



# Facilitator Guide

Stay safe online

# Key information

## Overview

This lesson on Staying safe online forms part of the EDS (Essential Digital Skills) training programme. The overall aim of the programme is to give people a practical understanding of the essential digital skills that will help them in their day-to-day lives. This lesson may be delivered as a one-off session or as part of the whole programme. If all lessons are to be run as a whole programme, this should be the third lesson (lesson 3). It has been designed to run face-to-face but can also be delivered virtually. The aim of this session is to help learners to stay safe online.

## Duration:

45 – 60 minutes

## Resources you will need

- 1 PowerPoint deck – EDS Lesson 3 – Stay safe online
- Access to a screen or projector to share slide content with the learners (not required for one-to-one learning)
- Optional: an additional device

## Resources the learner may need

- Paper/notebooks and pens
- A device of their choice
- Wi-Fi access is helpful to share resources and use the links that are included in the session. If Wi-Fi is available, make this information (i.e., network name and password) available / visible to the learners, at the start of the lesson

### **This lesson will help your learners to:**

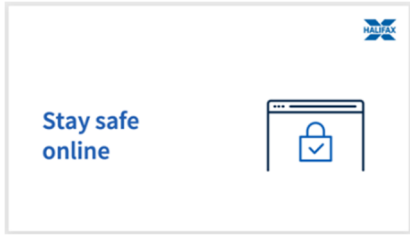
- Protect their personal information
- Secure their login information
- Recognise suspicious links
- Understand online risks
- Use security software
- Keep software up to date

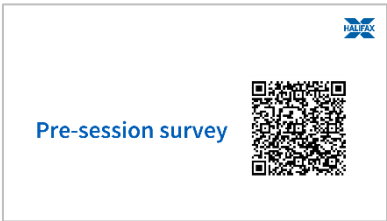
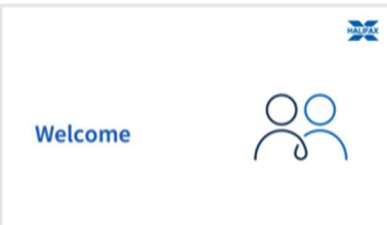
# Lesson plan

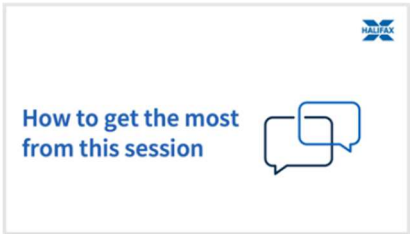
This lesson plan gives an overview of the content, approach and estimated timings for the lesson. The PowerPoint deck reflects the content included here. These notes are here to help you prepare for the session with extra detail and help to go alongside the PowerPoint deck.

In both the PowerPoint deck and the facilitator guide italics for a suggested script. This script is there to help you. You can adjust it to what feels comfortable for you. The rest of the guidance below are notes and guidance for you as the trainer to help you support your learners.

Please note that times are estimates. You can adjust timings to work for your learners and the length of the session. If you have a learner who already knows or can do a step or activity, you could suggest they help other learners.

Topic	Suggested format	Script / trainer notes	Slides and resources	Time
Holding slide	While you're waiting for people to come into the session and settle, we suggest having this slide on screen.	<p>TRAINER NOTES:</p> <ul style="list-style-type: none"> <li>Before the session starts: have the following webpages up and available: <ul style="list-style-type: none"> <li><a href="https://stopthinkfraud.campaign.gov.uk/">https://stopthinkfraud.campaign.gov.uk/</a></li> <li><a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a></li> </ul> </li> <li>Check what Wi-Fi network is available, its name and any password required; write up / make available to the learners</li> <li>Welcome people to the lesson</li> <li>Go to the next slide when you're ready to start the lesson</li> </ul>		n/a


