January 27, 2011

We have received reports of phishing scams in circulation targeting our credit union owners.

The phone call simply says they are "**the credit union**" calling to confirm their account number, PIN, etc.

The email notifies the owner that their account is inactive and requests them to provide account information (numbers, PIN, etc) to update their account.

The third incident involves a "spoof" site of the owner's credit union. When the owner logged onto his credit union website, they were taken to a "spoof" site but noticed immediately the web address was different than the usual credit union site. Note: This owner also was aware that he had malware on his computer so was being very cautious and aware of his computer activity.

It is very important that owners know they will never be contacted by their credit union and asked to provide PIN numbers, etc.

When a credit union contacts their owner by telephone, the name, telephone number and credit union employee's names will always be provided.

The following information on Phishing Scams is from the Canadian Anti-Fraud Centre (formerly known as Phonebusters)

Phishing

The word phishing comes from the analogy that Internet scammers are using email lures to 'fish' for passwords and financial data from the sea of Internet users.

Phishing, also called "brand spoofing" is the creation of email messages and Web pages that are replicas of existing, legitimate sites and businesses. These Web sites and emails are used to trick users into submitting personal, financial, or password data. These emails often ask for information such as credit card numbers, bank account information, social insurance numbers, and passwords that will be used to commit fraud.

The goal of criminals using brand spoofing is to lead consumers to believe that a request for information is coming from a legitimate company. In reality it is a malicious attempt to collect customer information for the purpose of committing fraud.

Tips on how to spot and avoid phishing scams

- *Protect your computer with anti-virus software, spyware filters, email filters and firewall programs*
- *Contact the financial institution immediately and report your suspicions.*
- *Do not reply to any email that requests your personal information.*
- *Look for misspelled words.*

Always report phishing or 'spoofed' emails.

If you've received one of these suspicious emails, report it to info@antifraudcentre.ca or the financial institution that it appears to be from.