Devon and Cornwall ALERT

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Stop! Think fraud.

Dear subscriber,

Did you know?

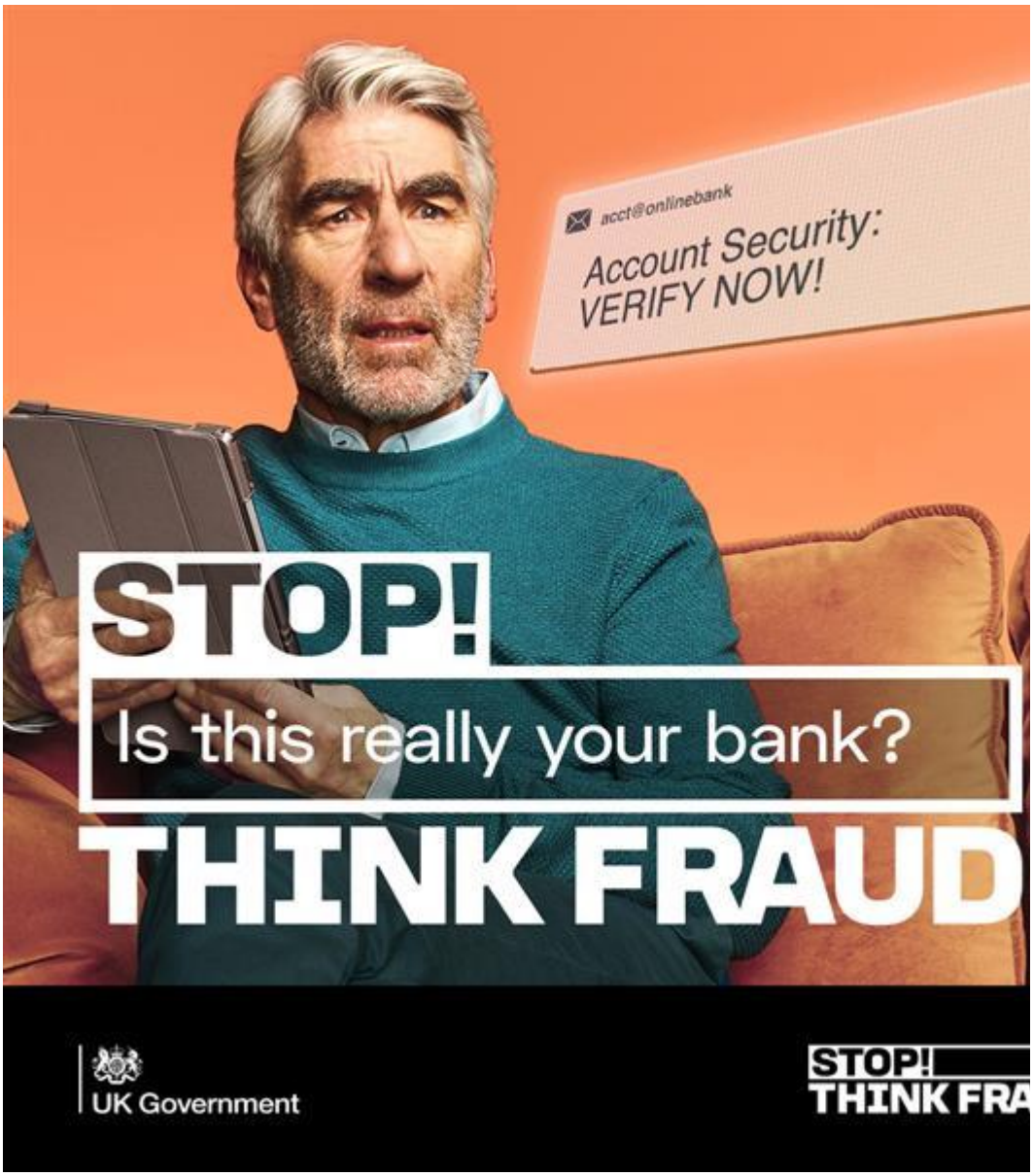
Fraud accounts for almost 40% of all crime. In just one year, 1 in 17 adults in England and Wales were victims of fraud. That's nearly 3 million of us.

1 in 5 businesses were also a victim of fraud over a 3 year period. In other words, fraud is rife and it can happen to anyone.

Think you're immune from fraud?

Fraudsters can use highly manipulative methods to get us when our defences are down. Nobody is immune from fraud. We can all be more alert to the risks, and we can all do more to protect ourselves.

4 ways to frustrate a fraudster



Q1. Do you stop to check who's really contacting you?

