CATEGORY TWO:
Avoiding Online Scams (Ages 9-11)

Learning objectives

To recognise suspicious emails which may be phishing for information or scams.

To understand why it is important not to share personal information such as usernames or passwords.

To understand the consequences of sharing personal information.

Links to the Financial Education Planning Framework

I know there are financial risks associated with spending money online e.g scams and phishing (9-11).

I can describe some ways to keep my money and personal information safe when using the internet e.g. protecting passwords and PINs (9-11).

I understand some consequences of financial scams and how they might make me feel (9-11).

CHALLENGE ENTRY OPTION

Come up with an idea that helps people make wise choices about how to protect their money when using the internet.

QUALITY MARK

YOUNG MONEY CHALLENGE

Q: How can we help others to avoid getting scammed online?

MATERIALS

PowerPoint slide for use in the scam role play activity.

INTRODUCTION

Going online is a great way to spend time socialising with friends, play games, watch something on YouTube or do other stuff. All of these activities offer high levels of enjoyment as they offer a way to get involved with others, so staying safe online is something that will help you to have an enjoyable time. Today we will explore how to identify scams to help us stay safe.

Watch this video to introduce online scams: **https://www.youtube.com/watch?v=ySHvOKOmnAk**

ACTIVITY 1

WHAT DO WE KNOW ABOUT SCAMS?

Ask the class what they know about online scams

Explain that a scam is when someone tricks you by getting you to give them something that belongs to you. Some scammers want to trick you into handing over information such as usernames, passwords, email addresses and bank account details. It is usually done as an email but can also be done on the phone. It could also be that you give them money for something that you do not receive or the item you receive is a disappointment and not what was expected.

ACTIVITY 2

SPOTTING A SCAM

The scene: A group of children were allowed to go on the computers at school and were told that, if they finished their work early, they could spend a bit of time playing an online maths game. While online playing the game, a pop-up ad has appeared for a competition to win £1,000. All they have to do is click on the link and enter information about themselves, including their name, address, and date of birth. It also asks them to enter some bank account details, including a debit card number, so the prize can be paid to the winner. One of the children gets excited about the possibility of winning £1,000 and starts entering their information, but their friend spots what they doing over their shoulder and warns them that it's probably a scam.

STEP 1

Get the children to work in small groups or pairs and see if they can identify the "red flags" in the advert that suggest it is a scam. Get them to consider both **what** is being asked for and **how** it is being asked (i.e. the language, spelling etc).

STEP 2

Ask the children to discuss in their groups what they think this type of scam is trying to achieve. They should think about **what** information is being asked for and **how** that information could be used by a scammer.

STEP 3

Finally, ask each group to come up with a list of ways we can protect **ourselves** and **others** from online scams.

At the end of the session, you may wish to explain that schools have cyber security protection that works to block this kind of scam entering the school's IT network so this incident would not likely happen in school. Explain that this exercise was done as a role play so that children could experience all that is involved in understanding the consequences of phishing and scams and how to keep safe.