

PILLAR 5



Money Smarts Challenge
Risk & Protection



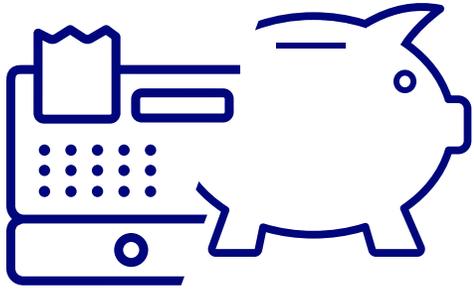
Welcome

Financial Wellbeing is about what you do with your pot of money, not the size of it. It's about making sure you can cover day-to-day expenses, plan for the future and manage the unexpected. This presentation covers risk and protection, examining the issue of risk and showing you how to develop strategies to protect against it.

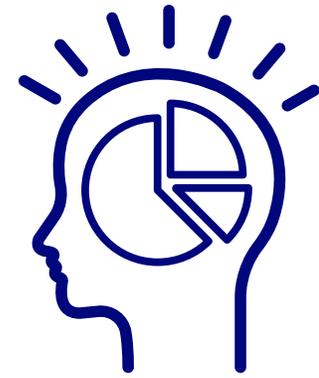


Risk & Protection is the fifth of six pillars of Financial Wellbeing. The following information shows your students how risk is everywhere and how they can navigate major financial challenges throughout their lives. The content is designed to give you a flavour of what you can expect your students to be quizzed on as part of the Money Smarts Challenge.

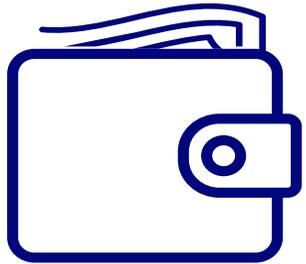




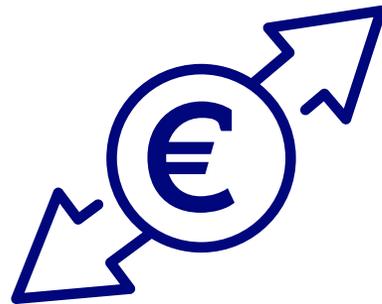
Spending and Saving



Financial Decision Making



Earnings and Income



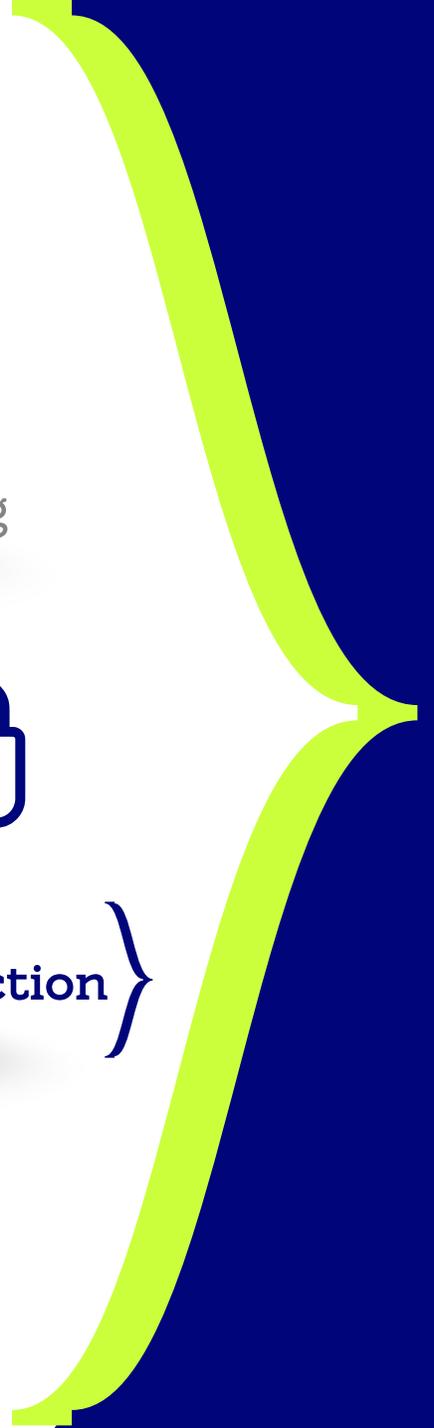
Credit and Debt



Investing

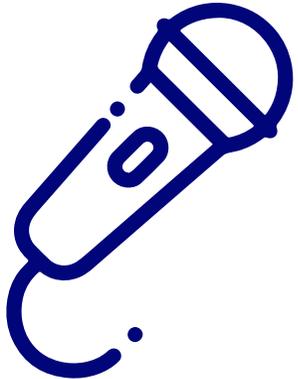


Risk and Protection



RISK AND PROTECTION

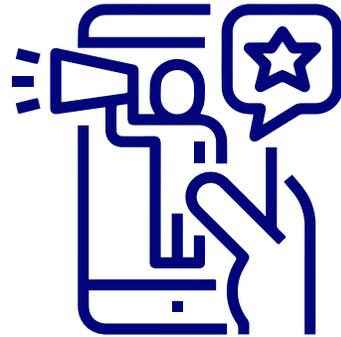
People face risks every day.
What risks might impact the following careers?



