Have a Complaint?
Need Help?

If you suspect you have received a phishing e-mail or phone call:

1. Report it immediately to the bank or company in question. Most financial institutions now have security warnings on their web sites and special hotlines.
2. Report it to the Canadian Anti-Fraud Centre at www.antifraudcentre.ca or call 1-888-495-8501.

If you suspect you may have been the victim of a phishing scam, or that someone may be using your personal information without your permission:

1. Call your bank immediately and let it know what happened. Get the bank's advice on whether to change the numbers of your accounts.
2. Contact your credit card issuer and discuss whether it may be advisable to cancel your credit card.
3. Consider adding a fraud alert on your credit file or report. To do this, contact one of these credit bureaus:
   - Equifax: Visit www.equifax.ca or call 1-800-465-7166.
   - TransUnion: Visit www.transunion.ca or call 1-800-663-9980.

www.ontario.ca/ConsumerServices

Be a Smart Consumer
... We Can Help

Ontario's **Ministry of Consumer Services** informs and protects people so they can shop with confidence when buying goods and services.

Visit us:
www.ontario.ca/ConsumerServices

Call us:
Greater Toronto Area 416-326-8800
Toll-free 1-800-889-9768

TTY
Greater Toronto Area 416-229-6086
Toll-free 1-877-666-6545

E-mail us:
consumer@ontario.ca

Smartphone user?

For more information about **phishing** scan this QR barcode with your smartphone.

Ontario

ISBN 978-1-4435-2627-2

PHISHING

What you need to know

MINISTRY OF CONSUMER SERVICES
www.ontario.ca/ConsumerServices

Ontario

Ontario's **Ministry of Consumer Services** informs and protects people so they can shop with confidence when buying goods and services.

Have you ever received an e-mail that looks like it's from your bank?

It's about a security breach that may have affected your account. It says it's urgent to confirm your login, account and credit card details. It gives you a link to the bank's website so you can take care of it right away.

Before you click on that link, think twice. It's almost certainly a scam. Someone is "phishing" for your personal information so they can steal your identity, your money, or both.

REMEMBER:

Legitimate financial institutions or credit card issuers never ask you to supply this kind of sensitive information in response to an email or phone call. If you receive this type of contact, don't trust it! Verify the contact by phoning the business in question at their published phone number.

How do I spot a phishing scam?

It is estimated that phishers are able to fool up to five per cent of people they target. Don't be one of them. Here's what to watch for:

1. First, you get an e-mail from what seems like a legitimate financial institution, or an online shopping service.

2. The e-mail may say that there has been a "breach of security" or that they've "launched a new website." They ask you to confirm your personal information by clicking on a link. They may even say you won't be able to access your account anymore if you don't.

3. If you click on the link, you will be sent to a web page. It may look a lot like the company's real website. But beware: it's not! It's a fake page that the scam artists have set up. They aim to trick you into giving them information such as:
   - Your account, credit card, or identity details.
   - Your date of birth.
   - Your passport number.
   - Your social insurance number.

Other types of phishing scams may ask you to call a customer service number. You will then be prompted to "log in" using account numbers and passwords.

You should be suspicious any time you receive a request for personal information of this kind.

How can I protect myself?

To avoid being a victim of phishing

- Never give your personal information to anyone who contacts you by phone or in an e-mail or popup window. Verify the contact by phoning the business in question at its published phone number.

- Never provide personal information about your accounts or credit cards online unless you know you're connected to a secure server.

To protect your bank and other accounts

- Log in to your online accounts from time to time. Don't leave them for as long as a month before you check each account.

- Check your bank, credit and debit card statements each month. Make sure all transactions are legitimate. If anything is suspicious, contact your bank and all card issuers.

- Protect your computer with anti-virus software, spyware filters, e-mail filters, and firewall programs. Make sure that they are regularly updated.

Did you know?

Phishing isn't the only fraud targeting electronic devices. Vishing (derived from Voice over Internet Protocol, or VoIP) zeroes in on mobile devices, while smishing (from Short Message Service, or SMS) is phishing using text messaging.