



Avoiding E-Fraud

Avoiding E-Fraud	1	E-Fraud Resources	3
Tips on How to Avoid E-Fraud	2		

An initiative of:

business
infosource
Canada - Saskatchewan
Business Service Centre

Funded by:



Western Economic
Diversification Canada

Diversification de l'économie
de l'Ouest Canada

Canada

Avoiding E-Fraud

As more and more people connect to the Internet, online fraud is on the rise. Although e-fraud is not commonplace (only about 0.03% of all business-to-consumer transactions), it does happen. Anytime you make an online purchase or sale you should be wary. Although impossible to eliminate, with the proper care you can ensure you are never the victim of online fraud.

For anyone who has ever been a victim of e-fraud, the problems with compensation can be endless due to the properties of the Internet. When online, you may never know exactly with whom you are dealing with; it may be someone who lives on the other side of the world. Resolving problems with someone you do not know can be more complicated in long-distance or cross-border transactions. Tracking people down is very difficult, as individuals who commit online fraud can disappear without a trace. Web sites can be created, and used to commit fraud, only to disappear soon thereafter. The almost complete anonymity of the Internet allows for many fraudsters to avoid being caught.

Types of E-Fraud?

Online fraud falls into many different categories - from unauthorized credit card use to false investment, and even sales from what seems to be a reputable company.

"The most common type of fraud on the Internet will be found in online auction dealings."

The most common type of fraud on the Internet is found in online auction dealings.

According to the National Consumers League fully 87% of Internet fraud comes from online auctions. When using online auctions you will rely on a seller you don't know to send you a product you have never seen. Sellers face a similar problem because they can never be sure if the buyer is on the up and up. Other high fraud areas to note include general merchandise sales (7%), Internet access services (2%), and computer equipment/software (1.3%). Credit card fraud is also something to be aware of. This affects everyone whether they are a buyer or seller. People can use your credit card number to make purchases or they can use someone else's card to purchase from you.

People have also made a living by practicing investment fraud over the Internet. Being able to reach large numbers of people through newsgroups, e-mail, and bulletin boards allows fraudsters to spread incorrect information almost instantly. People give false investment advice and then reap the rewards when individuals act on the advice.

Tips on How to Avoid E-Fraud

The Internet is no different from the real world in that, as long as you are careful, you can avoid problems. You would never buy a product from a stranger who telephoned you, offering something for sale and asking for your credit card number. So why would you buy something from a web site you know nothing about?

The best advice for avoiding e-fraud is very simple: Be careful. Avoiding e-fraud is not difficult, it just requires due diligence.

- When dealing with a company, before you make a purchase, be sure that they are someone you know and trust. Conduct research about the company to find out their track record and where they are physically located. Knowing as much as possible about the company will allow for a faster resolution, if there are any problems.
- Make sure you completely understand the offer. Read all the information about the products or services the company is offering. Ask for more information if you do not feel there is enough provided. Legitimate companies will have no problem sending you more information. If a company refuses or does not respond to your enquiries, do not take the risk of dealing with them.
- Never judge a web site by its appearance. Anyone can create a flashy web site. Just because it looks professional does not mean it is run by a professional!
- Never give out financial or other personal information, such as bank account or credit card numbers unless you are sure that the company is legitimate and the information is necessary for the transaction.
- Credit card payment is safest because you can dispute the charges if the goods are misrepresented or never arrive.

“Avoiding e-fraud is not difficult, it just requires due diligence.”

These tips can be applied in many different circumstances.

- Be cautious when using online auctions. Ebay has features that allow you to research the person you might be dealing with.
- There are also Internet middlemen you can use for online auctions. Escrow services like tradesafe.com can help you prevent being ripped off by holding your money until your purchase has been delivered.

Never trust investment advice received via e-mail, bulletin boards or newsgroups. If you feel a tip is genuine, research the company before you purchase.

For small business merchants credit card fraud is a very real problem. Most do not have the resources to discount lost sales. Because credit card laws protect the cardholder, there might be no recourse for a merchant, and they will end up without a product's payment. There are a number of web sites that are specifically designed to help small businesses deal with fraud. Antifraud.com offers business owners tools and resources to help fight fraud.

A fraud detection and risk management service available to online merchants is eFalcon (<http://www.efalcon.com/>). Some merchants have taken strong measures towards making their sites fraud-proof, by not accepting orders from people who use web-based e-mail addresses (eg. @hotmail.com, @yahoo.com etc...); often it is difficult to ascertain the identity of the address owner. Most online fraud is committed by individuals using web based e-mail addresses.

E-Fraud Resources

There are a number of informative sites that deal specifically with combating e-fraud such as www.scambusters.org and www.fraud.org. Scambusters has a free newsletter full of the latest information about Internet scams and viruses.