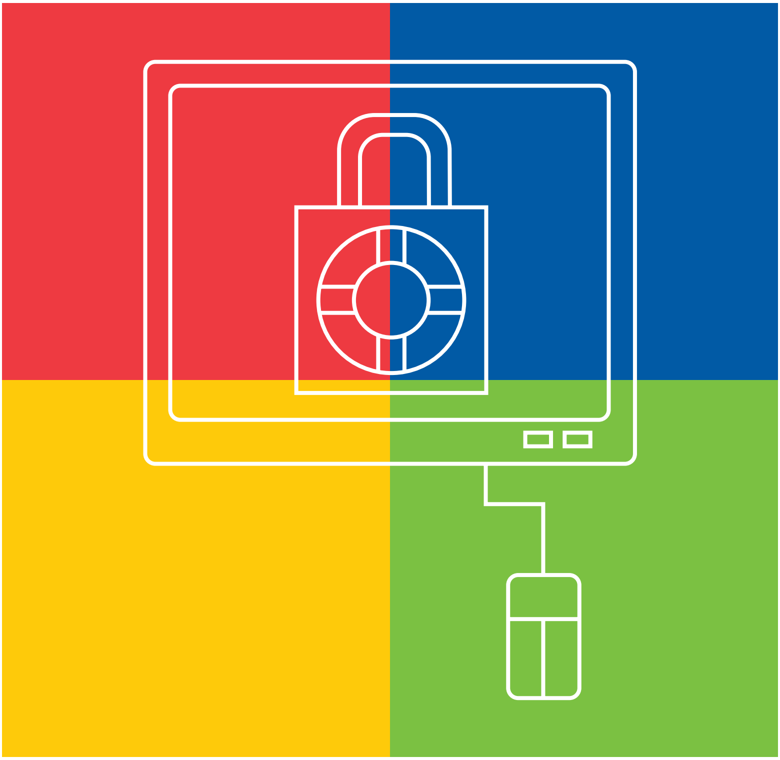


Singapore Online Safety Guide 2006

Foreword Statement

The Internet has clearly been the most amazing development of this generation, offering people all around the world unprecedented opportunities to communicate, have fun, and make money.

Where there is profit, there will be unscrupulous criminals trying to scam unwitting users of their funds.

The Singapore Online Safety Guide gives consumers and businesses stepping out into this brave online world the practical tips and advice they need to buy and sell safely.

Inside this handy reference guide, you will learn how to identify scams like phishing, use anti-fraud countermeasures like eBay's buyer protection services and credit card authentication systems to protect yourself from scams, and also practical, realistic advice on how you can go about recovering stolen funds or goods if you have gotten cheated.

Jointly produced by:

CaseTrust Be Sure

ebay.com.sg

National Crime Prevention Council

SPRING singapore

Contents

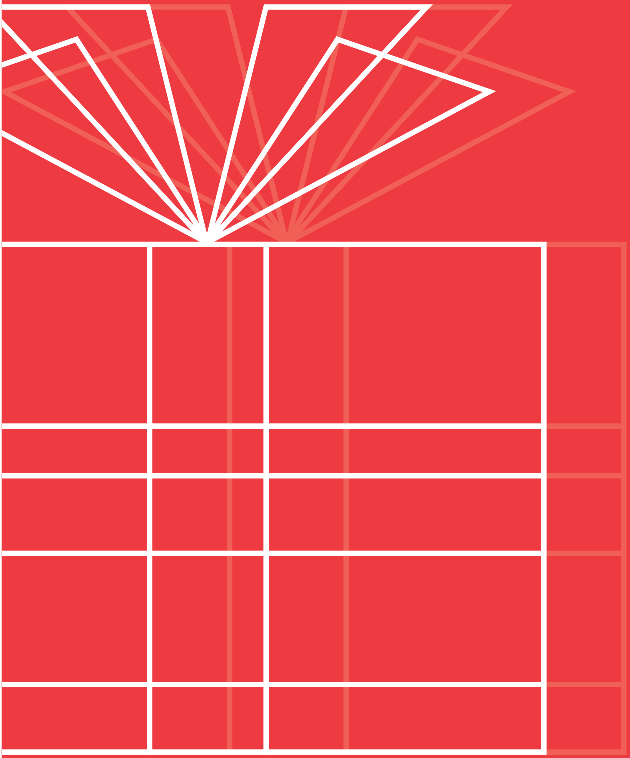
Part 1: Consumer

Part 2: Business

Part 3: Online Fraud

Part 4: Further Reading And References

Consumer



Shop Safely Online

Online shopping offers many advantages, from lower prices to exclusive items not available in Singapore. But there are risks, like non-delivery of goods or non-refund of damaged goods. A few simple practices can prevent you from becoming another sad statistic.

