

FOR IMMEDIATE RELEASE

Insecure Facebook pages lead to Interac e-mail money transfer scam

Burnaby, April 4, 2008: The British Columbia Crime Prevention Association has been advised by the RCMP of a new scam that uses *Facebook* pages to solicit money from friends of the pages' owner.

In a recent case, a Langley woman failed to properly set up her pages to ensure that only those in her close circle of friends were privy to her information. As a result, someone accessed her account and assumed her identity before sending off e-mail requests for money to friends whose contact details were listed within those insecure pages. Some of the friends fell for the scam and transferred money via Interac e-mail money transfer to the fraudster and they did not question the authorship of the e-mail because the victim's personal information was available to the identity thief to add legitimacy to the requests.

“Account takeover is a common technique used by identity thieves in the world of bank account fraud,” says Valerie MacLean, Executive Director, BC Crime Prevention Association, “but this is a different kind of account takeover - a twist with a personal touch. The shame of it is that this type of scam is preventable by taking advantage of the privacy configuration options offered by *Facebook*.”

BC Crime Prevention Association provides the following tips for *Facebook* users:

- Go to the Privacy Overview page and carefully review the options for sharing information – use the Edit Settings function to set access parameters to limit your exposure to others.
- Take advantage of the “Block People” and “Limited Profile” tools to allow only selected people to view your pages.
- Do not respond to an e-mail request to transfer money to a “friend” without there being a prior telephone conversation or face-to-face meeting at which the request for money was discussed. If there is no such prior discussion, contact the requestor by phone to confirm that they have requested money.
- Beware of e-mail “spoofing” in which someone purports to be your friend by sending you a message using their e-mail address. Wikipedia defines spoofing as a term used to describe fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message. The consequences of responding to one of these messages include giving out personal information that could be damaging to you if it falls into the wrong hands.
- General tips on Social Networking Sites including ‘10 Steps to Safe Online Social Networking’ can be found on the RCMP website at: http://www.rcmp-grc.gc.ca/scams/student_guide_e.htm#social
- For more information about *Interac* e-mail money transfers, visit the *Interac* website at: http://www.interac.ca/consumers/productsandservices_01_empt.php

This news release is one of a series in which the BCCPA offers advice under its Crime Shield banner to give the public the tools they need through education and awareness to protect themselves against crime.

Our Ask an Expert column is an additional resource for crime prevention information pertinent to British Columbia. The column can be viewed at www.bccpa.org. Topics will be frequently updated and refreshed depending upon response.

Media Contact:

Valerie MacLean

Executive Director

BC Crime Prevention Association

604-291-9959, ext.226

v.maclea@bccpa.org