Tech Savvy Seniors

Module 6

# Stay safe online and avoid scams

Session plan

# Table of contents


Session overview ..... 3

Learning architecture ..... 3

Learning outcomes ..... 3

Resources checklist ..... 4

Session summary ..... 5

Session plan ..... 6

1. Welcome (10 min) ..... 6

2. What are scams and why do they matter? (10 min) ..... 8

3. Common scams (20 min) ..... 10

4. Spotting warning signs (20 min) ..... 12

5. Prevention: Passwords, devices, privacy & habits (20 min) ..... 14

6. What to do if you're targeted (10 min) ..... 17

7. Built in flexibility (20 min) ..... 18

8. Wrap up (20 min) ..... 19

# Session overview

This 2–2.5-hour session is all about introducing older Australians to common online and phone-based scams and empowers them to protect their personal information. Learners explore different types of scams, how to spot red flags, and what to do if they're targeted.

The session builds on digital confidence while promoting safe habits.

## Learning architecture

This module forms part of a 12-module series.


## Learning outcomes

At the end of this session, learners will be able to:

1. Describe common types of online and phone scams.
2. Identify scam red flags in email, SMS, phone calls and websites.
3. Take steps to protect personal information.
4. Know how to block, delete, or report a suspected scam.
5. Understand where to go for help and support.

## Resources checklist

| This session requires the following resources: | |
|---|---|
| ☐ | Session plan (this document) |
| ☐ | PowerPoint presentation |
| ☐ | Learning Canvas - printed (one per learner) |
| ☐ | Pens for learners (one per learner) |
| ☐ | Butchers paper/markers or a whiteboard/markers may be useful to assist with capturing 'learning goals' which will be touched on throughout the session |
| ☐ | Library's Wi-Fi password |
| ☐ | Tech Savvy Seniors program schedule - printed (one per learner) |
| ☐ | Learners' own device (smartphone, tablet or computer) |
| ☐ | Internet-connected smartphones, tablets or computers (as available) |
| ☐ | Facilitator's computer for PowerPoint presentation and demonstrations |
| ☐ | Projector and screen (optional) |
| ☐ | Scan message examples, printed (if not using the PowerPoint presentation) |

# Session summary

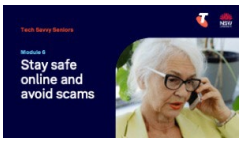
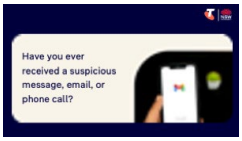
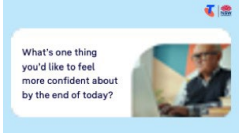
This session summary provides an overview of topics, the activities relevant to each topic and the duration.

| Duration | Topic | Useful links |
|---|---|---|
| 10 min | 1. Welcome | |
| 10 min | 2. What are scams and why do they matter? | |
| 20 min | 3. Common scams | |
| **10 min** | **Break** | |
| 20 min | 4. Spotting warning signs | • Scamwatch's Stop, Check, Protect method<br>• Complete one of BeConnected's short courses<br>• Complete ScamWatch's quiz (scroll down home page and select 'Start the quiz')<br>• Watch the video on NSW Government's website (scroll down page) |
| 20 min | 5. Prevention: Passwords, devices, privacy & habits | • Watch the 'Passwords and passphrases' video on NSW Government's website (scroll down page) |
| 10 min | 6. What to do if you're targeted | |
| **10 min** | **Break** | |
| 20 min | 7. Built in flexibility | |
| 20 min | 8. Wrap up | • iPhone: Scan a QR code with your iPhone or iPad<br>• Android: How do you scan QR codes on Android? |
| **Total duration: 2.5 hours** | | |

