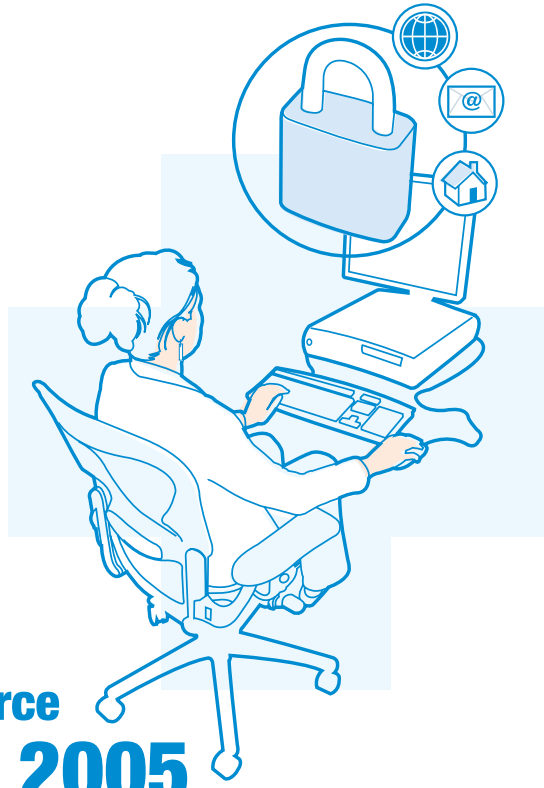


Australian e-Commerce Safety Guide 2005

Alastair MacGibbon, eBay Australia and New Zealand Trust & Safety Director

Alastair MacGibbon is a respected authority on Internet security.

At eBay, Alastair heads the Australian and New Zealand Trust & Safety team. Alastair is responsible for educating consumers about online safety, building partnerships with industry and government and assisting in the development of new technologies that keep eBay at the forefront of online safety.

Alastair also works closely with Australian and international law enforcement agencies to help bring offenders to justice.

Alastair has 15 years of national and international policing experience and is the founding Director of the Australian High Tech Crime Centre (AHTCC) - a national law enforcement unit hosted by the Australian Federal Police to coordinate Australia's efforts to combat serious crime involving technology.

During his time with the AHTCC, Alastair pioneered new thinking in law enforcement approaches to high tech crime investigations and harm minimisation strategies including innovative industry engagement and aggressive co-option of public sector agencies to the Centre.

Previously as a federal agent with the Australian Federal Police he served in numerous roles in Canberra, Sydney and Melbourne before becoming the AFP Overseas Liaison Officer at the Australian Embassy in Washington DC for three years.

Alastair is a graduate of the US Federal Bureau of Investigation's National Academy and has a Bachelor of Arts and a Master of International Studies from the University of Sydney.

Contents

Introduction from Alastair MacGibbon 4

Why shop online? 6

Australians' concerns about online shopping 7

Avoiding fraud: Shopping safely online 8

Sensible precautions for online shopping 9

Case study #1 13

Deterring identity fraud 14

How personal information is stolen 15

Preventing identity fraud 16

What consumers should do if they become identity fraud victims 19

Phishing: fraudulent spammed spoofed emails 20

Case study #2 22

Identifying fraudulent emails 23

Phishing tips and tools 24

Companies that offer online shopping protection 26

Eight reasons to feel confident shopping on eBay 29

Six rules for protecting your home PC when online 31

Recommended Australian resources 36

Introduction from Alastair MacGibbon

The Internet is a part of most Australians' everyday life and there is little wonder why – with easy access to a vast array of resources, services and information the Internet is highly appealing.

We use the Internet for work, play, education and increasingly for shopping. More Australians are shopping online than ever before. We have witnessed this at eBay Australia with the number of bidders on the site growing 75% in one year from December 2003 to December 2004. In fact eBay is the number one shopping destination in Australia, with over 2.7 million unique visitors in December 2004 according to AC Nielsen NetRatings.[1]

Evidence suggests that Internet shopping will continue to gather momentum – the convenience, selection and value for money is hard to resist.

An October 2004 survey undertaken on behalf of eBay by Sweeney Research found that the majority of Australian Internet users (67%) believe that online shopping is becoming safer.[2] While the survey suggests that confidence in online shopping is increasing it also points to a number of lingering concerns held by Internet users and non-users alike. Almost half of all people surveyed were concerned about using their credit card online. Even among Internet users surveyed, 37% expressed concern over this matter.

[1] eBay calculation based in part on data reported by ACNielsen through its Australian Internet User Survey of regular Internet users, July to December 2004, for the Australian Online shopping market (Copyright 2004, ACNielsen).

[2] Survey conducted by Sweeney Research, Understanding the Perceptions & Attitudes of the Australian Population: Trust &Safety Online Shopping, October 2004. Study no. 14240

The survey identified many other interesting attitudinal trends, including:

- 53% of people surveyed were concerned about their credit card details being intercepted
- 50% of people surveyed are worried about hackers obtaining personal/financial data
- Yet 60% of online shoppers believe that online shopping is becoming safer due to the range of safe payment methods available
- The 25-34 age group and higher income households have fewer concerns overall
- Concerns about online security increase with age – people over the age of 35 are more likely to read security policies frequently or every time they make an online purchase

Above all, the survey reveals that there is a need for sustained consumer education on Internet shopping.