Where you can buy from

- Big, well-known online retailers like Amazon.
- Online auction sites like eBay.
- Smaller, less well-known operations.
- Other online users, like from Web forums.
- "Sprees" or mass orders, where a person coordinates a bulk purchase to try and get discounts.

The risks

- Buying goods that do not get delivered.
- Goods received don't match the description.
- Delays and hassles with online purchases.
- Poor after-sales service.
- Misuse of your credit card details.

Shop Safely Online

Do your research and only deal with reputable sellers

- Check forums, seller feedback channels and consumer organisations to find out what others say about the seller, especially when buying from individuals.
- Do a search for the seller's physical address, telephone number and other contact details.
- Don't judge a person or company solely by their Web site or his online "personality".
- Read the fine print, and in some instances, click the links describing the purchase agreement.
- Be especially cautious, when buying from a foreign retailer or someone overseas.

Know the retailer or seller's return policy. Issues to look out for include

- What happens if purchased items are not received?
- What is the timeframe in which a buyer must contact a merchant and return the items?
- Will the merchant offer a full refund or a merchandise credit?
- If an item has been opened, can it be returned?
- How will refunds be handled for returned items?
- What buyer protection programmes does the site offer?

Making payment

- Check that the payment Web site is secure before you enter your credit card information. Look out for a padlock symbol in the bottom right of the browser window and a Web address beginning with "https://". Also watch out for warnings, like those about expired certificates.
- Click on the padlock to check that the seller is who they say they are and that their certificate is current and registered to the right address.
- A secure Web site isn't an absolute guarantee of safety – it says nothing about the business's other ethics, like refunds or exchange policies.
- Consumers can look for third party seals that accredit sites with safe handling policies and procedures such as the VeriSign or TrustE logos. Also, look for logos of credible payment providers, such as PayPal, which never require you to share your credit card information with the seller when you make a purchase online.

VeriSign PayPal™

- Money transfer services are designed to send money to a friend or relative in need, not as a payment vehicle when buying online. Services like Western Union and MoneyGram warn consumers against using their services for online shopping and transactions because they offer no recourse if something goes wrong.

Use your common sense and keep your guard up

- If a deal looks too good to be true, it probably is. Cross-check information on the Internet and see if anyone else has had problems.
- Buy from reputable companies.
- Keep your computer protected via updated patches, anti-virus and firewall software.
- Until the transaction is complete and even after, keep all correspondence between the seller and yourself so you can produce it in case of a dispute.

If things go wrong

- Contact the seller to see what has happened.
- If there is a third party involved, for example you bought the items from an auction Web site or a Web forum, contact this third party for assistance.
- If you paid with a credit card, call the bank to see if the payment can be halted or reversed.
- If you paid another third party payment provider, such as PayPal, contact them directly or visit their Web site to learn how to file a claim or see if you are covered under a buyer protection programme.
- Make a police report, and remember to bring all your correspondence with you.
- Consumer watch organisations like the Consumer Association of Singapore (CASE) can help mediate a solution.
- You may wish to engage a lawyer to pursue the case for you if you believe you have a case and a clearly identified seller, but be warned that this is an expensive process and there is no guarantee it will work, especially if the seller is overseas.

Case Study A

A Singapore-based toy collector loves shopping on eBay for more antique toys for his collection as the prices could be significantly lower than those charged by toy retailers.

One day, he discovered an attractively-priced antique action figure from a now-defunct toy company on sale. After checking the seller's feedback, the item description and its pictures to verify that the toy was an original, he decided to buy it.

Unfortunately, when his purchase arrived, he realised the toy's box was not an original, but a homemade carton made by the seller, something known in toy collecting circles as a "repro" or reproduction.

This reduced the value and the desirability of the toy drastically.

Upset, he made a complaint to eBay, and managed to obtain a partial refund of about one-third of his purchase price.

He was pleased with this resolution, which he said was a fair resolution for both him and the seller.

Use Online Auctions Safely

Online auctions that match willing buyers with willing sellers are one of the success stories of the Internet. However, the popularity of auctions has also attracted criminals looking to exploit the unwary or careless.

The risks

- You pay for something but it never arrives.
- You sell something but the buyer doesn't pay.
- You are conned into selling early or at a low price.
- You inadvertently disclose personal information to crooks, allowing them to hijack your painstakingly built-up auction identity.

Know how the system works

- If you are new to online auctions, take the time to read the online guides provided by the auction company so you understand how the system works and what the rules are.
- Understand what the auction company can do – and what it cannot do – if something goes wrong.
- Use a login name for the auction site that is different from your email address.
- Use strong passwords
- Update your contact information, including email address, if it changes.

