



Protect Your Business

Though you can't eliminate cyber threats entirely, there is a lot you can do to mitigate them

☐ HIRE A CYBERSECURITY FIRM.

The best defense against a cyberattack can be hiring a cybersecurity firm to check that your hardware, firewall, and router are up to date. They can test your system by trying to break in the same way a cybercriminal might and help you plug any holes that they detect.

☐ THINK BEFORE YOU CLICK.

To avoid phishing attacks that can infect your system with malware or ransomware, no one at your business should click on hyperlinks in any suspect e-mail without being very sure the communication is from a person or company they trust. Even if an e-mail seems legitimate at first, check that it has not been spoofed by looking for unfamiliar or foreign domain names, misspellings, or other anomalies.

☐ USE STRONG PASSWORDS.

The best passwords are long and complex, so skip your children's birthdays and pet names. Ideally, passwords should be at least 12 characters long. Also, never save it as part of an automated password prompt and be sure to change it every few months.

☐ USE MULTIFACTOR AUTHENTICATION.

This requires users of your system to identify themselves by more than a username and password. Usually this is done by sending the user a four-to-eight-digit code via SMS or e-mail that they then must enter to gain access. While it entails an extra step, it adds an extra level of protection to your system.

☐ HAVE AN OFFLINE BACKUP.

In ransomware attacks, cybercriminals will look for and destroy backup systems, which is why it's critical that yours is offline when not being used. If an attack occurs, you can use your backup to restore the system without having to pay the ransom.

☐ UPDATE AND PATCH YOUR SYSTEM.

Software developers regularly release security updates and patches that can help protect your software from attack, if you've updated your system. Sign up for notifications from the developers and then take the time to download and install any updates or patches.

☐ INVEST IN AN ANTIVIRUS PROGRAM.

Install and keep your antivirus and antimalware software current. Cybercriminals have developed sophisticated malware designed to evade older antivirus software. These programs are constantly updated to scan for the latest threats.

☐ OBTAIN CYBER INSURANCE.

Though you may think your business too small to be a target of cybercriminals, your system could be used as a gateway to access the systems of other companies with which you do business. To help protect your company, invest in a cybercrime insurance policy that will cover losses in the event of an attack, as well as providing assistance with cleaning up and securing your system to prevent future attacks. ♦