How to prevent phishing (for small businesses)

Phishing is one of the most common cyber scams affecting Canadians at home and at work. Cyber criminals use phishing messages to try and steal sensitive information from people by pretending to be a legitimate sender like their bank or a colleague. Unfortunately, they can be easy to fall for if you don't know the signs to watch for.

Cyber security is a shared responsibility, so it's important that everyone on your team knows how to spot the signs and fight phishing. Here are a few actionable steps you can take to protect your organization:

Get familiar with the signs of phishing

The best way to prevent phishing scams is knowing how to spot the signs.

Urgent or threatening language

Look out for messages pressuring you to respond quickly, especially if the request is odd.

Suspicious attachments and links

Look out for links with unfamiliar URLs and attachments with odd file names or file types (like an .exe) that you didn't ask for, especially from a suspicious sender.

Typos

Look out for incorrect email addresses, suspicious links and any unusual spelling or grammar errors.

Unprofessional design

Look out for inaccurate or blurry logos, or corporate emails with formatting issues.

Requests for sensitive information

Look out for links directing you to login pages and requests regarding your personal information (like someone asking for your account password).

Unexpected messages

Look out for receipts or invoices that you weren't expecting, or unexpected requests (like your boss asking you for gift cards that weren't previously discussed).

Secure your data and devices

Accidents happen. That's why you should always have a backup plan.

- Secure your network if you work from home or have a hybrid work model.
- Frequently back up your data and devices.
- Ask your employer about your company's cyber security plan and get familiar with it.
- Use a virtual private network (VPN) if you're using unsecure Wi-Fi.
- Don't use your work devices for personal use or lend them to anyone else.
- Enable multi-factor authentication (MFA) whenever possible.

Learn how to handle a phishing scam

If you become a victim of phishing, don't panic.

- ✅ **Contact your IT department immediately** and let them know what happened. If you don't have an IT department at your organization, alert your manager.
- ✅ Secure your account by **changing any affected passwords**.
- ✅ Make sure your **new passwords are strong and unique**.
- ✅ **Enable MFA** to add an extra layer of security to your accounts and devices.
- ✅ **Don't forward the message to anyone else in your organization**. If you need to share the email, have your supervisor or someone from IT come and see it on your screen.
- ✅ Find out who is in charge (you or your IT department) of **reporting the incident to the Canadian Anti-Fraud Centre** by filing a report online or calling them at **1-888-495-8501.**

Get more tips to protect yourself and your devices at:

GETCYBERSAFE.CA

1. CIRA, 2021 Cyber Security Survey, Canadian Internet Registry, 2022

Catalogue number: D96-92/2022E-PDF | ISBN: 978-0-660-45574-7