中文翻译版见背页

SPOT A SCAM STOP A SCAM

Burwood
Inc.1874

A QUICK GUIDE TO SPOT, AVOID, AND PROTECT YOURSELF AGAINST SCAMS

Mayor's Message

Cr John Faker
Mayor of Burwood

Scams target people of all backgrounds, ages and income levels.

Every year, scams cost Australians, businesses and the economy hundreds of millions of dollars and cause emotional harm to victims and their families.

One of the best ways to stop this type of fraud is to stay one step ahead of scammers by protecting yourself through awareness and education.

To help you stay one step ahead of scammers, Burwood Council has developed this resource to help create awareness on this issue and to encourage you to visit the Australian Competition and Consumer Commission (ACCC), the national consumer protection agency.

The top scams to avoid

As mentioned previously everyone is vulnerable to scams so everyone needs information about how to identify and avoid being scammed. Some people think that only the gullible and greedy fall victim to scams. The truth is scammers are clever and if you don't know what to look out for, anyone can fall victim to a scam.

Have you received an offer that seems too good to be true, perhaps a phone call to help fix your computer or a threat to pay money you do not owe, an alert from your bank or telecommunications provider about a problem with your account or even an invitation to 'befriend' or connect online? Scammers know how to press your buttons to get what they want.

They are getting smarter, moving with the times to take advantage of new technology, new products or services and major events to create believable stories that will convince you to part with your money or personal details.

However, thanks to the tens of thousands of scam reports received every year, the ACCC has prepared a list of common scams to reveal the secrets and tactics that scammer's don't want you to know.

We have provided you with a few examples in this brochure but for a more comprehensive list we encourage you to download The Little Black Book of Scams which is recognised internationally as an important tool for consumers and small businesses to learn about scams, available online at:

www.accc.gov.au/littleblackbookofscams

How scams work

The anatomy of a scam

Most scams follow the same pattern and once you understand this, the tricks of the scammer become easier to spot.

If you look carefully at all of the different types of scams outlined in this book, you'll soon notice that most scams go through three stages: (1) approach; (2) communication; and (3) payment. Understanding the basic parts of a scam will help you to avoid the current crop of scams and to be on guard against new scams that emerge in the future.

1. The approach: delivery method

When scammers approach you it will always come with a story designed to make you believe a lie.

The scammer will pretend to be something they are not, a government official, an expert investor, a lottery official or even a romantic admirer.

To deliver these lies to you, scammers will use a range of communication methods.

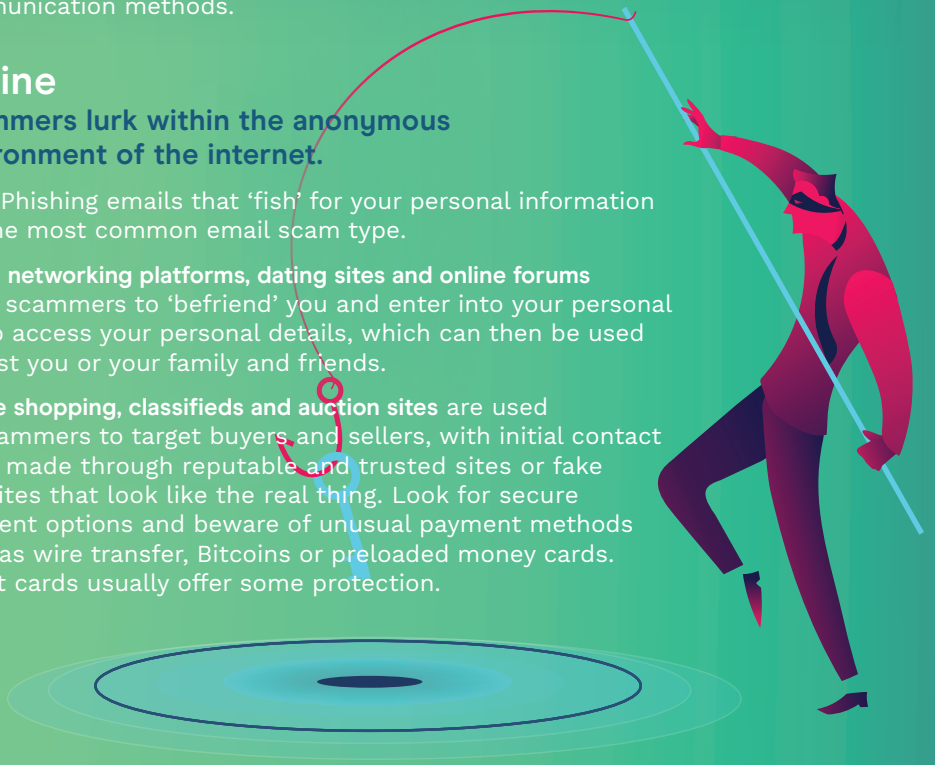
Online

Scammers lurk within the anonymous environment of the internet.

Email Phishing emails that 'fish' for your personal information are the most common email scam type.

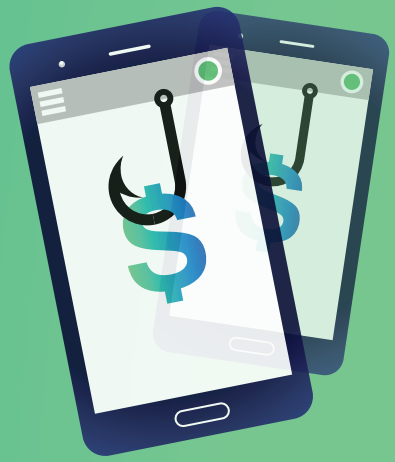
Social networking platforms, dating sites and online forums allow scammers to 'befriend' you and enter into your personal life to access your personal details, which can then be used against you or your family and friends.

Online shopping, classifieds and auction sites are used by scammers to target buyers and sellers, with initial contact often made through reputable and trusted sites or fake websites that look like the real thing. Look for secure payment options and beware of unusual payment methods such as wire transfer, Bitcoins or preloaded money cards. Credit cards usually offer some protection.



Over the phone

Scammers call and SMS too.



Phone calls are made by scammers to homes and businesses in a wide variety of scams, from threatening tax scams to offers of prizes or 'help' with computer viruses.

SMS text messages are used by scammers to send a whole range of scams including competition or prize scams. If you respond, you may be charged at premium rates or find yourself signed up to a subscription service.

At your door

Watch out - some scammers will come right to your door to try and scam you.

Door-to-door scams usually involve the scammer promoting goods or services that are not delivered or are of a very poor quality. You may even get billed for work that you did not want or agree to.

