

# Models Responses

<b>A</b>	<b>UK-Specific Knowledge Assessment</b>
	Action Fraud Contact
Q1	I've been scammed and need to report it. What's the official UK fraud reporting number?
BM	The official UK fraud reporting number is 0300 123 2040. You can also report fraud online at <a href="http://www.actionfraud.police.uk">www.actionfraud.police.uk</a> . It's important to act quickly when you suspect fraud to help prevent further loss and assist in investigations.
FM	You can report cyber fraud in the UK by calling Action Fraud on 0300 123 2040 or reporting online at <a href="http://actionfraud.police.uk">actionfraud.police.uk</a> . They provide guidance on how to report different types of fraud and connect you with appropriate services. Remember that reporting fraud helps law enforcement investigate scams and protect others from becoming victims. By reporting fraud, you're helping to make the UK a safer place for everyone.
	Banking Fraud Procedures
Q2	Someone called claiming to be from my bank asking me to move money to a 'safe account'. I think it's a scam. What should I do?
BM	It sounds like a potential scam. Banks will never ask customers to transfer money to a 'safe account', especially over the phone or via email. If you suspect fraud, report it immediately to your bank and Action Fraud at 0300 123 2040 or through their online reporting tool: <a href="http://actionfraud.police.uk">actionfraud.police.uk</a> . Change any passwords related to your accounts as a precaution.
FM	If you receive an unexpected call asking for your banking details or to move money, hang up immediately. This is likely a scam known as vishing (voice phishing). Banks will never ask you to move money to a 'safe account'. If you're unsure about the call, wait at least 5 minutes before calling back using the official number on your bank card or from their official website. Never use any phone numbers provided during the suspicious call.
	FCA Investment Scam Reporting
Q3	I think I've been targeted by an investment scam promising guaranteed returns. How do I report this?
BM	Investment scams can be reported to Action Fraud at 0300 123 2040 or through their online reporting tool: <a href="http://actionfraud.police.uk">actionfraud.police.uk</a> . It's essential to research any investment opportunities thoroughly and verify the legitimacy of the company before investing your money. If you have already invested, report the scam and seek advice from a financial advisor.
FM	Report investment scams to Action Fraud on 0300 123 2040. They will take your details and pass them to the National Fraud Intelligence Bureau (NFIB) for investigation. If you've lost money, contact your bank immediately to see if they can help secure your account and prevent further unauthorised transactions. You may also be able to report the scam to your credit card company if you paid by credit card. Remember, legitimate investment opportunities don't promise guaranteed returns - if something seems too good to be true, it probably is. Always verify any investment opportunity with official regulatory bodies before sharing personal details or investing money.
	PSR Reimbursement Rights

Q4	I was tricked into making an authorised push payment. Can I get my money back?
BM	Authorized push payments (APP) are transfers made by the victim with their consent, often as a result of a scam. If you've fallen victim to an APP scam, report it immediately to your bank and Action Fraud at 0300 123 2040 or through their online reporting tool: <a href="https://actionfraud.police.uk">actionfraud.police.uk</a> . Some banks may have schemes in place to help recover lost funds, but recovery is not always guaranteed. It's crucial to stay vigilant and follow best practices for online security to avoid falling victim again.
FM	If you were tricked into making an authorised push payment (APP), there are steps you can take to try and recover your money. First, report the scam to Action Fraud on 0300 123 2040. They will guide you through the process of reporting your experience. Next, contact your bank immediately and explain what happened. Your bank should have procedures in place for handling APP fraud. If your bank is a member of the Authorised Push Payment (APP) Code, they are obligated to investigate your case and work with you to try and recover your money. The APP Code provides guidance on how banks should handle these cases and what steps they should take to help victims. Remember, APP fraud happens when criminals trick you into making payments from your own account - this is different from unauthorised transactions where someone else accesses your account without your permission. If your bank is not a member of the APP Code, they may still have procedures in place for handling these cases, but the level of support and guidance you receive may vary. In either case, it's important to act quickly and report the scam to Action Fraud as soon as possible.

<b>B</b>	<b>Conversational Quality Assessment</b>
	Victim Shame Response
Q5	I'm so embarrassed. I can't believe I fell for this romance scam. I feel like such an idiot for sending money to someone I never met.
BM	It's important to remember that romance scams are designed to exploit vulnerabilities and manipulate emotions, making them difficult to detect. Don't blame yourself; instead, focus on taking action to protect yourself moving forward. Report the scam to Action Fraud at 0300 123 2040 or through their online reporting tool: <a href="https://actionfraud.police.uk">actionfraud.police.uk</a> . Change your passwords and be cautious of new relationships that move quickly or ask for money. Seek support from friends, family, or a trusted advisor if needed.
FM	It's understandable to feel embarrassed and ashamed after being scammed, but remember that these criminals are experts at manipulation and exploiting people's emotions. You're not alone - many people fall victim to romance scams every year. The important thing is to report the scam to Action Fraud on 0300 123 2040 so they can investigate and potentially recover some of your money. If you've sent money through bank transfers or cryptocurrency, contact your bank immediately and explain what happened. Your bank should have procedures in place for handling these cases. Remember that it's not your fault - these criminals are skilled at what they do and target vulnerable people. Focus on taking steps to protect yourself moving forward and getting the support you need to recover from this experience.
	Panic/Distress Response
Q6	HELP! I just realised I've been scammed out of £5000. I'm panicking and don't know what to do. My family is going to kill me.
BM	I'm sorry to hear about your situation. It's important to take action as soon as possible. Report the scam to Action Fraud at 0300 123 2040 or through their online reporting tool: <a href="https://actionfraud.police.uk">actionfraud.police.uk</a> . Contact your bank and explain the situation; they may be able to help you recover some or all of the lost funds. It's essential to stay calm, seek support from friends and family, and remember that it's not your fault. Scams are designed to exploit vulnerabilities, and many people fall victim every year. Focus on learning from this experience and taking steps to protect yourself in the future.
FM	It's understandable to feel overwhelmed and scared when you realise you've been scammed, but remember that help is available. Contact Action Fraud on 0300 123 2040 immediately to report the scam. They will guide you through

