

# Compromised Facebook accounts used to lure victims into PayPal scam



## Summary

Published on 18/08/20  
Reference 2007002

There has been a surge of reports where the recipient has received messages through Facebook Messenger from friends/family requesting to use their Pay Pal account to receive funds from the sale of items on EBay. Overall, between 1<sup>st</sup> June 2020 and 31<sup>st</sup> July 2020 a total of 95 reports have been made which specifically mention that the item sold was a camera.

Messages are sent by fraudsters purporting to be friends/family stating that they have sold a camera on eBay but that they are unable to process the payment as they either do not have a Pay Pal account or because their Pay Pal account is not working. The request is that the message recipient receives the funds into their own Pay Pal account, then, after transferring it into their own bank account, they forward it onto an account controlled by the fraudster.

If the victim agrees the payment is transferred into their Pay Pal account but, after the money is transferred out, the initial transaction is reversed leaving the account in negative balance.

Multiple reports have also been received from victims stating that their Facebook Messenger accounts have been hacked and that these fraudulent messages have been sent to all their contacts on their behalf.

The total reported loss for these reports is £44,035.

## What you need to do

**Verify financial requests:** Be wary of unusual messages asking for assistance with financial transactions. Even if the message appears to be from someone you know and trust, you should check it's really them that sent the message by calling them or speaking with them in person.

**Unusual financial requests:** Never respond to any requests to send money, or have money transferred through your account, by someone you don't know and trust.

**Secure your accounts:** You can protect your important online accounts by using a strong separate password and, where available, turn on two-factor authentication (2FA).

**If you have made a payment:** Inform your bank, or payment service provider, such as PayPal, as soon as possible. They can help you prevent any further losses. You should also monitor your bank statements regularly for any unusual activity.

For more information about how to protect yourself online, visit  
[www.cyberaware.gov.uk](http://www.cyberaware.gov.uk) and [takefive-stopfraud.org.uk](http://takefive-stopfraud.org.uk)

Every Report Matters

If you have been a victim of fraud or cyber crime, report it to us at [Actionfraud.police.uk](mailto:Actionfraud.police.uk), or by calling 0300 123 2040.