Scammers can pose as fake charity workers to collect donations. They will take advantage of recent events like floods and bushfires. Before donating ask for identification and see their official receipt book.

Bulk mailing is still used to send lottery and sweepstake scams, investment opportunities, Nigerian scams and fake inheritance letters.

2. Communication and grooming

If you give them a chance to talk to you, they will start using tricks in their scammers' toolbox to convince you to part with your money.

Scammer's tools can involve the following:

- Scammers spin elaborate, yet convincing stories to get what they want.
- They use your **personal details** to make you believe you have dealt with them before and make the scam appear legitimate.
- Scammers may **contact you regularly** to build trust and convince you that they are your friend, partner or romantic interest.
- They **play with your emotions** by using the excitement of a win, the promise of everlasting love, sympathy for an unfortunate accident, guilt about not helping or anxiety and fear of arrest or a fine.
- Scammers love to create a **sense of urgency** so you don't have time to think things through and react on emotions rather than logic.
- Similarly, they use **high pressure sales tactics** saying it is a limited offer, prices will rise or the market will move and the opportunity will be lost.
- A scam can have all the hallmarks of a real business using **glossy brochures** with technical industry jargon backed up with office fronts, call centres and professional websites.
- With access to the internet and clever software it is easy for scammers to create counterfeit and official-looking documents. A document that appears to have government approval or is filled with legal jargon can give a scam an air of authority.

The scammer's tools are designed to get you to lower your defences, build trust in the story and act quickly or irrationally and proceed to the final stage - sending the money.

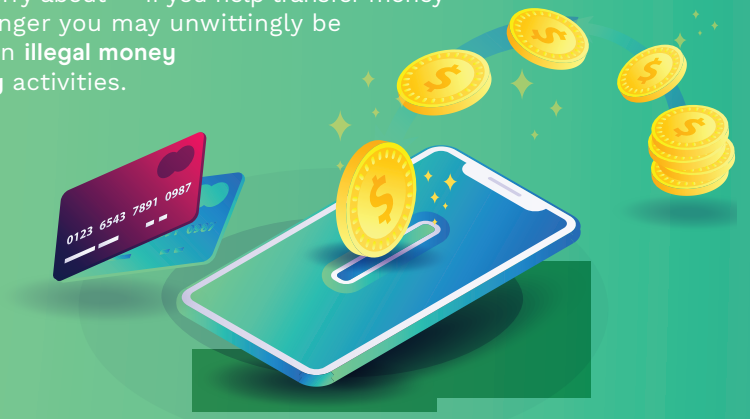
3. Sending the money

Sometimes the biggest clue you will have that it is a scam is the way the scammer asks you to pay.

Asking for money can come within minutes of the scam or after months of careful grooming. Scammers have their preferences for how you send your money.

Scammers have been known to direct victims to their nearest **money remittance** location (post office, wire transfer service or even the bank) to send money. They have been known to stay on the phone, give specific instructions and may even send a taxi to help with this. Scammers are willing to accept money by any means and this can include direct bank transfers, **preloaded debit cards, gift cards, iTunes cards** or virtual currency such as **Bitcoin**. Any request for payment by an unusual method is a tell-tale sign that it is part of a scam.

Credit cards usually offer some protection and you should also look for secure payment options where 'https' appears in the web address and the site has a closed padlock symbol. Don't send money to someone you have only met online or over the phone — especially if they are overseas. Be aware that scammers can also ask for payment in the form of valuable goods and expensive gifts such as jewellery or electronics. Paying money to scammers isn't the only thing you should worry about — if you help transfer money for a stranger you may unwittingly be involved in **illegal money laundering** activities.



Online shopping, classifieds and auction scams

Scammers love the ease of online shopping too.

How the scam works

Consumers and businesses are increasingly buying and selling online. Unfortunately, scammers like to shop online for victims.

Scammers can create very convincing **fake retailer websites** that look like the real thing, including on social media like Facebook. The biggest tip-off that a retail website is a scam is the method of payment – be wary if you are asked to pay by wire transfer or other unusual methods.

An **online auction scam** involves a scammer claiming that you have a second chance to buy an item that you placed a bid on because the winner has pulled out. The scammer will ask you to pay outside of the auction site's secure payment facility; if you do, your money will be lost you won't get what you paid for and the auction site will not be able to help you.

The **online classifieds scam** is a common scam targeting both buyers and sellers. Buyers should beware of scammers who post fake ads on legitimate classifieds websites. The ads can be for anything from rental properties to pets, used cars or cameras, and will often be cheaply priced. If you show interest in the item,the scammer may claim that they are travelling or have moved overseas and that an agent will deliver the goods following receipt of payment. Following payment you will not receive the goods or be able to contact the seller.

For sellers, a classified scammer will respond to your advertisement with a generous offer. If you accept it, the scammer will pay by cheque or money order. However, the amount that you receive is for more than the agreed price. In this **overpayment scam**, the 'buyer' may tell you that this was a mistake and will ask you to refund the excess amount by money transfer. The scammer hopes that you will transfer the money before you discover that their cheque has bounced or that the money order was phony. You will lose the money, as well as the item you sold if you have already sent it.

Protect yourself

- Find out exactly who you are dealing with. If it is an Australian retailer, you are in a much better position to sort out the problem if something goes wrong.
- Check if the seller is reputable, has a refund policy and complaint handling services.
- Avoid any arrangement that asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way. Never send money or give credit card or online account details to anyone you don't know or trust and never by email.
- Only pay via the website's secure payment method — look for a web address starting with 'https' and a closed padlock symbol.
- Never accept a cheque or money order for payment that is more than what you agreed upon or forward money on for anyone.

Identity Theft

All scams have the potential for identity theft. Protecting yourself from scams also means keeping your personal information safe.

Identify theft is a threat in every scam

Most people associate scams with attempts to trick you out of your money. However, your information is also valuable to scammers. Scammers steal your personal details to commit fraudulent activities like making unauthorised purchases on your credit card, or using your identity to open bank or telephone accounts. They might take out loans or carry out other illegal business under your name. They may even sell your information to other scammers for further illegal use.

