



# Smart Scam Guide



## What is a scam?

A scam is a dishonest attempt to steal your money or personal information. It can appear as an amazing deal, a quick way to get rich, or another offer that seems too good to be true.

## How do you spot a scam?

Scammers create pressure, use unusual payment methods, or try to scare you into acting quickly. If something feels off, slow down, double-check, and talk it over with someone you trust.



## Scam Red Flags



**Unexpected contact:** calls, texts or emails claiming to be from your bank, the ATO, police or a courier.



**Pressure:** “act now,” “keep this private,” or threats your account will be closed.



**Odd payment methods:** gift cards, crypto, wire transfers, or paying outside the platform.



**Links and files:** messages pushing you to click a link, open an invoice, scan a QR code or “verify” details.



**Strange web addresses:** small spelling changes, extra letters, or shortened links.



**Remote access:** told to install software so they can “fix” your device.



**Sender mismatch:** the display name looks right, but the email address or number does not.







**Secrecy or workarounds:** asked to move off the official site or skip normal steps.

## Phishing Scams

Scammers send emails or messages impersonating legitimate organisations, such as banks, tricking recipients into revealing sensitive information like passwords or banking details. Phishing scams can even be tailored to specific individuals or organisations with personalised emails and calls.


A common technique phishing scammers use is to send emails with copycat login pages, QR codes or attachments requiring you to share sensitive information and send back to the scammer. Do not click or engage with emails asking for any sensitive information. Always go directly to an organisation's website to contact them directly.

### Spot it:

-  Links or web addresses that look slightly wrong.
-  Attachments or QR codes you were not expecting.
-  Requests One-Time Passwords (OTPs) or remote access.
-  Phone numbers in the message that are not on the official site.

## Remote Access Scams

If you are ever unsure about who you are speaking to, disengage, and contact your bank or telecommunications provider directly. Scammers often pretend to be from tech support or a Government Agency, they claim there is a problem with the victim's computer or device and offer to help fix it remotely. They trick victims into granting remote access to their computers to install malware or steal personal information.

-  Remember that banks and telecommunications providers will not require access to your online banking.



---

## Online Marketplace Scams

If you are unsure about a buyer or seller, stop and contact the marketplace through official support.

Scammers will often pressure you to move to a different communication channel such as WhatsApp or Messenger. They can also send fake screenshots of payments, links for you to click to 'confirm delivery' or 'release funds' for deposits, courier fees, or gift cards.

You may also never receive the goods after you pay.

-  Only message and pay within the platform or use cash on collection after seeing the item.
-  Do not share one-time passwords or pay outside the platform.

## Tax Scams

Imposters pose as tax officials, demanding immediate payment for fake debts or offering fake refunds to trick individuals into providing personal or financial information.

- ATO Impersonation Scams
- Fake Tax Refunds
- Fake Tax Preparation Services

---

## Investment Scams

Fraudulent schemes promise high returns with low risk but end up swindling investors through fake ventures.

- Cryptocurrency scams
- Ponzi schemes
- Fake initial public offering scams
- Superannuation scams
- Celebrity endorsement scams

## Rental Scams

A rental scam involves someone posing as a landlord or property manager to advertise a nonexistent or unavailable rental property.

These scammers ask for upfront payments or deposits, then disappear with the money. They might also show a property they do not own, taking payments from multiple renters for the same place. Victims often lose their money and face significant inconvenience without a place to live.

---

## Romance Scams

Scammers create fake profiles on dating sites to develop relationships and then request money under false pretences preying on emotions for financial gain.

If they refuse to video call or phone call and ask for money, personal information or images, stop contact immediately and get a second opinion from someone you trust.



If you have fallen victim to a scam and someone contacts you claiming they can help you recover your lost money, be cautious—this is likely another scam.

# BankVic's Top 3 Safety Tips



Never share one-time passwords: not by phone, text or email.



Never pay with gift cards: no legitimate organisation requests them.



Be cautious on marketplaces: avoid unusual deposits and only pay through secure platforms and methods.

## What to do if you have been scammed?

### Step 1

If you have given any financial details or have already lost money, contact your bank immediately.

### Step 2

Report the scam to police at **cyber.gov.au** or at your nearest police station.

Additionally you can report the scam to Scamwatch at **scamwatch.gov.au**.

For support if you have been scammed, contact IDCARE at **1800 595 160** or visit **www.idcare.org**.