TOP 10 TIPS TO PROTECT YOURSELF AGAINST

IMPERSONATION SCAMS

SECURITY IN DEPTH

Today's scams are becoming more and more sophisticated. Previously, poor spelling and grammar made them easy to spot, but new technology means scams are becoming harder to detect.

Security in Depth is dedicated to providing comprehensive information and support to combat scams through collaboration with government agencies, industry experts, law enforcement bodies, and community organisations. We emphasise the importance of staying informed about the latest and evolving scams as a key strategy to protect yourself. By understanding the characteristics and warning signs of scams, especially impersonation scams, you can take proactive steps to safeguard your personal information. Additionally, in the unfortunate event that you become a victim of a scam, we are here to offer guidance and assistance. Our guide is specifically designed to educate you on identifying impersonation scams, protecting yourself against them, and knowing where to go for help when needed.

In this guide

What is an impersonation scam?

Impersonation scams are designed to look like they're from legitimate organisations that you know. They can appear to be from your bank, internet service provider, a government agency, retailer, or even a scammer pretending to be a friend or family member.

By pretending to be from someone you trust, scammers use a sense of urgency to trick you into paying money or providing personal information, such as important passwords, credit card or banking details.

Scammers use a range of methods to get in touch with you, including text messages, phone calls, emails, social media posts, and fake websites that look identical to official websites.

What is spoofing?

Impersonation scams are designed to look like they're from legitimate organisations that you know. They can appear to be from your bank, internet service provider, a government agency, retailer, or even a scammer pretending to be a friend or family member.

By pretending to be from someone you trust, scammers use a sense of urgency to trick you into paying money or providing personal information, such as important passwords, credit card or banking details.

Scammers use a range of methods to get in touch with you, including text messages, phone calls, emails, social media posts, and fake websites that look identical to official websites.

There are different types spoofingtechniques, including:

01. Caller ID spoofing: scammers alter their caller ID to show a phone number different to the one being used, making the call appear to come from a legitimate number.

02. SMS spoofing (or alpha tags): scammers alter their phone number to appear as a business name (for example, AusPost). It can make a text message appear in the same conversation or thread as genuine messages from an organisation.

03. Email spoofing: scammers alter their email address or sender name to make an email look like it's from a trusted source. They may fake the 'From' display name or the email address, often by changing or adding a letter or number to a legitimate domain name (for example, @amaz0n.com instead of @amazon.com).

Common impersonation scams

Bank impersonation scams

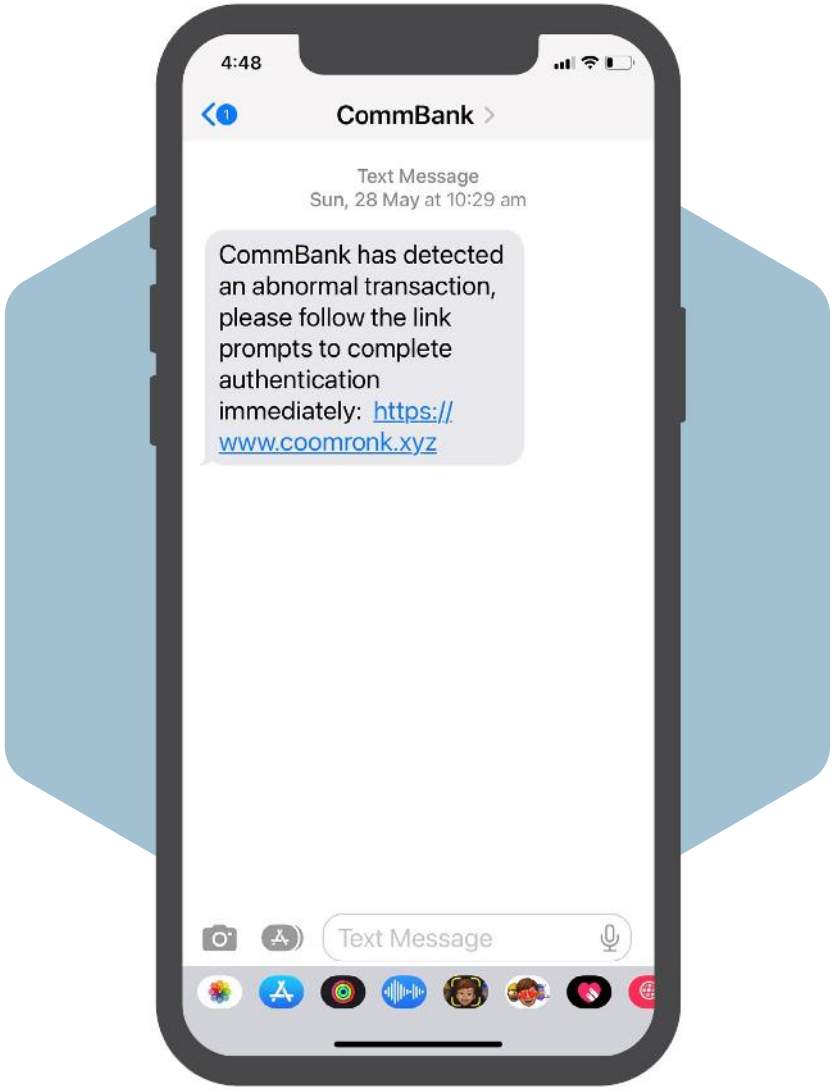
- You receive a call or a text message from someone claiming to be from your bank's security department. They inform you of a suspicious transaction, claiming your account has been compromised. They urge you to transfer money to a different account to 'keep it safe' or for 'further investigation'.

