Keeping safe against cybercrime

BARCLAYS | LifeSkills

Module overview

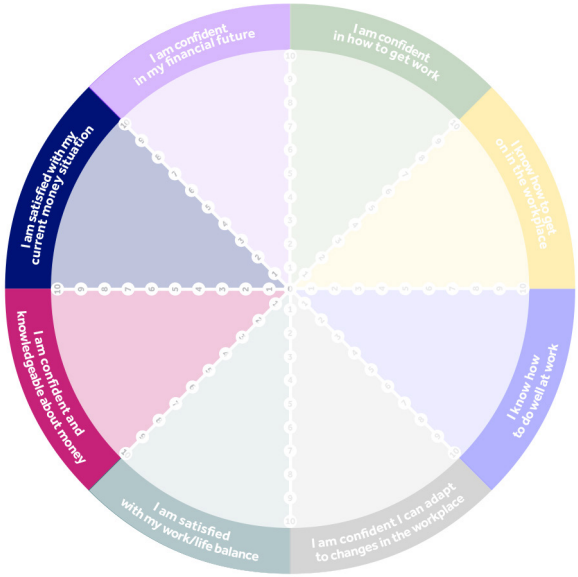
This module will focus on how individuals can keep their finances safe online by protecting their personal information and recognising risks of fraud, scams and identity theft.

Time	Key learning outcomes	Which will lead to
35 mins	By the end of the module, learners will be able to: • Identify ways to stay safe online and protect themselves from the most common types of fraud, scams and identity theft • Understand their digital footprint and why putting too much information online can increase their security risk • Understand where to go for support and advice should they be worried they have been a victim of fraud, scams or identity theft	• Reduced risk of becoming a victim to cybercrime • Increased use of practical methods to protect their finances and data from cybercriminals • Increased confidence and understanding of how to report cybercrime to help protect others

Important

Introduce the activity and theme and remind your learner of the coaching-based approach. Agree the desired outcome of the session with your learner.

Throughout the activity, we have included **'do now'**, **'do soon'** and **'do later'** actions which may help your learner to think about the next steps they could take. Alternatively, you could use the 'do now', 'do soon' and 'do later' headings to help your learner come up with their own actions.



Contents

Introduction

Time	Educator guidance	Expected outcome
2-3 mins	Refer back to your learner's LifeSkills wheel and discuss how they scored themselves in relation to this module. Discuss what they need to know or do to be able to increase how they rate their satisfaction with this area.	• Learners are reminded of where they are now and what they need to do to reach a higher satisfaction score in this area

Core activity one

Understanding the scale of cybercrime and personal data

Time	Educator guidance	Expected outcome
8-10 mins	**Start with the question:** **What can we do online today?** If suitable, on the left-hand side of a sheet of paper ask your learner to list as many uses as possible, for example, shop, make payments, pay taxes, socialise, find a partner, read news, play games, do quizzes etc. Prompt ideas where needed. **Follow up with the question:** **Have you ever considered how much information you give out across all online usage?** On the right-hand side of the same page, ask your learner to list the different types of information they give out across all those uses listed on the left. With the lists complete, ask your learner how much they know about keeping all of this information safe from cybercriminals? Approach follow up questions sensitively in case your learner has been a victim of cybercrime. Ask if they know any examples of fraud/ scams/identity theft or how fraudsters can get hold of your personal details. Explain that fraudsters accessing personal information online has become more common, as the following stats show.	• Learners will understand how much personal data they give out online • Learners will understand the scale of cybercrime today

Core activity one

Understanding the scale of cybercrime and personal data (cont'd)

Time	Educator guidance	Expected outcome
	Share these with your learner: • Frauds and scams are now Britain's number one crime[1] • 4.7 million cybercrimes were recorded in the 12 months to September 2017[2] • £190 billion is lost to the UK economy annually due to cybercrime[3] • £1.9 billion invested in cybersecurity by the UK government[4] • Millions of passwords are available to hackers due to data breaches	

1. Fraud and computer misuse statistics for England and Wales, ONS
2. Fraud and computer misuse statistics for England and Wales, ONS
3. Annual fraud indicator, 2017
4. National Cyber Security Strategy 2016-21

