MONEY SMART FOR SENIORS

Australian Multicultural Community Services

AMCS acknowledges financial support from the Ian Rollo Currie Estate Foundation and Perpetual Trustees.

Content

Acknowledgments

Money Smart for Seniors is an initiative of AMCS.

Resources have been co-developed by AMCS and our community members with inputs from eSafety Seniors, Goldsmiths Pty Ltd and House Studios.

AMCS acknowledges financial support from the Ian Rollo Currie Estate Foundation and Perpetual Trustees.

Disclaimer

Our first step in developing these resources was to ask community members about their experience of financial attacks and what they thought would be of most help. Money Smart for Seniors aims to answer their most common questions. However, our little program cannot be the total answer to all threats. We can only hope it is a step in the right direction for our community members.

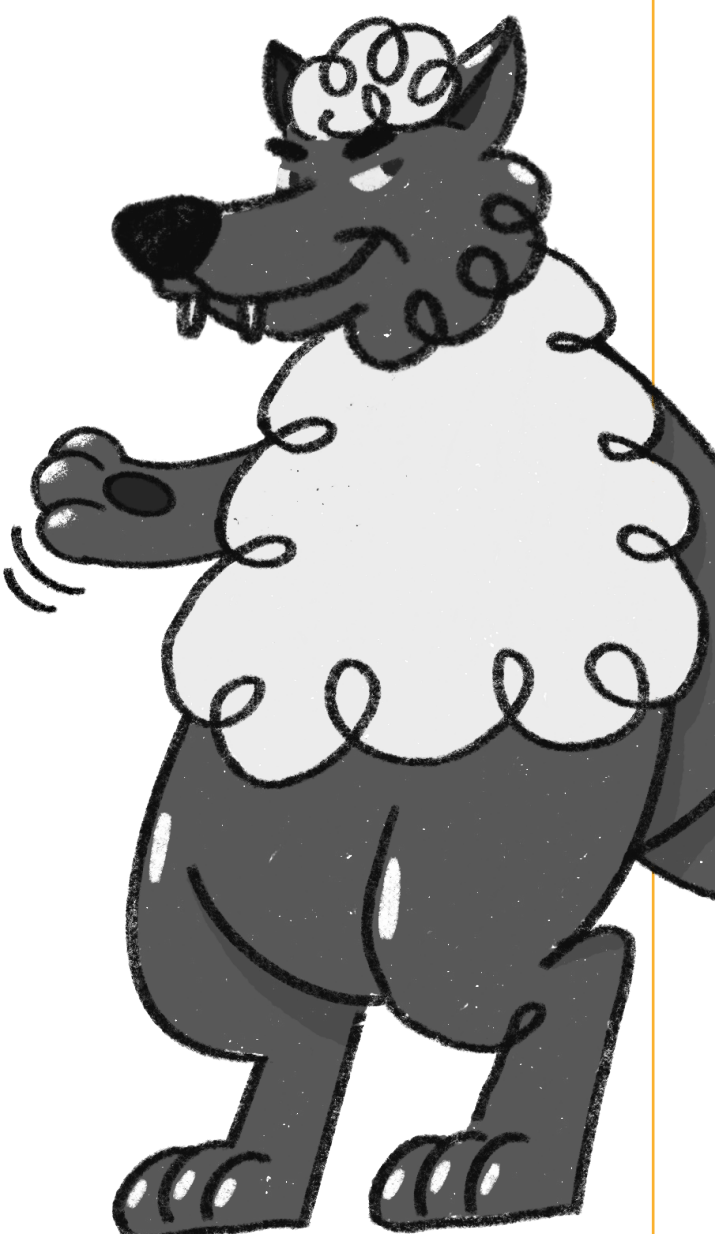
Welcome

The **'Money Smart for Seniors: Toolkit'** provides links to trusted sources of information and education to help you protect yourself from scams, fraud and elder abuse.

Attacks on finances can happen to anyone. The methods used are constantly changing and we all need to stay up to date, be alert and take protective action.

In this Toolkit we provide links to trusted sources of information for you to learn about what you can do to protect yourself.

Scamwatch video
Scan QR code or Click on code to watch video!



Someone who wants to attack your money may try to trick you by pretending to help you or to be a person you can trust, or even love.

In the traditional story, the wolf disguises himself as a sheep so he can hide among the other sheep and get close enough to kill for his next meal.

This is what people attacking you with scams, fraud or elder abuse do. They pretend to be kind and trustworthy so you will not suspect them.

Money Smart Seniors stand up for their rights and repel attacks on their money. Just as the tiger is strong enough to win against the wolf, Money Smart Seniors have strengths they can use to defeat financial attacks.

Keep reading to learn more about your tiger strengths. Follow the links to explore:

1. **Security** – protect your information and accounts
2. **Savvy** – be suspicious and spot possible attacks
3. **Say 'No'** – do not engage with suspect or unverified approaches
4. **Step away** – if something doesn't feel right, stop, even if you have started a conversation
5. **Share wisely** – keep your information private so it cannot be misused.

