

Stay Safe Guide 2024



Bank
Orange

bankorange.com.au

Stay Safe

Bank Orange takes your security seriously.

We are working with our customers and the community to keep each other safe from fraudsters and scammers who are taking advantage of peoples good nature and vulnerabilities.

There has been an increase in fraud and scam cases across the Orange region, and Australia. Our team focuses on scam and fraud prevention education through forms and proactive initiatives. Fraud is the overall definition of being swindled out of your hard earned money, and you can experience fraud through a number of different scams, data breaches or hacks.

If you believe you have fallen victim of fraud, contact your financial institution immediately.

Bank Orange provides complimentary education sessions through our Stay Safe and Digital Banking forums.

Visit bankorange.com.au/stay-safe for information on upcoming forums, the latest scams and fraud news as well as downloads and security guides.

“ If sounds too good to be true, it probably is. Know who you are dealing with. ”





1

STOP

Don't give money or personal information to anyone if you are unsure. Scammers will offer to help you or ask to verify who you are. They will pretend to be from organisations you know and trust.

2

THINK

Ask yourself could the message or call be fake? Never click on a link in a message. Only contact businesses or government using contact information from their official website or through their secure Apps.

3

PROTECT

Act quickly if something feels wrong. Contact your financial institution if you notice some unusual activity or if a scammer gets your money or information.

Data Breaches

Cyber-attacks on businesses can lead to a data breach, which could see your personal details being sold or made available on the dark web. Two of the most prominent recent cyber-attacks were those on Optus and Medibank, where some customers identity documents such as drivers' licence or passport numbers could be in the hands of criminals.

If you are advised you may have been impacted by a data breach, it is important to have a heightened sense of awareness and be on the lookout for any of the scams or suspicious activity outlined in this guide, and more.

Steps you can take to protect your personal information include:

- Secure your devices and monitor for unusual activity
- Change your online account passwords and enable multi-factor authentication
- Actively check your accounts for unusual activity such as items you haven't purchased
- Place limits on your bank accounts or ask your bank how you can secure your money

some data breaches come in the form of a 'brute force attack' where a particular business may be targeted by a computer robot guessing the login and passwords of it's users.

It is imperative to ensure you have a strong password, which you keep confidential, to decrease the effectiveness of these types of attacks. Below is a graph which demonstrates the direct connection between a brute force attack and the complexity of a password.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

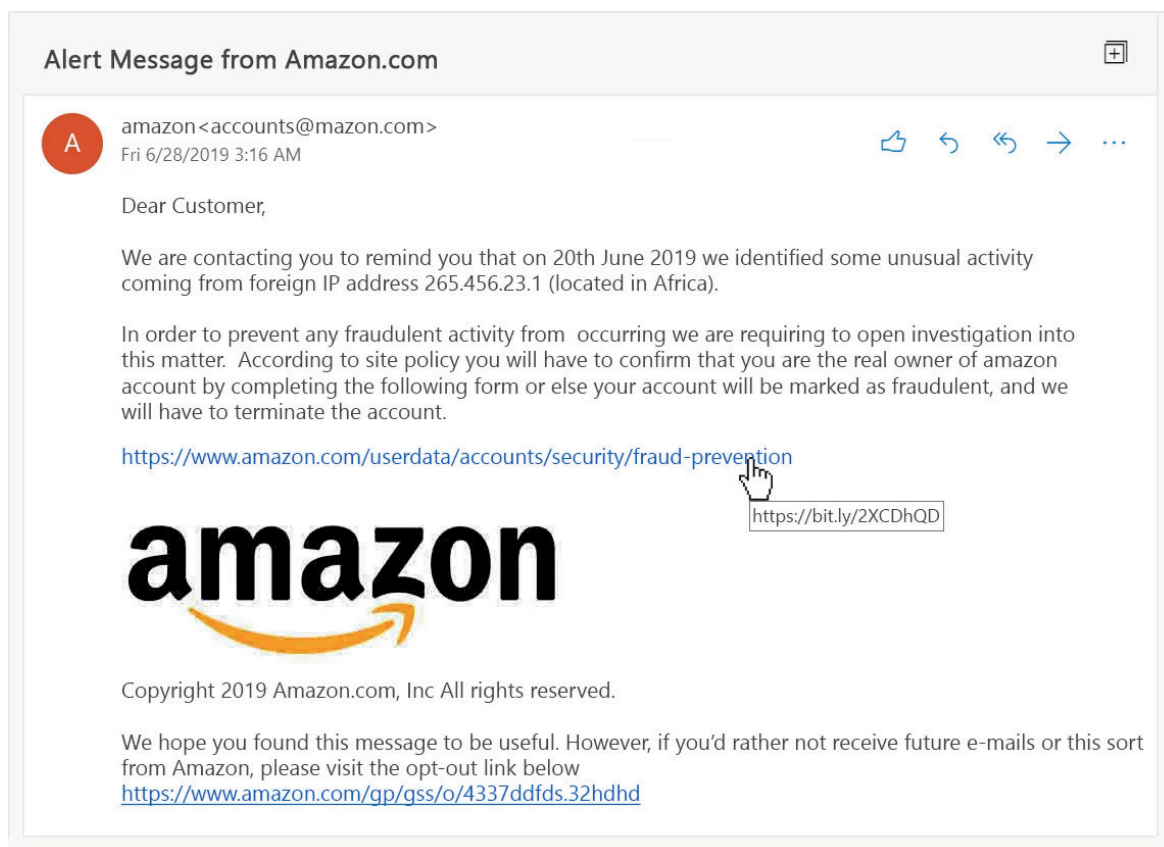
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