Core activity two

Different types of cybercrime

Time	Educator guidance	Expected outcome
8 mins	Talk through the following common types of cybercrime and ask your learner to suggest ways of staying safe/increasing protection against cybercrime. **Social engineering:** Social engineering is the act of tricking someone into divulging information or taking action, through email and other devices. The idea behind social engineering is to take advantage of a potential victim's natural tendencies and emotional reactions. **Website spoofing:** Where forged websites mimic legitimate sites. Fraudsters use a similar design, layout, font and colours to mislead customers into buying things like festival tickets and car insurance that do not exist. **Phishing:** A broad term for any attempt by cybercriminals to fool victims into sharing confidential information such as passwords, usernames, and financial details for malicious and criminal purposes. Large scale phishing attacks involve emails being sent to multiple victims in the hope that a small percentage will be successful.	• Learners will be able to identify the main threats that cybercriminals might use to target them • Learners will understand practical tools and measures they can put in place to help reduce their risk to cybercrime

Core activity two

Different types of cybercrime (cont'd)

Time	Educator guidance	Expected outcome
	Spear phishing: Where cybercriminals target a specific individual or audience to gain sensitive personal or business information. Anyone can be the target of a spear phishing attack. Cybercriminals spend much more time and effort on individual spear phishing attacks than they do on large scale phishing because they need to gather personal details about their victims to make the email seem as legitimate as possible. **Vishing:** This is the telephone equivalent of phishing. It is described as the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. **Smishing:** This is the text equivalent of phishing. It is when you receive an 'urgent' text message asking you to click on a link or call a number, with the intent to gain your sensitive personal or business information. **Malware:** A broad term to describe 'malicious software'. Malware is specifically designed to damage, disrupt or gain unauthorised access to a computer. Types of malware include computer viruses, worms and Trojan horses. **Ransomware:** A type of malware that can take over a computer and threaten the user until a sum of money is paid. Threats often include blocking the victim's access to the files on the computer or publishing data it contains on the internet.	
5 mins	Choose from the selection of **Case studies** or look at all of them depending on the time available and the knowledge of your learner. Read these through together and support your learner to identify the types of cybercrime. **Use the following questions as prompts to discuss the implications:** **What signs of a cyber threat could the individual have spotted?** **Which scenario poses the highest financial consequences to the individual?** **What could the individual have done differently next time?** Emphasise that cybercriminals also target victims through text messages, phone calls, chat rooms, and social media posts. It is essential that in both our personal and working lives we all have a good understanding of how to protect ourselves and the company we work for.	• Learners will gain understanding of different types of cybercrime through exploring case studies

Wrap up

Time	Educator guidance	Expected outcome
5-7 mins	With your learner, look through the **Top tips for staying safe online**. Which ones stand out most to your learner as priorities for them to action into their own lives? **Do now:** Change my main passwords to more secure ones, and don't repeat use of new passwords across different accounts/platforms **Do soon:** Check my privacy settings and how much personal information is public on my social media accounts, including birthday, hometown, pet names **Do later:** Install security software such as antivirus and two-factor authentication	• Learners will be able to identify their current gaps in protecting themselves online, and action priorities to improve their safety

Optional extension

Time	Educator guidance	Expected outcome
10-20 mins	Watch the film Data to go (produced by Cifas) or this Barclays advert about the risks of sharing personal information online. It exposes how much personal information is accessible to fraudsters via our social media accounts. Discuss with your learner why it is important to be careful about the information they share publicly, and which information fraudsters might be able to use. **Criminals could use the information publicly available or that you've shared (for example) to:** • Guess someone's password • Steal their identity • Apply for a credit card in their name • Scam them – as they already know quite a lot about them • Spear-phish one of their contacts by pretending to be them • Find out where they live and burgle them, if they know their holiday dates If appropriate, direct your learner to explore more hints and tips from Digital Wings.	• Learners to understand the 'hidden' information they may be sharing through their online use and how cybercriminals can use this information if not protected

Case study: James

Cybercrime: Vishing

James receives an unexpected call on his mobile. It shares his area code and his phone recognises the number as potentially the name of his bank. Thinking it's his bank calling, he picks up.

On the other end of the line, an automated voice tells him that his bank account has been compromised. To secure his account, he is told to call a given number urgently, as he risks losing all of his money that he won't get back. By calling the number instantly, the voice claims his bank can secure his account.

