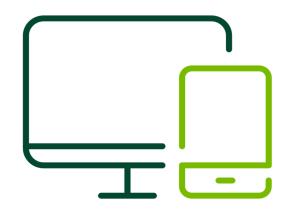


Facilitator Guide





Contents

Overview
Trainer briefing4
Agenda5
Overall session flow6
Hands-on scripts
FAQs
Trainer survey

Overview

Duration:

90 minutes for training session plus an optional extra 1 hour for 1-to-1 post-session support for those who need it.

Aims

This training aims to help learners set up and start to use the device provided, safely.

Resources:

Facilitator Guide x 1 copy [This document] Slides x 1 copy [040724-v5-dii-slides.ppt] Device: Lenovo M9 Tablet SIM card: Vodafone, 40Gb x 6 months MIFI Device: ZTE MF920n

Learning Objectives

By the end of this workshop learners should be able to:

- Set up their device
- Connect to the internet using their SIM card
- Create an email account
- Know how to keep safe online





Trainer briefing

This guide includes all the content and information you need to deliver a Direct to Learner (DTL) session to cover the Learning Objectives listed.

Learners

When delivering this training remember the learners come from all walks of life. For some learners, English is a second language so they may struggle or need help from family members, even children, during the session. This training may bring up some personal feelings for the learners. This might result in some emotions during the course. Encourage them to take a break if they need to.

Guide Format

This guide includes instructions and script as follows:

- For the overall session flow, including the discussion-based part of the session slide-by-slide script to talk through the content plus suggested questions to ask and responses to look for
- For the hands-on part of the session The actions to take (e.g. tap x button, scroll down to find y, etc) at each step of the activity, plus notes in a script-style format for you to guide the learners through these actions

The scripted content is written as though you are speaking directly to the learners. Though this gives an idea of what to say, it's important to inject your personality into the training to make it authentic, while making sure the key points are covered.

You'll find a set of frequently asked questions at the end of the guide, plus a QR code that links to a trainer feedback survey.

Session format

The intention here is to offer a safe space for hands-on and discussion-based participation during the session.

We have provided estimated timing of each section as a guide. We understand that each session timing will vary due to number of participants, their interactions, etc. The training is designed to be flexible to your needs. If, for example you are constrained by time, you can choose to prepare certain aspects of the device setup (e.g. sim card insertion) before the session starts. Though wherever possible, we recommend that learners take part in all the session topics (with support as needed) as this helps to builds their confidence.



Agenda

Module /Topic Title	Duration
Introduction	5 - 10 minutes
Get started	25 - 40 minutes
Reach out	10 - 15 minutes
Stay safe	20 minutes
Next steps	5 minutes



Overall session flow

Topic 1 - Introduction	
Slide/Resources	Approach
Getting started on your device	 Websites / pages to have open prior to session start: <u>https://www.lloydsbankacademy.co.uk/learn-for-life</u> - Academy site - for Individuals <u>https://deviceguides.vodafone.co.uk/lenovo/tab-m10-plus-3rd-gen-android-13/getting-started/insert-sim/</u> (step-by-step graphics to show how to insert the SIM card into the device) <u>https://support.vodafone.co.uk/SIM-eSIM/SIM</u> – this is Vodafone's general support page for SIMs <u>https://download.lenovo.com/consumer/mobiles_pub/tab_m9_ug_en.pdf</u> – this is the user guide for the Lenovo M9 tablet. QR code is on the 'what's next' slide <u>https://images-eu.ssl-images-amazon.com/images/I/91jtERixEmS.pdf</u> - this is user guide for the ZTE MIFI device <u>https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/turn-on-2-step-verification-2sv/</u> - how to turn on 2sv for various email, social media and other accounts



	Capture participant numbers once everyone has arrived (These should be sent to your Liverpool City Region contact after the session)
Welcome	 Facilitator note: Introduce yourself – state your role today and how you plan to help them Let them know this is a safe space to ask questions Encourage them to ask about words or phrases they are unclear on Today's session will last around 90 minutes (if delivering the full session)
	 First, a little about the Lloyds Academy and what it does. Lloyds Academy work with local and UK-wide partners to help reach people and communities we would not otherwise be able to. We work with charities like Crisis, housing associations, anti-poverty groups, prison services and organisations who work with refugees. You don't need to be a Lloyds bank customer to access our resources or training sessions. Lloyds Academy has a wealth of resources that you can tap into – so, aside from face-to-face and virtual sessions, we've got a bunch of online lessons that anyone can access from our website. We focus on three broad areas: Online essentials – This covers all aspects of digital, from getting started with a device through to more specific lessons like how to use Excel and context-specific topics like how to access Universal Credit online



	 Working life – which covers both employability topics like working on CVs and interview preps through to lessons and videos on things like collaboration and productivity tools, how to use email and so on Money management – The aim here is to increase people's confidence and show them how they can start to control their own finances
 Set up your device Connect to the internet Get started with email Keep safe online 	 Talk through the on-slide content: Here's what I'd like you to take away / know by the end of the session: You'll have set up your device so you can take it away with you and start using it safely We'll also make sure that you know how to connect your device to the internet, using your free SIM We'll help you get set up with an email account too We will look at some tips to help you to keep safe