Pre-session survey	Self-assessment survey of learners' skills at the start of a session	<p>TRAINER NOTE: Encourage learners to scan the QR code here and complete our short pre-session survey around levels of confidence in the session's topics today, plus what they would like to get out of the session.</p>	 <p>The slide features the Halifax logo in the top right corner. On the left, the text 'Pre-session survey' is displayed in blue. On the right, there is a large black and white QR code.</p>	5 mins
Welcome	<p>Start the lesson once everyone is settled and everything is set up.</p> <p>Offer a warm welcome, introduce yourself, and make participants comfortable.</p> <p>Explain the goals of the lesson and encourage questions and interaction.</p>	<p>TRAINER NOTES:</p> <ul style="list-style-type: none"> <li>• If this lesson marks the start of a programme, welcome people to the programme</li> <li>• If it is not, then welcome people to the lesson</li> <li>• <i>Welcome to today's lesson on staying safe online</i></li> <li>• <i>My name is [Your Name], and I'm here to help you today</i></li> <li>• <i>We're excited to be here with you as you start to safely explore the Internet</i></li> <li>• <i>We want to make this learning experience practical, relatable, and, most importantly, helpful to you</i></li> <li>• <i>In the room (or virtually), we also have [Any Co-Presenter's Name] who is here to help you during this session</i></li> </ul> <p>TRAINER NOTE: For small groups / virtual sessions, learners could introduce themselves at this point</p> <ul style="list-style-type: none"> <li>• <i>Being online can help you keep in touch with people, develop new skills, keep up to date on the latest news, and</i></li> </ul>	 <p>The slide features the Halifax logo in the top right corner. On the left, the text 'Welcome' is displayed in blue. On the right, there is a blue icon representing two stylized human figures.</p>	3 mins

		<p><i>shop online. It can even let you know if you might need an umbrella by checking the weather in just a few taps or clicks</i></p> <ul style="list-style-type: none"> <li>• <i>At some point, everyone worries about the possible risks of being online. You are not alone. This is not a reason to avoid being online though. There are plenty of ways to make sure you can enjoy the benefits and stay safe</i></li> <li>• <i>As we go through today's lesson, please do ask questions, and let us know if you need anything. If we can't help today, we'll make sure you get the help you need after the session</i></li> <li>• <i>Let us know if we're going too fast or too slow, or if you need a break. We want you to get the most out of today, so I'll be guided by you</i></li> </ul>		
How to get the most from this session	<p>Explain how to make the most of the session.</p> <p>Use the chat function for virtual delivery.</p>	<ul style="list-style-type: none"> <li>• <i>Before we begin, here's a few tips on how to get the most from this session</i></li> <li>• <i>If we mention any resources during the session, we'll share these with you at the end</i></li> <li>• <i>We want this lesson to be as interactive as possible, so we'll be asking questions as we go along – and we want you to ask lots of questions, too!</i></li> <li>• <i>Sometimes we'll have a short discussion about what we're looking at, or we might move on. It will depend on how we're doing for time</i></li> <li>• <i>Remember, it's all about learning together, so ask away and don't worry about how your question sounds, or getting the</i></li> </ul>		5 mins

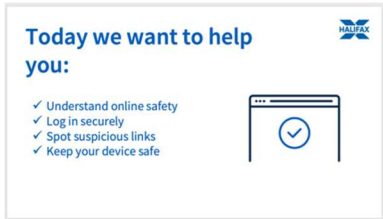
*right answer – Spoiler alert: sometimes there's no single right answer. It's your thoughts that matter most. And we're here to make your experience as easy and enjoyable as possible*



NOTE FOR VIRTUAL DELIVERY: Encourage people to comment and ask questions in the chat or experiment and try using the emojis. (Describe what an emoji is if needed)


- *To comment in the chat, find the chat box. It's usually on the side or at the bottom of your screen. Click (or tap) in the chat box, enter your comment, and hit 'Enter' or 'Send.' Your message will then appear in the chat for everyone to see. It's a great way to ask us questions or share your thoughts during our session. So, feel free to chat away!*
- *We'd like to make today as interactive as possible to make your experience more interesting*
- *First, we'll show the question on the screen. Read the question and possible answers. Pick the answer you think fits best and pop the letter for that answer (A, B, C, or D) in the chat (if and when you're ready). Don't worry about getting it right or wrong. Just go with your gut feeling!*