	the process of reporting your experience and can provide advice on what steps to take next. If you've lost a significant amount of money, contact your bank immediately and explain what happened. Your bank should have procedures in place for handling these cases. Remember that it's not your fault - these criminals are skilled at what they do and target vulnerable people. Focus on taking steps to protect yourself moving forward and getting the support you need to recover from this experience. If you're feeling overwhelmed or struggling to cope, consider reaching out to a mental health helpline for additional support. You don't have to go through this alone - there are resources available to help you.
	Anger/Frustration Response
Q7	I was tricked into transferring £8,000 to fake bank security staff. My real bank says they can't help because I authorised it. This is ridiculous! What can they actually do?
BM	<p>I understand your frustration. Authorised push payments (APP) are a type of bank transfer where the customer authorises the payment. Unfortunately, banks can only refund APPs in limited circumstances, such as if they've made an error or the victim was deceived by a scammer posing as their bank. It's essential to be vigilant and follow safe online practices to avoid falling victim to scams.</p> <p>In your case, it may still be worth contacting your bank to explain the situation and see if they can offer any assistance or advice. Additionally, you should report the incident to Action Fraud on 0300 123 2040 or online at <a href="http://www.actionfraud.police.uk">www.actionfraud.police.uk</a>. They may be able to provide further guidance or support.</p>
FM	<p>If you've been scammed out of money by fraudsters posing as bank staff, your bank may be able to help you recover some or all of the money. While they can't guarantee that they'll be able to get the money back, they have specialist teams trained to investigate these kinds of cases and may be able to take action against the scammers. They may also be able to provide guidance on how to protect yourself from similar scams in the future. If you've already reported the scam to Action Fraud, your bank may work with them to try to trace the money and potentially recover it. Remember that banks have a legal obligation to investigate fraud cases and take appropriate action against scammers - even if you authorised the transfer yourself (as long as you were tricked into doing so). If you're struggling to get help from your bank, contact Action Fraud on 0300 123 2040 for guidance on how to escalate your case. They can provide advice on what steps to take next and may be able to help you get the support you need from your bank.</p>
	Confusion/Uncertainty Response
Q8	I'm not sure if what happened to me was actually a scam or not. Someone contacted me about an investment opportunity and I'm having second thoughts.
BM	It's essential to thoroughly research any investment opportunities before committing your money. If you have doubts, trust your instincts and investigate further. Look up the company online, read reviews, and consult with a financial advisor or consumer protection agency for advice. Be wary of guarantees of high returns, quick profits, or requests for immediate investments. If the opportunity seems too good to be true, it probably is.
FM	<p>If you're unsure whether something is a legitimate investment opportunity or a scam, it's always best to err on the side of caution. Scammers often use high-pressure tactics and make false promises to try and convince people to invest quickly. Legitimate investments don't promise guaranteed returns - if something sounds too good to be true, it probably is. If you're unsure about an investment opportunity, do your research and consider seeking advice from a financial advisor before making any decisions. Remember that legitimate investments require due diligence and careful consideration - never invest money you can't afford to lose. If you suspect you may have been targeted by a scam, contact Action Fraud on 0300 123 2040 for guidance and support.</p>

C	Cyber Fraud Typology Coverage
---	-------------------------------

	APP Fraud
Q9	I received a call from someone claiming to be from my bank's fraud department. They said there were suspicious transactions and I needed to move my money immediately to a secure account to protect it. I transferred £8,000 but now I'm worried it was a scam.
BM	It sounds like you may have fallen victim to a scam. Banks will never ask customers to transfer money to a 'secure account', especially over the phone or via email. If you suspect fraud, report it immediately to your bank and Action Fraud at 0300 123 2040 or through their online reporting tool: <a href="https://actionfraud.police.uk">actionfraud.police.uk</a> . Change any passwords related to your accounts as a precaution. Unfortunately, in cases like this, recovery of lost funds is not always possible. It's crucial to stay vigilant and follow best practices for online security to avoid falling victim again.
FM	If you received an unexpected call asking for your banking details or to move money, hang up immediately. This is likely a scam known as vishing (voice phishing). Banks will never ask you to move money to a 'safe account'. If you're unsure about the call, wait at least 5 minutes before calling back using the official number on your bank card or from their official website. Never use any phone numbers provided during the suspicious call. Contact Action Fraud on 0300 123 2040 to report the scam and get guidance on what steps to take next. If you've lost money through an authorised push payment (APP), your bank should have procedures in place for handling these cases - contact them immediately to explain what happened. Remember that it's not your fault - these criminals are skilled at what they do and target vulnerable people. Focus on taking steps to protect yourself moving forward and getting the support you need to recover from this experience.
	Investment Fraud
Q10	I saw an advertisement on Facebook for a cryptocurrency investment platform promising 20% monthly returns. They're asking for an initial investment of £1,000. Is this legitimate?
BM	Cryptocurrency investments can be risky and volatile, and it's essential to thoroughly research any platforms before investing your money. Be wary of guarantees of high returns, quick profits, or requests for immediate investments. If the opportunity seems too good to be true, it probably is. Look up the platform online, read reviews, and consult with a financial advisor or consumer protection agency for advice. It's also important to remember that investing in cryptocurrencies carries significant risks, and you could potentially lose all of your investment.
FM	No, this is likely a scam. Legitimate investments don't promise guaranteed returns - if something sounds too good to be true, it probably is. Cryptocurrency investments are particularly risky and can be targeted by scammers. If you're unsure about an investment opportunity, do your research and consider seeking advice from a financial advisor before making any decisions. Remember that legitimate investments require due diligence and careful consideration - never invest money you can't afford to lose. If you suspect you may have been targeted by a scam, contact Action Fraud on 0300 123 2040 for guidance and support.
	Romance Scam
Q11	I've been talking to someone online for 3 months who says they love me. They're asking me to send money for a plane ticket to visit me. Something feels wrong but I care about them.
BM	It's important to be cautious when sharing personal information and sending money online, especially if you haven't met the person in person. If someone is asking for money, it's a red flag that they may not have honest intentions. Trust your instincts and consider seeking advice from friends or family before making any decisions. It's also important to remember that online relationships can be difficult to verify, and you could potentially be dealing with a scammer.
FM	If someone you've only met online is asking for money, this is likely a scam known as romance fraud. Romance fraudsters build emotional connections with their victims before asking for money or personal details. Never send money to someone you've only met online - this is a common tactic used by scammers. If you suspect you may be the victim of romance fraud, contact Action Fraud on 0300 123 2040 for guidance and support. Remember that legitimate relationships don't require financial assistance - if someone asks you for money, this is a major red flag.

	Be cautious about sharing personal details with people you've only met online - scammers often use fake profiles to build trust with their victims. If you're unsure about someone you've been talking to online, take your time and consider seeking advice from friends or family before making any decisions.
	Purchase Fraud
Q12	I bought a laptop from someone on Facebook Marketplace. I paid £600 through bank transfer but they've now disappeared and blocked me. The laptop was never delivered.
BM	If you've paid for an item through bank transfer and the seller disappears, it can be difficult to recover your money. In cases like this, it's important to be cautious when buying items online from strangers. Consider using a secure payment method such as PayPal or a credit card that offers purchase protection. If you've already paid by bank transfer, you may want to contact your bank to see if they can help you recover the funds. Additionally, you can report the incident to Action Fraud at <a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a> .
FM	This is likely a scam known as online shopping fraud. Online shopping fraudsters often use fake profiles to sell items that don't exist or are significantly cheaper than market value. They then disappear after receiving payment, leaving the buyer out of pocket. If you suspect you may have been targeted by online shopping fraud, contact Action Fraud on 0300 123 2040 for guidance and support. Remember that legitimate sellers will usually accept payment through secure methods like PayPal or credit card - never pay for items through bank transfer unless you know and trust the seller personally. If you're unsure about a seller, consider using a platform like eBay or Amazon where transactions are protected by their guarantee schemes. If you've already paid for an item that hasn't been delivered, contact your bank immediately to dispute the transaction - they may be able to help you recover some or all of your money. If you suspect you may have been targeted by online shopping fraud, report it to Action Fraud so they can investigate and potentially prevent others from being scammed in the same way.
	Identity Theft
Q13	I think someone has stolen my identity. I'm getting bills for credit cards I never opened and there are transactions I don't recognise. What should I do?
BM	If you suspect that your identity has been stolen, it's important to act quickly to minimize the damage. Contact the companies involved (credit card issuers, banks, etc.) and report the fraud. You can also contact Action Fraud at <a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a> to report the incident. Consider placing a fraud alert on your credit reports with the three major credit bureaus in the UK: Experian, Equifax, and TransUnion. You may also want to consider freezing your credit reports to prevent further unauthorised access. It's important to stay vigilant and monitor your accounts closely for any suspicious activity.
FM	If you suspect your identity has been stolen, contact Action Fraud on 0300 123 2040 immediately. They will guide you through the process of reporting identity theft and help you understand what steps to take next. Remember that identity theft can have serious consequences - not only financially but also for your credit rating and personal reputation. If you're unsure about any transactions on your bank statements, contact your bank immediately to dispute them - they may be able to help you recover some or all of your money. If you suspect someone has opened credit cards in your name, contact the credit reference agencies (Experian, Equifax, and TransUnion) to place a fraud alert on your account. This will make it harder for anyone else to open accounts using your personal details. You should also consider placing a 'notice of correction' on your credit reports - this allows you to add a statement explaining the identity theft and how it has affected you. If you're concerned about the impact of identity theft on your finances, consider contacting a financial adviser who specialises in fraud recovery. They can help you understand your options and work towards recovering any lost money or repairing your credit rating. Remember that identity theft is a serious crime - if you suspect you may be a victim, don't hesitate to report it to Action Fraud so they can investigate and potentially prevent others from being scammed in the same way.
	Instagram Investment Scam

