INTRODUCTION TO e-BANKING

Dr.M.Theivanayaki, Assistant Professor, Department of Business Administration (IB&RM), PSGR Krishnammal College for Women, Coimbatore

Dr.M.Ganeshwari, Assistant Professor, Department of Business Administration (IB&RM), PSGR Krishnammal College for Women, Coimbatore

S.Nilofar,II BBA RM, Department of Business Administration (IB&RM),

PSGR Krishnammal College for Women, Coimbatore

S.Haarishmitha, II BBA RM, Department of Business Administration (IB&RM),

PSGR Krishnammal College for Women, Coimbatore

INTRODUCTION

Online banking, also known as **internet banking**, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

Some banks operate as a "direct bank" (or “virtual bank”), where they rely completely on internet banking.

Internet and customer reluctance

When the clicks-and-bricks euphoria hit in the late 1990s, many banks began to view web-based banking as a strategic imperative. In 1996 OP Financial Group, also a cooperative bank, became the second online bank in the world and the first in Europe. The attraction of banks to online banking are fairly obvious: diminished transaction costs, easier integration of services, interactive marketing capabilities, and other benefits that boost customer lists and profit margins. Additionally, online banking services allow institutions to bundle more services into single packages, thereby luring customers and minimizing overhead.

A mergers-and-acquisitions wave swept the financial industries in the mid- and late 1990s, greatly expanding banks' customer bases. Following this, banks looked to the Web as a way of maintaining their customers and building loyalty. A number of different factors are causing bankers to shift more of their business to the virtual realm.

While financial institutions took steps to implement e-banking services in the mid-1990s, many consumers were hesitant to conduct monetary transactions over the internet. It took widespread adoption of electronic commerce, based on trailblazing companies such as America Online, Amazon.com and eBay, to make the idea of paying for items online widespread.

By 2000, 80% of U.S. banks offered e-banking. Customer use grew slowly. At Bank of America, for example, it took 10 years to acquire 2 million e-banking customers. However, a significant cultural change took place after the Y2K scare ended. In 2001, Bank of America became the first bank to top 3 million online banking customers, more than 20% of its customer base. In comparison, larger national institutions, such as Citigroup claimed 2.2 million online relationships globally, while J.P. Morgan Chase estimated it had more than 750,000 online banking customers. Wells Fargo had 2.5 million online banking customers, including small businesses. Online customers proved more loyal and profitable than regular customers. In October 2001, Bank of America customers executed a record 3.1 million electronic bill payments, totaling more than $1 billion. In 2009, a report by Gartner Group estimated that 47% of United States adults and 30% in the United Kingdom bank online.

The early 2000s saw the rise of the branch-less banks as internet only institutions. These internet-based banks incur lower overhead costs than their brick-and-mortar counterparts. In the United States, deposits at most direct banks are FDIC-insured and offer the same level of insurance protection as traditional banks.

First online banking services by region

The United States

Online banking was first introduced in the early 1980s in New York, United States.[6] Four major banks — Citibank, Chase Bank, Chemical Bank and Manufacturers Hanover — offered home banking services. Chemical introduced its Pronto services for individuals and small businesses in 1983, which enabled individual and small-business clients to maintain electronic checkbook registers, see account balances, and transfer funds between checking and savings accounts. Pronto failed to attract enough customers to break even and was abandoned in 1989. Other banks had a similar experience.

Since its inception in the United States, online banking has been federally governed by the *Electronic Funds Transfer Act of 1978*.

The United Kingdom

Almost simultaneously with the United States, online banking arrived in the United Kingdom. The UK's first home online banking services known as Homelink was set up by Bank of Scotland for customers of the Nottingham Building Society (NBS) in 1983. The system used was based on the UK's Prestel viewlink system and used a computer, such as the BBC Micro, or keyboard (Tandata Td1400) connected to the telephone system and television set. The system allowed on-line viewing of statements, bank transfers and bill payments. In order to make bank transfers and bill payments, a written instruction giving details of the intended recipient had to be sent to the NBS who set the details up on the Homelink system. Typical recipients were gas, electricity and telephone companies and accounts with other banks. Details of payments to be made were input into the NBS system by the account holder via Prestel. A cheque was then sent by NBS to the payee and an advice giving details of the payment was sent to the account holder. BACS was later used to transfer the payment directly.

