FINANCIAL FITNESS:

LEVEL UP

FRAUD 101

We all think fraud is something that happens to other people, until it happens to us.

Understanding fraud is like understanding magic. Confusing if you don't know the trick, but easy to spot once you know how it's done. If we all learn the tricks, we're less likely to be fooled.

EMAIL SCAM (PHISHING)

Phishing is a way criminals try to get sensitive information, like usernames and passwords via email. These messages look like they've come from someone you trust, such as your bank.

What to look out for: The email will ask you for personal information, or direct you to a website asking you to share information. It's also likely to have a generic opening (they probably won't address you by name), and incorrect spelling and grammar.

How to avoid: Don't click on any links. Don't open any attachments. If you're an HSBC customer, you can forward the email to **phishing@hsbc.com** and it'll be investigated.

SMS SCAM (SMISHING)

Criminals may send you fake text messages that look like they've come from someone you trust, such as your bank or utility provider.

What to look out for: They will try to get you to click on a link or reply to the message with personal or financial information.

How to avoid: If you're not sure, don't click on any links. Do not reply. Check to see what regular text messages look like from that organisation.

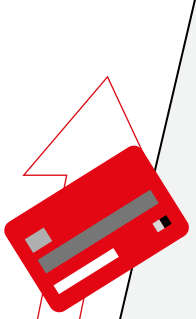
VOICE SCAM (VISHING)

You may receive an unexpected call, claiming to be from someone you'd normally trust, like your bank or the police, but in fact it's a criminal trying to scam you or get information from you so they can scam you in the future.

What to look out for: They might try to persuade you to transfer or move your money to a "safe place". They might ask for personal information, or even your account passwords, PIN or secure key codes.

How to avoid: Hang up the phone properly. Wait 15 seconds until the line is fully disconnected. Wait another 15 seconds before beginning a new call. Ring the company back on a number you know and trust. In the case of your bank, it would be the number on the back of your card.

AUTHORISED PUSH PAYMENTS

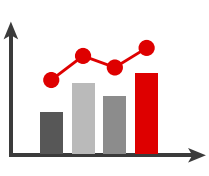


Authorised Push Payment (APP) scams happen when you're persuaded to send money to a criminal.

What to look out for: You may be tricked into sending money to a 'safe account' or an account you believe to be trustworthy, or be tricked into sending money to buy goods that don't exist.

How to avoid: If anyone asks you to divert a payment or move your savings – question it. Make sure you phone the bank or company directly and check on any changes to payment details.

INVESTMENT SCAMS



If you receive an offer for an investment opportunity that seems too good to be true, then it probably is, and has most likely come from a criminal.

What to look out for: They often use false testimonials, fake celebrity endorsements, spoof websites and fake companies with similar names to genuine investment organisations.

How to avoid: Check the Financial Conduct Authority (FCA) website to confirm the company is authorised.

MONEY MULES

Job adverts and offers from acquaintances which offer quick and easy ways to get money might seem harmless, but they are often run by organised crime groups. They try to get you to transfer money via your bank account in exchange for payment, making you a 'money mule'.

What to look out for: You'll be asked to provide your bank details, receive a payment into your account and then either withdraw it in cash or transfer it to another account. This can get you into serious trouble.

How to avoid: Never allow money to be transferred through your bank account in exchange for payment.

PAYMENT DIVERSION

Criminals monitor email traffic and, when payments are due, they send their own email that looks and feels like a genuine message from a company.

What to look out for: They will tell you that the bank details for your payment have changed and give you new details to send your money to.

How to avoid: Always check with the company you're paying, by calling their official phone number, not the phone number on the email, before making a payment with new bank details.

ROMANCE SCAMS

This type of fraud begins with a fast-moving, online relationship. Criminals try to lower your suspicions by appealing to your compassionate or romantic side, and then ask for money.

What to look out for: They'll go to great lengths to build rapport and form a highly emotional bond.

How to avoid: Never send money to someone you've only met online. Also, don't agree to accept money from them to send on their behalf.

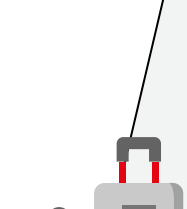
IDENTITY THEFT

Criminals may try to get important pieces of personal information which would allow them to open new accounts in your name, or to take over your account.

What to look out for: Online quizzes that tell you, for example, your personality type, may seem harmless, but they may get you to reveal personal details about yourself. The terms and conditions of these quizzes often allow the data you enter to be sold to third parties.

How to avoid: Avoid any short, fun quizzes that may pop up on social media and keep your profile private. Also, make sure you destroy bank statements and similar documents safely.

HOLIDAY SCAMS



There are many adverts that promise great holidays which are fake. Either the holiday doesn't exist, or it does exist but won't be what you think it is when you get there.

What to look out for: Check that the website you are booking the holiday through is legitimate, by looking for online reviews and recommendations. Also look out for incorrect spelling and grammar.

How to avoid: Be wary of unusually cheap holidays or high deposits, and always check the terms and conditions.

HSBC