Fraud Prevention

Awareness is the Key to Prevention

Although March is *Fraud Prevention Month*, being aware of scams that are circulating is not a one-month activity. Fraudsters gain access to personal information and funds from unsuspecting individuals every day of the year.

Awareness is the key to preventing yourself from becoming victim to unscrupulous fraudsters.

Remember, if it is too good to be true, it often is. Never grant anyone access to your personal or financial information. Never respond to unsolicited emails or phone calls. If you believe you have become a victim of fraud contact your local police.

Here are just a few of the many frauds individuals fall victim to everyday. For more examples of other scams please visit the Canadian Anti-Fraud Centre at www.antifraudcentre.ca.

Vacation Scams: Individuals receive a call advising they have won a vacation. Real company names such as *Expedia*, *Air Miles*, *Air Canada* and *WestJet* are used. The caller advises the potential victim that they are a preferred customer and have been awarded a credit or discount on a trip if booked immediately. High pressure sales tactics are used and the caller will request a credit card number in order to pay for fees such as taxes.

Timeshare Re-sale Scams: Timeshare owners are solicited over the phone and made an offer to sell their timeshare. In some cases the owner has advertised their timeshare for sale on the Internet. The suspect promises a quick sale with a high profit margin. Various fees are requested up front prior to the final sale; this includes maintenance fees, escrow fees and fees to cover taxes. Documentation and correspondence with the victim is conducted on a professional level to provide a level of authenticity. Victims are often solicited by companies in the United States but are required to transfer funds to bank accounts in Mexico through a bank to bank wire transfer.

Mystery Shopper Job Scam: Suspects use free online classified websites to recruit potential victims. The victim answers an enticing ad to become a mystery shopper. The 'employer' sends a letter, with mystery shopping tasks to be completed, and a cheque to help the victim fulfill their mystery shopping tasks. The victim will likely cash the cheque they were given first. One of the tasks will be to use a money transfer company and wire a large portion of the money to a name provided, in order to test the company's procedure and customer service skills. The victim will find out later that the cheque is counterfeit, thus making the victim accountable to pay for the funds that were wired.

Ransomware: A pop up message shows up on the computer stating "This IP address was used to visit websites containing pornography, child pornography, zoophile and child abuse. Your computer also contains video files with Pornographic content, elements of violence and child pornography! Spam messages with terrorist motives were also sent from your computer." The messages are socially engineered to appear as if coming from either the Canadian Security Intelligence Service (CSIS) or the RCMP and tell the consumer they need to pay $100-$250 via *Bitcoin*, *Ukash* or *PaySafe Card* to unlock their computer.

The Emergency Scam: Fraudsters use social media, the Internet and newspapers to target potential senior victims, a call is received claiming to be a family member or a close friend advising about an urgent situation that requires immediate funds. Common themes have been that the family member was arrested or got into an accident while traveling abroad. Fees are required for hospital expenses, lawyer fees or bail. Usually the potential victim is instructed to send money via a money service business like *Western Union* or *MoneyGram*.

Romance Scam: Fraudsters are targeting individuals who have turned to the Internet to seek a romantic mate. The suspect will gain the trust of the victim through displays of affection and will communicate through the phone and email for months if needed to build that trust. The suspect may claim to be located in a foreign country but will want to meet up with the victim in person. It is at this time that the suspect will advise that they can't afford to travel and will ask for money to cover travel costs. Other variations include the suspect claiming that there is an emergency with a sick relative and will ask for money to cover medical expenses.

Microsoft/Windows technician Scam: Suspects pretend to represent a well-known computer based company like Microsoft and claim that the victim's computer is sending out viruses or has been hacked and must be cleaned. The suspect will remotely gain access to the computer and may run some programs or change some settings. The suspect will then advise that a fee is required for the service of cleaning and request a credit card number to cover the payment. In some cases the suspect will send a transfer from the victim's computer through a money service business like *Western Union* or *MoneyGram*. The end result is that the victim pays for a service that was not needed as the computer was never infected.

Business Executive Scam: a phishing type wire fraud currently targeting businesses. The potential victim receives an email that appears to come from their employer's human resources or technical support department. Suspects create email addresses that mimic that of the real departments. An email message will be sent to the accounting department advising that the 'executive' is working off-site and has identified an outstanding payment that needs to be made as soon as possible. The 'executive' instructs the payment to be made and provides a name and a bank account where the funds, generally a large dollar amount, are to be sent. Losses are typically in the excess of $100,000.00.Financial Industry wire frauds occur when Canadian financial institutions and investment brokers receive fraudulent email requests from what they believe to be an existing client. Unbeknownst to them, the email account of their client has been compromised. A request is sent by the suspect to the financial institution/investment broker to have money transferred from "their" bank account usually to a foreign bank account.