Qudos Bank

Be scam safe

Learn how to protect yourself
from scams and financial fraud

Contents

At Qudos Bank, your safety and security are our top priority. It's part of our partnership with our customers and community.

To keep you safe, we employ a range of security measures to protect your personal information and transactions. It is important that you continue to stay informed and take the actions needed to protect yourself.

This booklet provides a brief overview of the principles behind common frauds and scams; how they work, what to look out for, and what to avoid. By furthering your awareness and knowledge of frauds and scams, together we can continue to protect you.

Visit www.qudosbank.com.au/fraud to find out more about how we protect you from fraud and how you can protect yourself.

What is Fraud?

The most common types of fraud are designed to obtain money

Before learning how to avoid scams and fraud, it's important you understand what they are.

Essentially, fraud is a deceptive or deceitful act that causes one person to receive a benefit that they are not entitled to while depriving another person of something.

The most common types of fraud are designed to obtain money. However, fraud can also be used to obtain property or goods illegally or to avoid paying for services provided. In short, it's any activity where someone is trying to cheat you out of something that is yours.

Scams are a specific type of fraud that usually involves persons deceitfully trying to obtain your personal information, identity, or monies.

Who is most likely to be targeted by fraud?

Every year, thousands of people are affected by fraud and scams. Scams target people of all backgrounds, ages, and income levels across Australia. There's no one group of people who are more likely to become a victim of a scam, and most of us would have experienced fraud and scams at some time.

Scams succeed because they look real and can catch you off guard when you're not expecting it. Scammers continue to be smarter and take advantage of new technology, new products or services and major events to create believable stories that aim to convince you into giving them your money or personal details.

Common scams to watch out for

Attempts to gain your personal information

Scammers are constantly evolving their tactics to steal your personal information and fraudulently use your identity to access your savings, open accounts or apply for loans and credit cards. Common scams include:

- Phishing - scammers will send you an email or SMS that looks like it's from a trusted organisation and try and trick you into entering your password into a fake website.
- Remote access scams - scammers call and try to convince you that you have a problem with your computer or that hackers are trying to access your computer and need their help to fix the issue. In reality, they gain remote access to your computer and steal your personal information, including your internet banking details to access your personal information and funds.
- Business Email Compromise scams (BECs) – a variation on phishing, where scammers generally compromise business email accounts, intercept legitimate invoices and change the details to include fraudulent payment information which subsequently gets paid by the unsuspecting recipient. Another technique involves CEO's and staff being impersonated and requesting monies to be paid or transferred.

They may use an almost identical email address, username, or fake invoice.

The key to staying safe is to be cautious of any incoming communication via text message, email, social media, or phone. If you spot warning signs, it pays to check with the company or person directly using their contact number on the public website or telephone directories.

Identity theft

Identity theft involves a scammer using your identity to steal your money – often by impersonating you and applying for a credit card in your name or gaining access to your bank accounts.

To avoid falling victim, keep bank statements, tax returns, and other documents that detail your personal financial information safe. Keep your mailbox locked to avoid theft and shred documents before throwing them away.

Buying or selling scams

Buying or selling goods and services brings you into contact with people that you've never met before. Sometimes those new people may be dishonest and they may try to scam you.

Common classified scams include fraudulent sellers offering goods for below market value and requesting money be paid through a channel that is difficult to trace e.g. wire transfer. Once payment is made, the seller disappears.

If you are selling something online or through classified sites, never send an item until payment has cleared in your bank account.

Overpayment is also another common scam where scammers send a fake receipt/confirmation that pretends to pay more than the asking price, then request that the excess money is refunded to them or a third party before you receive any monies.

The scammer's payment may never have been made, or if payment is made, this could subsequently be cancelled by the scammer (cheques bounce or credit card payments cancelled), and you never receive the monies as detailed.

Investment scams

Investment scams are one of the most common frauds reported to the Australian Consumer Complaints Commission (ACCC). They often begin with a cold-call promising very high returns for little risk. Common scams include:

1. Opportunities to invest in little-known companies on foreign stock markets.
2. Sports betting scams, promising to beat the odds.
3. Fake cryptocurrency or foreign exchange trading software that claims to predict future trends.

Stay safe by ignoring unsolicited offers and end any conversation where the caller is putting pressure on you to make a decision. If something appears too good to be true, then the chances are that it is a scam.

For more information on how to spot and avoid scams, visit www.qudosbank.com.au/fraud.

keep documents that detail your personal financial information safe

Jobs & employment scams

When you are looking for a new job, it is common to see ads promising ‘easy money’ for little effort. Job opportunities to be wary of include:

- Fake job ads where victims are asked to use their bank accounts to transfer money overseas but are helping to launder money.

- Pyramid schemes, where members are rewarded for recruiting more members, rather than by the sale of services or products. Most pyramid schemes cost money to join, which is passed up the tiers of the pyramid. When recruitment dries up, the pyramid fails and those at the bottom lose their investment.

