scam share

spotlight on...

PayPal Scams

Consumers who use PayPal to buy and sell goods online frequently receive scam emails and text messages.

what do PayPal scams look like?

Scam emails and texts often appear genuine and may include PayPal logos and branding. The aim of the messages is to encourage you to click on a link leading to a copycat PayPal website that asks you to enter your personal and financial information.
The most frequently reported scam emails and texts may say:

Your Account Has Been Limited
We've limited your account. After recent review of your account activity, we've decided that you are in violation of PayPal's Acceptable Use Policy. Click the link below to confirm your identity and review recent activity.

Check the security of your account

To avoid account suspension you need to accept our new terms and conditions. Please visit this link to confirm your account details...

Your account has been restricted due to a failed payment. Please log in using this link to remove any pending restrictions...

This email confirms that you have received a payment. It will not be reflected in your account balance until the buyer receives proof that the item has been shipped. Click on the link below to provide a tracking number so that we can release your funds.

We have limited your account due to safety concerns. Please visit this link to verify your details before we are forced to suspend services...

how can I tell if a message related to PayPal is a scam?

PayPal state on their website that they will NEVER ask customers for their password or credit card details via email or text.

PayPal NEVER hold funds on the condition that you confirm shipping.

If you are required to take action in relation to your account, PayPal will use the secure message service within accounts to contact you.

Genuine emails are sent from addresses ending in **paypal.com** and will include your name. If the email begins with 'Dear Customer' or Dear Client' it may be a scam.

Be suspicious of any unexpected message which appears to be from an official organisation and tells you that you must provide your details or a payment within a certain time frame.

what should I do if I get one of these messages?

Never click on links in unexpected emails or text messages and never enter any payment or personal details.

If you are unsure whether a message which appears to be from PayPal is genuine, **sign into your account on the official website.**

If you receive an email saying that funds have been received for an item you are selling, **log in to your account to check that the money has been fully deposited before sending the item.**

Report all scams to **Advice Direct Scotland** using their free consumer helpline: **0808 164 6000**

If you have lost money or are worried that you have given your bank details to scammers, contact **Police Scotland on 101**.

Find more information and advice on avoiding scams:

Advice Direct Scotland - www.consumeradvice.scot
Police Scotland - www.scotland.police.uk/keep-safe
Trading Standards Scotland - www.tsscot.co.uk/latest-scams
The National Cyber Security Centre - www.ncsc.co.uk

Trading Standards Scotland