Know your seller

- Get to know the seller – his profile, rating and transaction history. eBay's Feedback Rating system, for example, tracks all sales made by the seller and his buyer's comments, both good and bad, to help you evaluate him.
- Everything else being equal, pick the seller with a good, healthy record, and be wary of those with a lot of negative feedback.
- You should also be careful of sellers with few ratings, but note that everyone starts as a newbie at some point, so having few ratings doesn't automatically mean he is a bad guy!
- If the seller is a business, check their real-world existence. If they provide a phone number or address, give them a call or pay a visit, especially if it is a hefty purchase.
- It is clearly tougher to hunt down a dishonest seller outside Singapore if something does goes wrong, and expensive to call him to verify his details. But email is free, so ask the seller questions this way to get a sense of how he does business.
- Postage and handling costs may vary across different payment and delivery methods.
- Be specific about which postage method you are using, so you are aware of any additional surcharges that may apply.

Use Online Auctions Safely

Use your judgment

- Never give out your auction site or payment service provider User ID and password to anyone. Write it down, or save it in an unprotected file on your computer.
- Be careful about sharing information with sellers. You may need to give some personal information to a seller once you have won their auction, for example a delivery address, but remain conscious of the risks and don't give more information than you need to.
- There is never any reason someone would want your auction site password or other details.
- Be wary of phishing emails. These may appear to be from a trusted organisation but are really from criminals trying to lure you to a fake Web site to steal your personal information (see more on phishing in Part 3).
- If you think your auction account has been compromised, take action immediately. Check the site's online help files, and contact the site quickly before the hijacker can do any damage.
- Always make sure you are using a secure Internet connection to change or access your personal information. Look for "https://" at the beginning of the address and the padlock symbol.
- Check that communications between buyer and seller are not being blocked by spam filters by checking your spam folder regularly.

Use Online Auctions Safely

Avoid common scams

- Be wary of emails or messages which might be attempts to get your personal information by pretending to come from the auction company itself. Auction companies like eBay never send you emails asking for your PIN numbers, passwords or other personal information, or which link to a page that asks you for this kind of information.

- Don't fall for requests to close auctions early. The best bids usually come towards the end of the auction period.

- Read and understand Buyer Protection programmes, like those offered by eBay and PayPal. The eBay Standard Purchase Protection Programme, for example, will reimburse you up to $330 (minus $42 processing charge) if the item bought on eBay does not match the description or failed to arrive. PayPal's Buyer Protection works in a similar fashion, allowing you to recover funds from unscrupulous sellers for amounts up to US$1,000 on qualified eBay transactions.

- Make sure you have been paid before sending off the goods.

- For routine payments, online payment services like PayPal work very well especially if you are buying or selling from someone overseas. Another great bonus: PayPal's built-in security helps safeguard your transactions and financial information, keeping you secure through fraud-prevention technology, data encryption, sophisticated risk models, and anti-fraud agents. Additionally, PayPal's Verification Process and buyer protection policies provide added security.

- For big-ticket items like artworks or jewellery, use a reputable escrow service like eBay-approved Escrow.com (www.escrow.com) to safeguard the purchase. Escrow services hold items from the seller and the funds from the buyer in trust to prevent one party from cheating the other of the money or item. When both parties are satisfied with the items and the funds, the escrow service then delivers the items and the funds to the recipients.

Protect Your Home PC When Online

Keep your operating system and other software up to date

- Malicious programs such as viruses, worms and Trojans often exploit software loopholes to attack your computer.
- These loopholes are easily fixed by "patching" it with a small piece of software code to all your software, from the operating system like Windows to email software to browser.
- Keeping your computer system patched is a key defence, but it isn't a one-off thing, since 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 automatically check for these patches. If there is a new one, it will download and install the patches as they become available.

Install a personal firewall and configure it right

- A personal firewall is software that ensures that only programs and data you want is sent and received.
- Every home PC that connects to the Internet should have a personal firewall. Windows XP has a good firewall that comes built into the software, and companies like McAfee, Symantec and Trend Micro have very affordable firewalls on sale, or you can also download free firewalls like ZoneAlarm.
- After you install your firewall, you need to configure it. This gives the firewall a set of rules to follow. A good starting point is to only allow Internet Explorer or Firefox to access the Internet first, and add other programs as you go along, like Windows Media Player for streaming videos or Skype for voice over Internet chat.

