



Quick Guide to Safer Shopping

- ▶ Seven tips for secure online shopping
- ▶ Protect yourself from email and phone scams
- ▶ How safe are you? Test your security IQ

Visa lets you buy with confidence

You can feel confident about safety when you use your Visa credit, debit or prepaid card. Our multiple layers of security help prevent, detect, and resolve unauthorized use of your card information. And if fraud should occur, you will not be held liable for unauthorized charges.

Visa's Zero Liability policy¹ is our guarantee that cardholders will not be held responsible for fraudulent charges made with a Visa payment card.

Whether you are shopping online or in person you can get your money back if something goes wrong.

For instance, if:

- You're the victim of online fraud
 - Your goods aren't delivered
 - Your order arrives damaged.

Take the time to look at your monthly Visa statement and let your financial institution know as soon as possible if anything appears incorrect.

¹ - Visa's Zero Liability policy covers Australian and New Zealand-issued cards and does not apply to ATM transactions, PIN transactions not processed by Visa, or certain commercial card transactions. Cardholder must notify issuer promptly of any unauthorized use. Consult your issuer for details.



✓ Seven tips for safer online shopping



We all love the convenience of buying things over the internet, and it's safer than you think. The vast majority of online transactions go through safely - but there are also steps you can take to be a safer online shopper.

1. Make sure your computer has a **firewall** installed and keep your browser software and **anti-virus** program updated.
2. Never send payment information by **email**.
3. Shop with retailers you know of, or research them first to ensure they are **reputable** and reliable.
4. Make sure that your card details will be **encrypted** securely before being sent across the internet - look for an unbroken key or lock at the bottom of your browser window or check the website address, which should begin **https://** rather than **http://**.
5. Keep a **record** of your internet transactions, including the retailer's website address and telephone number.
6. Before buying, read the delivery and return **policies** that should be on the retailer's website. Can unsatisfactory items be sent back? If the items are faulty, can you get a refund or a credit note?
7. Use your Visa card and activate **Verified by Visa** - a free authentication service that provides password protection to ensure both you and the retailer are genuine.



Phoney fraud alert

Scams can come in the form of an email or a phone call claiming to be from your bank or financial institution. The scammer will usually tell you that your credit card or account has been cancelled because it was involved in criminal activity, or because they suspect your card or details have been stolen.

The scammer will ask you to confirm your card details so the “bank” can “investigate”. You may be advised to contact a fake fraud investigations body, or discouraged from contacting your bank or credit union.

If you receive a phishing email, it may ask you to visit a website to confirm your credit card details or to find out more information on the supposed fraud to your account.

What you can do

There are a few things that you can do, which will help you to avoid these types of fraud. If you receive an email claiming to be from Visa or a financial institution that asks you to enter your account details - delete it! Visa will NEVER send an email like this.

Never enter your personal, credit or debit card information on a website that you are not certain is genuine. Check the website address carefully. Scammers often set up fake websites with very similar addresses.

Visa plays an active role against scams such as phishing and works closely with industry partners and law enforcement agencies to shut down phishing websites. In the past year alone, Visa deactivated 85 percent of reported phishing attacks within 48 hours of notification.² If you receive a fraudulent email claiming to be from Visa or one of our issuing financial institutions that request your personal account information, you can forward it to phishing@visa.com.

2 - Source: RSA Repository 15 October 2007 - 15 October 2008 Data

Smarter ways to keep you protected

Verified by Visa

Verified by Visa is an easy way to increase the security of your online shopping experience. By adding a password to your existing Visa card, Verified by Visa ensures that only you can use your Visa card online. It's easy to activate for your existing Visa card, and it's free.

You can set up your Verified by Visa password through your card issuer and activate your card in just a few minutes. Once you activate your card, Verified by Visa protects you at every participating online store. All you need to do is enter your password when prompted during the transaction process.

Chip security

Visa and its partners are introducing chip technology to provide an extra layer of security. When a chip card is used at the point of sale, the transaction message sent by the chip card to authorize the transaction does not contain any data that can be used to counterfeit a chip or conduct an unauthorized chip transaction reusing the data from a previous transaction.

If you are travelling overseas with a chip card, it's a good idea to know your PIN number as many countries may require you to use your PIN instead of a signature to authorize a transaction.





Test your security IQ



THINK YOU KNOW IT ALL WHEN IT COMES TO CARD SECURITY?

Put yourself to the test with this quiz.

1. I keep a list of all my cards and their numbers in a safe place.

- a) yes
- b) no

2. I consistently check my card statements for accuracy of personal and billing data?

- a) yes
- b) no

3. I have up-to-date antivirus and anti-spyware protection installed on my computer?

- a) yes
- b) no

4. When discarding financial documents, I keep them folded in their envelopes

- a) yes
- b) no

5. I only respond to emails that ask for my personal financial information if they are from my bank

- a) yes
- b) no

6. I use the same username and password for all my accounts

- a) yes
- b) no

7. I always count my cash the moment I take it from an ATM?

- a) yes
- b) no

8. If someone else uses my Visa Debit card and I did not authorize the transaction, am I liable for the cost?

- a) yes
- b) no

9. Which of the following is better for detecting fraudulent card activity?

- a) Paper statements
- b) Online statements

10. Where is the cardholder verification number printed?

- a) on the front of the card
- b) on the back of the card
- c) in my monthly statement

Check your answers in the next column.

Security Quiz Answers

1. **(a)** Always keep a list of your cards, card numbers and customer service phone numbers in a safe place in case they are ever lost or stolen.
2. **(b)** Always check your card statements for accuracy to ensure there is no fraudulent activity.
3. **(a)** Keep your anti-virus and anti-spyware software up-to-date to help prevent fraudsters from getting your information.
4. **Always** shred any financial documents when you discard them.
5. **Never** respond to any email from Visa or another financial institution asking for personal data.
6. **It's** a good idea to use different usernames and passwords for all your accounts.
7. **Don't** count your cash at an ATM; wait until you are in a safe place
8. **No**, Visa's Zero Liability policy protects you from unauthorized purchases.
9. **Using** online statements provides a faster way to check for fraudulent activity between monthly paper statements
10. **The** cardholder verification number is on the back of your card.

▶ **9-10 correct:** top of the class;

▶ **5-8 correct:** you can improve your score by learning good safety habits;

▶ **1-4 correct:** you need to brush up on your safety habits!



✓ There's no safer way to shop than with Visa

HELP FOR A LOST OR STOLEN CARD

No matter where you are in the world [Visa Global Customer Assistance](#) will help you 24 hours a day, seven days a week.

What you should do ▶

■ If you are close to home

Immediately contact your financial institution to report the loss or theft and arrange for a replacement card to be mailed to you.

Keep a copy of the name of the financial institution that issued your card, its customer service phone number, and your Visa account number in a convenient place - separate from your card.

■ If you are travelling away from home

Before you leave on a trip, make a note of the toll-free emergency number for your destination and keep it with you, but separate from your card.

Immediately contact [Visa Global Customer Assistance](#) using our worldwide network of toll-free telephone numbers on our website.

In Australia - 1800 450 345

In New Zealand - 0508 600 300

Or place a collect call to +1 443 641 2004.

