Derbyshire Safeguarding Adults Board

Information Leaflet: Scams Targeting Students

Many scams are levied specifically at students. Be aware of any unsolicited contact that asks you for sensitive information or money. Scammers will often claim to be from legitimate organisations and authorities like the university, banks or the police. If you receive such correspondence and are unsure if it's legitimate, find contact details for the organisation in question and ask them directly. **NEVER** provide money or sensitive information to anyone who contacts you without prompting.

If you fall victim to a scam report the incident to Action Fraud on 0300 123 2040. You can obtain IT support from the University Email: itservicecentre@derby.ac.uk
IT Helpline (24/7): 01332 591234

Online (self-service guidance):
https://itservicecentre.derby.ac.uk/hc/en-us

Typical scams are

- **Home Office/Embassy fines** Students are contacted by phone or email by scammers claiming to be from the Home Office. They are often able to spoof real email addresses or phone numbers so appear legitimate. They will claim legitimacy by demonstrating that they know information about the student such as their address and passport number. They will claim that there is a problem such as a visa issue and demand that the student pays a fine.
- **Fraud allegations/police incidents** Students may be contacted by scammers claiming to be from the police. They will accuse students of perpetrating some kind of crime, often money laundering, or will claim some other serious incident has taken place. They will demand the student hands over bank account details and copies of identification to prove their innocence. This can result in the loss of tens of thousands of pounds.
- **Currency exchange scam** Scammers may advertise a service providing better currency exchange rates and will ask that money is transferred to them. Tens of thousands of pounds has been lost in some instances.

- **Spear-phishing scams** Spear phishing scams involve fraudulent emails being tailored to whoever they target. Cybercriminals may find information on a student (such as by stealing their username and password for any accounts they might have). These can often be very convincing. For example, a student may receive an email appearing to be from the University asking for payment of fees around the same time that the student receives correspondence about enrolment.
- **In-person scams** Students may be approached by people claiming to be representatives of the University such as professors or administrative staff. They may ask you to transfer money for tuition fees, accommodation fees or event tickets. No university representative will ever approach you in person asking you to transfer money, If you are approached in this way, do not provide any money or personal details, Report it immediately to Campus Security.
- **Private video chat scams** 'romance scammers' often engage in a form of 'sextortion' which involves scammers pretending to be romantically interested individuals who invite the target to engage in private video conversations. The scammers will record these and post the compromising images online. They will then extort the target for large sums of money in order to have the footage taken down. This scam is commonly levied at individuals from East Asia.

Your Bank should help you if you have been tricked by Social Engineering. So, what is Social Engineering?

Social engineering is about manipulating individuals so that they give up confidential information. The types of information being sought by scammers varies, but when people are targeted they are usually tricked into giving up their passwords, personal data or bank information and or access to their computer via the installation of malicious software.

Criminals use social engineering tactics because it is usually easier for them to misuse trust than it is to discover ways to hack software e.g. it is much easier to fool someone into giving out their password than it is to try hacking their password (unless the password is not strong).

The following guidance aims to raise awareness of social engineering by providing examples and types of methods used by scammers and tips on how to defend against them.

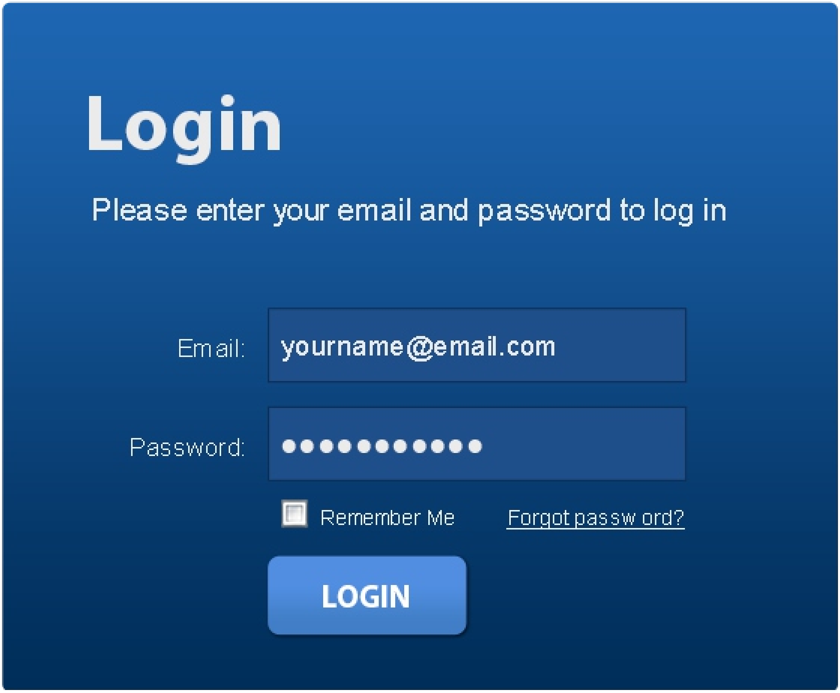
Examples of Social Engineering

- **Contact from a friend** Scammers gain access to an email account and send messages to their contacts e.g. a friend's email account may be compromised so you may receive scam messages from them. The scammers may get you to click a link or download an attachment in order to take control of your account, inject malicious software or steal data.

