

Lesson Plan

Online Banking

Resources needed

Copy of BankSafe on all computers

Learning Objectives

To understand how an online banking system works

To experience the security features of an online bank

To access bank accounts online

To transfer money between accounts, pay bills online, use standing orders and direct debits.

To gain an overall appreciation of the features of an online bank

Overview

In this lesson the students are going to use a fully functional, simulated online banking system. They will use functional security systems to access the bank accounts, realising that if they cannot follow the instructions to get through security, they will never have access to the bank. Once through security, they will be taken through the features of an online bank. This includes the transfer of money between accounts, paying bills online, using standing orders and direct debits, as well as changing passwords and other 'housekeeping' functions.

At the end of the practical exercise, students should consider the effects of online banking on society and also the advantages and disadvantages of online banking.

Homework

The students should make a list of the possible Advantages and Disadvantages to the individual of online banking.

Notes for Teachers

Advantages of online banking

On-line banking gives the user many benefits. Several accounts can be set up and used online, such as current, deposit and credit card accounts. They can be accessed 24 hours a day, 7 days a week and from anywhere in the world (providing the user has secure internet access). Balances can be checked online, money moved between accounts, bills paid, direct debits and standing orders set up or amended. The user doesn't have to leave the house or stand in queues or post off cheques, saving time and money. Online banking is fast and efficient.

Disadvantages of online banking

Security could be the biggest problem with online banking. The user **MUST** protect their personal information such as passwords, ID and PIN numbers. They should never be disclosed to anyone else. Many fraudsters send emails that look genuine asking for personal details (this is called 'phishing'). The bank will **NEVER** ask for these details by email. These 'phishing' emails should be ignored or the user could contact their bank. Passwords, PIN numbers etc. should **NEVER** be emailed to anyone as this may not be secure. The user should have security software (such as ESET NOD32 or Norton) installed on their computer to protect from viruses and hackers.