MORE SCAMS

Advance Fee Scams

The execution of this scam is simple.

A perpetrator alleges to have something of value.

Depending on the scam this might include things like:

- Debt Consolidation
- Loan Approval
- Access To a Large Pool of Money (Nigerian Scam)
- Business Opportunity or Investments
- Lost Funds and Family Inheritance
- Merchandise or Property
- Insurance or any "Future" benefit
- Cruise, Resort or Other Vacation Activities
- Credit Protection or Credit Restoration
- A Prize or a Gift

The perpetrator is willing to provide this/these products or services to you if you will first provide a fee or access to your financial resources (bank account, credit card).

Once you have paid the fee or surrendered your information you end up with neither money or product and services.

HEADS UP!

Generally there is some kind of urgency in the pitch. It will usually involve limited time, limited opportunity or there is someone already waiting "in the wings".

There might be an element of secrecy or confidentiality involved.

The purpose of this urgency and secrecy is to prevent any research on the individual or the offering.

Prevention

- Do not do business or respond to surveys over the phone.
- Request original documents rather than rely on someone's "word".
- Ask for a second independent opinion.
- Regardless of the urgency – take the time to do investigate.
- **If it sounds to good to be true, it probably is.**

Charity Scams

Over the Christmas Holiday period we will be deluged with requests that, while we have our wallets open during the festive season, we r remember the various Charities and Social Agencies with our generosity.

Albertans are well known for their social responsibility and generosity and that has been often been exploited by con artists and scammers.

HEADS UP!

Whenever possible donate directly to the organization. The experience of some organizations is that the marketing organization takes the lion's share of the revenue generated.

Door-to-Door canvassers for legitimate organizations can often provide you with a pre-addressed envelope to allow you to have more control of the transaction.

Use Due Diligence in dealing with an unknown charity. There are outside resources to verify their charitable status, their business license, GST number and addresses and phone numbers.

Be suspicious of someone who creates unusual urgency in his or her request for funds. Call the charity directly to confirm if they currently have a campaign in progress.

Call the police if you notice suspicious individuals canvassing in your neighborhood.

In some instances children have been used to assist the con artist and scammer perpetuate this crime.

The Spanish Lottery Scam

You have just won the lottery!
(P.S. If you don't keep this a secret your prize will be null and void).

The Spanish Lottery Scam and its variants are becoming one of the newest advance fee scams to appear in the email boxes and fax machines of many people.

These scams are very much like the 'Nigerian Letter or South African Letter scams.

Originally named for the first variant of this scam using the large national lottery in Spain variants of this scam are now surfacing naming other lotteries.

Participants in this scam can become victims of Identity Theft as the targets are asked to provide SIN numbers and other important personal and financial information.

Other targets report attempts to lure the

individuals out of the country with cash needed to pay "processing fees" in order to complete the transaction.

Still others have been asked for funds and banking information.

The perpetrators expect that the targets are unfamiliar with the rules, regulations and procedures of how International lottery winnings are processed.

HEADS UP!

If you receive an email or fax solicitation claiming you have won the lottery do not respond to the request for information.

Typically lotteries do not require you to identify yourself in order to purchase a ticket.

Spoofing

There has been a recent flood of email purported to be from a bank, a large retailer or a purveyor of services. All of them follow the same general pattern. They indicate that there is a problem with your account or a transaction is pending and they need some follow up.

Included in the email is a link that you are told to either click or paste into your browser. In the older versions of this scam you were supplied a form that you were requested to fill out and send by return mail.

This link will take you to a web site often containing images and a "storefront" that resembles the purported business named in the email.

Once there you are instructed to fill out a form that requests amongst other things; your user name and password for your account(s), your credit card number, your bank account information or personal information like your Social Insurance Number.

HEADS UP!

Do not respond to these emails or follow the link listed in the email.

If you are concerned go directly to the corporate web site and read the information directly. Often corporate email addresses are listed that allow you to address your concerns to the proper individual or department.

Collect Call Scam

Calgary and Edmonton police are getting a lot of complaints from subscribers who have received "COLLECT" calls from individuals who are inserting the words "POLICE EMERGENCY" in the long distance prompt.

This is generally not a collect call but is usually a Bill to Third Party call that is going to Lebanon or Pakistan.
Due to the nature of the Telco networks tracking down these individuals is difficult and time consuming. Typically, the calls end up being traced back to prison phones or out of country pay phones.

The solution is to either NOT accept the charges from the unknown callers or choose operator assistance.

HEADS UP!

Police Departments do not operate this way in placing calls to people.

This is an old scam and still continues to flourish, even after the education efforts by the Telecommunication companies to prevent this fraud.

Variations of this scam include using the same last name to make someone believe that it is a relative that is calling, similar to the "friend in need" scams.

The net result is the same.

The customers are being tricked into accepting the charges for the long distance phone call.