Protect Yourself from E-Mail and Telephone Fraud: Phishing and Vishing

What are phishing and vishing?

Phishing and vishing are two types of scams commonly used by fraudsters to trick someone into giving them personal information they can then use to their advantage. Once they have someone's personal information, fraudsters will usually try to take money out of the victim's bank account, use credit cards or open new credit accounts.

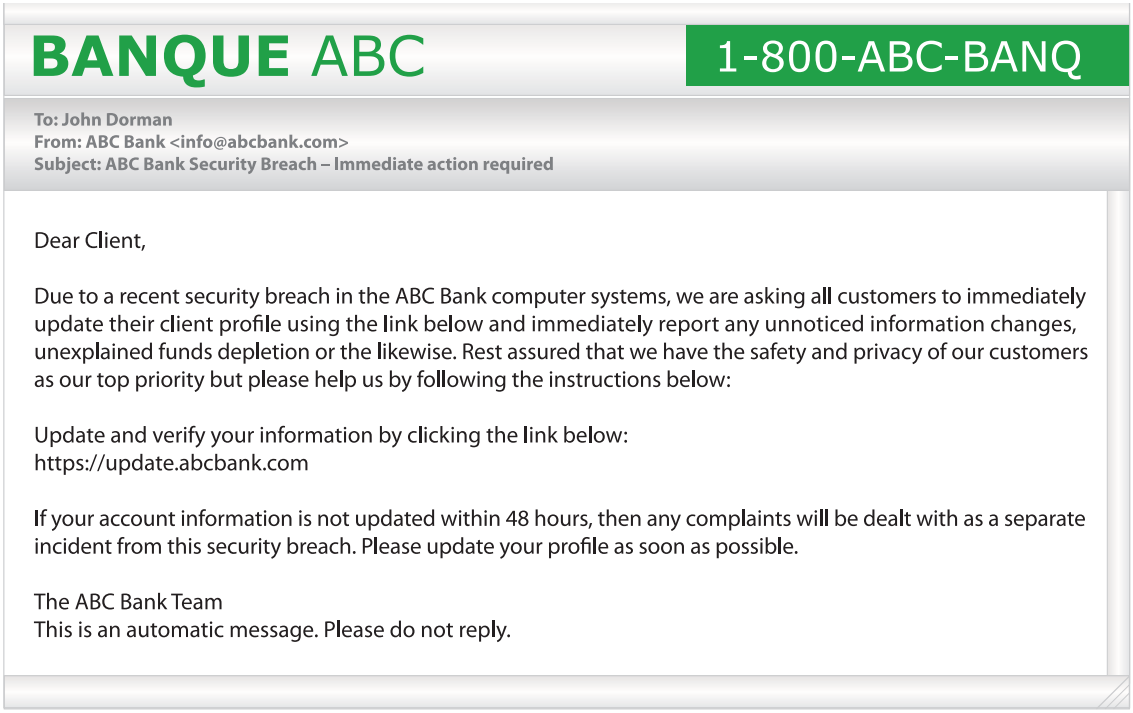
In phishing, the victim receives a fraudulent e-mail that looks like it comes from a legitimate company, asking them to click on a link that brings the victim to a fake website. The website often can be made to look like the victim's financial institution's website, so the victim does not notice the scam. The victim is then asked to enter or verify personal information (such as a credit card number, an online banking password or a Social Insurance Number) that is captured by the fraudster.

Vishing is the telephone version of phishing. The victim can be called directly by a fraudster, or can receive an invitation (by e-mail or voicemail message) to call a false customer support telephone number to fix a problem. Once victims are on the phone, an automated service may ask them to key in their account numbers, personal identification numbers (PINs), or passwords using the telephone keypad, or the fraudster can ask the victims to confirm some personal information.

Note that any legitimate company would NEVER ask you to provide your PIN or password over the phone or online.

Example of a phishing e-mail

Here is an example of a fraudulent e-mail:



BANQUE ABC 1-800-ABC-BANQ

To: John Dorman
From: ABC Bank <info@abcbank.com>
Subject: ABC Bank Security Breach – Immediate action required

Dear Client,

Due to a recent security breach in the ABC Bank computer systems, we are asking all customers to immediately update their client profile using the link below and immediately report any unnoticed information changes, unexplained funds depletion or the likewise. Rest assured that we have the safety and privacy of our customers as our top priority but please help us by following the instructions below:

Update and verify your information by clicking the link below:
https://update.abcbank.com

If your account information is not updated within 48 hours, then any complaints will be dealt with as a separate incident from this security breach. Please update your profile as soon as possible.

The ABC Bank Team
This is an automatic message. Please do not reply.

If you suspect phishing or vishing

If you suspect someone is trying to get your personal information either by phishing or vishing, don't give any personal information until you have verified whether the company is legitimate. If someone phones you to ask you for personal information, ask for the person's name, the name of the organization and the phone number where he or she can be reached. Then take the following steps:

1. Look up the organization's telephone number or website yourself. Look at the back of your credit card statements or other legitimate documents to see if the telephone number or website address matches the one you were given.

2. Call the company by using the phone number you have looked up yourself to verify that the person that has contacted you is indeed a member of the company's staff.

3. Contact the Better Business Bureau in your province or territory and ask questions about the company.

What to do if phishing or vishing happens to you

If you are a victim of phishing or vishing, start a written log of what happened and how you first noticed the fraud. Keep all documentation that you think may be helpful in the investigation. Then, follow the steps below, taking notes on the people you spoke with and exactly what they said:

1. Contact your local police and file a police report.
2. Contact the financial institutions, credit card companies, phone companies, and other lenders for any accounts you suspect may have been opened or tampered with.
3. Contact the two credit bureaus in Canada, Equifax and TransUnion. Ask that a "Fraud Alert" be placed in your credit file. At the same time, order copies of your credit report and review them. Make sure all the accounts and debts that show up on your report are yours. Report any incorrect information to the credit bureaus.
4. Contact the Canadian Anti Fraud Centre (CAFC) toll free at 1-888-495-8501 to report the fraud and get advice. The CAFC plays a crucial role in educating the public about specific mass marketing fraud pitches and in collecting and disseminating victim evidence, statistics and documentation, all of which are made available to law enforcement agencies.

Other FCAC information of interest

Tip sheets

- Protect Yourself from Credit Card Fraud
- Protect Yourself from Debit Card Fraud
- Protect Yourself from Identity Fraud
- Protect Yourself from from Real Estate Fraud

Publications

- Understanding Your Credit Report and Credit Score

Notes

About Financial Consumer Agency of Canada (FCAC)

With educational materials and interactive tools, the Financial Consumer Agency of Canada (FCAC) provides objective information about financial products and services to help Canadians increase their financial knowledge and confidence in managing their personal finances. FCAC informs consumers about their rights and responsibilities when dealing with banks and federally regulated trust, loan and insurance companies. FCAC also makes sure that federally regulated financial institutions, payment card network operators and external complaints bodies comply with legislation and industry commitments intended to protect consumers.

Contact Us:

Website: fcac.gc.ca

Toll-free: 1-866-461-3222

TTY: 613-947-7771 or 1-866-914-6097

Follow @FCACan on Twitter

Subscribe to FCACan YouTube Channel

IT PAYS TO KNOW

Cat. No.: FC5-8/16-2007E-PDF ISBN: 978-0-662-47120-2

March 2013