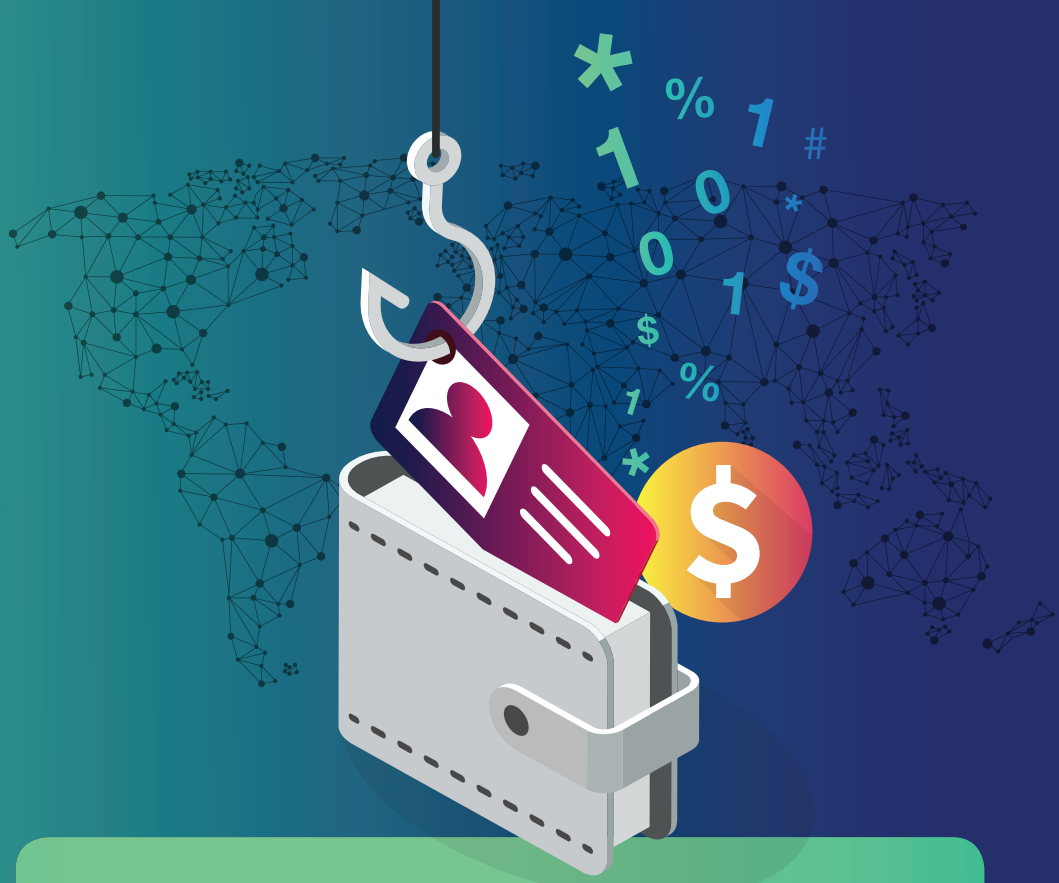
Having your identity stolen can be both financially and emotionally devastating. It can take months to reclaim your identity and the impact of having it stolen can last for years.

Phishing A scammer contacts you out of the blue via email, phone, Facebook or text message pretending to be from a legitimate business such as a bank, phone or internet service provider. They direct you to a fake version of the business's website asking for your personal details to verify customer records due to a technical error. They may call imitating a luxury goods retailer claiming that someone is trying use your credit card. They advise you to contact your bank but they don't hang up from their end and keep the line open. When you try to call the bank, you are still talking to the scammers who simulate a real call, imitate bank staff and ask for your account and security details. In either case, the scammer captures whatever information you give them and then uses it to access your accounts.

Fake surveys Scammers offer prizes or rewards such as gift cards to well-known retailers in return for completing an online survey. The survey requires you to answer a range of questions including disclosure of important dentification or banking details.

As part of any scam Scammers often ask for personal information in other scams. In a lottery scam, scammers often ask for a driver's licence or passport to 'prove your identity before they can release the prize money'. In dating and romance scams they might ask for information 'to sponsor their visa application to visit you in Australia'.

Remember: Giving away personal information to a scammer can be just as bad as giving away money. Keep your personal details to yourself and keep them secure.



Protect yourself

- **Think twice about what you say and do in an online environment**
  Be careful sharing information about yourself online, including social media, blogs and other online forums. Stop and think before filling in surveys, entering competitions, clicking on links or attachments, or even 'befriending', 'liking' or 'sharing' something online.
- **Beware of any request for your details or money**
  Scammers will try to trick you into handing over your data by using the names of well-known companies or government departments. If you think it's a scam, don't respond. Use the phone book or an online search to check the organisation's contact details. Never usethe contact details provided in the original request.

If you have provided personal identification information to scammers, contact IDCARE on 1300 432 273.

Threat and penalty scams

If a government authority or trusted company is telling you to pay up, stop, think and double-check.

How the scam works

Instead of offering a prize, money or rebate, these scams use threats designed to frighten you into handing over your money. The scammer may call you and threaten you with **arrest** or send you an email claiming you owe money for a **speeding fine**, a **tax office debt** or an **unpaid bill**.

During the phone call, scammers will pressure you into paying immediately and tell you the police will be sent to your house if you refuse. Scammers have been known to target vulnerable people in our community, such as newly arrived migrants. They pretend to be Immigration Department officials and threaten victims with **deportation** unless fees are paid to correct errors in their visas. A very similar scam involves the scammer pretending to be from the Australian Tax Office telling their victims they have an outstanding tax bill.

Scammers also pretend to be **trusted companies** such as your bank, gas, electricity, water or phone provider. They will threaten to cancel your service or charge you excessive penalty fees if you don't pay the bill immediately. Sometimes they may impersonate a business like Australia Post stating you have an item to pick up or you will be charged a holding fee every day you don't pay.

Whatever the case, they try to make you worried and act without stopping to think and check that the story is true.

If the scam is sent by email, it is likely to include an attachment or link to a fake website where you will be asked to download proof of the 'bill', 'fine' or 'delivery details'. Opening the attachment or downloading the file will result in infecting your computer with malware.

Protect yourself

- Don't be pressured by a threatening caller. Stop, think and check whether their story is true.
- A government agency or trusted company will never ask you to pay by unusual methods such as by gift card, wire transfers or Bitcoins.
- Verify the identity of the contact by calling the relevant organisation directly — find them through an independent source such as a phone book, past bill or online search.
- Do not use the contact details provided in emails or given to you during phone calls. Again, find them through an independent source.

Where to report a scam

You can help others by reporting a scam to the appropriate authorities. Your information will help these organisations build a better picture of the latest scams and warn other people about what to look out for.

The following organisations take reports about particular types of scams.

Scamwatch

Report scams to the ACCC via Scamwatch | www.scamwatch.gov.au

Stay one step ahead of scammers

Stay one step ahead of the scammers — visit the Scamwatch website to get the low-down on scams that target Australian consumers and small businesses. Find out more about how scams work, how to protect yourself and what to do if you've been scammed.