Topic 2 – Get started		
Slide/Resources	Approach	
Setting up your device	(See Get Started hands-on script in Facilitator Guide for detailed step-by-step instructions)	
Unbox Start Insert Power Setup Internet Secure	Talk through what we're going to cover in this hands-on part of the session:	
	 Talk around the device, charger, and any other items in the box (tool for inserting the SIM, Quick Start Guide and Safety info / warranty) Demonstrate the MiFi Device (more on the next slide) Insert the SIM card (detailed images on following slide) Power on (including talk around the charger) – plug in the charger ASK: what percentage power does it say? Setup and Personalisation / accessibility: language and vision settings as these are presented on initial power up (plus talk around the fact that the device will remember these, but you can change them any time) Connect to the network (talk about Wi-Fi – as they will need to know how to connect to their home Wi-Fi if appropriate, though note that during the training session they will be using their SIM card (mobile network)) 	



Your MiFi Device	(See Get Started hands-on script – Your MiFi Device step in Facilitator Guide)
Internet with SIM card Battery powered	This is a pocket size MiFi device, used for connecting to the internet using your SIM card. It is battery powered, the battery life this can go up to 8 hours on a full charge, depending on usage that can fluctuate a bit. The device will require charging using the cable provided. The device is unlocked, you can add whatever SIM card you need.
	At the top of the device, you will find the charging port.
	On the front, right of the screen there are four LED lights, they monitor the basics things with the device. The one at the top that will monitor the battery health of the device. Green Light means Battery level is high to medium. Red Light means Battery level is low, please charge. Next there is the Wi-Fi status. Blue light means Wi-Fi is on. Light off means Wi-Fi is off. The third light is for unread text messages. Fourth Light will monitor the mobile reception strength like you notice on your phone, Blue light means 4G faster internet connected and Green light means a slower 3G internet connection.
	At the bottom side of the device, you will find the power button on the opposite side to the power button you will find SIM card holder. We will look at this together shortly. The middle button for your reference is the WPS button, it lets you connect to the device without using the Wi-Fi name and password for the device but in this group environment <u>we recommend not to use this</u> as people may end up connecting to other people's devices so recommended NOT to press the WPS button!
	On the back of the device, you can find your Wi-Fi name which is referred to as " WiFi SSID: " The password for your Wi-Fi is referred to as " WiFi Key: ". This is how you connect your tablet to your MiFi to enable you to use the internet.
	TRAINER NOTE



	As mentioned above The middle button at the bottom side of the device is the WPS button, it lets you connect to the device without using the Wi-Fi name and password for the device but in this group environment <u>we recommend not to use this</u> as people may end up connecting to other people's devices creating stress and confusion, so recommended Not to press the WPS button!
Inserting your SIM	(See Get Started hands-on script - Insert SIM step in Facilitator Guide)
	Visuals are here to help the learners if they find it useful – let them know if this isn't helpful, not to worry and that we will come round and help them with this as required.
	 Give out SIM cards and MiFi device if not already done so Ask if anyone knows what these are / has used a SIM Card (e.g. with their phones) Explain this MiFi device allows you to connect to the internet with a SIM card TRAINER NOTE - Before they start this part of the hands-on session, make sure their devices are powered OFF.
	 Micro SIM - Explain what a SIM card is, what they have (40Gb data per month for 6 months). They may have some knowledge e.g. if they have a mobile phone. Show SIM card in its packaging, including the Mobile number. Remove and show the different SIM sizes (standard, micro and nano) Remove and make sure to choose the correct SIM sizes (Micro-SIM for the MiFi device) As the image on the right shows, on the bottom side of the device you have 2 buttons and a SIM card reader latch that you open. Remove the SIM cover and insert your Micro SIM card. Once the SIM card is inserted securely close the cover On the Back of the device, you will find your Wi-Fi name (WiFi SSID) and Your Wi-Fi Password (WiFi Key). When prompted to connect to the internet use this information



Internet	(See Get Started hands-on script – Internet step in the Facilitator Guide)
- Wi-Fi - Mobile Data - Data Allowance	This slide may enable some discussions and questions. Here are the main talking points to share:
	 Wireless network – This is also known as 'Wi-Fi' and is a way for your computer to connect to the internet without using wires or cables. Does anyone have internet at home? You can connect this device to your home network for example - you will need the password. You can also connect to public Wi-Fi networks Mobile data – This enables your device to get online when you're not connected to Wi-Fi. Your MiFi device connects you to the internet using SIM card which is your mobile data. Data allowance – If you aren't connected to Wi-Fi, using the internet on your smartphone or table uses mobile data, which is measured in megabytes (MB) and gigabytes (GB). Most phone and tablet contracts have monthly allowances for data usage. Once you use up your allowance, you might get charged for additional usage, or you might not be able to use mobile data until your allowance renews the next month Ask: Can you remember your Data Allowance? 40GB
 Movie 4.5 GB Music 720 MB Radio 600 MB Internet 180 MB 	 TRAINER NOTE – Some attendees may not understand what we mean by Megabytes and Gigabytes. Explain that this is how we measure internet use. Just like you measure weights with Grams and Kilograms. This slide shows typical Internet data usage (these are average data and not exact) we have the following examples: An average 90-minute Movie - 4.5GB of Data (1 Gigabyte = 1000 MB) Streaming Music online for 10 hours 720MB of Data



	 Listening to Digital Radio for 10 hours 600MB of Data Surfing the Internet for 3 hours 60 MB So, it's good to keep track of this if you are using mobile data. Average data usage for a 90-minute movie on your popular streaming platform is 4.5GB. So that means you could get around 8 movies out of your monthly data allowance, depending on their length. But if you streamed all those movies, you may not have much data left over for other things. How to set your Data Usage – learners may want to do this with you: Settings → Search for 'data warning and limit' or go to Network and Internet → Internet → Vodafone setting → Data warning and Limit here you can switch on 'Data warning' that tells you are reaching your data limit for the month. You can also set Data Limit so that you don't use more than what you have paid for each month. This is around the 40Gb per month for 6 months provision – show the SIM card information provided.
Keep yourself safe online • Take care with public Wi-Fi • Check websites are secure • Take Five message • Stop • Challenge • Datafrege	 TRAINER NOTE – Stress the importance of applying these principles while learners are using their devices remotely 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 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 Remember the Take Five Message:



	 Stop – Take a moment to think before taking any action regarding your finances or personal details Challenge – Question requests that seem too good to be true. Criminals often rush or panic you Protect – Contact your bank if you suspect a scam and report it to Action Fraud 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
Screen unlock options Face recognition Pattern PIN Password	(See <u>Get Started hands-on script - Secure step</u>)) First, talk through / check understanding of the term 'screen lock' and what this does / why you should set it up as part of keeping your device and data safe.
	 Face recognition – To set this up, you first need to create one of the other options. Do this as part of the setup Pattern unlock – This is a security feature commonly used on some phones. It allows you to set a unique pattern by connecting dots on the screen. To unlock your phone, you need to recreate this pattern PIN Unlock – To unlock your phone you simply type in a numeric pin code Password – Choosing this option you can type a password to unlock your phone. Password can be a combination of numbers, letters and symbols. We'll talk more about what makes a strong password in a little while



Keep your device safe	30 mins - Staying safe while using your device
 Lock your device Keep it up-to-date Create strong passwords Use a password manager 	TRAINER NOTE – No need to demo these, just talk through and signpost, where appropriate, further sources of advice/info.
the state of the state of the construction of the state	Suggested script:
	As with all your belongings, you will need to keep your device safe. There are plenty of ways to do this, beyond just keeping it with you or locked away when you are not using it.
	We've mentioned locking and unlocking your device – who can remember the different options to unlock? (facial recognition, patterns, PINs and passwords) Also mention the screen lock options through Settings → Display → Lock display (allows you to change the timeout duration, switch on 'double-tap to lock' etc).
	Another way to keep it safe is to make sure all the apps and the software on your device are always up to date. That means applying updates when you're prompted to do so. This software helps to fix, improve and secure your device. So, these updates include the latest security fixes as well as improvements and new features, so it's important to apply them as soon as possible. The best way to do this is set these updates to automatically install. On your tablet, you can do this by going into Settings > System > System Update and tapping the three dots at the top right of the System Update screen.
	You may occasionally see a prompt to update your device. If you do, don't ignore it. And make sure you are only downloading and installing these updates from trusted sources.
	It's important that when you're creating passwords – to access your device or any app or website that needs it – that you pick one that is not easily guessed. Protect your accounts by using strong and unique passwords. Don't reuse them. Scammers can easily guess weak passwords. So how to come up with a



strong password? Start by picking three random words, then join them all together. Change some letters from lower case to capitals, and swap others for numbers, to make it harder to guess. Never share your passwords or use the same password for multiple things. If you have trouble remembering your passwords, consider using a password manager, which can create strong passwords and store them safely for you. Now you have a Google account for instance, you may find that when you access websites that request a password, Google will offer to suggest a strong password and store this for you.
(See <u>Get Started hands-on script - Complete setup step</u>) Use this slide for the Lenovo M9 Tablets Part of setup is setting preferred navigation mode Default is ' 3-button navigation' – as shown here, the 3 buttons show on the navigation bar at the bottom of the screen:
Triangle = Go back (returns to previous menu or exits an app
Circle = Home (returns to home screen)
• Square = Switch apps – shows a list of open apps and switches between them
Can switch to gesture navigation during setup or later (hands-on script suggests all learners leave this as 3-button during setup to ensure consistency and for ease of training – they can change this later if required) Gesture navigation-specific gestures:
Swipe up from bottom – Return to Home screen



	 Swipe up from bottom and hold – View open apps Swipe from left / right – Switch to previous page Swipe from left or right at bottom – Switch between open apps Mention also basic gestures (available regardless of navigation mode): Tap – Select or open an item Press and hold – For frequently used app functions and customising the Home screen Swipe – Up to see list of all apps; down for Notifications; down twice for Quick settings Hold and drag – To move apps etc Spread and pinch – To zoom in and out
Apps • Apps and the Home screen • Try it out: the Camera app • Try it out: the Camera app	 (See <u>Get Started hands-on script - Navigation and apps step</u>) Apps help you to use your device. You can use different types of apps like the Camera to take pictures, games apps, online banking apps, talk to family and more. Apps and the Home screen – Let the participants feel comfortable with the device and show the apps situated on the home screen and other screens, swipe up to see list of all apps that are installed on the device Camera App – On the home screen you will see an icon that looks like a Camera Tap this icon



 Click the Camera app, this will open the app to allow you to take pictures You can then click the big button to take a picture, you can also take videos by choosing the video option
TRAINER NOTE: We have noted that the App named "Duo" (Google Duo app) icon looks similar to the Camera Icon so be aware of this and go around the room to make sure everyone is in the correct camera app. Allow participants to take pictures use the video and feel more comfortable.

