Booklet 5

Financial Harm Awareness



How to

protect your money in the bank from scams

AND

what <u>banks</u> do to protect <u>your</u> money from scams.



What do scammers do?



Scammers **look and sound like** real people, in real places doing real jobs.

Fake ID

But they are **not**!



Scammers make everything up.

Example 1

This scam has a fake email address.



The fake address will have **a small change**. It might be as small as adding or missing out an extra letter, symbol or punctuation mark.

This email should come from E.Stevens. It is asking for money.



Can you spot the difference?

Example 2



The scammer phones you and sounds **like** a bank or business that needs your bank details.

You need to be very careful.



Why do scammers do it?

If the scammers get your bank details....

they will trick you into giving them money or they will take all your money.



Scammers keep on trying in **different** ways. That is why **you** need to keep learning more about how to keep your money safe.

Stay alert!

Some people will fall for the scam!

Don't let it be you!

Learn about the different types of scams and 'What to Do' to protect your money in the bank or building society:

1. Scam emails can have harmful attachments.



Scam emails want you to open harmful attachments.



When you open the attachment, it acts **like** a peep hole for the scammer to spy on your personal bank details.



It copies your bank account number and passwords when you log onto your online banking. The scammer can then take all your money.

What to Do:



Never open an attachment from someone you don't know.

2. Scams can offer fake 'free' items.



Some emails seem to offer help or offer things for free.

For example, free covid testing kits, or even the offer of a free vaccine.

Often you find the offer is NOT free and you have to pay a charge.

What to Do:



Do NOT open email.

3. Scams can appear to give good news.



Some scams are text messages. These can be from businesses that have shut down.



For example, the text says you will get a refund for the holiday you booked.



You are expecting contact from the real company so you may fall for the fake text due to the chance timing.

What to Do:



Check out what the company are doing for their ex-customers from the real website.

4. Scams can sound like problems sorted.



For example, "You have recently been in a car accident" message. There will a few people who have been in a car accident.

What to Do:



Stop and Think! Is this real?



Check it out! Contact the company in another way eg website or phone number from previous letter.

5. Scammers can **pretend to be** from the police, a bank or business.



Some scams call you on the phone with a 'problem' and tell you to contact the police. The scammer leaves the phone line open.



This means when you call the police, you are still speaking to the scammer pretending to be the police.



It is like the scammer is reading lines from a play to trick you.

What to Do:



Before you phone the police, call a friend or family member. Then you will know if the scammer is still on the line.

OR



Phone the police from a different phone number - landline or mobile.

Other advice to help you:



Do **not** be rushed by the scammer.

Take your time to think.



Say you will phone them back later but do **NOT** contact them again.





If the scammer wants you to move your money, think about why you would do this. Is this idea from someone you trust or out of the blue?



Have you checked the information in another way/from someone else?

Talk to people you trust.



Feel unsure?....
contact your bank and/or



Fife Council's Trading Standards who know about recent scams.



If you feel scared, contact the police. Phone 101 or 999 if an emergency.

What banks do to protect your money from scams.

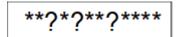
Banks make it clear that:



1. Banks and police will **never** ask you to transfer your money to a safe account.



2. Banks **never** phone you 'out of the blue' and ask for your password or pin.



3. If you phone your bank or they phone you, they **only** ask for a couple of letters or digits from your online password.



If anyone asks you for more of your password, **hang up**.



Call the bank again from a **different phone number**. Use the phone number on your bank card, bank statement or their website.

There is more that banks do

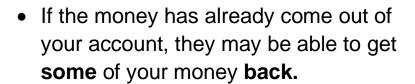
Banks make it clear that:



4. If you are asked to pay money for a service or investment, you can **contact your bank to ask** if they think the account is real.



5. If you have paid money to something you think is a scam, then **contact your bank** as soon as possible.





• They may also put **a block** on future payments.



6. Banks can help you and your carer.

Some banks have a **companion card**, which is a bank card that has a limited amount of money in the account and can only be topped up every 5 days.

This means the **carer has their own PIN number**, so they don't need to know or use your PIN number.



Even if your bank doesn't have a companion card service, you can **speak to your bank** about setting up a separate account for your carer to use.



7. Many banks have **community bank staff** who provide advice and help you to protect your money.



8. Most banks have more information online about what to look out for to protect your money. This is updated regularly.



For more information:

Fife Council website has other easy reads

www.fife.gov.uk/adultprotectioneasyread



R2 MRS/ASPTeam/FH Booklet 5 06.04.22