Register with the Scamwatch subscription service to receive free email alerts on new scams doing the rounds.
www.scamwatch.gov.au

Follow Scamwatch on Twitter at
@scamwatch_gov or
http://twitter.com/Scamwatch_gov

If you encounter a scam on a website or social media platform, report it to the site so it can be investigated and removed. If the scammers are impersonating a legitimate organisation like a government department or bank, let them know so they can warn others.

Other agencies

You should also consider reporting your scam to other agencies that specifically deal with certain types of scam.

Cybercrime	Australian Cybercrime Online Reporting Network (ACORN). Visit **www.acorn.gov.au**
Financial and investment scams	Financial and investment scams. Australian Securities and Investments Commission (ASIC).Visit **www.moneysmart.gov.au** or call the ASIC infoline on **1300 300 630**
Fraud and theft	Your local police. Call **13 1444**
Spam emails and SMS	Australian Communications and Media Authority (ACMA).Visit **www.acma.gov.au** or call the ACMA Customer Service Centre on **1300 850 115**
Tax related scams	Australian Taxation Office (ATO). To report a tax scam or verify whether a person contacting you from the ATO is legitimate: Call **1800 008 540** or forward your email tax scam to **ReportEmailFraud@ato.gov.au** t
Banking	Your bank or financial institution

Contact your local consumer protection agency

While the ACCC is the national agency dealing with general consumer protection matters, state and territory agencies may also be able to assist you.

New South Wales Fair Trading
www.fairtrading.nsw.gov.au

13 32 20

More information

The Australian Government has some great resources on how to stay secure and safe online.

- Stay Smart Online Service: **www.staysmartonline.gov.au**
- CyberSmart website: **www.cybersmart.gov.au**
- Protecting Yourself Online publication: **www.ag.gov.au/cybersecurity**

The golden rules to protect yourself

Be alert to the fact that scams exist

When dealing with uninvited contacts from people or businesses, whether it's over the phone, by mail, email, in person or on a social networking site, always consider the possibility that the approach may be a scam. Remember, if it looks too good to be true, it probably is.

Know who you're dealing with

If you've only ever met someone online or are unsure of the legitimacy of a business, take some time to do a bit more research. Do a Google image search on photos or search the internet for others who may have had dealings with them.

Do not open suspicious texts, pop-up windows or emails — delete them

If unsure, verify the identity of the contact through an independent source such as a phone book or online search. Don't use the contact details provided in the message sent to you.

Keep your personal details secure

Put a lock on your mailbox and shred your bills and other important documents before throwing them out. Keep your passwords and pin numbers in a safe place. Be very careful about how much personal information you share on social media sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.

Beware of unusual payment methods

Scammers often ask for payment by wire transfers, preloaded cards and even iTunes cards and Bitcoin. These are nearly always a sign that it is part of a scam.

Keep your mobile devices and computers secure

Always use password protection, don't share access with others (including remotely), update security software and back up content. Protect your WiFi network with a password and avoid using public computers or WiFi hotspots to access online banking or provide personal information.

Choose your passwords carefully

Choose passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper and lowercase letters, numbers and symbols. Don't use the same password for every account/profile, and don't share your passwords with anyone.

Beware of any requests for your details or money

Never send money or give credit card numbers, online account details or copies of personal documents to anyone you don't know or trust. Don't agree to transfer money or goods for someone else: money laundering is a criminal offence.

Be careful when shopping online

Beware of offers that seem too good to be true, and always use an online shopping service that you know and trust. Think twice before using virtual currencies (like Bitcoin) — they do not have the same protections as other transaction methods, which means you can't get your money back once you send it.

在哪里可以寻求帮助或支持

如果您因为受骗而损失金钱，或将您的个人信息泄露给了诈骗者，那就无法收回你的金钱。但是，您可以立即采取措施限制损失的程度，保护自己免受进一步损失。

联系您的银行或信用合作社

如果您已向诈骗者汇款或提供个人银行信息，请立即联系您的银行或信用合作社。如果诈骗者有您的帐户详细信息，银行可能会停止转帐或停止兑现支票，或关闭您的帐户。如果您的信用卡被欺诈性收费，您的信用卡提供商可能会执行“退款”(将交易反转)。

恢复被盗身份

如果您怀疑自己是身份盗用的受害者，请务必迅速采取行动，以降低财务损失或其他损失的风险。

请联系**IDCARE**。这是一项由政府资助的免费服务，为身份犯罪的受害者提供支持。IDCARE可以帮助您制定相应计划，以采取适当的措施来修复对您的声誉、信用记录和身份造成的损害。浏览IDCARE网站www.idcare.org 或致电1300 432 273。

申请**联邦政府受害者证书**——证书有助于支持您声称自己是身份犯罪的受害者，并可用于帮助您与政府或金融机构重新建立您的信誉。请浏览总检察长办公室网站www.ag.gov.au(或致电02 6141 6666)，了解有关保护和恢复身份的更多信息。

联系辅导或支持服务

如果您自己或您认识的人被骗，可能因此而患有情绪紧张或抑郁症，请咨询您的全科医生，当地健康专家或您信任的人。您也可以考虑联系辅导或支持服务，例如：

生命热线(Lifeline)

当您在危机中需要支持时，请致电13 1114(7天24小时全天候)联系生命热线或访问www.lifeline.org.au。

Beyondblue

有关抑郁或焦虑的信息，请致电1300 224 636联系Beyondblue或访问www.beyondblue.org.au。

儿童帮助热线(Kids helpline)

为5至25岁的年轻人提供热线电话和网上辅导及支持服务。请致电 1800 551 800 联系儿童帮助热线，或访问www.kidshelpline.com.au。

澳大利亚财务辅导 (Financial Counselling Australia)

如果您遇到财务困境，请致电1800 007 007与免费的财务辅导员交谈，或浏览www.financialcounsellingaustralia.org.au。

Burwood
Inc.1874

本手册中的信息来自于：
《防诈骗小黑书》(The Little Black Book of Scams)
https://www.accc.gov.au/publications/the-little-black-book-of-scams

Where to find help or support

If you've lost money to a scam or given out your personal details to a scammer, you're unlikely to get your money back. However, there are steps you can take straight away to limit the damage and protect yourself from further loss.

Contact your bank or credit union

If you've sent money or personal banking information to a scammer, contact your bank or credit union immediately. They may be able to stop a money transfer or cheque, or close your account if the scammer has your account details. Your credit card provider may be able to perform a 'charge back' (reverse the transaction) if your credit card was billed fraudulently.

Recover your stolen identity

If you suspect you are a victim of identity theft, it is important that you act quickly to reduce your risk of financial loss or other damages.

Contact **IDCARE** — a free, government-funded service that provides support to victims of identity crime. IDCARE can help you to develop a response plan to take the appropriate steps for repairing damage to your reputation, credit history and identity. Visit the IDCARE website at www.idcare.org or call 1300 432 273.

