Scam Prevention and Awareness Webinar – Transcript

Scam prevention and awareness session

Introduction

Speaker 1 - Christina

Welcome and thank you for joining our scam awareness and prevention virtual session.
I'm Christina, I'm here today with my colleague Sarah, and we're both fraud and scam education and awareness managers at *Bank of Melbourne. we are both passionate about scam prevention and helping our local community.*
We are here today to Increase your scam prevention knowledge and to empower you to avoid scams.
The more we know about scams, the warning signs, scammers tactics, and share this with family and friends, the better we will be able to help protect each other from the scammers and in turn reduce their impact on the community.
It is a conversation unfortunately that needs to continue indefinitely, as scammers are always looking for new and creative ways to steal our information and money.

"Before we begin today, I would like to acknowledge the traditional owners of the land on which we meet and pay my respects to elders both past, present and emerging.
I also acknowledge and pay respects to those here today who identify as being Aboriginal and Torres Strait Islander and recognise the diversity of Indigenous peoples, countries, and culture in Australia.
we acknowledge our role in supporting an inclusive and diverse nation where all of our cultural backgrounds are recognised and respected."

Australian Community Impact.

We hear a lot during these sessions and our discussions with the community that 'I won't fall for a scam', 'it won't happen to me' and 'I know how to spot a scam' and while some of these statements might be true for some, it is important to note that scammers are also very smart, convincing and are working on new ways to target us in the hope we will believe them.
With this in mind let's take a look at the impact of scams on everyday Australians.
Scammers are very clever and very active in our communities, if you have ever been impacted by a scam or know someone that has, you're not alone.
In 2020 Australians lost nearly $851 million dollars to a variety of scams and this number appears to be trending up and not down. With all scam types reporting increases in both the number of Australians targeted and the amount of financial loss.
It is also known that this number is significantly underestimated as it only includes scams that have been reported to Australian Government agencies.
The numbers do not include:
Those unaware that they are being scammed.
People who have been emotionally impacted and decided not to report.
People who are unaware of how, when or where to report scams.
Living in Australia, what does this mean for you?
It means that for every person impacted by a scam, they stand to lose on average $7677.
Some victims have lost less and some a lot more; amounts in the hundreds of thousands have been reported and in some cases millions. It not always just money that is lost it can be personal information that scammers use for their gain, for example applying for credit in your name.
Where do you think the money from scams is going?
You are right, not to anything good.
Stolen funds get broken up into various transactions or purchases by money mules, and could fund organised crime, individual criminals, or terrorist groups, in Australia or internationally.
the statistics you will see today, have been sourced from the ACCC and other Bank of Melbourne partners, including Scamwatch and IDCARE.

Definitions.

To get us started, it is important for us to understand the difference between a fraud and a scam.
A Fraud is when the customer did not authorise the transaction and/or method of loss. An example of fraud could be that your credit card is lost or stolen and then used by the fraudster.
The volume of fraud that runs through our banking platforms in comparison to legitimate transactions is minimal. However, the increasing number of customers who are tricked into sending money to criminals is concerning.
A Scam is when the customer willingly participated in the transaction but has been misled regarding the benefit or purpose. They can be more challenging to detect as they are disguised as genuine transactions.

Scammers will often gain your trust quickly and have you believing that the bank, your family, and friends are the ones to be wary of. They will coach you in what to say to the bank, in an attempt disguise the transactions as genuine, making it very challenging for us to help you and stop the financial loss before it happens. They will try to isolate you and tell you not to talk to your family and friends, because they know if you do, they might stop you from engaging with them.

Protection

At Bank of Melbourne we have support teams who are working around the clock to detect suspicious behaviour and keep you and your money safe.