Protect Your Home PC When Online

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

- Anti-virus software scans your computer for viruses, worms, and Trojans. This is an essential program given the many viruses, worms and Trojans in circulation, and the damage such programs can cause to your computer.
- Once installed, do a full scan and remember to configure your anti-virus software so it updates itself daily.
- Spyware scanners are a great complement to anti-virus software. They detect and protect against a variety of nasty programs which may be secretly installed on your PC to find out what sites you surf to spam you with ads, or to remember your keystrokes and send them to a malicious hacker.
- No matter how good an anti-virus program is, it will sometimes miss a new worm or virus, so pay attention to your computer's behaviour as well. For example, a slowdown or constant hard disk spinning could mean the presence of an undetected virus in your system.
- Consider all email attachments and Web links in unsolicited or suspicious emails as potentially dangerous.

Protect Your Home PC When Online

Install spam filter software

- Spam filters help you control junk email, and are a nice program to have to ensure you are not deluged with offers of fake Rolex watches, pornographic Web sites – or worse, phishing emails.
- Most filters work by checking incoming email for whitelisted or blacklisted keywords to decide whether to block the email or let it through.
- More sophisticated spam programmes use an artificial intelligence engine to analyse the contents of the email to improve the accuracy of the filtering.
- Even the best filters today won't be able to successfully block all spam, so do not assume all emails delivered to your inbox are legitimate, even if they appear to be from known sources.

Turn off insecure features in your PC's browser

- Web browsers like Internet Explorer allow us to surf the Web, access our email from anywhere in the world and shop online. However, attackers have also come up with ways to install harmful Web-based programmes if you visit their Web site.
- Access your browser's security menu to check what they are and turn off unwanted features. Microsoft Internet Explorer's security features can be accessed and set via the Tools/Internet Options menu.
- If you do not want to miss out on all the interesting animations and other multimedia online, a good compromise is to configure your browser to prompt before allowing programmes or scripts like Java, Javascript, ActiveX, IFrame to run, rather than automatically disabling them.

Protect Your Home PC When Online

Special tips for broadband users

- Broadband users face additional threats compared to dial-up users. They are more attractive to malicious users since their high bandwidth make them good “zombie” machines to hijack. Broadband users also typically spend more time online, leaving their PCs on and connection open, and this makes them easier to identify and target.
- Heavy broadband users should consider purchasing a firewall device, or a home broadband modem/router. This way, their computer cannot be directly reached via the Internet and thus has a greater level of protection than what software-based personal firewalls can provide.
- Turning your PC off when it’s not in use will help you cut down on the time available for attackers and malicious programs to attack your computer – and this also has the added benefit of a lower power bill too!

!

FASTEN UP! to protect yourself from cyber-threats.

Firewall: Install a personal firewall.

Anti-virus: Install anti-virus software and update it regularly.

Scams: Beware of emails or Web sites with great offers that sound too good to be true.

Updates: Operating systems and applications software should be updated regularly.

Passwords: Create strong passwords and keep them safe.

Reproduced with permission from the Infocomm Development Authority of Singapore. For more on FASTEN UP! visit www.singcert.org.sg/awareness

Use Instant Messaging Safely

Instant messaging allows people to chat in real time over the Internet in a similar way to mobile phone text messages. Advanced systems allow Webcam and voice communication. The main systems are: AIM, ICQ, Skype, MSN Messenger and Yahoo! Messenger.

The risks

- People aren't necessarily who they say they are online.
- Social interaction can be very persuasive when it comes to making you do something unsafe. For example, a common attack is to persuade someone to download and run a virus-infected piece of software.
- There is no guarantee of privacy. Conversations are not encrypted and can be saved for use offline.
- IM software is also vulnerable to virus or other attacks.
- Online chatrooms, accessible through instant messaging, are generally unwholesome places.

Use Instant Messaging Safely

How to use it safely

- Never give out passwords, credit card information or other private data like home addresses, or your photos.
- Don't let children use instant messaging chatrooms unsupervised.
- Block strangers. If your software allows it, set up the system so that only people on your "allow" list can contact you.
- Be careful of what you key into your online profile. Consider leaving it blank or entering fictitious data.
- Use a different password for your IM from that used for your computer system or email password.
- IM is not encrypted, so don't use it to transmit information such as credit card numbers or other sensitive information.
- Disable automatic downloads.
- Be very wary of disclosing any private information to a stranger you meet via instant messaging. Even apparently innocent information like the name of your employer or school attended can be used against you by fraudsters.
- Verify information you receive on instant messaging elsewhere. In particular, check any security "advice" you get.
- Keep your IM software up-to-date.

Blog Safely

A Web log or 'blog' is a Web site that is regularly updated, much like a diary or a ship's log. Services such as Blogger, LiveJournal, WordPress, and MSN Spaces have made it easy for people to set up their own blogs.

While you can read a blog online, a program called an RSS reader allows you to read posts from many blogs in one place.

The majority of blogs are created by private individuals who write about subjects that matter to them, but there are also corporate and commercial blogs.

