Devon and Cornwall ALERT

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Watch out for this WhatsApp scam

Dear Subscriber,

Large community and religious WhatsApp groups are being targeted by scammers who infiltrate them to try and deceive their members into sending them money. Since January of this year, 268 people have reported falling victim to this scam.

The fraud often begins when a member of the group receives a WhatsApp audio call from the fraudster, pretending, or claiming, to be a member of the group. This is done in order to gain the individual's trust, and often the scammer will use a false profile picture and / or display name, so at first glance it would appear to be a genuine member of the group.

The fraudster will then call the victim and say they are sending a one-time passcode which will allow them to join an upcoming video call for group members. The scammer then asks the victim to share this passcode with them so they can be "registered" for the video call. What's really happening is that the scammer is asking for a registration code to register the victim's WhatsApp account to a new device where they then "port" their WhatsApp profile over.

Once the fraudster has access to the victim's WhatsApp account, they will enable two-step verification which makes it impossible for the victim to access their account. The scammer will then message other members of the group, or friends and family in the victim's contacts, asking them to transfer money urgently as they are in desperate need of help.

Oliver Shaw, Detective Chief Superintendent and Head of Action Fraud and the National Fraud Intelligence Bureau (NFIB) said:

"WhatsApp continues to be a popular platform for community and religious groups, but sadly also for fraudsters. Here, the scammers rely on the goodwill of group members and their intrinsic desire to help others in distress.

"We urge people always to be wary when receiving contact via WhatsApp or other messaging platforms. This is particularly the case when being asked to provide account information – despite the fact that you may recognise the individual's profile picture and / or name.

"Never share your account information with anyone, and if you think it's a fraudulent approach, report the message and block the sender within WhatsApp. To make your account more secure, we advise setting up two-step verification to provide an extra layer of protection. This makes it increasingly more difficult for fraudsters to gain access to somebody else's WhatsApp account".

Analysis of Action Fraud reports indicate that victims targeted by this scam are often part of large WhatsApp community, alumni and academic, work groups, and religious groups (such as church or prayer groups).

What can you do to avoid being a victim?

- **Never** share your account's two-factor authentication (2FA) code (that's the six digit code you receive via SMS).

- **Set up two-step verification** to give an extra layer of protection to your account. Tap Settings > Account >Two-step verification > Enable.

- **THINK. CALL**. If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity.

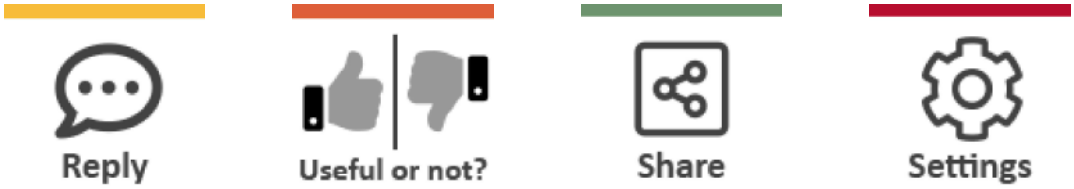
- You can **report spam messages or block a sender within WhatsApp**. Press and hold on the message bubble, select 'Report' and then follow the instructions.

If you have been a victim of fraud or cybercrime, report it at www.actionfraud.police.uk or by calling 0300 123 2040. In Scotland, victims of fraud and cybercrime should report to Police Scotland on 101.

(If you have found this information useful, please forward the email to a friend, family member or colleague)

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

To reply or forward please use the below or these links: Reply, Rate, Forward / Share.



To login to your account click here, to report a fault click here, or unsubscribe

---

Information, advice and feedback

Information displayed in this section may not be directly related to the above message.

Who can see your data:

The organisations listed below are available "Information Providers". The ones that you currently share your data with and are willing to receive messages from are marked with a tick. If you are happy with these settings you do not need to do anything. To find out more about any of them and to change this list, please click the setting button below.

- ☑ Action Fraud (NFIB)
- ☑ The Police (Recommended)
- ☑ Get Safe Online
- ☑ Local Authority
- ☑ Neighbourhood Watch
- ☑ Office of the Police & Crime Commissioner

Review more info and update these settings