Small/Medium Business (SMBs) Guide to Safe Remote Work

First, separate your business into two groups: on-premises and remote workers. Enable remote work policies for all non-necessary people (and those whose immune systems are weakened) and establish a clean office environment for those who must remain.

For those working remotely, several crucial things must be done. This group will be accessing data outside of the primary company connection for extended periods, so securing the corporate device (as well as its connection to the internet) is crucial.

Working around pandemics is a new thing, so most SMBs in particular are only recently thinking about what to do when *requiring* employees to be away from the office…but still meeting the need to protect the company device, data, and connection to the internet.

Tips for securing remote workers

1. **Use a secure VPN.**

It is not just about company device cybersecurity, but about protecting that device's connection to the internet while it is dealing with company data. It is crucial to select a VPN that encrypts data. It is extra-important to verify because a connection leak of corporate data could still bring the same disaster with leaked intellectual property.

2. **Update everything.**

Take a moment for updating each device, and then schedule a weekly reminder on your company calendar. Exploiting late patches is one of the main ways to snag corporate data through a malware attack, so it is worth a checkbox on the list of things to do during remote work.

3. **Use laptops as a standard user, not an admin.**

If something or someone does take control of a company device but logged in as a standard user, they will not be able to do nearly the same kind of damage as an administrator and will be much less able to launch an attack at the company.

4. **Enable MFA on everything that supports it.**

If malicious actors cannot get into the account itself without the second piece of verification, an attacker will not be able to impersonate a user in the first place. Multi-factor authentication (MFA) is the best way to lock down identity management at home and at the office.

5. **Create a separate VLAN.**

Put your work devices in their own virtual network to contain any damage that might come should your work device be attacked. That way, the infection does not spread onto the home Wi-Fi network onto any personal devices connected at the residence. In addition, it is easier to shut down access to just one piece of your network rather than disabling your entire Wi-Fi network during a malware attack.

6. **Beware of current events in the inbox.**

The Coronavirus is often used as phish-bait. Some emails claim to be from the World Health Organization; others from the CDC. They all want you and your employees to click during a weak moment.

Tips for on-premises workers

For those in the office, here are the basics for a cleaner business:

- **Sanitize the most common surfaces** at the close of your business day, preferably when there are few or no people around. Do not rely on your facilities staff or cleaners for this part.
- **Dispose of all garbage outside of the office** (including cleaning waste) at the end of the business day.
- **Sanitize your keyboard/laptop/phone right before you leave** at the end of the business day, put them in your bag, and then do not touch them again while you are on the premises.
- **Sanitize your hands right after leaving** the office. Break the habit of face touching.
- **Do not lick envelopes** to seal office mail. Use a moist sponge or paper towel.
- **Plan for decreased productivity** should staff be ill.