What is Phishing?

Phishing is a type of fraud that is designed to trick individuals into disclosing confidential and financial information for the purpose of identity theft.

How it Works

- You receive an unsolicited email appearing to be from a legitimate and reputable company, like RBC.
- The email may raise concerns that your account information is out of date or that you have received money. There is usually a sense of urgency and there may be a consequence associated with the request. For example, you are asked to validate your account information in order to prevent it from being suspended or terminated.
- You are asked to take action by following instructions that usually involve having you click on a link that takes you to a fake web-site. The fake web-site appears valid, often complete with a legitimate company's brand name and logo. Often the link and the URL address of the fake web-site look very similar to the URL address used by the real company that is being spoofed.
- You are asked to provide or update your personal and financial information by completing an online form or by responding to the email directly. You may be asked to provide a variety of information such as credit card numbers, account numbers, passwords, date of birth, drivers licence number, and social insurance or social security numbers.
- Once the information is provided, it is captured by the fraudster who may use it to gain access to accounts or to steal your identity.

Tips to Help You Spot and Avoid a Phishing Scheme

As a general rule you should not provide your confidential and financial information over the Internet in response to unsolicited requests you receive. Most financial institutions, will never ask you to provide sensitive information such as your account numbers, PINs, passwords, Social Insurance number or Social Security number through regular email. If you receive such a request, do not respond and contact your financial institution **immediately.**

Here are some additional tips to help you spot and avoid a potential phishing scheme:

- If you don't know the source of an email or if it looks suspicious in any way, do not open it and delete it immediately. This is the best preventative measure to avoid falling victim to a phishing scheme.

- Just because an email or web-site appears to be from a legitimate company doesn't mean it is.
- Phishing schemes are designed to look real and fraudsters will often use logos, trademarks, or even the entire look and feel of a valid web page to trick users into believing that it is genuine. Inspect any trademarks or logos that are used in the email or web-site. If the image appears to be different or distorted, the email or web-site is likely a fake.
- Phishing schemes sometimes contain misspelled words. Look for these either in the message or in the hyperlink if one is provided.
- Avoid responding to an unexpected web page or pop-up window appearing to be from a legitimate company that requests that you provide confidential information for a purpose that seems legitimate, e.g. to prevent a security threat or to validate an account, as it is likely a fake.
- Never click on a link contained in an email that you suspect may be fraudulent. The link could take you to a fake web-site or initiate the installation of unwanted software onto your computer.
- If you have a relationship with the company mentioned in a suspect email and you wish to call them to verify the request, do not use any telephone numbers provided in the email message, as they may be fake as well.
- Always be suspicious of web pages containing forms that collect confidential information, and do not use standard security features such as SSL encryption. Whenever you submit confidential or financial information online, always ensure that the web-site you are communicating with is secure. You can check the security of a web page by looking for a security symbol such as a closed padlock in your browser screen. You can also check the URL in the browser address bar. It should start with "https:" rather than just "http" as this signifies that the session is encrypted.
