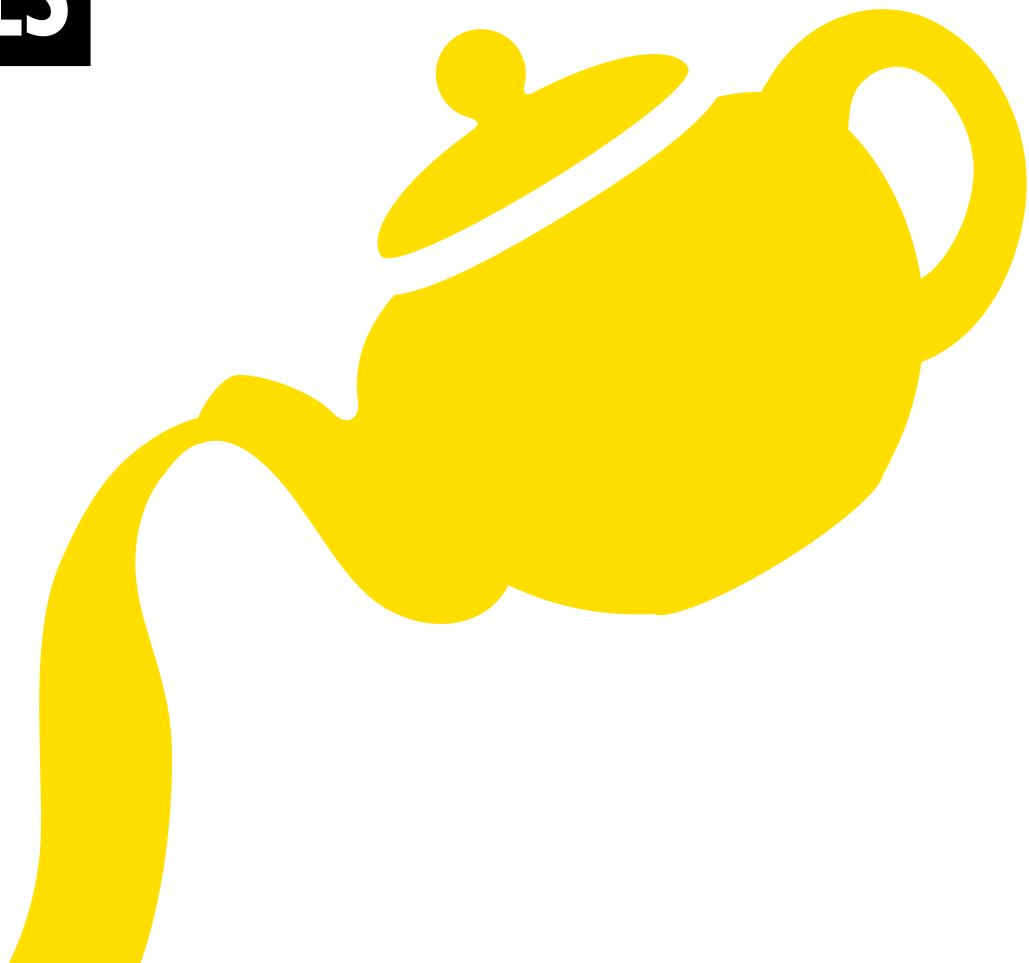
TAKE FIVE TO STOP FRAUD™

TAKE FIVE OVER TEA

TOOLKIT AND RESOURCES FOR ORGANISATIONS



WELCOME TO TAKE FIVE OVER TEA

Welcome to the Take Five over tea toolkit – a handy pack of information and resources to empower charities and organisations to help people protect themselves 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**.

WHAT'S TAKE FIVE ALL ABOUT?

Take Five is a national campaign to help consumers and businesses prevent fraud by taking a moment the next time they are asked for their personal details. It aims to engage, empower 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 membership includes the nation's major banks, credit, debit and charge card issuers, card payment acquirers, and a range of partners, including the Government, charities, law enforcement, UK retailers, telecom providers and Cifas.

AND WHY IS IT 'OVER TEA'?

Older people are often targeted when it comes to financial fraud - to help address this particular issue, we are partnering with Age UK to hold events all over the UK called Take Five Over Tea.

The aim of Take Five Over Tea is to encourage people to sit down with their parents/grandparents or anyone else they think may be particularly vulnerable to a scam in an informal setting where they are more likely to take in the advice being given. By hosting events like this we can reach as many people as possible and raise awareness.