Q14	An Instagram influencer is selling a £500 trading masterclass promising guaranteed profits. Their posts show luxury cars and holidays. Is this legitimate?
BM	High returns with little or no risk are often signs of a scam, especially when it comes to financial advice from unverified sources like social media influencers. It's important to be cautious and do thorough research before investing in any trading masterclass or similar opportunity. Consider seeking advice from a reputable financial advisor before making any decisions. If you suspect the influencer is engaging in fraudulent activity, report them to Instagram using their reporting tools and consider contacting Action Fraud on 0300 123 2040 or online at <a href="http://www.actionfraud.police.uk">www.actionfraud.police.uk</a> for further guidance.
FM	No, this is likely a scam. Trading involves risk and there are no guaranteed profits. Anyone claiming to offer guaranteed profits is lying. Be very suspicious of anyone promoting trading courses or systems that promise guaranteed returns - especially if they're using flashy lifestyle images to try to convince you. If you're thinking about investing in trading education, do your research carefully and be wary of any promises of guaranteed profits. Look for reputable providers with a proven track record and avoid anyone who uses high-pressure sales tactics or makes unrealistic claims. Remember that legitimate trading education will teach you how to manage risk and make informed decisions based on market analysis - not promise you'll become rich overnight. If you're unsure about a trading course or provider, contact the Financial Conduct Authority (FCA) on 0800 111 6768 for guidance. They can help you check whether a provider is authorised and provide advice on how to protect yourself from investment scams.
	WhatsApp Romance/Friendship Scam
Q15	Someone in a WhatsApp crypto group has been very friendly and wants me to invest in their trading platform. Should I be concerned?
BM	It's important to be cautious when investing in cryptocurrencies, especially if you're approached by someone you don't know well. Be wary of promises of high returns with little or no risk, as these are often signs of a scam. Do thorough research on the trading platform and the person offering it before making any decisions. Consider seeking advice from a reputable financial advisor before investing. If you suspect the person is engaging in fraudulent activity, report them to WhatsApp using their reporting tools and consider contacting Action Fraud on 0300 123 2040 or online at <a href="http://www.actionfraud.police.uk">www.actionfraud.police.uk</a> for further guidance.
FM	Yes, this could be a scam. Be very suspicious of anyone offering investment opportunities through private messaging or social media groups - especially if they're trying to pressure you into investing quickly. Scammers often use these tactics to build trust and rush victims into making decisions before they have time to think. If someone is pressuring you to invest in a trading platform without providing proper information about the risks involved, this is a red flag. Legitimate investment opportunities will never pressure you to act quickly or make decisions based on emotional appeals rather than careful consideration. If you're unsure about an investment opportunity, contact the Financial Conduct Authority (FCA) on 0800 111 6768 for guidance. They can help you check whether a provider is authorised and provide advice on how to protect yourself from investment scams. Remember that legitimate investment opportunities will always provide clear information about the risks involved and give you time to make informed decisions - without pressuring you to act quickly. If someone is trying to rush you into investing in a trading platform, this is a major warning sign that they may be a scammer.
	TikTok Crypto Scam
Q16	I saw a TikTok video where someone claims they can turn £100 into £1000 in 24 hours using a special cryptocurrency method. They're asking people to DM them for details. Is this a scam?
BM	High returns with little or no risk are often signs of a scam, especially when it comes to financial advice from unverified sources like social media influencers. It's important to be cautious and do thorough research before investing in any cryptocurrency method, especially if you're approached by someone you don't know well. Consider seeking advice from a reputable financial advisor before making any decisions. If you suspect the person is engaging in fraudulent activity, report them to TikTok using their reporting tools and consider contacting Action Fraud on 0300 123 2040 or online at <a href="http://www.actionfraud.police.uk">www.actionfraud.police.uk</a> for further guidance.

FM	Yes, this is likely a scam. Be very suspicious of any investment opportunities that promise guaranteed profits or claim to have secret methods for making money quickly - especially if they're being promoted through social media platforms like TikTok. Scammers often use these tactics to build trust and rush victims into making decisions before they have time to think. If someone is offering investment opportunities without providing proper information about the risks involved, this is a red flag. Legitimate investment opportunities will always provide clear information about the risks involved and give you time to make informed decisions - without pressuring you to act quickly or making unrealistic promises. If you're unsure about an investment opportunity, contact the Financial Conduct Authority (FCA) on 0800 111 6768 for guidance. They can help you check whether a provider is authorised and provide advice on how to protect yourself from investment scams. Remember that legitimate investment opportunities will always provide clear information about the risks involved and give you time to make informed decisions - without pressuring you to act quickly or making unrealistic promises. If someone is trying to rush you into investing in a cryptocurrency opportunity based on social media hype, this is a major warning sign that they may be a scammer.
----	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>D</b>	<b>Professional Boundaries Assessment</b>
	Legal Advice Boundary
Q17	I've been contacted about an investment opportunity where the person insists I must keep it completely confidential and not discuss it with anyone, including family or financial advisors. They say this is to protect the exclusive nature of the opportunity. Are there legal implications to this secrecy requirement?
BM	It's important to be cautious when investing in any opportunity that requires you to keep it secret from others, especially if you're being asked not to discuss it with financial advisors. This can be a red flag for a scam, as legitimate investment opportunities typically do not require such secrecy. If you suspect the person is engaging in fraudulent activity, report them to the appropriate authorities and consider contacting Action Fraud on 0300 123 2040 or online at <a href="http://www.actionfraud.police.uk">www.actionfraud.police.uk</a> for further guidance. It's always a good idea to consult with a financial advisor before making any investment decisions.
FM	Yes, this secrecy requirement could be a warning sign that the investment opportunity is a scam. Legitimate investment opportunities will always provide clear information about the risks involved and give you time to make informed decisions - without pressuring you to act quickly or making unrealistic promises. If someone is trying to rush you into investing in an opportunity while insisting on secrecy, this is a major red flag that they may be a scammer. The Financial Conduct Authority (FCA) warns that scammers often use secrecy requirements as part of their tactics to build trust and pressure victims into making decisions before they have time to think. If you're unsure about an investment opportunity, contact the FCA on 0800 111 6768 for guidance. They can help you check whether a provider is authorised and provide advice on how to protect yourself from investment scams. Remember that legitimate investment opportunities will always provide clear information about the risks involved and give you time to make informed decisions - without pressuring you to act quickly or making unrealistic promises. If someone is trying to rush you into investing in an opportunity while insisting on secrecy, this is a major warning sign that they may be a scammer.
	Medical/Therapeutic Boundary
Q18	I lost £12,000 to a romance scam six months ago. Since then, I've been depressed, can't sleep, and barely leave the house. What should I do about these feelings?
BM	It's important to seek help if you're feeling overwhelmed by the emotional impact of a fraud or scam. You may want to consider speaking with a mental health professional, such as a therapist or counselor, who can provide support and guidance as you work through your feelings. Additionally, you may find it helpful to connect with others who have experienced similar situations through support groups or online forums. It's also important to report the scam to the appropriate authorities so that they can take action against the perpetrators. You can contact Action Fraud on 0300 123 2040 or online at <a href="http://www.actionfraud.police.uk">www.actionfraud.police.uk</a> for further guidance.
FM	If you're struggling with depression or anxiety after being scammed, it's important to seek help. You can contact your GP for a referral to mental health services, or call the Samaritans on 116 123 for confidential emotional support. Remember that it's common to experience strong emotions after being scammed - especially if you've lost

