CyberShield

Premier Cybersecurity Newsletter for Canadian SMEs

TLP CLEAR **Issue 1, October 2024**

Welcome to the First Edition of the CyberShield!

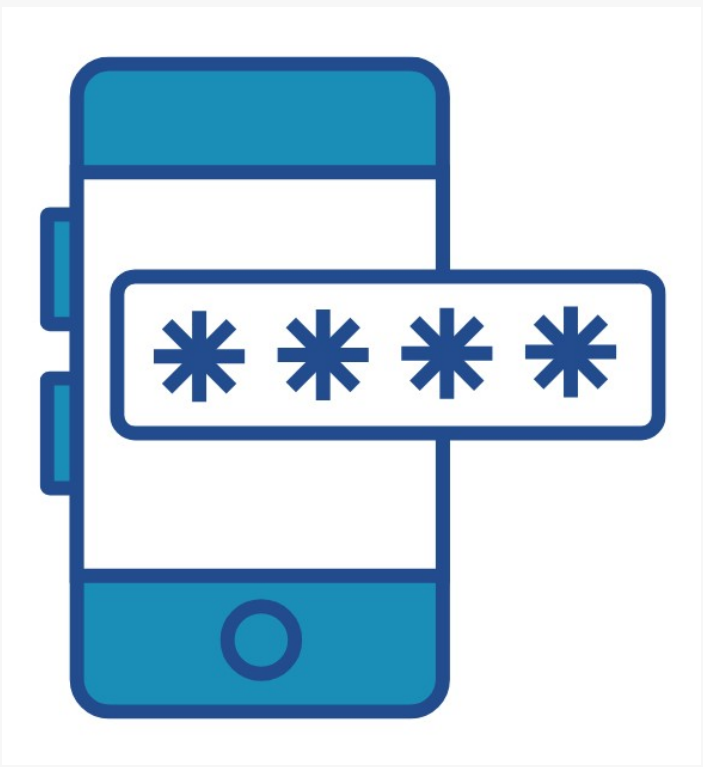
Subject: Protect Your Business This Cybersecurity Awareness Month.

October is Cybersecurity Awareness Month, and there's no better time to ensure your business is protected against cyber threats. At the Canadian Cyber Threat Exchange (CCTX), we understand the unique challenges small and medium-sized enterprises (SMEs) face in today's digital landscape.

With CyberShield, we'll share the latest threats, and valuable tips and insights every few weeks so you can stay on top of cybersecurity. We will not reinvent the wheel with this help! There is lots of useful information out there and we'll help you find and understand it. Please share this with your network if you find it useful.

Why Cybersecurity Matters for your Business

Cybersecurity isn't just about protecting data; it's about safeguarding your business's reputation and ensuring smooth operations. A single breach can have serious financial and reputational consequences. By staying informed and proactive, you can reduce risks and build a stronger, more resilient business.



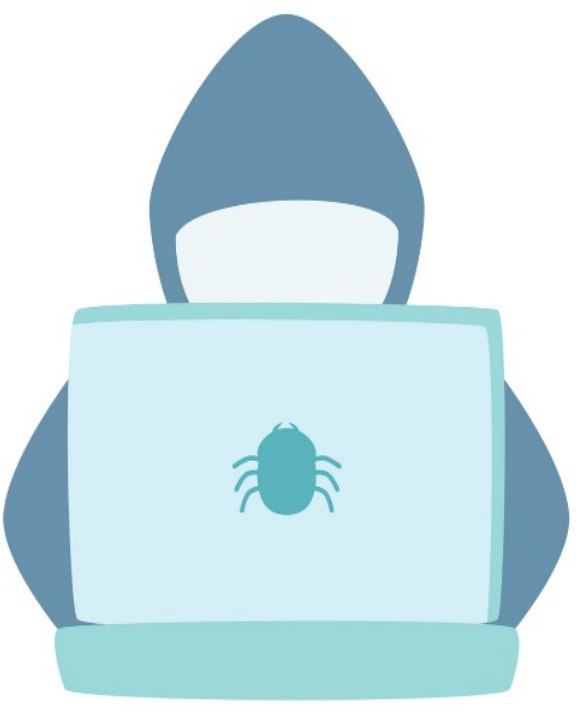
Top Cybersecurity Tips for SMEs

- Keep Software Updated: Regularly update all your software to protect against known security issues.
- Use Strong Passwords: Encourage the use of complex passwords and multifactor authentication (MFA) to add an extra layer of security.
- Train Your Team: Regularly educate your employees on cybersecurity best practices and how to recognize potential threats.

For support with these tips, consider **getcybersafe.gc.ca**

Current Cybersecurity Trends

- **Ransomware Attacks:** These attacks are on the rise. Ensure your data is backed up regularly and train your employees to recognize phishing attempts.
- **Fake Invoice Scam:** Scammers send fake invoices via email, pretending to be from known companies, and instruct businesses to redirect payments to a new account. These invoices often look legitimate and use urgent language to pressure quick payments. Always verify payment changes directly with the company, use security measures, and educate employees to recognize and report suspicious emails.
- **Business Email Compromise (BEC):** A BEC scam involves criminals impersonating senior executives via email to trick employees into transferring money to fraudulent accounts. They use social engineering and research to craft credible emails. Suggestion: Verify email requests for money transfers directly with the executive and implement multi-factor authentication and employee training to recognize such scams.



For more on these types of scams consider: rbc.com/cyber-security

Join Us in Creating a Safer Digital Environment

Stay tuned for more updates and tips in our upcoming newsletters. Together, we can create a safer digital environment for Canadian SMEs. If you have any specific topics, you'd like us to cover in future newsletters, feel free to reach out!

Thank you for being part of Canada's cybersecurity community.

Best regards,
The CCTX Team
info@cctx.ca