

Consumer Affairs Victoria

eCommerce Factsheet

Online security

June 2004

When you're considering the safety of using credit cards for online purchases, you need to ask yourself two things: How safe are my credit card details while they are travelling over the web? How safe are my card details once they reach their destination?

Need more information?

Call Consumer Affairs Victoria Helpline on 1300 55 81 81

Key Term

Phishing - Scammers send out spam that pretends to be from a particular well-known company. The message says the receiver needs to click on a link in the message and enter some personal information such as credit card details. Criminals then use the credit card or steal funds from bank accounts.

Keep your details safe

The Internet is a great place to search for information, join virtual communities, or shop with convenience from a greater choice of stores and products. But the Internet also attracts fraudsters looking to take advantage of people who don't take precautions.

Your credit card, account numbers, passwords, and other personal details are very desirable to criminals. They want to drain funds from your bank account or purchase items and have you pick up the tab.

Don't provide credit card or account numbers unless you are certain they will be used appropriately.

Get used to thinking about the following issues and soon they will become second nature when surfing the Web:

- Check the authenticity of the website. Do you know this trader? Verify the domain name displayed on your browser's website address line, or access websites of online stores through your browser's bookmarks. For Australian company sites, look for the ".au" ending in the browser's website address line.
- Don't send credit card numbers via e-mail. Only enter card details on a secure website with a locked padlock or key icon. You can double-check the site's authenticity by double-clicking on the locked padlock icon. The "subject" within the "details" tab should correspond with the name of the company or bank.

Key Term

HTTP
(Hypertext Transfer Protocol) – A set of rules that govern how information and data are sent and received over the internet.

Key Term

HTTPS
(Hypertext Transfer Protocol over Secure Socket Layer) – A protocol that is built into browsers that encrypts and decrypts web pages sent over the internet.

- Don't respond to e-mail messages asking you to click on a link and enter credit card or other details. Be wary of messages with phrases such as: "Urgent, system problems", "Bills or charges due", "Provide your account details to reactivate your account", and "You have won a free gift." These messages are usually fraudulent and may be a "phishing" scam. Legitimate companies and banks do not send e-mail messages asking for credit card or account details.
- Never access Internet banking sites from public computers (e.g. in a cybercafe) or from hyperlinks sent in e-mail messages.
- If in doubt, contact the business on the telephone.
- If you think you may have sent personal details to a suspicious site or in reply to a suspicious e-mail, contact your bank or credit card provider right away.

How safe are my credit card details as they travel over the web?

That depends on whether the trader uses a secure ordering system. A secure ordering system protects a buyer's credit card details while they are in transit over the web.

Both standard internet browsers, Netscape Navigator and Microsoft Internet Explorer, use a method called Secure Sockets Layer (SSL) to transmit data securely. SSL encrypts or scrambles your data before sending it over the web.

You can tell if your data is being encrypted if there is an unbroken key or closed padlock at the bottom of your browser window. The web address at the top of your browser should also start with `https://` instead of `http://`.

SSL technology provides a secure connection that keeps your data private during transmission over the internet. Even if someone managed to intercept your order while it is in transit over the web, they would not be able to decrypt or unscramble the data.

How safe are my card details once they reach their destination?

This depends on how the trader processes online orders and how secure their arrangements are for protecting any information they receive.

Many traders have an arrangement set up with their bank so that all payment details are sent directly to the bank without going through the trader's computer system. The bank processes the payment and notifies the trader that the payment has been approved. This means that your credit card details are never known to the trader and can't be stored on their computer system.

Other traders, however, do receive your credit card details with the order and process the payment with the bank themselves. When traders use this arrangement, you need to be sure they will keep your credit card details safe.

Check the trader's security policy

It's easy to tell whether a trader is using encryption to protect credit card details while they are in transit – the address line starts with `https://` instead of `http://` and there is an unbroken padlock or key at the bottom of the browser window.

But, unless the trader actually tells people, there is no obvious way to determine how the trader is processing online orders or what they are doing with their customers' credit card details.

An online business that asks you to trust them with their credit card details should provide a document that describes the company's security policy. The security policy should detail:

- The level of encryption used in the SSL process. 40-bit is the minimum. The next most secure level – 128-bit – is the level of encryption used by most banks.
- Whether the trader uses a bank's payment gateway or its own ordering system to process an order; ie, whether the trader sees and stores credit card details or whether they are passed unseen directly to a bank.
- If the trader processes the order, how long it stores credit card details and how it protects them against outside predators and its own employees.

Date of Issue:
June 2004

What to do if something goes wrong

If unauthorised transactions start to appear on your credit card statement, you should raise the matter directly with the institution or bank that issued the credit card.

In Australia, all account institutions that sign up to the revised EFT Code of Conduct must have complaint-handling procedures that meet certain minimum standards.

The account institution can't get out of their obligations to you because another party involved in the transaction caused the problem. Possible other parties include other account institutions, telephone companies, internet providers and merchants.

You don't have to make an additional complaint to one of these other parties. You can simply make the complaint to your account institution. They will then follow up on the complaint with the other parties.

More information

Information on eCommerce is available from:

**Consumer Affairs Victoria
Victorian Consumer &
Business Centre**

113 Exhibition Street
Melbourne 3000

Telephone: 1300 55 81 81

Website www.consumer.vic.gov.au

Useful Contact

FIDO

The Australian Securities and Investment Commission's consumer watch site that contains information and alerts about investment scams and fraud, and publishes the revised EFT Code of Conduct. Visit their website at www.fido.asic.gov.au.

Further reading

Consumer Affairs Victoria has a range of eCommerce related factsheets:

- Buying a computer
- Domain names
- Getting a refund on the web
- Internet service providers
- Online auctions
- Online privacy
- Online scams
- Shopping online
- Spam
- Tips for business
- Top 10 tips for shopping online



The information contained in this fact sheet is of a general nature only and should not be regarded as a substitute for a reference to the legislation or professional advice.
Authorised by the Victorian Government, 121 Exhibition Street, Melbourne, Victoria, 3000.
Printed by Midway Press Print Management, 9 Third Avenue, Sunshine, 3020.
eC-04-02-908