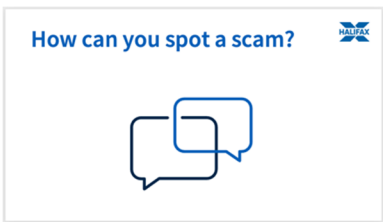

<p>How confident are you about staying safe online?</p>	<p>Quiz question with follow up discussion.</p>	<ul style="list-style-type: none"> <li>• <i>Before we start, how confident are you currently about staying safe online? Please share your comfort level in the chat by typing the letter corresponding to your answer:</i> <ul style="list-style-type: none"> <li>A. <i>Very</i></li> <li>B. <i>A little bit</i></li> <li>C. <i>Not very</i></li> <li>D. <i>Not at all</i></li> </ul> </li> </ul> <p>NOTE FOR VIRTUAL DELIVERY: Ask participants to comment with their answer in the chat box</p> <p>TRAINER NOTE: Reassure learners:</p> <ul style="list-style-type: none"> <li>• <i>Remember, the fact that you're here shows you're already taking steps to boost your online safety. Today's lesson is designed to build your confidence, and we'll cover essential strategies to help you stay safe online</i></li> </ul> <p>TRAINER NOTE: Follow-up discussion</p> <ul style="list-style-type: none"> <li>• <i>Very – Fantastic! You're off to a great start, and today's lesson will reinforce your knowledge</i></li> <li>• <i>A little bit – That's okay. This lesson is tailored to help you get the skills you need</i></li> <li>• <i>Not very – No worries. We're here to guide you, and you'll find you will get better with a bit of practice</i></li> <li>• <i>Not at all – Don't worry. We're here to support you every step of the way. As we progress, you'll see how these things are within your reach</i></li> </ul>		<p>5 mins</p>
---	---	---	---	---------------


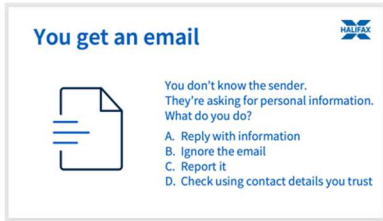


		<ul style="list-style-type: none"> <li>• <i>Feel free to engage in the chat, and remember, this is a learning journey. Your questions and insights are valuable. Let's proceed and continue developing your online safety skills</i></li> </ul>		
Today we want to help you:	<p>Explain what they will learn today.</p> <p>Participants will learn how to stay safe online, protect their personal information, recognise risks, and use security measures.</p>	<ul style="list-style-type: none"> <li>• <i>Today, we want to make sure you leave feeling more confident in your ability to stay safe online</i></li> <li>1. <i>We'll explain how to stay safe online and keep your personal information safe</i></li> <li>2. <i>You'll learn how to keep your information you use to get into your device and online accounts (like usernames and passwords) safe. Tip: Don't share them with anyone or write them down and leave them near your device</i></li> <li>3. <i>You'll learn how to spot suspicious links in emails, websites, social media messages, and pop-ups</i></li> <li>4. <i>And, last but not least, we'll help you find and download tools to keep your devices safe and up to date</i></li> <li>• <i>Every device is a bit different, so we'll provide general steps, tips, and what to look for. If you need more specific guidance for your device, just let us know, and we'll help you. We're here to make this as practical and useful for you as possible</i></li> <li>• <i>And if you need further help with your device, we'll share some helpful resources at the end of the lesson</i></li> </ul>	 <p>The graphic is a light blue box with a white border. It has a title 'Today we want to help you:' in blue. Below the title is a list of four items, each preceded by a blue checkmark: 'Understand online safety', 'Log in securely', 'Spot suspicious links', and 'Keep your device safe'. To the right of the list is a blue icon of a computer monitor with a white checkmark inside a circle on its screen. In the top right corner of the box is a small blue logo with the word 'HALIFAX' in white.</p>	2 mins



