Fraud Prevention Tips for Online Buyer

During the last few years there has been an increase in online fraudulent of global scope and geometrically increasing proportions. There are now actual companies that specialize in spam and other illegal marketing techniques, like Phishing and Hacking, which take every opportunity to make a few pennies. Even though their net income per person is miniscule, it becomes significant when multiplied by hundreds of thousands or even millions. Added to this threat are the man amateur fraudulent artists around the world who troll the Internet for credit card and financial information to use for fraudulent purposes. Finally, identity thieves are reaping high rewards at the expense of both the target and the online retailer.

Below are advice and tips for credit card customers or buyers when receiving an e-mail that may be fraudulent:

1. Buyers need to be cautious about e-mails that offer credit services because many unsolicited e-mails are fraudulent. Buyers also should not simply click on Internet hyperlinks within received e-mails. Instead, buyers can type in the known URL into the address bar of the web browser.
2. Buyers need to be wary of e-mails which offer prizes or discounts and then asking them to choose a User ID and Password. Most people use the same access information for several accounts because they are easier to remember. The thieves will collect your login information and try them at other sites, like financial institutions or credit-card sites.
3. Buyers should never respond to e-mails that request for credit card information and also do not ever respond to e-mails that ask them to go to a website to verify personal (and credit card) information. If buyers have doubts about the authenticity of an e-mail, do not respond to the e-mail. Alternatively, they can call the sender to verify or manually type in the web address.
4. Buyers need to be wary of e-mails with a sense of urgency which attempts to rush buyers into action. For example, "Update now or we'll close your account… …" Please note that fraudulent e-mails often include misspelling and poor grammar within the e-mails.

Additionally, below are advice and tips for both Credit card customers and Merchants when purchasing items over the Internet:

1. Buyers and merchants must not open e-mails from unknown senders. Merchants should not simply process credit card orders that originate from free e-mail addresses or from e-mail forwarding addresses. In such cases, merchants should ask the buyer for an ISP or domain-based e-mail address that can be traced back before processing the order.
2. Buyers must only give their credit card details to reliable websites which are from reputable companies. In addition, reputable merchant sites usually use encryption technologies to protect credit card information.
3. Merchant should not process credit card orders unless the credit card information of that buyer is complete. If the shipping address and the billing address on the order are different, merchants need to call the buyer to confirm the order. Merchants may even want to make it a policy to ship only to the billing address on the credit card.
4. Buyers must be very careful with to whom to give personal identification information, such as mother’s maiden name and social security number. Buyers have to ask if the information can be kept confidential and inquire how it will be used and with whom will the information be shared.
5. Buyer also must never send account information, such as account numbers or PIN in an e-mail as it may be intercepted.

Besides the advice and tips on how to prevent credit card fraudulent above, buyers also can apply fraudulent detection web services such as FraudLabs™ Credit Card Fraud Detection Web Service from FraudLabs™ in order to reduce credit card fraudulent.

Fraud Prevention Tips for Online Buyer

FraudLabs™ Credit Card Fraud Detection Web Service is the proprietary credit card fraudulent detection service that is integrated with our IP2Location™ technology (geolocation service provider) to reduce credit card fraudulent for buyers. It screens and detects online credit card fraudulent where every transaction goes through a strict assessment process which reviews over a dozen aspects of online purchase parameters to determine high risk orders, such as IP address, email address and billing address and returns fraudulent analysis results together with a fraudulent score in real-time. Through our analysis, we have been able to identify traits and patterns that are associated with fraudulent orders, before the payment is processed.

Please visit http://www.fraudlabs.com for more information about the FraudLabs™ Credit Card Fraud Detection Web Service, or email sales@fraudlabs.com.