

Canadian Small Business Cyber Survival Guide



By John Hewie, National Security Officer, Microsoft Canada

According to a [report](#) from Innovation, Science and Economic Development Canada, almost 98 per cent of all employers in the country are small businesses. They are a big part of our national economy employing approximately 9.7 million Canadians. Over the past two and a half years, small businesses have endured a number of challenges. Many have demonstrated resilience by adopting technology that allowed them to reach their customers online, improve their operations and stay competitive.

Today, businesses of all sizes must continue to be vigilant to cyber attacks. The cybercriminals have professionalized considerably in recent years improving their ability to target small and medium sized businesses at scale. This includes making it easier for more criminals with limited technical skills to illegally profit from cybercrime. Techniques such as ransomware, business email compromise (BEC) and other fraud schemes are now commonplace even for Canadian non-profit organizations with a handful of employees. Canadian law enforcement is taking steps to combat these threats, but since most cybercrime operations are launched from overseas in countries where risk of prosecution is low, their capabilities have limits.

According to a [survey](#) from the Insurance Bureau of Canada (IBC), almost half (47 percent) of Canadian small businesses do not allocate any portion of their annual operating budget to cyber security. The same study found that 41 percent of small businesses that suffered a cyber attack reported **that it cost them at least \$100,000.**

The stakes are high for businesses when it comes to cyber attacks with profits, sensitive information, customer data and brand reputation all on the line. We know it is often cost prohibitive to have an in-house IT or security expert on staff for small businesses. But what we know about cybercriminals is that they're opportunistic. They typically look to exploit organizations with minimal security controls because it is cheap and easy for them. So with basic security hygiene, businesses can protect against [98% of cyber attacks](#).

Prioritizing foundational cyber best practices can prevent the most common types of attacks. Let's look at what these mean for a small business and make them practical to implement. Small businesses using

Microsoft 365 are also encouraged to review their personalized [Secure Score](#) dashboard and prioritized list of recommended security configuration actions.

Protect your accounts

Cybercriminals typically don't "break in", they "log in" by either guessing your password or tricking you to give up your password through a phishing attack. Enable [Two-Step Verification](#) or [Multi-Factor Authentication](#) (MFA) on all of your important accounts. This single action prevents the vast majority of account compromises Microsoft sees in its online services, even with continued use of weak passwords. Most cloud services and devices offer MFA options today and should be enabled wherever possible. Use an authenticator app such as [Microsoft Authenticator](#) over SMS one-time codes if available.

Creating and remembering passwords can seem like a full-time job. While Microsoft offers [passwordless](#) options for some services, the reality today is we still need to manage a lot of passwords. Using a password manager to ensure each user account (or at least the important ones) has a complex and unique password is a must for any small business, especially if an account doesn't support MFA. More info on what to look for in password managers can be found at [GetCyberSafe](#). [Microsoft Edge](#) enables you to [manage multiple passwords and offers a built-in password generator](#) with the ability to sync to mobile devices. Password managers require a master password so make sure it is strong and you protect it well.

Keep up to date

Reduce the risk of malware that exploits software vulnerabilities by ensuring your organization's devices and any infrastructure and applications maintain the latest vendor provided software updates. Windows PCs, Macs, iPhones, Android phones and network routers all get frequent vendor updates. Don't defer these updates as it may put your device at risk from malware. Attackers reverse engineer vendor security updates and develop malware to target unpatched applications and devices quickly. A device management solution such as [Microsoft Intune](#) makes this process easier. If you are still running Windows 10, consider the free upgrade to Windows 11 to take advantage of many [new security features](#).

Antivirus and antimalware defences

The built in [Microsoft Defender](#) next generation antivirus and malware defence capabilities are core to Windows 10 and 11, turned on by default and may be all a small business requires in terms of endpoint protection. [Microsoft Edge](#) has a host of [security and privacy features](#) such as [SmartScreen](#), which helps users avoid phishing and malware while browsing by blocking known bad sites and files.

Backup your important data

Cloud storage such as [Microsoft OneDrive](#) is a great solution to back up your important files. If you lose your device, you won't lose your important files and photos. OneDrive has a recycle bin to recover from those accidental deletions and Windows Defender and OneDrive work together to help [detect and recover from ransomware](#). There is also a [Personal Vault](#) feature to provide added protection for your most sensitive personal information. An offline backup copy of your most important data is also always good practice as a last resort if you need to recover your files. External USB hard drives that stay disconnected when not in use are an inexpensive option but should be tested regularly since storage media can be prone to failure over time.

Foster cybersecurity culture within your small business

Employees are your first line of defense and boosting or enhancing end user knowledge on security threats can go a long way to help reduce the risk of data exposure to phishing and other cyber attacks. Basic [phishing awareness](#) should be at the top of your training list while also educating users about suspicious websites and installing unapproved apps or free software on work devices. To support you in your cybersecurity awareness training, Microsoft offers a [Cyber Smart Kit](#) with helpful videos and infographics as well as [self paced learning modules](#) to teach key cybersecurity concepts. The Government of Canada also provides many resources at [GetCyberSafe.gc.ca](#). If your organization uses Microsoft 365, you can also deploy a security awareness training program with [Attack simulation training](#), a premium feature of Microsoft Defender for Office. Attack simulation training provides personalized and targeted phishing training and is available in over 30 languages.

BONUS: Enhancing your Small Business Network Security

A relatively easy way to add an additional layer of security for your local small business network is to configure your network router to use a domain name server (DNS) service that blocks access to known malicious domains. When you configure this once on your network router, all devices that use your small business network benefit. Review the privacy policies when choosing a DNS provider to ensure it aligns with how you might want your internet usage data being used.

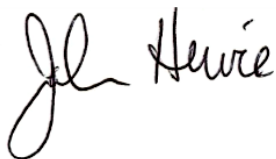
Report cybercrime and fraud

Only a small percentage of cybercrimes or frauds are reported to police in Canada, making it difficult for law enforcement to keep up with the ever-changing threat landscape.

1. If you have been a victim of a scam, fraud or cybercrime, please contact your local police as soon as possible. The Canadian Center for Cybersecurity provides detailed instructions and what to expect [here](#).
2. Consider reporting attempted scams or fraud to the Canadian Anti-Fraud Centre [here](#). Reporting may help link multiple crimes together and contribute to further investments in Canada to combat cybercrime.

Avoid becoming a victim of a cyber attack

An attempted cyber attack against Canadian small businesses is inevitable in today's world, but that doesn't mean organizations need to become victims. Committing to applying the cyber best practices outlined above can help protect your small business against most cyber attacks.



National Security Officer