# Session plan

## 1.Welcome (10 min)

| Overview |
|---|
| **Purpose:**<br>• Introduce Module 6: Stay safe online and avoid scams, including the flow (discussion and reflection focus)<br>• Set a safe, calm tone; reduce anxiety about 'pressing the wrong thing'<br>• Introduce the Learning Canvas as a personal guide they can use during the session and take home<br>• Gather learner goals to tailor the 'Built-in flexibility' section later |

| Timing breakdown | Content |
|---|---|
| **Session overview**<br>10 min<br>  <br><br>  <br><br>  <br><br>  <br><br>  <br> | On arrival, ensure each learner has a device, printed Learning Canvas and pen. Group learners by device so they can support each other.<br>**Deliver:** An Acknowledgement of Country.<br>**Say:**<br>• Welcome! Today is all about staying safe online and protecting yourself from scams. We'll explore different ways scammers try to trick people through emails, text messages, phone calls, and fake websites.<br>• You don't need to be an expert to stay safe — we'll focus on practical steps you can take on your phone or computer to avoid falling for common traps.<br>• By the end of this session, you'll be able to:<br>  • Describe common types of online and phone scams.<br>  • Identify scam red flags in email, SMS, phone calls and websites.<br>  • Take steps to protect personal information.<br>  • Block, delete, or report a suspected scam.<br>  • Understand where to go for help and support.<br>**Introduce Learning Canvas:**<br>• Use your printed Learning Canvas to write notes in your own words, tick off skills as you learn them, and highlight what feels most useful to you. Writing things down helps you remember and understand them better, and makes it easier to recall later. Take your Canvas home to keep practising. On the back, you'll find extra tips and trusted links if you want to explore more.<br>**Ask:**<br>• Have you ever received a suspicious message, email, or phone call?<br>• What did you do — or what would you do — if you weren't sure?<br>• What's one thing you'd like to feel more confident about by the end of today?<br>(Write answers on a whiteboard or butchers paper. These will help shape the **'Built-in Flexibility'** section later in the session.)<br>**Confirm** everyone has a device; pair anyone without.<br>**Transition:** |

| | |
|---|---|
| | • Scams are becoming more common and more convincing, so you're not alone if you've ever felt unsure. Today we'll learn how to pause, check, and stay in control. |

# 2. What are scams and why do they matter ? (10 min)

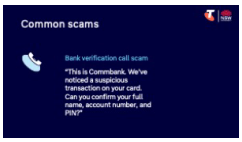
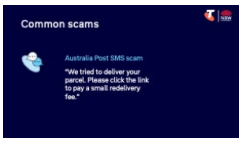
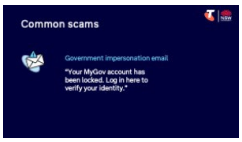
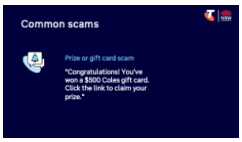
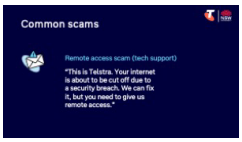
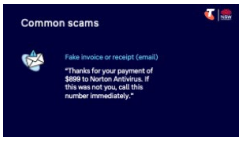
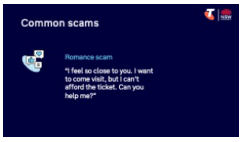
| Overview |
|---|
| **Purpose:**<br>• Introduce scams in simple, non-threatening terms.<br>• Help learners understand the goal of a scam, why scammers target people, and why awareness matters. |

