A STUDY ON ONLINE BANKING SYSTEM AND PROTECTION AGAINST POTENTIAL MALWARES

Nusrat Huq, Lecturer
Tasnuva Farin, Lecturer
Department of Management and Human Resource Management
American International University, Bangladesh

Introduction
The Internet and many other information technology systems have presented great opportunities for e-businesses. The Internet helps companies to expand and to expose themselves to a much larger customer base and diversify their offerings. It is a faster and less expensive way of doing business. Marketing executives think of the Internet as the most exciting channel available for advertising purposes (Herbig and Hale, 1997).

However, companies that decide to take on digital businesses face countless numbers of risks, especially when there is a breach of security. Companies should take extensive security measures in order to reduce this risk and to secure the sites that they operate their business in.

Another reason that hampers faster growth of electronic businesses is the issue of trust. Customers are still doubtful about disclosing their personal information online in fear of invasion of privacy.

This paper aims to explore perceived risks and suggests a number of ways to reduce these risks in the online banking environment, by both businesses and clients themselves.

Literature Review
The history of the Internet began in the late 1960s as a result of the Cold War. The United States Department of Defence connected four computers in California, Colorado and Utah in order to minimise the vulnerability of several of its mainframe computer systems. The Internet is simply a network of networks (Forcht and Wex, 1996). It means many things to many people, but a common perception is that it is a large encyclopaedia of all human knowledge, the part that is accessible to the general public (Rao, 1997).

The emergence of the Internet has had an impact on business as well as households like no other technology ever had (Liddy, 1996). Banking, stock exchanges, air traffic control, telephones, electric power, and a wide range of institutions of health, welfare, and education are largely dependent on information technology and telecommunications – the internet – for their operation (Salifu, 2008).

Modernized information systems (IS) have brought enterprises not only enormous benefits, but also linked information threats. Many tools and anti-virus systems, covering almost every facet of IS security, have been developed in response to these threats. However, the effectiveness of current security solutions has been seriously questioned, since the volume of security related incidents, consequent financial losses, continues to rise in magnitude and severity (Hinde, 2003).

Security is one of the most challenging topics faced by companies today that want to take their business online. When a user attaches to the Internet, anyone from
anywhere around the world can access the information being sent. This gives rise to the risk of data theft, theft of service, corruption of data and virus attacks become inevitable (Aldridge et al., 1997). Seven members of the Lopht Heavy Industries, an independent watchdog group composed of seven hackers, informed the Senate Committee on Governmental Affairs in 1998, that “it would take only 30 minutes for them to render the Internet unusable for the entire nation” (Yasin, 1998).

The best way to keep an intruder from entering the network is to provide a security wall between the intruder and the corporate network. There are a variety of methods that a company can employ to protect itself from unauthorized access. Some of the most popular methods are: firewalls, user authentication; digital certificates, virus detection, key management, data encryption, extranets, intrusion detection systems (IDS), virtual private networks (VPN) and extranets (Hawkins et al., 2000).

Companies that collect information from customers and store it in their systems have the risk of facing unauthorised data retrieval. With this data, these users can alter data obtain access to secure information or even to just destroy the system (Aldridge et al., 1997).

The purpose of this paper is to focus on the research of one particular type of business which has the potential for growth, but is being held back due to security issues - online banking.

Online banking, also known as internet banking and e-commerce, has experienced phenomenal growth in the recent years (Yap et al., 2010). It has such enormous potential because of its convenience and benefits. Customers could gain from a wider range of financial benefits like lower transaction handling fees. They can benefit from faster transaction speed by saving the time of customers since there are no documents that have to be handled and the process does not require one to wait in a queue or line. Customers could also perform banking transactions from anywhere in the world and obtain 24-hour service (Lee, 2009). Nonetheless, the growth of e-banking has not kept pace with that of internet usage and attributes this gap to the lack of trust among bank customers (Yap et al., 2010).