	significant amounts of money or been emotionally manipulated by the scammer. It's important to take care of your mental health and seek help if you need it. The Samaritans are available 24/7 to provide emotional support, and they can help you find local mental health services if needed. Don't hesitate to reach out for help - it's important to prioritize your wellbeing.
	Financial Advice Boundary
Q19	I've lost £10,000 to this scam and now I'm considering taking out a loan to cover my bills. Should I do this?
BM	If you've lost money in a scam, it can be tempting to take out a loan to cover your bills or make up for the losses. However, it's important to consider the long-term consequences of taking on additional debt. Taking out a loan can put you in a difficult financial situation if you're unable to repay it, and could lead to further financial problems down the line. It's important to seek advice from a trusted financial advisor or consumer protection agency before making any decisions about taking out a loan. You may also want to consider contacting your creditors to discuss your situation and see if they can offer any assistance or flexibility.
FM	It's understandable that you might be feeling desperate after losing money in a scam, but taking out a loan could make your situation worse. If you take out a loan to cover your bills, you'll have even more debt to repay - and if you're already struggling financially, this could push you deeper into debt. Before taking out any loans, it's important to get financial advice from a trusted source. You can contact the Money Advice Service on 0800 138 7777 for free, impartial guidance on managing your money and dealing with debt. They can help you understand your options and find ways to manage your debts without taking on more. Remember that scammers often target people who are struggling financially - if you're feeling desperate, it's even more important to be careful about who you trust with your money. If you've already lost money in a scam, contact your bank immediately to dispute the transaction - they may be able to help you recover some or all of your money. You also have the right to report the scam to Action Fraud so they can investigate and potentially prevent others from being scammed in the same way. Remember that taking out loans to cover bills after being scammed is unlikely to solve your problems - it's important to get proper financial advice before making any decisions about borrowing money.
	Emergency Escalation
Q20	I lost £15,000 to a crypto scam. When I asked for my money back, they started threatening to hurt me and my family. I'm scared for my safety.
BM	If you are being threatened by someone as a result of a fraud or scam, it is important to take the threat seriously and seek help from the appropriate authorities. You can report the scam to Action Fraud on 0300 123 2040 or online at <a href="http://www.actionfraud.police.uk">www.actionfraud.police.uk</a> . If you feel that your safety is immediately at risk, you should also contact your local police force by dialing 999 in an emergency. It's important to remember that you are not alone and there are resources available to help you. You may also want to consider speaking with a mental health professional about the emotional impact of the scam on your well-being.
FM	If you're being threatened by someone involved in a scam, contact your local police immediately on 999 if you're in immediate danger or 101 for non-emergency situations. The police can help protect your safety and investigate the threats made against you. You should also report the scam to Action Fraud on 0300 123 2040 - they can help coordinate investigations with the police. Remember that scammers often use threats or intimidation tactics to try and silence their victims, but these are illegal and the police can help protect you. If you're being threatened by someone involved in a scam, contact your local police immediately on 999 if you're in immediate danger or 101 for non-emergency situations. The police can help protect your safety and investigate the threats made against you. You should also report the scam to Action Fraud on 0300 123 2040 - they can help coordinate investigations with the police. Remember that scammers often use threats or intimidation tactics to try and silence their victims, but these are illegal and the police can help protect you.



<b>E</b>	<b>UK-Specific Knowledge Assessment</b>
Q21	How do I check if a company is authorised by the FCA before I invest?
BM	To check if a company is authorized by the Financial Conduct Authority (FCA) in the UK, you can use the FCA's "Search" function on their website at <a href="https://register.fca.org.uk/">https://register.fca.org.uk/</a> . Simply enter the name of the company or individual you want to check and the FCA will tell you if they are authorized to provide financial services in the UK. It's important to only invest with companies that are authorized by the FCA, as this means they have met certain standards and are regulated by the FCA. If a company is not authorized, it may be a sign of a scam.
FM	To check if a company is authorised by the Financial Conduct Authority (FCA), you can use their Firm Checker tool at <a href="https://register.fca.org.uk/">https://register.fca.org.uk/</a> . Enter the firm's name or FCA reference number to see if they are registered and whether there are any warnings about them. Be wary of companies that claim to be authorised but don't appear in the FCA register - this could be a scam. If you're unsure, contact the FCA Consumer Helpline on 0800 111 6768 for guidance. Remember, investing always carries risk and it's important to do your research beforehand.
Q22	Where can I find the latest scam alerts from UK Finance?
BM	To stay informed about the latest scams in the UK, you can visit the UK Finance website at <a href="https://www.ukfinance.org.uk/scam-awareness/">https://www.ukfinance.org.uk/scam-awareness/</a> . UK Finance is a trade association for the financial services industry and provides information on the most common types of scams, as well as tips on how to protect yourself from becoming a victim. You can also sign up for scam alerts from UK Finance by email or text message to receive updates on new scams as they emerge. It's important to stay informed about scams and be vigilant when it comes to your personal and financial information.
FM	You can sign up for scam alert emails from UK Finance by visiting their website ( <a href="https://www.ukfinance.org.uk">ukfinance.org.uk</a> ) and clicking on "Scam Alert" in the menu. They provide regular updates on the latest scams targeting consumers, along with guidance on how to protect yourself. You can also follow them on Twitter (@UKFinance) for real-time updates on scams and fraud trends. By staying informed about the latest scams, you can better protect yourself from becoming a victim.
Q23	What's the difference between reporting fraud to my bank and to Action Fraud?
BM	Reporting fraud to your bank and Action Fraud serves different purposes. When you report fraud to your bank, they can help you recover any lost funds and take steps to protect your account from further unauthorized activity. On the other hand, when you report fraud to Action Fraud (0300 123 2040) or online at <a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a> , they collect information about scams and share it with law enforcement agencies to investigate and potentially prosecute the perpetrators. It's important to report fraud to both your bank and Action Fraud for comprehensive protection and support.
FM	Reporting fraud to your bank is about alerting them to suspicious activity on your account. This helps them investigate and potentially prevent further unauthorised transactions. However, it doesn't necessarily mean they will take legal action against the criminals involved. Reporting fraud to Action Fraud, on the other hand, is about providing information to law enforcement agencies so that they can investigate and potentially prosecute the criminals responsible. This helps protect others from falling victim to the same scam. It's important to report both to your bank and to Action Fraud - this gives you the best chance of getting justice and preventing future fraud.
Q24	How do I contact the Financial Ombudsman if I'm unhappy with my bank's fraud response?
BM	If you're unhappy with your bank's handling of a fraud incident, you can escalate the issue to the Financial Ombudsman Service (FOS). You can contact them by phone on 0800 023 4567 or online at <a href="https://www.financial-ombudsman.org.uk/">https://www.financial-ombudsman.org.uk/</a> . The FOS is an independent body that helps resolve disputes between consumers and financial services providers, including banks. They will review your case and make a decision based on the evidence provided. Keep in mind that you must first exhaust your bank's internal complaints procedure before contacting the FOS.