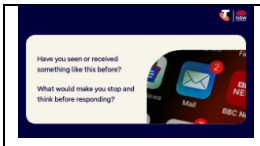
| Timing breakdown | Content |
|---|---|
| **What are scams and why do they matter?**<br>10 min<br>  <br><br>  <br> | **Say:**<br>• A scam is when someone tries to trick you into giving away your money, personal details, or access to your device.<br>• Scammers pretend to be someone they're not — like your bank, the government, or a phone company — to get you to trust them.<br>• Learning how they work can help you stay safe.<br>**Explain** how scams work:<br>• Scams can be delivered in many ways:<br>  • Emails<br>  • Text messages (SMS)<br>  • Phone calls (real or robocalls)<br>  • Pop-up messages while browsing the internet<br>  • Social media or messaging apps<br>• They're designed to make you act fast or without thinking. Once you've given your information or money, scammers usually disappear, and it can be very difficult to recover what you've lost.<br>**Explain** what scammers want:<br>• Bank or credit card numbers<br>• Personal details (name, date of birth, address, Medicare number)<br>• Passwords<br>• Access to your computer or phone<br>• Money (via bank transfers or gift cards)<br>• Your contact list (to scam others in your name)<br>**Explain** why scammers target people:<br>• They cast a wide net — sending messages to thousands of people hoping just a few will fall for it.<br>• Older Australians are sometimes targeted because scammers assume they're more trusting or less familiar with technology.<br>• They use emotional tricks to get you to act:<br>  • Urgency: "Act now to avoid losing access"<br>  • Fear: "Your bank account is compromised"<br>  • Temptation: "You've won a prize"<br>  • Curiosity or trust: "Your parcel is waiting"<br>**Explain** why awareness matters: |

| | |
|---|---|
| | • Scams are becoming more common and harder to spot — they often look and sound like the real thing.<br>• Scammers are clever: they use logos, language, and even caller ID tricks to fool people.<br>• If you know what to expect and what signs to look for, you can pause, think, and protect yourself.<br>• Learning to spot a scam also helps you protect your friends, family, and community.<br>• Being aware helps you feel more in control — it's not about being scared, it's about being ready, confident, and smart.<br>**Ask:**<br>• Why do you think people fall for scams?<br>Sample answers: "It looks like it came from a real company", "It sounded urgent", "It made me panic"<br>• Why are older Australians often targeted?<br>Sample answers: "They may be home more often", "They may trust phone calls more", "They may not know what to check"<br>**Transition:**<br>• Many scams follow the same tricks — once you learn to spot the signs, you can protect yourself and your loved ones. |

# 3. Common scams (20 min)

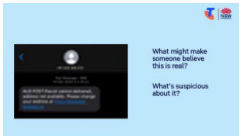
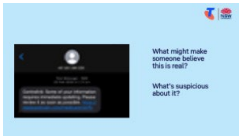
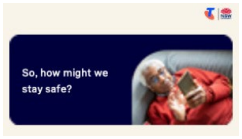
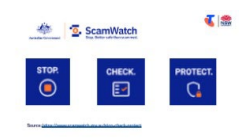
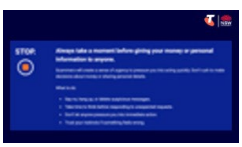
| Overview |
|---|
| **Purpose:**<br>• Help learners recognise the most common types of scams they may encounter, and understand how each type typically works. |

| Timing breakdown | Content |
|---|---|
| Common scams<br>20 min<br>  <br><br>  <br><br>  <br><br>  <br><br>  <br><br>  <br><br>  <br> | **Say:**<br>• Now let's look at some of the most common scams that people are reporting — including emails, text messages, phone calls, and even fake tech support. These scams might look different, but they often follow the same pattern.<br>**Do:** Present common scams (below) and **ask**:<br>• **What makes this message look real or fake?** (branding, language, sender address, links)<br>• **What is the intention or goal of this message — what are the scammers trying to get from you?** (money, personal details, access)<br>• **How might this scam work if someone followed the instructions?** (e.g. leads to fake login, installs software/malware, asks for payment)<br>**Common scams:**<br>• **Bank verification call scam:** "This is your bank. We've noticed a suspicious transaction on your card. Can you confirm your full name, account number, and PIN?"<br>Scammers use fear and urgency to pressure you into revealing personal and banking details.<br>• **Australia Post SMS scam:** "We tried to deliver your parcel. Please click the link to pay a small redelivery fee."<br>The link often leads to a fake payment page designed to steal credit card details.<br>• **Government impersonation email:** "Your MyGov account has been locked. Log in here to verify your identity."<br>The link leads to a fake login page that steals your username and password.<br>• **Prize or gift card scam:** "Congratulations! You've won a $500 Coles gift card. Click the link to claim your prize."<br>The goal is to either collect personal information or install malware on your device.<br>• **Fake invoice or receipt (email):** "Thanks for your payment of $899 to Norton Antivirus. If this was not you, call this number immediately."<br>When you call, scammers ask for remote access or banking details to "reverse the charge."<br>• **Romance scam:** "I feel so close to you. I want to come visit, but I can't afford the ticket. Can you help me?"<br>Scammers build emotional trust to ask for money, often repeatedly.<br>**Ask:**<br>• Have you seen or received something like this before?<br>• What would make you stop and think before responding?<br>**Transition:** |