LET'S WORK TOGETHER

By joining forces we have a better chance of putting scammers out of a job.

We need you to help us spread the message and get involved in the campaign so we can all help protect the nation against financial fraud. To help you do this, we've packed this toolkit with everything you'll need to get the word out there and organise your own events:

- Event checklist to make sure you have everything ready.
- Guidance on using your social media channels with guiding examples.
- Cheat sheets on the basics of fraud and advice.
- Campaign materials and assets such as posters and leaflets – free to use and ready to print or add alongside your own communications.

ORGANISING YOUR EVENT

EVENT CHECKLIST

Putting an event together takes a little bit of organisation, so we've included a checklist for you to work from. Here are a few ideas to get you started:

- ❒ Pick a date to host tea ideally over the next few weeks.
- ❒ Put up the posters and hand out the advice leaflets found in this pack.
- ❒ Advertise the event to your local community – focusing on an older demographic and local organisations.
- ❒ Promote the event through your social channels and ask your followers to spread the word
- ❒ Nominate speakers/volunteers who can relay the Take Five message during the session – focusing on the main types of fraud:
  - Phone
  - Online
  - Postal
  - Email
- ❒ Prepare a stall with the relevant literature from Take Five that attendees can take home for reference – you can download and print off information from the Take Five website.

GETTING THE WORD OUT

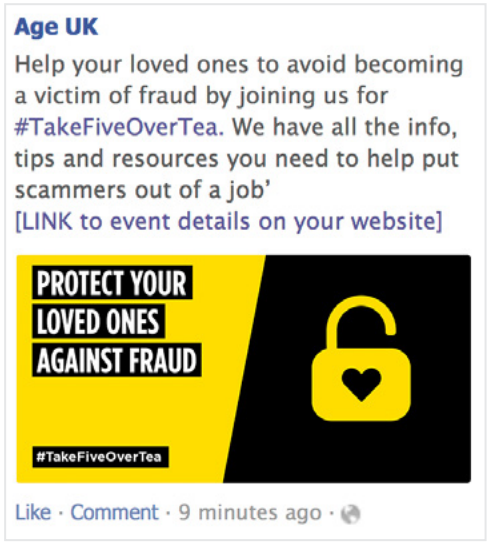
This campaign is all about spreading the word and raising as much awareness as possible. We've reached thousands through our social channels and so can you.

When creating social content, make sure to use **#TakeFiveOverTea** to support the campaign messaging and let us know about your event by tweeting us **@TakeFive**. Also, share your event with us on Twitter and Facebook!

Feel free to use the images included in this toolkit to help spread the message or create your own event imagery.

Example Tweet:

Example Facebook Post:



BASIC INFORMATION AND CHEAT SHEETS:

The following cheat sheets have been designed to be a starting point for your presentation, outlining the main details and setting the scene. For more information to share, see the resources that come after this section.

TYPES OF FRAUD

TAKE FIVE TO STOP 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.

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.

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.

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.

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.