Phishing

A scammer contacts you pretending to be from a legitimate business such a bank, telephone or internet service provider. You may be contacted by email, social media, phone call, or text message. A Phishing call can also lead to a remote access scam, outlined on page 4.

Phishing messages are designed to look genuine, and often copy the format used by the organisation the scammer is pretending to represent, including their branding and logo. They will take you to a fake website that looks like the real deal, but has a slightly different address. For example, if the legitimate site is 'www.realbank.com.au', the scammer may use an address like 'www.reallbank.com'.

Common Phishing text messages, emails or phone calls are from Australia Post, Telstra, Microsoft, Government or financial institutions. If in doubt, get in contact with those agencies directly through your normal means, or a google search, not through any contact information provided in the text or email.





Remote access

Remote access scams try to convince you that you have a computer or internet problem and that you need to buy new software to fix the problem.

The scammer will phone you and pretend to be a staff member from a large telecommunications or computer company, such as Telstra, the NBN or Microsoft. Alternatively they may claim to be from a technical support service provider.

They will tell you that your computer has been sending error messages or that it has a virus. They may mention problems with your internet connection or your phone line and say this has affected your computer's recent performance. They may claim that your broadband connection has been hacked.

The caller will request remote access to your computer to 'find out what the problem is'. The scammer may try to talk you into buying unnecessary software or a service to 'fix' the computer, or they may ask you for your personal details and your bank or credit card details.

The scammer may initially sound professional and knowledgeable—however they will be very persistent and may become abusive if you don't do what they ask.

You don't have to be a Telstra or Microsoft customer to be called by these scammers. You don't even have to own a computer!

- Never give an unsolicited caller remote access to your computer.
- Never give your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
- If you receive a phone call out of the blue about your computer and remote access is requested – hang up – even if they mention a well-known company such as Telstra. Telstra does not request credit card details over the phone to fix computer or telephone problems, and is not affiliated with any companies that do.
- Remember that you can still receive scam calls even if you have a private number or have listed your number on the Australian Government's Do Not Call Register. Scammers can obtain your number fraudulently.
- Make sure your computer is protected with regularly updated anti-virus and anti-spyware software, and a good firewall. Research first and only purchase software from a source that you know and trust.
- If you have fallen victim to a scam or you receive a lot of unsolicited emails and phone calls consider changing your email address and phone numbers.

Scam websites


You've been thinking about buying a new barbeque, then you see an ad on social media for a website that is selling brand-named barbeques for an amazing prize. You click on the link in the ad and it takes you to a website.

World of BBQ

1 <http://bigworldofbbqz.com/familybbq>

BIG WORLD OF BBQS LOG IN | MY ORDER | MY ACCOUNT | \$AUD ▼

Home Products Customer Info Search ...



