TAKE FIVE TO STOP FRAUD™

TAKE FIVE OVER TEA

WITH YOUR FAMILY AND LOVED ONES

WELCOME TO TAKE FIVE OVER TEA

Hello! Welcome to the Take Five Over Tea toolkit – a handy pack of information and resources to help you protect your loved ones against fraud.

The aim of Take Five Over Tea is to encourage people to put the kettle on and sit down with their parents/ grandparents or anyone else they think may be particularly vulnerable to a financial scam.

Financial fraud happens every **fifteen seconds** across the UK and cost the nation a staggering **£768.8 million** in 2016. That's around **£2,000,000** a day, or **£1400** every minute!

What's more, **2 in 5** people have been personally affected by fraud, or know someone that has. Together with you, we want to make it **0**.

HERE'S WHAT YOU NEED

We have put together information to help you and your loved ones to Take Five in this handy little pack. All you need to do is put the kettle on, find a comfortable space and discuss the following advice.

WHAT'S TAKE FIVE ALL ABOUT?

Take Five is a national campaign to help consumers and businesses stop fraud by taking a moment the next time they are asked for their personal details. It aims to engage, encourage and educate people on how best to protect themselves against financial fraud, such as email deception and phone scams.

Take Five is created in collaboration with Financial Fraud Action UK whose members are the nation's major banks, credit, debit and charge card issuers, and card payment acquirers, plus a range of partners, including the Government, law enforcement, charities, UK retailers, telecom providers and Cifas.

WHY THIS IS IMPORTANT FOR YOU AND YOUR FAMILY

Older people are often directly targeted by fraudsters because they believe older generations have more disposable income from their savings or pensions. The increased sophistication of financial services and associated technologies also means it can be harder to spot the obvious signs of a scam as easily, which are most likely to occur over the phone.

By taking the time to talk to your loved ones, they have a much better chance of spotting a scam and preventing themselves from becoming a victim.

TYPES OF FRAUD

As communication technology becomes more sophisticated, so do the techniques used by fraudsters. They now have a number of different ways to reach people, so here's a rundown of the most common to keep an eye out for.

1. PHONE SCAMS

Also known as vishing, scammers can call you on your mobile or landline, claiming to be from your bank or some other trusted organisation. They may already have some of your details which they use to convince you they are legitimate. If you ever get a call from someone claiming to be from your bank, they will never ask you for details such as your PIN or full online banking password.

2. TEXT MESSAGE SCAMS

A text might not be from who you think – smishing is when criminals pretend a message is from your bank or another organisation you trust. They usually tell you there has been fraud on your account and ask you to deal with it by calling a number or visiting a fake website to update your personal details. Your bank will never send you texts like this, so the next time something suspicious pops through, do not click any links and contact your bank on a number you know to be correct such as the one listed on your statement, their website or on the back of your debit or credit card.

TYPES OF FRAUD (CONTINUED)

TAKE FIVE TO STOP FRAUD™

3. EMAIL SCAMS

Our inboxes often receive a number of unsolicited emails and whilst most are harmless, it's a good way for scammers to 'phish' for information. Typical scam emails appear to come from your bank or another trusted source and can look very convincing. Little details such as them using 'dear customer' instead of your name and the email address of the sender can be giveaways, as can poor spelling and strange formatting in the email. Never click any links if you are unsure, and don't download any attachments unless you are certain what they are.

4. POP-UPS AND MISLEADING WEBSITES

From online shopping and banking through to alarmist pop-ups, the internet gives scammers a number of ways to commit fraud. The general rule of thumb is to ignore and close all pop-ups when generally browsing, especially those which promise ways to get rich quickly, or saying that your computer is running slowly. The same goes for websites that you are directed to from unsolicited emails.

THINGS YOU CAN DO TO PREVENT FRAUD

TAKE FIVE TO STOP FRAUD™

If you receive a request to provide personal or financial information whether over the phone, in an email or online, always take a moment to reflect and step back from the situation. Here are some general tips to keep in mind:

1. NEVER DISCLOSE SECURITY DETAILS

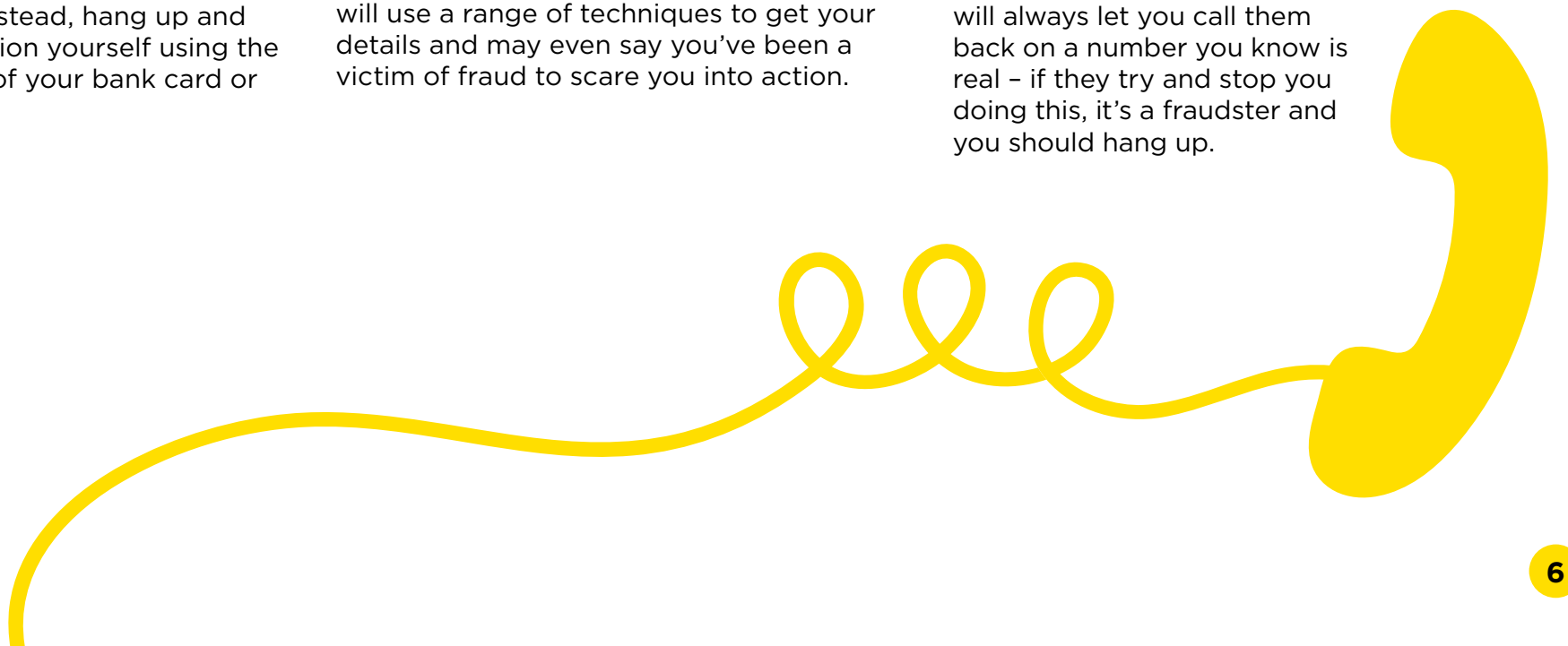
A genuine bank or organisation will never ask you for details such as your PIN or card number over the phone or in writing. Before you share anything with anyone, stop and think. Unless you're 100% sure who you're talking to, don't disclose any personal or financial details. Instead, hang up and contact the organisation yourself using the number on the back of your bank card or on their website.

2. DON'T ASSUME AN EMAIL OR PHONE CALL IS AUTHENTIC

Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine. Criminals will use a range of techniques to get your details and may even say you've been a victim of fraud to scare you into action.

3. DON'T BE RUSHED OR PRESSURED

Under no circumstances would a genuine bank or another trusted organisation force you to make a financial transaction on the spot; they would never ask you to transfer money into another account even if they say it is for fraud reasons. They will always let you call them back on a number you know is real – if they try and stop you doing this, it's a fraudster and you should hang up.



THINGS YOU CAN DO TO PREVENT FRAUD (CONTINUED)

4. LISTEN TO YOUR INSTINCTS

If something feels wrong then it is usually right to question it. Criminals may lull you into a false sense of security when you're out and about or rely on your defences being down when you're in the comfort of your own home. If your gut-feeling is telling you something is wrong, take the time to make choices and keep your details safe.

If you've taken all these steps and still feel unsure about what you're being asked, never hesitate to contact your bank or financial service provider on a number you trust, such as the one listed on their website or on the back of your payment card.

5. STAY IN CONTROL

Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel overwhelmed when faced with unexpected or complex conversations. Remember that it's ok to stop the discussion if you do not feel in control of it.

REMEMBER

TAKE FIVE TO STOP FRAUD™

YOUR BANK OR THE POLICE WILL NEVER:

- Phone and ask you for your PIN or full banking password, including tapping them into your phone.
- Ask you to withdraw money to hand over to them for safe-keeping.
- Ask you to transfer money to a new or other account for fraud reasons, even if they say it is in your name.
- Send someone to your home to collect cash, PIN, cards or cheque books, even if they say you have been a victim of fraud.
- Ask you to purchase goods using your card and then hand them over for safe-keeping.

ANTI-FRAUD CHECKLIST

Here are a few questions you can ask yourself every time you are contacted by someone you don't know who asks for personal details. If any of the following situations come about, do not give any personal details and seek advice from a family member or contact the company in question.

1. Has the phone call or offer come unsolicited? Was it expected or out of the blue?
2. Are they asking to confirm sensitive details such as your name, address or bank-account details?
3. Are they looking for a fast/instant response of some kind?
4. Are they asking for money?
5. Is the caller avoiding using the actual name of your bank or utilities company?
6. Are they offering a prize, free gift or trial?
7. If they say they are the police or investigating something, do not give away sensitive information.
8. Does an email from your bank or another company have an odd email address?
9. Is the formatting strange or are there spelling mistakes?
10. Are you being asked to change your password despite not sending a request to do so?

TO STOP FRAUD™

FURTHER INFORMATION

For more information on Take Five and how to prevent fraud, visit us at **https://takefive-stopfraud.org.uk**, and stay in touch on:

facebook.com/TakeFiveStopFraud

twitter.com/TakeFive