



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.

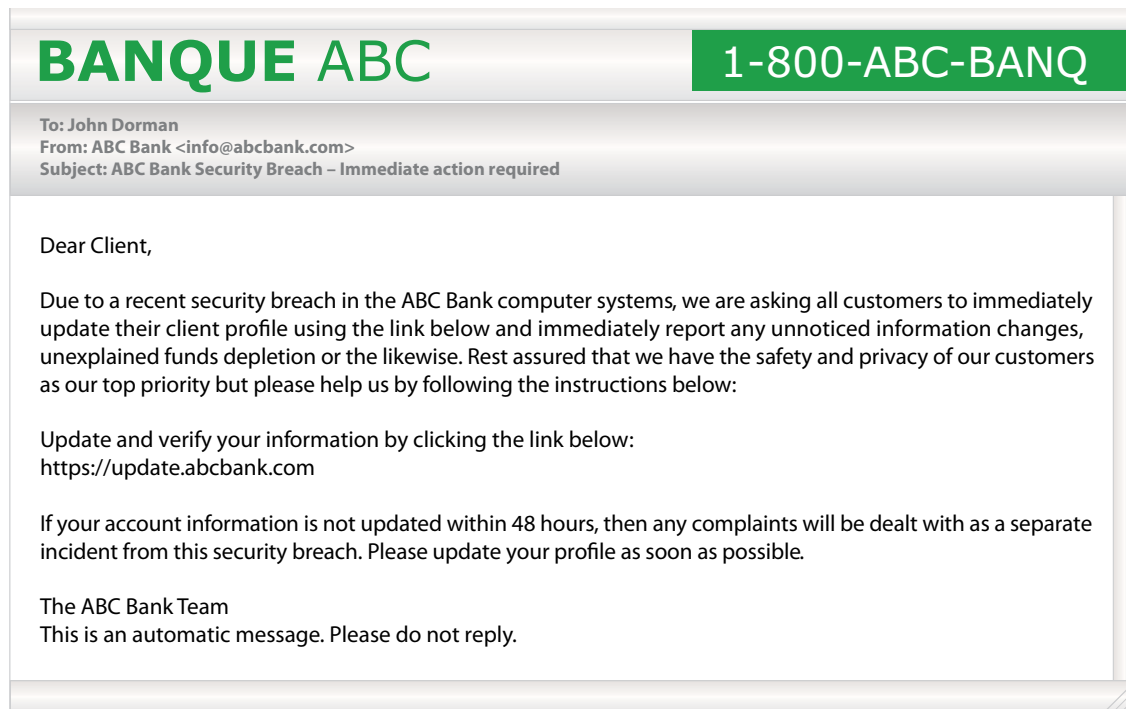
In phishing, the victim receives a fraudulent e-mail that looks like it comes from a legitimate company, asking them to click on a link that brings the victim to a fake website. The website often can be made to look like the victim's financial institution's website, so the victim does not notice the 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:



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. Call PhoneBusters, a national anti-fraud call centre that collects and analyzes information on fraud, and assists law enforcement agencies in investigations.
5. Contact Reporting Economic Crime Online (RECOL) through www.recol.ca. This website is a joint initiative of international, federal and provincial law enforcement agencies, and regulators and private commercial organizations that investigate complaints related to economic crime.

Other FCAC information of interest

Tip sheets

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

Publications

- Understanding Your Credit Report and Credit Score