Topic 3 – Reach out	
Slide/Resources	Approach
<section-header><section-header><section-header><section-header><section-header><section-header><section-header><image/><image/></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	10-15 mins hands-on session (See <u>Reach Out hands-on script</u> for step-by-step instructions – up to and including Start using Gmail step) Email is a great way to keep in touch with friends and family and is much quicker and cheaper than sending a card or letter in the post. You can write to people online, send pictures and even upload short videos to an email. Having an email address is also useful in other ways. It means you can do everyday tasks like shopping and banking online. It's also now the main way companies and organisations keep in touch with customers. Email is definitely a handy thing to have as it will keep you connected with the wider world. We're going to work through how to set up a Gmail email account. You may already have a Google account and know the email address and password. If that's the case, you can use that email address. If you can't



	 remember the password, would like another email account or just don't have one yet, then this next activity is for you. TRAINER NOTE: If any learner would like to know more about setting up another email account, this can be done as a separate 1-to-1 after the session. Mention: You can access email on various devices, like phones, tablets, laptops, or computers Most devices have built-in email apps, and you can also download email apps from app stores or browsers
You get an email Important of the state of	 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? A. Reply with information B. Ignore the email C. Report it D. Check with the sender using contact details you trust Take a moment to choose your answer TRAINER NOTE – The correct responses here are C. Report it and D. Check with the sender using contact details you trust



	 C. Report it: If you ever receive an email that seems suspicious or requests personal information, report it. If you have received an email which you're not quite sure about, forward it to report@phishing.gov.uk 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 Follow-up discussion: 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.
Downloading apps • Find Play Store • Search Google Lens • Install Google Lens	(See Reach Out hands-on script for step-by-step instructions – from <u>Access Play Store app</u> step) Having a Google account means you've got access to more than just Gmail. You can also use things like the Google Play Store app. This is where you can get more apps on your device, so we're going to look at how to use the Play store to get a new app – we've picked the Google Lens app as it can be quite a useful one to have. Google Lens uses your camera to do lots of wonderful things like, translate words, identify plants, use QR codes and so much more.



	Adding apps to your device – You can add other apps that may be useful for you. You can add apps like, emails, games, banking, and more. The "Play Store" has a library of apps from which you can choose the ones to download and use on your device Let's download Google Lens app now.
Topic 4 – Stay safe	
Slide/Resources	Approach
<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	 Suggested script: When you start to use your device – Can you remember information you gave out when you first logged into your device? (Looking for: name, contact details, date of birth plus username/email address and password /PIN / pattern info) This data is held and remembered on your device, and it's the first piece of personal data that is stored there Using apps and websites – Now think about data you share or enter when you're setting up and using the different apps and websites. This may be similar to when you first logged into your device, plus it may include other information, depending on the type of app or site What kind of content would you share on a social media site for example? (Looking for: photos, videos, maybe location info etc). Talk about how this information might be used by others and the need to be careful about what you post and who might see it – e.g. holiday snaps that tell people you're not at home all week



 want payment through a direct bank transfer, don't go ahead with the purchase If you are buying or selling items on social media such as Facebook Marketplace, just like in real lif buying something from someone unknown or a guy down the pub, be careful. Things to think abowhen buying on social media, someone may ask you to put down a deposit or send payment in advance to secure your Item. It could be possible that they'll take off with your money and give you nothing in return. Never agree to pay for an item before you receive it. If the seller continues pressuring you or implies it's urgent that you pay in advance, it's possible it could be a scam and b to be safe. Beware of anything that's for sale for a fraction of the proper retail price. It could be that the item listing non-working electronics or counterfeit designer clothing. Or may take you away fr the platform to take your money. So best to be safe Back up your valuables – this includes all your precious photos and videos, as well as important contacts and documents – anything that is of value to you. If you're not sure whether something nee backing up, just ask 'would it be a problem if I lost this?'. Backups mean that even if your device is lost 		 If you are buying or selling items on social media such as Facebook Marketplace, just like in real life buying something from someone unknown or a guy down the pub, be careful. Things to think about when buying on social media, someone may ask you to put down a deposit or send payment in advance to secure your Item. It could be possible that they'll take off with your money and give you nothing in return. Never agree to pay for an item before you receive it. If the seller continues pressuring you or implies it's urgent that you pay in advance, it's possible it could be a scam and best to be safe. Beware of anything that's for sale for a fraction of the proper retail price. It could be that the item listing non-working electronics or counterfeit designer clothing. Or may take you away from the platform to take your money. So best to be safe Back up your valuables— this includes all your precious photos and videos, as well as important contacts and documents – anything that is of value to you. If you're not sure whether something needs backing up, just ask 'would it be a problem if I lost this?'. Backups mean that even if your device is lost or stolen, you'll still be able to access your data. Backing up just means taking a copy of all your important
---	--	---



 That 'somewhere safe' may be on the internet – using what we call 'cloud' storage. This is online storage, available to you on your devices through your Google accounts. You'll get a certain amount of cloud storage space included for free with your Google account, and you can buy more if you need it. Then if you need to access your backed up data – for instance if your device is broken or you're getting a new one – you can log into your Google account from elsewhere to retrieve your data The other type of 'somewhere safe' is a separate physical device. This can be a useful option if you don't have cloud storage, or if you have a lot of data to back up
TRAINER NOTE – This article gives more detail on the Google backups: <u>https://support.google.com/android/answer/2819582?hl=en</u>
If you're no longer using the device – if you are preparing to pass your device on, you'll need to clear out all your personal data. We recommend you do two things here:
 First, remove that device from any online accounts you have, for instance your Google account. Google has a simple feature to remove a single device, or even 'remove all devices' so that if you – or anyone else – tries to log into your account from that device, they'll need to enter the login details, including password
 Secondly, clear down all the data that's stored on the device itself, by doing a 'Factory reset'. This literally means resetting the device back to what it looked like when it came out of the factory. Make sure that before you do this, you've backed up any data that you're likely to need elsewhere. To do a factory reset on your tablet, go to Settings → System →Reset options → Erase all data (factory reset) then tap 'Erase all data'



More ideas to stay safe

Enable 2-factor authentication
 Use / install security software
 Don't share personal information
 Check your social media profile
 and privacy settings



Suggested script:

- Two-factor authentication (2FA) also called multi-factor authentication (MFA) and 2-step verification (2SV) adds an extra layer of security to your accounts. This might involve a text being sent to your phone with a code you use, a fingerprint or face scan or an app. 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>https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/turn-on-2-step-verification-2sv/</u>
- Antivirus and security software help keep your devices safe. There's built-in security software for your devices (including Google Play Protect plus Android built-in security protection tools). You can also get separate software for your laptop or PC 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 that device's built-in software. Phones and tablets don't need antivirus software, just make sure that when you install or download apps, you do this from your official app store. Plus, don't forget to update these apps when a new version is available, to keep their own security features up to date
- **Don't share personal information** this applies to all your devices, including your phone. Sadly, not everyone has good intentions online, so it's good to always be protective of your personal information even around family members and friends. Think of this information as private to you, and always think twice when someone is asking for things like date of birth, address or other contact details or banking details
- **Check your social media profile and privacy settings** while these apps are a great way to share with friends and family, you need to think about who else might be viewing these. So, when setting



	up your social media – and every so often after this – do check your public profile. This will show you what everyone can see. Then you can tweak or change who you want to see this, through your privacy settings. You may not want everyone to see photos of your children for instance. And those holiday snaps tell people that you're not at home this week, too
You meet someone online Image: Constraints They ask for your personal information What do you do? A. Share my information Say no. Don't share S. Say no. Don't share Image: Constraints D. Seek advice Image: Constraints	 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? A. Share my personal information with them B. Say no and not share any personal information C. Ask them why they need this information D. Seek advice from someone I trust Take a moment to choose your answer. TRAINER NOTE – The correct responses here are: 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



	D. Seek advice from someone I trust –Seeking advice adds an extra layer of security. If you're unsure about the situation, talking it though with someone you trust provides valuable insights
	Discuss the answers and share tips based on the responses.
	Emphasise the importance of protecting personal information online and the potential risks of sharing such details with strangers.
	Let's discuss why these are the recommended choices:
	You need to protect your personal information online
	Saying no to sharing sensitive details helps protect your privacy and security
	• 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
What to do if something 🛃 🔛 🕬	If you encounter a problem online, quick action is key. Here's what to do:
Contact Action Fraud: 0300 123 2040 actionfraud.police.uk Tell your bank Call 159 Change your passwords Scan your device	Contact authorities – If you suspect a scam, report it to Action Fraud on 0300 123 2040 or online at Action Fraud. In Scotland, you can contact Police Scotland on 101
	Gather evidence – Keep any screenshots or any relevant data related to the incident together. This
	evidence can be really helpful for reporting and potential investigations
	TRAINER NOTE – This is a good opportunity to demo how to take a screenshot on their device: press and hold the volume down and power buttons together. Show how the screenshot is then displayed bottom left



	 of screen, and that you can go into it, edit if required (e.g. to crop) then tap the tick/check icon to save it. Then show in the Photos app the new album called Screenshots, with your saved screenshot there. Tell your bank – If your bank account is affected, contact your bank immediately. They can secure your accounts and investigate. 159 is a new, secure number that contacts you directly to your bank if you think you're being scammed 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. Scan your device – Run an antivirus and malware scan on your devices to make sure your data is safe Taking these steps quickly can make a big difference. Stay alert, seek help, and take action if you encounter a problem.
What you've done today • Set up your device • Connected to the Internet • Got started with email • Learnt how to keep safe online	Recap what they've done so far. Let them know that we have an extra hour available now if anyone would like 1:1 support.
What's next?	10 mins - Recap, onward journey and signposting Signpost related content on the Academy website <u>https://www.lloydsbankacademy.co.uk/learn-for-</u> <u>life/get-started-online/</u>



	Encourage them to search for this site. Alternatively, they could use their device or phone cameras to scan the QR code here. This is where we can now use the downloaded app, Google Lens. find the Google Lens app on your device and use it to scan this code. As you point your camera at the QR code, you'll see a frame around the code and a prompt to open the website it links to, using your web browser. There's also a QR code for the Vodaphone site, for any questions around SIMS (e.g. how to top up after their
	6 months): <u>https://support.vodafone.co.uk/SIM-eSIM/SIM</u> There's the Digital Helpline number: a free dedicated service offering 1:1 help with digital needs. Available to anyone 18 or over and who live in UK / Channel Islands – you don't need to be a Lloyds Bank customer. Mon-Fri 9am-5pm, quote 'Digital Inclusion Initiative'
	You can use the QR code to link to the user guide for your tablets - contains everything we've been through in the 'setting up your device' part of this session as well as other useful info in an easy-to-read format <u>https://download.lenovo.com/consumer/mobiles_pub/tab_m9_ug_en.pdf</u> Lenovo M9 tablet You can use the QR code to access the user guide for the ZTE MiFi device which explains all the features available <u>https://images-eu.ssl-images-amazon.com/images/I/91jtERixEmS.pdf</u>
Feedback 🛃	Final activity: accessing and completing the feedback survey
Please give us feedback!	So, for your last activity today before you go, we'd like you to access the feedback survey for this session. You can see a QR code here – so find the camera app on your device and use it to scan this code. As you point your camera at the QR code, you'll see a frame around the code and a prompt to open the website it links to, using your web browser. Once you've tapped this, you'll see a short form to fill in. Alternatively, type the URL into your web browser.