Apply for a **Commonwealth Victims' Certificate** — a certificate helps support your claim that you've been the victim of identity crime and can be used to help re-establish your credentials with government or financial institutions. Visit the Attorney-General's Department at www.ag.gov.au (or call 02 6141 6666) to learn more about protecting and recovering your identity.

Contact a counselling or support service

If you or someone you know has been scammed and may be suffering from emotional stress or depression, please talk to your GP, local health professional or someone you trust. You may also consider contacting counselling or support services, such as:

Lifeline

When you need support in a crisis, contact Lifeline on 13 1114 (24/7) or visit www.lifeline.org.au

Beyondblue

For information about depression or anxiety, contact beyondblue on 1300 224 636 or visit www.beyondblue.org.au

Kids helpline

Telephone and online counselling and support service for young people aged between five and 25 years. Contact Kids helpline on 1800 551 800 or visit www.kidshelpline.com.au

Financial Counselling Australia

If you are in financial distress call 1800 007 007 to talk to a free financial counsellor or visit www.financialcounsellingaustralia.org.au.

Burwood
Inc.1874

Information in this booklet has been sourced from
The Little Black Book of Scams
https://www.accc.gov.au/publications/the-little-black-book-of-scams

保护自己的黄金法则

警惕诈骗存在的事实

当处理来自个人或企业的不速之客的联系时，无论是通过电话、邮件、电子邮件、面对面还是在社交网站上，总是要警惕这种方法可能是骗局。请记住，如果看起来好得令人难以置信，那可能就是骗局。

知道您在和谁打交道

如果您只是在网上认识某人或不确定某项业务的合法性，请花一些时间再做一些调查研究。将照片进行Google图片搜索，或在互联网上搜索可能曾经与他们打过交道的其他人。

不要打开可疑文本、弹出的窗口或电子邮件——直接删除即可

如果不确定，请通过电话簿或上网搜索等独立来源验证联系人的身份。请勿使用发送给您的邮件中所提供的联系信息。

确保您的个人信息安全

请给信箱上锁。在丢弃账单和其他重要文件之前，请先将其撕碎。将密码和个人识别码保存在安全的地方。请注意您在社交媒体网站上分享的个人信息量。诈骗者可以使用您的信息和图片来创建虚假身份或实施针对您的骗局。

谨防不寻常的付款方式

诈骗者经常要求通过电汇、预付卡甚至Google Play、Steam或iTunes卡和比特币付款。这几乎总是可以表明这是骗局的一部分。

确保移动设备和计算机的安全

始终使用密码保护，不与他人共享使用(包括远程)，更新安全软件和备份内容。使用密码保护自己的WiFi网络，避免使用公共电脑或WiFi热点访问网上银行或提供个人信息。

仔细选择密码

选择其他人难以猜测的密码并定期更新。保密性强的密码应既包括大写也包括小写字母，还有数字和符号的混合。不要为每个帐户/个人资料使用相同的密码，也不要与任何人分享您的密码。

当心对您的个人信息或金钱进行索取的任何要求

切勿向您不认识或信任的任何人汇款或提供信用卡号码，网上帐户详细信息或个人文件副本。不要同意为他人转移金钱或货物：洗钱是一种刑事犯罪。

上网购物时要小心

谨防那些看起来好得令人难以置信的优惠，并只使用您了解并信任的网上购物服务。在使用虚拟货币(比如比特币)之前要三思而后行——他们没有与其他交易方法相同的保护措施，这意味着钱一旦发送出去，就无法回收。

在哪里举报骗局

向有关当局举报诈骗，您就可以帮助他人。您的信息将帮助这些组织更好地了解最新的骗局，并提醒其他人应该注意什么。

以下组织会接受有关特定类型的诈骗的情况的举报。

诈骗监察(Scamwatch)

通过Scamwatch向澳大利亚竞争与消费者委员会(ACCC)报告诈骗行为——请浏览网站www.scamwatch.gov.au。

比诈骗者领先一步

比诈骗者领先一步——访问Scamwatch网站，了解针对澳大利亚消费者和小企业的骗局。详细了解诈骗如何运作，如何保护自己，以及如果被骗，应该怎么办。

在Scamwatch登记订阅服务，即可收到有关新一轮诈骗手段的免费电子邮件提醒。
www.scamwatch.gov.au

在Twitter上关注Scamwatch **@scamwatch_gov**或
http://twitter.com/Scamwatch_gov。

如果您在网站或社交媒体平台上遇到骗局，请将其报告给网站，以便对其进行调查和删除。如果诈骗者冒充政府部门或银行这样的合法组织，也让他们知道，以便他们可以警告他人。

其它机构

您还应该考虑将您遇到的骗局报告给其它专门处理特定类型骗局的机构。

网络犯罪	澳大利亚网络犯罪在线举报网络 (Australian Cybercrime Online Reporting Network, ACORN)——浏览**www.acorn.gov.au**
金融和投资骗局	澳大利亚证券和投资委员会(Australian Securities and Investments Commission, ASIC)——浏览**www.moneysmart.gov.au**或致电ASIC资讯热线**1300 300 630**
欺诈和盗窃	您当地的警察——电话**13 1444**
垃圾邮件和短信	澳大利亚通信和媒体管理局(Australian Communications and Media Authority, ACMA)——访问**www.acma.gov.au**或致电ACMA客户服务中心**1300 850 115**
与税务相关的骗局	澳大利亚税务局(Australian Taxation Office, ATO)——报告税务骗局或验证声称来自ATO与您联系的人是否属实：致电**1800 008 540** 或将您的税务骗局的电子邮件转发至**ReportEmailFraud@ato.gov.au**
银行业	您的银行或金融机构

联系当地的消费者保护机构

虽然ACCC是处理一般消费者保护事务的国家机构，但州和地区机构也可以为您提供帮助。

新南威尔士州公平交易办公室(New South Wales Fair Trading)
www.fairtrading.nsw.gov.au
13 32 20

更多信息

澳大利亚政府在如何保持上网安全和可靠方面拥有一些非常好的资源。

- Stay Smart网络服务——**www.staysmartonline.gov.au**
- CyberSmart网站——**www.cybersmart.gov.au**
- Stay Smart网上指南——请浏览**www.staysmartonline.gov.au/get-involved/guides**

威胁和惩罚骗局

如果政府机构或可以信任的公司告诉您付钱，请先止步，仔细思考，小心核查。

这种诈骗的运作方式

这些骗局不是通过提供奖品、金钱或回扣，而是使用威胁手段来吓唬您交出自己的钱。诈骗者可能会打电话给您并威胁要**逮捕**您，或者发送一封电子邮件，声称您有尚未偿付的**超速罚款、欠税务局债务**或有**未付账单**。

