Police Advisory Notice to Churches

WhatsApp Takeovers

Background

Leicestershire Police's Cyber Crime Unit proactively monitor crime reports to identify new and emerging trends in cyber criminality.

It has been identified that churchgoers who share groups on the messaging app WhatsApp are being targeted by criminals seeking to take over their accounts.

At this time, this appears to be targeted towards members of the African and Caribbean community, although the exact reasoning for this cannot be established at this time. It is possible that this offending will expand to include individuals of all backgrounds who use WhatsApp to discuss matters relating to a church.

WhatsApp accounts are linked directly to the telephone number of the owner.

When a WhatsApp account is compromised, the legitimate owner of the account will be unable to access it, and it will be under the sole control of the criminal(s). They will be able to send and receive messages under the guise of the legitimate owner.

Methodology

In order to obtain access to a WhatsApp account, the criminals will attempt to register the target phone number to a new device, as if the account owner had purchased a new phone.

To register the account to that new device, a text message containing a short numerical code is sent to the phone number. If the criminal is able to obtain this code, they can input this in to their device and gain access to the account.

The aim of the criminal is to engineer a situation where the account owner willingly hands over this code on false pretences.

Specifically, within church groups, this has been done as follows:

1. A *previously* compromised account is used to message members of the group stating that an online meeting is being set up, either for prayers or to discuss church matters.
2. The criminal, using a legitimate group member's account, states that they will send a code to the target, which they will need in order to add them to the meeting.
3. The criminal attempts to register the target phone number, triggering the confirmation text message to be sent.

4. The targeted victim is asked to provide that code in order to join the meeting.
5. Once the victim gives the code over, their account is registered to a new device by the criminals, who subsequently revoke the legitimate owner's access.

It is not necessarily important to understand the technicalities of the offence. The key message is that the criminals cannot access the account without knowing the code that has been sent to the target.

Key Messages

The advice to prevent these offences is simple, and we would appreciate your support in passing it on. Key headlines are underlined below, along with an advisory note containing more detail.

Never share access codes with anybody – this document relates specifically to WhatsApp, but this advice is important for all online accounts. These codes are generally six digits long, and sent via text message. Even if the request comes from somebody you trust, there is no legitimate reason why anybody would ever need to know these codes, and you should never share them.

Double check any unusual messages – criminals use previously compromised accounts to carry out further offences. If you receive a message, even from somebody you know, asking you to do something, check this with them first. You may wish to call them, or ask them in person.

Activate two step verification on WhatsApp – this is a security feature which requires an additional memorable code, set by the user, before any changes can be made on the account. A guide on how to do this is included in Appendix A.

Report any fraud or cyber offences to Action Fraud – all cyber and fraud offences are reported nationally through the Action Fraud service. This can be done at their website (www.actionfraud.police.uk) or via the telephone (0300 123 2040).

Conclusion

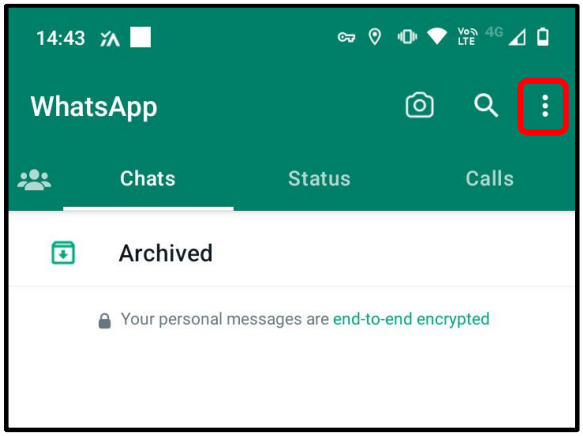
Leicestershire Police are committed to working with the community, and leaders within it, to protect individuals from cyber crime. Your assistance in this work is greatly appreciated.

If you wish to arrange a visit to your congregation, where we can provide additional guidance on how to avoid becoming victim of cyber crime, please get in touch via email:

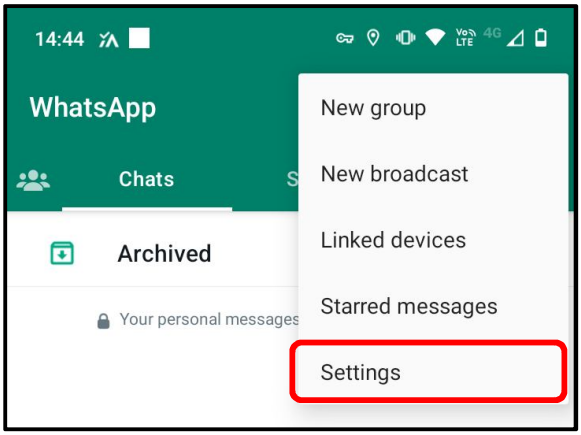
cyber.protect@leics.police.uk

Appendix A

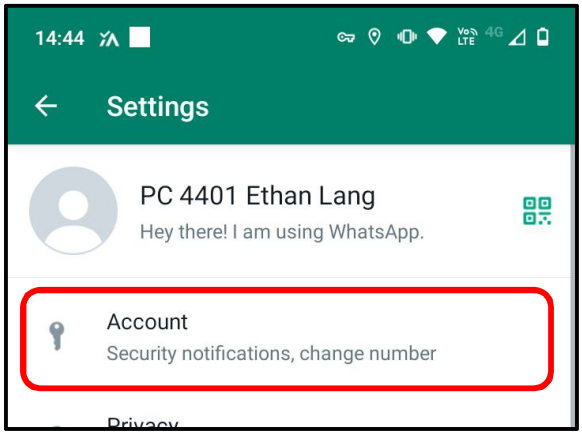
Two Step Verification



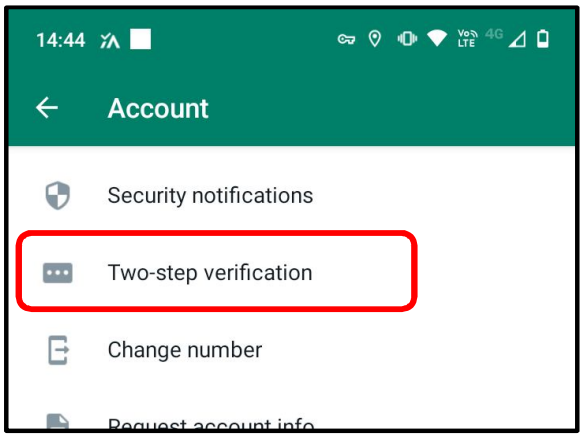
Select the three dots from the top right hand of the WhatsApp home screen.



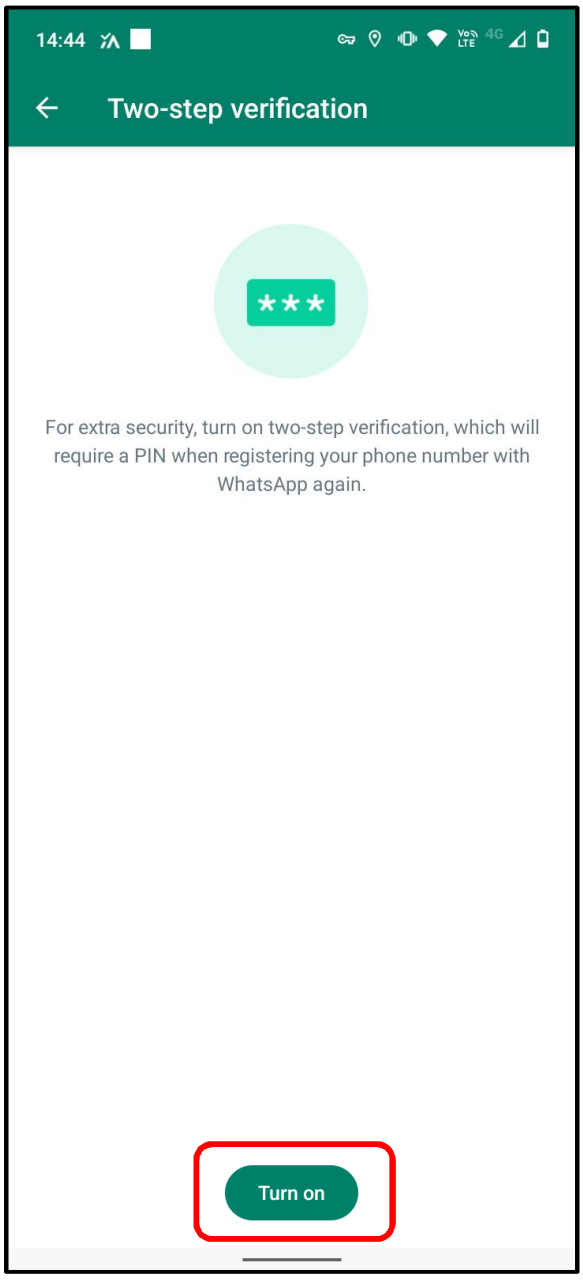
Select ‘Settings’ from the menu that appears.



Select ‘Account’



Select ‘Two-step verification’ from the list presented.



Select ‘Turn on’.

Create a **memorable** six digit PIN, but avoid birthdays.

Confirm this PIN.

Register your email address.

Confirm your email address.

Two step verification is now active, and this six digit code will be required to register the account to a new device.

NEVER SHARE THIS CODE.