

LESSON 9: Activity 2

Teacher resource sheet: Common scams

A scam is designed to con you out of your money or your personal details such as your bank account details, PIN numbers or internet banking login details. It can happen over the phone; by email, text or letter; on a false copy of a real website; through social networking sites; at your front door or on the street.

The scams that are out there and how to guard against them

If it sounds too good to be true, it usually is! There is no such thing as free money, but scammers will try to convince you that there is.

- Think twice before responding to a friend's message requesting money. It could be a scam that involves someone hacking into your friend's email or social media account. Never click on links within emails that you feel a friend or acquaintance would not ordinarily send or that you are unfamiliar with. Some scammers tell you that you have won an incredible prize – but you know you never entered a competition or lottery. Stop, think and be sceptical - this is a **lottery** or **prize scam**.
- Some scammers telephone you and tell you there is a problem with your PC. They then say they can fix the problem for you if you give them your credit card details or remote access to your PC. They then use these personal details to steal your money. This is a **phishing scam**.
- Use your bank and credit cards safely and securely. Scammers can copy your card in just a few seconds – this type of scam is called "**skimming**". Never let your cards out of your sight and never give anyone your PIN number.
- Take care when buying or selling goods online or through a newspaper. Never accept large sums of cash, cheques, or money transfers as payment. If you are selling something valuable like a car, ask the buyer to get you a draft from their bank or to transfer the money to your bank account.
If you are selling an item for sale in the local newspaper or on a website, for example your car, never accept a cheque or draft for an amount over the asking price.
- Never respond to a scam as this might make you a target for other scams. Scammers sell lists of people who have responded to scams on to other scammers. Scams can be very convincing – scammers can email you claiming to work for a company you deal with or using the logo of the company.

What do you do if you have been caught out by a scam?

If you think you have been the victim of a scam or fraud and you have given someone your bank account or credit card information, inform your bank or credit card company immediately so they can tell you what action they need to take. You should also contact:

- Garda Bureau of Fraud Investigations on (01) 6663777 or contact your local Garda station immediately
- Competition and Consumer Protection Commission (www.consumerhelp.ie/contact-us)
- Your friends and family so they won't get caught out
If you were scammed somewhere else in Europe tell the European Consumer Centre Ireland