This booklet has been produced with consumers in mind and provides a guide to e-commerce safety in an easy to read format.

There is no silver bullet to ending online crime but I firmly believe that the first and best step in the fight is empowering people with the information they need to make sensible decisions. I trust that you will find this a useful resource.

I would like to thank the many organisations and people who came together to facilitate the creation of this resource.

Alastair MacGibbon
Trust & Safety Director
eBay Australia & New Zealand

Why shop online?

The impact of the Internet on our lifestyle has been immense. Today, people from all walks of life access entire libraries, entertainment venues, post offices and financial centres from their workplace, home, a desktop or a shirt pocket all via the Internet.

Shopping online for a range of everyday items such as cars, gifts, homewares, fashion, gadgets and groceries from the comfort of your lounge room is an everyday occurrence for many Australians.

The ease and selection that the Internet provides shoppers has changed the face of retailing. More and more consumers visit a shop's website to make their choices before going to the shop itself; and in a rapidly swelling tide, many shoppers bypass the store altogether and order directly from the websites of their favourite brands and outlets.

Online stores are open 24 hours a day, seven days a week and their inventories are often more complete than those of their brick and mortar counterparts. The Internet makes it easy for shoppers to compare products within or between stores, to read product reviews from other customers and authorities, to access vendor return policies and to find warranty information.

Australians' concerns about online shopping

Increasingly, Australian consumers are expecting merchants – from major department stores to specialised small businesses – to make their products easily available on the Internet. They are also expecting these online retailers to make transactions simple and secure.

The October 2004 Sweeney survey shows that the majority (67%) of Australian Internet users believe that buying online is becoming safer. 60% of people surveyed said this was largely due to the increasing range of safe payment systems available.

The survey also reveals the top security concerns of Australian Internet users, which are:

- Credit card details being intercepted (53%)
- Hackers obtaining personal/financial data (50%)
- Not being reimbursed if something goes wrong (44%)
- Not receiving the exact item purchased (42%)

"Online transactions can be as secure, if not more secure than payments made by mail or in a shop; and fraud can be avoided if consumers understand a few simple steps they should take when they buy and sell online."

Avoiding fraud: Shopping safely online

Online fraud can take many forms from non-delivery of goods to non-refund of damaged goods. In many cases, both online and offline fraud can be deterred by following a few simple practices.

Offline consumers should take measures to protect themselves in brick and mortar stores, such as:

- not leaving a purse in an unattended shopping trolley
- concealing their PIN (personal identification number) at checkout
- not carrying large amounts of cash in their wallets
- not letting their credit card out of sight after it has been handed over for payment

Similarly when they are online shoppers need to take sensible precautions when buying goods.

Do not let your credit card out of sight after it has been handed over for payment

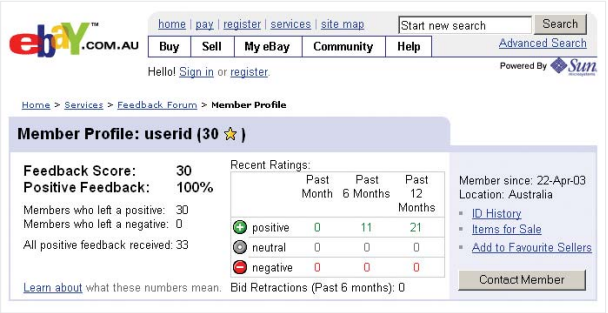
"Online crimes mirror those of the offline world. As such many solutions to online and offline crime are the same. Empowering individuals to make sensible decisions and an open and transparent community are the foundations of any crime-fighting strategy – the Internet provides a platform that easily enables this."

Sensible precautions for online shopping

1. Learn as much as possible about the product and seller: Shoppers will feel more secure and confident if they are familiar with the merchants from whom they are buying.

The Internet offers a platform for retailers to provide information about their companies and histories. Shoppers are empowered to undertake research about the products and companies. Shoppers might also learn about a retailer from their reputation, previous purchases, referrals through friends or reviews and comments by other shoppers found online.

Asking the seller questions is another simple way to obtain more information on a product and get a sense of the seller's customer service standards.



eBay's feedback and rating score can be used to assess members' online trading history

Sensible precautions for online shopping

Continued...

2. Understand retailers' refund policies: Look for and ask about refund policies. Questions to ask should focus on:

- the required timeframe in which a buyer must contact the retailer and return the items
- whether a full refund will be offered or a merchandise credit provided
- whether an item that has been opened or used can be returned

For retailers without refund policies, consumers may be able to access buyer protection programs from either the shopping site or through the payment method they use. This ensures that if there is a problem that the payment will be covered or refunded as a result of the protection guarantee - for example, many credit cards have chargeback facilities.