Hands-on scripts

Hands-on script for Topic 2 – Get started		
Step	Script	Action
Unbox Tablet	OK, let's get started by opening the box to see what's inside. The first thing you'll see is the tablet itself. We'll power this up soon, but first we'll be putting the SIM card inside it, so don't switch it on just yet. We've also got a charger so you can charge up the battery from the mains. When we do start powering up, you'll see that you have got some battery charge already there, so you may not need to connect the charger during today's session.	 Open box and remove: Tablet Charger Manual
Unbox MiFi	This is a pocket size MIFI device, used for connecting to the internet using your SIM card. It is battery powered, the battery life can go up to 8 hours on a full charge, depending on usage that can fluctuate a bit. The device is unlocked, you can add whatever SIM card you need. At the top of the device, you will find the charging port.	 Open box and remove: MiFi Charger



On the front, right of the screen there are four LED lights, they monitor the basics things with the device.	
The one at the top that will monitor the battery health of the device. Green Light means Battery level is high to medium. Red Light means Battery level is low, please charge.	
Next there is the Wi-Fi status. Blue light means Wi-Fi is on. Light off means Wi-Fi is off.	
The third light is for unread text messages.	
Fourth Light will monitor the mobile reception strength like you notice on your phone, Blue light means 4G faster internet connected and Green light means a slower 3G internet connection.	
At the bottom side of the device, you will find the power button on the opposite side to the power button you will find SIM card holder. We will look at this together shortly.	
The middle button for your reference is the WPS button, it lets you connect to the device without using the Wi-Fi name and password for the device but in this group environment we recommend not to use this as people may end up connecting to other people's devices so recommended NOT to press the WPS button!	



	On the back of the device, you can find your Wi-Fi name which is referred to as " WiFi SSID: " The password for your Wi-Fi is referred to as " WiFi Key: ". This is how you connect your tablet to your MiFi to enable you to use the internet.	
Insert SIM	So let's get at the SIM card now. Has anyone used these before? You use SIM cards in various devices – most often, in mobile phones. These ones have a certain amount of data loaded on them, which you can use to access the internet, to do things like download and stream movies and music, for example.	• Open up the envelope with the SIM card in it
	SIMs come in 3 different sizes, and you can press out the bits to get the size that is right for your device. These MIFI device use the medium size, the Micro SIM. You can see the pre-set options to press-out, go down to the first press out middle size (micro-SIM).	 Show SIM with pre-cut sizes Press out first outlines to get to the micro-SIM
	Now you need to find where to insert the SIM. The Sim card is inserted into the MiFi, along the bottom side you will see two buttons. The SIM card reader is next to the buttons. It's flush with the rest of the edge and you just open it using your fingernail, the card reader opens up.	 Show where the SIM card reader is on MiFi Use fingernail to open card reader
	To fit the SIM into the card holder, follow the image on slide 8, pop in your sim card as shown.	• Put SIM card in the reader,



	Now close card holder back into place	• close card holder back into place
Power on MiFi	We're now ready to power up the MiFi. First find the power button – it on the same side as the Sim Card reader. Press on and you will see the front LED lights power on.	 Press power button
Power on Tablet	We're now ready to power up the tablet. First find the power button – that's the smaller of the two buttons on the opposite side to the card reader. Press and hold this button until you see the Lenovo logo appear on the screen This start-up process might take a minute or so. What you're looking for is a screen that says 'Hello' or 'Welcome'	 Press and Hold Power Button
Setup	Before we get going, let's check out the setup options. First, tap where it says 'English (United Kingdom)'. You'll see there are other languages that you can pick for your device. Use your finger to scroll down the list. We'll stick with English for this session, but feel free to change this language afterwards if you want.	 Tap 'English (United Kingdom)' and explore available languages from drop-down, then tap 'Cancel'
	Let's look at Vision Settings or 'Accessibility' now. There are a few options here that you can set, to make the screen easier for you to see and read onscreen content. Check out the options here – display size and text or Font size. Have a little play with this to see the effect of making the font size bigger or smaller, then try	 Tap 'vision settings' or 'Accessibility' and explore Display size, Font size, etc Tap 'back' triangle



	with the Display size. There's also a couple of options to make text clearer by making it bold or giving higher contrast The Magnification option lets you zoom in on a particular area of the screen – you can then use your fingers to move around the screen to see different parts of it in this magnified view. Select to Speak and TalkBack let you hear text that appears on the screen, rather than reading it. With Select to Speak, you tap where you want the device to read out specific bits of content. With TalkBack, it will read all the content until you tell it to stop.	
Start	Now let's tap Start. You'll see some links to a few Terms and Conditions around privacy and the user experience programme. Feel free to tap on these if you want to read them, then tap to tick the 'I have read and agree to the service agreements above' box and tap 'Next'	 Tap 'Start' Tap 'I have read and agree to the service agreements above' Tap 'Next'
Internet	Now the device wants to know how you want to connect to the internet. When you're at home, if you have broadband Wi-Fi set up and you want to use this, you'd pick the name of that network here, then you'd be prompted to type in the password for it – that info is usually displayed on the router or hub. As you have your MiFi, we will choose this as your Internet connection. At The back of your MiFi you will find your Wi-Fi name which is referred to as " WiFi SSID: ". Choose this from the list of Wi-Fi Networks on your Tablet device. Next on your Tablet device you will be prompted to add your password. You will find your password again on the back of your MiFi, referred to as " WiFi Key ". Add	 Select Wi-Fi, find your MiFi Name (WiFi SSID) at the back and select this Type in Password (WiFi Key) into your Tablet Tap Connect



	this into the password section then tap connect. This will now connect your Tablet to your MiFi for your internet connection.	
Setup options	If you then get a screen titled 'Copy apps and data', just tap 'Don't copy'. This is all about if you have a Google account or other content on your phone for example, and you want to copy any of this across to your tablet. We'll leave it for now, but you can always do this later if you want.	 (Tap 'Don't copy' if required)
	Then you'll be asked 'who's going to use this device?' Pick 'an adult or teenager' here.	 Tap 'An adult or teenager'
	Then you'll see a sign-in screen. If you had a Google account already, you could sign into it here. For now, we're going to skip this step, but we will be creating a Google account later in this session. You'll get a little message asking if you really want to skip – just tap 'skip' here too	 Tap 'skip' (Sign in screen) and confirm 'skip' on popup
	On the Date and time screen, just check that the date and time are correct, then tap 'Next'	 Tap 'Next' (Date and time screen)
	Then you'll see a list of Google services that you can turn on and off using these 'toggle' switches. Try using these now, by switching 'Send usage and diagnostic data' off, then tap 'Accept'	 Switch 'send usage and diagnostic data' off then tap 'Accept'



