KNOW FRAUD

KNOW THE FACTS. STOP THE FRAUD.
8 THINGS YOUR BANK WILL NEVER ASK YOU TO DO...

1. Ask for your full PIN number or any online banking passwords over the phone or via email.
2. Send someone to your home to collect cash, bank cards or anything else.
3. Ask you to email or text personal or banking information.
4. Send an email with a link to a page which asks you to enter your online banking log-in details.
5. Ask you to authorise the transfer of funds to a new account or hand over cash.
6. Call to advise you to buy diamonds, land or other commodities.
7. Ask you to carry out a test transaction online.
8. Provide banking services through any mobile apps other than the bank’s official apps.

If it looks suspicious or it sounds suspicious, report it to your bank.

* Know Fraud is a trademark of the National Fraud Intelligence Bureau, which is part of the City of London Police

**Keeping your money safe is your bank’s number one priority**

That’s why they’ve set up secure procedures to protect you from fraudsters...

But these criminals are often sophisticated and their techniques are constantly changing. One ploy is to pretend they work for the Police or your bank. Dangerous though this is, there are tell-tale requests a fraudster may make that your bank never will. Knowing what these are can ensure you don’t fall victim to an attack.
**KEEP YOUR CARDS CLOSE TO YOUR CHEST**

**SCAM 1. COLD CALLS, ‘VISHING’ AND COURIERS**

*WHAT TO LOOK OUT FOR: SUSPICIOUS CALLS FROM YOUR BANK OR THE POLICE, WITH OFFERS TO VISIT YOUR HOME*

In these cases a fraudster will say they are from the bank or police, and that a fraudulent credit card payment has been spotted or a card that is due to expire needs to be replaced. To convince the intended victim they are genuine, the caller will suggest the customer hangs up and calls the bank back on the number printed on the back of their debit or credit card. But the fraudster never actually disconnects the line so that when you call the real number you are still speaking to them.

Usually the fraudster will then ask for the customer’s PIN and then send a courier to the victim’s home to collect the bank card, promising to provide a new one. By now the assailant has obtained the victim’s name, address, bank details, card and PIN — enough to make large bogus payments. The technique of using a telephone call to steal personal or banking information is known as “vishing”.

**OTHER TYPES OF COURIER FRAUD TO BE AWARE OF**

Customers are asked by their bank to participate in a fake police investigation, usually involving a corrupt bank employee who has been stealing from customer accounts. Typically they will be asked to withdraw substantial sums of money over the counter at their bank without arousing the suspicion of the staff. They are then told to wait at home for it to be collected by a courier for safe keeping. Alternatively some customers are asked to transfer their money to a “safe” account, which really belongs to the fraudster.

**BEWARE**

Fraudsters may keep the line open even after you hang up. If possible, use another phone or wait at least 2 minutes before picking up and dialing again.
Too good to be true? It probably is!

Scam 2. The dodgy investment fraud

What to look out for:
Brochures through the post and cold calls from “investment brokers” you don’t know offering big money deals.

Fraudsters pressure would-be victims with calls to their home urging them to hand over thousands of pounds in return for “buy now or lose out” investments in diamonds, rare earth metals, storage, wine or even carbon credits. But the commodities are often overpriced or non-existent.

Some people have been lured into handing over their entire pension pot after the promise of high returns. The average victim of an investment scam loses £20,000.

Brian, aged 66, Leicestershire. Former civil servant.

He was called by a persuasive man claiming to be a broker for a Japanese company selling shares. Brian was sceptical at first but a slick, professional looking website with a Japanese contact number convinced him to invest around £350,000. When Brian’s family became aware they contacted the police who could prove the man had operated other websites offering fraudulent investment deals, confirming suspicions that Brian had become this criminal’s latest victim.

“IT’s a once in a lifetime opportunity and you could do very nicely out of this…”

Real life victim

Criminals use persuasive, hard-sell tactics, that often include using impressive job titles, technical jargon and creating a sense of urgency.

Criminals will often advise victims to keep the investment a secret.

Beware of companies that give only PO box addresses and mobile contact numbers.
BEWARE OF THE UPFRONT STUNT

SCAM 3. COMPENSATION CON ARTISTS

WHAT TO LOOK OUT FOR:
CALLS OR TEXTS ASKING FOR UPFRONT PAYMENT IN RETURN FOR BIG MONEY COMPENSATION

Criminals call or text to say the customer is owed thousands of pounds in compensation or refunds from their bank for taking out Payment Protection Insurance (PPI). Some fraudsters have said they are from Trading Standards to gain trust.

These cheats will then ask for upfront fees of around £250 to “process” the compensation. Would-be victims may also be asked to give their bank details or supply a serial number from a prepaid voucher or card (like UKASH), which is effectively the same as handing over cash.

Fraudsters called Emma to say she was entitled to around £8,000 in compensation, but would have to give some cash upfront to cover tax and insurance costs. She followed their instructions and made a series of payments from her savings account. She was then told that there had been a mistake and the amount of compensation had been miscalculated. She was actually owed £18,000, they said. Once again she was asked to provide cash upfront to cover transfer costs.

Emma never received her compensation.

“WE CAN HELP YOU GET THE COMPENSATION YOU DESERVE”
Criminals trawl the internet and send “phishing” emails to obtain the sort of private information that makes it easier for them to defraud victims. They are also increasingly befriending people on social media, striking up a relationship online before openly asking for money.

Fraudsters who commit ‘romance’ or ‘relationship’ fraud will build confidence over time and then eventually ask for cash, concocting worthy causes such as a struggling business or ailing relative.

New Comment

Don’t worry, I’ll definitely pay you back...you know me!

All examples in this booklet are based on reports made by genuine victims. Names were changed to protect their identities.
IF YOU SUSPECT YOU’VE BECOME A VICTIM OF FRAUD

1. STOP SENDING MONEY. TELL YOUR BANK IMMEDIATELY USING THE NUMBER ON THEIR WEBSITE OR OTHER COMMUNICATIONS. REPORT THE FRAUD TO POLICE BY CONTACTING ACTION FRAUD EITHER VIA THE WEBSITE WWW.ACTIONFRAUD.POLICE.UK OR BY CALLING 0300 123 2040 (TEXTPHONE 0300 123 2050).

2. IF YOU ARE THE VICTIM OF ‘SHARE’ INVESTMENT FRAUD, YOU SHOULD ALSO REPORT IT TO THE FINANCIAL CONDUCT AUTHORITY CONSUMER HELPLINE ON 0800 111 6768 (FREEPHONE).

3. BEWARE OF OTHER SCAMS. YOU ARE LIKELY TO BE TARGETED AGAIN, PARTICULARLY BY FIRMS OFFERING TO RECOVER FUNDS YOU HAVE LOST.

* Know Fraud is a trademark of the National Fraud Intelligence Bureau, which is part of the City of London Police

FOR MORE INFORMATION ON FRAUD, PLEASE VISIT US ONLINE AT: WWW.KNOWFRAUD.CO.UK