We also have some very sophisticated technology supporting you. In fact, Bank of Melbourne fraud and scam detection is the best in the market.
We detect and confirm transactions against your unique spending patterns and alert you when something is not right. An example is where we may contact you to confirm a transaction is taking place that may be unusual based on your normal spending behaviour or send you a code to enter when you complete certain transactions, so we know it is really you. That is why it is vital not to share these codes with anyone else and that all your contact details are up to date with the bank.
If you believe you have been impacted by a scam it is vital you contact us immediately so we can attempt to recover any funds. Unfortunately, in most cases locating the money and recovery is very difficult as the money may have been moved offshore or taken out in cash. It is also worth noting the difference between a recovery and a refund.
A recovery is not a refund it is when we attempt to find the money you willingly authorised and transferred. It is a request that we send to the individual/scammer or their bank to return the money to you, if the money is gone it can be too late to recover.
Our branch employees are also there to help and protect you so please talk to them and raise any questions or concerns you have and be honest in your interactions with us, to help us determine what is happening.
In addition to technology and alerts we also help through education and awareness initiatives, like today's presentation, there is also lots of helpful information on our website.
Another key part of protection is partnering with government initiatives. Bank of Melbourne partners with several Government initiatives to increase scam awareness for all Australians. For example, the ACCC, law enforcement, IDCARE and many more.

Agenda.

In today's presentation we will cover:
The Types of Scams and how you may be targeted.
We will explore several types of scams via case studies, based on real life scenarios, this will help you identify the possible warning signs for different scam types.
We will direct you to the available resources that you can access for support and reporting.

Types of Scams.

Scammers have many techniques that they use to try and convince you into giving them your money and/or your personal information. They cast a wide net and hope to scam as many people as possible to maximise their gain.
Displayed is a list of the different scam types. We will explore some of the most common scams impacting our customers and communities.
Not all the scam types we cover today will be applicable to you. But as we go through each one, consider the other people in your life who may be more vulnerable to these scams and share what you learn and already know to help them.

Phone.

Currently the most popular method for scammers today is to target you via the phone.
More than half of all reported scams start via the phone. This could be a home, mobile or business phone number, even if you have a private number or are registered on the do not call list, unfortunately it does not stop scammers.
Usually, these calls are from someone pretending to be a reputable business/company that you are familiar with for example your bank, telco, internet provider, a company questioning transactions with you or even a government agency like the ATO.
During these calls they may ask you for personal information, demand you pay money or in some cases they will state they are going to pay you money in the form of a refund or deposit for your help in return.
When receiving calls listen out for the potential warning signs that it could be a scam call:
Someone is applying pressure for you to do something immediately, for example pay a bill or transfer money.
There is a treat or penalty for not completing their actions, for example arrest or prosecution.
You are asked to download software on your computer or mobile device.
Or log into online banking whilst on the call
Remember Never follow instructions from an unsolicited caller, always validate requests by calling the genuine company on their publicly listed number, do not call back using the number provided by the unsolicited caller.
Always take the time to pause and consider if the call is genuine and would this company/provider contact me to request this type of action. You might even take the time to check with a family member, a friend, or the bank if you have concerns.

Remote Access Scam Case study.

A phone scam that is increasing at an alarming rate is one we call a remote access scam. It is called this as it involves you giving another party access to your computer or mobile device remotely, by downloading software. Let us look at an example.
Dani received a call from someone pretending to be a representative from her phone company, it is a company she was familiar with.
The caller advised that they needed her help to catch a fraudster and was directed not to tell anyone, including her bank as it would jeopardise the investigation.
Dani was then instructed to download software; She followed the instructions and accepted all screen prompts that were presented. Not understanding this was giving the caller full access to her computer.
Dani was asked to log onto online banking and confirm her account number to receive a deposit.
The caller then asked Dani to check her balance had increased by $10,000 from a deposit the caller had placed in her account. The screen disappeared and reappeared, and the caller advised they were hot on the path to the fraudster.
The caller requested the $10,000 deposit be withdrawn in cash and returned to the internet provider via a wire transfer.