Security

Protect your information and accounts

You do not leave the keys to your home lying around!

You need to be just as careful with the keys to your personal information and money.

Use phone and computer security

Keep all your devices – phone, computer, tablet – as secure as possible against attack.

Here are some suggestions to try:

- Firewall, virus scan, anti-spyware
- Enable auto-updates
- Automatic time-out screen locks and password protected screensavers
- Automatic logout for multiple login attempt fails.

Strong passwords

- Passphrases are the more secure version of passwords and are made up of four or more random words. Use a different passphrase for each account and do not recycle parts of any old ones. Your passphrase should be:
  - › Long – at least 14 characters
  - › Unpredictable – use four or more random words with numbers, symbols, and upper and lowercase letters
  - › Unique – don't reuse your passphrases
  - › You can check the strength of a password using the NSW Government's password strength tester at:

Test your password
Scan QR code or Click on code to check your password

- Use a password manager to give you a specific and 'hard to break' password for each account or website you need to access.

Managing passwords
Scan QR code to watch video!

Multi-factor authentication

Where available, switch on multi-factor authentication for your accounts. Multi-factor authentication (also known as 2-step authentication) adds an extra layer of security. This means that when you log into an account with your password, you will be asked to complete an extra step to confirm that it's really you doing this – like enter a code from a text message or use face recognition identification.

Multi-factor authentication
Scan QR code to read more!

Use a secure connection

Public WiFi is often available in public spaces, for example, the street, a café, hotel, library, airport or train. Do not use Public WiFi to access important accounts, send sensitive information or enter passwords. Stay secure by using a trusted internet connection (for example, at home or at work) or by using your own mobile data (directly or via hotspot).

Privacy when online
Scan QR code to read more!

Learn more

Advanced online security
Scan QR code to watch video!

Savvy

Be suspicious and spot possible attacks

Always stop and think – could this be a wolf?

Watch out for scams

Scammers pretend to be from organisations you know and trust like businesses you deal with, or government agencies, to try and get you to reveal important personal and financial information. They may contact you via a phone call, email, text, or through social media. Scammers will use your personal details to steal your money or commit another crime.

Some common warning signs are:

- You get an unexpected email, text, phone call or social media message
- There's a deadline or sense of urgency, demanding a payment or asking you to confirm personal details
- Links that do not look genuine, such as having an unusual website link or the sender's email address doesn't look right
- There's a promise of financial benefit or a threat of fines, debts or jail.

Stop – don't give money or personal information to anyone if unsure. Scammers often ask you to verify who you are or ask you to make a payment. Never log into your online accounts or verify details via a link in a message or click on links or open attachments in emails from unknown senders or that are suspicious.

Think – ask yourself could the message or call be fake? Beware of unexpected calls, messages and emails. Delete or hang up. Contact the organisation directly by looking up their official website and phone number.

Protect – act quickly if something feels wrong. Contact your bank if you notice some unusual activity or if a scammer gets your money or information.

To keep up to date with the latest scams to avoid, subscribe to Scamwatch email alerts.

You may also like to read the 'Little Book of Scams' available in English and a number of other languages.

Avoiding scams
Scan QR code to read more!

Little Book of Scams
Scan QR code to read more!

Shop securely online

When shopping online, make sure you use trusted sellers and look up customer reviews. Before entering your personal information, check that the website uses 'https' at the beginning of its domain name or has a security icon, usually a small, locked padlock on its browser to indicate it is a more secure website. When making a purchase, use a secure payment method such as PayPal, BPAY or your credit card.

Shopping online
Scan QR code to read more!

Be alert to elder abuse

Financial abuse includes using someone's property, finance or other assets illegally or wrongly. Abusers may borrow money and not repay it; use the older person's accounts, credit cards, online banking or digital passwords without permission; apply pressure to hand over personal property like jewellery; or misuse an Enduring Power of Attorney.

Your financial wellbeing is important to your life. You have a right to feel safe and to make your own decisions – including about money.

- If someone tells you they need you to give them money, and you don't think it is a good idea – you don't have to do it
- And if someone takes money from you – you can stop that from happening again
- And if someone says you cannot see your grandchildren unless you sign some documents – you can find another way to work things through
- It is possible to take back your own choices and your dignity, without losing the support and love of those around you.

AMCS Money Talks
Scan QR code to read more!

Help is available

Seniors Rights Victoria	1300 368 821
National Debt Helpline	1800 007 007
1800 ELDERHelp	1800 353 374

If you are concerned for your immediate safety or that of someone else call 000

Say ‘No’

Do not engage with suspect or unverified approaches

Ask yourself “Did I start this conversation?”

If contact has been made with you by email, text, phone or social media message then you must assume it could be a scam.

- Do not engage or respond
- Do not click links
- Do not download apps
- Do not provide personal details
- Do not read out verification codes.

You don’t have to be rude, but you must be firm. You have a right to keep your finances and personal information secure.

It is simple. Just say a firm ‘No’.

If you think it may be a genuine question, you can take the time you need to check.

