

ACCOUNT TAKEOVERS

Never share the code.



That six-digit code texted to you is the key to your account. Scammers – often using a friend's hacked account – will ask for it with a believable story.

CODE REQUESTS OFTEN COME FROM...



A friend's account

"I sent my code to you by mistake"



A group member

"You need a code to join the group call"



A vote or prize

"Vote for my niece – send me the code"

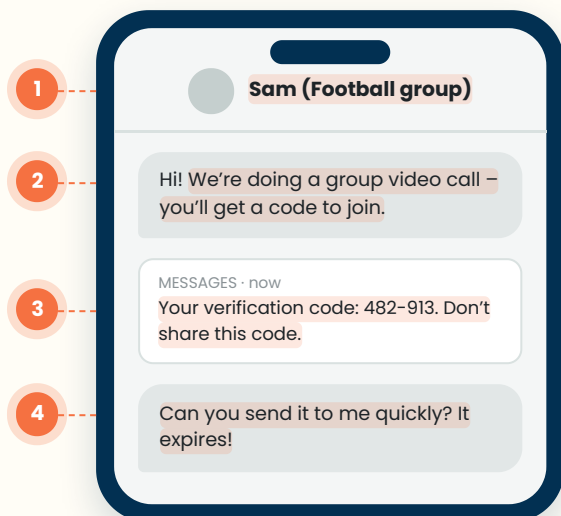


Fake "support"

"Confirm your code to keep your account"

Anatomy of a takeover

Could you spot all four warning signs?



Four warning signs

1

A familiar name

Accounts get hacked. A friend's name doesn't mean it's your friend.

2

A believable story

Group calls, votes and "mistakes" are all excuses to get your code.

3

The code says don't share

The text itself warns you. The code is only ever for you.

4

A rush

"Quick, it expires" stops you asking why they need it.



At work

- **Work group chats can be hijacked too.** Check odd requests by phone.
- **Money or gift-card request** from a colleague's account? Call them first.



At home

- **Turn on two-step verification in WhatsApp** (Settings › Account) and your social apps.
- **Friend asking for money by message?** Call them before you send a penny.

Shared a code? Act now.

Sign back in to the app with your number to log them out, then warn your contacts another way.



WARN CONTACTS

Use another app or call

Your hijacked account may ask them for money.



REPORT IT

0300 123 2040

Report Fraud (in Scotland, call 101).



LOST MONEY?

159

Call your bank's fraud team.