Secure	The next screen asks you to choose how you want to unlock the screen on your device. This locks after a period of time – we'll see in a little while how to change that time period. Then to get back in, you'll need to use what they call a 'screen unlock mode'. We'll start by picking Face recognition – has anyone used this on their phone? When you pick this option, it asks you to combine it with one of the others – pattern, PIN or password. So pick the one you'd like to use – for instance, Face recognition + pattern. It will then prompt you to enter the details – the pattern, the PIN or the password. It asks for this info twice, then tap 'Confirm' Then it tells you about how face recognition works. There's a box that you can tick to 'raise to wake' which means when you pick up the device and face it, it will wake up Tap 'Continue' then position your face in the outline oval in the next screen for it to recognise your face, then tap 'Continue' once it's confirmed that has been done	 Choose Face recognition Choose Face recognition + pattern Draw a pattern and tap 'next' Repeat the pattern and tap 'confirm' Tick 'Enable 'raise to wake' checkbox and tap Continue Position your face in the shape and tap 'Continue' when face recognition is confirmed
Apps on startup	The next screen shows some apps that will be included when you start using your tablet – so you don't have to go in and download them individually. The first lot are all grouped together and include some useful apps so we'll keep these for now - then there's a couple that you can untick if you want. You can always add and remove apps at any time, so if there's any here that you find you're not using, or there are others you want that you haven't got we'll show you how to remove or add these.	 Untick Google News and Google Podcasts then tap 'OK'
Complete setup	You'll then see a screen with a couple of 'anything else?' options – one for the Lenovo ID which is optional so we'll leave this for now. The other is about how	 Check System navigation says '3-button navigation'; if not, tap



	you'll navigate around your device. It should say '3-button navigation'. If it says 'gesture navigation', just tap then pick '3-button navigation' to change it over, so we're all using it the same way to start. Just like the other settings, you can always change this later if you want. Tap 'Finish' on that screen, then tap 'Finish device setup'.	this option and change it to 3- button then tap 'Finish' then tap 'Finish device setup'
Home screen	This should be all you need for the setup. If you get a screen which mentions Google Play, just find the little circle button and tap it. Then you'll be in the Home screen – this is the main screen from where you can find your way around all the apps, settings and other content on your device.	 If Google Play screen is displayed, tap circle button
Navigation and apps	Let's just find our way around the Home screen and start navigating to get familiar with what you get on your device right now. For instance, there are many apps already installed. To find these, swipe up from the bottom of the screen. Let's take a look at one of these apps – can you find the clock app and go into it? To get back to our list of apps, just tap the icon with the four squares. Can you find the Settings app? You'll need to scroll down a bit to find it. Now tap the triangle button. This takes you back to the last screen or app you were in – in this case, it's the clock app. To get back to the Home screen, tap the circle button And to show all the apps that are active or open right now, tap the square button. You can close any of these apps by just swiping them up to the top of the screen. Or tap 'clear all' to close them all in one go.	 Swipe up from bottom to show list of apps Tap the clock app Tap the four-squares to show the app list again Scroll down and tap Settings Tap the triangle to go back to the last screen (clock app) Tap the circle to return to the Home screen Tap the square to show all open apps Tap 'clear all' Swipe up again to apps list



Now find the apps list again by swiping up from the button. This time we're going into the camera app. Why not take a photo while you're there?		ap the camera app Take a photo	
---	--	-----------------------------------	--

Hands-on script for Topic 3 – Reach out		
Step	Script	Action
Find where to add a Google account	OK, let's start from the Home screen. We want to find Settings, which is an app, so swipe up to see the Apps list, ten scroll through the apps until you find the Settings one – it looks like a cog. Now scroll through the different settings until you find the Passwords and Accounts section. You'll see an option to Add an account, so tap on that then	 From Home screen, swipe up to Apps list then scroll to find Settings Scroll to find Passwords and Accounts then tap '+ Add
	pick Google from the list of accounts	account' and select 'Google'
Provide personal	Confirm that 'an adult or a teenager' is going to use the account here	• Tap 'An adult or a teenager'
details	Next, you'll see the sign in screen. Tap where it says 'Create account'. A little message will pop up with options for the type of account you're creating, so tap 'For my personal use' here	Tap 'Create account'Tap 'For my personal use'
	Now it's time to fill in your details. On this screen, notice that you only have to enter your first name.	 Type in first name and tap 'Next'
	Under 'basic information', it's asking for your birthday and gender. Note that this is a one-off step and you're unlikely to be asked this information again by Google. Under 'Gender', there are multiple options including 'rather not say'	 Type in birthday (day, month and year fields) Select Gender (e.g. 'rather not say')
Set up email credentials	On this next screen, you get the chance to pick an email address. Sometimes, Google will suggest one, based on your name. You can choose one they suggest or create one you prefer. They will then check to see if someone's	• Type in an email address (and make a note of it)



