Starling Bank

TAKE FIVE TO STOP FRAUD™

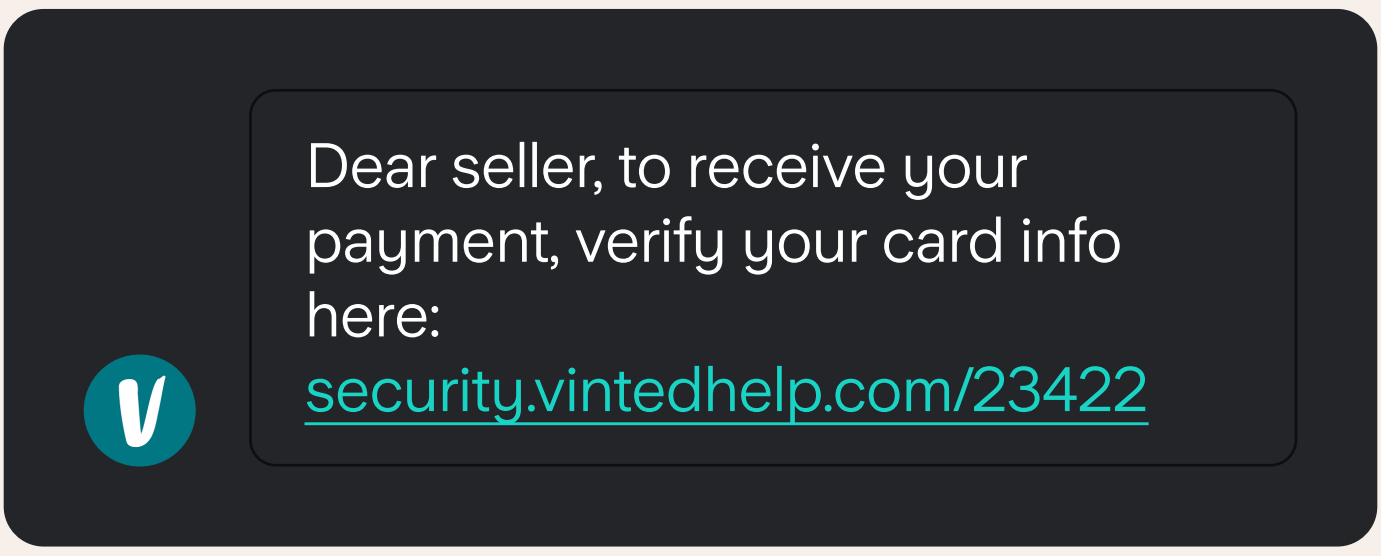
Keep yourself safe from

Online Marketplace Verification Scams

Online marketplaces such as Etsy, Depop or Vinted have unfortunately become popular platforms for criminals to scam people. Fraudsters pretend to be buyers of items, but actually have hidden intentions to trick you into paying money from your bank account.

First-time sellers are often targeted by receiving messages from scammers on the platforms or by an email with interest to buy their items. Once a sale is agreed, links are shared with sellers which direct the victim to a new webpage to claim payment for the sale by entering their card details on the screen. These links lead to fake websites and live chats where fraudsters impersonate employees of the marketplace.

Sellers may be told by the fraudster posing as a buyer that they need to complete an account or card verification before they can receive their payment. These criminals could also tell you, you need to authorise a ‘temporary payment’ or freeze the payment amount. This is a scam. You may receive a notification from your banking app asking you to verify a payment. If you go ahead and verify it, this will authorise a payment out of your bank account.



Top tips for avoiding marketplace scams:

- If you're new to marketplace platforms, familiarise yourself with the platform’s buying and selling terms and conditions.
- Carry out the buying and selling process through the retailer’s platform, don’t complete a sale through emails or messages you may be sent.
- Never reveal your personal information to anyone on these platforms. Criminals might send a request that looks like it’s from the marketplace via email, asking for payment information or personal details. If you’ve received suspicious emails or messages, do not click on any links.
- If you’re asked to look out for a notification from your banking app and then asked by someone claiming to be a representative of the marketplace to authenticate the payment, reject the authentication of the payment and find the marketplace’s number on their website to contact them directly.
- Check the sender's email address. Be cautious if it looks suspicious or is unfamiliar. Verify its legitimacy by contacting the marketplace platform directly.
- Phishing emails often contain mistakes. Pay attention to the quality of language used in the email.

If you’re ever unsure about a payment you've been asked to make, or already made, get in touch with us on your app or by calling 159. We’re here to help you. You might also want to speak to Victim Support, an independent charity that can provide support to victims of crime and traumatic events. Their **helpline** is open 24/7.