



Scams

Key crime prevention tips

- Know how to spot a scam.
- Check the facts.
- Be cautious with direct contact.
- Protect yourself.

Scam prevention checklist

- A scam is an attempt to intentionally mislead a person, usually for financial gain.
- Scams can come via mail, email, telephone, over the internet and door-to-door.

Know how to spot a scam

- If it sounds too good to be true, it is probably a scam.
- Use the S.T.O.P method to identify scam or 'Phishing' Emails. Is the Email?
 - **S**uspicious – unexpected, has spelling errors and/or doesn't look right
 - **T**elling you to click on something or provide personal information
 - **O**ffering something amazing
 - **P**ushing you to act quickly.

Check the facts

- Check the company website to confirm offers.
- Check the company has a telephone number and/or email address.
- Check if the company has an Australian Business Number or Australian Company Number at Abr.business.gov.au.
- Don't rely on glowing testimonials provided by the seller.

Be cautious with direct contact

- Do not respond to unsolicited offers and deals.
- Do not respond to requests for your personal information.
- Do not use phone numbers provided in unsolicited emails. Search for company's publicly available phone number.
- Do not click on a link provided in an unsolicited email. Type in the web address or search for the company by name.
- Do not give out personal information on incoming calls. Call the company back using a publicly available number.

Protect yourself

- Never send money or bank details to claim a prize.

Other things you can do

- When shopping online:
 - Check for the closed padlock symbol which shows it is a secure site.
 - Use a secure third-party payment facility.
 - Read the terms and conditions before paying.
- When banking online:
 - Do not open emails or click on links asking for your banking details. Banks never ask for your banking details in emails
 - Report suspicious emails to your bank.
 - Do not provide your banking information by email.
 - Always log off when you are finished.
- Regularly monitor your account transactions.



VICTORIA POLICE

- When using social media:
 - Limit the amount and type of personal information you put online.
 - Don't advertise your holiday plans online.
 - Set the security and privacy settings to limit access to your account and check the settings regularly.
 - Regularly update your privacy settings.

What to do if you have been scammed

- Call your bank to report the incident.

Report it

- Report door-to-door scams, scams from interstate or overseas, financial or credit card scams, and scam emails: [cyber.gov.au/acsc/report](https://www.cyber.gov.au/acsc/report).

Additional resources

- Stay Smart Online – Australian Government: www.cyber.gov.au.
- Consumer Affairs Victoria provides information about consumer scams: www.consumer.vic.gov.au/resources-and-tools/scams/consumer-scams.
- Scam Watch – Australian Competition and Consumer Commission: www.scamwatch.gov.au.

**For more information, visit
police.vic.gov.au/your-safety**