- You receive a text message or email asking you to click on a link to verify your account details. The link takes you to a fake website designed to capture your username, password and other personal information.

How do you know it's a scam?

While your bank may contact you if there's suspicious activity on your account, it will never ask you to transfer funds to another account. Nor will it ask for any account or personal details, including your password, PIN or one-time passcode in an unsolicited text, email or phone call.

Scammers can make a phone number look like your bank's caller ID, but don't take that as proof of who you're speaking to. They may also appear to have information about you, but any details they hold have likely been fraudulently obtained.



Example of a bank impersonation text from a spoofed number asking you to click on a link to verify your details.

Bank impersonation scams

- A caller claiming to be from an internet service provider, telecommunications or computer company, informs you there's a problem with your internet or computer. They may say it's been hacked, has a virus, is running slow or is about to be disconnected. They guide you to download an app or software to give them remote access to your computer so they can 'fix it'.

- A warning message appears on your computer screen urging you to immediately call the listed phone number for help with a problem that's been detected.

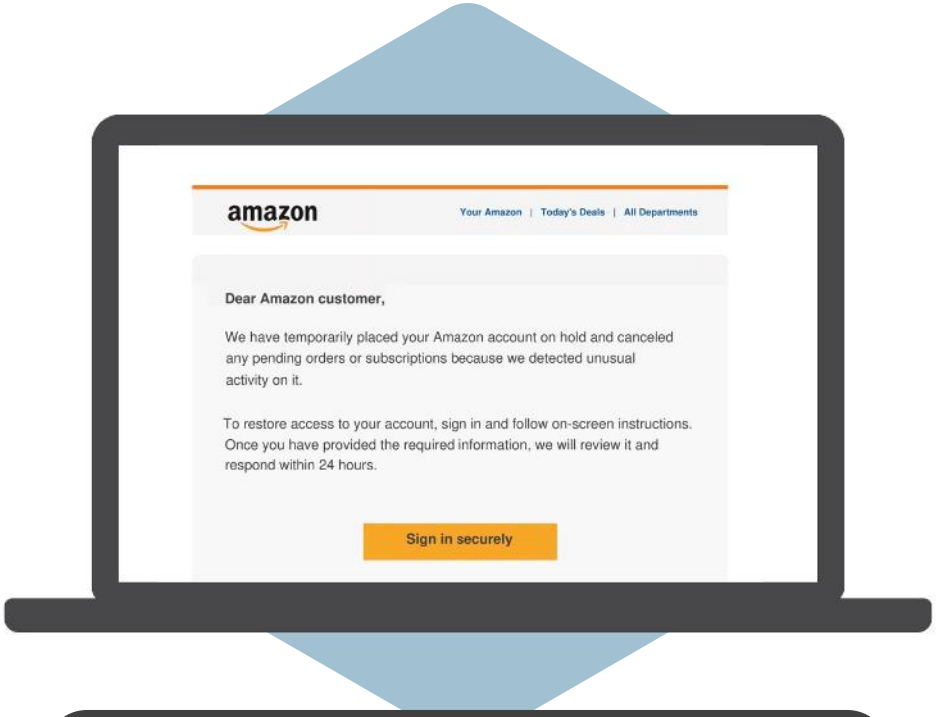
How do you know it's a scam?