Singer



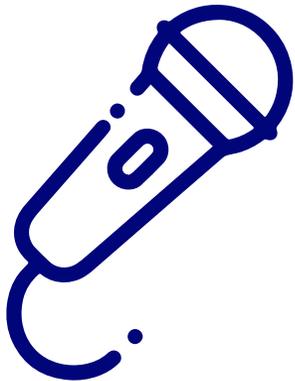
Footballer



Influencer

RISK AND PROTECTION

People face risks every day.
What risks might impact the following careers?



Singer

Losing voice
Insurance on voice



Footballer

Sports injury
Contract with club to cover injury



Influencer

Reduced followers
Strategy for posting comments

FRAUD

Fraud is a risk that is present everyday. It can happen to anyone at any time. In fact, you may be familiar with a few of these fraudulent practices:

VISHING is a phone scam where fraudsters target people by phone. They claim to be a bank or a service provider and trick you into giving personal, financial and security info over the phone

SMISHING is a text message scam. Fraudsters claim to be from important organisations. The text will ask you to click on a link to a website. The website is fake and the phone number leads to the fraudster. They will seek personal, financial or security info from you.

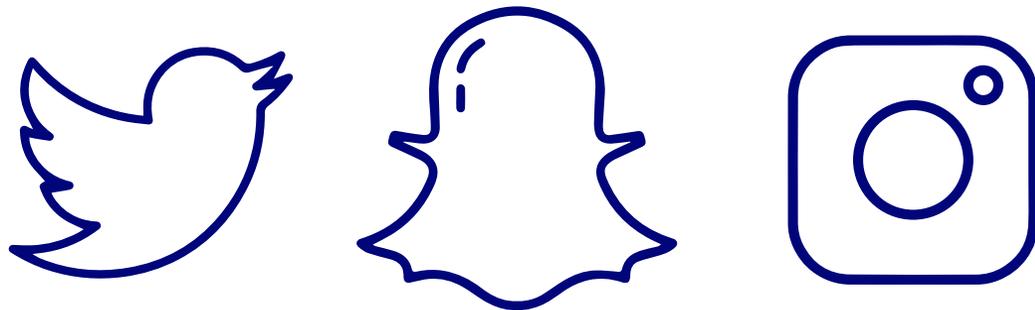
PHISHING is an email scam where the fraudster sends fake emails that look like they are from a reputable company. They urge you to click on a link and enter your personal and financial details.

TWISHING uses Twitter to send fake comments like 'Help me I'm in trouble', miracle products and work from home offers - all which are scams.

SOCIAL MEDIA

Social Media is a fantastic way to communicate with your friends and family. However, social media is a haven for scams that are designed to take advantage of users.

Social Engineering is where fraudsters use social media to find out information about you and then use this in a phishing or vishing scam.



Be alert when banking online

Banking online with Bank of Ireland and other reputable banks is very secure. However, you should following these top tips to keep it that way.

- Using public WiFi carries risk and may not be secure
- Always look for https:// and the padlock symbol in the address bar
- Have active antivirus/antispysware on your device
- Regularly clear your browser's cache
- Never share your bank details with anyone, even the bank
- Keep PINs and passwords private from everyone
- Create strong passwords using a mix of letters, numbers and symbols
- Remember that card issuers and banks never ask for PIN or security details
- Always cover your PIN at an ATM
- Always keep your card in sight if you are paying for something
- Never let anyone else use your bank account
- Never accept payment for use of your bank accounts



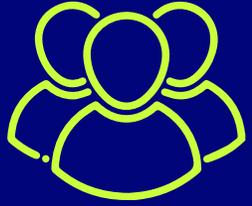
Only a donkey becomes a money mule

Money mules are people recruited by fraudsters to help them transfer stolen money from bank accounts.

Fraudsters recruit money mules by targeting students. They offer them money in return for lodging cash or cheques into a bank account, often using the excuse that they cannot open an account themselves.

Never ever let anyone use your bank account and never accept payment for use of your bank account

- ✓ **Be Informed**
- ✓ **Be Alert**
- ✓ **Be Secure**



GROUP WORK

In small groups, ask your students to consider the following scenario before presenting their answer back to the class.

- Discuss how you would deal with a difficult or suspicious situation, including a potential scam if you were faced with it.



SAMPLE QUESTIONS

1. What type of fraud is Phishing?

- a) Text messages
- b) Emails
- c) Twitter DMs

2. Vishing is a phone scam where fraudsters target people by phone. But what is it called when scammers try to contact you by text message?

3. What are money mules?



DISCLAIMER

This document has been prepared by Bank of Ireland for informational purposes only. Not to be reproduced, in whole or in part, without prior permission. Any information contained herein is believed by the Bank to be accurate and true but the Bank expresses no representation or warranty of such accuracy and accepts no responsibility whatsoever for any loss or damage caused by any act or omission taken as a result of the information contained in this document. An individual should obtain independent legal advice before making any decision. Bank of Ireland is not responsible for the information on any third party webpages in this document.

Bank of Ireland is regulated by the Central Bank of Ireland.