Not wanting to lose his money, and given the urgency, James calls the number given. The person on the other end asks for his personal details, including postcode, account number, card number and its expiry date. In a panic, James provides all these details, and the person on the other end of the phone reassures him that he's done the right thing and his money is 'safe'.

The next day when checking his account, James notices that the money in his account has almost entirely gone. He calls the known number of his bank and they inform him that he has been a victim of a scam.

What could James do to reduce the risk of being a victim to vishing?

- Never give out personal information over the phone
- Use a caller ID app – a good caller ID app can help boost your phone's spam call detection and blocking capabilities
- Never call a number given to you without cross-checking it on the company's official website
- Hang up if you get a suspicious call. Before calling back the legitimate number of the company, do a bit of research on internet. It's then a good idea to go online and find the number for the relevant company or department they were claiming to be from to check if they were genuine

Other common types of vishing scenarios include:

- Overdue or unpaid taxes to HM Revenue and Customs (HMRC)
- Prize or contest winnings (such as a cruise or an 'all expense paid' vacation)
- Fake computer tech support calling to remotely access your computer to fix a problem
- Faked government agencies (such as a court or law enforcement agency)

Case study: Shauna

Cybercrime: Phishing and website spoofing

In April, Shauna received an email from HMRC that said:

> Dear Tax Payer,
>
> You are eligible to receive a refund of up to 425.58 GBP. In order to do so, you are required to submit an official claim application using the information you have registered with us.
>
> **Claim your tax**
>
> Note: If you will not complete the refund form now, you will not be able to claim your annual tax refund online.
>
> Best regards,
>
> Luke Sullivan
>
> **Why you got this email**
> You registered for a refund through Government Gateway

The email had the right logos, the display name of the sender looked genuine and the hyperlink directed to the correct-looking URL link. However, as Shauna wasn't expecting a refund, had not applied for one and was surprised by the urgency of the email, she checked the HMRC website. She discovered that HMRC would never send notifications by email about tax rebates or refunds.

She discovered that it was a spoof and was lucky not to accidently give her personal data away.

What else could Shauna have checked to realise that this was a spoof?

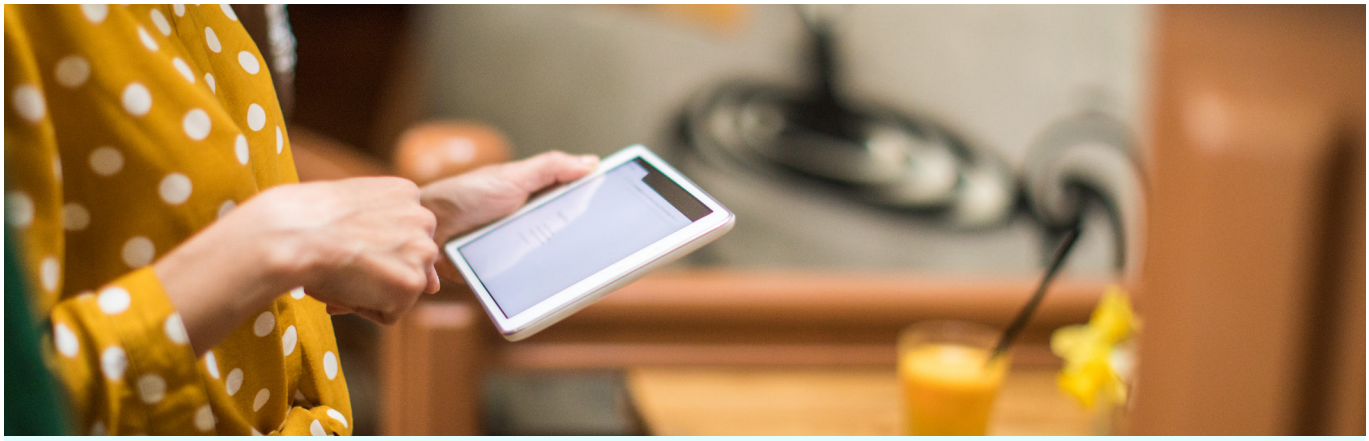
- By checking with HMRC's website she discovered that with spoof email you should never:
  - Visit any website directed to from within the email
  - Open any attachments
  - Disclose any personal or payment information
- Check the URL link before clicking it. Cybercriminals are now so sophisticated that they can set up a spoof website address that is typed exactly the same as the real one, but they'll replace lower case vowels with accented letters. It's always best to type its web address directly into your browser
- They didn't know her – her name is missing
- They ask you to click a link
- They want you to do it now – create a sense of urgency which may have put pressure on Shauna to do it quickly

---

To help protect other people, Shauna reported the spoof email to a dedicated anti-fraud email address at HMRC – most large organisations will have one of these, to help stay one step ahead of the cybercriminals.