The risks

- **Privacy.** Even if you write under an assumed name or keep it anonymous, there's no guarantee that your details can't be discovered.
- **Embarrassment.** You might write or put up something that you later regret. There are instances of people failing job interviews because of embarrassing revelations on their blogs. Others have lost their jobs because their employer has taken exception to something they've written online. Still others would regret photographs of themselves in compromising positions that have gotten them in hot soup socially.
- **Legal.** The laws of libel apply to blogs too, and so do confidentiality clauses in contracts.
- **Persistence.** Once something is posted on the Internet, it is, effectively, permanently public. Even if you subsequently delete the post, it may have been cached in a search engine archive, a company server or in the Internet archive.

- **Freely accessible.** Blogs are public and thanks to search engines like Technorati or blog references like Tomorrow.sg, it is very easy for people to find information about them. A small, select audience for your blog today can grow to include your parents, employers and government officials tomorrow.
- **Spam.** As search engines rate sites that are widely cited and linked to, spammers will try to use the 'comment' feature on blogs to include links to sites they are promoting.

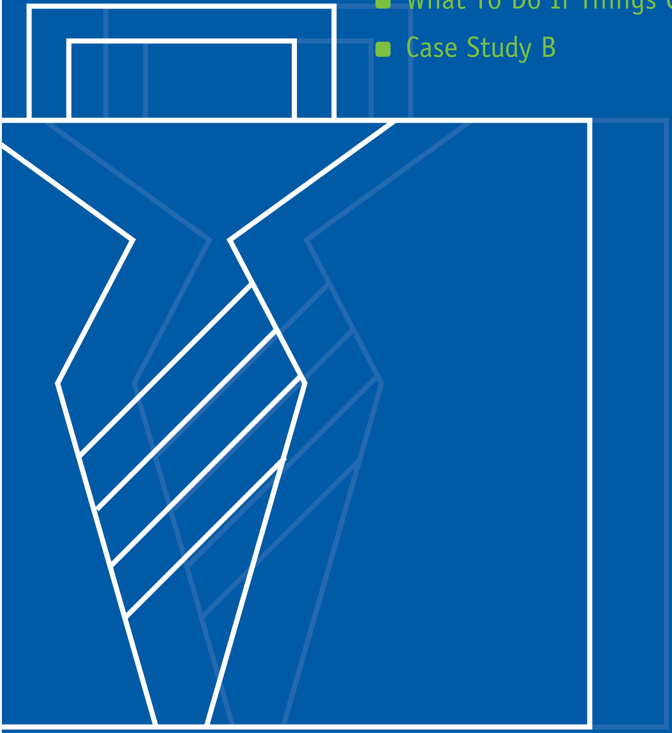
How to protect yourself

- If you're new to blogging, start cautiously. Understand the features of the software you use, blogging etiquette, and how the blogging community (the 'blogosphere') works.
- Don't post confidential information like credit card numbers, passport details, your home address, that may help someone guess your password and from there, to steal your identity.
- Also consider creating a "throwaway" email address from popular Web-based mail services like Yahoo or Hotmail just for the blog, and with a different password from your usual one. This ensures that even if your blog identity is compromised, your email or auction identity will not be affected.
- Don't say anything that you might regret later. As a general rule, if you wouldn't say it to your boss or your grandmother, don't say it online.

- Use the features built into your blogging software to restrict anonymous comments.
- If your child is blogging, check his blog regularly to ensure no confidential information is uploaded that may become a security risk, for example her photo and the school she goes to.

Singapore blogger Wendy Cheng, better known as Xiaxue, is one of the most controversial figures on the local blogging scene. In July 2005, the outspoken 22-year-old's blog was hacked into, and expletives and taunts left in place of the usual content. In October, she drew so much flak for controversial comments about handicapped toilets that two of the three sponsors she had then withdrew their endorsement of her blog.

Business



Taking Your Business Online: Safety Tips

1. **Write a good business security plan.** Write down the possible threats and scenarios that can cause a breakdown, and what to do should this happen. And remember to communicate this plan to all your staff to lessen your chances of security breach.

2. **Look after your servers.** The servers running your Web site, payment system, and customer database are the heart of your business, so it pays to invest a little more to get reliable, durable hardware, and ensure the servers are stored in a secure location like data centres.

3. **Control access to critical information.** Ensure that only authorised users have access to critical information, and consider implementing stringent access control systems like two-factor authentication or biometrics for these key systems and users.

4. **Choose a business-class IT partner.** An experienced technology firm will help you with security issues, which will save you time learning all the technical details.

5. **Train staff in business security.** Proper training in issues like password management and looking out for unauthorised users in the office not only reduces the risk of problems at work, but it can improve employees' IT skills, make them more confident online and encourage them to use better security at home too.

