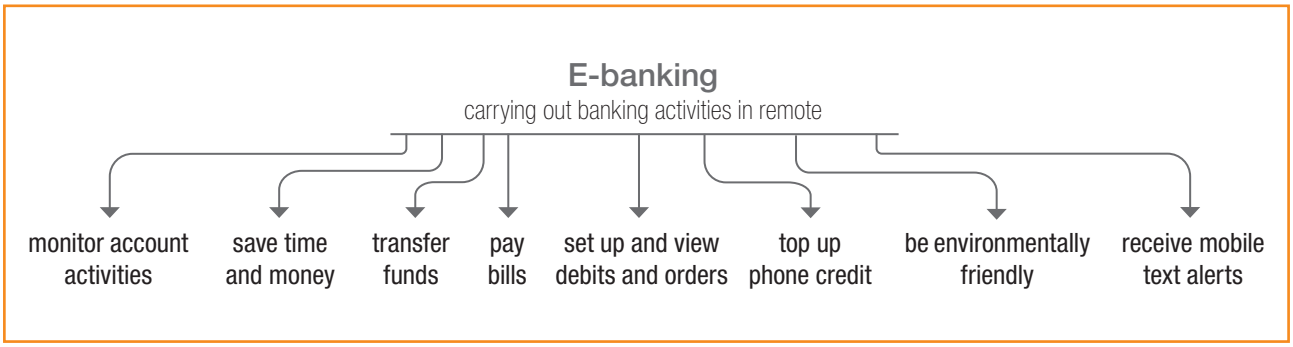
E-banking



A generation ago, managing money and banking transactions only took place inside the bank premises and required the physical presence of the customers. The widespread introduction of the ATM in the late 1970s was the first great leap in the evolution of personal banking, which gave customers more control and autonomy over when and how they could access their money. However, it was the spread of computer technology and the Internet that opened up new opportunities for banks, which started offering additional e-banking services to their customers. Some new virtual banks have emerged too, which operate entirely online with no high street branches.

E-banking enables customers to carry out most standard banking activities in remote, by logging in to a secure website from a computer or via a mobile device (known as mobile banking or M-banking). In the age of smart phones, some banking apps have been devised too: for example, a mobile deposit app deposits cheques by simply taking a picture and uploading it to the personal account and a mobile wallet app lets customers interact with a terminal to pay for their purchases, as if they were opening their leather wallets.

Through online banking customers can:

- **monitor** their account activities, balances and bank statements in real time, anywhere and at any time;
- **save time and money** because banking fees are cheaper than rates in brick and mortar banks;
- **transfer funds** between or to other accounts;
- **pay** phone, utility or credit card bills;
- **set up and view** direct debits and standing orders;
- **buy and sell** shares, bonds and other investment products;
- **top-up phone credit**;
- **be environmentally friendly** by switching off paper statements for current accounts and credit cards and store or view them online;
- **receive mobile text alerts** to keep track of finances and payments.

Despite its advantages, some people are still sceptical about e-banking because they are:

- computer illiterate and feel intimidated at using computers;
- afraid of copycat sites and identity theft from hackers, who can steal sensitive data through fraudulent emails that mimic the bank's credential (called phishing) and lure customers into revealing account numbers or passwords;
- used to a more personal and direct contact with bank clerks.

1 Complete the sentences with a suitable ending.

1. In the past bank customers used to .....
2. The first step towards a more personal form of banking .....
3. Nowadays, high street banks offer their customers .....
4. E-banking can be carried out .....
5. If you take a picture of a cheque .....
6. Brick-and-mortar banks charge .....
7. E-banking is environmentally friendly because .....
8. People who are not used to using computers .....
9. Phishing is a form of .....
10. The lack of a face-to-face conversation with a bank clerk .....

Trivia

The most dangerous financial malware is called Zeus and it has stolen more than 70,000 passwords and account numbers from banks and businesses including NASA, the Bank of America and Amazon.

2 Fill in the blanks with the missing words.

closed ■ block ■ https ■ spreading ■ log in ■ warrant ■ users ■ additional ■ measures ■ authenticate ■ account ■ easy ■ anti-virus ■ secure ■ active

What Are Banks Doing to Make Online Banking Safer?

Even though online banking is commonplace in today's world, we may not realise all the **1.** ..... banks take to ensure **2.** ..... online banking for their customers. Although many banks have their own technology and online banking guarantees, there are common measures taken by all banks to **3.** ..... their customers' secure online banking experience. These include:

- an **up-to-date 4.** ..... **protection** that allows banks to detect viruses and prevent them from **5.** .....;
- firewalls that help banks **6.** ..... unauthorised access to individuals or networks, and create a more secure online banking environment;
- a **Secure Socket Layer (SSL) encryption** that creates a safer connection with the browser when users **7.** ....., fill out an application, register for services and more. Although the technology is sophisticated, it's **8.** ..... to make sure that SSL encryption is **9.** ..... on the page because the padlock logo, on the bottom of the website browser, is **10.** ..... A secure Internet website address, as seen in the address bar of the browser, begins with **11.** ..... If there is no "s", it means that the website is not secure and **12.** ..... should not do online banking on it;
- **cookies**, short texts which are placed on the computer after an initial login, allow banks to recognise or **13.** ..... that computer when a user logs in to an account again. If a new computer is used to log in to that same **14.** ....., or cookies are erased, **15.** ..... information will be required at the next login.

3 You will hear a reporter. Complete the summarising table.

Hackers' Last Cyber Attack Fuels Fears over Bank Security	
Bank hacked:	**1.** ..... in **2.** .....
Money stolen:	**3.** $ ..... from **4.** ..... of New York
Due to:	**5.** ..... that allowed **6.** ..... to carry out bank **7.** ..... to accounts in the **8.** ..... and Sri Lanka
Further attack:	**9.** $ ..... million failed for a **10.** ..... mistake in the transactions are looking into the hack with **11.** .....
Security researchers:	
Type of malware:	a Trojan or similar **12.** ..... to gain **13.** ..... control of the bank's system think a **14.** ..... flaw made the security system vulnerable and hackers could the bank's **15.** .....
Investigators:	
Cause:	still under investigation: was the malware really **16.** ..... or the bank's weak?