Online consumers are afforded the same legal protection as offline consumers. According to the Australian Competition & Consumer Commission "Australian consumers purchasing goods online have the same rights as those purchasing goods in a shopping centre."[3]

3. Choose a secure password to protect account information: Many people use passwords for online stores that can be guessed, like their birthday, a family member's name or even their username. Instead, a password should contain a combination of upper and lower case letters and numbers and symbols that no one else can guess. You should also use different passwords for different accounts. It is also helpful to periodically change your password to help ensure that it cannot be guessed.

4. Use a secure checkout and payment process: When paying online, consumers should take precautions when entering credit card or bank account information at each online

[3] Australian Competition & Consumer Commission media release "ACCC warns online trading must comply with consumer protection laws", 23 September 2004.

retailer they visit. Entering these details on several different merchant websites increases the likelihood of your personal information being compromised. There are safe and easy-to-use payment services which allow shoppers to enter account information only once into a highly secure and reputable site that protects this financial information from improper use. Future purchases should be made from that one account to avoid the need to enter credit card or banking information separately into the websites of individual retailers.

Additionally, many websites use a technology called Secure Sockets Layer (SSL) to encrypt personal and financial information sent over the Internet. A browser will display the icon of a locked padlock at the bottom of the screen to indicate encryption. Also consumers can look for third party seals that accredit sites with safe handling policies and procedures such as the VeriSign or TrustE logos.

5. If an offer sounds highly suspicious or too good to be true, it probably is: While Internet shops frequently offer lower prices than brick and mortar stores, shoppers should be wary of unreasonably low prices or unusually attractive promises. With any purchase online or offline, shoppers should read the fine print (or, in some instances, click the links describing the purchase agreement). If in doubt, don't proceed with the purchase – there will always be other options available when shopping online.

6. Protect your computer: Each computer connected to the Internet must have up-to-date anti-virus and anti-spam software as well as firewall protection. These are the first steps in a number of protective measures that are outlined by the Australian Computer Emergency Response Team (AusCERT) on pages 31-35 of this booklet.

Sensible precautions for online shopping

Continued...

7. Read and understand safe trading guidelines: Always follow the safe trading guidelines provided by the site you are shopping on.

8. If you don't receive the item you paid for: Retain copies of all correspondence and communication as this may help solve disputes between buyers and sellers. Communicate with the seller or retailer. If this fails, contact the service or financial institution used to make the payment to see if it can be reversed. Contact your local police service to make a complaint if you are willing to provide a statement.

What to do if you think fraud has occurred

"First and foremost, a buyer should contact the retailer from which the product was purchased. If agreement can't be reached, the consumer should contact either the payment method or service used to dispute charges and finally contact the police to report the incident."

Case study #1

Chargeback facility provides recourse

Sydney school teacher Angela heard a lot about eBay from friends and family who regularly bought and sold on the site. So when Angela needed to buy a birthday present for her sister she decided to try eBay.

While searching for a gift, Angela found a bracelet that her sister had always wanted. Prior to making a bid on the bracelet she did not read eBay's safe trading guidelines. Angela had been told to check a seller's feedback score, which she did but she forgot to read the comments left by other buyers about the seller in question.

Throughout the process the seller maintained active communication and Angela was elated when she finally won the auction. She was particularly pleased that the bracelet was scheduled to arrive in time for her sister's birthday.

However, as the birthday approached and the bracelet did not arrive, it became apparent that there was a problem. Angela emailed the seller but did not receive a response.

Angela proceeded to check the seller's feedback messages and discovered that many other people had recently suffered the same problem.

She immediately emailed eBay, who advised her to contact her financial institution. Angela had paid using her credit card with a chargeback facility and was able to claim back the cost of the bracelet. By reporting the problem quickly the bank was able to reverse the payment and the issue was resolved.

Deterring identity fraud

Identity fraud affects consumers at home, at work, in shopping centres and on the Internet. The Australasian Centre for Policing Research defines identity fraud as "the gaining of money, goods, services or other benefits through the use of a false identity."[4]

An Australian Government report estimated that the cost of identity fraud in Australia was $1.1 billion for 2001-2002.[5] This figure does not account for the non-financial costs to organisations or victims, "nor the amount of undetected identity fraud."

According to a recent US survey, identity thefts are more common offline than online, and also eight times more expensive for their victims. So while online victims suffered losses averaging US$551, their offline counterparts lost US$4,543 on average. One contributing factor for this gap was the ease and speed with which online customers can detect an anomaly.[6]

Shopping and paying bills online helps consumers to review their account information and transaction history quickly and easily. Online bill payment and statement review also reduces the risk of a paper trail being available for misuse by criminals.

[4] Standardisation Of Definitions Of Identity Crime Terms Discussion Paper, prepared by the ACPR (for the Police Commissioners' Australasian Identity Crime Working Party (AICWP)) and the AUSTRAC POI Steering Committee May 2004

[5] ID Theft: A kit to prevent and respond to identity theft, by the National Crime Prevention Program. Published February 2004. ISBN: 0 642 21084 5

[6] Research by Javelin Strategy and Research and Better Business Bureaus, Inc. for "The 2005 Identity Fraud Survey Report" released 26 January 2005.

"In recent years there has been publicity surrounding identity fraud perpetrated via the Internet. However, the majority of identity fraud actually occurs in the offline world when a thief obtains an individual's personal financial information, such as credit card numbers, through the mail or their discarded rubbish."