6. **Use encryption.** Encrypting email and files means that only authorised users are allowed to access them. This can be a powerful guarantee of privacy and security.

7. **Prevent data theft using removable devices.** Be wary of portable storage devices, such as MP3 players, digital cameras and pen drives, which can be used to introduce a virus, or steal confidential data from it. For key systems, consider removing or disabling the USB connection slots to head off this problem.

Protect Your Web Site

Make sure your ecommerce Web site is secure. If you have created your own ecommerce server rather than using a third party hosting company, it is especially important to make sure that the hardware and software is secure. In summary:

- Use the latest version of any ecommerce software. Old versions may have flaws that hackers can exploit.
- Use strong passwords throughout the system. Don't leave any password set to its default value.
- Make sure the server is protected by an effective firewall and anti-virus software.
- Monitor log files carefully to spot any attempts at intrusion. If you do not have the expertise to do this, consider hiring a security specialist firm to do this.
- Your payment system should never store customers' private information and credit card details.
- Protect your SSL details and keep them secret.
- Consider getting a professional security firm to test the defences on your ecommerce server, something called "penetration testing" in security parlance.

Selling Commercially On Auction Sites

Many businesses use auction sites as an online shop to sell their goods. But there are risks, which are similar to the ones faced by private sellers, but magnified by the volume of business you do. To protect yourself:

- Don't send goods until you are certain that you have received payment.
- Ensure you have all the documentation for the sale and delivery of the goods, even after you have collected payment. This is because the buyer can dispute the purchase with his credit card company even after he picks up the item, and you will need the documentation to prove your case.
- If you're on eBay, use 'Buyer Requirements' tools to control who can buy from you. For example, exclude buyers who aren't in Singapore or who have negative feedback ratings.
- Manage your staff so that only trained, appropriate people are able to deal with online orders.
- Consider getting professional advice. Commercial selling requires as much planning as any other outlet and there are plenty of companies that specialise in helping newcomers and managing online auction stores for them. There are also plenty of books and online resources to help you.
- Remember: if it sounds too good to be true, it probably is.

Build Trust

Effective selling on auction sites, as elsewhere, depends on trust. You can build trust by:

- Giving detailed product descriptions.
- Good quality pictures of the products for items that require this, for example, clothes or real estate.
- Clear return policies or warranties.
- Providing good customer service when something goes wrong.
- Offering easily found and verified information about your business, such as a phone number and business address.
- Sign up for third-party verification services, like TrustSG, which is operated by the National Trust Council.

CaseTrust
Be Sure

- Using trustworthy payment mechanisms like credit cards or PayPal to increase customer confidence.

How To Detect Fraud And Chargebacks

Learn to spot the warning signs that might indicate a suspicious order:

- Ordering the most expensive products or unusually large quantities.
- Different credit card and delivery addresses.
- PO Box delivery addresses.
- Hotel delivery addresses.
- Sending international orders to countries where there is known risk, for example, Nigeria.
- Unusual order patterns: for example, orders placed in the middle of the night or in rapid succession.

!

If you suspect a fraud, there are some ways you can check:

» Call the 'buyer' and ask to speak to the cardholder. Do they sound genuine?

» Ask for a fax of the back strip of the credit card or proof of name and address.

» Check card details with your payment provider to see if the address, security code and postal code match.

Take steps to protect yourself against fraud:

» Consider only delivering to credit card billing addresses.

» For business-to-business sales, do a credit check on new customers.

» Consider adopting a verification programme like Verified by Visa or MasterCard SecureCode, and enforcing the use of it for high-value or suspicious transactions. Take advantage of any fraud screening programmes run by your payment services provider or bank.

» Ask for the card security code for credit cards (the extra three security digits on the signature strip) and check it.

Best Practices To Avoid Fraud And Chargebacks

Dealing effectively with customer issues is a great way to minimise risk – and reduce chargebacks*. By communicating clearly and keeping good records, you can avoid many potential problems today – which are much easier than trying to resolve them with a credit card company tomorrow.

Here are some additional tips to help you lower your risks

- Provide realistic delivery time estimates and use tracking that shows proof that the items were received
- Describe the sale item in as much detail as possible. Include clear images and measurements so that customers have a good understanding of what they're getting.
- Make sure you clearly disclose the total cost to customers up front – the price, taxes, postage costs, etc.
- Provide customers with a way to contact you should they have a problem. Often a simple email exchange or phone call clears up a misunderstanding instantly.
- Make every effort to know your customer and to respond promptly and courteously to any customer service requests.
- Keep as much information as you can about the transaction and your customer, including email or other correspondence.
- Publish your return policy in your auction listings or on your Web site. Also include your return policy in email correspondence with your customer. Please note that certain laws and credit card issuer policies provide that buyers may have chargeback rights for merchandise that is not delivered or is defective, even if your policy indicates that all sales are final and that you do not allow returns.

