ELECTRONIC BANKING SECURITY - AT A GLANCE

Author

Prof.G.Chinna Durai M.com., M.Phil., Ph.D., (SET), (NET),
Assistant Professor of Corporate Secretaryship,
Sourashtra College,
Madurai, Tamilnadu – 625004.
Email: prof.gc.soucollege9919@gmail.com
Phone. No: 99525 51254

Co-Author

Dr.V.Sureshbabu M.com., M.Phil., Ph.D.,
Assistant Professor of Commerce,
Mannar Thirumalai Naicker College,
Madurai, Tamilnadu – 625004.
Email: nithyasureshbabu5@gmail.com
Phone. No: 94864 86668

ABSTRACT

Electronic banking is changing the banking industry, having the major effects on banking relationships. Banking is now no longer confined to the branches were one has to approach the branch in person, to withdraw cash or deposit a cheque or request a statement of accounts. In true electronic banking, any inquiry or transaction is processed online without any reference to the branch at any time. An electronic banking, thus, now is more of a norm rather than an exception in many developed countries due to the fact that it is the cheapest way of providing banking services. Apart from the many advantages of electronic banking have certain security problems. The challenges that oppose electronic banking are the concerns of security and privacy of information. The current focus of security of information transfer is on the session layer protocols and the flaws in end to end computing. A secure of this transaction requires a secure protocol to communicate over untrusted channels and a trusted code at both endpoints. The solution addresses the use of secure protocols because trusted channels don't really exist in most of the environment, especially since we are dealing with linking to the average consumers. Hence, the researchers undertaken to study the "Electronic Banking Security – At a Glance".

Keywords: *E-banking, Phishing, Spam, Spyware and Hacking.*

INTRODUCTION

Information technology developments in the banking sector have sped up communication and transactions for clients. It is vital to extend this banking feature to clients for maximizing the advantages for both clients and service providers. Internet is the cheapest delivery channel for banking products as it allows the entity to reduce their branch networks and downsize the number of service staff. The navigability of the website is a very important part of Electronic banking because it can become one of the biggest competitive advantages of a financial entity. Due to increase in technology usage the banking sector's performance increases day by day. Electronic banking is becoming the indispensable part of modern day banking services.

It is notoriously difficult to predict the future, but some educated guesses can be made using past and current experiences. In our view, the next developments in e - banking will involve new products and services that were not feasible in traditional banking models. This could involve enabling instant payments using mobile devices, or tools to help people manage their multi-bank financial portfolio, simultaneously. Internet only banking may also become more viable as the functionality of e - banking systems grows, and customers adapt to the new ways of conducting their financial activities. International banking might become a reality for ordinary consumers as banking payments systems are increasingly harmonised across borders. E-banking has the potential to be a very rich and pleasant experience, and may provide more opportunities for banks to develop mutually satisfying, tailor made services to enrich relationship with customers. As technology evolves, the opportunities to extend the relationship beyond what is possible in the physical world continue to grow and will only be limited by a bank's ability to innovate or commitment to e - banking.

OBJECTIVES

- To study the out lay of Electronic banking system in India.
- To analyses the various types of electronic banking frauds in India.

METHODOLOGY

The research study purely conceptual based research and only uses secondary data such as journals, websites and text books. The study does not use primary data information.

TYPES OF ELECTRONIC BANKING FRAUDS

The disclosure of important information that should remain confidential, by unauthorized persons or that exceed their authority can cause significant losses for financial institutions. Alteration of information by entering, modifying or overwriting data into the system without authorization or by exceeding one's authority is a type of attack that could potentially harm greatly the banks and their customers. Security threats can affect a financial institution through numerous vulnerabilities. No single control or security device can adequately protect a system connected to a public network. Many problems concerning the security of transactions are the result of unprotected data being sent between clients and servers. The problems of the systems today are inherent within the setup of the communications and also within the computers itself. The current focus of security is on session-layer protocols and the flaws in end-to-end computing. A secure end-to-end transaction requires a secure protocol to communicate over untrusted channels, and a trustee code at both endpoints. It is really important to have a secure protocol because the trusted channels really don't exist in most of the environment. The following ways are used to collapse the electronic banking security.