<p>What being safe means</p>	<p>Compare online safety to real-world safety.</p> <p>Emphasise the need for similar steps in the digital world.</p> <p>Encourage participants to think about safety measures they use in everyday life.</p>	<ul style="list-style-type: none"> <li>• <i>Let's start with a simple question – in your everyday life, what are some things you do to stay safe in the real world? Take a moment to think about it and feel free to share your thoughts</i></li> </ul> <p>TRAINER NOTE: Pause for a brief discussion</p> <ul style="list-style-type: none"> <li>• <i>These habits you've just mentioned are important for your safety in the real world. Now let's link that to what it means to be safe online. Imagine the online world as an extension of our physical world. Just as you lock your front door when you leave home to protect your belongings, the online world has its own set of safety rules</i></li> <li>• <i>So, think about what you do to stay safe in your everyday life. Locking your front door to protect your belongings for example. Well, in the online world, we have similar steps to take</i></li> <li>• <i>Let's start thinking about how to stay safe in the digital world</i></li> </ul>		<p>4 mins</p>
<p>Know the risks</p>	<p>Set the scene and define key terms</p> <p>Encourage discussion around tips to keep safe online</p>	<ul style="list-style-type: none"> <li>• <i>Let's start by discussing various online risks. Fraud, scams, and scammers are terms we use to talk about online risks</i></li> </ul> <p>TRAINER NOTE: Ask learners if they can explain the terms before giving the definitions</p> <ul style="list-style-type: none"> <li>• <i>Fraud is when someone tricks you to get your money or personal information. Imagine someone pretending to be</i></li> </ul>		<p>5 mins</p>

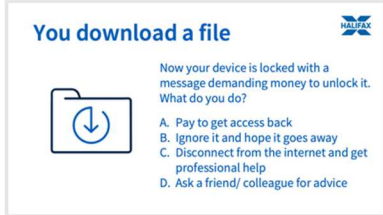
	Then pose a series of scenario-based questions to develop and reinforce good practice	<p><i>something they're not, just to take your stuff. So, it's all about being careful and not falling for those tricks</i></p> <ul style="list-style-type: none"> <li>• <i>Scams are just another name for the types of fraud. You'll often hear people use them both. If someone has been scammed, they've been tricked out of their money and/or personal details</i></li> <li>• <i>Scammers are the people who do this. Sometimes they're known as 'fraudsters.' They're the ones attempting to trick people into giving them their money or personal details</i></li> <li>• <i>Now, scammers are usually after one of two things: money or personal details. People often worry most about the loss of money, but you need to look after your personal details too</i></li> </ul>		
Which of these help you stay safe online?	Quiz question.	<ul style="list-style-type: none"> <li>• <i>What are some of the ways you can stay safe online?</i></li> <li>A. <i>Having strong passwords</i></li> <li>B. <i>Not clicking on links I'm unsure about</i></li> <li>C. <i>Keeping my phone locked</i></li> <li>D. <i>Not sharing my personal details unless I know the sender</i></li> </ul> <p>TRAINER NOTE – All these are correct - spend time discussing why, especially if anyone has missed one or more of these</p>		2 mins

How can you spot a scam?	Reassure learners and introduce next activity.	<ul style="list-style-type: none"> <li><i>Spotting scam messages can be tricky, and some of the more advanced scams can even fool the experts</i></li> </ul> <p>TRAINER NOTE: Ask learners if they know any ways to spot a scam. Then reveal the answers on the next slide</p>		2 mins
How to spot a scam: answers	Answers to question on previous slide.	<ul style="list-style-type: none"> <li><i>Here are some common themes that may indicate you've been targeted by a scam:</i> <ul style="list-style-type: none"> <li><i>Importance – Some scammers pretend to be from well-known businesses to make you think the message is important. Don't fall for it</i></li> <li><i>Spelling and odd layout – Mistakes in messages could be a sign of a scam – although these days, more scammers are using AI to create their messages</i></li> <li><i>Time pressure – If a message asks you to do something quickly, be cautious</i></li> <li><i>Reward – If something seems too good to be true, it's often a scam</i></li> <li><i>Current events – Scammers may try to take advantage of current news to make you believe they're real</i></li> </ul> </li> </ul>		5 mins

