What to do if you are a victim of a phishing scam

Phishing is a cyber criminal's attempt to send you malware or steal sensitive information from you by pretending to be a legitimate sender like a bank, online store or even someone you know. It also happens to be one of the most popular cyber scams out there, which means phishing is **very** common.

After all,
3.4 billion
phishing emails are sent worldwide everyday.[1]

Unfortunately, phishing scams can be easy to fall for if you don't know how to spot them.

And accidents happen.
16% of Canadians
say that they took risks online that threatened their cyber security.[2]

If you are a victim of phishing, here are simple steps you can do to recover and secure your accounts and devices:

✅ Change affected passwords

You should also update all accounts to use strong and unique passwords. Consider using passphrases made of four or more random words and 15 or more characters for extra security.

✅ Call your financial institution

If you shared any financial information (like a credit card number), contact your bank. Your financial institution can help recover lost finances and monitor your transactions to prevent further losses.

✅ Check your device for viruses or other malware

If there was a suspicious link or attachment in the message, install anti-virus software and scan your device for viruses that may have been downloaded.

✅ Enable multi-factor authentication (MFA)

MFA adds an extra layer of security to your accounts and devices. This makes it harder for cyber criminals to access your data, even if they steal your password.

✅ Consider deleting your inactive accounts

If cyber criminals gain access to your accounts, they can send phishing links to your contact list. Deleting or suspending your inactive accounts may prevent this.

✅ Report the incident

You can report phishing scams and other instances of online fraud to the Canadian Anti-Fraud Centre by visiting **www.antifraudcentre-centreantifraude.ca**, or calling **1-888-495-8501**. You can also report the incident to your local police department.

You have the power to fight phishing scams!

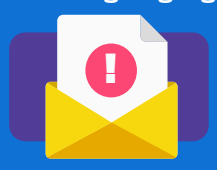
The best way to protect yourself against phishing attempts is learning how to spot the signs of a scam.

Watch out for:

Urgent or threatening language

Requests for sensitive information

Offers that are too good to be true



Suspicious attachments and file types

Typos, incorrect sender email addresses and links

Unprofessional design and incorrect or blurry logos

Get more tips to protect yourself and your devices at:

GETCYBERSAFE.CA

1. EarthWeb, 2022 How many phishing emails are sent daily in 2022?
2. EKOS, Get Cyber Safe Awareness Tracking Survey, 2022

Catalogue number: D96-91/2022E-PDF | ISBN: 978-0-660-45572-3