Investment fraud on the Internet

The Internet is a quick and easy way for scam artists to find potential victims for their investment scams. With the Internet, fraudsters can operate anonymously from anywhere in the world, making them hard to catch. Once you've given your money to an online scam artist, it's likely gone for good.

Here are a few things to watch out for.

Spam e-mail

Spam is unsolicited e-mail that usually promotes a certain product or service, including investments. Because spam e-mails are cheap and easy to create, scam artists can use them to reach thousands of potential victims at a time.

Common types of spam

There are many types of spam e-mails that are really scams. Here are some of the most common.

Affinity fraud

Affinity fraud is a type of scam that targets groups of people who know each other. For example, victims could be members of online communities or social networking websites.

The Internet is a great environment for affinity fraud. Fraudsters take advantage of how easy it is for people to share information in chat rooms, on social networking websites or by forwarding emails. Victims of affinity frauds are often friends or family who innocently share information about the fake investment scheme.

Pyramid scheme

A common type of affinity fraud is the pyramid (or Ponzi) scheme. Typically, investors are recruited through promises of getting high returns quickly. Be wary of e-mails that promise you can "make big money working from home" or "turn $10 into $20,000 in just six weeks."

Early investors may receive returns fairly quickly from "interest cheques." They're often so pleased with their returns that they re-invest, or recruit friends and family as new investors. Here's the catch: The investment doesn't exist. The "interest cheques" are paid from investors' own money and the contributions of new investors. The scheme eventually collapses when the number of new investors drops.

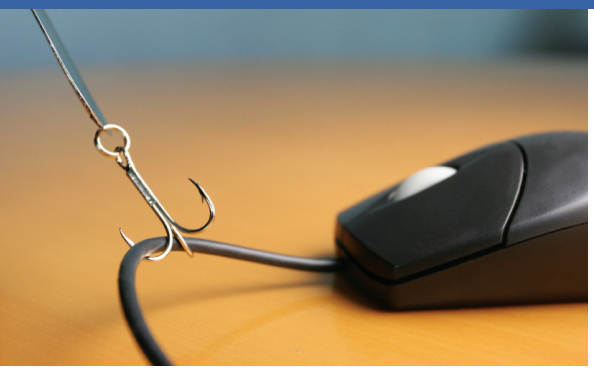
The pump and dump

In a typical pump and dump, you receive an e-mail promoting an incredible deal on a low-priced stock. What you don't know is that the person or company touting the stock owns a large amount of it.

As more and more investors buy shares, the value skyrockets. Once the price hits a peak, the scam artist sells their shares and the value of the stock plummets. You're left holding worthless shares.

You can read about more types of scams and their common warning signs in the CSA's guide, *Protect your money: Avoiding frauds and scams*.

CSA ACVM
Canadian Securities Administrators
Autorités canadiennes en valeurs mobilières



Spoofed websites

You may get an e-mail that looks like it came from your bank, credit card company or another legitimate business. These messages usually ask you to click on a link that will then take you to a fake or "spoofed" website. This website could look just like the company's real website.

On the spoofed website, you'll be asked to enter personal information like your:

- account number
- password
- credit card information
- social insurance number

The scam artist then uses your personal information to commit identity theft. This type of scam is often called phishing.

What you can do

Here are some things you can do to avoid falling for online scams.

Ignore spam

Never reply to spam e-mails. Even if you just reply to ask the sender to remove you from their mailing list, that tells them that they've found an active e-mail address. Instead, delete the e-mail and block further e-mail from that sender.

You can also install anti-spam software that prevents spam e-mails from reaching your inbox.

Don't give out your personal information

Banks, credit card companies and other legitimate businesses will never ask you to provide personal information through regular e-mail. If you get an e-mail that asks you for confidential information, do not click on any links provided and do not give out any information.

It's also a good idea to install software, such as anti-virus or anti-spyware programs, that can prevent fraudsters from hacking onto your computer to steal your information.

You may also want to avoid using public computers to access any online accounts. Many people have access to these computers, and if you leave any trace of your personal information behind, they'll have access to that, too.

Research your investments

The best way to protect your money is to be an informed investor. Before you buy any investment, find out as much as you can about it. Read financial documents like the prospectus and financial statements, which you can find on **www.sedar.com**. Public companies and investment funds are required by securities law to file these and other documents on the System for Electronic Document Analysis and Retrieval (SEDAR).

You can also get information from:

- analysts' reports
- financial newspapers and websites
- investment newsletters
- chat rooms and online communities

You can get a lot of useful information from these sources, but remember each source only forms part of the overall picture of a company. Be skeptical of what you read and check as many different sources as you can to get a more complete picture. You can also get a second opinion from an independent financial adviser.

Contact your local regulator

Securities regulators oversee Canada's capital markets and the advisers who sell and manage securities traded in those markets. You can contact your local securities regulator to check the registration of an individual or firm, and to find out if they have been involved in any disciplinary actions.

You can also contact your local securities regulator to find out what your options are if you think you've been scammed. For contact information, visit the Canadian Securities Administrators website at **www.securities-administrators.ca**.

CSA ACVM
Canadian Securities Administrators
Autorités canadiennes en valeurs mobilières