CyberShield

Premier Cybersecurity Newsletter for Canadian SMEs

TLP CLEAR **Issue 2, November 2024**

Welcome to the Second Edition of the CyberShield!

At the Canadian Cyber Threat Exchange (CCTX), we continue to prioritize cybersecurity for small and medium-sized enterprises (SMEs) in Canada. In this edition, we focus on a critical threat: phishing attacks. Stay informed and proactive with our tips and insights to protect your business.

INSIDE

Understanding Phishing Attacks

- What is Phishing?
- Common Tactics Used by Phishers

Phishing Prevention Tips

- Educate Your Team
- Implement Technical Defenses
- Responding to Phishing Incidents

Understanding Phishing Attacks

What is Phishing? Phishing is a cyber attack where attackers impersonate legitimate entities to steal sensitive information such as usernames, passwords, and financial details. These attacks often come in the form of deceptive emails, messages, or websites.

Common Tactics Used by Phishers

- **Email Spoofing:** Attackers send emails that appear to be from trusted sources.
- **Spear Phishing**: Targeted attacks aimed at specific individuals or organizations.
- **Clone Phishing**: Duplicating legitimate emails with malicious links or attachments.

Learn more about different types of phishing campaigns, how you can identify them, and tips to protect yourself:
20 types of phishing attacks + phishing examples - Norton

Phishing Prevention Tips

Educate Your Team

- **Regular Training:** Conduct regular training sessions to help employees recognize phishing attempts.
- **Simulated Phishing Exercises**: Test your team with simulated phishing attacks to improve their awareness and response.

Implement Technical Defenses

- **Email Filtering:** Use advanced email filtering solutions to block phishing emails.
- **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security.
- **Anti-Phishing Software:** Deploy software that detects and blocks phishing attempts.

Responding to Phishing Incidents

- **Report Suspicious Emails:** Encourage employees to report any suspicious emails immediately.
- **Incident Response Plan:** Have a clear plan in place to respond to phishing incidents, including isolating affected systems and notifying stakeholders.
- **Regular Backups:** Ensure regular backups of critical data to minimize damage in case of a successful attack.

See special considerations for protecting your business during the holidays, here:
How to protect your business against cyber attacks

Why It Matters

Phishing attacks can lead to significant financial losses, data breaches, and damage to your business's reputation. By staying informed and implementing robust security measures, you can protect your business from these threats.

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

Thanks for being part of Canada's cybersecurity community.

The CCTX Team
info@cctx.ca