



## **Financial Crime Trend Bulletin:**

### **Phishing**

**2018-01-01**

**FRAUD: Recognize, Reject, Report**

## **Purpose**

This bulletin was prepared to provide awareness and prevent victimization on a growing trend – Phishing scams.

## **Overview**

Phishing scams are traditionally associated with misleading and deceptive emails, falsely claiming to be from a legitimate organization such as a financial institution, business or Government agency in an attempt to have the consumer surrender private and personal information.

Scammers are expanding the way they contact consumers. Telemarketing campaigns and text messaging are used increasingly to contact and mislead potential victims into providing their private and financial information. Moreover, some of these unsolicited phishing campaigns are designed to get victims to click on malicious links or attachments that result in the installation of malicious software such as key loggers.

## **Warning Signs – How to Protect Yourself**

- Beware of unsolicited emails, text messages or phone calls from individuals or organizations prompting you to click on an attachment or link.
- Watch for spelling and formatting errors.
- Check the embedded hyperlink in the suspicious email by hovering your mouse over the link to verify the address.
- Do not click on any attachments; they can contain viruses and spyware.
- Go with your gut. If an email seems fishy it probably is.

If you think you or someone you know has been a victim of fraud, please contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or report online at <http://www.antifraudcentre.ca>