** A chargeback occurs when a cardholder disputes a credit card purchase.*

Best Practices To Avoid Fraud And Chargebacks

Use the helpful checklist for typical decision points when considering whether or not to accept payment.

	DECISION POINT	CONSIDERATION
✓	Price of Item	The higher the price, the lower your tolerance for risk.
✓	New Buyer	There could be higher risk in dealing with a new buyer.
✓	Auction on eBay	To assess risk, use feedback scores and comments as well as checking that postage information is highly visible to the buyer.
✓	Questionable Behaviours	Rush shipments at any cost, sending partial payment from different sources (credit cards, PayPal multiple accounts, etc), or not making full payments should be cause for concern.
✓		If you're asked to send a high-priced item to a location in one country but billed to another, there could be a higher risk and you should use your best judgment.

What To Do If Things Go Wrong

- Try to contact the seller to see what has happened, and see if you can come to an agreement.
- If the buyer made the purchase with a credit card and then turns around to dispute the transaction with his bank, you will need to have the relevant materials like transaction logs, email messages, delivery order, and other documentation to counter his claims and avoid a chargeback from your bank.
- If the transaction was made through an online payment provider such as PayPal, visit their Web site to learn how they can help you resolve your issue. Plus, with PayPal, buyers and sellers have a place to go to help them work out their differences – PayPal Dispute Resolution Center.
- If you intend to make a police report, get your IT manager to pull out data like the transaction logs and IP address of the user to assist investigations. Even account names and passwords can be useful to provide a link to the scammer.
- You can also start a lawsuit to pursue the case. This will cost money and time, and success will depend heavily on whether you can identify the perpetrator, which can be difficult if he is overseas.

Case Study B

Scammers make fraudulent orders at Team Digital's Web site every few days.

Thanks to PayPal's sophisticated fraud detection system though, the company which sells digital devices like mobile phones and MP3 players online is usually able to identify such attempts and do not send the products to the criminals. "The first fraud attempt occurred not long after we started our online store in 2001, and we were saved by PayPal, which warned us that the account was being investigated and not to ship the item," said Team Digital spokesman Ken Chia.

Team Digital, which used to accept credit card payment, has since stopped doing so due to credit card fraud – the company has lost an estimated $10,000 to online fraud. It was also formerly using another payment service similar to PayPal, but stopped as it found that customers recognised and trusted the PayPal name.

Phishing And Other Online Scams

Phishing & Other Online Scams

Phishing

Probably the most popular online scam is "phishing". In this type of scam, criminals spam a large numbers of online consumers with phony emails soliciting personal account information in hopes that some will take the bait.

Phishing emails have only one purpose: to persuade their victims to divulge personal data, such as account user names, financial information and passwords, which the scammer can then sell to other criminals, or use to take over and loot the account. Because these emails look authentic, as many as five percent of recipients reply with personal information that can lead to identity theft and other crimes.

In typical phishing emails, the scammer will pretend to be a bank, payment company or other service provider's security department doing a spot check on its customers, and demand that the customer respond with his User ID and passwords. A variant of this phishing email asks the customer to go to a fake Web site operated by the scammer to key in his details.

Popular targets include well-known companies like Citibank, eBay and PayPal. In Singapore, banks including DBS and OCBC, and even financial industry regulator Monetary Authority of Singapore, have been targeted by such scams.

Escrow Scam

Playing on a buyer's worry about the safety of online transactions, the scammer helpfully offers to pay for the use of his recommended escrow site to transfer funds. Unfortunately, this escrow site is bogus and once your funds or item is sent, that is the last you will hear of it.