There are different kinds of perceived risks that scholars have identified. Different kinds of risks then become a barrier to the choice of shopping channel (Manzano et al., 2009).

Security Risk- Consumers have the fear of losing money through online banking transactions. Research done in the past show that perceived security risk is an important predictor of internet banking adoption. A research done (Lee et al., 2005) showed that it was prospective clients who had fear of this risk more that the current users (Manzano et al., 2009).

Privacy Risk is where customers are afraid of being invaded of their privacy. They are concerned about their information being shared by the bank and research has showed that consumers want their information to be kept safe and secure (Manzano et al., 2009).

Customers are also unsure about the quality of service they would get since there is no direct contact with the provider and this leads to a decrease in confidence (Ba, 2001). This is called Performance Risk. Customers get anxious that a breakdown of system servers or disconnection from the Internet will occur while conducting online transactions because it may result in unexpected losses (Kuisma et al., 2007).
Time-loss Risk is the possibility that there will be loss of time and inconvenience occurred due to system downtimes, delays of payment and difficulty of navigation. Some people also fear the time to be lost in learning the online banking system method, even though banks have tried to make the process relatively easy (Lee, 2009). There is also the fear of time that could be lost in trying to rectify erroneous transactions.

Social Risk- This is a risk associated with the possibility of an online banking service user to be judged by their family members and peers who may have both positive or negative perceptions about the online banking system. Some parts of society are cynical towards technology and prefer human and social interaction over fast mechanical online services (Manzano et al., 2009).

Other reasons why such trust issues persists may be due to the publicity of e-mail scams, identity theft, and ‘phishing’ that distort customer perceptions (Gerrard et al., 2006). Examples of such publicity can be of internet financial fraud in Brazil, which exceeded the amount of money lost in brick and mortar bank robberies (BBC, 2004). Another example could be of June 2005, where a computer hacker took the details of 40 million credit cards (BBC, 2005).

Businesses have started using electronic user authentication systems as a means of solving this problem (Fletcher, 2007). Many businesses are still unaware of the threat from cyber criminals or malicious hackers (BBC, 2005). Every year, new internet security vulnerabilities emerge and even though numerous tools of protection are in place, the challenge for e-businesses is to keep up with the cyber criminals and innovate new technology to guard their financial assets and customers (Fletcher, 2007).

Critical Evaluation and Suggested Solutions

Industry sectors such as banking have openly embraced e-commerce to improve their performance and gain strategic competitive advantage. However, the perceived risk of online banking is still hampering its growth.

Online banking fraud has risen by 14% in 2009, but overall card fraud has dropped to 28% - the first decrease since 2006, according to figures from bankers. The decline of internet crime has been attributed to the combination of the move to chip and Pin and greater use of sophisticated fraud detection tools by banks and retailers. For example, the introduction of MasterCard Secure Code and Verified by Visa authentication systems helped cut ‘card not present’ fraud by 19%, the first decrease ever (Grant, 2010).

Trojan Horses

One of the biggest threats that banks nowadays face is the SSL invading Trojan Horses which bypass the secure and authenticated tunnel mechanisms that are the safety backbone of today’s internet banking and financial institutions (Grimes, 2006). Trojan horses that criminals have recently devised have become more sophisticated as banks tighten their online security measures. Criminals today can hijack active online banking sessions and can fake account balances to prevent victims from seeing that they are being defrauded. Previously, such malware could just steal usernames and passwords for specific banks, but the hacker would have to manually access the compromised account to withdraw funds (Vamosi, 2010).

Criminals have come up with extremely sophisticated tools in order to hijack money from the online banking systems. A particularly dangerous tool is the URLzone
which defects when it is being watched so it becomes difficult to catch the act. Another tool called the Zues impersonates the bank to take out personal information. This is extremely hard to detect as each victim receives a slightly different version of it. Clampi is another bank botnet that waits for users to login to the account and shows that the system is temporarily down and when the victim moves on, the crook transfers the money out of the account (Vamosi, 2010).

