How to identify sneaky ‘sellers’ who are out to scam

Do not let scammers pull the wool over your eyes. They prey on unsuspecting shoppers with deals that sound too good to be true.

From posing as sellers on social media platforms to sending you fake parcel delivery notifications, scammers on online shopping sites can cost you dearly.

Read on to learn how you can shop smart and protect yourself from common shopping scams.

WATCH OUT FOR THESE SCAMS

Here are 3 common types of online shopping scams. See how they work and how to protect yourself from them.

E-commerce scam

1. When browsing online platforms like Carousell and Facebook, you come across an ad for a deal that sounds too good to be true or a limited-time offer (e.g. for personal accessories and electronics).
2. After indicating that you want to make a purchase, you are asked to make a funds transfer to the ‘seller’s’ bank account.
3. Once you do so, the ‘seller’ disappears and the product never arrives or turns out to be a fake. As payment was not made via the e-commerce platform, you are left with no way to recover your funds.

Online marketplace phishing scam

1. You come across an ad or sponsored post promoting heavily discounted items on an online platform like Carousell, Facebook Marketplace, Instagram or TikTok.
2. When you access the link provided in the post to make the purchase, you are taken to a separate website where you are asked to enter your banking credentials or card details. Alternatively, you may be taken to a messaging app (e.g. WhatsApp or Telegram). The scammer then asks you to access a link to place a

deposit or make payment (including for customs fees/delivery charges).

3. The website you are taken to is actually a spoofed one that is designed to appear legitimate. The scammer uses the site to steal your banking credentials or card details.

Parcel delivery phishing scam

1. A scammer, posing as a member of logistics company, sends you a message claiming that the delivery of your parcel has failed or that your parcel is held at customs.
2. You are asked to access a link – which takes you to a spoofed website – to supposedly confirm your mailing address and make a small payment so the company can release your parcel for delivery.
3. After entering your banking credentials or card details for payment, you later discover that unauthorised transactions have been made using your card.

HOW TO PROTECT YOURSELF FROM ONLINE SHOPPING SCAMS

Found a deal that seems too good to be true?	**Always** check the credibility of online sellers by reading reviews. Only make purchases from **reputable merchants**.
Received a link from a seller through a social messaging platform and asked to access it to share sensitive information or make payment?	• **Do not** make payment through links sent to you via social messaging platforms (e.g. WhatsApp or Telegram). • **Do not** provide your Access Code, PIN, card details or One-Time Password to anyone. **Never** key such information into unverified webpages. • **Always** read the notifications we send you carefully. **Notify** us immediately if you see a transaction you did not make.
Asked to place a deposit for a purchase?	**Avoid** placing deposits. If it is necessary to make payment in advance, use the platform's secured payment options. If possible, choose an arrangement that only releases your payment to the seller after you have received your item.
Prompted to authorise a payment using your digital token or SMS One-Time Password?	**Check all authorisation requests** before you approve them.

Asked to make payment for failed delivery or a parcel held at customs?	**Be cautious** when you are asked to pay an additional fee due to failed delivery or your parcel being held at customs.