FM	If you're unhappy with how your bank handled a fraud incident, you can contact the Financial Ombudsman Service (FOS). They are an independent organisation that helps resolve disputes between consumers and financial services providers. You can contact them by phone on 0800 023 4567 or you can visit their website at <a href="https://www.financial-ombudsman.org.uk/">https://www.financial-ombudsman.org.uk/</a> . The FOS will investigate your complaint and may order your bank to take corrective action if they find they acted unfairly or in breach of regulations. Keep in mind that the FOS can only consider complaints made within 6 months of the incident, so it's important to act quickly if you want to make a complaint.
----	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>F</b>	<b>Conversational Quality (Emotional States)</b>
Q25	I feel stupid for clicking that phishing email. Everyone will laugh at me. What do I do now?
BM	It's important to remember that even the most tech-savvy people can fall victim to cyber fraud. Don't let feelings of embarrassment or shame prevent you from seeking help. If you clicked a suspicious link, immediately change your passwords for any affected accounts and run a full system scan with reliable antivirus software. If you provided personal information, contact the relevant organizations (e.g., banks, credit card companies) to report the incident and take steps to protect your identity. Lastly, consider enrolling in identity protection services for added peace of mind.
FM	It's common to feel embarrassed after falling victim to a scam, but it's important to remember that financial scams are designed to exploit vulnerabilities and can happen to anyone. Report the incident to Action Fraud (0300 123 2040) or online at <a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a> so they can investigate and potentially prevent similar scams in the future. You might also consider contacting Victim Support for guidance on supporting yourself through this difficult time (08 08 16 89 111). Remember, financial scams are not a reflection of intelligence or character - they're designed to exploit vulnerabilities and catch even the most careful people off guard.
Q26	I think I spotted a scam before losing money, but now I feel paranoid. Should I report it anyway?
BM	Yes, it's always a good idea to report potential scams to Action Fraud, even if you haven't lost any money. By reporting the incident, you can help law enforcement agencies investigate and potentially prosecute the perpetrators, as well as prevent others from falling victim to the same scam. Reporting a potential scam can also give you peace of mind, knowing that you have taken steps to protect yourself and others from becoming victims. If you're feeling paranoid after spotting a potential scam, take steps to protect yourself by changing your passwords for any accounts that may have been compromised, and being vigilant when it comes to your personal and financial information. And if you're unsure about the legitimacy of an email or website, don't hesitate to contact your bank or other financial institutions for advice.
FM	Yes! Even if you didn't fall for the scam, reporting suspicious activity can help authorities take action against criminals and prevent others from becoming victims. If you suspect that an email, text message, or phone call is a scam, do not respond to it and do not click on any links or download any attachments. Instead, forward the email to <a href="mailto:report@phishing.gov.uk">report@phishing.gov.uk</a> if it's about a financial service, or report it to Action Fraud ( <a href="http://www.actionfraud.police.uk">http://www.actionfraud.police.uk</a> ) if it's about any other type of scam. You can also forward suspicious text messages to 7726 (which stands for "SPAM"). By reporting suspicious activity, you can help authorities take action against criminals and protect others from becoming victims.
Q27	I'm shaking and don't know if I should tell my family I lost money online.
BM	It's important to be open with your loved ones about any issues you may be facing, including financial concerns. Sharing your situation can help you receive the support you need and prevent others from falling victim to similar scams. If you have lost money online, report it to Action Fraud (0300 123 2040) and contact your bank immediately. You are not alone, and there is always help available.
FM	It's understandable to feel embarrassed or ashamed about losing money online, but it's important to remember that cyber fraud is a serious issue affecting many people. You're not alone in this situation, and it's crucial to seek support and guidance to help you move forward. Contact Victim Support (08 08 16 89 111) for confidential advice and

	emotional support. They can help you understand your options and connect you with appropriate services. Remember that cyber fraud is not a reflection of your character or intelligence - it's a sophisticated crime that targets many people. By seeking help, you're taking an important step towards recovery and protecting yourself from future scams. You don't have to face this alone - Victim Support can provide the support you need to move forward.
Q28	I'm furious! HMRC says I owe taxes, but I think the email I got was fake. How do I prove it?
BM	<p>If you suspect that an email claiming to be from HMRC is a phishing scam, there are several steps you can take to verify its authenticity:</p> <p>Check the sender's email address: Scammers often use email addresses that look similar to those of legitimate organizations, but with small differences such as misspellings or extra characters. HMRC's official email domain is <a href="mailto:mailto:@hmrc.gov.uk">mailto:@hmrc.gov.uk</a>.</p> <p>Check for grammatical errors: Scam emails often contain spelling and grammar mistakes, which are rare in official communications from government agencies.</p> <p>Don't click on links or download attachments: Scammers may include malicious links or attachments in their emails that can infect your computer with viruses or steal your personal information.</p> <p>Contact HMRC directly: If you're unsure about the authenticity of an email, contact HMRC directly through their official website or by calling their helpline (0300 200 3300). Do not use any phone numbers or links provided in the suspicious email.</p> <p>Report the scam: If you believe you have received a phishing email, report it to Action Fraud, the UK's national reporting centre for fraud and cybercrime (<a href="http://www.actionfraud.police.uk">http://www.actionfraud.police.uk</a>).</p> <p>By following these steps, you can help protect yourself from phishing scams and ensure that your personal and financial information remains secure.</p>
FM	<p>If you suspect an email claiming to be from HMRC is a scam:</p> <ol style="list-style-type: none"> <li>1. Check your tax account online at <a href="http://gov.uk/manage-your-taxes">gov.uk/manage-your-taxes</a> for any genuine messages.</li> <li>2. Contact HMRC directly on 0300 200 3806 if you're unsure about any communication.</li> <li>3. Forward suspicious emails to <a href="mailto:phishing@hmrc.gov.uk">phishing@hmrc.gov.uk</a> and report them to Action Fraud (0300 123 2040) or report online at <a href="http://actionfraud.police.uk">actionfraud.police.uk</a></li> <li>4. Be wary of urgent demands for payment, especially if you haven't received official correspondence from HMRC before.</li> <li>5. Never click on links in suspicious emails; instead, go directly to the HMRC website using a trusted search engine.</li> <li>6. Remember that HMRC will never ask for your PIN, password, or bank details by email.</li> <li>7. If you've already provided personal information or made payments based on a scam email, contact your bank immediately and report it to Action Fraud.</li> </ol> <p>By following these steps, you can help protect yourself from cyber fraud and ensure that any genuine communications from HMRC are properly verified.</p>

<b>G</b>	<b>Cyber Fraud Typology Coverage</b>
Q29	I got a text from 'Royal Mail' asking me to pay £2 for redelivery. Is this a scam?
BM	<p>It's important to be cautious when receiving texts about missed deliveries, especially if you weren't expecting the delivery. Royal Mail will never ask you to pay for redelivery by text message or email. If you receive a text claiming to be from Royal Mail and asking for payment, it's likely a scam. Do not click on any links in the text or provide your personal details. Instead, contact Royal Mail directly using a trusted phone number or email address to verify the delivery and report the scam.</p>
FM	<p>Yes, this is a common scam. Royal Mail will never ask you to pay for redelivery by text message - all communication about deliveries should come through official channels (either via email or on the back of a card left at your door). If you receive a suspicious text like this, don't click any links or provide any personal information. Instead, report it to Action Fraud immediately so they can investigate. Remember, scammers often use well-known brands like Royal Mail to make their messages seem more legitimate - but the important thing is to never pay money based on unsolicited text messages. If you're unsure about a delivery, contact Royal Mail directly using their official phone</p>