		<ul style="list-style-type: none"> <li>○ <i>Always ask yourself, "Was I expecting this message?" If not, it could be a scam</i></li> </ul>		
Types of scams	Introduce next topic.	<ul style="list-style-type: none"> <li>• <i>Understanding these risks is important – just as it's important to be aware of potential dangers in the physical world</i></li> <li>• <i>Let's look at a few examples</i></li> </ul> <p>TRAINER NOTE – Examples start from the next slide</p>		2 mins
You get an email	Quiz question and follow up discussion.	<ul style="list-style-type: none"> <li>• <i>Let's test your instincts in a common online scenario. Imagine you receive an email from an unknown sender asking for your personal information. What would you do in this situation?</i></li> <li>• <i>Take a moment to choose your answer</i></li> </ul> <p>TRAINER NOTE – The correct responses here are C. Report it and D. Check with the sender using contact details you trust</p> <ul style="list-style-type: none"> <li>• C. Report it: If you ever receive an email that seems suspicious or requests personal information, report it. If</li> </ul>		5 mins


		<p>you have received an email which you're not quite sure about, forward it to <a href="mailto:report@phishing.gov.uk">report@phishing.gov.uk</a></p> <ul style="list-style-type: none"> <li>• D. Check with the sender using contact details you trust: If you know the person that the message is supposed to have been sent by, it's a good idea to check with them directly and make sure they sent it. If the message comes from a business or organisation, you can find their contact details by searching online – don't trust the contact details in the email. You can then explain the email you have received and check they are aware of it.</li> <li>• <i>Now, let's discuss why these are the right choices. These kinds of emails are attempts to trick people into sharing sensitive information. Reporting them helps prevent others from falling for these types of traps. Checking using another channel that you know, and trust can give you an extra line of safety before responding to or interacting with the email. Online safety is a shared responsibility, and being aware of these situations will help you to navigate the digital world securely. Feel free to share any experiences or thoughts you might have on this topic</i></li> </ul>		
--	--	---	--	--


<p>You meet someone online</p>	<p>Quiz question and follow up discussion.</p>	<ul style="list-style-type: none"> <li>• <i>Let's explore another scenario related to online interactions. You've been chatting with someone online. They ask for your personal information, including your full name, address, and phone number. What would you do in this situation?</i> <ul style="list-style-type: none"> <li>A. <i>Share my personal information with them</i></li> <li>B. <i>Say no and not share any personal information</i></li> <li>C. <i>Ask them why they need this information</i></li> <li>D. <i>Seek advice from someone I trust</i></li> </ul> </li> <li>• <i>Take a moment to choose your answer.</i></li> </ul> <p>TRAINER NOTES:</p> <ul style="list-style-type: none"> <li>• The correct responses here are: <ul style="list-style-type: none"> <li>○ B. Say no and not share any personal information – Take care and be cautious when sharing personal details online, especially with someone you've just met. Your privacy is important, and sharing information like this can pose risks</li> <li>○ D. Seek advice from someone I trust –Seeking advice adds an extra layer of security. If you're unsure about the situation, talking it through with someone you trust provides valuable insights</li> </ul> </li> <li>• Discuss the answers and share tips based on the responses</li> </ul>	<div data-bbox="1556 188 1937 406"> <p><b>You meet someone online</b> </p> <p>They ask for your personal information. What do you do?</p> <ul style="list-style-type: none"> <li>A. Share my information</li> <li>B. Say no. Don't share</li> <li>C. Ask why they need it</li> <li>D. Seek advice</li> </ul>  </div>	<p>5 mins</p>
--------------------------------	--	--	--	---------------

		<ul style="list-style-type: none"> <li>• Emphasise the importance of protecting personal information online and the potential risks of sharing such details with strangers</li> <li>• <i>Let's discuss why these are the recommended choices.</i></li> <li>• <i>You need to protect your personal information online</i></li> <li>• <i>Saying no to sharing sensitive details helps protect your privacy and security</i></li> <li>• <i>Seeking advice helps you make sure that you make informed decisions. It also highlights the importance of involving people you trust in your online interactions</i></li> <li>• <i>Feel free to share any thoughts or experiences related to this scenario</i></li> </ul>		
You download a file	Quiz question and follow up discussion.	<ul style="list-style-type: none"> <li>• <i>Let's do one final scenario</i></li> <li>• <i>You recently downloaded a file from an unfamiliar website, and now your computer is locked with a ransom message demanding money to unlock it. What steps would you take?</i></li> <li>• <i>Immediately pay the ransom to unlock my computer</i></li> <li>• <i>Ignore the message and hope it goes away</i></li> <li>• <i>Disconnect my computer from the internet and seek professional help</i></li> <li>• <i>Ask a friend or colleague for advice</i></li> </ul>		5 mins