How personal information is stolen

Stolen credit cards, credit card numbers and bank account numbers are some of the types of information criminals can use to perpetrate identity fraud. Such information allows a criminal to access existing credit cards and bank accounts and may assist them in opening new accounts that will be charged to the victim. Consider the following simple ways personal information can be obtained by criminals:

- Rubbish that contains discarded mail or paperwork with account information
- A wallet or purse that contains receipts with account information and various forms of identification
- Mail that contains account numbers and statements highlighting credit limits and/or savings
- Phishing – the use of fake emails, spyware and websites tricking people into entering their data online (see page 20 for more information)
- A fraudulent Australia Post change-of-address form to divert someone's mail to another location
- Stealing business records by finding information at a person's place of work or by removing files from an office
- The handling of credit cards not in the presence of the card holders, for example at a hotel or restaurant (using credit card skimming devices)
- Stealing from a friend, neighbour or family member, where access to your personal details or the few pieces of personally identifying paper required may be comparatively simple

"Identity thieves often develop creative ways to draw unsuspecting victims into providing the information they need to steal their identities. Seemingly innocuous incidents may be staged simply to gain access to personal financial information. Some people have been targeted by signing up for a raffle or by completing a survey at a shopping centre, where they have provided their account numbers or other personal information the criminal can use."

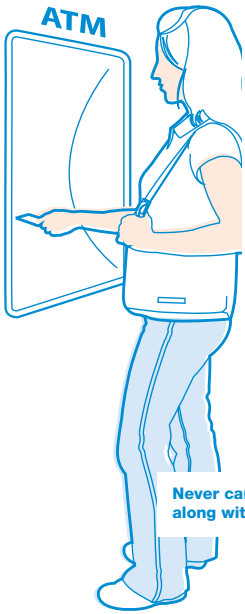
Preventing identity fraud

Combining common-sense with the resources available through the Internet and other electronic systems can lower the occurrence of identity fraud.

Consumers should regularly review their credit card and bank statements to indentify any fraudulent charges or withdrawals. Often people don't know they've been victimised until months after the stolen information is used.

To help prevent identity fraud consumers should follow these practices:

- Only carry credit cards on your person that are needed on a regular basis
- Contact your bank, credit agency or any card issuer (such as Medicare, the RTA etc) immediately if cards are lost or stolen
- Never carry PINs or passwords in a wallet along with the cards they activate
- Read and understand your credit card statements (and any other statements such as telephone, electricity and gas)
- Keep a low credit limit on your credit cards
- Sign new or renewed credit cards immediately
- Close accounts that you are not using or that you don't need
- When paying bills online, use a payment service that protects your personal financial information, such as PayPal (www.paypal.com.au)
- Never give personal financial information to unknown callers or salespeople over the phone, on the Internet or in person



Never carry PINs or passwords in a wallet along with the cards they activate

- Instead of throwing out potentially sensitive information like unneeded tax records and bank or credit card statements, use a shredder to destroy these documents
- Put a lock on your mailbox and collect mail every day
- Ensure all emails and attachments are screened by up-to-date anti-virus and anti-spam software
- Dont reply to emails that ask for personal information
- Order a credit report regularly and review it to ensure it is accurate. Credit reporting agencies such as Baycorp Advantage and Dunn & Bradstreet provide this service. In addition, some credit reporting agencies provide a credit alert service that allows you to monitor your credit file so that you receive email notification when a credit application is made using your personal details
- Use electronic statements for banking and credit card accounts. These can be viewed anytime of day or night to monitor against fraudulent use and eliminate paper statements that can be stolen
- Keep personal information in a locked filing cabinet at home

What consumers should do if they become identity fraud victims

Sometimes it can take many months before a victim of identity fraud becomes aware of the problem. As soon as it is discovered the victim should take the following steps:

- Contact the police and report the crime
- Obtain a copy of your credit file to confirm someone has used your identity
- Contact the credit providers involved and inform them of the fraudulent activity, otherwise they may hold you responsible for any bad debt incurred
- Monitor your credit file

To obtain a copy of your credit file contact :

Baycorp Advantage
Public Access Division
PO Box 966
North Sydney NSW 2060
Tel: Public Enquiries: (02) 9464 6000
Fax: (02) 9951 7880
Email: assist.au@baycorpadvantage.com
Website: www.mycreditfile.com.au

Also Contact:

The Office of the Federal Privacy Commissioner
GPO Box 5218
Sydney NSW 2001
Tel: 1300 363 992
TTY: 1800 620 241 (this number is dedicated for the hearing impaired only)
Facsimile: (02) 9284 9666
Email: privacy@privacy.gov.au
Website: www.privacy.gov.au

Banking and Financial Services Ombudsman
GPO Box 3
MELBOURNE VIC 3001
Tel: 1300 78 08 08
(03) 9613 7345
Website: www.abio.org.au

Victims of identity theft should keep detailed logs of all correspondence relating to attempts to report and correct the fraudulent activity.