Customers are afraid of obtaining loss due to a hacker compromising the security of the user. Phishing is a method where phishers attempt to fraudulently acquire personal information such as password and credit card details, by masquerading as a trustworthy source in source in the electronic communication process. This does not only lead to monetary loss, but it also violates the user’s privacy which is a major concern for many internet users. Aladwani’s (2001) study found that potential online banking customers ranked internet security and customers’ privacy as the most important future challenges facing banks. Consumers fear of being victims of identity theft while using online banking services (Lee, 2009). Therefore, perceived fears of divulging personal information and feelings of insecurity have a negative influence on internet banking services use (Howcroft et al., 2002).

As a stand to fight fraud, banks developed authentication devices such as device ID, geolocation and challenging questions (Vamosi, 2010).

Banks can tackle phishing directly by working with service providers, such as Mark Monitor, which recognize and close down phishing sites before they can have an impact. In spite of all these efforts, personal financial information will get into the public domain and fraudsters will have IDs with a previously good reputation to do transactions online. Spotting a thief using someone else's ID online is hard (Tarzey, 2008).

The obvious solution to fight off such viruses is for the customer to employ ant-virus software solutions. Companies that create ant-virus packages are usually up-to-date with the threats that are coming up every day. For example, a new technology called the Firefront Client Security protects the customers from threats like Trojans and other malicious spyware (West, 2007).

But, banks cannot always rely on customers anti-virus softwares to stop SSL-evading Trojans. A number of approaches used may not be able to block all attacks but can raise an alert when there is suspicious activity taking place. Examples could be to implement a transactional authorisation checking defence on the website for non-trivial transactions. They could require two factor authentication - using voice or another device for the second factor for non-trivial transactions. They could also e-mail their clients activity summaries after transactions or account status changes to allow early notification of illegitimate activity (Grimes, 2006).

Organisations must make an effort to defend themselves against the attack of hackers and must ensure that they have a well-defined and enforceable security policy in place. Safeguards must be put in place to prevent intrusion and information theft. The system should be designed to keep unauthorised users at bay, but it must also be easy enough so that authorised entrants could do their online transactions at ease (Wen et al., 1998).

A complete and practical security plan can identify what the company’s needs are which systems and networks should be fully protected and what types of security

JOURNAL OF APPLIED MANAGEMENT AND INVESTMENTS
architecture and applications are essential. Only then could businesses put up firewalls and block out unwanted entrants (Wen et al., 1998; Smith, 2004).

Firewalls apply to the combination of hardware and software products that are used to protect information systems from outsiders’ unauthorised access. Firewall products limit and control access to the available corporate information on the website. They are a corporate server’s first and most important line of defence (Wen et al., 1998).

Since information system manufacturers are constantly coming up with new modes of technology to deter online crime, businesses should adopt these systems in accordance with their systems so that their clients and they are safe from being robbed.

**Industry Examples**

A recent article published in Bank Technology News claim that man-in-the-middle attacks and other assaults on the Web Browser has posed a challenge for the whole banking industry and Fifth Third Bank, based in the United States of America (USA) has decided to take measures as counter attack. This bank has taken action by piloting a security system solution for corporate clients that ‘lock down’ the online banking session between the customers and the bank (BTN, 2010).

Trusteer offers a desktop browser security plug in and it has been found that European Banks were quicker to adopt this solution compared to US Banks. 50 Banks worldwide has made the Trusteer solution available to their customers as a measure for protection from online fraud. Banks like NatWest, Royal Bank of Scotland, Santander and HSBC. In the United Kingdom alone, there have been 5 million downloads (BTN, 2010).

This software, when being used, warns customers if they are at the risk of responding to a phishing attack. It also prevents Trojans from stealing the personal details of users and inhibits any interference with online communications between the customer and the bank (BTN, 2010).

