Mail

- Fraudsters send letters claiming you have won the lottery or saying they are clairvoyants predicting good fortune.

How to avoid:

- If money is asked for, do not send. Typing errors will indicate it is not genuine.

Social media

- If an account is hacked the victim can be extorted for money or the account used for fraudulent activities.
- Fraudsters target job seekers with fake job opportunities on social media.

How to avoid:

- Use 2 step Authentication. Keep passwords secure and use different ones for each account.
- Check who is sending messages and contact the organisation directly if you have doubts about the authenticity.

Romance scams

- The scammer befriends the victim online and often uses fake pictures. They then ask for money for a pretend emergency.

How to avoid:

- Never send money to someone you have only met online.

Where to get help or advice:

Citizens Advice Consumer Service

To report a scam or for civil advice call **0808 223 1133**

Please quote this reference when calling the Citizens Advice Consumer Service:

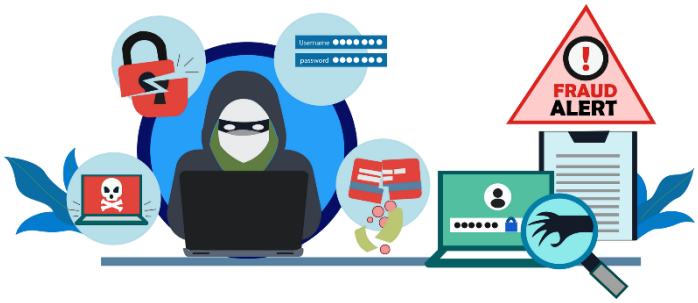
Ref

Action Fraud

To report fraud call **0300 123 2040**

For more information:

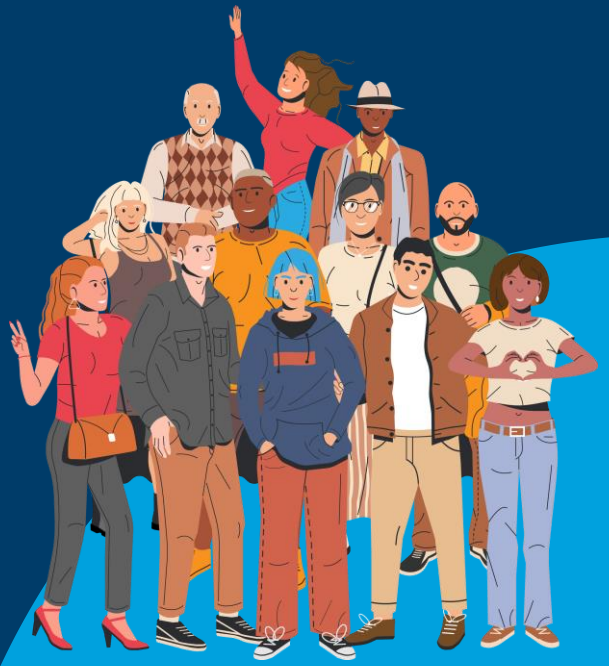
www.friendsagainstscams.org.uk
www.actionfraud.police.uk
www.takefive-stopfraud.org.uk



Version 2 - February 2024

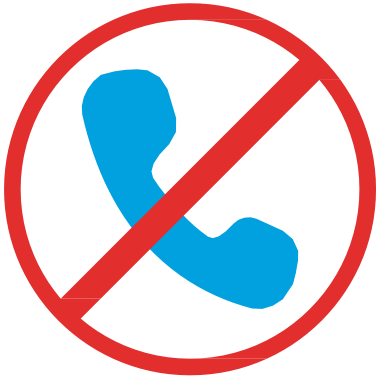
10 LATEST SCAMS TO WATCH OUT FOR

East Sussex Trading Standards



East Sussex County Council

eastsussex.gov.uk



Telephone scams & nuisance calls

- Callers can inform you there is an "urgent problem" such as your bank account has been compromised. The scammer may ask for your bank details or offer for a courier to come and collect the bank card.

How to avoid:

- Do not give PIN numbers or passwords or hand over your card.
- Always verify a caller's identity by contacting the company afterwards using an official number.
- To contact your bank, use the number on the back of your bank card.
- Many telephone providers have free call-barring services and call blocking devices are also available.

Investment/Cryptocurrency

- There are many fake sites advertising high returns on investments.

How to avoid:

- Check reviews, think before investing.

Friend or family in need

- Beware of messages or emails claiming to be from friends or family asking for help or money.

How to avoid:

- Verify their identity before sending money or personal information.
- Never click on a link in a text if the sender is unknown.
- Report unwanted texts to 7726.

Fake QR codes

- These can be pasted over genuine ones for example in a car park. You are directed to a fake site where money is lost.

How to avoid:

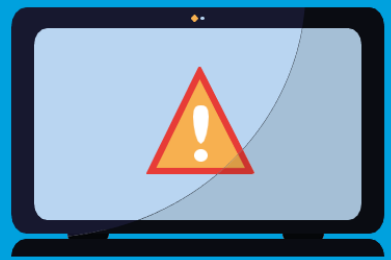
- Look for signs of another code underneath the one shown.
- Visit the website directly rather than scanning the QR code.

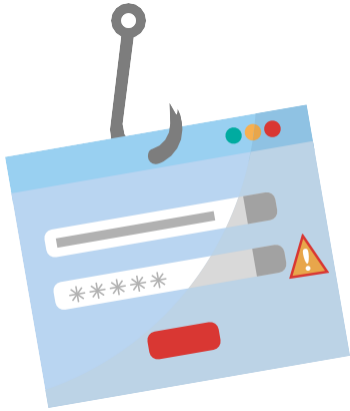
Parcel delivery

- Messages are sent saying you need to pay for the re-delivery of a parcel.

How to avoid:

- Don’t pay. It is the senders responsibility to pay for delivery fees.





Scams & phishing emails

- Attackers deceive people into revealing sensitive information. They pretend to be an organisation such as the DVLA or TV licensing.

How to avoid:

- Always check the address of the sender by hovering over or clicking the sender's name.
- Be wary of links to click which may take you to an external page where card details are requested.

Online marketplace

- If you're selling items online, fake buyers may contact you asking you to pay the couriers fee, promising a refund once delivered. The "buyer" will not reimburse the seller.

How to avoid:

- Request the buyer to collect the item themselves.
- Alternatively, deliver the item to the buyer if possible.