

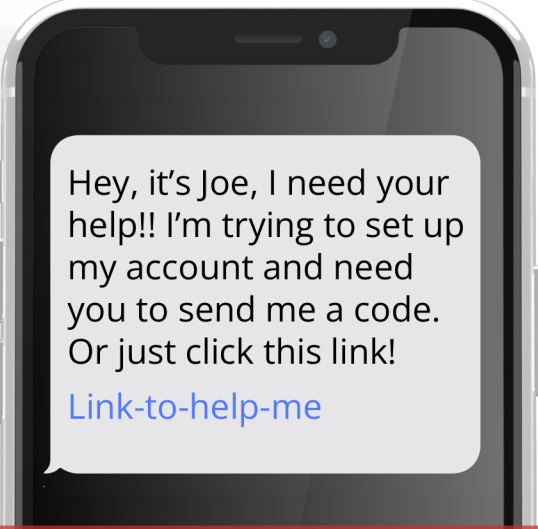
# THE "HELP ME SET UP A NEW ACCOUNT" SCAM

Fraudsters use compromised social media accounts, impersonating people on your friends list to ask you for a favour. Stay skeptical!

Fraudsters will claim they need your help setting up a new account, asking you to **provide a code**, or to **click on a link** to complete the setup.

Once you provide the code or click on the link, **your own account gets compromised**.

Once compromised, the fraudsters **impersonate you, sending messages from your account** to your contacts asking for the same favour.



Hey, it's Joe, I need your help!! I'm trying to set up my account and need you to send me a code. Or just click this link!  
[Link-to-help-me](#)

Clicking on a malicious link can lead to bank account takeovers, identity theft or malware infection.

## HOW TO PROTECT YOURSELF

If you receive a message on social media, email, text message or a phone call asking for a favour, contact the person directly using the phone number you have in your contact list.

Never click on links from unsolicited messages.

If you receive a request to provide a code, it is likely part of the dual authentication process to access your account. Never provide the requested code!

Remember that simply clicking on a link can potentially infect your cellphone or device and put you at risk for identity fraud.

If you are asked to provide a code to someone, remember that their account could be compromised. If the code is provided, you are potentially giving them access to your account.

Combating cybercrime  
through collaboration



KnowledgeFlow.org