The software that Dani had installed on her computer is a form of 'remote access software'. This allowed the Scammer to take full control of her computer, including viewing her browser when she signed into Online Banking.
The scammer then performed a funds transfer from her available credit card balance into her everyday transaction account. This made it look like she had received additional money via a deposit when the money was actually her own. She then withdrew the cash and sent it to the scammers.
This type of scam has many variations, although a number of things remain consistent:
They start with contact usually via the phone, where the caller is someone pretending to be from a reputable company and or a company you are familiar with.
You are asked to download software (to access your computer).
It may look like you receive a deposit of money or a larger than expected refund and be instructed to transfer it back via online banking or a different method.
Remember in these cases the money is your money, not the scammers.
The caller may become aggressive if you do not comply with their requests or ask that you remain on the phone when you attend the bank so they can instruct you what to do and say.
You maybe prompted to call a reputable company from a popup message to help with technical support – please note tech companies like Microsoft advise they do not include numbers for you to call via a popup message.
Common ways to spot this type of scam.
You receive an unsolicited call from someone pretending to be from a reputable company.
A scammer may tell you not to tell anyone or they may coach you on what to say to the bank.
On the call you might be asked or instructed to download software or application like Team viewer, anydesk to allow remote access to your computer or device.
You are asked to pay money via an unusual payment method – money transfer agent, gift cards, crypto currency, cash rather than online banking.
Caller is aggressive, pushy, or demanding.
You receive a popup with a contact number for tech support.
To protect yourself from Remote access scams
Do not download software that allows others to control your devices or follow instructions from an unsolicited call.
Confirm all instructions prior to completing any actions with the company directly. Ensure you use contact information that is publicly sourced via the phone book not what is provided by the caller.
Be aware of the caller's behaviour, consider would this company or organisation ask me to do this.

Hang up at any point that the behaviour is not quite right and speak to trusted friends and family for a second opinion before you take any action.
Remember Never disclosure your security codes, like your Bank of Melbourne SMS code for online banking transactions to anyone. This is how we keep you safe and know it is you completing the transaction. It is ok to hang up and seek help.
Someone who has remote access to your computer or device has access to everything, can see everything and they can also download other types of Malicious software.
If you suspect this has happened to you turn off your computer or device. Do not use this device until it has been professional cleaned by a reputable technician and contact your bank immediately.

Threat and Penalty – Case Study.

Another common phone scam is a threat and penalty scam, Let's look at a case study involving this type of scam:
Jane received a call from someone pretending to be from the Australian Taxation Office.
She was told she had a tax debt and if she did not pay it immediately, she would be arrested and go to jail.
Jane was instructed to purchase iTunes gift cards to pay the debt.
The caller was very persistent, and the threat sounded legitimate. Jane did not want to be arrested and was scared, so she followed the caller's instructions and paid the money.

To spot this type of scam again be very cautious of unsolicited calls in which the caller requires urgent action, also any payment requests in crypto currency, gift cards or any other unusual payment method should be considered suspicious.
Scammers may also request remote access to your device to help you complete these types of payments.
To protect yourself from threat and penalty scams
Be cautious of calls from unknown numbers, private or international numbers that hang up before you can answer the call. Do not call back just ignore them.
Hang up the phone and call the company directly using the contact information in the phone book or listed on their website. Do not use the number provided by the caller.
Don't be pressured by a caller, always stop, think and check whether the story sounds genuine. Use your instincts if it doesn't feel right or is unexpected, it is ok to hang up.
Be wary of requests to pay via unusual payment methods like gift cards, crypto currency or via overseas transfers.
I will now hand over to Sarah to talk to us about more scam types.

Speaker 2 - Sarah

Online.

We have looked at the types of Scams you may receive via the phone; now let's consider some scams online or computer scams.
Online Scams are the second most successful way scammers target you, with more than 30% of all scams occurring online via email, internet or social networks.
Online scams can present in so many ways as you can see on the screen.
We will look at some of the more common online scams starting with a phishing email.

Phishing – Case Study.

