Millions of people could become victims of scams, according to a poll by YouGov. And its findings have led banks to launch an initiative called Know Fraud, No Fraud, highlighting eight things your bank will never ask you to do.

It's hoped this will help combat fraudsters.

The eight things your bank will never 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.

Vishing and phishing

Phishing is a word used to describe emails which fish for personal information such as your Pin or password. Typically an email will say you need to 'verify' your account by providing these details, or the account will be suspended.

Vishing is the telephone version of phishing – a cold call from fraudsters pretending to be your bank will aim to persuade you to tell them your Pin or password information. Sometimes they say there's been suspicious activity on your account or your card is about to expire.

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.

Alternatively the fraudsters will say they're from the police and they need you to help with a secret investigation into a bank employee.

Courier fraud

Vishing is often used in conjunction with courier fraud. Having extracted key security information on the phone, the criminal may also say that they are sending an official courier to your home to collect the corresponding card. These couriers will have 'official' identification.

Once the criminals have both your Pin and card they can withdraw large amounts of cash.

Another ruse is for the conman to tell the customer they're investigating a rogue bank employee. They'll ask the customer 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.

But it's all a con: Your bank will never send someone to your home to collect cash, bank cards or anything else.

Other types of fraud

So-called compensation con artists 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).

They will then ask for upfront fees of around £250 to 'process' the compensation. Once they've handed over their money, that's the last the victim hears of it.

The final fraudsters highlighted are relationship tricksters. Operating on dating websites or social media, conmen befriend their target and build up a relationship over time. Eventually they ask for cash to help save an imaginary ailing business or sick relative.

If you've been a victim of fraud already, beware of cold calls from people who say they can help you recover the money you lost – fraudsters will often try to trick a victim for a second time.