Limited time only 2
0D 6H 1M 32SEC

Family BBQ
~~\$767~~ \$267 3

*pay by bank transfer for a further 10% off 4

ADD TO CART

- 1. It's not secure.** When online shopping, always look for the https (not http) and the padlock icon in the address bar to ensure there's a secure connection between you and the website. Don't rely on this alone, as some scam websites use https too.
- 2. It has a sense of urgency.** Scammers try to create a sense of urgency to encourage you to do something quickly. Don't rush — take the time to do your research and consider whether a website is real.
- 3. The deal is too good to be true.** The price might be enticing, but remember that scams often present offers that really are too good to be true.
- 4. It's using a non-secure payment method.** Think about how they're asking you to pay. Scammers often ask you to pay by non-secure payment methods such as wire, bank or international funds transfers, money orders, pre-loaded gift cards, and cryptocurrency like Bitcoin. These methods are difficult to track and it's rare to recover money sent this way. Always look for secure payment options such as PayPal or credit card.

Social Media Scams

Scammers set up fake profiles on social media, They pretend to be from the government, a real business, employer, investment firm, or even a friend, family member or romantic interest.

They may:

- use the same logo of the real organisation or photo of the person they are pretending to be
- impersonate famous people to 'recommend' goods or services
- create fake identities to befriend you and win your trust.



Scammers also set up accounts as sellers on popular online marketplaces such as Facebook; Gumtree; or eBay.

Protect yourself by using secure payment methods recommended by the marketplace or platform. Keep communications within the platform. Where it's available, check the person you are paying (payee) matches the account or PayPal you are paying. If not, don't pay. Many payments are now made instantly and it's unlikely you will get your money back.



PayID

PayID is a legitimate form of electronic payment introduced to overcome incorrect payments as well as reduce fraud — by showing the recipient's name to the person making the transaction. To set up a PayID, consumers can use their phone number, email address or ABN as a form of identification. The bank will verify the person owns this information, and then link the person's bank account to this unique identifier.

To transfer money using PayID, most online banking systems will ask for the PayID of the recipient. By simply typing in the phone number, email address or ABN, it will show the name of the intended recipient. If it is correct, the customer can authorise payment to be made. If the name shown is incorrect, the customer can easily cancel the transaction.

If you're advertising an item online, a scammer will make contact to purchase the item. They usually will not question the price, and they are unlikely to even want to view the item. In many cases, they will say a family member or friend will collect it from you. The offender will then urge you to accept payment through PayID. Once you've shared your PayID (usually phone number or email address) and the scammer has this information, a few things may happen.

The offender will say they have made the payment, but it cannot be processed because you don't have a suitable PayID account. You will be told you either need to "upgrade" the account and/or make an additional payment to release the funds. The offender will then say they have paid the extra amount required and ask you to reimburse the additional funds they have spent. If you do transfer any money, it will go straight to the scammer and be lost.

As part of this, offenders will create text messages and emails that appear to be from PayID, confirming payments or advising of problems. Scarily, such messages may even appear in an existing SMS thread with your bank. You may think they are genuine, but they are fake, designed to deceive you into transferring money to the offender.

There are several warning signs to look out for when selling goods online:

- PayID is a free service. There are no costs associated with using it, and therefore no fees will ever need to be paid
- PayID is administered through individual banks. PayID will never communicate directly with customers through texts, emails, or phone calls. Any correspondence which says it is "from PayID" is fake
- a genuine buyer will usually inspect and collect any goods. A buyer who says they will send a family member or friend to collect the item is a red flag, especially if they are unwilling to pay in cash.

Identify theft

Identify theft can be a result of any of the scams previously listed.

What scammers do with your personal information

With your personal information, scammers can:

- access and drain your bank account or open new bank accounts in your name and take out loans or lines of credit
- take out phone plans and other contracts
- purchase expensive goods in your name
- steal your superannuation or gain access to your government online services
- access your email to find more sensitive information or access your social media accounts and impersonate you to scam your family and friends

Signs that your identity has been compromised

- You are unable to log into your social media or email account, or your profile has been logged into from an unusual location.
- You notice that amounts of money go missing from your bank account without any explanation.
- You are refused a financial service or an application for a loan or your credit card has been declined.
- You receive bills, invoices or receipts addressed to you for goods or services you didn't purchase yourself.
- You are contacted by businesses or individuals who believe they have been dealing with you even though you have had no contact with them.



