



# Online crime

When it comes to online activity there are many places that fraudsters could try to target innocent internet users. Here are some points to note about online crime.

## AUCTION AND TRADING SITES

- Whilst shopping on auction sites such as eBay never move your transaction away from the security of the website to a bank transfer. eBay has buyer protection and works closely with PayPal who also have consumer protection. By moving your payment away from the site, you will risk losing any protection they would have provided you with.
- When shopping on local trading sites such as Gumtree never pay for anything before you've received it even if the person seems trustworthy.

## TICKETS, HOLIDAYS AND EVENTS

- The above rules also go for similar purchases like tickets and holidays. If the vendor encourages direct bank transfers then they are usually fraudulent.
- Ensure your booking is ABTA or ATOL protected for a holiday and STAR protected for tickets and events.
- Stay wise to 'too good to be true' offers and read the consumer advice that these websites offer - if there isn't any consumer advice on there, this is a red flag.

## ONLINE DATING

Online dating is a great, modern way to find love but unfortunately some people use this platform to manipulate innocent daters and try to take money or details. Criminals will quickly build relationships and ask to move the conversation away from the dating website so that there is no trace of the chat. In 2018, victims of romance scams lost an average of £11,145\* each and 4,555 reports of 'Fauxmance' were made to Action Fraud. On average, female victims lost around £39 million\*\*.

If someone seems very interested but has a lot of excuses as to why they can't actually meet in person, it could be cause for alarm. If they then start to ask for money to get around their excuses, for example car trouble or a family emergency, it's time to start to think whether this person may or may not be legitimate.

- Stay on the dating site and be hesitant to move the conversation onto another platform too soon.
- Don't be convinced by profile pictures, they can easily be fake.
- Do your own research on the person. See if you can find them on Facebook or any other social networking site to see if they look like a legitimate person. Can you confirm anything that they are telling you about themselves?
- Never send money to someone you have not met.
- Never receive or transfer money on someone else's behalf as they may be asking you to launder money.

## MONEY MULES

Money mules are recruited by criminals, usually by email or via social media direct messaging, offering a one-off or series of payments in exchange for providing their account details. Criminals are looking for money transfer agent (a money mule) to launder the funds obtained as a result of fraudulent or criminal activity. After being recruited by the fraudsters, money mules receive funds into their account which they then withdraw and move to wherever else the criminal would like it to go, often minus a commission payment.

Young people are being more frequently targeted for this kind of activity through Twitter and Instagram direct messages where they will use slang to describe what they want to happen. For example a 'square' means the bank account that they want to access and 'K drops' is the amount of money that they want to move i.e £10,000 is 10k drops. Victims of this kind of fraud could have their bank accounts closed down for committing fraud, and this could lead to them being refused for loans, mobile phone contracts and opening other accounts with other banks.

\* bbc.co.uk - women 'victims in 63% of romance scams' | \*\* refinery.co.uk - this is how much women lost in romance scams in 2019