How to spot & avoid Facebook scam

RED FLAGS

A SECOND 'FRIEND' REQUEST FROM THE SAME PERSON

It is very possible that this is an account cloning scam. Alert the person that someone might be impersonating them on Facebook. It will also help to report the account as 'pretending to be someone else'.

ASKING FOR URGENT FINANCIAL HELP

Always check your facts before you help friends in trouble, especially if it is an urgent request for financial assistance. Never reply directly to an online account that could have been hacked. Find another way to contact your friend, based on information that you already have in your possession.

ACCOUNT ONLY HAS A FEW POSTED PHOTOS

Fake accounts tend not to post lots of photos. The scammer's aim is to use minimum effort to create the illusion that a real person is behind the account so they don't bother too much with fleshing out a personal life.

LIMITED OR UNREALISTIC BIOGRAPHY INFORMATION

If the biography information on the account seems fanciful or just plain unrealistic, then it's likely to be a fake account.

BLANK PROFILE

Blank walls are a dead giveaway for a fake account. If your possible 'new friend' has either no activity or just a few likes – then be suspicious.

PROTECT YOURSELF FROM IDENTITY THEFT ON SOCIAL MEDIA

Make your social media profile private.

Set the privacy of your posts to 'friends only'.

Look yourself up from time to time to see if there are any suspicious accounts using your name.

Do not just click on any link you see on your timeline, or receive on messaging apps.

Enable login alerts and multi-factor authentication.