France

After a test period with 2,500 users starting in 1984, online banking services were launched in 1988, using Minitel terminals that were distributed freely to the population by the government.

By 1990, 6.5 million Minitels were installed in households. Online banking was one of the most popular services.

Online banking services later migrated to Internet.

Japan

In January 1997, the first online banking service was launched by Sumitomo Bank.By 2010, most major banks implemented online banking services, however, the types of services offered varied. According to a poll conducted by Japanese Bankers Association (JBA) in 2012, 65.2% were the users of personal internet banking.

Banks and the World Wide Web

Around 1994, banks saw the rising popularity of the internet as an opportunity to advertise their services. Initially, they used the internet as another brochure, without interaction with the customer. Early sites featured pictures of the bank's officers or buildings, and provided customers with maps of branches and ATM locations, phone numbers to call for further information and simple listings of products.

Interactive banking on the Web

In 1995, Wells Fargo was the first U.S. bank to add account services to its website, with other banks quickly following suit. That same year, Presidential became the first U.S. bank to open bank accounts over the internet. According to research by Online Banking Report, at the end of 1999 less than 0.4% of households in the U.S. were using online banking. At the beginning of 2004, some 33 million U.S. households (31%) were using some form of online banking. Five years later, 47% of Americans used online banking, according to a survey by Gartner Group. Meanwhile, in the UK online banking grew from 63% to 70% of internet users between 2011 and 2012.

Operation

To access a financial institution's online banking facility, a customer with internet access will need to register with the institution for the service, and set up a password and other credentials for customer verification. The credentials for online banking is normally not the same as for telephone or mobile banking. Financial institutions now routinely allocate customers numbers, whether or not customers have indicated an intention to access their online banking facility. Customer numbers are normally not the same as account numbers, because a number of customer accounts can be linked to the one customer number. Technically, the customer number can be linked to any account with the financial institution that the customer controls, though the financial institution may limit the range of accounts that may be accessed to, say, cheque, savings, loan, credit card and similar accounts.

The customer visits the financial institution's secure website, and enters the online banking facility using the customer number and credentials previously set up.

Each financial institution can determine the types of financial transactions which a customer may transact through online banking, but usually includes obtaining account balances, a list of recent transactions, electronic bill payments, financing loans and funds transfers between a customer's or another's accounts. Most banks set limits on the amounts that may be transacted, and other restrictions. Most banks also enable customers to download copies of bank statements, which can be printed at the customer's premises (some banks charge a fee for mailing hard copies of bank statements). Some banks also enable customers to download transactions directly into the customer's accounting software. The facility may also enable the customer to order a cheque book, statements, report loss of credit cards, stop payment on a cheque, advise change of address and other routine actions.

Features

Online banking facilities typically have many features and capabilities in common, but also have some that are application specific. The common features fall broadly into several categories:

- A bank customer can perform non-transactional tasks through online banking, including:
    - Viewing account balances
    - Viewing recent transactions
    - Downloading bank statements, for example in PDF format
    - Viewing images of paid cheques
    - Ordering cheque books
    - Download periodic account statements
    - Downloading applications for M-banking, E-banking etc.
- Bank customers can transact banking tasks through online banking, including:
    - Funds transfers between the customer's linked accounts
    - Paying third parties, including bill payments (see, e.g., BPAY) and third party fund transfers (see, e.g., FAST)
    - Investment purchase or sale
    - Loan applications and transactions, such as repayments of enrollments
    - Credit card applications
    - Register utility billers and make bill payments
- Financial institution administration
- Management of multiple users having varying levels of authority
- Transaction approval process

Some financial institutions offer special internet banking services, for example:

- Personal financial management support, such as importing data into personal accounting software. Some online banking platforms support account aggregation to allow the customers to monitor all of their accounts in one place whether they are with their main bank or with other institutions.

