Stay safe from fraud

Criminals use exceptional circumstances, like the current COVID-19 situation to lull people into believing that the contact they're making is genuine.

They pretend to be from your building society, bank or the police and claim they're dealing with coronavirus-related issues that require you to respond by paying money or providing personal information that will allow them to access your account.

They often use pressure tactics to stop you thinking about want they want you to do for them.

To be clear, a building society or bank will never:

- Ask you to disclose details about your accounts or where relevant
- Encourage you to move funds from your own account into a different "safe" account
- Encourage you to order and pay for UK cash via the phone or internet.
- Charge up-front fees for repayment holidays
- Make home visits to collect mortgage arrears on your doorstep
- Demand an immediate payment of mortgage arrears over the phone
- Demand payment of mortgage arrears via email providing you with a link through which to make payments.

Individuals who approach you saying they're building society or bank employees and who pressurise you in the ways listed above are criminals.

COVID-19 Scams to be aware of

The following are some of the recent scams fraudsters have been using that you need to be aware of.

Door to Door Scams

Fraudsters have been targeting vulnerable people and those who are self-isolating by going door to door offering to do shopping, collect medication, cleaning and other odd jobs.

This may seem like a genuine act of kindness, but fraudsters are asking for payment upfront and not returning.

Online Shopping Scams

Fraudsters like to pose as legitimate online sellers on platforms such as eBay, enticing people to buy products or services that are either extortionately priced, fake, poor quality or non-existent.

Recently fraudsters have exploited the COVID-19 situation by selling in demand products such as hand sanitisers, face masks and home testing kits online. Worryingly they've also been selling products that claim to protect you or cure you from COVID-19.

Email Scams (Phishing)

Fraudsters have exploited the recent economic uncertainty and people's money worries from COVID-19, by sending emails posing as trusted organisations such as HMRC and banks saying that you can get a refund on taxes, utilities and other bills. This is to trick people affected financially by COVID-19 into providing sensitive information.

These emails direct you to a website or provide you with a phone number where they'll ask you to provide personal and financial information which they'll then use to carry out fraudulent activities, such as using your credit card to stealing your money.

Texting Scams (Smishing)

Fraudsters use clever methods such as spoofing (replicating) official looking numbers, for example from the government and other trusted organisations, to lull people into thinking that they're receiving genuine texts.

Recently fraudsters took advantage of a Coronavirus alert from GOV.UK, spoofing (replicating) the number to send texts to people warning that they've been fined and providing them with a link to a bogus payment page.

Fake Mobile Apps

Fraudsters create enticing or copycat mobile phone applications to get people to download malware onto their phone which then gives them access to personal and financial information.

Recently fraudsters created phone applications that claimed to give you updates on the current Coronavirus infection rate in your area but instead of doing that, they'll lock your phone and demand a ransom.

Impersonation Scams

Fraudsters impersonate trusted organisations such as government departments, banks and building societies to persuade people to make fraudulent transactions.

Some recent examples of impersonation scams include texts and emails impersonating HMRC asking people to provide banking details to apply for a 'goodwill payment', requests from people impersonating suppliers of services asking people to change their bank transfer mandate due to the current circumstances and requests from people impersonating charitable organisations asking for donations for COVID-19 related causes.

Tips you can take to avoid being scammed:

- Be cautious and listen to your instincts. Don't be afraid to hang up, bin it, delete it or shut the door.

- Take your time; don't be rushed.

- Be suspicious of requests for money up front. If someone attempts this approach to persuade you into accepting a service, they're unlikely to be genuine. Check with family and friends before accepting offers of helps if you're unsure.

- If you're online, be aware of fake news and use trusted sources such as gov.uk or NHS.uk websites. Make sure you type the addresses in and don't click on links in emails.

- Only purchase goods from legitimate retailers and take a moment to think before parting with money or personal information.

- Know who you're dealing with - if you need help, talk to someone you know or get in touch with your local Council.

- Protect your financial information, especially from people you don't know. Never give your bank card or PIN to a stranger.

Remember

Stop – Take a moment to think.

Challenge – Don't be afraid to ask questions or to say "No" and end the conversation.

Protect – If you think you've been the victim of fraud, contact the building society or bank from which you've made the payment immediately

For more information on protecting yourself from fraudulent activities visit https://takefive-stopfraud.org.uk/

If you think you've been scammed, report it to Action Fraud on 0300 123 2040 and if you need advice, call the Citizens Advice Consumer Helpline on 0808 223 1133. If you are in immediate danger, contact the police on 999.