| | |
|---|---|
|  | • You don’t need to memorise every type of scam — just learn the red flags and trust your instincts. If something doesn’t feel right, it’s okay to pause and check directly with the organisation. We’ll learn about red flags and checks after a quick break. |
| 10 min | Break |

# 4. Spotting warning signs (20 min)

| Overview |
|---|
| **Purpose:**<br>• Help learners identify common red flags in scam messages and practise checking the legitimacy of emails, SMS, and calls before taking action. |

| Timing breakdown | Content |
|---|---|
| **Spotting warning signs**<br>10 min<br>  <br><br>  <br>  <br>  | **Say:**<br>• Scammers are getting smarter — but so can we. Once you know what to look for, you'll be much more confident in deciding what to trust and what to delete.<br>**Explain** key red flags to look for in suspicious emails, texts, or phone calls:<br>• Requests for **urgent action** or **threats** ("act now or lose access")<br>• Unusual or **unknown sender** address or number<br>• **Poor spelling**, strange grammar, or generic greetings ("Dear customer")<br>• **Links** that don't match the official website (hover to check!)<br>• Asking for **personal info**, passwords or banking details<br>• **Offers** that are "too good to be true" (lottery, refunds, gifts)<br>• Messages that make you **feel** panicked, rushed, or confused<br>**Try it:**<br>• Present scam message examples (on PowerPoint or printed) and ask learners to identify (by calling out or highlighting) anything suspicious.<br>**Ask:**<br>• What might make someone believe this is real?<br>• What's suspicious about it? |
| **What to do**<br>10 min<br>  <br><br>  <br><br>  | **Say:**<br>• We know what scammers are after —money, personal details, or access to your devices — and how they might get it. For example, if you follow the instructions, you might be led to a fake login page, accidentally install harmful software, or be asked for payment or a password.<br>**Ask:**<br>• So, how might we stay safe?<br>Encourage Reponses, then explain safe actions (below).<br>**Explain** the first two steps in Scamwatch's Stop, Check, Protect method:<br>1. **Stop – Always take a moment before giving your money or personal information to anyone.**<br>• Scammers will create a sense of urgency to pressure you into acting quickly. Don't rush to make decisions about money or sharing personal details.<br>• What to do:<br>• Say no, hang up, or delete suspicious messages. |

- Take time to think before responding to unexpected requests.
- Don't let anyone pressure you into immediate action.
- Trust your instincts if something feels wrong.

2. Check – **Make sure the person or organisation you're dealing with is real.**
   - Scammers pretend to be from organisations you know and trust. Always verify who you're really dealing with before taking any action.
   - What to do:
     - Contact the organisation directly using phone numbers or email addresses you find on their official website or app.
     - Research investment opportunities or offers through official sources like ASIC.
     - Get a second opinion from family, friends, or professionals.
   - Look for red flags:
     - **Urgency** – "Act now", "urgent", "your account will be locked"
     - **Fear** – "You've been hacked", "You'll lose access"
     - **Temptation** – "You've won a prize", "Click to get a refund"
     - **Unfamiliar sender or number** – Does the address or number seem odd?
     - **Poor grammar or spelling**
     - **Strange links** – Hover over links (or press and hold) to preview the website address
     - **Requests for personal info** – Never give passwords or bank details via email or text

**Tip:**

- **Paste the words in the message into a search engine** such as Google. You may find it reported as a scam.