Other agencies that can be notified under specific circumstances are:

Australian Taxation Office (if the theft involves the misuse of a tax file number) Tel: 132 861
Website: www.ato.gov.au

Department of Foreign Affairs (if the theft has been used to commit passport fraud) Tel: 131 232
Website: www.passports.gov.au

The Australian Securities and Investments Commission (if the theft has been used in the creation or amendment of a company record) Tel: 1300 300 630
Email: infoline@asic.gov.au
Website: www.asic.gov.au

Centrelink (if the theft has been used to obtain illegal payments) Tel: 137 320
Website: www.centrelink.gov.au

Phishing: fraudulent spammed spoofed emails

Some thieves on the Internet simply go fishing for sensitive information, or “phishing” as the practice has come to be known. The “ph” is a common substitute for the letter “f” among Internet insiders, and phishing is an attempt by scammers to trawl the sea of online consumers in the hope of netting unsuspecting victims.

Identity thieves send a massive number of generic emails (also known as spam) asking recipients to update account information for their banks, credit cards or online payment service or popular shopping sites.

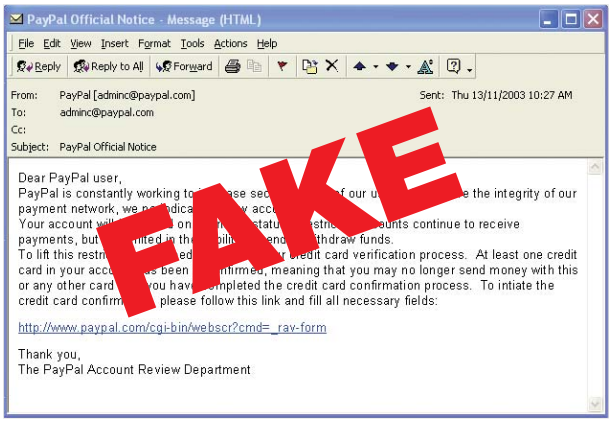
Sometimes these emails appear to have been sent from a legitimate company such as Citibank, Visa, Westpac, ANZ, National, Commonwealth, eBay and PayPal, among a range of other corporations. In fact, the fraudster’s identity has been hidden behind these credible sources, in a practice called “spoofing,” which goes hand in hand with “phishing”. The email will often convey a sense of urgency and may assert that the recipient’s account information has expired, been over charged, compromised or lost and that the account holder needs to contact the company immediately. Phishing emails often contain links to an official-looking website to “assist” this contact. Other times, emails ask the recipient to download and submit an electronic form.

Phishing criminals sometimes hide malicious software, known as spyware, in email attachments or the phoney websites that victims are directed to. Once on a victim’s computer this software may allow the criminal to see what is being typed, and to find sensitive information stored on the computer, such as Internet banking login names and passwords.

Phishers have only one purpose: to obtain personal information such as account user names and passwords, credit card numbers and bank account details, even other personal data such as date of birth, phone numbers and addresses. This information allows the phisher to commit crime for financial gain.

Many phishing emails appear very convincing. Some commentators suggest that between 1-5% of recipients respond to phishing emails. It has also been reported that a large number of computers unknowingly host “spyware” programs, leaving consumers exposed as potential victims of financial loss, identity theft and other crimes.

Criminals continue to use phishing because it is profitable even if a small fraction of the recipients respond: it is an inexpensive crime to attempt and to repeat regularly.



Case study #2:

Email by cautious bidder prevents phishing case

Misty loves her work as a Gold PowerSeller on eBay. Based in Canberra, she sells 20 laptops a week - a tidy earner for a final year law student. As a committed eBay Australia member, Misty is always conscious of maintaining eBay security measures and following eBay safe trading guidelines.

So it was surprising one afternoon when she found herself reading an email from a former bidder on one of her items which had already sold. The bidder had received a second chance offer that requested payment be made via Western Union instead of a more secure payment system such as PayPal or a credit card.

This shocked Misty as she doesn't ask her bidders to pay through Western Union and didn't send a second chance offer for the auction that had closed months before.

The bidder had been the target of a fraudster who sent a forged second chance offer email to the failed bidder in the guise of the seller.

The fraudster offered the bidder a laptop for $651 (the Second Chance Offer price). This was well below the final price of $1300 that the laptop had sold for.

The low asking price looked suspicious to the potential buyer, who decided to confirm the amount with Misty using the email address they had kept from their previous correspondence.

Fortunately, Misty recognised the problem immediately. By using common sense the bidder had prevented a potential case of fraud and the problem was resolved quickly and satisfactorily for all involved.

