We are Money@CampusLife

The award-winning Money@CampusLife team are here to provide information, advice and guidance on student money-related issues to the diverse student population at Swansea University and our prospective students. We aim to empower students to take control of their finances in order to limit the impact of financial issues to ensure students achieve their maximum potential whilst ensuring a positive student experience.

We advise on student funding, financial hardship, budgeting and provide specific assistance to students who have additional considerations. The list of considerations can include being a student parent, a care leaver, a carer, having a learning difficulty or being estranged from your family, plus more.

How Can We Help - EU Students

- Advice on funding from Student Finance
- Face to face advisory sessions
- Help with financial hardship
- Budgeting workshops

How Can We Help - International Students

- Face to face advisory sessions
- Help with financial hardship
- Budgeting workshops

Information provided in partnership with

INTERNATIONAL @CAMPUSLIFE

1920-2020 Swansea University Prifysgol Abertawe

Follow CampuslifeSU on Facebook, Twitter and Instagram

Contact Money@CampusLife

Email: money.campuslife@swansea.ac.uk

Telephone: 01792 606699

If you would like to speak with an advisor face-to-face, we operate drop-in sessions at the following times and locations:

Campus	Monday	Tuesday	Thursday
Singleton: Keir Hardie Building	09:30 - 12:30	13:00 - 16:00	09:30 - 12:30
Bay: Tower Information Centre	13:00 - 16:00	09:30 - 12:30	13:00 - 16:00

Please note, calls to Student Finance can only be made between 10am and 4pm

SCAMS TO SPOT AND STOP

Swansea University
Prifysgol Abertawe

Brought to you by
Money@CampusLife
www.swansea.ac.uk/money-campuslife

Advance-fee fraud

You get an email from ex-ministers or the royal family, often from a foreign country. They will ask for your bank details to deposit a large sum of money so they can get out of the country and offer to pay you a fee. The scammers will use the details you send to clear-out your bank account. Similar schemes exist with wills and claiming an inheritance from a long-lost relative.

SPOT
Check the email as the name the message is from and the email will not match. Bad spelling and grammar can also be a give-away.

STOP
Ignore the email and never send payment details or personal information.

Authorised push payment fraud

Fraudsters intercept or hack your e-mail account. They then pose as a legitimate business asking for payment. This often occurs when you're in the process of buying a house, having building work done on your home or booking a holiday.

SPOT
Difficult as it normally occurs at a time when you're expecting to be asked for payment. Don't assume all emails are genuine.

STOP
Check the company you expect to be paying did send you the email and the bank details match.

Computer software fraud

Scammers pretending to be from Apple or Microsoft contact you by phone or email and say they need your payment details to fix, update or validate your software.

SPOT
It's very unlikely computer companies would make an unrequested phone call about these kind of issues.

STOP
If in doubt, contact your computer or software supplier directly and never give out your payment details.

Vishing

A phone call where the scammers pretend to be from your bank, building society or even a government agency. The scammers will attempt to get you to reveal your personal details.

SPOT
The caller will be desperately trying to get you to reveal your information, which no legitimate caller would ask you to do.

STOP
Just hang-up the phone. If you want to check your account, call your bank or building society on the number on your debit or credit card.

Phishing

An email scam where you appear to get a message from a legitimate source, such as your bank, asking you to click a link and log into your account. They may say your account has been locked or there is a large transfer of money. In reality, the link in the email goes to a fake website, which collects your information.

SPOT
Scammers will use a general greeting such as Dear Sir, Dear Madam or Dear Customer. Legitimate emails will use your name.
A real email will come from a recognisable address (e.g. noreply@bank.com). Scammers email addresses will be filled in with random letters or numbers (e.g. noreply@1234.bank.com), or have deliberate spelling mistakes.

STOP
Never click the links in a suspicious email. If you think there might be a legitimate problem with an account, go to the website directly and log in.

Smishing

Scammers will contact you by SMS claiming to be from your bank saying you need to update your personal details, or there is some kind of issue. The text might contain a link or a phone number to call. Both are fake and will attempt to get you to reveal your details.

SPOT
The phone number in the text is not the same as the one on your credit or debit card.

STOP
If in doubt, call the number on your card and find out if they have tried to contact you.
Don't click any links in text messages. Always go directly to the website and login as normal.

Pharming

Scammers target the website you are visiting.
You type in the correct website address, but you then get directed to a fake version, where you inadvertently put in your login details and secure information.

SPOT
Look at the website address. It will show up as a selection of numbers, or perhaps something similar to the real name, but with letters switched around or a different spelling.

STOP
Be observant when you're logging into websites.
Keep your operating system and anti-virus software up-to-date.

Ticket scams

You buy your ticket for an event but the person, or website, you're buying from either doesn't send the tickets, or sends you fakes.

SPOT
If it's a website you've never heard of, or doesn't have proper contact details, or only lists a mobile phone number or PO Box, then you should avoid it.

STOP
Avoid buying tickets off social media or online auction sites where it might be difficult to trace the seller and get a refund.
Check the website you're buying from is a member of the **Society of Ticket Agents and Retailers** (STAR) www.star.org.uk

There are so many other scams that fraudsters are operating such as Dating fraud, Online Auction scams & Recruitment fraud to name but a few. Check out our webpages for more information:
www.swansea.ac.uk/money-campuslife/scams

Safe account scams

Scammers will contact you claiming to be your bank. They will say your account has been compromised and will encourage you to transfer all of your money from your bank to a "safe account".

SPOT
Banks will NEVER ask you to transfer money into a "safe account".

STOP
If you've been contacted on the phone, just hang up, and if you're worried about your account security, call your bank directly.