

BETTER BUSINESS BUREAU OF MAINLAND B.C. CONSUMER RELEASE

August 9, 2007

DON'T GET HOOKED BY 'PHISHING' BAIT

=====

VANCOUVER: You, like many email users throughout BC, have received yet another email that looks like it's from a local bank, credit union, or company. You might even have an account with them, making it more difficult to ignore and delete. Phishing emails, designed to hook you into giving your password, credit card information or your Social Insurance Number, or asking for or offering you money, are still rampant and now even more sophisticated than before.

These emails appear to be genuine, including a few corporate logos and links, which supposedly take you to the company's legitimate website. Instead, the link takes you to a "look-alike" site and into the hands of identity thieves. Looks can be deceiving. In other words, that Bank of Montreal email you've received is likely not from Bank of Montreal; similarly, TD Canada Trust has not sent emails with a link to a website asking for confirmation, update, and verification of your account data.

Bank Phishing

In most cases you are lured to the phony sites by being told you need to "update" or "verify" your banking information, or that "unusual account activity" has been identified and you will need to log into your account or a link provided to resolve the issue. The email may threaten to suspend or even cancel your bank account if you don't supply the requested information. Remember, legitimate financial institutions already have their customer's account information and have absolutely no reason to request it by email. By mass mailing to every email address they can find, the "phishers" are sometimes able to convince up to 5% of recipients to respond to them.

E-card Phishing

Phishing emails could also take the form of an e-card. You might receive an email notifying you of an online greeting card from a "Schoolmate," "Friend," etc. If you don't know the person sending you this card, think twice before clicking on that link to view this card. It could contain software which could harm your computer. A popular worm program, the Storm, compromises your computer's security and relays your computer's information (i.e., email addresses, confidential files) to the phisher's computer.

"Don't get hooked", said Lynda Pasacreta, President, Better Business Bureau of Mainland BC. "Protect yourself by taking caution to whom and how you give your information."

The BBB offers the following tips to avoid being lured by phishers:

- Treat unsolicited email requests for personal data with extreme suspicion. Unsolicited means the email wasn't sent in response to a request you have made. Phishing emails often contain spelling and grammar errors, or missing words. A good rule of thumb to follow is "If you didn't send them an email, then delete theirs."
- Do not reply. If the email is from a bank that you do have a relationship with, look over the entire message. Be aware that phony emails may contain 800 numbers that will take you offshore or to a call center set up by the phishers. Do not call the provided toll-free numbers or respond by email. Instead, call the bank for verification using the phone number provided on the back of your bank card or on your account statement.

- Be aware. Go online regularly and review your bank statements to check your banking activities and verify all transactions. Notify your bank immediately of any erroneous or suspicious transactions.
- Be careful when submitting personal or financial information on websites. Read the website security and privacy policy. To determine if the website is secure, look for the “padlock” icon on your browser’s status bar and the “s” in the website address (i.e., <https://>).
- Be preventative. Update anti-virus software and security patches to system software regularly. Phishing emails can contain viruses that may harm your computer if opened.

For more information regarding phishing, visit www.bbbvan.org.

For more information, please contact:

Lynda Pasacreta, President
Tel: (604) 688-8731
Email: president@bbbvan.org

- OR -

Simone Lis, Director of Operations
Tel: (604) 681-7476
Email: simone@bbbvan.org