TOPIC 8

How do we keep our money safe?

This topic helps you to:

- find out how to keep money safe;
- understand what fraud is and how to avoid it;
- understand how to buy safely online.

How do we keep our money safe?

Lots of the things we have learned about help us to keep our money safe.

- Storing money in an account.
- Being careful while using an ATM.
- Checking bank statements regularly.
- Using chip and PIN when buying.

Let's look at some of the issues around keeping our money safe.

What is fraud?

You may have heard of 'scams' or 'cons'. These are **FRAUD** – being dishonest in order to steal money.

Identity fraud (or theft)

Identity fraud is where someone gets hold of another person's bank details, and uses them to spend money in the victim's name.

Aisha realises that her debit card is missing. She checks her bank statement and sees debits she doesn't recognise.

A fraudster is using her card details.

A fraudster might also apply for a loan or credit card in the victim's name. They spend the borrowed money using the victim's identity, and the victim is sent the bill.

How do we avoid fraud?

Layers of security help to protect us against fraud.

When buying online, we might enter letters from a password to prove we are the cardholder. Online stores have security that 'encrypts' the data we send, so that fraudsters can't read it.

Account security

If we use online banking to check account statements or make payments, security makes it hard for fraudsters to access the account.

Carl logs in to his account online. He must enter the following:

Unique customer number: _____

1st and 3rd digits of PIN: _ _

2nd and 4th letters of password: _ _

Keep your details secret

A PIN and a password must be secret. Pick things that you can memorise – you should not write them down where someone else could find them.

You give out card details when buying online, and type digits from your PIN when logging in to your account.

But be careful. If someone asks for your details, on the phone or online, be sure you know who is asking.

Carl receives the following email.

YOUR BANK PLC

Dear valued customer,

We are investigating our online security and believe your account may have been hacked. Please do not be alarmed – reply to this email with your customer number, password and PIN so we can verify your details.

This is a fraudster trying to get the details needed to log in to Carl's account. A bank will **never** ask for your entire PIN.

This method of posing as someone that you trust in order to make you give out your details is called **PHISHING**.

The fraudster is 'fishing' for your details.

Carl does not reply to the email. He calls his bank branch.

CARL

Did you send me an email asking for my PIN?

BANK WORKER

No, we would not do that. Please don't give out your details

Report suspicions straight away

- If you suspect that someone is using your details to commit fraud, **report** it to your bank straight away.
- If your card goes missing, ring your card provider immediately and **cancel** it. This stops anyone from using your card.

How do we buy safely online?

We looked at selling items online in Topic 5b. If you *buy* items online, you must be cautious.

- Is the website trusted and well-known?
- If you bid in an online auction, does the seller have good feedback?

Plus, always ask yourself: **is this offer too good to be true?** Some people try to trick buyers.

Matt sees a listing on an auction website

BRAND NEW SuperTab 6.0
BOX – GREAT CONDITION

Matt has never seen this tablet sold for less than £200. He bids £50 and buys the item

But he receives an empty box, as described by the seller

ONLINE ACTIVITY

Are the offers in ACTIVITY 8 too good to be true?

FURTHER . . .

Complete the online activities and end-of-topic quiz to expand your learning for Topic 8.