Security

Five security token devices for online banking

Security of a customer's financial information is very important, without which online banking could not operate. Similarly the reputational risks to banks themselves are important.[10] Financial institutions have set up various security processes to reduce the risk of unauthorized online access to a customer's records, but there is no consistency to the various approaches adopted.

The use of a secure website has been almost universally embraced.

Though single password authentication is still in use, it by itself is not considered secure enough for online banking in some countries. Basically there are two different security methods in use for online banking:

- The PIN/TAN system where the PIN represents a password, used for the login and TANs representing one-time passwords to authenticate transactions. TANs can be distributed in different ways, the most popular one is to send a list of TANs to the online banking user by postal letter. Another way of using TANs is to generate them by need using a security token. These token generated TANs depend on the time and a unique secret, stored in the security token (two-factor authentication or 2FA).

    More advanced TAN generators (chipTAN) also include the transaction data into the TAN generation process after displaying it on their own screen to allow the user to discover man-in-the-middle attacks carried out by Trojans trying to secretly manipulate the transaction data in the background of the PC.

    Another way to provide TANs to an online banking user is to send the TAN of the current bank transaction to the user's (GSM) mobile phone via SMS. The SMS text usually quotes the transaction amount and details, the TAN is only valid for a short period of time. Especially in Germany, Austria and the Netherlands many banks have adopted this "SMS TAN" service.

    Usually online banking with PIN/TAN is done via a web browser using SSL secured connections, so that there is no additional encryption needed.

    - Signature based online banking where all transactions are signed and encrypted digitally. The Keys for the signature generation and encryption can be stored on smartcards or any memory medium, depending on the concrete implementation (see, e.g., the Spanish ID card *DNI electrónico*).

Attacks

Attacks on online banking used today are based on deceiving the user to steal login data and valid TANs. Two well known examples for those attacks are phishing and pharming. Cross-site scripting and keylogger/Trojan horses can also be used to steal login information.

A method to attack signature based online banking methods is to manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background.

A 2008 U.S. Federal Deposit Insurance Corporation Technology Incident Report, compiled from suspicious activity reports banks file quarterly, lists 536 cases of computer intrusion, with an average loss per incident of $30,000. That adds up to a nearly $16-million loss in the second quarter of 2007. Computer intrusions increased by 150 percent between the first quarter of 2007 and the second. In 80 percent of the cases, the source of the intrusion is unknown but it occurred during online banking, the report states.

Another kind of attack is the so-called man-in-the-browser attack, a variation of the man-in-the-middle attack where a Trojan horse permits a remote attacker to secretly modify the destination account number and also the amount in the web browser.

As a reaction to advanced security processes allowing the user to cross-check the transaction data on a secure device there are also combined attacks using malwareand social engineering to persuade the user himself to transfer money to the fraudsters on the ground of false claims (like the claim the bank would require a "test transfer" or the claim a company had falsely transferred money to the user's account and he should "send it back").Users should therefore never perform bank transfers they have not initiated themselves.

Countermeasures

There exist several countermeasures which try to avoid attacks. Digital certificates are used against phishing and pharming, in signature based online banking variants (HBCI/FinTS) the use of "Secoder" card readers is a measurement to uncover software side manipulations of the transaction data.[16]

In 2001, the U.S. Federal Financial Institutions Examination Council issued guidance for multifactor authentication (MFA) and then required to be in place by the end of 2006.

In 2012, the European Union Agency for Network and Information Security advised all banks to consider the PC systems of their users being infected by malware by default and therefore use security processes where the user can cross-check the transaction data against manipulations like for example (provided the security of the mobile phone holds up) SMS TAN where the transaction data is sent along with the TAN number or standalone smartcard readers with an own screen including the transaction data into the TAN generation process while displaying it beforehand to the user to counter man-in-the-middle attacks