		<p>TRAINER NOTES:</p> <ul style="list-style-type: none"> <li>• The recommended course of action here is: <ul style="list-style-type: none"> <li>○ C. Disconnect my computer from the internet and seek professional help – In case of a ransomware attack, you should isolate your computer from the internet to prevent further damage. Seeking professional assistance will help you safely resolve the ransomware incident</li> </ul> </li> <li>• Discuss the answers and share best practices based on the responses</li> <li>• Stress the importance of not paying ransoms, disconnecting from the internet to prevent further damage, and seeking professional assistance to resolve ransomware incidents</li> <li>• <i>Thank you for sharing your responses</i></li> <li>• <i>Paying ransoms is not recommended</i></li> <li>• <i>The best practice involves disconnecting your computer from the internet to contain the situation and seeking help from professionals who can address the issue safely</i></li> <li>• <i>Scammers often use various tactics - like pretending to be someone else, sending messages with links or requests for your personal details, and sometimes even pretend to be romantic interests. They might also try to trick you when you're shopping online. Always be cautious and check the</i></li> </ul>		
--	--	--	--	--


		<p><i>sender can be trusted before responding or clicking on links</i></p> <ul style="list-style-type: none"> <li>• <i>Spotting and talking about these risks are the first step in staying safe online</i></li> </ul> <p>TRAINER NOTE: pause to discuss any questions or thoughts they might have on this topic</p>		
How to reduce the risks	Two slides with practical tips on keeping safe online and reducing the risks	<p>TRAINER NOTE: Stress the importance of applying these principles while learners are using their devices remotely</p> <ul style="list-style-type: none"> <li>• <i>Let's continue our journey to reduce online risks with practical steps</i></li> <li>• <i>Securing your devices – Set up a screen lock, like a password or fingerprint, on all your devices. Locking your devices, when you're not using them, helps keep your personal details safe, especially if you lose your device</i></li> <li>• <i>Be careful with public Wi-Fi –Public Wi-Fi can be tempting but risky. Scammers might set up their own "free Wi-Fi" to access your device. If you use public Wi-Fi, avoid logging into sensitive accounts, like your bank</i></li> <li>• <i>Take care visiting websites – Make sure you're on secure websites, especially those from those you trust. Look for a padlock icon and "https" in the web address. Check for spelling and grammar errors on the site.</i></li> <li>• <i>Remember the Take Five Message:</i></li> </ul>	 <p>The slide is titled "How to reduce the risks" and features the Halifax logo in the top right corner. It contains a bulleted list of four tips: "Keep devices safe", "Take care with public Wi-Fi", "Check websites are secure", and "Follow the Take Five message – Stop, Challenge, Protect". To the right of the text is a diagram showing a desktop monitor and a smartphone, both with Wi-Fi signal icons above them, connected by a curved line representing a wireless network.</p>	7 mins

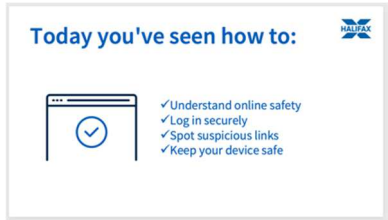
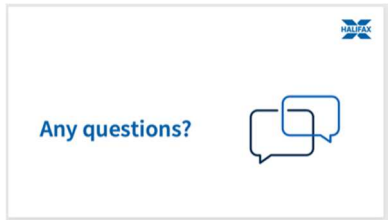
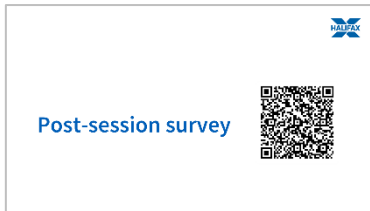
		<ul style="list-style-type: none"> <li>• <i>Stop – Take a moment to think before taking any action regarding your finances or personal details.</i></li> <li>• <i>Challenge – Question requests that seem too good to be true. Criminals often rush or panic you</i></li> <li>• <i>Protect – Contact your bank if you suspect a scam and report it to Action Fraud</i></li> <li>• <i>Staying safe online is about being careful and staying informed. Don't rush into sharing personal information, and always double-check if something seems unusual</i></li> <li>• <i>Staying safe online is about being careful and staying informed. Don't rush into sharing personal information, and always double-check if something seems unusual</i></li> </ul> <ul style="list-style-type: none"> <li>• <i>Let's explore practical steps to reduce online risks and keep yourself safe:</i></li> <li>• <i>Make sure you apply the latest updates on your devices. These updates help keep your data safe. You'll often get notifications to update; it's best to do this when you get them. You can also set your device to update automatically</i></li> <li>• <i>Protect your accounts by using strong and unique passwords. Don't reuse them. Scammers can easily guess weak passwords. A strong password could be a combination of three random words, with some letters changed to make it harder to guess</i></li> <li>• <i>Never share your passwords or use the same password for multiple things. If you have trouble remembering your</i></li> </ul>	 <p><b>How to reduce the risks</b></p> <ul style="list-style-type: none"> <li>✓ Keep things up to date</li> <li>✓ Create strong passwords</li> <li>✓ Use a password manager</li> <li>✓ Enable 2-factor authentication</li> <li>✓ Install security software</li> </ul>	
--	--	--	--	--