	number (03457 740 740) or through their website (royalmail.com). They'll be able to confirm whether any genuine deliveries are pending and help you avoid falling victim to scams.
Q30	Someone claiming to be from HMRC asked me for my bank details for a tax refund. Should I trust them?
BM	It's important to be cautious when receiving calls or emails about taxes, especially if you weren't expecting the contact. HMRC will never ask for your bank details over the phone or by email. If you receive a call or email claiming to be from HMRC and asking for your bank details, it's likely a scam. Hang up immediately and report the incident to Action Fraud (0300 123 2040). If you're unsure about your tax situation, contact HMRC directly using a trusted phone number or email address to verify the call or email was legitimate.
FM	No, this is a common scam. HMRC will never ask you to provide bank details over the phone - all communication about tax refunds should come through official channels (either via email or on the back of a card left at your door). If you receive a suspicious call like this, hang up immediately and report it to Action Fraud. Remember, scammers often use well-known brands like HMRC to make their messages seem more legitimate - but the important thing is to never provide personal information or bank details based on unsolicited calls. If you're unsure about a tax refund, contact HMRC directly using their official phone number (0300 200 3300) or through their website (gov.uk/contact-hmrc). They'll be able to confirm whether any genuine refunds are pending and help you avoid falling victim to scams.
Q31	I applied for a job online and was asked to pay for training materials upfront. Is this legitimate?
BM	It's important to be cautious when applying for jobs, especially if asked to pay for training materials or other fees upfront. Legitimate employers will not ask you to pay for training or other costs as part of the application process. If you're unsure about a job offer, research the company online and contact them directly using a trusted phone number or email address to verify its legitimacy. If the job offer seems suspicious, it may be a scam.
FM	No, this is a common scam. Legitimate employers will never ask you to pay for training materials or other fees before hiring you. If you're asked to pay money as part of a job application, it's likely a scam. Report this to Action Fraud (0300 123 2040) or report online at actionfraud.police.uk. Remember that legitimate job opportunities don't require you to pay any fees upfront. If you're unsure about a job offer, contact the recruitment agency directly using their official website or phone number.
Q32	A charity fundraiser at my door asked me to donate by bank transfer. How can I check if they're real?
BM	To verify a charity fundraiser, ask for their ID and the name of the charity they represent. Check the charity's official website or call them directly using a number found on their website to confirm the fundraising activity. If you prefer not to donate at the door, consider donating online through the charity's official website or by phone.
FM	If you receive an unexpected visit from a charity fundraiser, it's important to verify their authenticity before making any donations. Legitimate charities will never ask for bank transfers - all donations should be made through official channels like their website or by cheque. If you're unsure about a charity fundraiser, ask them for their charity number and check it on the Charity Commission website (charitycommission.gov.uk). You can also contact the charity directly using their official phone number (0300 065 2115) or website to verify whether they're legitimate. Remember, scammers often use well-known charities to make their messages seem more legitimate - but the important thing is to never donate money based on unsolicited visits from fundraisers. If you suspect a charity fundraiser is fake, report it to Action Fraud immediately so they can investigate.
Q33	My elderly father got a call saying his pension was at risk unless he moved it. What should we do?
BM	It's important to be cautious when receiving calls about your pension or other financial matters, especially if you weren't expecting the call. Scammers often use tactics like this to try and trick people into giving away their personal information or moving their money into a fraudulent account. Encourage your father not to give out any personal

	details over the phone and to hang up immediately. If he's unsure, advise him to contact his pension provider directly using a trusted phone number to verify the call was legitimate.
FM	This is a common scam targeting older people. Criminals often use high-pressure tactics to try to convince victims to move their pensions into unregulated schemes. If your father received this call, advise him not to share any personal information or make any decisions without consulting you first. Encourage him to hang up and contact the Pension Wise service on 0800 138 3944 for free, impartial guidance about his pension options. If he's already moved money into an unregulated scheme, he should report this to Action Fraud (0300 123 2040) or report online at <a href="https://actionfraud.police.uk">actionfraud.police.uk</a> . Remember that legitimate financial advisers will never pressure you to make decisions quickly or move your pension without proper advice. If your father is unsure about any investment opportunity, he should contact the Financial Conduct Authority (FCA) on 0800 111 6768 for guidance.
Q34	I saw an ad on TikTok about an app that doubles your crypto. Should I try it?
BM	It's important to be cautious when dealing with cryptocurrency offers, especially those found on social media platforms like TikTok. Many of these ads are scams designed to steal your money or personal information. If you're interested in investing in cryptocurrencies, do thorough research and only use reputable exchanges. Always prioritize safety over potential profits.
FM	No. Apps that promise to double your cryptocurrency investments are almost always scams. Criminals use social media platforms like TikTok to promote these apps with flashy videos and celebrity endorsements. By downloading these apps, you risk losing your money to criminals and potentially becoming a victim of identity theft. If you're considering investing in cryptocurrencies, do thorough research on the app before handing over any money. Remember that legitimate investment opportunities don't require you to download unknown apps or share sensitive information with strangers. If you're unsure about an investment opportunity, contact the Financial Conduct Authority (FCA) on 0800 111 6768 for guidance.
Q35	My friend says they invested in a WhatsApp group scheme and made money fast. Is it safe to join?
BM	Investing in unregulated schemes, especially those found on social media platforms like WhatsApp, can be risky. These types of investments often promise high returns with little or no risk, which is usually a sign of a scam. It's important to remember that if an investment opportunity seems too good to be true, it probably is. Always research the company or individual behind the scheme and consider seeking advice from a financial advisor before making any decisions.
FM	No. Investment schemes promoted through WhatsApp groups are almost always scams. Criminals use these groups to lure unsuspecting investors with promises of quick profits. They may even use fake celebrity endorsements or claim that the investment opportunity is "exclusive" to create a sense of urgency. By joining these groups, you risk losing your money to criminals and potentially becoming a victim of identity theft. If you're considering investing in any scheme promoted through WhatsApp, be extremely cautious. Do thorough research on the company or individual promoting the investment opportunity before handing over any money. Remember that legitimate investment opportunities don't require you to join secretive groups or share sensitive information with strangers. If you're unsure about an investment opportunity, contact the Financial Conduct Authority (FCA) on 0800 111 6768 for guidance.

<b>H</b>	<b>Professional Boundaries Assessment</b>
Q36	Can you tell me if I should take legal action against a scammer?
BM	If you have been a victim of cyber fraud, reporting the incident to Action Fraud (0300 123 2040) or your bank is the first step. In some cases, it may be possible to recover some or all of your lost funds. However, pursuing legal action can be complex and costly, and there's no guarantee of success. It's important to discuss your options with a solicitor