Legitimate companies will never call to tell you there's an issue with your internet connection or computer (they expect you to contact them when there's a problem). They will never ask you to download any type of software or app that gives them access to your device. Close suspicious pop-up messages by clicking the 'x' in the top right corner of the box. If that doesn't work, try clicking outside the box or close the web page it appears on. If the pop-up still hasn't disappeared, try holding the ALT and F4 keys on your Windows computer to close the web browser. On an Apple computer, select Force Quit from the Apple menu and select the browser you want to close

Account Suspension

- You receive an email or a text message claiming to be from an organisation you know, such as Amazon, PayPal or Netflix. It informs you that your account has been suspended due to suspicious activity and that you'll need to click on a link to confirm your identity so they know it's really you. Scammers use scare tactics to direct you to a fake website that captures personal details such as your username, password, and banking or credit card details.

- A warning message appears on your computer screen urging you to immediately call the listed phone number for help with a problem that's been detected.



How do you know it's a scam?

Amazon, PayPal and Netflix will never ask for personal information such as your passwords, bank or credit card details through a link in an unsolicited emailor text. While organisations differ in their approachto contacting customers, it's best to play it safe and always treat these types of emails, texts or calls with caution.

If you're unsure whether a message is really from the business it claims to be from, contact them directly by doing a search for their contact details online. Never use the contact details provided in the text, email or phone call.

Look out for scare tactics

Scammers use scare tactics to create a sense of urgency to get you to act. Here are some things they may say to catch your attention:

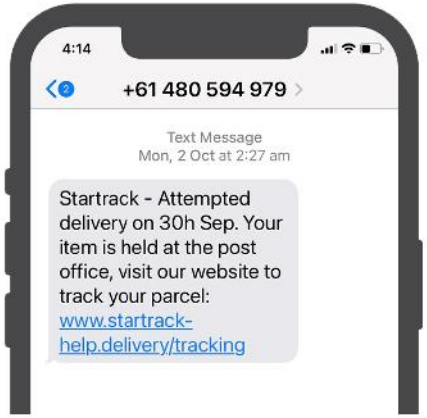
- Unusual account activity has been detected
- Unauthorised login attempts
- Your account is blocked / locked
- Your payment was declined
- We're unable to validate your billing information

Unsuccessful delivery attempt

You receive an email or text message claiming to be from Australia Post or a courier company such as FedEx informing you that there's a problem or hold up with your delivery. To receive your package, you will need to pay a shipping cost or 'update your details'.

How do you know it's a scam?

Australia Post, FedEx and other legitimate courier companies will never text, email or call to ask for personal information or payment. If you're expecting a delivery, it's best to track your delivery through their secure app or via the online tracking service in your order confirmation email. If you don't have one, call the courier company direct to enquire about the status of your parcel.



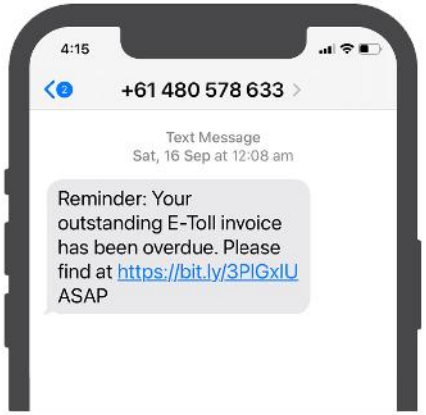
Example of a text message claiming to be from a courier company

Toll road scam

You receive a text from a toll road operator informing you that your toll payment is overdue. You need to take immediate action to avoid paying a fine, so they include a link for you to arrange payment but it takes you to a fake website designed to steal your financial details.

How do you know it's a scam?

If you've been sent a text claiming you have an overdue toll road account or insufficient funds, it could be a scam. Visit the toll operator's website or app to log into your account to check your recent activity



Example of a text message claiming to be from a courier coExample of a toll road scam text.mpany

Fake investment scams

You see an amazing investment opportunity that appears to be endorsed by a celebrity or finance influencer. It promises a guaranteed high return with little to no risk. When you enquire, you're directed to a professional looking website and receive sophisticated promotional material.

