TAKE FIVE OVER TEA

TOOLKIT AND RESOURCES FOR CHARITIES AND 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 and scams.

Many people may already know the dos and don’ts of financial fraud and scams – that no-one should ever contact them out of the blue to ask for their full PIN or full password, or ever make them feel pressured into moving money to another account. The trouble is, in the heat of the moment, it’s easy to forget this.

With criminals becoming more sophisticated in their approaches, we’re here to provide you with the knowledge and confidence to Stop and Challenge any requests for your information.

Take Five Over Tea encourages people to stick the kettle on and sit down with their parents/grandparents or anyone else they think may be particularly vulnerable to fraud and scams, whether that’s in the comfort of their own home or even virtually!

WHAT'S TAKE FIVE ALL ABOUT?

Take Five to Stop Fraud is a national campaign that encourages consumers to stop and think the next time they are asked to make a payment or for their personal or financial information. It aims to educate and empower people to reject, refuse or ignore requests that could be fraudulent, including email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations.

Led by UK Finance, the Take Five campaign is delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector organisations.

AND WHY IS IT 'OVER TEA'?

We all think we're savvy when it comes to fraud and scams, but the truth is any one of us can fall for one. After all, trusting someone is something everyone tends to do instinctively. Take Five Over Tea urges you to take the time to educate your loved ones on fraud and scams so they have a much better chance of spotting the signs.

Criminals are becoming more sophisticated, using tactics such as social engineering and number spoofing, to gain our trust and make it harder for us to spot the obvious signs of a scam as easily. To help address this particular issue, we are encouraging you to hold events all over the UK called Take Five Over Tea, where in an informal setting people 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 criminals 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 fraud and scams. 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 scams, including actionable advice.
- Access to our campaign materials and assets such as posters and leaflets made available in both English or Welsh – free to use, and available as either print-ready or co-brandable file types that can be used 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, time, and venue to host Take Five Over Tea.
- ☐ Put up the posters and hand out the advice leaflets found in this pack or from the **toolkit section** of the Take Five website.
- ☐ Advertise the event to your local community – focusing on local organisations.
- ☐ Promote the event through your social channels and ask your followers to spread the word by using the hashtag #TakeFiveTellFive. You may also wish to utilise paid for advertising to further promote your event and engage with local media outlets.
- ☐ Source speakers/volunteers who can relay the Take Five message during the session – focusing on the main types of fraud and scams:
  - Impersonation scams
  - Investment scams
  - Purchase scams
  - Romance scams
  - Courier fraud
  - Doorstep scams
- ☐ 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** or tagging us on Facebook **@TakeFiveStopFraud** or Instagram **@takefivetostopfraud** so we too can help promote your event.

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 and Instagram Post:

BASIC INFORMATION AND CHEAT SHEETS

TAKE FIVE TO STOP FRAUD™

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 AND SCAMS

TAKE FIVE TO STOP FRAUD™

As technology becomes more sophisticated, so do the techniques used by criminals. They now use a wide variety of methods to trick people, so here's a rundown of the most common to keep an eye out for.

IMPERSONATION SCAMS

Criminals are experts at impersonating trusted organisations, including banks, the police, and government departments such as HMRC, to convince you to make a payment or share your personal and financial details. They often use alarmist language and time-pressure to convince you to take immediate action, and may already have some of your details, which they use to add a layer of authenticity to their scam. If you receive an urgent request for your money or information, STOP: take a moment to stop and think.

PURCHASE SCAMS

From designer wear to the latest kitchen gadgets, you can find anything when shopping online, and with more of us opting to use this service in the hopes of finding a bargain it can be easy to fall for a purchase scam. Criminals advertise goods/services at "too good to be true" prices often via social media or auction sites to trick people into purchasing something that doesn't exist. They often use images taken from genuine sellers' to convince you they're the real deal. They may also ask for payment prior to delivery and send fake receipts and invoices that seem to be from the payment provider.

INVESTMENT SCAMS

A simple search engine click for terms, such as "best bonds" or "cryptocurrency" can result in numerous paid adverts or comparison websites' results claiming to be from legitimate investment firms offering guaranteed returns with minimal risk. In many cases, you're asked to complete a "Contact Form" with your details for a call back to be arranged.

Criminals also often use the names and logos of genuine investment firms to set up cloned websites. You may receive paperwork with official branding or even receive initial payments as a result of your investment to convince you to invest larger sums of money.

Investment opportunities advertised on social media may seem genuine, using celebrity endorsements or testimonials from people who've allegedly received large profits, but in reality, these are fake.