Here's an example of a phishing email (spelt ph), in this example criminals pretended to be from Bank of Melbourne using a similar marketing template to make their request seem more legitimate, we have highlighted a couple of the tips to help spot this type of scam.
You can see it asks the user to click on the link to reactivate or verify their account.
There are no salutations, and there is a sense of urgency to complete the action.
We will never ask you to confirm transactions, personal details or unlock your banking via a link sent through an email or SMS text message, nor will we ever send you a link that goes directly to sign into internet banking.
If you receive an email with a link and you are unsure if it is genuine, you can hover your mouse over the link without clinking on it to display the web address or URL this will take you to.
The example on screen is not a genuine Bank of Melbourne link and it is hard to identify where it would take you, therefore it is best not to click the link.
If you are unsure, please contact Bank of Melbourne or your bank directly and ask about the email.
Bank of Melbourne related emails that look like this should be sent to hoax@Bank of Melbourne.com.au, do not open any links and delete the email or SMS text message immediately after you have forwarded it.
If you do ever click on a suspicious link and you are unsure, please turn off your computer and contact your bank immediately.

False Billing.

False billing is another way a scammer may attempt to get your money or personal information.
Like the previous example, false billing is when scammers pretend to be from organisations and use the organisations templates to convince you it is a legitimate bill or invoice. In some instances, malicious software may be installed on your device by clicking a link or opening an attachment.
Another slightly different version is a sophisticated scam called a Business Email Compromise or a BEC scam. In these scenarios' payment details are modified to the scammers account details and added to bills, invoices, or other payment requests usually for large payments like a house deposit or large business purchase.

To spot this type of scam, consider if.

You have accounts with this provider,
Have the payment details changed from previous bills?
Is this a once off large payment?
Did the payment instructions come from an email?

To protect yourself against false billing and BEC scams:

Always confirm all new or changed account details verbally with the provider directly. Do not use the contact information in the email or invoice as the email account may have been compromised by a scammer.
Use official online websites and apps to make payments or contact the provider directly on a trusted number.
Ensure you have up to date security software and encrypt or password protect confidential emails.

Investment Scam – Case Study.

Another common online scam we will explore is investment scams, In the last 3 years Australians lost the most money to this scam. Let's talk through this example.
Steve is a 65-year-old retiree, he received an unexpected call about an investment opportunity.
The caller sounded very professional and knowledgeable on investment matters. They answered all of Steve's questions and followed up with a call from a 'senior advisor'.
Steve decided to explore this new investment opportunity and
over the next 12 months, Steve made several transfers starting with $10k.
He was referred to a very professional looking website and set up an online account, which showed his money increasing in value. He was even at times able to withdraw some money which increased his confidence that the investment was genuine, he invested more money, to a total of $200 000.
Steve only realised this was a scam when he had no more money to invest and the website went offline, and he could no longer access his account or contact the offshore group by phone.
Steve discovered the company was a fake and not registered with the Australian Securities Investment Commission (ASIC). He was too embarrassed to tell anyone or report it to police. Sadly, none of Steve's money was recovered.
Some ways you can spot an investment scam:
You receive unsolicited contact via social media, online advertisement, phone, or email.
A promise of high returns on investments over a short period of time.
Pressure and intimidation to make financial decisions on the spot and invest right away.
The opportunity is backed by a fake celebrity endorsement.
Investment's opportunities in crypto currency where a broker or company takes control of the investing for you.
Your money is going overseas, or transfers made payable to accounts in different names for the same investment.
You are told not to tell anyone or coached on what to say to the bank.
You offered training and assistance with your investment through providing remote access to your device.
To protect yourself from Investment scams consider
does it seem too good to be true, it probably is! Be suspicious of investment opportunities that promise a high return with little or no risk.
Do not give your personal or financial details to unsolicited callers or reply to emails, SMS or advertisements offering financial advice or investment opportunities.
Always contact the company or organisation directly using a trusted phone number, not what is provided via an email, advertisement, or popup message.
Always do thorough research on apps, investment companies or advisors. Any business or person that offers or advises you about financial products must hold an Australian Financial Services licence.
Check if a financial advisor is registered via the ASIC website.
You can find out more via www.moneysmart.gov.au
Do not let anyone pressure you into making decisions about your money always seek a trusted second opinion from a licenced professional.
Install and keep security software up to date on all devices. Do not open or use any links in suspicious emails, texts, or pop-up windows.
Remember if its sounds too good to be true it probably is!