Case study: Kelly

Cybercrime: Early pension release scam



Kelly was called out of the blue by an investment company claiming they could help her to release cash from her pension before she turned 55, in four years time.

It started out as a free pension review, so Kelly thought why not. The result of the quick review told Kelly that she could take cash from her pension, labelled as a 'saving advance'.

Kelly provided her details online and her pension funds were transferred from her legitimate pension scheme into one set up by the new investor.

Over the course of a few months, Kelly was 'loaned' amounts of cash (adding up to around half of her pension) with the company involved taking a fee each time, often as much as 30%. This fee was often unclear and didn't include the tax she will owe for accessing her pension early.

After a year, the money remaining in the scheme after fees and tax were paid was invested in high-risk products, until one day it was simply stolen outright leaving her with no savings for herself, or wider family.

What could Kelly have done to have avoided being a victim to early pension release scams?

- If you get a cold call about your pension, the safest thing to do is hang up – it's illegal and probably a scam. Report pension cold calls to the Information Commissioner's Office (ICO)
- If you get offers via email, text or online adverts, you should simply ignore them
- Be wary if you're contacted about any financial product or opportunity and they mention using your pension
- Professional advice on pensions is not free – a free offer out of the blue is probably a scam
- Always check that anyone offering you advice or other financial services is FCA authorised and permitted to give advice on pensions
- If you don't use an FCA-authorised firm, you also won't have access to the Financial Ombudsman Service or Financial Services Compensation Scheme so you're unlikely to get your money back if things go wrong
- Always be wary if you're contacted out of the blue, pressured to invest quickly or promised returns that sound too good to be true
- If you intend to use the money in your pension to repay debts, you should contact a free debt adviser first to see what else you could do. Taking money from your pension early might help your immediate debts, but it's a very expensive way to free up money

Keeping safe against cybercrime

Top tips for staying safe online

Tips for safe passwords

- At least eight characters
- Include a combination of upper case, lower case, numbers and special symbols such as !@£$^%,:
- Don't reuse passwords for multiple logins

Stay safe on your smartphone/tablet/laptop

- Only download apps from official app stores
- Activate a screen lock and use a password or biometrics to unlock the screen
- Fingerprint and other biometric technology is more secure than using passwords
- Some apparently public wifi services are actually set up by hackers precisely to intercept information. Hackers can also easily spy on open wifi. To avoid the hacker's tricks:
  - Do not conduct financial transactions or send sensitive data without additional encryption in place, such as a VPN, or use your mobile network instead
  - Be careful about the sites you visit on public wifi – it's OK to check the news but not do your online banking
  - Use secure sites whilst on public wifi – look out for the padlock in the web browser and https (not http) at the start
- Install security software such as anti-virus and two-factor authentication. This kind of software is often available for free
- Keep all security software and operating systems updated (this can be set to update automatically)

Staying safe on social media

Short of removing your digital footprint altogether, you can:

- Control your privacy settings
- Not approve access to additional permissions if you do quizzes on social media
- Only approve followers on social media that you recognise
- Use a search engine to find yourself and make sure there's nothing online you don't want hackers to know
- Keep tabs on what your friends and family post about you

Staying safe from cybercriminals

- Always be wary if you're contacted out of the blue, pressured to action something quickly or promised returns that sound too good to be true
- Never give out personal information over the phone or via email
- Use a caller ID app – a good caller ID app can help boost your phone's spam call detection and blocking capabilities
- Never click any link or download any documents from suspicious emails

For further advice on how to stay safe online please visit:

- Cyber Aware
- Get Safe Online or the National Cyber Security Centre
- Take Five, Stop Fraud
- Which? scams alert service provide examples on the latest scams doing the rounds
- Report cybercrime to Action Fraud
- Money Mules
- Avoid investment and pension scams