		<p><i>passwords, consider using a password manager, which can create strong passwords and store them safely for you</i></p> <ul style="list-style-type: none"> <li>• <i>Two-factor authentication (2FA) - also called multi-factor authentication (MFA) and 2-step verification (2SV) adds an extra layer of security to your accounts. It could be a code sent to your phone, a fingerprint or face scan. It's a great way to keep your accounts extra safe. If you want to know more about this, there's a gov.uk site to help you, which includes how to go about setting this up: <u>Turn on 2-step verification (2SV) - Stop! Think Fraud</u> (<a href="https://stopthinkfraud.campaign.gov.uk">stopthinkfraud.campaign.gov.uk</a>)</i></li> <li>• <i>Install antivirus and security software to help keep your devices safe. There's built-in antivirus software for Apple and Windows devices. You can also get separate software – some are free, others you pay for, though they may offer a free trial. It's a good idea to ask around and do your research when you're thinking of getting this, to make sure anything you get doesn't conflict with your device's built-in software. Phones and tablets don't need antivirus software, just make sure you only install or download apps from your official app store – and don't forget to update these apps when a new version is available, to keep their own security features up-to-date</i></li> </ul>		
--	--	---	--	--


		<ul style="list-style-type: none"> <li>• <i>Tip: You can practice using search engines to search to advice stay up to date about how to stay safe online. This is a good way to stay up to date with the latest know-how</i></li> </ul>		
How often should you change your passwords?	Activity slide: Ask participants to comment with their answer to the question in the chat box	<ul style="list-style-type: none"> <li>• <i>How often should you change your passwords?</i> <ul style="list-style-type: none"> <li>A. <i>Every 1 - 3 months</i></li> <li>B. <i>Every 6-12 months</i></li> <li>C. <i>When prompted by the system or device</i></li> <li>D. <i>When I know my device has been hacked</i></li> </ul> </li> </ul> <p>NOTE FOR VIRTUAL DELIVERY – Ask participants to comment with their answer (A, B, C or D) in the chat box</p> <p>TRAINER NOTES:</p> <ul style="list-style-type: none"> <li>• There isn't a one-size-fits-all answer when it comes to how often you should change your password, and it often depends on the specific app, site, or system you're using. The frequency of password changes can vary based on different factors</li> <li>• Discuss the answers and share best practices based on the responses</li> <li>• <i>Let's discuss the options:</i> <ul style="list-style-type: none"> <li>A. <i>Every 1 - 3 months – Some systems may recommend regular changes, but this can be overdoing it</i></li> </ul> </li> </ul>		5 mins