Identifying fraudulent emails

It is difficult to detect fraudulent emails – as phishers have become increasingly sophisticated in their attacks. However, there are certain characteristics Internet users should look for that are common to many spoof emails:

- **A sense of urgency/threats to accounts:** Some spoof emails declare that the recipient's account has been billed or is in jeopardy and that authenticating information is required to keep the account from being closed, suspended, billed or restricted
- **Lost information:** Consumers should be wary of claims that a company is updating its files or accounts. Companies like banks, PayPal and eBay are not likely to lose account information
- **Personal information requests:** Requests for a recipient to enter sensitive personal information such as a user ID, password or bank account details by clicking on a link or completing an email form should be treated with suspicion
- **Sender's address:** Email recipients should not rely on the sender's email address to validate the true origin of the email. The "From" field of emails can be easily altered to disguise the true sender
- **Links:** Links that appear to connect to a particular site may be forged. Always open up a new browser window and manually type in the website address

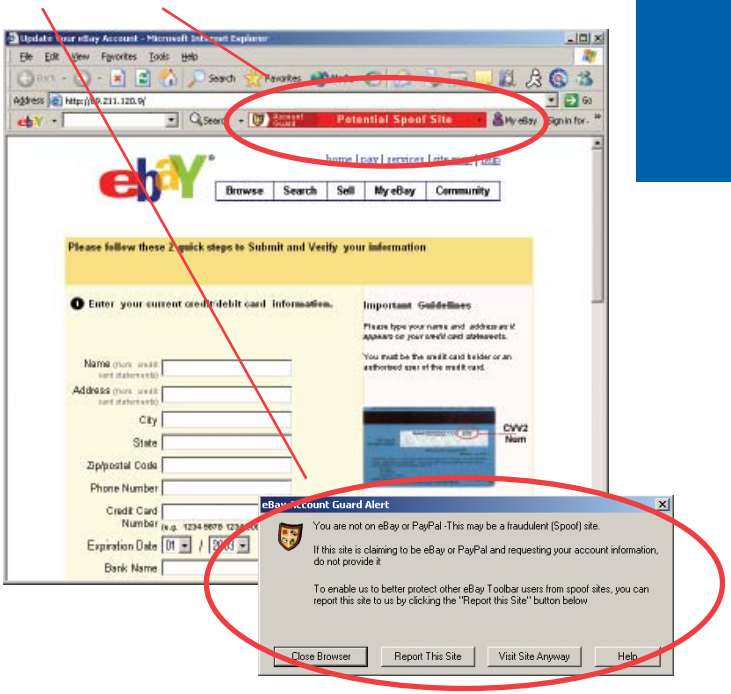
Phishing tips and tools

The likelihood of a phishing attempt working can be greatly reduced if you:

- Keep anti-virus, anti-spam, anti-spyware and firewall software up-to-date (they typically come bundled in one software package)
- Regularly scan for computer viruses and spyware
- Use the most current versions of browsers and operating systems
- In the same way that you would never reveal your bank account PIN to anyone, including the bank teller, never tell anyone your online account details. Legitimate companies will never ask for your personal details by email
- Some companies with an online presence offer email verification. For example, if you receive an email that purports to be from eBay that you suspect may be spoofed, email it to spoof@ebay.com.au so that the source can be investigated and eBay can get back to you on the authenticity of the email. PayPal offers a similar service at spoof@paypal.com
- If you are uncertain of a link in an email stay safe by opening a new browser and typing in the correct URL of the website
- The eBay toolbar helps identify if you are on a legitimate eBay website. The toolbar features Account Guard, which turns green if you are on an eBay website, grey for unknown and red for caution. The toolbar is free to download from eBay.com.au
- Keep separate passwords for each online account so if one is stolen it will not provide access to others

- Check online account statements regularly
- Some companies are introducing ways to communicate directly with their members on their websites – assuring members and account holders that the communications are intended for them. For example, eBay's *My Messages* is a new service where members are assured that all messages received come directly from eBay (no third parties can send messages to *My Messages*)

The eBay Toolbar and Account Guard helps indentify if you are on a legitimate eBay site



Companies that offer online shopping protection

PayPal

The October 2004 Sweeney Research found that the greatest Internet shopping security concern held by Australian Internet users is having their credit card details intercepted (53% of total survey).

Many of the potential concerns that surround the safety of online shopping, including the risk of interception and unauthorised use of a credit card, have been resolved by online payment services. The premier service of this type is PayPal, which has set the benchmark for secure Internet transactions and ease of use.

Purchasing something using PayPal is safer and more convenient than entering sensitive credit card or bank account data into each website: PayPal (PayPal.com.au) users simply carry out transactions through their PayPal accounts. PayPal then charges each purchase to the individual's credit card. Because PayPal transactions are based on the user's email address, merchants don't have access to the user's account information.

Online shoppers who pay each site directly to order products or services must submit their sensitive credit card or bank account details for each transaction. This crucial data is then stored by numerous individual retailers. With multiple merchants and servers maintaining this information, the likelihood of a breach of this information increases significantly.

PayPal allows online shoppers to set up a single account that can be used to purchase from millions of merchants around the world. Those who register with PayPal need only provide their account information once and then it is stored on a secure, highly encrypted server.

PayPal offers additional security, including PayPal Buyer Protection which provides coverage against loss of up to $1,500 on qualified eBay transactions. eBay sellers who qualify to offer PayPal Buyer Protection must have at least a 50 feedback rating that is 98% positive.

If PayPal users are victims of spoof, the company offers a complete refund to qualified account holders.

PayPal's dedicated team of investigators works directly with victims of theft and law enforcement to locate and prosecute criminals, anywhere in the world.

PayPal offers fraud prevention tips and safe shopping guidelines for buyers and sellers at its online Security Centre.