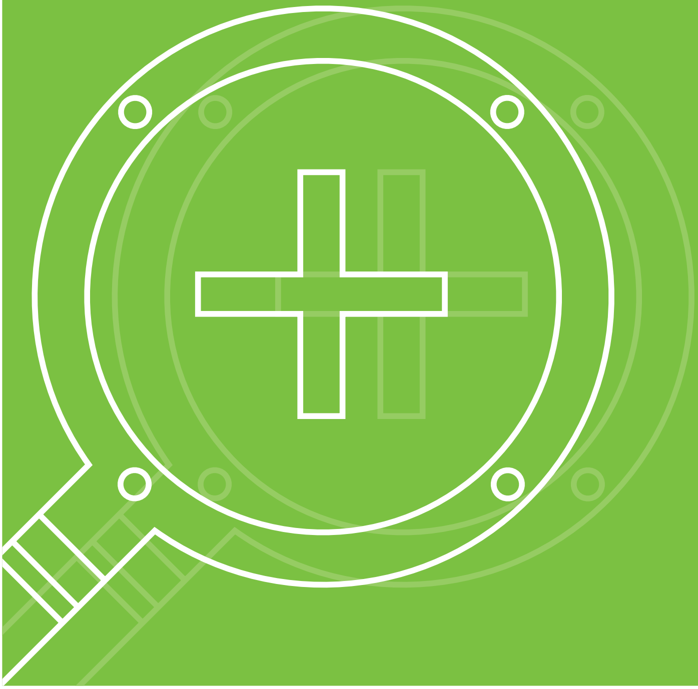
To counter this, double-check the escrow site with tools like http://www.networksolutions.com/en_US/whois/index.jhtml to check if the site is registered. Note also when the site was registered: a recent registration is one of the biggest warning signs that the site is likely to be fraudulent one.

Middleman Scam

Clever scammers trying to avoid leaving a paper trail of their scam for the authorities have turned to "middlemen" to help them move stolen funds around. In return for help, they offer these middlemen a generous cut of the funds – typically stolen from the accounts of identity theft or phishing victims – transferred. First the scammer moves the money into the "middleman's" account, and he is then told to move it to yet another person's account.

Further Reading And References

- Internet Security
- Laws That Affect Online Transactions
- Getting Help
- eBay Singapore's Safe Trading Tips



Internet Security

The Singapore Computer Emergency Response Team (SingCERT)

Check out SingCERT's Web site regularly for the latest security news and learn more about the right online security measures you can adopt to effectively protect yourself.

http://www.singcert.org.sg/awareness/

Singapore Antispam Resource Centre

Learn how to combat spam at this Web site maintained by the Infocomm Development Authority.

http://www.antispam.org.sg

TrustSG

You can shop with complete peace of mind at online merchants with the TrustSG seal, as they have undergone rigorous checks by the National Trust Council on all their processes.

http://www.case.org.sg/ctwebfront.htm

Right Click

Learn the right online habits at this cyber-wellness programme.

http://www.bsa.org/singapore/events/rightclick/index.cfm

National Crime Prevention Council

Find out more about cybercrime and Internet safety on this site run by non-profit organisation National Crime Prevention Council to promote public awareness on crime.

http://www.ncpc.gov.sg/

Laws That Affect Online Transactions

Electronic Transactions Act (Chapter 88)

Legislation governing electronic transactions, including issues like how long online merchants here must keep transaction records and how they must protect such records.

http://agcvldb4.agc.gov.sg/

Computer Misuse Act (Chapter 50A)

Legislation governing the use of computers here, covering issues like hacking into someone else's computer.

http://agcvldb4.agc.gov.sg/

Getting Help

eBay and PayPal's Buyer Protection

Unlike other auction sites or payment providers, eBay andPayPal offer users robust buyer protection to help lower the risks of buying from unknown users on a Web forum.

http://pages.ebay.com.sg/help/tp/isgw-buyer-protection-steps.html

http://pages.ebay.com.sg/export/tips.html

https://www.paypal.com/cgi-bin/webscr?cmd=xpt/general/PayPalStaySafe-outside

Singapore Police Force

Find out where your nearest police station is located so you can lodge a police report against online scammers here.

http://www.spf.gov.sg/contactus/contactus_index.htm

Consumers Association of Singapore (CASE)

Singapore's consumer watchdog body can help you mediate a settlement with a merchant.

http://www.case.org.sg

PayPal's Verification Process

Credit card verification process for added security.

https://www.paypal.com/us/cgi-bin/webscr?cmd=p/gen/verification-faq-outside

Notes:

eBay Singapore's Safe Trading Tips

1. Make sure your computer anti-virus is updated and that you have done a full system scan within the last seven days.
2. Only trade on reputable sites like eBay, and key in the address yourself.
3. Check that the site is secure by looking out for a padlock logo on the right bottom corner of the page, and double-click it to check that the certificate is current and issued to the right company.
4. Read through and make sure you understand the transaction conditions of the trading site and payment mechanism.
5. Go through the item descriptions and pictures carefully. Don't be shy about asking for more information or a clearer picture if you are in doubt.
6. Check the seller's ratings.
7. Ask yourself if the offer sounds too good to be true.
8. Pay with a reputable, secure payment method with strong buyer protection policies like PayPal.
9. If a valuable item is involved, use an escrow service, like the eBay-approved Escrow.com.
10. Check your bank and credit account regularly for unauthorised transactions, and report any promptly.

Jointly produced by:

CaseTrust Be Sure

ebay.com.sg

NATIONAL CRIME PREVENTION COUNCIL

SPRING singapore