

Cyber Check

Eight ways to protect your small business

It can feel overwhelming to try and keep up with cyber trends and stay aware of new threats – especially while running a business. Here are nine tips to help protect you and your operation:

☐ Train your employees

Education is key when it comes to security. Regular training and refresher sessions are a great way to get your employees familiar with the basics:

- Look out for *suspicious emails* with urgent, fear-inducing subject lines, or updates from scammers posing as someone from your company. Not sure? Don't click.
- Never provide your login information, financial account or allow access to your devices to someone over the phone, unless you've confirmed the request is from a trusted source.
- Require employees to create strong passwords, such as a phrase containing random words or letters.
- Share protocol for how to report and respond to a suspected incident, such as ransomware or email compromise.
- Make sure employees understand your policy for computer access and using their own devices.

☐ Protect against viruses, spyware and other malicious code

Use anti-virus and anti-spyware software, and ensure that all software installed on your network is regularly updated. Putting off installing updates on your computer and phone software can expose your business to cyber attacks.

Use a web filtering service or technology that prevents traffic to malicious or suspicious sites.

☐ Back up your data

Be sure to back up your data so you can access it outside of your system in case you are hit by a cyber attack. It doesn't matter whether data is stored in the cloud, on-premises, or in a hybrid data center, businesses should back up all files to media that is not connected to the Internet.

☐ Create strong passwords and authentication

Use complex, hard-to-guess passwords that contain random words, a combination of capital and lowercase letters, numbers and symbols. Change passwords frequently or use a password manager and multi-factor authentication.

☐ Secure your Wi-Fi networks

Your Wi-Fi should be secured with a password - ideally one that is longer than 12 characters and uses a combination of numbers, letters and symbols.

Change the password on your Wi-Fi network away from the default, and if you provide guests access to Wi-Fi make sure they cannot access your employee network.

☐ Use trusted POS vendors

Choose an established bank or processor who uses the most secure tools and anti-fraud services. Isolate your payment systems from other systems in your operation, and ensure all remote access by your POS service provider is authenticated and logged.

☐ Provide firewall security for Internet connection

A firewall is a set of related programs that prevents outsiders from accessing data on a private network. Make sure your operating system's firewall is enabled and properly configured. If your employees work from home, ensure their home systems are also protected by a firewall.

☐ Control access to computers

Regulate physical access to your computers and create a user account for each employee. Keep mobile devices and laptops locked up or protected by passwords when unattended. Limit administrative access to servers and software to employees who require it for their job.

If you think you've been hacked, act

If you believe your organization has experienced a breach, please *reach out to your broker*. They will work with you to understand the extent and scope of the breach, review your coverage, and assist you if you need to submit a claim.

Find out if Wawanesa Cyber Coverage is right for your business.

Wawanesa is providing this information based on industry best practices to help protect against cyber threats. While there's no guarantee you or your team won't be the victim of a security breach, these tips can make you a less attractive target to cybercriminals and may mitigate any potential damage.

v.102021