

News Release

For Immediate Release
April 21, 2005

1 of 3

Canadian Bankers Association and the RCMP Remind Canadians to be Cautious About Unsolicited E-mail

TORONTO – The Canadian Bankers Association (CBA) and the Royal Canadian Mounted Police (RCMP) remind Canadians to use caution when they receive unsolicited e-mail that asks them to reveal personal or financial information. Fraudulent e-mails have been circulating that appear to be from legitimate organizations – such as banks, credit card companies, online retailers and government agencies – asking consumers to update or verify some personal information, including credit card numbers, social insurance numbers or online banking passwords.

Known as e-mail fraud, phishing or brand spoofing, these fraudulent spam e-mails are sent out randomly to thousands of recipients at once, whether or not they are customers of the organization being spoofed. They will have a sense of urgency, warning recipients that the access to their accounts will be limited or their accounts will be closed if they do not respond. In other cases, the e-mails will promise financial benefit for the recipient if they reply, or ask for a verification of information to help protect the recipient from identity theft. The e-mails will then link to a fraudulent website which, again, could appear legitimate, but is actually a phoney website operated by fraudsters in the hopes of tricking unsuspecting consumers into revealing personal information.

“We have seen an increase in these fraudulent spam e-mails, so we wanted to remind people that a bank would never send an e-mail to customers asking them to verify their personal information,” said Caroline Hubberstey, Director of Public and Community Affairs at the Canadian Bankers Association. “One of the best ways to prevent e-mail fraud is to ensure that people know what to look for and that they can identify these e-mails for what they are: a scam. Most Canadians are pretty savvy when it comes to recognizing fraudulent e-mails, but we think it is important to reinforce good e-mail habits.”

Some of the fraudulent e-mails may look professional at first glance, using corporate logos, but closer inspection may reveal spelling and grammatical errors, unusual language or branding that is not consistent with that of the organization being spoofed.

- more -

For more information:

Melanie Minos, Manager, Media Relations

Tel: (416) 362-6093, ext. 220

Cell: (416) 587-7733

E-mail: mminos@cba.ca



CANADIAN BANKERS ASSOCIATION

Building a Better Understanding

Canadian Bankers Association and the RCMP Remind Canadians to be Cautious About Unsolicited E-mail *(continued)*

2 of 3

“We recommend that consumers use a healthy dose of skepticism when they receive any unsolicited e-mail, particularly if they are asked to reveal personal or financial information. Legitimate companies normally don’t do that,” said Sergeant Michel Haché, Identity Theft Coordinator, Commercial Crime Branch of the RCMP. “If you do receive one of these e-mails, report it to the organization being spoofed and to law enforcement through PhoneBusters and Reporting Economic Crime On-Line (RECOL). After that, delete the e-mail. When consumers report these e-mails, we can work with the organizations being spoofed to quickly shut down these bogus websites and prevent people from becoming victims.”

How to Avoid E-mail Fraud

While banks and law enforcement take extensive steps to protect people, there are some simple steps Canadians can take to protect themselves:

- Be skeptical of any unsolicited e-mail asking you to provide personal information, no matter how legitimate it looks. If you are unsure, contact the company it purportedly comes from: but make sure you use a phone number, e-mail address or website address that you know is legitimate. Do not use the ones provided in the e-mail.
- Never send personal and/or financial information by e-mail.
- Always enter your bank’s website using the website address (URL) that you know is accurate. Contact your local bank to get the correct website address if you’re unsure.
- Fraudulent e-mails are not personalized and, instead, are addressed in general terms, such as “Dear valued customer”.
- Check the domain name shown as the link in the e-mail. When you click the link, if it does not match the name that appears in the browser at the top of the screen, then it may be a fraudulent website.
- If you receive an e-mail notifying you that an e-mail money transfer is being sent from a person you don’t know, delete the e-mail as it is likely fraudulent.
- Make sure your home computer is protected by installing anti-spam, anti-spyware and anti-virus software and personal firewalls, and keep these up-to-date. Also check for operating system patches and upgrades on a regular basis.
- Regularly review your bank and credit card statements and immediately report any unauthorized transactions to your financial institution. Also check your credit report at least once a year by contacting credit reporting agencies Equifax Canada or TransUnion Canada.

- more -



Canadian Bankers Association and the RCMP Remind Canadians to be Cautious About Unsolicited E-mail *(continued)*

3 of 3

For more information on how to recognize and report a fraudulent e-mail and how to protect yourself against financial fraud, visit the CBA website at www.cba.ca/e-mail-fraud.

Report Fraudulent E-mails

Fraudulent bank e-mails should be reported to banks and law enforcement through:

Banks

Links to the banks' reporting information can be found on the CBA website at www.cba.ca/report-it.

PhoneBusters

Phone: 1-888-495-8501

E-mail: info@phonebusters.com

Website: www.phonebusters.com

RECOL (Reporting Economic Crime On-Line)

Website: www.recol.ca

The Canadian Bankers Association is an industry association representing the domestic and foreign-chartered banks of Canada and their 237,000 employees.

- 30 -

