



FEDERAL EMPLOYEES (KINGSTON) CREDIT UNION LIMITED

464 Princess Street, Kingston, ON K7L 1C2
501-4499 Bath Road, Amherstview, ON K7N 1A6

Tel: 548-4094 Fax: 546-5225
Tel: 634-3875 Fax: 634-1711

NEWSLETTER – APRIL 2011

FRAUD

RECOGNIZE IT! REPORT IT! STOP IT!

Mail Fraud

Mail fraud is a type of scam perpetrated when fraudsters masquerade as a legitimate person or business. They send out letters for the purpose of taking advantage of people either financially, or for the purpose of acquiring personal and/or financial information that is later used to commit fraud.

One common example of this type of fraud involves a fraudster sending out letters notifying bank cardholders that they have won a large cash prize as part of a computer rewards program. A seemingly legitimate cheque is enclosed along with instructions to use the cheque to pay clearance fees on the prize. Unfortunately, the cheque does not clear, and the recipient is then out of pocket for the money they sent to process their "prize".

How To Protect Yourself - Do not act on the letter.

Identity Theft

Identity theft is one of the fastest growing crimes in North America. Identity theft occurs when someone steals your personal information including your social insurance number, driver's licence number, date of birth, health card number, credit card number or your debit card PIN number. This information is used to open new financial accounts in your name. Fraudsters obtain your personal information in a variety of ways including:

- They steal wallets or purses containing your identification, debit and credit cards.
- They steal your mail including statements, tax information, pre-approved credit offers etc.
- They find personal information in your home, garbage, that you share online or steal it from their employers' records.

How To Protect Yourself

- Carry only the credit and debit cards that you need, leave others at home.
- Sign your new cards immediately.
- Do not carry your social insurance number or birth certificate. Keep in a safe, secure place.
- Do not attach or write your PIN number to the card.
- Shred all personal information documents.
- Frequently check your credit report for changes or unusual activity.
- Pay attention to your billing cycles and follow up if you have not received a bill.

Email Fraud

Email fraud or phishing is a scam where fraudsters attempt to acquire personal and/or financial information, such as passwords, card numbers, etc., by masquerading as a trustworthy person or business through electronic communications. Phishing is typically carried out using email or an instant message, although phone contact has been used as well. In some instances, the fraudster sends authentic-looking emails, appearing to come from legitimate companies, requesting recipients to disclose personal and/or financial information that is later used to commit fraud.

How To Protect Yourself

- If you receive an email that you suspect is fraudulent, do not respond.
- If you have already responded to this kind of email and have disclosed your personal financial information, please contact your financial institution immediately.
- Do not provide personal or financial information to anyone in an email.
- Be suspicious of email attachments from unknown sources. If you do not know or recognize the sender of the email, do not open the attachment.
- Always check that emails you have received do not contain viruses by running your anti-virus software.
- Do not share or provide your personal information.
- Consider purchasing a firewall, which will help prevent unauthorized access to or from your computer. A firewall will also detect attacks or attempted intrusions by upgrading regularly.
- Anti-virus programs help protect your computer from viruses that spread damaging computer code on your computer without the user's knowledge. This code is used to collect and transmit personal information or infect and harm your system. Users should set their anti-virus software to automatically update as new releases become available for your protection.
- Anti-spyware programs will protect computer users from spyware that gathers information about the user including keystrokes, screen images and your online habits. Again, update the program regularly to ensure that you are protected from the most recent spyware.

Other Security Suggestions:

- Make your passwords complex and difficult for others to guess: Use multiple characters including numbers and symbols.
- Change your passwords regularly.
- Avoid using computer applications that offer to save your password for you.
- Keep your passwords and personal identification numbers safe, and do not share them.
- Use different passwords for your logins at internet sites.
- Never leave your computer logged on.
- Exit or log off sites when you are finished your transactions.
- Do not send personal information through an email.
- Do not conduct online financial transactions on a public computer.

**If a scam artist contacts you or if you've been defrauded,
call PhoneBusters at 1-888-495-8501**

PhoneBusters will gather evidence; identify new trends and alert law enforcement in Canada and abroad. By reporting, you prevent others from becoming victims and help put an end to fraud.