**Say:**

- There's no shame in being unsure. Even experts double check messages. If something doesn't feel right, pause and get a second opinion.

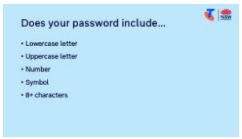
**Extension activities:**

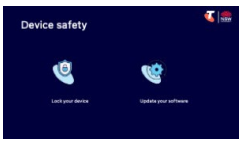
- **Complete one of BeConnected's short courses**
- **Complete ScamWatch's quiz (scroll down home page and select 'Start the quiz')**
- **Watch the video on NSW Government's website (scroll down page)**

**Transition:**

- Now that we've learned how to spot scams, let's focus on what we can do to protect ourselves day-to-day — like creating strong passwords, updating our devices, and making good choices online.

# 5. Prevention : Passwords, devices, privacy & habits (20 min)

| Overview | |
|---|---|
| **Purpose:**<br>• Teach learners simple ways to protect their devices and personal information using passwords, device updates, and safer everyday habits.<br>• Reinforce that prevention is key. | |
| **Timing breakdown** | **Content** |
| **Prevention**<br>1 min | **Say:**<br>• Scammers don't always get in through one big trick — sometimes it's little things like weak passwords, old software, or sharing too much online that open the door.<br>• Let's explore how to stay safe day to day, with simple changes that make a big difference. |
| **Password safety**<br>5 min<br>  | **Say:**<br>• Passwords protect your personal information and access to your accounts. Cyber criminals are coming up with better ways to find out people's passwords. If you can create strong passwords and keep them secure, you'll be a step ahead in protecting your accounts.<br>**Explain** how to create strong passwords:<br>• Use a mix of capital and lowercase letters, numbers and symbols (e.g. Happy$Fish24!)<br>• Make passwords long and memorable — try using a sentence, a few unrelated words, or the first initial of the words in an obscure lyric (e.g. "MyCatLovesSocks.88")<br>• Avoid common or predictable passwords like "123456", names, birthdates, or common words<br>• Avoid using the same password on multiple sites<br>• Never share your passwords unless with someone you fully trust (e.g. a carer)<br>• Turn on **2-factor authentication** (2FA) when it's available. This means after entering your password, you'll also enter a code sent to your phone or email — an extra layer of protection.<br>**Try it:**<br>• Using butcher's paper and markers, invite learners to brainstorm examples of safe passwords.<br>• Check the passwords against the 'how to create strong passwords' criteria.<br>**Extension activities:**<br>• **Watch the 'Passwords and passphrases' video on NSW Government's website (scroll down page)** |

