



## A fraud involving WhatsApp groups

WhatsApp groups are being targeted by scammers who infiltrate these groups, then deceive the group's members into sending them money.

This 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.

Please 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.

### **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.

by calling 0300 123 2040.



**Message Sent By**  
Linzi Berryman  
(Police, Alert Officer, Devon & Cornwall)

---

To reply or forward please use the below or these links: [Reply](#), [Rate](#), [Forward / Share](#).



Reply



Useful or not?



Share



Settings

To login to your account [click here](#), to report a fault [click here](#), or [unsubscribe](#)



You are receiving this message because you are registered on Devon and Cornwall Alert. Various organisations are licensed to send messages via this system, we call these organisations "Information Providers". Please note that this message was sent by The Police and that The Police does not necessarily represent the views of Devon and Cornwall Alert or other Information Providers who may send you messages via this system.

You can instantly review the messages you receive and configure which Information Providers can see your information by clicking [here](#), or you can [unsubscribe](#) completely, (you can also review our terms and conditions and Privacy Policy from these links).

This email communication makes use of a "Clear Image"(gif) to track results of the email campaign. If you wish to turn off this tracking for future emails, you can do so by not downloading the images in the e-mail itself. All links in the body of this email are shortened to allow click through monitoring.

VISAV Limited is the company which built and owns the Neighbourhood Alert platform that powers this system. VISAV's authorised staff can see your data and is registered with the Information Commissioner's Office as the national Data Controller for the entire database. VISAV needs to see your data in order to be able to manage the system and provide support; it cannot use it for commercial or promotional purposes unless you specifically opt-in to Membership benefits. [Review the website terms](#).