in touch
in business®

inspire inform involve insight
"it's everybody's business"

In Web with Nicky Jurd
Protect Against Credit Card Fraud

ACCEPTING CREDIT CARDS IS AN ESSENTIAL STEP IF A BUSINESS IS TO PLAY IN THE ECOMMERCE WORLD.

While there's a lot of talk surrounding the risk of using your credit card to pay for purchases online, few businesses realise there is a far greater risk they will bear the financial burden of a fraudulent credit card transaction. With some careful planning, and common sense, you can avoid being caught out by some very clever tricksters.

How do the scams work?

An online credit card transaction is similar to a telephone, mail or fax order is that it is considered by your bank as a card not present transaction. As a business who accepts credit cards, most banks consider merchants responsible for charge backs, which can leave you out of pocket.
Here's a simple scam example: You are an online retailer and you have send goods to an address. The goods were paid for with a recently stolen credit card number and the owner issues a charge back. The bank refunds the credit card owner, and you are out of pocket for the goods sent, and the postage paid.

What should you do?

You are responsible for ensuring you are charging your customer's credit card. This is tricky when you are transacting with someone you've never met, and you're unable to see the card and check their signature. There are some things you can do to minimise your risk and exposure to fraud, but understand some methods pour ice on your sale.

Use a real-time credit card payment system

When your website uses a real-time credit card payment system the customer receives immediate notification if their transaction has been approved or declined. During the transaction the bank will check the number against known stolen credit cards.

This method also removes the significant burden of storing credit card numbers in a secure online environment as the card is charged immediately by your bank. This system ensures you are not the victim of a hack on your website to obtain credit card numbers for fraudulent use.

Ask for the card security code

Also known as a card verification method, the security code is a 3 or 4 digit number which is not recorded in the credit card's magnetic data strip and is not recorded on transaction receipts. This means the only way to know a security code is to read it off the card, and this ensures the customer is holding the card and reducing the change of you taking a transaction from a recently stolen number.

By collecting the security code, even if you are unable to confirm the number this will still provide some protection from fraud. For instance, if a person is unable to give you the security code there's a strong chance they do not actually have the card in front of them, in which case you can decide if you would like to continue with the transaction.

Collect your customer's personal details

Ensure you ask for a customer's postal address, physical address, phone number, email address and any other details you might require to do business with your customer. Their willingness to part with these details may be an indicator of fraud.

Check their physical address carefully for the possibility of a bogus address, and consider doing a search on Google Maps to check the legitimacy of the address. You may also consider not posting goods to a shortlist of countries known for high levels of credit card fraud such as Nigeria, Indonesia and Romania.

Be smart

Although we always associate caveat emptor with buying a product, sellers must also use the same common sense a buyer would. If a transaction seems too good to be true, it probably is.

Nicky Jurd

Partner - cityofcairns.com

This article appeared in the February 2009 Edition of the ITIB Magazine