Romance Scam – Case Study.

Another prevalent online scam is romance scams.
Romance and relationships scams are heart breaking, each year they cost Australian's millions of dollars. Let's explore an example now.
Mr Smith met Maureen online - she lives overseas.
Although they never met face to face, within 4 months they were engaged.
Maureen indicated she was involved in a serious accident and needed money for her medical bills.
Mr Smith completed 10 transfers totalling $320k.
Once Maureen knew she had taken all of Mr Smith's life savings she ceased all contact with him.
Mr Smith realised something did not feel right once Maureen ceased contact.
He spoke to his bank to get his money back, but Maureen had already withdrawn all the money and it could not be recovered.
It's always important to consider that a romantic connection formed online could be a scam, even if you speak to them on the phone all the time.
Some ways you can spot a romance scam:
The scammers are quick to change "chat" platforms from a Dating site to social media or whatsapp. This is to avoid you being suspicious of their false profiles and to stop you from reporting them.
You have never met in person; and they provide excuses as to why you cannot video chat.
They confess love quickly and propose before meeting.
They ask for money with an elaborate story – an accident, family issues or are stuck in another country.
These scammers isolate you from your family and friends with extremely frequent contact, they build trust and explain that no one will understand your connection.
To protect yourself from relationship scams:
Do not send money or provide your personal details to someone you have only interacted with online or via the phone.
Be cautious of unknown "friends" when using the internet and online services. Not everyone is who they say they are online.
Be vigilant about what you share. Also be aware of friends that may have had their social media account compromised, the scammer will set up a duplicate profile and start chatting to you, you will think it is your friend when it is a scammer.
Do an online search of your admirer to see if they are who they say they are. Often you will discover the same photo used with name variations attached to multiple profiles.
Watch out for admirers who wish to contact you outside of the dating/social media website after just a few contacts.
Romance and friendship scams can happen to anyone, especially at times when you may feel lonely or vulnerable, it's important to try and remove emotion from your decision making when money is involved, no matter how caring or persistent your new partner is, remember they do this for a living.
If you ever have any doubts, turn off your phone or your computer and give yourself some time to consider your situation. Talk to a friend or family member.

At your door.

Scammers have moved on from traditional door to door scams, targeting us using technology, though some may happen at your front door.
Here are some examples of how you may be targeted at your door:
You could have a scammer impersonating a charity or tradesperson.
You could receive lottery or scratchie in your letter box, stating you have won money or a holiday.
You could have your mail taken from your letter box and then your identity stolen.
Scammers may even collect money from you in person, often in conjunction with another scam type.
Be very cautious of people who come to your door. There is an increase in impersonation scams, and they can be quite sophisticated. For example, getting a call from someone pretending to be from the bank saying your card has been compromised and sending people dressed in a bank uniform to pick up your card and PIN from your home or acting as a courier to collect gift cards or cash.
Please be safe, do not let anyone into your home that you do not know and never give your cards and PINS to anyone to take away.

Scam Warning Signs.

Throughout the scenarios you have heard today you may have noticed some of the warning signs.
We want you to feel confident and have the knowledge that if you see or hear any of these warning signs you will cease communication and report it right away.
The warning signs are:
You are asked to share your passwords, security code or SMS code with anyone including family and friends.
If an offer claims to be a win win, you cannot lose or has no risk or seems too good to be true.
You receive unsolicited contact via phone email or SMS text, popup message with pressure or intimidation to complete an action on the spot.
Your personal information is requested.
You are instructed to pay or transfer money for an out of the blue request.
The contact persons details are vague / confusing / or lack of return contact details.
You are told not to tell anyone or coached in what to say if asked.
Your gut instincts suggest something doesn't feel right.
If in doubt, hang up the phone, delete the emails, shut the door, and bin the letter.
If you believe you or someone you know may have been impacted by a scam, it's important you advise your bank, report it and talk about it.
It could be your insight and conversation that stops you or someone you know losing money.

Protect Yourself.