PayPal makes the riskiest part of transactions safer, without compromising speed or efficiency. In addition PayPal is a foremost resource for assurance online, a safety service that makes it easier to shop with confidence and to establish mutual trust between buyer and seller. eBay's marketplace of 135 million members overwhelmingly choose PayPal as the preferred payment option.

Companies that offer online shopping protection

Continued...

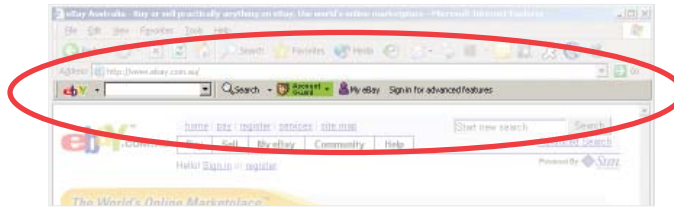
eBay

As the World's Online Marketplace, eBay is well equipped to provide one of the safest, most secure and trustworthy shopping environments. The eBay Security Centre at www.ebay.com.au/securitycentre is the single source for direct information about safe shopping in the eBay marketplace.

eBay's Feedback Profile system empowers members of eBay to comment on their transaction experience. Using this, buyers and sellers can check an individual's online reputation before engaging in a transaction with them.

Additional assurance can be found with the PayPal Buyer Protection Program that provides coverage against loss of up to $1,500 on qualified eBay transactions. This program protects buyers against non-delivered items as well as items that are significantly different from their descriptions. For transactions that do not qualify for PayPal Buyer Protection, eBay members may be covered up to $375 by the eBay Buyer Protection Program.

The eBay Toolbar and Account Guard helps combat Internet fraud as well. Designed to allow eBay users to track items on which they bid, the toolbar also helps recognise, reject and report potential spoof sites. Icons indicate if the user is on a verified eBay or PayPal site or can warn if the site might be fraudulent.



The eBay Toolbar and Account Guard helps combat Internet fraud

Eight reasons to feel confident shopping on eBay

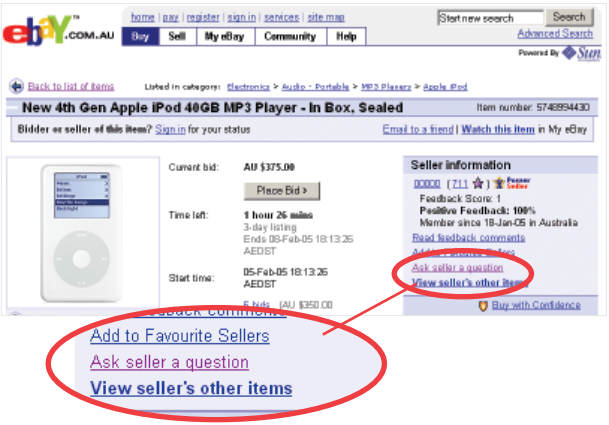
With 135 million registered users worldwide, trading in more than 50,000 categories, eBay is one of the safest marketplaces in the world.

1. eBay's Security and Resolution Centre at www.ebay.com.au/securitycentre is the source for direct information about safety and security when using eBay.
2. eBay Feedback provides buyers with information about a seller's overall rating (much like an online reputation) from previous buyers and their comments.
3. Buyers can use PayPal, a safe and secure way to pay online. Currently PayPal has more than 63 million member accounts in 45 countries
4. PayPal Buyer Protection offers up to $1,500 of coverage against fraud, items not received or items substantially different from their descriptions. Qualified sellers display the PayPal Buyer Protection symbol.
5. There are more than 1,000 employees around the world at eBay and PayPal dedicated to making eBay one of the safest places in the world to trade. They have backgrounds in law enforcement, customer support, advanced computer engineering and analysis.
6. The Account Guard feature on the free eBay Toolbar helps protect members from spoof sites and enables them to report such sites.
7. eBay users can email the seller before bidding or sending payment by using the "Ask the Seller a Question" link. This capability offers increased confidence for buyers who want to verify a name, city or phone number before paying.

Eight reasons to feel confident buying on eBay

Continued...

8. Shoppers have access to educational resources at eBay. eBay Explained (http://pages.ebay.com.au/ebayexplained) offers online tutorials on how to buy and sell safely on eBay. Additionally, many product categories have buying guides to alert visitors to special areas of consideration.



eBay users can email the seller before bidding or sending payment by using the "Ask the seller a question" link.

"eBay shoppers should never use wire transfer services such as Western Union or Moneygram. They are not designed for this purpose and offer no recourse should things go wrong."

Six rules for protecting your home PC when online

The following information has been supplied by AusCERT. AusCERT is the national Computer Emergency Response Team for Australia and a leading CERT in the Asia/Pacific region. As a trusted Australian contact within a worldwide network of computer security experts, AusCERT provides computer incident prevention, response and mitigation strategies, a national alert service and an incident reporting scheme on behalf of the Australian Government.

Protecting yourself online is no different to protecting yourself and your home. Putting a lock on your front door makes sense. So does taking safety precautions when you connect your PC to the Internet.

The following six steps are affordable, relatively easy to implement and importantly require only a small amount of ongoing maintenance.