Phishing

A person's personal details are obtained by fraudsters posing as bankers, who float a site similar to that of the person's bank. They are asked to provide all personal information about themselves and their account to the bank on the pretext of database up gradation. The number and password are then used to carry out transactions on their behalf without their knowledge. Phishing involves using a form of spam to fraudulently gain access to people's online banking details. As well as targeting online banking customers, phishing emails may target online auction sites or other online payment facilities. Typically, a phishing email will ask an online banking customer to follow a link in order to update personal bank account details. If the link is followed, the victim downloads a program which captures his or her banking login details and sends them to a third party. Website cloning is the duplication of a website for criminal use. Often times websites cloning will take the form of known chat room or trade sites so that people will either unknowingly give information to the criminal or make a "fake" purchase, willingly giving money for a product that does not actually exist.

Spam

Spam is an electronic 'junk mail' or unwanted messages sent to your email account or mobile phone. These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details.

Spyware

Spyware such as Trojan Horse is generally considered to be software that is secretly installed on a computer and takes things from it without the permission or knowledge of the user. Spyware may take personal information, business information, bandwidth; or processing capacity and secretly gives it to someone else. "Trojan Horse" scheme unfolds when malicious software (malware) embeds to a consumer's computer without the consumer being aware of it. Trojans often come in links or as attachments from unknown email senders. After installation the software detects when a person accesses online banking sites and records the username and password to transmit to the offender.

Card skimming

Card skimming is the illegal copying and capture of magnetic stripe and PIN data on credit and debit cards. Skimming can occur at any bank ATM or via a compromised EFTPOS machine. Captured card and PIN details are encoded into a counterfeit card and used to make fraudulent account withdrawals and transactions.

ATM Skimming

Fraudsters can attach false casings and PIN pad overlay devices onto genuine existing ATMs, or they can attach a camouflaged skimming device onto a card reader entry used in tandem with a concealed camera to capture and record PIN entry details.

EFTPOS Skimming

Electronic Fund Transfer at Point of Sale a foreign device is implanted into an EFTPOS machine that is capable of copying and capturing card and Personal Identification Number PIN details processed through the machine. A compromised EFTPOS terminal can only be detected by a physical inspection.

Hacking

Hacking includes gaining illegal entry into a Personal Computer system. Nowadays, the hacking of Internet Protocol (IP) addresses is very universal as it permits the hackers to imagine a fake online character and carry out illegal dealings exclusive of using his factual individuality.

An identity theft

A large number of identity theft crimes occur over the internet. Criminals can get a hold of your personal information through your computer and then set up fake bank accounts or take put loans in your name.

CONCLUSION

Electronic banking has helped greatly in providing banking services with easy and efficiency globally. It has reduced time waist and high charges associated with the traditional banking system. It has led to banking-as-you-go, and encourages cashless banking. Fraudsters have as well taken advantage of the platform to perpetrate serious crimes that affect both the bank as an institution, and the bank customers. The damage caused by bank fraudsters has gone a long way affecting negatively the economy of many countries.

There is every need to curb this ugly trend with the banking sector. A number of proposals have been presented by researchers on measures to mitigate frauds associated with the banking system. This includes full integration biometrics in electronic banking, user identity at each transaction, use of personal identity, etc. Not all the findings have been integrated in electronic banking to mitigate frauds due to heavy weight of biometrics and its implementation in real time transactions as well as human rights violations.

The researchers are of the view that, the integration a biometric security and a system that unveils users anonymity with electronic banking system will help to mitigate and combat electronic banking frauds.

REFERENCE

- Aleksandar Lukic, (2015) "Benefits and Security Threats in Electronic Banking" International Journal of Managerial Studies and Research (IJMSR) Volume No.3, issue No.6, June, pp 44-45 ISSN 2349-0330.
- Vyas, S, (2012) Impact of E-Banking on Traditional Banking Services, International Journal of Computer Science & Communication Networks, Vol. No.2, issue No.3. ISSN 2854-4982.
- Amtul, F, (2011), "E-Banking Security Issues – Is There A Solution in Biometrics", Journal of Internet Banking and Commerce, Vol. 16, Issue. 2.
- Shah, M. and Clarke, S, (2009) "E-Banking Management: Issues, Solutions, and Strategies", Hershey – Publication, New York, 2009.
- http://www.encyclopedia.com