Financial Crime Trend Bulletin:

Internet Fraud

2017-10-01

FRAUD: RECOGNIZE, REJECT, REPORT

Purpose

October is Cyber Security Awareness Month, and while Canadians continue to fall victim to a number of online scams, The Canadian Anti-Fraud Centre remains dedicated to assisting in the prevention and fight against Cybercrime. This fraud bulletin was prepared to help Canadians Recognize, Reject and Report these scams.

Ongoing Internet Scams

Romance Fraud

Fraudsters create fake profiles on social networking and online dating websites with the intention of luring potential victims into online relationships. The fraudsters have shown that they are willing to develop the relationship over an extended period of time; this increases the trust level between the victim and the fraudster which results in the potential victim usually losing more money.

Wire Fraud

Business Executive Scam
The *Business Executive Scam* involves a potential victim who receives an email that appears to come from someone they know such their employer's own chief executive officer, chief financial officer, human resource department or technical support department. Fraudsters will mimic or even take over a victim's email account. They then use the fake account to send a message to the accounting department advising that the executive is working at home or off-site, and the executive has identified an outstanding payment that needs to be made ASAP. The executive instructs that a payment be wired, generally a large dollar amount (e.g. in excess of $100,000), to an identified person or business.

The Supplier Swindle
Canadian businesses lose significant amounts of money to fraudsters claiming to represent their regular supplier. The scam targets businesses that have existing relationships and accounts with suppliers and wholesalers. The scam usually involves a spoofed email informing the buyers of a change in payment arrangements. The email notice provides new banking details and requests that future payments be made to this "new" account.

Continuity Scams

As E-Commerce continues to grow, so do the opportunities to be victimized through online purchases– specifically with a credit card. Continuity scams largely take place when someone who is online observes a pop-up or advertisement offering a *free* trial or *free* gift upon completion of a survey. Consumers who participate are often asked to provide a credit card to pay for shipping and handling. Unless victims review the *terms and conditions of the offer*, it's unlikely they will see the hidden fees associated to the offer, which includes overpriced monthly charges that are nearly impossible to cancel.

Phishing

Any unsolicited email falsely claiming to be from a legitimate organization such as a financial institution, business or government agency in an attempt to have the consumer surrender private and personal information. The email usually request or direct the consumer to visit a website where they are asked to update or provide personal and/or financial information.

Counterfeit Merchandise

Fraudsters trick Canadian consumers into buying counterfeit goods at discounted prices through spoofed websites. A spoofed website is when a fraudster imitates a legitimate website (for instance, retailers such as Canada Goose, UGG, Lululemon, Michael Kors, Coach and many more). When the consumer receives the product, it will be of low quality and will lack the name brand or certification. Counterfeit products can also result in personal injury.

Binary Options

Similar to gambling, binary options work much like a wager. All or nothing "bets" are invested based on how an asset will perform within a certain timeframe. The asset could be a stock, currency or commodity.

Websites are designed to attract users to trade binary options, and many claim to be risk free or to reimburse for lost wages. Initially, a virtual gain is seen, but there is no way to access the profits because they are non-existent. Currently in Canada, no business is registered or authorized to sell or market binary options.

It is always risky to invest in offshore companies, however investors that buy into a binary option run the risk of having their identity stolen, accumulating losses for unauthorized withdrawals on their credit cards and incurring high interest payments on an investment that doesn't exist.

Protect yourself online

If used insecurely, the internet provides an environment whereby consumers and businesses can be affected by a range of different scams. It is important to familiarize yourself with the common online scams to protect yourself.

Please visit our website at www.antifraudcentre.ca for a broader list of online scams.

If you think you or someone you know has been a victim of fraud, please contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or report online at www.antifraudcentre.ca