# *Protecting Yourself from Fraudulent E-mails and Telephone Calls*

## "PHISHING" AND "VISHING"

"Phishing" is the practice of sending fraudulent e-mails. (See sample included.) This type of e-mail looks like an on-line message from a legitimate financial institution, retailer or government agency, but it isn't. The phony e-mail tells the person receiving it (called the "recipient") to click on a link provided in the e-mail. This takes consumers to a bogus Web site — which looks a lot like their service provider's site — and asks them to provide or verify personal information such as a credit card number, an on-line banking password or a social insurance number. Fraud artists use this information to take money out of consumers' bank accounts or to steal their identity.

"Vishing" is the telephone version of phishing. It hooks consumers by sending them a phony e-mail, then gives them a phony telephone number to call. As with phishing, the e-mail looks like a message from a service provider such as PayPal or eBay, which allows users to pay on line. The e-mail message tells recipients that there is a problem with their account. However, instead of giving them a link to a phony Web site, the vishing e-mail gives consumers a false "customer support" telephone number to call. When consumers dial that number, an automated service answers and prompts them to "log in" by keying in their account number or password, using the telephone keypad provided.

Fraudsters also call consumers at home, or leave voicemail messages for them, telling them that their account is at risk, and suggesting they call Customer Support "immediately". The scam artists may even try to gain consumers' trust by telling them they want to "confirm" their personal information — such as their full name, address or credit card number — which they repeat back to the consumers.

The aim of these scams is to trigger a "gut" reaction in consumers, by alarming them and demanding an immediate response.

### *Here is a sample of a fraudulent e-mail:*

ABC BANK

1-800-ABC-BANK

Due to a recent security breach in the ABC Bank computer systems, we are asking all customers to immediately update with 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 as soon as possible.**

**Part of the ABC Bank Team.**
**This is an automatic message. Please do not reply.**

Site Map | FAQ | Agreements | Trademarks and Disclaimers | Privacy & Security

## *What to do if you receive one of these messages*

- Do NOT respond to an e-mail, or a voicemail message or telephone call, that asks you to disclose personal information such as an on-line password, a debit or credit card number, or a personal identification number (PIN).
- Do NOT use the phone number provided in the e-mail or telephone message until you first check if the number is legitimate. To do this, call the organization, using a telephone number that you, yourself, have looked up. If the e-mail or telephone message appears to be from your financial institution, call them at the phone number listed on the back of your debit or credit card, or on your monthly statement.
- Sometimes a financial institution will call you, or leave a voicemail message, if they suspect that there has been fraudulent activity on your debit or credit card, or on your account. A legitimate financial institution will ask you a number of questions to make sure they are speaking to one of their clients. However, the institution will NEVER ask you to provide your PIN or password over the phone.
- Be careful about how and with whom you share personal and financial information.
- You can report suspicious incidents on line, on the Web site of the organization Reporting Economic Crime Online (RECOL), at: **www.recol.ca**. This Web site is a joint initiative of international, federal and provincial law enforcement agencies, and regulators and private commercial organizations, that have a legitimate interest in getting copies of complaints related to economic crime.
- You can also report such incidents to PhoneBusters, by going to their Web site at: **www.phonebusters.com** or by calling them toll-free at: **1-888-495-8501**. PhoneBusters is a national anti-fraud call centre, jointly operated by the Ontario Provincial Police and the Royal Canadian Mounted Police. It is the central agency in Canada that collects information on complaints related to identity theft and telemarketing, as well as fraud letters such as the Nigerian scam letter, which asks recipients to send money.

## *Where to go for more information*

Many financial institutions, and on-line service providers and retailers, post information on their Web sites to help consumers recognize examples of phishing or vishing, and advise them what to do if they have given personal information to an organization that is not legitimate.

Some financial institutions have made a public commitment to protect customers in case of fraud. The Financial Consumer Agency of Canada (FCAC) oversees the public commitments made by federally regulated financial institutions. If you are the victim of fraud because of a phishing or vishing scam and your federally regulated financial institution is holding you liable, or if you need more information about your rights and responsibilities, contact FCAC. You can call our Consumer Contact Centre toll-free at: **1-866-461-3222**, or visit our Web site at: **www.fcac.gc.ca**. (Consumers with hearing problems can call our TTY number at 613-947-7771, or toll-free at 1-866-914-6097.)

*This tip sheet is part of a series. To see or order FCAC's other tip sheets, please call us or visit our Web site.*


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