I think after today it's clear we can all be impacted by scams and want to stop the scammers, time to consider the following tips to help protect yourself and others from scams:
Consider Is the request genuine? Always research who you are dealing with and/or get a trusted second opinion. – take the time to consider, research and talk about requests before you act. Urgency is a tactic used by scammers to trick you into doing what they want.
Ask yourself questions:
Is the company registered with ASIC as a registered business?
Would they contact me in this way about this topic?
Does this sound right? Is it too good to be true?
Wouldn't everyone one be investing and be wealthy if this deal was real?
Contact providers directly using a publicly listed phone number to check if the offer or request is genuine
Google image search photos of potential new friendships.
Keep Security software up to date on all devices. Do not open suspicious texts pop-up windows or emails - delete – always delete them! Don't use contact information within suspicious emails or pop ups and don't click on links they may contain.
Keep your personal/business details secure includes passwords and security codes, put a lock on your mailbox, and shred to destroy any old bills, letters or documents containing your personal information. Never share your passwords and security codes with anyone; these are the banks way of protecting you and your money.
Limit information you share on social media like birth dates, maiden names and don't complete those get to know you quizzes. Scammers use socials to get information about you to personalise scam attempts and even hack your passwords.
Use unique passwords for all online accounts and change frequently –have complex and unique passwords for every service you use – especially your online banking and email accounts, please don't share any of these details with anyone including loved ones. If available turn on and use multifactor authentication to prevent unorthorised access.
Beware of requests for your details and or money; this includes unusual payments and deposits You should be on high alert if you are requested to make any payments via an unusual method like a wire transfer, pre-loaded credit card, iTunes gift cards or digital currency bitcoin, these are nearly always a scam. Only provide your account details to those you trust, and do not agree to transfer money or goods on behalf of someone else.
Be open with the bank regarding your transactions. The bank needs all the information to protect you and your money
scammers often provide instructions and coach you on what to say to the bank so we're not suspicious of the scam. For example, you're told to tell the bank it's for another purpose such as renovations or car purchases, talk to your bank and please be honest - we're here to help keep you safe.
Regularly visit your banks' security page. Scams are always evolving, staying up to date helps you avoid being impacted by new scams.
Never give a stranger or unsolicited caller remote access to your computer or device Providing anyone with remote access to your device is like giving them your front door keys and alarm codes, allowing them to access everything, including your money and personal information. Australians lost 8.4 million to this scam alone in 2020, Remote access scams is one of the highest reported scams impacting Australians today.

Help and Support.

We have spoken about lots of different types of scams, but where can you go for help and support if you have been impacted?

We recommend speaking to someone from your bank or a trusted family member or friend.
Check out our handy be safe and secure guide available from our website.
Bank of Melbourne have partnered with IDCARE who are an Australian not for profit organisation. They offer a range of support services for those impacted by scams, including helping you re-establish your identity after it has been stolen.

There are also several counselling services available: for example, Lifeline, Beyond Blue and Financial Counselling Australia.
Remember scammer will try to isolate you from your support network and tell you not to share what you are doing with anyone.
Please continue to talk about different scams so that others know they exist, have open conversations with family and friends about any unusual calls emails or new relationships and listen out for scam warning signs.

Reporting.

As we mentioned earlier, we know many people impacted by scams do not report them and the numbers of Australians impacted is underestimated.
If you get caught up in what you think is a scam, been targeted or approached by a scammer, always contact your bank, and report it. You can also report scams to Scamwatch or the Australian Cyber Security Centre (if it is a cybercrime)
These reported cybercrimes filter back into law enforcement and help our government keep track of the impact of these crimes on our communities.
There are additional places you could use to report scams, depending on the type of scam.
Sometimes the organisation that is being impersonated may like to know, so they can help stop the scammers too.

Stay Safe.

Thank you joining us to learn more about scam prevention.
Please start a conversation with your family and friends about what you have learnt about scams.
The information you share with a loved one or friend could stop them falling for a scam in the future.
If you are ever unsure, please talk to us.
For more information about scams visit the Bank of Melbourne security pages
Thank you.