		<p><i>B. Every 6-12 months – This can be a more manageable option while still giving quite a high level of protection</i></p> <p><i>C. When prompted by the system or device – Many systems prompt password changes at recommended times</i></p> <p><i>D. When I know my device has been hacked – Always change your password straight away if you know or suspect that something has happened to your device</i></p> <ul style="list-style-type: none"> <li><i>The frequency often depends on how sensitive the information involved is, how important it is to you to keep safe, and if there are any other security measures in place, like 2FA. Always follow the recommendations of the specific service you're using.</i></li> </ul>		
How confident are you in reporting online scams?	Activity slide: Ask participants to comment with their answer to the question in the chat box.	<ul style="list-style-type: none"> <li><i>How confident are you in knowing how to report online threats or scams?</i></li> <li><i>A. I know exactly how to do this</i></li> <li><i>B. I know a bit about this</i></li> <li><i>C. I'm not sure I could do this</i></li> <li><i>D. I don't know how to do this</i></li> </ul> <p>TRAINER NOTES:</p> <ul style="list-style-type: none"> <li>Discuss the answers and share tips based on the responses</li> <li>Based on the answers, address any concerns, move to next slide, and offer additional guidance as needed</li> </ul>		3 mins

<p>What to do if something happens</p>	<p>Address what participants should do if they encounter threats or scams online.</p> <p>Emphasise the importance of prompt action, including reporting incidents, contacting relevant authorities, and securing accounts.</p>	<ul style="list-style-type: none"> <li>• <i>If you encounter a problem online, quick action is key. Here's what to do:</i> <ul style="list-style-type: none"> <li>○ <i>Contact authorities: If you suspect a scam, report it to Action Fraud at 0300 123 2040 or online at <u>Action Fraud</u>. In Scotland, you can contact Police Scotland at 101.</i></li> <li>○ <i>Gather evidence – Keep any screenshots or any relevant data related to the incident together. This evidence can be helpful for reporting and potential investigations</i></li> <li>○ <i>Tell your bank – If your bank account is affected, contact your bank immediately. They can secure your accounts and investigate</i></li> <li>○ <i>Change your passwords – If you think someone might have your password, change it right away. Make sure your new passwords are strong and unique for each account</i></li> <li>○ <i>Scan for your device – Run an antivirus and malware scan on your devices to make sure your data is safe</i></li> <li>○ <i>Taking these steps quickly can make a big difference</i></li> <li>○ <i>Stay alert, seek help, and take action if you encounter a problem</i></li> </ul> </li> </ul>	<div data-bbox="1565 188 1951 405"> <p><b>What to do if something happens</b></p>  <p>Contact Action Fraud: 0300 123 2040 <a href="https://actionfraud.police.uk">actionfraud.police.uk</a> Tell your bank Change your passwords Scan your device</p> </div>	<p>8 mins</p>
--	--	---	---	---------------

Today you've seen how to:	Recap and summarise key points covered in the lesson.	<ul style="list-style-type: none"> <li>• <i>You've covered a lot in this lesson, and I want to highlight what you've achieved and what comes next:</i></li> <li>• <i>You now know how to protect your personal information and keep the details you use to access your devices and online accounts secure</i></li> <li>• <i>You can spot suspicious links and understand various online risks</i></li> <li>• <i>You've learned how to use security software effectively and how important it is to keep your software up to date</i></li> <li>• <i>You're well-equipped to navigate online more safely</i></li> </ul>		5 mins
Any questions?	An opportunity for learners to ask anything they haven't so far during the session	TRAINER NOTE: Ask if they have any questions, comments or feedback that you can help with. You could consider this as an opportunity to check level of confidence in doing these in future, ask what they found most useful, anything they'd like to know more about (or to go through again before the lesson ends) and where they think they'll need more practice.		
Post-session survey	Self-assessment survey of learners' skills at the end of the session	TRAINER NOTE: Encourage learners to scan the QR code here and complete our short pre-session survey around levels of confidence in the session's topics today, plus what they would like to get out of the session.		5 mins



What's next	<p>Signpost the Academy website or any future sessions where applicable.</p> <p>Direct learners to additional help and resources.</p>	<p>TRAINER NOTE:</p> <ul style="list-style-type: none"> <li>• Signpost related content on the Academy website <a href="https://www.learnwithhalifax.co.uk/">https://www.learnwithhalifax.co.uk/</a></li> <li>• Encourage them to search for this site. Alternatively, they could use their phone cameras to scan the QR code here.</li> <li>• If part of a programme, share the date and topic of the next session</li> </ul>		5 mins
-------------	---	---	---	--------