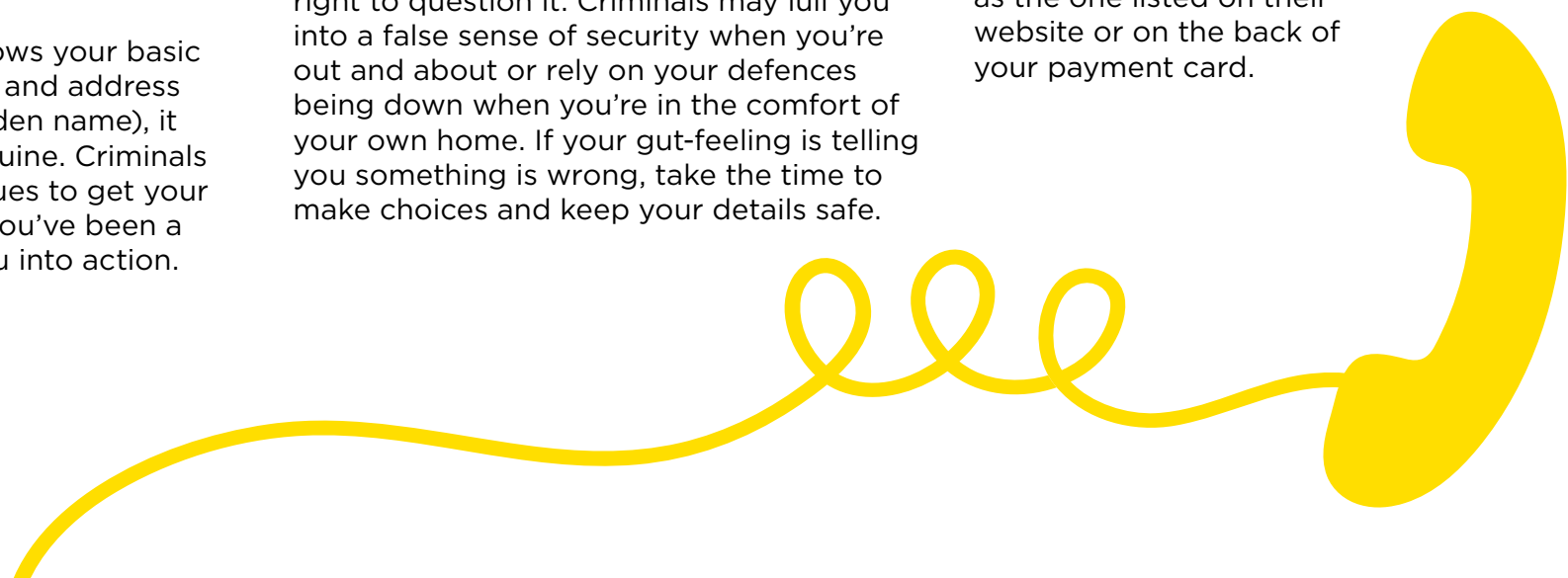
4. LISTEN TO YOUR INSTINCTS

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.

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 don't feel in control of it.

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.



REMEMBER

TAKE FIVE TO STOP FRAUD™

YOUR BANK OR THE POLICE WILL NEVER:

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

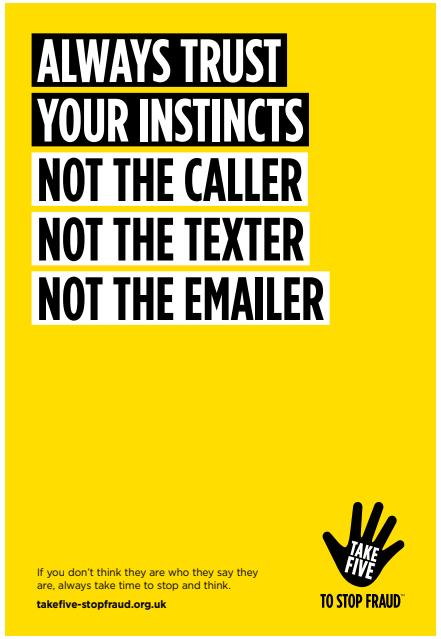
SUPPORTING MATERIALS

The following assets have been designed by us to be used by you. Please feel free to use everything you see here to help spread the message and make your event a success.

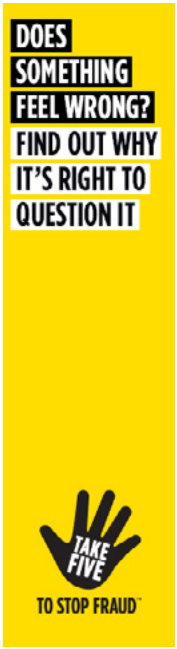
These are all available at **https://takefive-stopfraud.org.uk/resources/campaign-materials/**

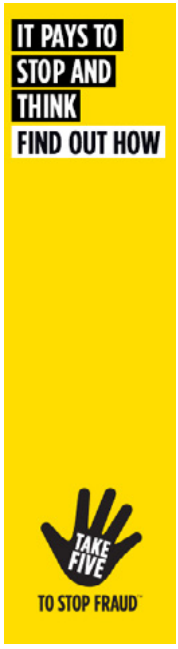
ENDORSEMENT LOGO

KEY MESSAGES TO PRINT

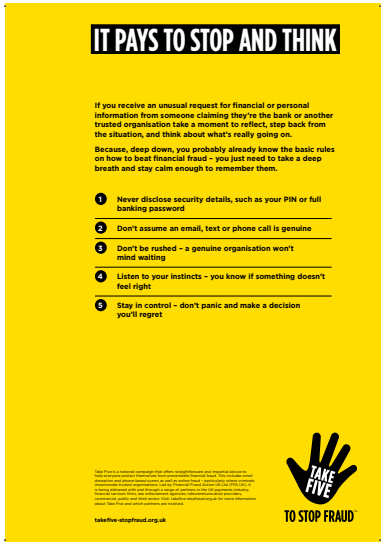


WEB BANNERS





LEAFLETS



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