TYPES OF FRAUD AND SCAMS (CONTINUED)

ROMANCE SCAMS

The ease of online dating services often means you can find the love of your life in the comfort of your own home. However, this also provides criminals with an opportunity to gain your trust and build a relationship with you by using information and fake identities found on social media – also known as catfishing. Criminals will claim to declare strong feelings for you just after a few conversations before pretending to need money for a personal emergency or flights to visit you.

DOORSTEP SCAMS

Doorstep criminals can come in all sorts of disguises, from dodgy salesmen to unscrupulous tradespeople and, can be very convincing. They may claim to have noticed something about your property that needs work or improvement, such as the roof, and offer to fix it for an inflated price with payment required upfront. Some criminals may even convince you to visit your bank branch to withdraw money whilst they set up their equipment.

COURIER FRAUD

If you're contacted by someone purporting to be from your bank or the police, take a moment to question their authenticity. If the caller is from the bank, they may claim that their system has spotted a fraudulent payment on your card or that it is due to expire and needs to be replaced. They may even confirm personal details about you, such as your full name and address and offer you peace of mind by having someone such as a courier collect your card to save you from having to go to your bank or local police station. You may even be asked to write down your PIN and place it in a separate envelope to that of your card.

HOW CAN YOU PROTECT YOURSELF AGAINST FRAUD AND SCAMS

If you receive a request to provide personal or financial information whether that's over the phone, in an email, online or through social media always remember:

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

STOP: Taking a moment to stop and think before parting with your money or information could keep you safe.
CHALLENGE: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
PROTECT: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

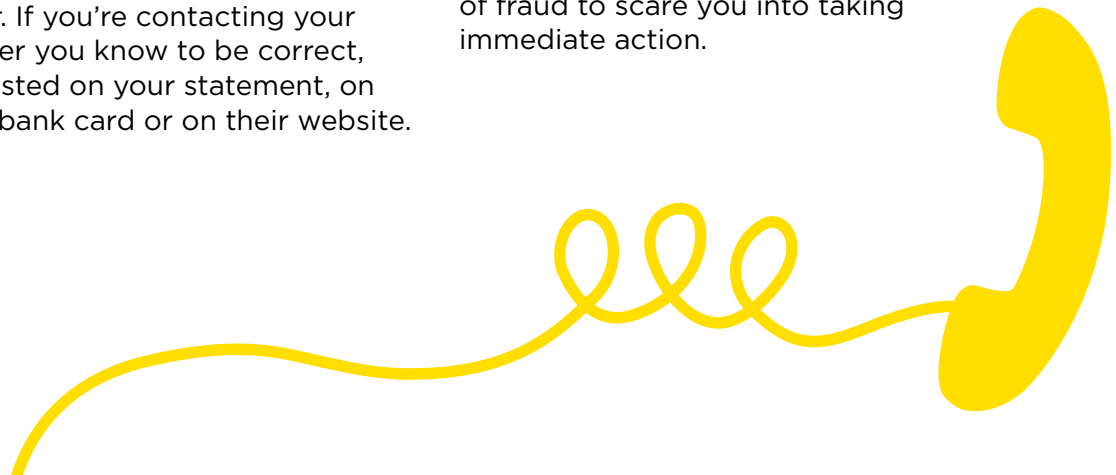
Here are some general tips to keep in mind to help protect your money and information:

1. AVOID DISCLOSIING 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 a known email or phone number. If you're contacting your bank use a number you know to be correct, such as the one listed on your statement, on the back of your bank card or on their website.

2. EMAILS, PHONE CALLS AND TEXTS MAY NOT BE AUTHENTIC

Just because someone knows your basic details (such as your name and address mother's maiden name or date of birth), 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 taking immediate action.



3. CONTACT ORGANISATIONS DIRECTLY

Criminals may offer a phone number for you to call which in some cases matches the number on the back of your bank card to give the impression that the call is genuine. The number offered is not genuine or, where a genuine number is suggested, the criminal will keep the line open and pass you to a different individual in order to convince you to share your personal and financial information.

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 hang up, wait a few minutes before calling them on a number you know to be genuine, such as the one on the back of your card.

HOW CAN YOU PROTECT YOURSELF AGAINST FRAUD AND SCAMS

TAKE FIVE TO STOP FRAUD™

4. STOP AND CHALLENGE UNEXPECTED REQUESTS

If you receive an unexpected request for your money or information, have the confidence to stop and challenge its authenticity. Criminals may lull you into a false sense of security when you're out and about or rely on your defenses being down when you're in the comfort of your own home. Remember it's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

5. PROTECT OTHERS BY REPORTING FRAUD AND SCAMS

Reporting fraud and scams could help recover your money and catch the criminals responsible. If you've fallen for a scam, report it to Action Fraud on 0300 123 2040 or via **actionfraud.police.uk**. If you're in Scotland, please report to Police Scotland directly by calling 101 or Advice Direct Scotland on 0808 164 6000.

