GUIDANCE ON POTENTIAL FRAUD RISKS FOR DAVIES CUSTOMERS

Below we will discuss some of the most common financial scams, how to reduce your chances of falling victim to them, where to report them and what to do if you do get tricked by a scam.

Social media scams

Personal information provided online can be sold to third party users, which is how some scammers might have your personal information. Or you might have simply put too much of your personal details on your public profile. What you share on social media can be seen by a lot of people, so make sure you only connect with people you know and keep important details private.

The first step to keep safe online is to review all social media presence and make sure that all information that can identify you is kept safe. You can do this by checking the privacy settings on all social media websites, as well as remove any dates of birth, mentions of your address and email from your profile and only provide this information to people you trust.

If you use a shared computer, make sure to log out of your accounts.

Make sure you use a strong password and avoid reusing them – if one of your passwords becomes compromised, all accounts sharing the same password are now at risk.

Keeping your personal details safe can save you a world of trouble when it comes to scammers!

Scam calls/cold calls/vishing

A 'scam call' is when someone rings you and pretends to be someone you normally would trust and provide your sensitive data to such as insurance companies, banks, police, hospitals, HMRC, Home Office etc.

The aim of that call is for you to provide your banking information and ideally transfer money to the fraudsters account.

Some **common things** a scam caller might say are:

- Your cancelled/non-existent policy has an outstanding balance that you need to pay.
- Your policy is due for a review.
- We can give you the same cover for an ultra-low price.
- You have been involved in an accident and are due a big pay out (usually tens of thousands of pounds).
-
-

- You have a refund pending but they are unable to process this as they do not have your banking details (which is why all companies will only issue refunds to cards you have paid with originally, to prevent this from happening).
- Your account is at risk of fraud, to avoid it you need to transfer your money to a "safe" account.

Plus, many more.

It is important to stay vigilant, sometimes scam callers are very persuasive and seem genuine. Here are some additional tips on how to **spot** a scam:

- Say you will call them back, if they provide you with a number, say you will ring the number found on your policy/bank details/company's website.
- The caller pressures you into making a decision or asks you to keep quiet about this call.
- Robocalls and automated messages.
- The caller mispronounces company names or forgets their own name (scammers often use fake names).
- The caller provides you with outdated details (an address you don't live at anymore or a previous surname).

So, what can you do?

- Set up a scam code to include in communications so that you know the call is genuine.
- Hang up the phone.
- Call back on a number you can trust.
- Do not provide personal details.
- Do not log onto your computer if prompted.
- Do not let anyone take control of your computer or say what you can see on your computer screen.

Scam messages and emails

Like with scam calls, fraudsters might use messaging services like SMS, WhatsApp or email to try and get personal and financial information about you.

Things to look out for when receiving text messages and emails are:

- Spelling mistakes
- Links to fake sites or fake numbers to call.
- Messages prompting you to click a link to log in or give banking details.
- Angry or threatening tone in the message.
-

- How the does it greet you? Genuine companies will always use your correctly spelled surname and sometimes include a part of your account number.
- Check the email address, if unsure, compare it to any previous messages received from the company (we will always email you from a '@davies-group.com' email address).
- If you receive a message prompting you to pay, always call the company on a number you can trust.

What can you do?

- Always make sure the message is genuine, do not reply to it and call the sender, but **DO NOT** use the number provided in the message/email.
- If it's prompting you to visit a website, it is always best to google the page instead. See point above if you're still unsure.
- Take your time, do not give in to threatening messages.
- Check the email address (Davies will always email you from a '@davies-group.com' email address, be aware of variations such as @davies-group.co.uk or org.uk as these are not genuine).

Useful source of information

https://www.lloydsbank.com/help-guidance/protecting-yourself-from-fraud/latest-scams.html

I've given my money to a scammer, what can I do?

Report it to Action Fraud via www.actionfraud.police.uk or by calling 0300 123 2040.

Contact your bank's fraud team.

If you feel comfortable, share the scam with your friends to raise awareness.