Protect yourself

Do not allow remote access.

01

This includes your computer, tablet, or phone. The scammer may ask you to install software that will allow them access to 'fix' something with your computer, which they will then use to access your Internet Banking.

Do not give anyone your Internet Banking or Mobile App password.

02

Bank Orange and other service providers such as financial institutions, Australian Government and telecommunications companies will not ask you for your login or password. If you wish to have a 'back up' for an additional person to have access to your account, contact Your Team Orange to set a family member up as an authorised account user, rather than sharing your login credentials.

Do not use your birthday or other common passwords

03

Try to avoid using common phrases such as 'password', your city, street or pets names. Use a combination of letters, numbers and special characters.

Do not click on unknown links

04

These can be sent by either text or email and may contain a virus. If you know the sender of the link, confirm with them that it is safe to open. If the link is from an unknown number or spam account, block the number from contacting you in the future.

Do not open unknown attachments

05

If you receive an unexpected invoice, photos or attachments from an unknown sender, it may contain a virus. Note that these scams often come from users that you do know. Do not forward these emails.



Local stories

In our local experience, many scams rely on customers being convinced to provide personal details or access to their bank accounts to scammers. You are the best protector of your personal information. Keep them safe at all times. Do not disclose security information to anyone, no matter what they say. The names have been changed in the following case studies for privacy.



Susie received an urgent call from Tim, who said he was from her telephone company's security department. Tim claimed he had detected a hacker who was sending her random advertising emails with a malware (a malicious computer program) that could be used to access all of Susie's personal details. Susie agreed to receive Tim's help and downloaded and installed a computer program that gave Tim access to her computer. Over a period of time, Tim scammed Susie out of more than \$90,000.



Mark was scammed out of \$8,000 on two separate occasions by a scammer who was impersonating a fraud investigations team at a well-known financial institution. The scammer convinced the man to withdraw cash in various large amounts over a period of a couple of months and deposit the money into a bank account. The man mistakenly believed he was being helpful and compliant but instead he was unknowingly depositing his cash straight into the bank account of a scammer. Unfortunately, as cash transactions were over the counter, the money will be more difficult to recover.

Reporting fraud

If you have experienced a scam or fraud, contact us immediately. Trust your instincts and if you receive any suspicious calls, emails or SMS messages or notice unusual activity on your account, it is important to let us know.



(02) 6362 4466

During branch opening hours

or

1300 705 750

Out of hours support

If you contact us as soon as you are aware of suspicious activity, we will be in a better position to secure your account, prevent further loss and try to recover your money.

We will do what we can to help, however in most cases we are unlikely to get your money back.

It is also important to report and fraud and scam activity including those you have prevented to the local Police and lodge an online report via the ACCC's Scamwatch Service at <https://www.scamwatch.gov.au/report-a-scam>.

Resources.

- Bank Orange Stay Safe - Resources, latest news and contact information.
<https://www.bankorange.com.au/stay-safe>
- Scamwatch – Provides information about how to recognise, avoid and report scams.
<https://www.scamwatch.gov.au/>
- ASIC – Australian Securities and Investment Commission (Report suspicious Business activity)
<https://asic.gov.au/>
- ACMA – Australian Communications and Media Authority. Report SPAM, unsolicited SMS
<https://www.acma.gov.au/>
- ACCC – Australian Competition and Consumer Commission .Report Scams, information on consumer awareness information.
<https://www.accc.gov.au/>
- Reportcyber - Reportcyber, Australian Cyber Security Centre
<https://www.cyber.gov.au/acsc/report>
- APRA – Australian Prudential Regulation Authority (Oversees conduct of participants of superannuation industry)
<https://www.apra.gov.au/>
- AFP - Australian Federal Police
<https://www.afp.gov.au/>
- AusTRAC – Australian Transaction Reports and Analysis Centre
<https://www.austrac.gov.au/>
- BDM - NSW Registry of Births, Deaths and Marriages (information on reducing identity theft)
<https://www.nsw.gov.au/births-deaths-marriages>
- IDCARE is Australia and New Zealand's national identity & cyber support service
<https://www.idcare.org/>





Orange Credit Union Limited T/A Bank Orange ABN 34 087 650 477 AFSL/Australian
Credit Licence 240768