1. Keep your operating system and other software up to date

- Malicious programs such as viruses, worms and trojans often exploit software defects
- Software defects can be fixed by applying a small piece of software code or patch. By keeping your computer system software patched you can do a lot to help prevent your PC being compromised
- New defects in software are discovered all the time, so it is important to keep your system patches up to date
- When your PC is connected to the Internet it can be configured to do periodic checks. This will determine whether there are any new patches for your particular operating system and download and install the patches as they become available - with little or no intervention on your part

Six rules for protecting your home PC when online

Continued...

- Patches should also be applied for email applications, all browser applications, such as Microsoft Internet Explorer, and other software in common use, e.g. Microsoft Office applications (Word, Excel etc)

2. Install a personal firewall and allow only essential in and outbound Internet connections

- A personal firewall is a piece of software or hardware that checks and controls your PC's Internet connections according to a pre-defined rule set
- Every home PC that connects to the Internet should have a personal firewall
- Scanning is a process attackers use to find computers on the Internet open to attack. When your PC is scanned, the attacker's computer attempts to make a connection to your PC
- There are some forms of attack that your firewall may not be able to detect and block. This is why users should apply the whole range of security measures described here

3. Install anti-virus and anti-spyware software and keep them updated

- It is essential to have up to date anti-virus software with the number of viruses, worms and trojans in circulation
- Once installed configure your anti-virus software so it updates itself at least daily
- Spyware scanners complement anti-virus software. They detect and protect against a variety of programs which can be secretly installed on your PC by attackers for malicious purposes

- Anti-virus software cannot protect against the newest worms, viruses and trojans. Regard opening email attachments and clicking on web links in unsolicited or suspicious emails as potentially dangerous

4. Install spam filter software

- Spam filters operate according to a pre-defined set of rules. The filter examines incoming email, and based on the characteristics of the email determines whether it is spam. It will then either block the email or let it through
- Fraudsters can use spam to help steal users' online banking credentials. They send spam pretending to be from a bank, eBay, PayPal or any other organisation that retains personal account information. The spam requires the recipient to disclose their account credentials on a fake website or by responding to the email. Spam designed to get users to visit a website with embedded malicious code is also sent out with the aim of logging a user's keystrokes and transferring the data to a computer controlled by the fraudster
- Spam filters will not successfully block spam all of the time. Do not assume all emails delivered to your inbox are legitimate and worthy of your complete trust, even if they appear to be from known sources

5. Turn off insecure features in your PC's browser

- Web browsers allow us to surf the web, access our email from any where in the world and shop online. It is possible for attackers to write harmful web-based programs which will automatically be installed on your PC if you connect to an attacker's website with your PC's browser

Six rules for protecting your home PC when online

Continued...

- Different browsers use different security features. For example Microsoft Internet Explorer's security features can be accessed and set via the Tools/Internet Options menu
- Home users may prefer to configure their browsers to prompt before allowing these programs or scripts (eg, Java, Javascript, ActiveX, IFrame) to run rather than automatically disabling them
- Although anti-virus software can help protect your PC from most harmful web based programs, it is still recommended that as many of the security features on your browser be turned on as possible, as anti-virus software will not detect all malicious code on the Internet

6. Special tips for broadband users

- Broadband users face additional threats that dial-up users don't. They are more attractive to target because of their high bandwidth and they tend to leave their PCs on and connection open
- Broadband users should consider purchasing a combined broadband modem/router device in order to give their PC a private network address. This way it cannot be directly reached via the Internet and is given a greater level of protection than a software-based personal firewall would provide by itself
- By turning your PC off when it's not in use you will reduce the time available for attackers and malicious programs to attack your computer and reduce your power consumption in the process

AusCERT

Broadband users should consider purchasing a combined broadband modem/router device in order to give their PC a private network address.

Recommended Australian resources

The following are online resources recommended for information about online fraud and prevention:

General e-security

Deptartment of Communications, Information Technology and the Arts
www.dcita.gov.au/e-security

Internet Industry Association security portal for advice to small businesses online
www.security.iia.net.au/

IT Security threats

National incident reporting service
www.national.auscert.org.au/

Download *Australian Computer Crime and Security Survey 2004*
www.auscert.org.au

Spam

Australian Communications Authority
www.aca.gov.au/ and click on the SPAM link.

Department of Communications, Information Technology and the Arts www.dcita.gov.au/spam

Online content regulation and complaints

Australian Broadcasting Authority
www.aba.gov.au/internet/complaints/complaints.htm

Online scams

Australian Securities and Investments Commission
www.fido.asic.gov.au/fido/fido.nsf

Reporting crimes online to police and tips for online safety

Australian High Tech Crime Centre
www.ahtcc.gov.au

Identity theft

Attorney-General's Department
www.ag.gov.au/agd/www/ncphome.nsf/page/identity_theft

Australasian Centre for Policing Research
www.acpr.gov.au
When bad things happen to your good name brochure:
www.acpr.gov.au/pdf/IDCrime_brochure.pdf

Consumer rights

Australian Competition and Consumer Commission
www.accc.gov.au

eBay

The *e-Commerce Safety Guide* is available from eBay's Security and Resolution Centre at
www.ebay.com.au/securitycentre