SCAM TEXT MESSAGE ADVICE

BBC RIP-OFF BRITAIN

Rip Off Britain's tech expert David McClelland and solicitor Gary Rycroft have put together this handy guide to help you avoid falling victim to fraudsters...

How can I tell a scam text from a genuine text message?

- Don't panic!
- It's natural to think you have to reply straight away, but think about it first
- Take some time to look at the message closely.

Gary says...

"The key message is to be really suspicious about any message that you get out of the blue."

A good place to start is looking for the following signs that indicate the message may be a scam:

- Unknown numbers
- Requests for payment or payment details
- 'Urgent' requests
- Carefully examine website links & check for any characters out of place
- Spelling or grammatical errors

David says

"A number of legitimate companies are now not including links in messages they send to their customers"

- Fraudsters are finding ways around some of these indicators, including 'spoofing'. This is where fraudsters use identity masking technology to change the name or number that is displayed as the sender. This can make it look like the text has come from your bank's number or from an organisation like 'NHS' or 'GOV UK'. So even if it looks like the text has come from a legitimate source, you still need to take it with a pinch of salt!
- If in doubt, contact the company or organisation you think sent the text and ask if it's genuine. Look online for a number for them – don't try to call the number the text came from.
- Some organisations and companies have information on their website about how they will contact customers or users.

"REMEMBER... Scams and threats don't just apply to text messages but other messaging services too - such as WhatsApp and Facebook Messenger. Be extra vigilant for the **"Hi Mum and Dad"** scam message. This is where scammers impersonate your family members, particularly adult children, in order to ask you for money. **'Hi Dad, I've broken my phone and I'm using a mate's phone. I need to talk its urgent can you text me on WhatsApp on my new number please.'**

If you receive a message like this don't be tempted to transfer money immediately, enquire further by asking who specifically it is by name and by calling them or asking for a voice note.

David says

What do I do if it turns out the message is a scam?

- Don't reply to a scam text. It informs the scammers your number is active and you could be bombarded with more scam messages.
- Do not click on any links, even if they look genuine. Clicking a link could result in malware being downloaded onto your phone that compromises your data.
- Do not share personal or banking information.
- You can report the scam text by forwarding it to 7726, which is a free reporting service provided by phone operators. This information can then be used by your provider to investigate the origin of the text message and arrange to block or ban the sender.

I've replied to a scam text, what should I do?

- If you've shared your banking details, you should contact your bank immediately.
- If you've shared your password, change the passwords on any of your accounts which use the same password.
- If you've lost money, tell your bank and report it as a crime to Action Fraud (for England, Wales and Northern Ireland) or Police Scotland (for Scotland).