

# Fraud on online marketplaces

Whether furniture, electronics or tickets are involved – online marketplaces and small ad platforms such as Tutti, Ricardo or Facebook Marketplace are handy and popular. But they are also a playground for fraudsters. They use increasingly ingenious scam, especially as far as payment and shipment are concerned.

## This is how to protect yourself:

- **Look out for conspicuous communication:** If communication takes an unexpectedly swift or pressing turn, cease all contact.
- **Be wary of channel changes:** Watch out for people wanting to move from the sales platform to WhatsApp, text messages or e-mail communications. Reputable sellers or buyers have no reason to move to private channels.
- **Don't pass on any sensitive data to receive payment:** You never need any e-banking access details for any payment receipts, and there is no need to scan any QR code either.
- **Never pass on any codes or text messages:** Never pass on any text message codes, TWINT log-ins, e-banking or card data to third parties, not even for purported identification purposes.
- **In case of any suspicion, file a report:** Immediately report suspicious offers and contacts to the platform involved.

## This is how this scam works

Fraudsters use a clever approach: They write to users on platforms such as Tutti, Ricardo or Facebook Marketplace – often posing as legitimate buyers. The supposed deal is quickly done, but then the trap is set: Sellers will receive an e-mail, text or WhatsApp message supposedly originating from the marketplace involved.

It contains a link or QR code which will direct you to a fake website for payment and/or shipping purposes so to process the credit involved. The linked site looks very similar to the real post office, banking or TWINT websites. If you enter your details there, you fall straight into the trap. The attackers are trying to obtain TWINT, banking or credit card details – or to convince their victims to install PayPal, Revolut or something of a similar nature.

### Be wary of channel changes

Fraudsters like to quickly change from the sales platform to another channel of communication, such as WhatsApp, text message or e-mail. The reason: Away from the official platform, you are less protected, and sellers can hardly ever track fraudulent behaviour. Reputable sellers or buyers have no reason to move to private channels – in particular when sensitive topics such as payment or shipping are involved.

### A typical example:

*You offer something for sale on an online marketplace. Shortly after, a purported buyer sends you a friendly message to say they are interested. They suggest paying via TWINT and sending the goods by post. They are also sending you a link for a "credit" in the name of the marketplace. The website looks real, but is asking you for your TWINT or payment data.*

*Instead of receiving money, you unwittingly pass on your sensitive details to a fraudster.*

