



AFP

AUSTRALIAN FEDERAL POLICE



AUSTRALIAN BANKERS' ASSOCIATION INC.

ONLINE SHOPPING FACT SHEET

TIPS FOR SHOPPING SAFELY ONLINE



1. If it looks too good to be true, it probably is

Beware of get rich quick schemes or products with extraordinary claims or financial products with extraordinary returns. Use some common sense before purchasing or signing up to products and services.

2. Shop at secure websites

A secure website uses protective encryption technology to transfer information from your computer to the online merchant's computer system which keeps safe confidential information such as credit card details. Identify a secured website by looking for "https" in the web address or URL (an unsecured website address starts with "http").

3. Research the merchant before placing an order

Do business with companies you know and trust. Reliable companies should advertise their physical business address and at least one phone number, either for customer service or for ordering products. Call the phone number and ask questions to determine if the business is legitimate.

4. Read the website's privacy and security policies

Read the terms and conditions of the contract to make sure you understand the delivery options/charges, return policy, and product or service warranty. For international transactions, ensure you are aware of the current exchange rate and any applicable duties and taxes. Ensure the business has a fair and clear process for submitting complaints and/or cancelling orders.

5. What is the safest way to pay?

The safest way to pay online is with a credit card or a scheme debit card¹ because consumers can dispute the charges if something goes wrong. Using a single credit card for all online purchases can make it easier to track any irregularity on your account.

Consumers can dispute a transaction if:

- Mail order goods fail to arrive, or arrive broken, or faulty;
- You get charged for a transaction twice, or for a higher amount than you authorised;
- You cancel a direct debit authority but the merchant is still directly debiting your account;
- Your credit card is stolen and is being used illegally to buy things – either by forging your signature or buying things over the telephone or online.

¹ These are cards issued by banks using a scheme network such as Visa or MasterCard. A scheme debit card transaction involves a cardholder accessing funds in a deposit account.

Usually, in these circumstances, your card provider will reverse the transaction immediately. The provider then seeks a chargeback from the merchant's bank. Unless the merchant can establish that you, or the secondary card holder, did in fact receive the goods or authorise the transaction, the reversal will remain in place. Time limits do apply to reversing transactions, so always check your statements carefully and take immediate action if you cannot account for a transaction that you see. Statements can also be checked via telephone and Internet banking.

6. Provide only necessary information about yourself

Sometimes businesses request large amounts of information they don't need, so think about limiting the amount of information you provide. Never send your credit card number by email. Emails are not secure.

7. Save all transaction details

Print out or make note of the seller's identification, the item description and the time, date and price you paid or the bid on the item. Print and save copies of your order confirmation screen and all email communications.

8. Keep your password private

Most e-commerce websites require shoppers to log-in before placing or viewing an order. The shopper is usually required to provide a username and a password. Never reveal your password to anyone.

9. Check the website address

By checking the web address of the company and typing in the URL (Uniform Resource Locator), you can make sure that you are dealing with the correct company.

Banks and other legitimate businesses don't ask for sensitive information via email. Don't respond to any request for financial information that comes to you in an email. Don't click on any link embedded within a suspicious email, and always call the retailer or financial institution to verify your account status before divulging any information.

Buyers can also research a website to see how long the site has been online and where it is hosted, see <http://www.domaintools.com>.

10. Install and keep up to date a firewall, anti-virus software and anti-spyware software

This provides additional layers of protection that help to reduce your risk of exposure from viruses that can rob your computer of valuable personal information.