在通话过程中，骗子会迫使您立即付款，并告诉您，如果您拒绝，就会派遣警察到您家。众所周知，骗子会针对社区中的弱势群体，例如新来的移民。他们假装成移民局的官员，威胁受害者支付费用以纠正他们的签证错误，否则会将他们**驱逐出境**。还有一个非常类似的骗局，骗子假装来自澳大利亚税务局，告诉受害者说他们有一笔未付税款。

诈骗者还会假装是可以**信任的公司**，如您的银行、天然气、电力、水或电话提供商。他们会威胁说如果您不立即支付账单，将取消服务或向您收取相当高额的罚款。有时，他们可能冒充像澳大利亚邮政这样的企业，通知您去提取一件物品，否则每天都需要支付手续费。

无论具体情况如何，他们都会试图让您担心，然后不经过思考，也不去检查故事是否属实就采取行动。

如果骗局通过电子邮件发送，则可能包含附件或链接到虚假网站，在那里您将被要求下载“账单”、“罚款”或“交付详细信息”的证明。一旦打开附件或下载文件就会导致您的电脑感染恶意软件。

保护自己

- 不要理会打电话的人给您施加压力。先停顿一下，思考清楚，核查他们的故事是否属实。
- 政府机构或可以信赖的公司绝不会要求您通过礼品卡、电汇或比特币等不寻常的方式付款。
- 验证联系人的身份，可以通过直接打电话到相关组织——通过电话簿、过去账单或网上搜索等独立来源找到这些机构。
- 请勿使用他们的电子邮件中所提供的或在通话期间提供给您的联系方式。重复一次，一定要通过独立的来源去查找他们。

身份盗窃

所有骗局都有可能导致身份信息被盗用。保护自己免受诈骗也意味着保护您的个人信息安全。

每种骗局都有身份盗窃的危险

大多数人会将骗局与骗钱联系在一起。但是，您的信息对诈骗者也很有价值。诈骗者窃取您的个人信息以进行欺诈性活动，例如使用您的信用卡进行未经授权的购买，或使用您的身份开设银行或电话帐户。他们可能会以您的名义贷款或进行其它非法业务。他们甚至可能会将您的信息出售给其他诈骗者，以便其进一步非法使用。

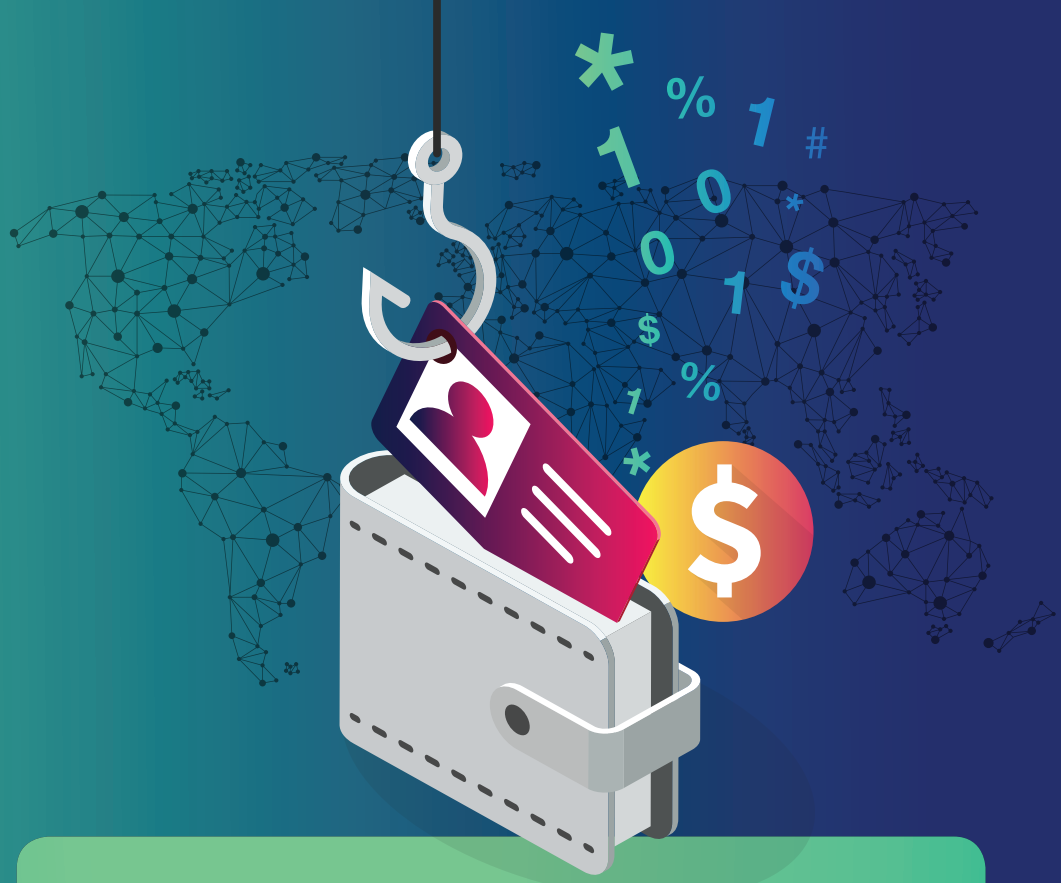
身份被盗在财务上和情感上都可能是毁灭性的。可能需要很多个月的时间才能回收您的身份，而且身份被盗的影响可能会持续多年。

网络钓鱼——诈骗者通过电子邮件、电话、脸书或短信突然与您联系，假装来自合法的企业，如银行、电话公司或互联网服务商。他们会引导您访问该企业网站的虚假版本，要求您提供个人详细信息，借口说出现技术错误需要验证客户记录。他们可能会打电话模仿奢侈品零售商声称有人正在尝试使用您的信用卡。他们建议您联系您的银行，但他们不会挂断电话并保持连线状态。当您尝试致电银行时，您仍然在与模拟真实电话的诈骗者交谈，他们模仿银行工作人员并询问您的帐户和安全信息。在任何一种情况下，诈骗者都会记录您提供给他们的任何信息，然后使用它来进入您的帐户。

假冒调查——诈骗者需要您完成网上调查，作为交换，他们会提供知名零售商礼品卡等奖品或奖励。调查会要求您回答一系列问题，包括披露重要身份证明或银行详细信息。

作为任何骗局的一部分——诈骗者经常在其它诈骗活动中询问个人信息。在彩票诈骗中，诈骗者经常要求提供驾驶执照或护照“证明您的身份才能发放奖金”。在约会和浪漫诈骗中，他们可能会要求提供信息以“赞助他们的签证申请，来澳大利亚探访您”。