Use caution when reviewing employment opportunities. Even if you act unwittingly, you may still be committing a crime by potentially laundering illicit proceeds of crime.

Review all unsolicited communication with a cautious attitude and never transfer funds to a stranger overseas

Threats & extortion

Scams targeting people that demand payment for protection from a ‘threat’ are increasing.

The threats are created by the fraudsters themselves through ‘malware’ (malicious software) that infect the victim’s computer, or by unsolicited phone calls, which falsely accuse the victim of wrongdoing e.g. avoiding taxes.

These scams rely on pressure and intimidation to work. If you receive a message or a call that could be for a legitimate reason, call the relevant organisation using the number on their website. Never send money or give credit card details, account details, or personal information to anyone you don’t know or trust by email or over the phone.

Unexpected money

If you’re contacted to say that you are the lucky recipient of a surprise windfall, it may be that you are being targeted by an unexpected money scam. Victims are asked to pay money to receive something of greater value – an inheritance they didn’t know they were entitled to, a tax rebate, or a reward for helping someone move money outside of a country.

Review all unsolicited communication with a cautious attitude and never transfer funds to a stranger overseas.

Unexpected winnings

These scams involve scammers contacting victims to tell them they have won a competition but that a fee must be paid to unlock the prize. Once the initial fee is sent, further fees may be requested as a complicated story is invented about why the prize can't be released immediately. Variations include:

- Lottery wins, often for foreign lotteries
- Holiday scams, with fake travel vouchers offered
- Scratchie scams, with actual scratch cards delivered in the mail

It's important to remember that you can't win a competition that you didn't enter and it's very likely to be a scam.

Dating and relationship scams

Unfortunately, not everyone using online dating applications and sites are who they say they are. Sometimes fraudsters create fake profiles that claim to be eligible singles, and sometimes they may be living outside Australia. Common reasons for being overseas include being an active-duty soldier, oil rig worker, or medic with international organisations.

After a relationship has been established, the fake profile (person) has an emergency - often an unexpected medical or visa expense and requests financial help from their new love. Payment is often requested by money transfer or gift cards, which means that they are almost impossible to track or to reclaim.

Never send money to someone you haven't met – no matter how strongly you may feel for them.

For more information on how to spot and avoid scams, visit www.qudosbank.com.au/fraud.

How to spot frauds

While the tactics of scams and fraud are constantly evolving, there are some core traits that most scams include. Awareness and being able to spot these will assist you in not falling victim and giving out your personal information or monies.

»»

If a deal sounds too good to be true, it's very likely that it is

Scam warning signs include:

1. **Unsolicited contact**
   Scams often begin with someone contacting you unexpectedly. With any unsolicited contact, it's important to independently verify that the person is who they say they are.

2. **An offer is too good to be true**
   Scams will often promise high returns with low risk. If a deal sounds too good to be true, it's very likely that it is.

3. **You're asked to keep quiet**
   Scammers often try to isolate their victims from support network and their banks. If you're asked to keep quiet about an opportunity or about someone you're talking to online, it could be a red flag that everything is not as it should be.

4. **You're asked to make payment to another party**
   A large number of frauds involve victims being asked to pay a fee to unlock a greater reward. No legitimate business or seller will ask you to pay an upfront fee to receive a prize, or to sell something that you own.

5. **You are asked to use an unusual payment method**
   Online scams often request payment in the form of direct money transfers, telegraphic transfer, pre-paid gift cards, or cryptocurrency. These forms of payment are very difficult to trace and recall, which means that if they are used to send money to a scammer then it's very unlikely that it will be recovered.

What to do if you've been scammed

Fraud can affect anyone and even the most careful person can be taken advantage of.

If you or someone you know has been the victim of fraud, there are four important steps to take:

1. **Let us know**
   If you have been targeted by a scam relating to your Qudos account, visit our webpage www.qudosbank.com.au/report to find out who to contact.

2. **Contact the police**
   Many victims are reluctant to report fraud as they're concerned that their family or the police may think less of them. However, victims of fraud are encouraged to report the incident to ensure those responsible can be prosecuted and others aren't taken advantage of.

3. **Report cyber crimes to Australian Cyber Security Centre (ACSC);**
   The Australian Cyber Security Centre (ACSC) leads the Australian Government's efforts to improve cyber security and help make Australia the safest place to connect online with 24/7 worldwide cyber threat monitoring services.

4. **Report the fraud or scam to 'ScamWatch'**
   To assist the ACCC in monitoring scam trends and taking action where appropriate, including working with industries and looking for innovative ways to disrupt scams. This also assists in keeping Australians informed about the latest scams in circulation.

Many victims are reluctant to report fraud as they're concerned that their family or the police may think less of them

You can learn more about how to protect yourself online and report cyber-crimes at www.cyber.gov.au.

For more information or assistance, visit www.qudosbank.com.au/staysafe