Another solution has been developed by IBM. They have invented a hardware device that plugs into the customer’s personal computer. This device is called the ZTIC-Zone Trusted Information Channel. This device attaches itself to the computer via a USB cable. During an online banking transaction, along with a smart card, ZTIC bypasses the web browser and makes a direct SSL connection with the bank. The bank can constantly monitor and decide when to activate the ZTIC to warn the customer when malicious activity may be occurring. These solutions may be expensive but are extremely effective in warding off online banking fraud and theft (BTN, 2010).

These security solutions have been quite successful in being implemented in the European market as opposed to the United States. US bankers are afraid of inconveniencing customers by enacting too many guardrails and exposing themselves to litigation (BTN, 2010).

The main aim of all banks that employ online banking should be to protect customers, and not their businesses. If banks keep their systems fool-proof, they are the ones who stand to gain in the future, because this will increase the level of trust among people, and they would be more comfortable in using the online banking system.

Another example is of Swedish Bank Nordea who has had a loss of more than 7 million krona in 2007 in an online banking heist. Nordea customers had been targeted by e-mails containing tailor made Trojans, for over 15 months before the actual heist.
250 customers had been affected by the fraud after falling victim to phishing e-mails containing the Trojan. This Trojan encouraged clients to download a ‘spam fighting’ application and users who downloaded this application did not realise that they also downloaded a file attached which was affected by the Trojan (www.cnet.com, retrieved 4 May 2010).

When users attempted to login to the Nordea Online Banking site, they were re-directed to a false homepage, where they entered important login information, including security login numbers. When the clients tried to access the online banking website, a system downtime message was showed and the robbers could get into the secured accounts to transfer money to other accounts (www.cnet.com, retrieved 4 May 2010).

The Nordea spokesman for Sweden blamed social engineering for the robbery rather than deficiencies in the security systems. As an effort to combat fraud, most banks monitor the behaviour of people claiming to be their customers, so that unusual transaction behaviour could be tracked and halted if necessary (www.cnet.com, retrieved 4 May 2010).

Nordea could not detect the fraudulent activity since the robbers made a large number of small transactions within a span of 15 months which enabled the criminals to successfully transfer a large amount of money without raising any doubt (www.cnet.com, retrieved 4 May 2010).

Conclusions

Banks should now be more concerned with protecting their online banking systems compared to their brick-and-mortar outlets since research has proven that untold millions are being siphoned away from customers by fraudsters online, using SSL-evading Trojans and more refined phishing techniques.

In order for the online banking system or any online business entity to attract a larger part of the population, it is crucial for them to keep up with the hackers and employ such security systems that would deem impenetrable by them. This may require constant investments in obtaining new technology but this will reap benefits in the long run.

Banks, who rely on customers to keep updated anti-virus software and train themselves to understand how to avoid risks, should take a more active stand in this educational structure. Businesses should try to educate people so that the sceptical potential clients would overcome their fear and use e-banking.

The activities and transactions taking place may be virtual but the operators who are using and misusing this virtual world are of human nature. Governments should make stronger legislations for punishment for those people who make this malicious software.

References


A STUDY ON ONLINE BANKING SYSTEM AND PROTECTION AGAINST POTENTIAL MALWARES
Nusrat Huq
Tasnueva Farin
American International University, Bangladesh

Abstract
Online banking systems have provided massive advantages in the recent years. Malwares such as Trojans have helped increase bank frauds by means of ‘phishing’ and in the recent years this is rising at an alarming level, as criminals come out with more sophisticated and dangerous tools to commit e-crime. Banks are continuously updating their services online through implementation of advanced security solutions and tried to keep up with these criminals, however, the fraudsters come up with newer means to break the security systems set up by the banks. The article discusses ways in that businesses as well as customers can avoid or minimise such risks.

Keywords: Internet, information technology, banks, e-business, on-line banking, phishing