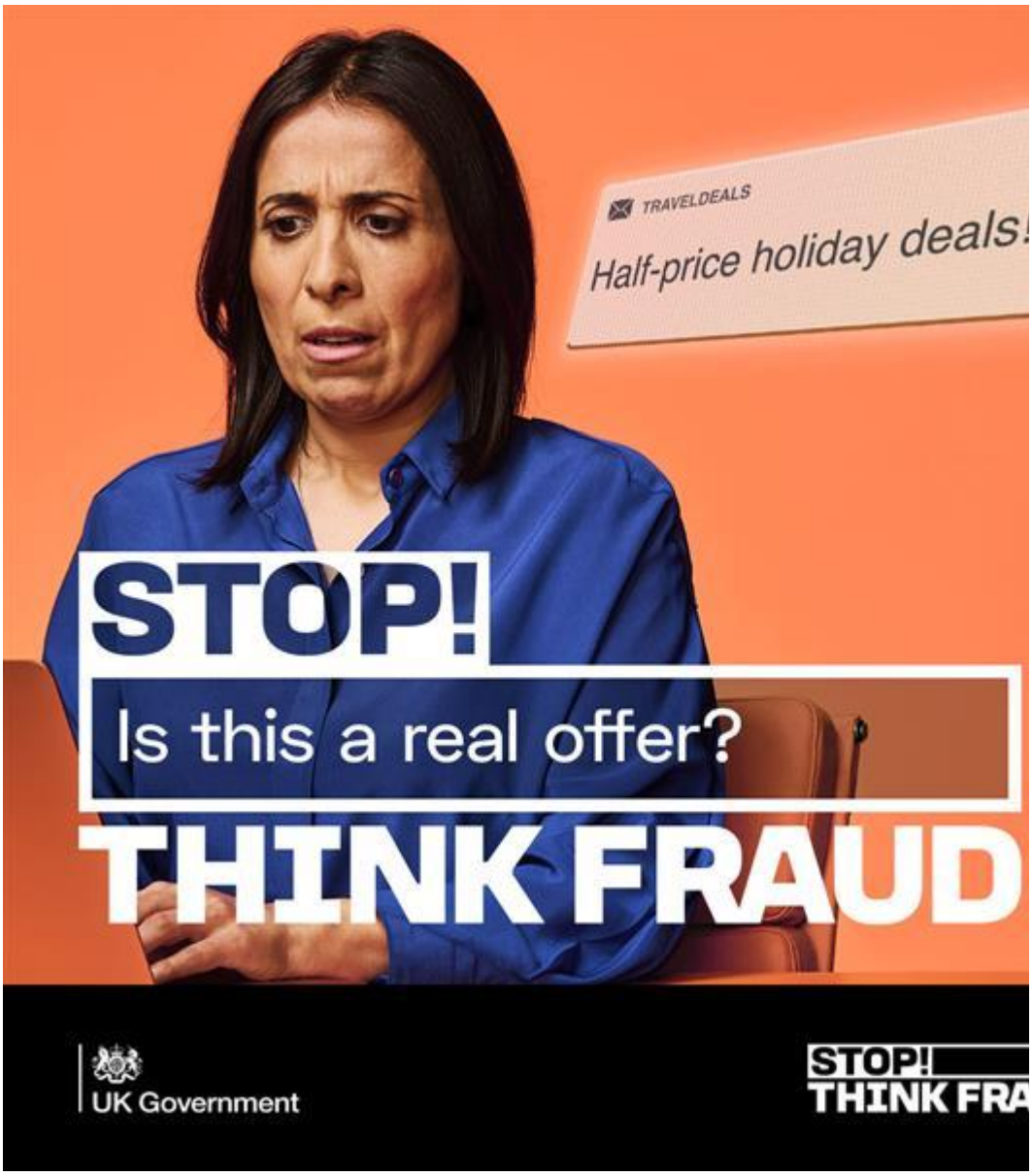
Fraudsters often call or message people, pretending to be from their bank, other well-known and trusted companies, or even someone they know. They can be very convincing, particularly if they've already managed to get hold of some personal information, for example by looking on social media. Having earned their victim's trust, they often ask them to hand over confidential information, make a payment or give them access to their phone or computer.

How to reduce your risk

Never take calls or messages like this at face value – always take time to stop, think and check if the caller or sender is who they say they are.

If you've received a suspicious call or message:

- don’t be rushed into a quick decision – think carefully before handing over money, personal details or access to your device
- if you have any doubts, hang up and do not call the number provided
- be aware that fraudsters can spoof phone numbers, so the number that appears on your caller ID may not be proof of who they are
- instead, check with the organisation directly using contact details you know are correct, such as those on a utility bill, official website, on the back of your card or by 159 for banks
- if you get a message from a family member asking you to send money, use known contact details to check if it’s real



Q2. Do you automatically trust offers and click on links?

“Half-price tickets to a sold-out gig!” “Incredible savings on a last-minute holiday – hurry!” Fraudsters know most people love a bargain, so they use discounts, time pressure and FOMO (fear of missing out) to pressure them into paying out for non-existent deals. Or they urge people to click on links in phishing messages that can take them to a fake website, where the fraudster can steal cash and personal details, or infect the victim’s device.

How to reduce your risk

If you see a tempting offer:

- don’t be rushed into a quick decision – always take time to stop, think and check if the message, offer or advert is genuine
- don’t automatically click a link, particularly in unexpected messages
- if you’re not 100% sure, don’t use the link to click through – go direct to the organisation’s website
- always stay on trusted websites and use the site’s recommended payment methods
- avoid paying by bank transfer or virtual currency
- think carefully before you hand over any money or personal details

Q3. Do you use the same password for different accounts?

Lots of people use the same password for multiple accounts, such as email, bank account and social media accounts. Less to remember, right? But imagine if a fraudster gets hold of that password. Now they can access all of their victim’s online accounts.

How to reduce your risk

Choose a different password for each account. Too difficult to remember them all? You can keep track of passwords using a password manager, or by using three random words to make them more memorable.

You should:

- never choose a password that features names, places and numbers that are personal to you
- choose a different password for each account that is strong and hard to guess but if you can’t change them all at once, prioritise your email account

Q4. Do you use 2-step verification?

Even if someone has chosen strong and unique passwords for their email and bank accounts, there’s always a risk – however small – that a fraudster could get hold of them. If they do, there’s nothing to stop them accessing those accounts to steal money and other personal details.

How to reduce your risk

Setup 2-step verification (2SV) on your most important accounts, such as email and social media. 2SV works by asking for more information to prove your identity when you're logging into an online account. It's one of the most effective ways to protect your online accounts from criminals.

For more information, please visit: https://stopthinkfraud.campaign.gov.uk

(If you found this information useful, please forward it to friends, family and colleagues)

Message Sent By
Action Fraud
(Action Fraud, Administrator, National)