| Timing breakdown | Content |
|---|---|
| **Device safety**<br>10 min<br><br>  <br> | **Say:**<br>• Think of your phone, tablet or computer like your home. Locking your device is like locking your front door — it stops strangers from walking in and seeing what's inside. But scammers can also sneak in through software flaws — like windows left open. That's why keeping your device updated is like shutting and locking those windows — it closes the gaps scammers might use to get in..<br><br>**Explain** how to:<br>• **Lock your device:**<br>  • Use a passcode, fingerprint, or facial recognition to unlock your device<br>  • Make sure your computers has a user password to log in<br>  • Lock your device when not using it (especially in public)<br>• **Update your software:**<br>  • Updates fix bugs and close security gaps that scammers try to exploit<br>  • Turn on automatic updates if possible, so you don't miss important fixes<br>  • Only download updates through your device's Settings or App Store — never from pop-up ads or strange links<br>  • Updates also improve functionality!<br><br>**Try it:**<br>• Set up a lock screen (code, fingerprint, or face recognition)<br>  iPhone: Settings > Face ID & Passcode or Touch ID & Passcode > Turn Passcode On<br>  Android: Settings > Security or Lock Screen > Screen lock > Choose pattern, PIN, or password<br>• Walk through how to check for updates in the Settings menu<br>  iPhone: Settings > General > Software Update<br>  Android: Settings > System > System Update<br>• Turn on automatic updates<br>  iPhone: Settings > App Store > Toggle on 'App Updates'<br>  Android: Play Store > Tap profile picture > Settings > Network preferences > Auto-update apps > Select Wi-Fi only<br><br>**Explain** what to do if your device is lost or stolen:<br>• Try to **find it**:<br>  • If you've previously activated a locator like Find Devices for Apple, Find Hub for Android, or SmartThingsFind for Samsung and your device has an active connection, you may be able to **track its location**. If it shows your mobile in an unfamiliar place, contact the police rather than trying to retrieve it yourself.<br>  • **Check lost property** and the **local police station** if you think you left it in a public place or building.<br>• **Block access**:<br>  • You can **secure/mark as lost/turn on Stole Protection and erase** your device remotely (Find Devices for Apple, Find Hub for Android). |

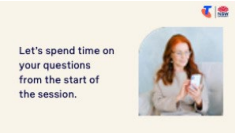
| | |
|---|---|
| | • **Suspend your mobile service** by contacting your service provider (e.g. Telstra).<br>• You can **block your mobile device's IMEI** so no one can use it even if they insert another SIM card from another carrier within Australia. Contact your service provider to do so. If your device is found, your service provider can unblock your mobile for you.<br>• **Change the usernames and passwords** on your social media, banking, email, and any other apps with your personal information. |
| **Safer online habits**<br>5 min<br><br>  <br><br><br>  <br> | **Say:**<br>• Good online habits help protect your privacy and prevent scammers from getting access to your personal or financial information. Simple things like thinking before you click, being careful with what you post, and checking links can keep you safe every day.<br><br>**Share** tips:<br>• **Think before you post**: avoid sharing your birthday, home address, phone number, travel plans and your location<br>• **Only shop on trusted websites** that begin with **https://** and show a padlock icon<br>• **Avoid public Wi-Fi** for online banking or logging into important accounts — scammers can steal your details<br>• **Log out of accounts** when using shared or public computers (or avoid logging in altogether!)<br>• **Use privacy settings** on social media to limit who can see your posts<br>• **Don't accept friend requests** or messages from people you don't know<br>• **Be cautious** of pop-up ads, competitions, or prize messages — they're often scams<br>• **Check app permissions** — some apps collect unnecessary data<br>• **Dispose of devices safely** (learn more - Cyber.gov.au QR code on Learning Canvas) |

# 6. What to do if you're targeted (10 min)

| Overview | |
|---|---|
| **Purpose:**<br>• Help learners understand what to do if they think they've been scammed, clicked a suspicious link, or shared personal information. Emphasise calm, clear next steps and where to seek trusted help. | |
| **Timing breakdown** | **Content** |
| Recognising and dealing with spam<br>10 min<br>  | **Say:**<br>• Even when you're careful, mistakes can happen — and that's okay. Scammers are clever, and many people fall for scams every day. The most important thing is what you do *next*.<br>**Explain** the third step in Scamwatch's Stop, Check, Protect method:<br>3. **Protect – Act quickly if something feels wrong.**<br>• The sooner you act, the better you can protect yourself and others from scammers.<br>• What to do:<br>• Contact your bank immediately if you think you've lost money or shared financial details.<br>• Contact IDCARE (www.idcare.org or call 1800 595 160) if you want support to recover — they can help you create a plan to limit the damage of scams.<br>• Report to Scamwatch (www.scamwatch.gov.au) to help protect others.<br>• Report to police (www.cyber.gov.au).<br>• Change passwords and security details if you think they've been compromised.<br>• Monitor your bank statements and credit reports for unusual activity.<br>• Report the scam to the impersonated organisation and platform where the scam is happening.<br>• Being scammed can feel overwhelming. Support is available at Lifeline on 13 11 14 or Beyond Blue on 1300 22 4636.<br>**Transition:**<br>• Great work! Next, let's spend some time on the questions and goals you raised at the start of today's session. |
| **10 min** | **Break** |

