

Scam & Fraud Awareness



**SUSU Advice
Centre**



SCAM AND FRAUD AWARENESS

A scam is a scheme to con people out of money.

There are lots of different ways scammers do this, from tricking people into giving them personal details, to impersonating an official organisation like a bank to get people to directly hand over money.

Most victims don't report scams. But the impacts can be huge. People can:

- lose their life savings.
- Suffer emotional trauma or mental health problems.
- Lose their confidence.
- Suffer long-term health problems.
- Struggle with their academic work or to fund their place at University.

COMMON SCAMS

There are lots of different scams out there. By knowing what to look out for you can help protect yourself. Common scams include:

- ***Emails scams***

These messages contain links to genuine-looking websites that are designed to steal personal and financial information.

- ***Upfront payment/fee scams***

They usually ask for an upfront payment to unlock either a cash prize, a PPI claim amount or for initiating a service.

- ***Doorstep selling***

These all begin with the person getting an unrequested knock on their door. They are often for expensive home improvements which the victim did not want or was pressured into.



- ***Investment scams***

Often conducted either online or over the phone, these can result in people losing thousands of pounds for non-existent stocks, shares and other investments such as rare wine or art.

- ***Antivirus/computer***

People are cold called and told they have a problem with their computer which, for a fee, can be fixed. Alternatively, the victim might initiate the contact in response to an online advert or prompt claiming that their device has been infected with a virus.

- ***Currency scams***

People are asked to send money to someone with the promise of excellent conversion rates. A person will send a small amount initially and receive the money back and then send much more which gets stolen.

SCAMS AND THE COST-OF-LIVING CRISIS

The increased financial pressures many are facing has put more people into difficult situations. We've already seen scammers exploiting this.

SOME OF THE SCAMS TO LOOK OUT FOR INCLUDE:

- Scammers **pretending to be energy companies**, luring people with "too good to be true" deals to steal their money.
- Fake sales representatives selling **counterfeit shopping vouchers**.
- Fraudsters sending out **phishing emails pretending to offer an energy rebate or government support** to obtain people's personal information.

You can find out more about current scams on Action Fraud's website at

www.actionfraud.police.uk/news



WARNING SIGNS OF A SCAM

- It seems too good to be true.
- Someone you don't know contacts you unexpectedly.
- You're being urged to respond quickly.
- You've been asked to pay for something urgently or in an unusual way.
- You've been asked to give away personal information.

If you think someone might be trying to scam you, get advice. Contact The Advice Centre on 02380 59 2085 or email advice@susu.org.

HOW TO PROTECT YOURSELF FROM SCAMS

- Don't be rushed into making any quick decisions.
- Never give money or personal details, like passwords or bank details, to anyone you don't know, trust or have only met online.
- Before you buy anything do research the company or website you're using.
- Pay by debit or with credit card.
- Make sure your antivirus software is up to date and keep your online accounts secure.
- Be suspicious – scammers can be very smart.

SUSPECT A SCAM?

There are **3 important things** you can do if you suspect you're the target of a scam.



1. Protect yourself from further risks.

- Contact your bank straight away to let them know what's happened.
- If the scam is a pension transfer, contact the provider immediately, along with the Pensions Advisory Service
- Change any relevant log-in details and check for viruses if you were scammed on a computer.

2. Check if you can get your money back

- Again, make sure you tell your bank what happened straight away. Most banks should reimburse you if you've transferred money to someone because of a scam.
- If you've paid by Direct Debit, you should be able to get a full refund under the Direct Debit Guarantee
- If you've paid by card or PayPal, you may be able to get some money back through the 'chargeback scheme'.

3. Report the scam and get advice

- Call The Advice Centre on 02380 59 2085 or email advice@susu.org. We can help you understand the next steps and offer support to help you alert the University.
- Report the scam to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk. They're the national reporting centre for fraud and can also give you a crime reference number.

It's also important to talk.

By sharing your experiences with family and friends they can be prepared, and together we can put a stop to scams.