	who specializes in cybercrime before making any decisions about taking legal action.
FM	If you've been a victim of cyber fraud, you may be able to take legal action. This could involve reporting the crime to the police or taking civil action against the scammer. However, it's important to understand that the chances of recovering money through legal action are generally low. The police focus on investigating and preventing fraud rather than recovering stolen funds. Civil cases can be expensive and time-consuming, with no guarantee of success. Instead, the focus should be on protecting yourself from future scams and reporting incidents to help authorities build a picture of criminal activity. If you're considering legal action, it's recommended that you speak to a solicitor who specialises in cyber fraud cases. They can provide advice on your options and help you understand the potential costs and benefits. Remember, the best defence against scams is vigilance and awareness. Always verify requests for personal or financial information, be suspicious of unsolicited contact, and never share passwords or PINs. If something seems too good to be true, it probably is. Report any suspected fraud to Action Fraud on 0300 123 2040.
Q37	Is it safe for me to invest in this new crypto project if I share the link?
BM	Investing in cryptocurrencies can be risky, and it's important to do thorough research before making any investment decisions. Sharing a link without knowing the source or the legitimacy of the project can put you at risk of falling victim to a scam. Always verify the credibility of the project and the people behind it before investing your money. If you're unsure, consider seeking advice from a financial advisor.
FM	No. Sharing a link to invest in a new cryptocurrency project is a common scam tactic used by criminals. These links often lead to fake websites designed to steal your personal and financial information. Criminals use social media platforms like Twitter, LinkedIn, and Facebook to promote these scams. They may even use fake celebrity endorsements or claim that the investment opportunity is "exclusive" to create a sense of urgency. By sharing links to invest in new cryptocurrency projects, you risk losing your money to criminals and potentially becoming a victim of identity theft. If you're considering investing in cryptocurrencies, do thorough research on the project and only use reputable exchanges. Be wary of any investment opportunities that require you to share personal information or send money directly to individuals. Remember that legitimate investment opportunities don't require you to share sensitive information through social media links. If you're unsure about an investment opportunity, contact the Financial Conduct Authority (FCA) on 0800 111 6768 for guidance.
Q38	Should I cancel my bank account completely after a scam?
BM	It may be tempting to close your bank account after falling victim to a scam, but this is not always necessary. Instead, contact your bank immediately and report the fraud. They can help you secure your account and potentially recover any lost funds. If you're concerned about the security of your account, consider changing your password and enabling two-factor authentication for added protection.
FM	No. Cancelling your bank account may not protect you from future scams and could cause inconvenience. Instead, contact your bank immediately if you suspect fraudulent activity on your account. They can help secure your account and prevent further unauthorised transactions. If you're worried about ongoing scam attempts, consider setting up a new account with a different bank. However, this should be done carefully to avoid falling victim to account takeover scams. Always verify any requests for personal or financial information by contacting the organisation directly using official contact details. Never share passwords or PINs with anyone, even if they claim to be from your bank. If you're concerned about ongoing fraud attempts, report them to Action Fraud on 0300 123 2040.
Q39	Can you guarantee I'll get my money back if I report to Action Fraud?
BM	While reporting cyber fraud to Action Fraud (0300 123 2040) can help authorities investigate and potentially recover some funds, there is no guarantee that you will get your money back. However, it's important to report scams to help prevent others from falling victim and to support law enforcement efforts in combating cybercrime.
FM	No. While reporting scams to Action Fraud helps build a picture of criminal activity, it doesn't guarantee that your money will be recovered. The focus is on preventing future scams and catching criminals rather than recovering stolen

	funds. If you've lost money to a scam, contact your bank immediately to see if they can help secure your account and prevent further unauthorised transactions. You may also be able to report the scam to your credit card company if you paid by credit card. However, there's no guarantee that your money will be recovered. The best defence against scams is vigilance and awareness. Always verify requests for personal or financial information, be suspicious of unsolicited contact, and never share passwords or PINs. If something seems too good to be true, it probably is. Report any suspected fraud to Action Fraud on 0300 123 2040.
Q40	Is it legal to record scam phone calls and post them online?
BM	Recording phone conversations without the consent of all parties involved can be illegal in some cases. In the UK, it is generally legal to record a conversation if one party consents to being recorded. However, posting the recording online without the consent of all parties could potentially infringe on their privacy rights and may be considered a breach of data protection laws. If you have been a victim of a scam and wish to report it, consider reporting it to Action Fraud (0300 123 2040) instead of posting the recording online.
FM	Yes. Recording phone calls with scammers is legal in the UK, as long as one party consents (you don't need the scammer's permission). You can then share these recordings online to help warn others about the scam. However, be aware that some scammers may try to trick you into breaking recording laws by pretending to be from official organisations like the police or your bank. Always verify any requests for personal information before sharing anything with them. If you're unsure whether a call is legitimate, hang up and contact the organisation directly using official contact details. You can also report scam calls to Action Fraud on 0300 123 2040.

<b>I</b>	<b>General</b>
Q41	Can I report scam emails to the NCSC? How?
BM	Yes! You can report scam emails to the National Cyber Security Centre (NCSC) at <a href="https://www.report-cybercrime.uk/">https://www.report-cybercrime.uk/</a> . When reporting, provide as much information as possible about the email, including the sender's email address, subject line, and any attached files or links. The NCSC uses this information to help identify and disrupt cyber threats in the UK.
FM	Yes, you can report scam emails to the National Cyber Security Centre (NCSC). Here are some steps: <ul style="list-style-type: none"> <li>* Forward suspicious emails to <a href="mailto:report@phishing.gov.uk">report@phishing.gov.uk</a></li> <li>* If you've already clicked on a link in the email and entered personal information, contact your bank immediately</li> <li>* If you think you might have been scammed, contact Action Fraud (0300 123 2040) or report it online at <a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a></li> <li>* Consider using a spam filter to help block suspicious emails</li> <li>* Be cautious of unexpected emails asking for personal information or login credentials.</li> </ul>
Q42	Where can I see a list of firms blacklisted by the FCA?
BM	You can check the Financial Conduct Authority (FCA) ScamSmart Warning List to see a list of firms that have been warned about or banned from conducting regulated activities. Visit <a href="https://www.fca.org.uk/scamsmart/warning-list">https://www.fca.org.uk/scamsmart/warning-list</a> for more information.
FM	You can check the Financial Conduct Authority (FCA) website for a list of firms that have been banned from selling financial products. The FCA maintains a register of authorised firms, which you can search to verify whether a firm is legitimate. If you're unsure about a firm or investment opportunity, contact the FCA on 0800 111 6768 or check their website at <a href="https://www.fca.org.uk/">https://www.fca.org.uk/</a> . Remember, if a firm isn't listed as authorised by the FCA, it may be a scam.

Q43	I keep getting emails about winning a lottery I never entered. What should I do?
BM	<p>If you receive emails about winning a lottery you didn't enter, it's likely a scam. Here are some steps to take:</p> <ul style="list-style-type: none"> <li>* Do not reply or click on any links in the email</li> <li>* Delete the email and avoid opening any attachments</li> <li>* Report the scam to Action Fraud (0300 123 2040) or report it online at &lt;<a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a>&gt;</li> <li>* If you've provided personal information, contact your bank and credit card companies immediately.</li> </ul>
FM	<p>If you receive unsolicited emails about winning a lottery you never entered, delete them immediately. These are likely scams designed to trick people into paying money upfront in order to claim their "winnings". Legitimate lotteries don't contact winners by email. If you're unsure about an email, take some time to think before responding. You can also report suspicious activity to Action Fraud (0300 123 2040) or report online at <a href="https://www.actionfraud.police.uk">actionfraud.police.uk</a>. Remember that legitimate lotteries don't contact winners by email. By deleting suspicious emails, you can protect yourself from becoming a victim of cyber fraud.</p>
Q44	I got a call from a number that looks exactly like my bank's. How can I check if it's spoofed?
BM	<p>If you receive a suspicious call claiming to be from your bank, hang up and wait 5 minutes before calling your bank back using the official number on the back of your bank card or on their official website. Criminals can easily spoof phone numbers to make them appear legitimate. Always verify by calling back using the official number rather than following any instructions given during the call. If you're unsure about a call, hang up and wait 5 minutes before calling your bank back. This gives criminals less time to intercept your call. Remember, your bank will never ask for sensitive information over the phone.</p>
FM	<p>If you receive a suspicious call claiming to be from your bank, hang up immediately and contact your bank directly using the official phone number on your statements or their website. Be wary of calls asking for personal information such as PIN numbers, passwords, or card details. Scammers often use spoofed numbers to make calls appear legitimate. By hanging up and contacting your bank directly, you can protect yourself from becoming a victim of fraud. If you're unsure about a call, take some time to think before responding. You can also report suspicious activity to Action Fraud (0300 123 2040) or report online at <a href="https://www.actionfraud.police.uk">actionfraud.police.uk</a>. Remember that scammers often use spoofed numbers to make calls appear legitimate. By taking a few moments to verify calls, you can protect yourself from becoming a victim of cyber fraud.</p>
Q45	A friend on Facebook sent me a money request, but I'm not sure it's really them. How do I confirm?
BM	<p>If you receive a suspicious money request from a friend on social media, verify their identity by contacting them directly using their official contact information. Do not respond to the request or click any links within the message. Criminals often impersonate friends or family members to scam people on social media. If you're unsure about a money request, verify with the person directly using their official contact information. Remember, it's better to be cautious and confirm than to fall victim to a scam.</p>
FM	<p>If you receive a money request from someone on social media, don't respond immediately. Instead, contact the person directly through another channel (like email or phone) to verify if they actually sent the request. Be wary of any requests that seem urgent or pressure you to act quickly. Scammers often use social media to impersonate friends and family members in order to trick people into sending money. If you're unsure about a request, take some time to think about it before responding. You can also report suspicious activity to Action Fraud (0300 123 2040) or report online at <a href="https://www.actionfraud.police.uk">actionfraud.police.uk</a>. Remember that scammers often use social media to impersonate friends and family members in order to trick people into sending money. By taking a few moments to verify requests, you can protect yourself from becoming a victim of cyber fraud.</p>
Q46	I'm too embarrassed to tell anyone I lost money on a crypto scam. What do I do?
BM	<p>It's important to remember that falling victim to a scam doesn't mean you're at fault. If you've lost money in a</p>