	already registered that address – if no one has, it's all yours! So you might need to try a few options, if the first one you come up with is already taken. Once you have an email address, you'll be asked to set up a password for it, too. It needs to be at least 6 characters long, with a mix of upper and lower case letters, numbers and (optionally) symbols. Make it something you can remember but is not easily guessed by others. If you're stuck, just think of 3 short words, string them all together and swap out some letters for numbers –	 Type in a password and tap 'Next'
Add phone number	like '1' instead of 'i' and zero instead of '0'You'll be asked if you want to add a phone number to this account. This is optional, so if you don't want to, just tap 'skip'. Having a phone number attached can help if you forget your password for example. You can always add one – or remove it – later on.	• Tapʻskip'
Review and pick settings	Then there are a few screens for you to review your details and choose settings. First, tap 'next' on the review screen. Then tap 'Express' option on the 'choose your settings screen and tap Next. The next screen is all about how Google may use your data and you can choose to Accept all or Reject all. For now, let's Reject All – you can always go in later and change these if you want to. Then you'll get a screen confirming these preferences and talking about cookies – what these are and how Google uses them. At the bottom of this screen, tap 'Confirm'. Then there's a screen that shows the general terms and conditions. There's a button at the bottom of this screen, to tap 'I agree'. The last screen is all about Google's data backup and storage service. By default, this is switched on, which means that your data is backed up and stored with your Google account. This is useful if you want to sign into your Google account on other devices (like your phone), or if you stop using your	 Tap 'Next' Tap 'Express (1 step)' and tap 'Next' Scroll down and tap 'Reject all' Tap 'Confirm' Tap 'I agree' Tap 'Accept'



	tablet and want to access your data from a new device. Just tap 'Accept' on this screen. Once you've done this, you should see the Passwords and accounts settings screen, with a shortened format of your email address (they asterisk out part of the email address here).	
Access Gmail	Now you've set up your Gmail account, you can access email, so let's go there now. Tap the circle to get back to the Home screen, then swipe up to get the list of apps and find Gmail there – alternatively, there should be a 'Google' area on your home screen with the Gmail app there. Look for the multi-coloured 'M'. You may see some information or news items which you can just tap 'Got it' or 'Take me to Gmail' to get through. You'll then get asked if it's OK for Gmail to send notifications – for example to let you know that you've got a new email message. Tap 'allow' to let this happen.	 Tap circle button Tap Google widget then pick Gmail app Tap 'Got it' Tap 'Take me to Gmail' Tap 'allow'
Start using Gmail	You've already received your first email, from the Google Community Team. Take a moment to tap this item and read through it. If you want to find out more about using email, see us after the session, or check out our other resources – we'll show you where these are at the end of the session.	 Tap 'Google Community Team' email and scroll through this
Access Play Store app	Now let's look at using the Google Play store. First, find the Play store icon – this might be on your Home screen – look for a multi-coloured triangle, pointing to the side. If you can't see it, just swipe to see your apps list then scroll until you find Google Play Store.	• Find Play Store icon then tap to open it
Notifications etc on first start up	You might be asked about other services to add – just tap 'No thanks' for now You might also get a little popup message about Google optimising app installs – just tap 'OK' on this one	Tap 'no thanks'Tap 'OK'
Finding an app	In the Play Store, you can find an app either by searching for it, or by scrolling down and looking in the categories. It's a bit like using streaming services, if you've done that before on your TV or another device. Try scrolling down now, to see the different apps and categories.	 Scroll down to see the different content / categories



	Now find the search field at the top of your screen, and type 'Google Lens' there.	 Type 'Google Lens' in the search field
Install the app	You'll see the Google Lens app on your screen, along with other sponsored or related apps. Tap the 'Install' button on the right, then once it's finished installing, tap the 'Open' button.	Tap 'Install'Tap 'Open'
Privacy Notice	The first time you open the app you will see a privacy notice. Attendees can read the notice and choose to 'accept all' or 'reject all'.	Tap 'accept all' or 'reject all
Start using the app	You will now see a camera icon, click on this and it will open your camera you can then read QR codes. Place camera over your Tablet packaging and search and see what happens.	 Click camera icon or Google Lens app Search items using your camera

Annex

FAQs

Q: How do I change the amount of time before the screen locks?

A: Go to Settings then scroll down to find Display. Scroll down to the Lock Display section, then tap Screen timeout. You can then pick the time you want.

Q. How do I back up my data?

A. Go to Settings then scroll down to find System. Scroll down to tap on Backup, then under Backup by Google One, tap the Back up now button. You may be asked to confirm this action with your password / PIN / pattern.

Q. How do I clear out all my personal information?

A. A 'factory reset' will clear all data from your tablet's storage. To do this, go to Settings then tap on System, then Reset Options. Tap on Erase all data (factory reset) then tap on Erase all data. **Note that this will not clear data that you have backed up to your Google account (see 'How do I back up my data?').**

Q. How do I see how much data I have left this month?

A. Go to Settings then tap Network and Internet. Tap Internet - Vodafone UK then tap the cog icon. The 'App data usage' is shown on the following screen.

Q. Can I still use my SIM card after the 6 months of free data?

A. Yes – you can top up your data to keep using your SIM. When you first start to use your SIM, Vodafone will send you a message on your device to let you know how to do this online or via their app.

Q. Is my Biometric data/Thumbprint/Face recognition stored on the cloud?

A. No, the data is stored securely on your devices so that only you can have access to this device. If you get another device, this will have its own security.

Trainer survey

We'd love to hear how you found the experience of running this session.

Please scan this QR code to access our trainer feedback survey



