Online Banking

Matthew N. O. Sadiku[1], Adebowale E. Shadare[2], Sarhan M. Musa[3]

[1,2]Department of Electrical & Computer Engineering, Prairie View A&M University, Prairie View, TX 77446, USA
[3]Department of Engineering Technology, Prairie View A&M University, Prairie View, TX 77446, USA

Abstract— The Internet is rapidly changing the global marketplace and the banking industry is no exception. The banking industry is now providing products and services online. Online banking allows customers to conduct their banking transactions over the Internet. It also facilitates e-society and e-commerce particularly online shopping and online sales. Today online banking is a global phenomenon. The aim of this paper is to provide a brief introduction to online banking.

Keywords— online banking, electronic banking, Internet banking, Internet-based banking, mobile banking.

I.   INTRODUCTION

The Internet has been a catalyst of change for many industries. It is providing a platform for businesses and organizations to extend their services and products to customers. Like other commercial enterprises and the adoption of automatic teller machines (ATMs), banks are taking advantage of the Internet to provide information services to their customers.

Online banking, which is also known as electronic banking or Internet banking, can be traced back to home banking (or distance banking) offered in the mid-1980s. Home banking took two forms: phone-based banking and PC-based banking. Online banking now offers products and services that go beyond home banking and traditional banking. It provides a variety of activities and transactions that customers, small businesses, and large corporations can perform via the Internet. Such transactions include opening an account, paying bills and mortgages, digital currency, ATMs, accessing account information anytime-and-anywhere, providing status of their account and available funds, and storing important documents online [1]. The system supports online bill payment, electronic funds transfer, online shopping, and checkbook transactions. Online banking allows rapid flow of money which helps e-commerce. Users typically access bank websites through the public Wi-Fi networks.

Due to the many advantages of online banking, a flood of banks have entered the industry, creating keen competition and providing increased value to customers. The acceptance of online banking has been rapid all over the world. Even some online-only banks have arisen. These banks must correctly authenticate their customers and be available at all times.

II.   ONLINE BANKING ADOPTION

Online banking is being used by more and more people who are less technically savvy.

Some customers will readily accept online banking, some will do so at a slower pace, while some will never.

Despite investment made on online banking and the numerous benefits it offers, the adoption has been slow. In order to fully adopt online banking, we must understand the factors that hinder or facilitate online banking. The key factors that influence users' acceptance of online banking includes convenience, free service or lower fees, easy to use, user satisfaction, speedy transactions, no bank queues, website features or user interface, compatibility, bank trustworthiness, availability of technology, and accessibility in 24 hours. Online banking also enables real time information exchange. Lack of trust, distrust, privacy, usability, and security are the major concerns customers have against online banking [2]. Online banks should proactively provide more preventive security measures for their services.

III.   MOBILE BANKING

Mobile banking is another form of online banking that uses mobile phones to perform banking transactions. It allows you to quickly and conveniently access your accounts from your mobile phone. It is like having your own personal bank teller anytime, anywhere. Mobile banking supports your securely depositing checks, paying bills or checking your balance all at your fingertips [3].

IV.   CYBER ATTACKS

Security alone is not sufficient for safe online banking. Customers who are patronizing these services play a crucial role. Social engineering tactics are used to lure customers and influence them to act in certain ways or provide certain personal information. Common attacks include phishing, spoofing, malware, virus, worm, identity theft, account information theft, account hijacking, and man in the middle attacks. Customers of online banking may indirectly become targets for these attacks [4].

The goals of targeted cyber attacks are to credit card and banking information, and modify online transactions or inject new transactions. This may lead to accounts being

fraudulently debited or money being transferred to wrong accounts. Three different kinds of attacks have been identified for banking transactions: credential stealing, channel breaking, and content manipulation [5].

Security is a shared responsibility. Although users are encouraged to maintain up-to-date copies of firewall, anti-virus, and anti-spyware on their systems, online banks are basically responsible for providing their protection mechanism. No single strategy can protect an online bank from cyber attacks. A comprehensive approach is needed to provide security controls and protect online information.

Several authentication schemes can be used by online banking in a user-centric context to authorize transactions. Banks should provide interface and navigation systems to prevent cybercrimes. This should not lead to a complex login procedure, which may discourage some customers. Bankers could organize sessions to train and educate customers and businesses on security and privacy issues.

V.   CONCLUSION

The banking industry has persuaded consumers to adopt ATMs, telephone or home banking, and now online banking. The demand for online banking has increased worldwide, but some banks are falling behind their competition. Most traditional banks have proactively encouraged this convenient, cost-saving means by persuading customers to sign up with "peace of mind." Online banking will continue to facilitate e-commerce and serve as a strong catalyst for economic development.

Since online banking involves sensitive transactions, future commitment of customers to online banking depends on trust and security. Online banking is yet to deeply penetrate developing nations such as in Africa and Asia where Internet usage is limited. In such countries, distrust of banking system exists. Ultimately, customers will only use channels that they trust and feel comfortable with [6,7].

REFERENCES

[1] S. P. Wan, "Online banking and beyond: Internet-related offerings from U.S. Banks," in H. Bidgoli (ed.), *The Internet Encyclopedia*. Hoboken, NJ: John Wiley & Sons, 2004, vol. 2, pp. 720-732.

[2] M. Mujinga, M. M. Eloff, and J. H. Kroeze, "Online banking users' perceptions in South Africa: an exploratory empirical study," *IST-Africa 2016 Conference Proceedings*, 2016, pp. 1-7.

[3] C. Chuchen, "The perception of mobile banking adoption: the study of behavoiral, security, and trust in Thailand," *International Journal of Social Science and Humanity*, vol. 6, no. 7, July 2016, pp.547-550.

[4] K. Ivaturi and L. Janczewski, "Social engineering preparedness of online banks: an Asia-Pacific perspective," *Journal of Global Information Technology Management*, vol. 16, no. 4, 2013, pp. 21-46.

[5] M. Alhanahnah and D. W. Chadwick, "Boosting usability for protecting online banking applications against APTs," *Proceedings of Cybersecurity andCyberforensics Conference*, 2016, pp. 70-76.

[6] J. C. Tanner, "Online banking: where the money is?" *Telecom Asia*, Nov. 1999, pp.51-54.

[7] J. S. Benamati and M. A. Serva, "Trust and distrust in online banking: their role in developing countries," *Information Technology for Development*, vol. 13, no. 2, 2007, pp. 161-175.

ABOUT THE AUTHORS

Matthew N.O. Sadiku (sadiku@ieee.org) is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.

Adebowale Shadare (shadareadebowale@yahoo.com) is a doctoral student at Prairie View A&M University, Texas. He is the author of several papers.

Sarhan M. Musa (smmusa@pvamu.edu) is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.