Contact the organisation directly either in-person, or by looking up their official website or phone number. They will know if they have tried to contact you and will be able to let you know what it’s about.

Learn more

All about scams
Scan QR code to read more!

Step Away

If something doesn't feel right, stop, even if you have started a conversation

Whether speaking with someone you think you know, or with a stranger, you may start to feel uncomfortable about the conversation. Something is not quite right. Maybe you have grown to trust, or even love, this person.

- They may be starting to ask about money – little questions – they may need a little help from you.
- They may be suggesting a better way for you to invest your money, to get a better interest rate or save on tax.
- They may be trying to help you protect your money – perhaps they suggest your bank account has been compromised and you need to move your money.

You must stop and step away.

Scammers can spend months or even years cultivating a relationship with you. After all that time it is natural to feel committed to the interaction and find it hard to draw the line. But you must.

Have you met this person in real life? How do you know they are who they say they are? Could this be a wolf?

It can be very hard to step away from these situations. If you are facing a wolf, they have invested a lot of time in their attack and will not give up easily. If you can, ask a trusted person to support you.

You can also get confidential support and advice from:

IDCare

Scan QR code
to visit website!

Lifeline

Scan QR code
to visit website!

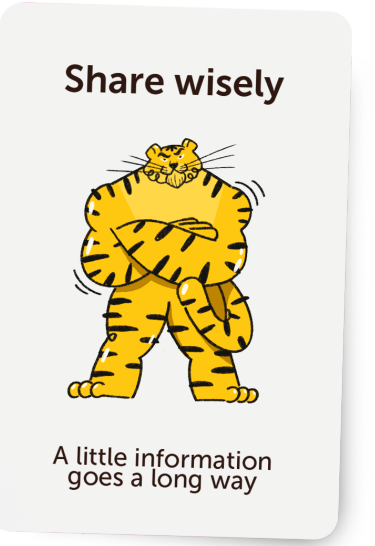
Learn more

Scan QR code
to watch video!

Share Wisely

Keep your information private so it cannot be misused

Someone can use your personal information to gain advantage – either by accessing your money directly, or by taking on debts in your name, for example.



Be careful about what you share publicly

Have you checked your social media settings? Can anyone see your Facebook pages? Is your birthday visible? Your address?

Identity theft
Scan QR code to read more!

Do your banking yourself

As more and more services go online, it is too easy to ask someone else to help you. But once you have shared your PIN or password, or someone has set it up for you, they now have access to all your money. Even the closest, most trustworthy people in your life can be tempted. Perhaps they hit a difficult time and think they can borrow from you, or perhaps it is more than that.

It is important that you keep control of your money and make your own decisions about it. You can:

- Learn about online banking
- Attend the bank in person
- Use the National Relay Service (NRS)
- Translating and Interpreting Service (TIS).

Practise online banking
Scan QR code to read more!

Introducing online banking
Scan QR code to read more!

National Relay Service
Scan QR code to read more!

Translating and Interpreting Service
Scan QR code to read more!

Watch out for data breaches

A data breach occurs when personal information held by an organisation is accessed or disclosed without authorisation, or is lost. Many organisations and government agencies have a legal responsibility to tell you if your personal information is involved in a data breach that is likely to cause you serious harm.

If your information is involved in a data breach, make sure you act quickly and get advice provided by the Office of the Australian Information Commissioner. The action you take depends on the information involved. Keep a record of what you do. You can also get free support and advice from IDCare.

To find out if a site or app you use has had a data breach you can check services such as haveibeenpwned.com. If this has happened, change your passwords straight away.

Australian Information Commissioner
Scan QR code to read more!

IDCare Help
Scan QR code to read more!

Has my email been compromised?
Scan QR code to read more!

Protect

If you think you are the victim of a scam, don't be embarrassed and don't keep it to yourself. There are steps you can take to fix the problem:

- Contact your bank or financial institution immediately to stop any further payments to the scammer
- If you have experienced cybercrime and lost money online, you can report it to the police via ReportCyber.
- If you are concerned that your personal information has been exposed and misused, contact Australia's National Identity and Cyber Support Service IDCare.
- Report the scam to the National Anti-Scam Centre via the scamwatch.gov.au/report-a-scam page. This helps to warn people about current scams, monitor trends and disrupt scams where possible.
- Spread the word to your friends and family to protect them.

ReportCyber
Scan QR code to read more!

IDCare
Scan QR code to read more!

Report a Scam to Scamwatch
Scan QR code to read more!

Extra Learning

Please explore any of the following trusted or government websites to learn more.

Australian Signals Directorate

Scan QR code to read more!

Scamwatch

Scan QR code to watch video!

eSafety Commissioner

Scan QR code to watch video!

IDCare

Scan QR code to watch video!

Australian Multicultural
Community Services

Enquiries:
Australian Multicultural Community Services Ltd.
info@amcservices.org.au
(03) 9689 9170

MONEY SMART FOR SENIORS | TOOLKIT
Version 6.1, August 2025