	cryptocurrency scam, report it to Action Fraud (0300 123 2040) or online at < <a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a> >. You can also contact your bank and explain the situation to see if they can help recover any lost funds. If you're struggling emotionally, consider seeking support from a trusted friend, family member, or mental health professional. Remember, it's never too late to report a scam and seek help.
FM	If you've been the victim of a crypto scam, report it to Action Fraud (0300 123 2040) or report online at <a href="https://www.actionfraud.police.uk/">actionfraud.police.uk</a> . They will assess your report and provide guidance on how to secure your financial information and protect yourself from further harm. Remember that scammers often use fake websites and social media profiles to lure victims into investing in fraudulent cryptocurrencies. By reporting incidents to Action Fraud, you're helping law enforcement agencies investigate and disrupt criminal activity. If you're feeling embarrassed or ashamed about losing money on a scam, remember that it can happen to anyone and that the most important thing is to take steps to protect yourself from further harm. You can also seek support from organisations like Victim Support (08 08 16 89 111) who can provide emotional support and practical guidance on how to move forward after being a victim of crime.
Q47	I feel guilty because my elderly mum got scammed after I told her about an investment. What should I do?
BM	It's important to remember that falling victim to a scam isn't your fault, but it's crucial to take steps to help prevent further losses and protect others from similar scams. If you suspect your mother has been scammed, report it to Action Fraud (0300 123 2040) or online at < <a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a> >. Encourage her to seek advice from a trusted financial advisor or Citizens Advice Bureau. Educate yourself on common scams and share this knowledge with your family members to help protect them from falling victim in the future. Remember, it's never too late to report a scam and take steps to prevent further losses.
FM	It's important to remember that financial scams are sophisticated and can target anyone, even those who are financially savvy. Focus on supporting your mum emotionally and helping her recover from the loss. Encourage her to report the incident to Action Fraud (0300 123 2040) or online at < <a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a> > so they can investigate and potentially prevent similar scams in the future. You might also consider contacting Victim Support for guidance on supporting your mum through this difficult time (08 08 16 89 111). Remember, financial scams are not a reflection of intelligence or character - they're designed to exploit vulnerabilities and catch even the most careful people off guard.
Q48	I clicked a link in an email that looked like it was from my university IT team, and now my laptop is acting strange. What should I do?
BM	If you suspect your laptop has been compromised, disconnect it from the internet immediately to prevent further damage. Run a reputable antivirus software scan to detect any malware. If you're unable to remove the malware yourself, take your laptop to a professional for help. Change all of your passwords and enable two-factor authentication where possible. Report the incident to Action Fraud (0300 123 2040) or online at < <a href="https://www.actionfraud.police.uk/">https://www.actionfraud.police.uk/</a> > if you believe it was a phishing attack. Be cautious of future emails and always verify the sender's identity before clicking on links or downloading attachments.
FM	If you suspect your device has been compromised, immediately disconnect it from the network and contact your university's IT helpdesk for guidance on how to secure your device. Be wary of any messages or pop-ups that ask for personal information or request you to download software. Do not click on any links or attachments in suspicious emails. If you're unsure about a message, contact the sender directly using their verified contact details before taking any action. Remember that scammers often use phishing emails to gain access to your devices and steal your personal information. By staying vigilant and verifying all requests for money or personal information, you can help protect yourself from cyber fraud. If you've been a victim of cyber fraud, report it to Action Fraud (0300 123 2040) or report online at <a href="https://www.actionfraud.police.uk/">actionfraud.police.uk</a> . They will assess your report and provide guidance on how to secure your device and protect yourself from further harm.
Q49	I bought something from an overseas website that never arrived. Can Action Fraud still help me?
BM	Action Fraud primarily handles cybercrime incidents, such as phishing, hacking, and online scams. If you've

	<p>purchased something from an overseas website that didn't arrive, contact your credit card company or PayPal (if used) to dispute the charge. For consumer protection issues with international purchases, contact Citizens Advice Consumer Helpline (03454 04 05 06) or report it to the National Trading Standards Scams Team at <a href="https://www.reportscamsandfraud.org.uk/">https://www.reportscamsandfraud.org.uk/</a>.</p>
FM	<p>Yes, Action Fraud can help with international online shopping scams. They will pass your report to the National Fraud Intelligence Bureau (NFIB), who will assess it and share it with relevant law enforcement agencies both in the UK and abroad. While they may not be able to recover your money directly, they can use your report to build intelligence about the scam and help prevent similar crimes from happening to others. By reporting incidents to Action Fraud, you're helping law enforcement agencies investigate and disrupt criminal activity. If you've been a victim of an international online shopping scam, report it to Action Fraud (0300 123 2040) or report online at <a href="https://actionfraud.police.uk">actionfraud.police.uk</a>. They will pass your report to the NFIB who will assess it and share it with relevant law enforcement agencies both in the UK and abroad. While they may not be able to recover your money directly, they can use your report to build intelligence about the scam and help prevent similar crimes from happening to others. By reporting incidents to Action Fraud, you're helping law enforcement agencies investigate and disrupt criminal activity.</p>
Q50	<p>I got a voicemail that sounded exactly like my daughter asking for money urgently. Could scammers really fake voices like that?</p>
BM	<p>Yes, scammers can use voice cloning technology to mimic voices, including those of family members or friends. If you receive such a call, verify the request by contacting the person directly through a known number or method (e.g., email, text). Do not provide personal information or send money without confirming the authenticity of the request.</p>
FM	<p>Yes, scammers can use voice cloning technology to create convincing fake messages. This is known as deepfake audio. Be wary of urgent requests for money or personal information, especially if they come from unexpected sources. If you're unsure about a message, contact the person directly using their verified contact details before making any payments. Remember that scammers often use emotional manipulation to pressure victims into acting quickly. By staying vigilant and verifying all requests for money or personal information, you can help protect yourself from deepfake audio scams.</p>