sovereign®
INSURANCE

10 tips to enhance your business's cyber security

Considering the growing shift towards online business operations, it's becoming increasingly vital for small and medium-sized businesses to prioritize cyber security. Here are ten tips to enhance your business's cyber security:

1. Take stock of assets

Create a company asset inventory list for all company assets to monitor in event of a cyber security incident, such as physical devices (desktop computers, laptops, serves, mobile devices), physical peripherals (printers, monitors, keyboards), connected devices (POS systems, thermostats, security systems), physical storage devices (external hard drives, USB keys) and digital assets (social media accounts, websites, cloud services).

2. Secure your accounts and devices

Monitor which devices have access to customer data, business financial data and proprietary data. Ensure that access to programs, software, sensitive information is limited to those who have business need. Use unique passwords for every business device and account. Enable multi-factor authentication (MFA) on accounts where it's available. To maintain software security, use legitimate versions from reputable vendors. If your business uses a web hosting service for your website, make sure they have a security plan and monitor your website regularly. If you rely on an electronic point-of-sale (POS) system, ensure that it's behind a firewall, set up encryption, have a unique password, limit access to authorized employees, and keep your anti-virus and anti-malware software up to date.

3. Secure your network

Cyber criminals can attack your network to steal data and perform other malicious activity. Protect your network with firewall and anti-virus software. A virtual private network (VPN) can help to secure your business's information between your devices and the internet. Take steps to secure your Wi-Fi network by creating a network name that doesn't use personal information, along with a unique password. Avoid connecting to open, free Wi-Fi connections unless they are secured with a password and encryption.

4. Develop a backup system

If you need to quickly recover damaged or loss of data due to a cyber attack, you should back up your data on more than one system. To store back-ups in a secure and easy to recover way, you can use cloud storage, external hard drives, external storage such as USB key. Protect your backup system with strong passwords and encryption. Remember to disconnect external storage devices. Set yourself reminders to back up your data weekly.

5. Protect customer and sensitive data

A breach in your cyber security systems could mean the loss of your customers' information, such as customer data, financial data, employee data and proprietary data. Save customer and sensitive data on online databases or on your backup devices, but make sure where you store data is encrypted, and secured with a strong password. If you use a web hosting service or e-commerce platform, select the highest security level you can afford.

6. Enable automatic updates

Update your device operating systems and applications regularly and install security patches. You can enable your devices and software to update automatically or set updates for a time when systems aren't as actively used, such as overnight. If automatic updates aren't available, install updates as soon as you are prompted.

7. Develop a cyber security plan

Create a cyber security plan that details procedures for day-to-day operation that employees need to follow. This plan can include an internet usage policy, rules for email and messaging safety, a social media policy, a bring your own device (BYOD), telework plan, and a employee departure plan. Remember to update the cyber security plan with the latest cyber threats and information.

8. Train employees

Cyber security requires the effort of all employees. One employee's mistake could lead to a virus being installed on a work device and infecting your entire system. It's important to establish cyber security as a fundamental part of your business so that employees understand their impact on cyber security from a personal and business standpoint. Clearly communicate your business's cyber security plan and develop training and awareness programs for employees.

9. Establish an incident response plan

If something unexpected occurs, it's important to establish an incident response plan. Consider including the following steps when creating your incident response plan: detection, respond, and recover. The detection section can include details on how and who should employees report a cyber security issue to, what internal and external partners do you need to notify and how you might communicate the incident publicly. The respond section of the plan can include details on disconnecting devices from the network, suspending employee access temporarily to address the issue, change any affected passwords and enable MFA, and seek professional services to resolve the issue if necessary. The recover section can include information on restoring your system from a backup, updating all software, anti-virus, firewall and firmware once your system is running again, run anti-malware and anti-virus software on all connected devices and identify flaws in your cyber security plan that led to the attack and adjust the plan. Test your response plan through checklists, walkthroughs, simulations and system tests.

10. Stay up to date

The cyber threat landscape is evolving with new vulnerabilities being discovered and new tactics being discovered. You can keep your organization up to date and aware of current cyber threats by keeping up with news, alerts and resources provided by the Get Cyber Safe public awareness campaign and the Canadian Centre for Cyber Security.

Source: "Ten steps to mitigate risks". Get Cyber Safe – Government of Canada. Retrieved on October 3, 2024. https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-guide-small-businesses#C

sovereign® INSURANCE