If you receive a scam text message you can forward it to 7726 to help phone providers take early action and block numbers that generate spam on their networks. If a scam text claims to be from your bank, then you should also report it to them.

You can also forward fake emails you've received to **report@phishing.gov.uk**.

Make sure you report scam ads appearing in paid-for space online by visiting the **Advertising Standard Authority's website** where you can complete their quick reporting form.

ALWAYS REMEMBER

TAKE FIVE TO STOP FRAUD™

- Only provide organisations that you trust and have given consent to with your personal or financial details.
- Question uninvited approaches and contact companies directly using a known email or phone number to verify requests.
- Just because someone knows your basic details doesn't mean they're genuine.
- Never disclose your PIN or let anyone persuade you to hand over your bank card, financial information or withdraw cash.
- One-Time Passcodes (OTPs) should be treated in the same way as your PIN in that they should never be shared with anyone, including your bank. Before entering your passcode make sure you check it accurately describes the transaction/purchase you're about to make.
- Be suspicious of any "too good to be true" offers or prices – if it's at a rock bottom price ask yourself why.
- Avoid clicking on any links or attachments in social media posts, emails or texts.
- Request copies of your personal credit report from a credit reference agency on a regular basis to check for any entries you don't recognise.
- Cancel any lost or stolen credit or debit cards immediately.
- Keep your personal information secure when using your card over the phone, on the internet, or in shops by ensuring that others can't overhear you or see your information.

YOUR BANK OR THE POLICE WILL NEVER:

- Ask you for your One-Time Passcode (OTP), PIN or full banking password, including tapping them into your phone.
- Ask you to transfer money to a 'safe account' for fraud reasons, even if they say it is in your name.
- Call you to ask to verify your personal details or PIN by phone.
- Send a courier to collect cash, PIN, cards or cheque books, even if they say you have been a victim of fraud or a scam.
- Contact you to participate in an investigation in which you need to withdraw money from your bank or to purchase high-value goods for safe-keeping.

ALWAYS REMEMBER

TAKE FIVE TO STOP FRAUD™

- Be cautious of approaches presenting you with exclusive investment opportunities. It could be a scam if you're being pressurised to act quickly. It's also important that you do your research and proceed with extreme caution before making any investments.
- Where possible, use a credit card when making purchases over £100 and up to £30,000 as you receive protection under Section 75.
- Read online reviews to check websites and sellers are genuine, and ask to see high value items in person or via video link, as well as getting copies of the relevant documentation to ensure the seller owns the item.
- Use the secure payment method recommended by reputable online retailers and auction sites instead of paying via bank transfer.
- Avoid sending money to someone you've never met in person, particularly if you have only recently met online.
- Check the **Financial Conduct Authority's register** for regulated firms, individuals and bodies. You can check their website is genuine by checking their web address. It should always begin with **fca.org.uk** or **register.fca.org.uk**. Ensure you only use the contact details listed on the Register to confirm you're dealing with the genuine firm before parting with your money and information.
- Only let someone in if you're expecting them or they're a trusted friend, family member or professional. You can also ask to check their credentials and confirm they're genuine by contacting the organisation they're from directly using a known number and not using the contact details provided to you.

SUPPORTING MATERIALS

We want organisations and businesses to be able to spread the message and get involved in the campaign which is why we have designed and produced collateral for you to use for free.

You can access our full suite of campaign materials, available in both English and Welsh, by visiting https://takefive-stopfraud.org.uk/toolkit/ to help make your event a success. We have also provided braille and large-print versions of our leaflets which can be found here.

Before using any of our material, please ensure that you've downloaded and read our brand guidelines.

ENDORSEMENT LOGO

TAKE FIVE TO STOP FRAUD™

FURTHER INFORMATION

For more information on Take Five and advice on keeping safe from fraud and scams, visit us at **https://takefive-stopfraud.org.uk**, where you can also access our full suite of campaign materials in our **toolkit**, which includes print-ready collateral for sharing with your family and friends.

Stay in touch on:

facebook.com/TakeFiveStopFraud

twitter.com/TakeFive

instagram.com/takefivetostopfraud/

If you have any enquiries, please contact takefive@ukfinance.org.uk and we'll endeavor to provide our assistance. We'd also love to see photos from your events so make sure you tag us on social media, or alternatively send them directly to us.