

# Six ways you might be scammed if you sell items online, and how to protect yourself



Most of the online advice related to defending against the scams within online marketplaces is geared towards the buyer experience. However, recent trends indicate that sellers are also being increasingly targeted. Here are some of the most common scams, and how to avoid them:

## 1 *Direct message*

Scammers may try and message you pretending to be interested in your product, but instead try to persuade you to part with personal information such as banking account or credit card details.

### RECOMMENDATION

Never part with sensitive information through direct message, and report any users you suspect of fraudulent activity.

## 2 *Account compromise*

If a scammer obtains your login details through phishing or data theft activities, they may pretend to be you to manipulate listings, shipments, modify automated payout settings, and communicate with current and previous buyers.

### RECOMMENDATION

Protect your account with multi-factor authentication (MFA). This will provide an enhanced layer of security as an additional authentication factor will still be needed to successfully access the account.

## 3 *Payment account verification scam*

Sometimes scammers will pretend to be from the customer service team of an online selling platform, claiming that there is an issue with your account. They prompt you to click on a link to complete your account verification. However, the website is actually under the attacker's control and can be used to steal personal and financial information.

### RECOMMENDATION

Use caution and validate messages by contacting the support team separately using the information published on the marketplace website.

# Six ways you might be scammed if you sell items online, and how to protect yourself



## 4 Conducting transactions 'off-platform'

If a scammer obtains your login details through phishing or data theft activities, they may pretend to be you to manipulate listings, shipments, modify automated payout settings, and communicate with current and previous buyers.

### RECOMMENDATION

Protect your account with multi-factor authentication (MFA). This will provide an enhanced layer of security as an additional authentication factor will still be needed to successfully access the account.

## 5 Shipment detail changes

Scammers use information from previous listings, including photos, to target their attacks. Watch out for messages from people who claim to be someone who purchased an item you sold recently, asking you to change the shipping details - they are hoping to time it right so that you send the item to the scammer instead of your previously legitimate buyer.

### RECOMMENDATION

If a buyer asks you to change the shipping address, consider suggesting that they change their address using the online marketplace itself and contact support facilitate the change prior to shipping.

## 6 Using the 'friends and family' payment option

Social media sites like Reddit have become very popular for posting used items to sell. These transactions typically take place using money transfer platforms, such as Paypal, Zelle, or Venmo. Scammers may convince you to use the "friends and family" payment option. However, sending or receiving money with this option enabled removes many of the mechanisms in place to protect you from chargebacks and other fraudulent activity.

### RECOMMENDATION

While it is useful to use social media to advertise your items, always ensure that the actual transaction is carried out using a dedicated platform which offers protection for sellers and buyers. Reasonable buyers will be willing and able to conduct business following the standard platform transaction process.