Work From Home Security Checklist

The current crisis has hackers licking their chops and looking for opportunities to crack the cyber defenses of businesses worldwide. There are already numerous examples of scams specifically related to the Coronavirus, and more are on their way.

The checklist below is designed to help you ensure that you and your employees are following cyber security best practices while working from home.

Employer	Employee
☐ Use your company computer – not your home computer. If you have an IT provider, ask them to make sure this machine has security protections in place. And don't let anyone else use it including your kids, spouse or friends.	☐ Ask your employees to work from their work computers, and ensure they know not to use work computers for personal tasks.
☐ Don't use your work computer for personal tasks. Surf the web, do your online shopping and check social media on personal devices only.	☐ Develop an Acceptable Use Policy and Work from Home policy to clarify what employees can and cannot do with work machines. This is a must.
☐ Log out of company applications when you are done using them.	☐ Implement Multi Factor Authentication (MFA) on any accounts that offer it. This is a significant step in reducing your vulnerability.
☐ Store your passwords in a password management application. They are secure, encrypted, and there are lots of free options.	☐ Give only relevant employees access to confidential company data. The more people accessing your data, the higher your chances of being breached.
☐ Ensure you are connecting to your office network using either a secure VPN, remote connection software, or cloud-based solution.	☐ Encrypt your hard drives. Your IT provider can help you do this.
☐ Keep your devices safe. Log out when you are done for the day, lock your office door if possible, never leave your device in the car, and turn on any "find my device" features.	☐ Keep your devices safe. Log out when you are done for the day, lock your office door if possible, never leave your device in the car, and turn on any "find my device" features.
☐ Be educated. Stay up-to-date on common phishing schemes and cyber-attacks. Knowledge is power!	☐ Offer your employees a cyber security training solution. There are lots of options, so if you want to learn more just let us know.
☐ Be skeptical. If something seems off, it probably is. If you're concerned that you have experienced a cyber security incident, let your IT provider know ASAP.	☐ Be skeptical. If something seems off it probably is. If you're concerned that you, or one of your employees, have experienced a cyber security incident, let your IT provider know ASAP.

if you are looking to implement an Acceptable Use Policy (AUP), or a Work from Home Policy, we've put together templates and checklists that you can use a guide. If you would like a copy of either document, or you have questions about securing your business, we're here to help. Just call us or send us an email and someone will be in touch with you soon.