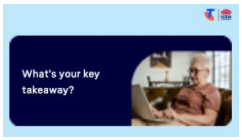
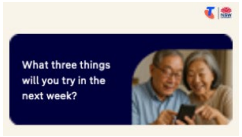
# 7. Built in flexibility (20 min)

| Overview |
|---|
| **Purpose:**<br>• To address the questions and skills learners were hoping this session covers<br>• To practice skills<br>• If time and learner confidence allow, introduce one or more extension activities from earlier sections |

| Timing breakdown | Content |
|---|---|
| Flexible time<br>20 min<br>  | **Facilitator note:**<br>• If learners identified **additional questions or topics** in the Welcome section:<br>  • Refer to the list you captured<br>  • **Say:** "Let's go through the things you said you most wanted to learn today. I'll demonstrate each one, and then you'll have a go."<br>  • If some learners would prefer to focus on practicing instead, divide the group accordingly<br>• If there are **no further learner questions**, recap key skills<br>• If **time and learner confidence allow**, introduce extension activities covered earlier in the session<br><br>**Extension activities:**<br>• Complete one of BeConnected's short courses<br>• Complete Scamwatch's quiz (scroll down home page and select 'Start the quiz')<br>• Watch the video on NSW Government's website (scroll down page)<br>• Watch the 'Passwords and passphrases' video on NSW Government's website (scroll down page)<br><br>**Transition:**<br>• Let's wrap up by reflecting on what you've learned today and planning your next steps. |

# 8. Wrap up (20 min)

| Overview |
|---|
| **Purpose:**<br>• Consolidate learning and celebrate progress.<br>• Demonstrate scanning QR codes on the Learning Canvas for trusted follow-up resources.<br>• Set a simple action for the week and signpost support. |

| Timing breakdown | Content |
|---|---|
| **Reflection**<br>10 min<br>  <br>  <br>  | **Say:**<br>• We've covered some key information on how to stay safe online and avoid scams. Let's take a moment to celebrate what you've learned and record it so you can refer back to it later.<br>**Say:**<br>• Let's revisit your Learning Canvas - tick the skills you can do.<br>**Ask:**<br>• What's your key takeaway from today's session?<br>Learners note reflections on their Learning Canvas. Invite responses.<br>• What three things will you try in the next week?<br>E.g. share what you learned with someone, create strong passwords, visit the QR codes to learn more.<br>Learners note actions on their Learning Canvas. Invite responses. |
| **Support**<br>10 min<br>  | **Say:**<br>• There are a QR codes on the back of your Learning Canvas that provides more information online.<br>• There's a lot of information online, so don't feel you need to access it. We'll cover lots more in our Tech Savvy Seniors program.<br>• But being able to scan a QR code is a handy skill. A QR code is a visual link to a website. It saves you from needing to type the URL/web address into your browser. So, let's practice today's final skill!<br>**Demonstrate** how to:<br>• Scan QR codes (Open the **Camera** > point at QR code on Canvas > tap the link)<br>**Try it:**<br>• Guide learners to scan the QR codes on the back of the Learning Canvas.<br>**Explain:**<br>• Where learners can go for support (e.g. 1:1 help at the library, tech groups, or other programs).<br>Learners note support on Learning Canvas.<br>• Show Tech Savvy Seniors program and provide the schedule for upcoming sessions.<br>**Say:**<br>• Well done! You've all achieved something new today. Keep practising little and often. We look forward to seeing you at another session. |