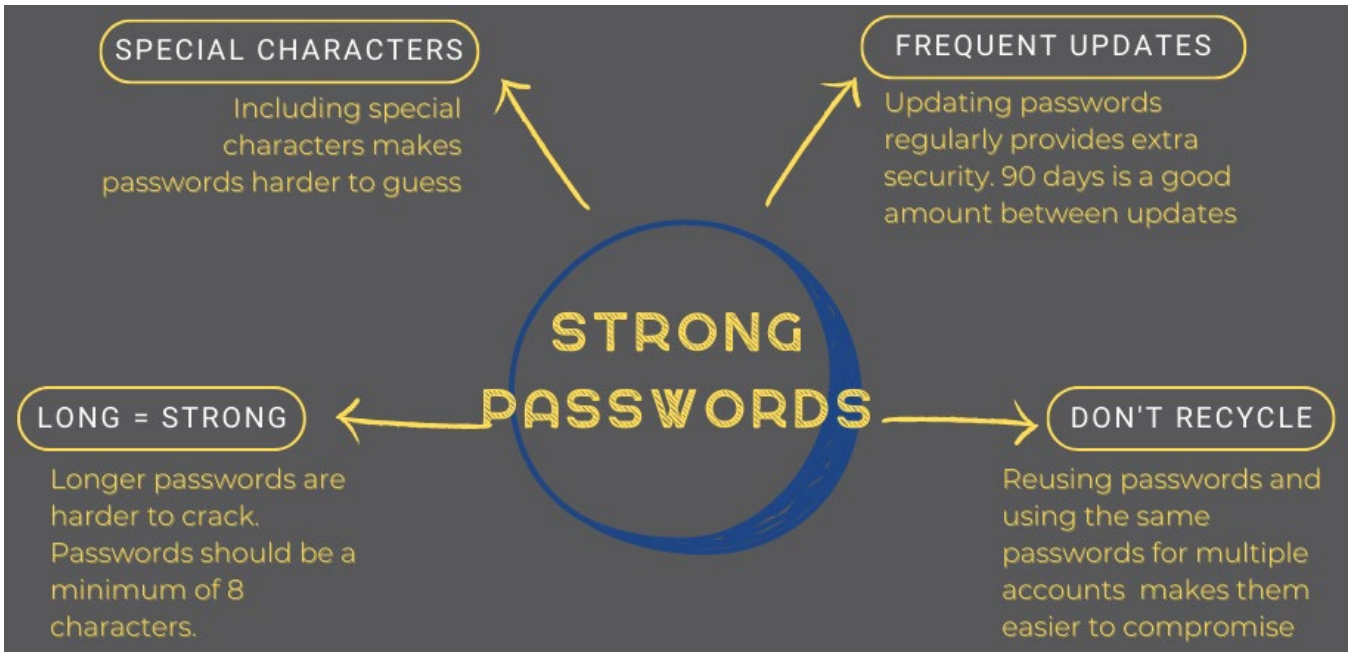
June 2024

5. Set Up a Firewall

Many devices come with firewalls, often they're on out of the box. We recommend ensuring that both the network and the devices on the network have firewalls enabled. Creating multiple layers of security makes networks much harder to penetrate.

6. Use Strong, Unique Passwords

Strong, unique, frequently updated passwords are an essential defense component for businesses and individuals alike. Passwords should not include personal details because they're easily guessed. Ensure that your employees update passwords every 180 days or less and require multi-factor authentication.



7. Secure Modems, Routers, and Their Networks

Securing networks is a basic step that every internet service provider (ISP) both recommends and, in most cases, assists in completing. Wi-Fi passwords should be strong and unique just like all other passwords. Securing modems and routers is a slightly different story. Modems and routers contain a gateway which allows access to the device by a computer. This is where users will change settings, set up network security, and maintain the interface. Ensuring the gateways are password protected creates another small layer to secure home networks. These devices often come with very generic usernames and passwords which makes them easy to gain access to. Strong, unique passwords are key!

8. Inbox Hygiene

Reducing the amount of spam coming to an inbox reduces the risk that an employee will click on or open something malicious. Ensure that your employees mark spam in their email clients. Your I.T. support group should set up a way to report suspicious or malicious looking messages and encourage employees to use this tool.

9. Train Employees on Cybersecurity Best Practices and Policies

Training your employees allows them to take an active part in defending against cyberthreats both for your business and in their personal lives. Set up regular and dynamic cybersecurity training to keep knowledge fresh. Programs such as KnowBe4; Ninjio; TitanHQ; and Wizer may be some good options to look at.

10. Hire a Reputable I.T. support group / Managed Service Provider (MSP)

Having the right people around makes all the difference. Hire a team of I.T. professionals to help you create impactful policies, train employees, and secure networks and devices. There is no governmental oversight currently on I.T. professionals or companies. Do your research, ask questions, get references. Hiring the wrong company or individual could cost you big. For an updated list of suggested IT vendors, you can always visit the AoA IT Dept.'s helpdesk and download a copy of the most recent listing.

Convenience Should Never Take Priority Over Security !!

An additional item to consider for both remote and in-house employees is permissions. Cloud computing has created increased vulnerabilities for many companies.

Improper authorization, where organization-wide access and/or administrative controls are granted to an individual that has no need for such permissions, can be a huge problem. 99% of your company does not need administrative access to their computers or your network, including C level. While it may seem more practical to allow "trusted" individuals to have certain permissions, unless their job requires it, they don't need them.

The importance of working from secure environments cannot be overstated. Cybercrime is a growing threat that every company, and individual, should take seriously. Ensure you take the proper steps to educate your remote workers on how to secure a home network. Express the importance of security to staff on a regular basis, regardless of where they work. No organization is completely safe from cybercrime but that doesn't mean your organization should be an easy target.