Student Guide to Fraud
WU and LSE

WesternUnion WU Business Solutions

LSE THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

How to protect yourself from payment scams

Students have been targeted in recent years by criminals offering assistance to transfer or exchange money internationally, usually claiming they can provide a no-cost money transfer service or provide discounts, gifts or commissions. The claims are wide and varied and can include pre-loaded debit cards, gift cards, iTunes cards, concessions, memberships or even discounts and reductions of your tuition fees.

They encourage you to send money to an illegitimate bank account, collect the numbers on the back of the victim's cards and reach out to you in a variety of disguises such as by phone, post, email and via the internet including many social platforms. The fraudster could impersonate anyone—an official pretending to be from your university or college, or a legitimate organisation (such as the UK Home Office, an education agent, or event UKCISA), an agent working with your college, or even a senior student from the same university.

In some cases, the fraudsters do not pass payments on to the university, they may deduct charges or devalue the payment before passing it, if at all. You may be offered to accept a payment and then be asked to pass that on to somebody else, in fact, the person contacting you may be part of a much wider serious crime organisation involved with money laundering. This is a very serious offence that can lead to severe consequences for you as well as the institution.

In this guide, we will share some of the common types of frauds and scams targeted at students and some dos and don'ts that will help you protect yourself from fraud, phishing, and card payment scams.

Common Types of Scams

There are three primary forms of card payment fraud, which you should be aware of:

Phishing Scam

A term used to describe sending communications (emails, texts, instant messages) with a link that takes you to a fake website designed to steal personal and identifier information. The primary delivery medium is email. It's relatively easy to spot a phishing scam as it will often contain strange-looking senders disguised to look legitimate on the surface. You should investigate beyond just looking at the title or body of an email and ensure the email address and domain are what you expect.

Card Payment Scams

This involves the unauthorised use of your credit or debit card data (card number, billing address, security code and expiry date) to purchase products and services in a non-face-to-face setting, such as via e-commerce websites or over the telephone. Such attacks will commonly use compromised card details, perhaps obtained through a phishing scam.

Impersonation Scams

These are often referred to as authorised push payment or bank transfer scams. This happens when the victim is tricked into making bank transfers to an account posing as a legitimate payee. Another level of impersonation fraud occurs when victim details are used by fraudsters to apply for financed goods, services, or financial products. Such details can be obtained from phishing attacks or social engineering.

Case Examples. Tuition Fee Scams

Scenario 1 – "Let me help you pay your tuition Fees"

You can be approached by a fraudster and/or another student either in person or via social media. They will offer to provide help to pay forthcoming tuition fees. The fraudster will either utilise your email account or their email account having collected all the payment log in details from you.

The fraudster will ask that you pay up 10% of the fees upfront as an administrative fee and then once received the fraudster will initiate the tuition fee payment using a stolen bank, debit/credit details. However, the fraudster is well aware the payment is unlikely to be successful and will disappear before the payment is rejected.

Scenario 2 – "I have paid your fees in full"

The fraudster will appear to have made a successful payment by sending you a copy of the invoice showing the full payment made. In reality, all they have done is made a successful £1 payment using a stolen debit/credit card and then altered the invoice to make it seem like they have made a full tuition fee payment. They will then ask you for an administrative fee of 10% and then they will disappear with the money.

Consequences

- Losing money on tuition fees can have serious consequences on your studies and admission.
- Money Laundering is a serious criminal offence, and it is treated as such by Law Enforcement. Indirectly, you get involved in that process and there could be an enquiry.
- Severe impact on your reputation and that of the institution.

Case Examples. Refund Scams

Case 1 – “Can I use your bank account, please?”

You can be approached by a fraudster and/or another student either in person or via social media. They will ask you to process a payment from a bank account/credit or debit card for their tuition fees and then once the payment has been successful, they will want you to get the educational establishment to refund the money. The fraudsters will likely coach you about how to do it or may even do it themselves using your email account. Once the refund has been completed the fraudsters may give you some monies or incentives for their trouble.

Consequences

Whatever scenario the student gets involved with there are some serious consequences attached to both.

- Refund Scams are clear examples of Money Laundering
- Reputational Damage
- Financial and Psychological Impact

Dos and Don'ts
to Protect Yourself from Fraudsters

1

Learn about Scams and Security

Learn more about Tuition Fee and Refunds Scam, Money Laundering, Secure websites, Phishing, and Card Payment Scams.

3

Use telephone preference services and two-factor authentication

Request for a number to call back. Usually, a fraudster will never give out their details. Do not share anything over a phone call.

2

Reach out to the University Fees, Income, and Credit Control Division

When in doubt, always contact the University finance division. Never be pressured by any deadline, threats of retaliation or threats to revoke your student visa if payment is not made.

4

Save every proof of conversation, interaction, or transfer

Save any conversation, email interactions, chat with your agent, senior student, a person from the University – anyone can be a fraudster.

Dos and Don'ts
to Protect Yourself from Fraudsters

1

Never Share Bank Details with anyone.

Do not share your bank account number, credit or debit card details, PIN with anyone. Your bank will never ask for full details over the phone, like the PIN.

2

Never Share Personal Information on the phone, email, post, or social media

Avoid sharing any details about your college/ institution, University login credentials with anyone, especially on social media with strangers, any third party, agent.

3

Resist the urge to act immediately and never transfer funds to someone you don't know.

Look for words like warning, urgent, important, deportation, threats, deadline. Fraudsters often employ this tactic to scare their victims and make them transfer funds immediately. Stay calm, be aware and sceptical of such scams and act accordingly.

4

Avoid Too Good to Be True Deals.

Be cautious of unsolicited offers of easy money or discounts. If it sounds too good to be true, it probably is. There are no discounts on tuition fees offered via our social media channels.

5

Do not confirm any information.

Do not share or confirm any personal information like name, pin code, address, phone number, date of birth. Fraudsters often have incomplete information about you and reach out to fill in the gaps to conduct a scam. Be always suspicious and alert.

6

Report anything suspicious as soon as you can.

Report the incident or if you feel someone else can be a victim of fraud. Reach out to the University' Fees, Income and Credit Control team, your bank, and even the police.

Further Information

Western Union Business Solutions

GPStudents@westernunion.com

+44 1733 871871

LSE

Fees@lse.ac.uk

0207 107 5555