How do you know it's a scam?

If a deal sounds too good to be true, it probably is. Scammers use high-pressure tactics to convince you to act quickly so you don't 'miss out'. Beware of emails, websites or ads with testimonials and over-the-top promises of big returns.

The 'adviser' who is helping you may claim they don't need an Australian financial services (AFS) licence. If they do provide one, always check that the person you're dealing with is the true holder of the licence.

Fake websites

You see an ad on Facebook for a well-known BBQ brand selling for $100 when it's normally priced at $900. You click on the link to the retailer site and see that credit card payments attract a 2.99% fee, so you opt to pay by direct bank transfer to receive a further 5% discount. You receive a confirmation email but no BBQ.

How do you know it's a scam?

Fake websites have prices that are too good to be true, unusual forms of payment, and other red flags such as a URL that tries to look like an official store's URL (for example, webberbbqs.com versus the real weber.com).

Scammers can also pay for ads on social media and search engines such as Google (known as sponsored ads), so tread carefully when clicking on these types of ads.

01 Beware of unsolicited calls. Let calls from phone numbers you don't recognise go to voicemail.

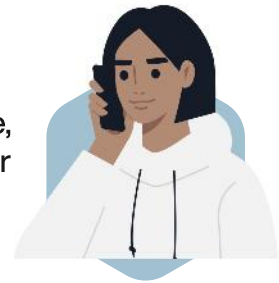
02 Stop and think before you provide personal or financial details over unsolicited communications. Ask yourself: could it be fake?

03 Beware of emails that use scare tactics. Check the display name and email address. Do they match? For example, the 'From' field displays Amazon Support but the email address is amazon support830@gmail.com

04 Don't trust a text message just because it appears in the same thread as other messages from an organisation you know. It could still be a scam message.

05 If you're unsure about a message or call you've received, contact the organisation it claims to be from. Get in touch via their official website or secure app on your smart-phone or tablet.

06 Never provide your password, PIN, or one-time code to anyone over the phone, even if they claim to be from your bank or a government agency and they read out information about your account.



07 Never tap on links in text messages. While it's possible for some to be harmless, it's best to play it safe. Same goes for attachments and links in emails unless you are certain about the sender.

08 Never follow instructions from an unsolicited caller who wants you to download an app or install software that provides them with access to your device. Hang up immediately.

09 Never log into your online accounts via a link in an email or text. Instead, enter the company's URL into your web browser or use their secure app to access your account.

10 Before making a payment online, always check the website's URL (is it the official site?), look for unusual payment methods and poorly worded or missing information in the About Us, Shipping and Returns and other sections found at the bottom of the website.

If you're ever in doubt, do a search online by entering the name of the organisation or website in question and the word 'scam'.

Think you've been scammed?

Where to go for help

Being scammed can take a financial and emotional toll, so it's important to seek help and act quickly. There are several steps you can take:

1. Contact your bank immediately to stop any further transactions from happening.

2. Contact IDCARE, a free support service for people who have been impacted by scams or identity theft. Call 1800 595 160 or visit idcare.org

3. Change your passwords immediately and ensure they are strong.

4. Report the scam to Scamwatch to warn others: scamwatch.gov.au/report-a-scam

5. Get support for yourself. If you don't feel comfortable speaking to friends or family, contact Lifeline or Beyond Blue for a confidential chat. And if you've lost a significant amount of money, speak to the National Debt Helpline.

Beyond Blue: 1300 22 4636 (24/7) or visit beyondblue.org.au
Lifeline: 13 11 14 (24/7) or visit lifeline.org.au
National Debt Helpline: 1800 007 007 (weekdays, 9.30am to 4.30pm) or visit ndh.org.au

The Little Black Book of Scams is an internationally recognised tool to help you learn more about a range of common scams and how you can protect yourself against them.

Visit the Scamwatch website to stay up to date with the latest scams and advice on how to protect yourself against them.

About Cyber Aware

Cyber Aware is a program initiated by Security in Depth aimed at improving the digital literacy, confidence, and cybersecurity awareness of older Australians. This initiative provides access to free computer training, brief online tutorials, and a wide array of educational materials covering diverse subjects. The Cyber Aware platform and its educational content are curated and maintained by Security in Depth.