MySchool® Insurance Program Newsline

MAY 2021

4 ways to lockout cybercriminals and protect your business

You don't let strangers walk through the front door of your daycare or private school; but, are you unintentionally letting in cybercriminals?

Small businesses with limited IT security resources are often easy targets for cybercriminals. Follow these four cybersecurity tips to protect your business and the privacy of your staff, clients and vendors:

1 Train your employees

Human error is the number one cyber threat that businesses face. The wrong click on a phishing email can download a malicious file, putting your business and sensitive data at risk—even when you're on a mobile device!

Your first defence against a cyberattack is to teach all employees common red flags:

- **Suspicious subject line or sender?** Don't click!
- **Legitimate email address or URL?** Hover your mouse over the address to look for extra words or different extensions; for example, the URL or email ends in .ca when it should be .com.
- **Is the attachment an executable file?** Cybercriminals often hide malware in executable files, which end with extensions such as .exe, .scr or .bat.
- **When in doubt, delete the email** and call the sender to verify their communication. If the email was legitimate, they'll applaud your caution and resend their message.

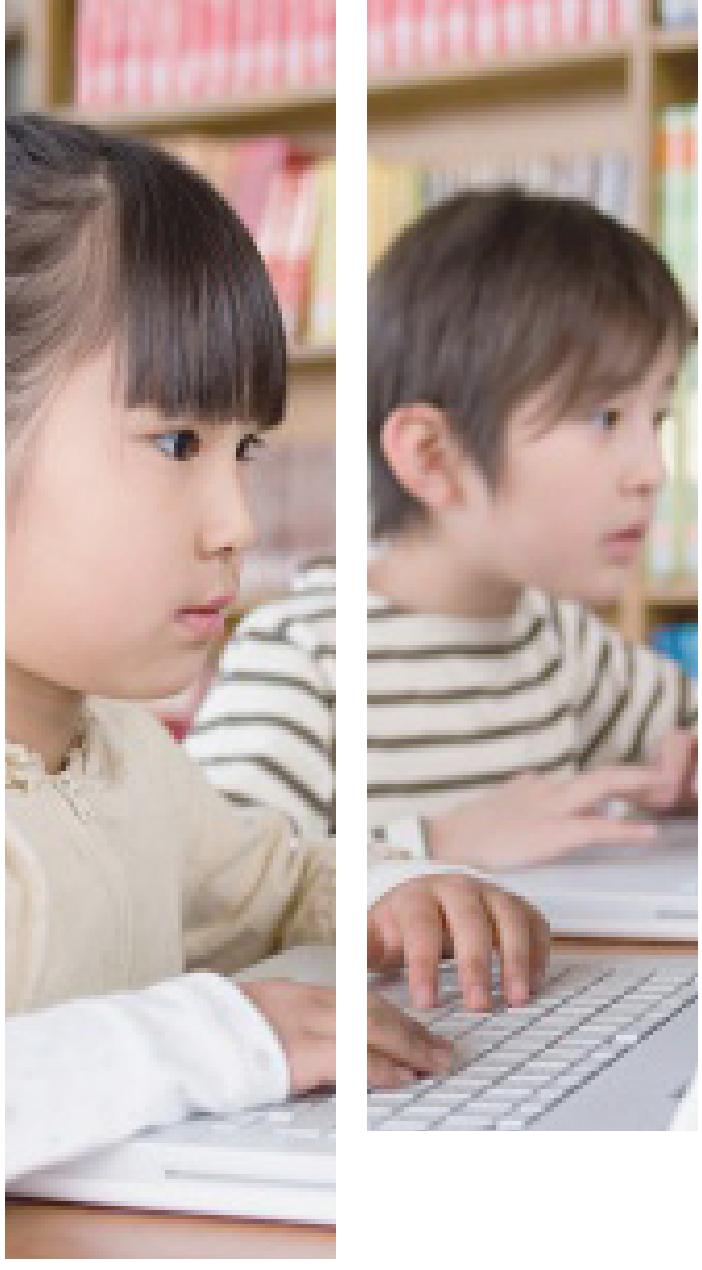
1 in 5 small businesses will experience a cyberattack.

2 CREATE STRONG PASSWORDS

Your business has a high-grade lock and alarm, but what about your passwords? Strong passwords are not a pain in the neck—they are vital to keeping cybercriminals out of your computers, mobile devices and company data!

Here are three ways to create strong passwords:

- **Use a passphrase,** which is a combination of words with special characters mixed in. You should also mix lowercase and uppercase letters. For example: oNe#tWo@tHreE
- **Don't use the same password multiple times.** Create distinct passwords for every site and application.
- **Regularly update your passwords.** Don't wait for an attempted or successful cyber breach before updating passwords. All employees should do this every couple of months.



3 UPDATE SOFTWARE & ANTI-VIRUS PROTECTION

Cybercriminals are constantly adapting, and updates are released to stay ahead of these changing threats. Are you regularly updating your devices, including mobile phones? If not, you're putting your business at a higher risk of a cyber-attack.

As new versions become available, make sure to update your:

- Operating system
- Software and apps
- Anti-virus / firewall protection

Two-factor authentication

is a best practice. This requires employees to enter their password and then verify the login through a secondary system, such as an authenticator app on their smartphone. This is highly recommended for networked businesses.

4 INVEST IN CYBER COVERAGE

When it comes to cybercrime, it's not a matter of if but when. Your cyber liability insurer can work with your IT team to respond and recover in the event of a cyber breach.

Does your IT contract include resources to respond to a cyberattack, including extortion payments, lost business income and notifying affected clients?

Fortunately, cyber liability insurance can cover:

- expenses to fight and recover from a cyber attack, such as IT forensics, data recovery and system repair;
- losses related to social engineering, and telephone or electronic fraud;
- cyber ransom negotiations and arrangement of payments;
- lost income if your business must temporarily close;
- expenses to notify regulators and parties whose private data was stolen from your electronic or paper files;
- legal costs if a client claims to have suffered financially as a result of the breach; and,
- costs to manage and mitigate reputational damage.

Helping you navigate

the hard insurance market

Catastrophic weather events, increasing material costs, labour shortages and COVID-19 have impacted businesses in many ways, including insurance companies. In response to these challenges, insurers are increasing rates and deductibles and rethinking their appetite for certain classes of business.

CCV and the MySchool Insurance Program have been serving the childcare and private school sector for more than 30 years. You can trust the MySchool team to leverage our expertise and size to negotiate the best coverage and rates for your childcare business or private school.

Protect your company from cybercrime for less than a **cup of coffee a day!**

Most traditional commercial insurance policies only protect physical assets. Adding cyber liability insurance can protect your business from privacy breaches and cyberattacks.

Contact the MySchool team today!
1.800.461.8562 or myschool@ccvinsurance.com

CCV INSURANCE & FINANCIAL a division of Rogers Insurance Canada Ltd.
MySchool Insurance Program
Proudly serving the members of:
The Association of Day Care Operators of Ontario
CCMA
OFIS Ontario Federation of Independent Schools