请记住：向诈骗者提供个人信息与给钱一样糟糕。请妥善保留个人信息并确保其安全。



保护自己

- **在网络环境中，无论讲什么话，或做什么事，都要三思而后行**
  在网上分享自己的信息应当心，包括社交媒体、博客和其它网上论坛。在填写调查、参加抽奖、点击链接或附件，甚至“加好友”、“点赞”或“分享”某些内容之前，请先停下来，思考妥当之后再做。
- **警惕任何索取您的个人信息或金钱的请求**
  诈骗者会试图通过使用知名公司或政府部门的名称来欺骗您透露自己的信息。如果您认为这是一个骗局，请不要回应。使用电话簿或在网上搜索来查找该组织的联系信息。切勿使用他们在原始电邮中提供的联系信息。

如果您向诈骗者提供了个人身份信息，请致电1300 432 273联系IDCARE。

网上购物、分类广告和拍卖骗局

诈骗者也非常喜欢网上购物的便利性。

这种诈骗的运作方式

越来越多的消费者和企业在网上购买和销售物品。不幸的是，诈骗者喜欢在网上寻找受害者。

诈骗者可以创建非常有说服力的**假零售网站**，看起来像真实的东西，包括脸书等社交媒体。辨别零售网站是否是骗局的最大窍门是看他们的付款方式——如果要求您通过电汇或其他不寻常的方式付款，请谨慎行事。

网上拍卖骗局是指诈骗者声称您有第二次机会购买您出价的物品，因为获胜者退出了。诈骗者会要求您在拍卖网站的安全支付系统之外付款；如果您这样做，钱将会丢失，您将无法得到您所支付的物品，拍卖网站也无法帮助您。

网上分类广告诈骗是针对买家和卖家的常见骗局。买家应该小心那些在合法分类广告网站上发布虚假广告的诈骗者。广告范围很广，涉及从出租物业到宠物，二手车或相机的任何物品，并且通常价格便宜。如果您对该项目表现出兴趣，则诈骗者可能声称他们正在旅行或已经移居海外，并且代理人将在收到付款后交付货物。付款后，您将无法收到货物，也无法联系卖家。

对于卖家，分类广告诈骗者会以慷慨的报价回复您的广告。如果您接受，诈骗者将通过支票或汇票支付。但是，您收到的金额会远远超过约定的价格。在这种**多付款骗局**中，“买方”可能会告诉您这是一个错误，并会要求您通过汇款退还多余的金额。诈骗者希望您在发现他们的支票出现跳票或者汇票是虚假的之前汇出这笔钱。如果您已经发出了钱，那么这些钱以及您所销售的物品就都回不来了。

保护自己

- 准确了解您在与谁打交道。如果是澳大利亚零售商，一旦出现问题，解决问题更容易。
- 检查卖家是否有信誉，是否有退款政策和投诉处理服务。
- 应该避免接受任何通过汇票、电汇、国际资金转账、预付卡或电子货币要求预付款的安排。以这种方式发送的钱很少能够退回。切勿通过电子邮件向任何您不了解或不信任的人发送资金，或在网上提供信用卡或网上交易账户详细信息。
- 只能通过网站的安全付款方式付款——查找并使用以“https”开头、以及有封闭的挂锁符号的网址。
- 永远不要接受支付金额超过您的约定金额的支票或汇票，永远不要替任何人转钱。

打电话

诈骗者也会打电话和发短信。

诈骗者通过**打电话**对家庭和企业进行各种各样的诈骗，从威胁税务诈骗到提供奖品或“帮助”处理电脑病毒。

诈骗者使用**短信**发送一系列诈骗，包括抽奖或奖品诈骗。如果您回复，可能会被收取高额费用或发现自己已注册订阅服务。

上门

小心 —— 一些诈骗者会来到您家门口试图欺骗您。

挨家挨户诈骗通常是指欺诈者推销根本不会送货的或品质很差的商品或服务。甚至您不想要或不同意的工作，他们也会向您收费。

诈骗者可以扮成**假慈善工作者**来收集捐款。他们会利用洪水和森林大火等近期事件。您在捐赠之前应该要求他们出示身份证明，并查看他们的正式收据簿。

大宗邮件仍然用于发送彩票和抽奖诈骗，投资机会、尼日利亚诈骗和假遗产继承信件。

2. 沟通与诱骗

如果您给他们一个与您交谈的机会，他们就会开始用他们的诈骗工具箱中所有的伎俩来说服您把自己的钱给他们。

诈骗者的伎俩可能包括以下方面：

- 诈骗者会精心编造**令人信服的故事**来获得他们想要的东西。
- 通过使用您的**个人信息**，他们让您觉得自己以前已经与他们打过交道，这样使该骗局看起来是正当的。
- 诈骗者可能会**定期与您联系**以建立信任并使您确信他们是您的朋友、合作伙伴或浪漫的对象。
- 他们通过利用您对赢奖的兴奋，对永恒之爱的承诺，对不幸事故的同情，对没有能够提供帮助的内疚，或对被逮捕或被罚款焦虑和恐惧来**玩弄您的情绪**。
- 诈骗者喜欢创造一种**紧迫感**，因此您没有时间考虑清楚，从而做出感性的反应而不是理性的反应。
- 同样，他们使用**高压销售策略**，声称优惠是有时间限制的，价格会上涨或市场会改变，机会将会丧失。
- 骗局会使用**光鲜的小册子**和技术行业术语，使用办公室前台、呼叫中心和专业网站，拥有真实业务的所有特征。
- 通过访问互联网和聪明的软件，诈骗者很容易制作**赝品和貌似官方真品的假文件**。一份似乎得到政府批准或充满法律术语的文件可能会让骗局显得冠冕堂皇，看似很有权威。

诈骗者的具体手段都是为了让您降低防御能力，建立对他们的故事的信任，从而快速或非理性地采取行动，并进入最后阶段——付钱。

3. 付钱

有时您能够判断诈骗的最大线索就是诈骗者要求您用方式什么付钱。

在骗局的几分钟内或经过几个月的感情培养之后，就会开始要钱。至于您如何汇款，诈骗者也有他们喜欢的方式。

有时候，诈骗者会将受害者引导至最近的**汇款**地点(邮局、电汇服务、甚至银行)汇款。也有时候，他们会保持手机连线，一步一步地给出具体的指示，甚至可能会给您派一辆出租车来帮助解决这个问题。诈骗者愿意以任何方式接受资金，这可能包括**直接银行转账、预付借记卡、礼品卡、Google Play、Steam**或**iTunes卡**或虚拟货币(如**比特币**)。任何不寻常的付款方式的要求都使他们露出马脚，表明是一场骗局。