- **Contact from a trusted source** A form of **phishing** involves scammers pretending to be trusted sources like banks, tech companies or your place of work. They will try and steal your login credentials or other sensitive data or inject malicious software.
  It is common for scammers to mimic University staff.

- **Answering your unasked questions** These attempts rely on **trusted authority** and involve the scammer posing as a well-known organisation. They might claim to be responding to your request to fix a problem e.g. they may claim to be from Microsoft and want to take control of your machine to remove a virus.

- **Creating distrust** Perpetrators of this may include people you know personally. They will gain access to other's accounts (like email or social media) and use them to spread lies and incriminating information through messages, doctored images etc. Their goal is either extortion or damage to reputation.
- **Trust and Authority** Scammers will appear to come from legitimate sources or people you know.
- **Urgency** They will present scenarios that need you to act as soon as possible to make you panic and not stop to think.
- **Generosity** You may be exploited by requests for charitable donations in response to a distressing story.
- **Verification** Fake log-in screens or stories which involve you needing to verify yourself are used to harvest log in credentials and other data.
- **Temptation** Scammers might tell you you've won a valuable prize, tempting you to take the risk and hand over data or control to claim it.



Login

Please enter your email and password to log in

Email: yourname@email.com

Password: ●●●●●●●●●●●●

Name	Method	Defence
Phishing	Typically involves the sending of emails to multiple recipients usually to get victims to click links and reply with information	Don't reply or click on links you are unsure of. Check company emails on official websites, protect your devices with anti-virus software and apply strong spam filters in your email settings.
Spear-phishing	Targeted at you specifically and will use information about you to sound more convincing. An example of this is where scammers pretend to be management staff and ask you for data or money	If they claim to be a person you know, contact that person by other means to verify the request.
Whaling	These are spear-phishing attempts aimed at senior individuals in an institution. Scammers will put more effort into these as there is a greater potential pay-out.	If you are a senior (higher grade) University member, be wary that you may be subject to this.
Shared Document phishing	These are fake messages claiming that a document has been shared with you.	Do not click suspicious links or download files you are not expecting to receive.
Vishing	Vishing is short for 'voice-phishing'. It involves scammers calling their targeted individuals on the phone to convince them to part with confidential information.	Be suspicious of unknown numbers and unsolicited calls. Do not agree to hand over sensitive data or install software on your device on the advice of people who call you. If they claim to be from a legitimate source, find contact information from an official website and call them back.
SMShing/Smishing	SMShing or smishing both refer to phishing attempts sent via text. The same principles for other phishing attacks apply.	Google numbers to see if they are official or if someone has posted on forums about them being scams. Don't click suspicious links or reply to texts you suspect are SMShing attempts
Social Media Phishing	Scammers utilise social media. They may create fake profiles that look real, exploit existing profiles and use your publicly available information to trick you.	Be wary of unsolicited messages. Do not click links that look suspicious or come from strangers.

Guidance on Phishing Emails

A phishing email is a hoax designed to get hold of your personal details or money. These emails come in many shapes and sizes, but a lot of the time they'll be designed to look 'legitimate' - for example, they may claim to be sent from:

- DHL/UPS/Royal Mail
- your bank
- an area of the University, e.g. the Library
- a high-profile member of the University.

Once you've opened an email, it will normally ask you to take action – to click on a link or open an attachment. This is usually what provides the scammers with the personal information they're seeking.

How to avoid getting caught out

1. **Read emails carefully before acting.** Phishing emails may include a generic greeting (e.g. 'Dear sir'), an overly-friendly tone, grammatical errors or an urgent request. Take a moment to consider the contents of the email before doing what it asks.
2. **Exercise caution when opening links and attachments**. Hover over any links to make sure they're legitimate.
3. **Never reply to an email asking for your passwords, PINs or other account details.**
   The University will never email or phone you to ask for your account details. Likewise, any email asking for bank details will be fraudulent, without exception.
4. **Verify the source.** Check the sender's email address when you receive an email and when you reply. Malicious scammers might be able to spoof the 'From' address in an email to make it look like it come from someone you know, but when you reply the address may change. If in doubt, type in the email address manually.
5. **Report it.** Report anything suspicious to the IT Helpline, including attachments or links you've clicked on.
6. **Turn on two-step authentication.** This will ensure that only you can access your account.

More information about scams and financial abuse can be found on the DSAB website www.DerbyshireSAB.org.uk

Follow us on Twitter @DerbyshireSAB

Like us on Facebook @DerbyshireSAB