信用卡通常可以提供一些保护，您还应该查看安全的付款方式，如网址中出现“https”字样，并且网站上有一个封闭的挂锁符号。不要向在网上或通过电话认识的人汇款——特别是如果他们在海外。请注意，诈骗者还可以要求以贵重物品和贵重礼品(如珠宝或电子产品)的形式付款。向诈骗者付钱并不是您应该担心的唯一问题——如果您帮助为陌生人转账，就可能会无意中卷入**非法洗钱**活动。

市长寄语

John Faker市议员
Burwood市长

不论您的背景、年龄和收入水平如何，您都有可能成为诈骗的目标。

每年，诈骗都会使澳大利亚居民、企业和经济损失上亿澳元，并对受害者和其家人造成情绪上的伤害。

阻止诈骗的最佳方法之一，就是通过个人意识和教育保护自己，领先诈骗者一步。

为了让您领先一步，Burwood市议会整理了本指南，以帮助大家提高对诈骗问题的认识。同时，我们也鼓励您访问全国消费者保护机构——澳大利亚竞争与消费者委员会(ACCC)的网站。

需要防范的最常见骗局

正如之前所说，每个人都有可能受到诈骗，所以每个人都需要了解有关如何识别和避免被骗的信息。有些人认为只有轻信和贪婪才会成为骗局的受害者。事实是诈骗者很聪明，如果您不知道需要注意什么，任何人都可能成为骗局的牺牲品。

您是否收到过好得难以置信的提议，可能是打电话来帮助修理您的电脑，也可能是威胁您支付子虚乌有的欠款、银行或电信提供商发出的关于您帐户问题的提醒，甚至是邀请“加好友”或上网连线？诈骗者知道如何打动您以获得他们想要的东西。

他们变得越来越高明，与时俱进，利用新技术、新产品或服务以及发生的重大事件来创造可信的故事，取得您的信任，然后说服您将自己的资金或个人信息发送给他们。

然而，根据每年收到的成千上万的诈骗报告，ACCC已经准备了一份常见诈骗清单，以揭示诈骗者不希望您知道的诈骗秘密和策略。

本手册为您提供了一些示例，如需获取更全面的信息，建议您下载《防诈骗小黑书》(The Little Black Book of Scams)。此书获得国际认可，是帮助消费者和小型企业了解诈骗手段的重要工具，您可前往下方网站在线获取：
www.accc.gov.au/littleblackbookofscams

诈骗如何运作

骗局的解析

大多数诈骗都遵循相同的模式，一旦理解了这一点，就会更容易辨识骗局。

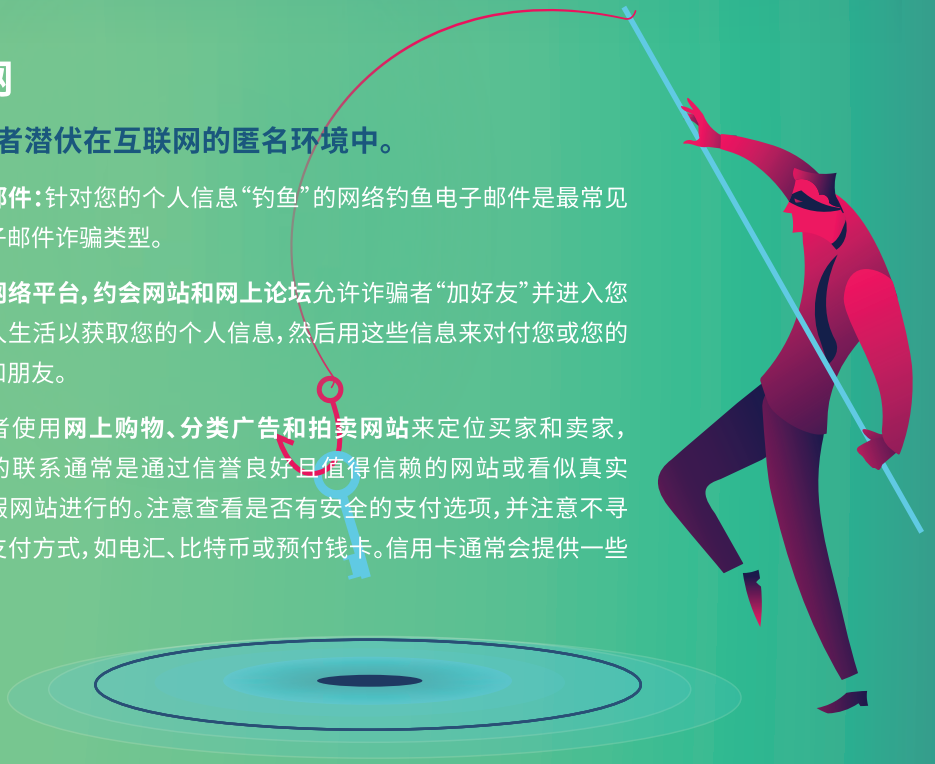
如果仔细查看本书中列出的所有不同类型的诈骗，您很快就会注意到大多数骗局都包括三个阶段：(1)接近；(2)沟通；(3)付款。了解诈骗的基本组成部分会帮助您避免当前常见的诈骗形式，并防范未来出现的新诈骗。

1. 接近：交付方法

当诈骗者接近您时，总会带着一个编造出来让您相信的谎言故事。

诈骗者总会冒充其他人，政府官员、专家投资者、彩票官员甚至是浪漫的崇拜者。

为了向您提供这些谎言，诈骗者将使用一系列不同的沟通方法。



上网

诈骗者潜伏在互联网的匿名环境中。

电子邮件：针对您的个人信息“钓鱼”的网络钓鱼电子邮件是最常见的电子邮件诈骗类型。

社交网络平台，约会网站和网上论坛允许诈骗者“加好友”并进入您的个人生活以获取您的个人信息，然后用这些信息来对付您或您的家人和朋友。

诈骗者使用**网上购物、分类广告和拍卖网站**来定位买家和卖家，最初的联系通常是通过信誉良好且值得信赖的网站或看似真实的虚假网站进行的。注意查看是否有安全的支付选项，并注意不寻常的支付方式，如电汇、比特币或预付钱卡。信用卡通常会提供一些保护。

FLIP FOR ENGLISH TRANSLATION

识别诈骗，阻止诈骗!

SPOT A SCAM STOP A SCAM

Burwood
Inc.1874

诈骗识别、避免与
自我保护的快速指南