REVIEW STUDY ON THE SECURITY OF
ELECTRONIC PAYMENT SYSTEMS

Tamara Adel AL-Maaitah ✉

PhD Student, Department of Management, Faculty of Business Studies,

School of Business Innovation & Technopreneurship, University Malaysia Perlis, Perlis, Malaysia

tamara_198992@yahoo.com

Abdullah Osman

Professor, Department of Management, Faculty of Business Studies,

School of Business Innovation & Technopreneurship, University Malaysia Perlis, Perlis, Malaysia

Mohammad Suberi

Professor, Department of Management, Faculty of Business Studies,

School of Business Innovation & Technopreneurship, University Malaysia Perlis, Perlis, Malaysia

Dirar AL-Maaitah

PhD Student, Department of Management, Faculty leadership and management,

University Sains Islam Malaysia, Kuala Lumpur, Malaysia

Fairouz AL-Dhmour

Professor, Department of Management Information System, Faculty of Business Administration,

Mutah University, Mutah, Jordan

Abstract

The financial organizations try to cut the cost of partisans over direct deal with the clients and share information with the Internet users plus encourage clients to pay on-line. One of the core difficulties confronted by Organizations in terms of dealing and paying on-line that Internet users are anxious and averse to send sensitive information over the Internet. Actually clients are afraid that through the transactions hackers and Internet interlopers will bargain their

information. This study proposes that there are some security characters such as authentication, authorization, privacy and encryption can influence user's perceptions of security for electronic finance transactions and contribute on the road to enhancing customers' observations that the E-finance transactions are confident and safe to send over sensitive information and pay on-line.

Keyword: Cyber security, Clients, Hacking, E-finance transactions. Electronic payments

INTRODUCTION

The appearance of Internet, the enhancement of Information Technology, and the rapid evolution of wireless telecommunication between institutes and individuals have influenced the financial system significantly and also have enlarged the use of Electronic Finance E-Finance locally as well as comprehensively (Tao & Shin ,2010).

Electronic Finance has affected businesses, individual consumers and has also modification the trading dealings. Most institutions need to implement the new technology in the new environment and improve their businesses efficiency to gain competitive advantage and to be successful in the worldwide economy.

One of the fresh challenges in the competitive and worldwide economy is E-Finance plus electronic payment. E-finance technology is considered one of the most major causes to increase competitive advantage in the worldwide economy. Thus organizations try to grow the trading of information and electronic payment, and increase the means of transactions between exchange partners (suppliers and customers). This can be done breaking the blocks that limit information sharing. When the capacity of transactions and information distribution increases; the level of the linked risk will also rises. Hence organizations need to certify the security of data and the system itself to defend the clients' information being shared (Ratnasingham, 1998).

Nowadays most organizations try to complete their data exchange with E-Finance and gain from the related cost saving and convenience offered to clients, at the similar time they want appropriate security system to ensure that during the financial transactions and electronic payment, all customers' information will be protected. The researchers noticed that privacy is a significant important factor influencing e-businesses and E-Commerce Therefore electronic payment technology need to provide security mechanisms as a sufficient protections in the form of digital signatures, encryption and Web seal assurances…etc., whereby e-finance users perceptions can be gained. The fast growth of Internet and E-Finance usage require a fast and similar growth in security system to satisfy the E-Finance) users especially those who use the electronic payment transactions

EXISTING LITERATURE

Evolution of Electronic Payment

Organizations were used to treaty with financial trades in the traditional method such as paper Work. But with start of communication and internet technology best of financial Techniques dealt with it automatically.Though the attendance of internet and the advance of electronic communications technology influence radically the growth of E-Finance. Accordingly E- finance defined as the provision of financial facilities and market by electronic communication and computation (Shamim ,2007).

Electronic payment systems started since a quit long time. However in developed countries the interbank payment system was activated by telephone networks and mainframe networks. Furthermore, in 1970s Automated Clearing House (ACH) produced in the US) in order to create payment of pays and other vital payments. Meanwhile European Giro system apply electronic plan in order to decrease paper work as it is in credit cards organizations. On the other hand, the number of Automated Teller Machine (ATM) has greater than before from 18,500 in 1980 to 324,000 in 2000 and then increased by time to be well spread in the new year's (Laukkanen et al., 2002)).

Internet Banking Methods

The Internet banking refers to the implementation above the Internet of trade and commercial banking services with individual and company customers with bank transfers, payments, settlements, documentary collections, credits, card business and others (Goldfinger ,2001).

Global banking figures from the Bank of International Settlements and the European Central Bank shows that the general payment tools used for the payment of day-to-day purchases include cash, checks, debit cards, and credit cards. In general, EPS can be classified into five categories (et al ,2003) which are listed below:

1. Electronic-cash: transactions are established by the interchange of electronic currency.

2. Pre-paid card: clients use a pre-paid card for a specified quantity through making an entry of the sole card number on merchant sites. The rate of the card is reduced via the volume paid to the merchant.

3. Credit cards: a server validates customers and confirms with the bank whether adequate resources are obtainable prior to procurement; charges are posted anti a customer's account; and the customer is payable later for the charges and fees the balance of the account to the bank.

4. Debit cards: a customer keeps a positive balance in the account, and cash is withdrawn from the account when a debit transaction is achieved.

5. Electronic checks: an organization electronically settles transactions among the buyer's bank and the seller's bank in the structure of an electronic check.

The main motivation for e-commerce and e-business is to offer a more effective service, primarily in terms of costs. Hence, paying online with traditional payment systems such as credit cards is rather inconsistent, agreed that credit cards are one of the maximum costly of all accessible mainstream payment means for together end consumers and merchants, overcome perhaps just via paper checks (Laudon &Traver,2004).

There are numerous limitations of traditional payment systems in the perspective of e-commerce can be defined. Current payment systems, such as credit cards, are inadequate for trade customer digital commerce from the following viewpoints as:

1-Lack of usability: Available payment systems for the Internet need from the client to present a vast amount of information, or create payments by complex developed web site interfaces. E.g. credit card payments by a web site are not the easiest way to pay, as these need entering broad amounts of personal data and contact features in a web form (Abrazhevich ,2004).

2-Lack of security: Existing payment systems for the Internet are an easy target for theft cash and personal information. Consumers have to present credit card or payment account features and other personal information online. This data is sometimes transmitted in an un-secured way. In practice this happens even in spite of introduction of secure transactions mechanisms, such as Secured Socket Layer. Providing these details by mail or over the telephone also entails security risks (Guttmann ,2003).

3-Lack of trust: Consumers tend not to trust offered systems with the long history of fraud, misuse or low reliability. In the present situation, money damage by customers is quite possible when using current payment systems, such as credit cards for Internet payments. Possible customers often mention this risk as the main reason why they do not trust a payment service and for that reason do not create Internet guidelines (McCloskey ,2006).

4- Lack of applicability: Particular web sites don't support a particular payment means, thus limiting customer's ability to pay. Credit cards work just with merchants who have signed-up to the services of the matching credit card company, and do not support direct business-to-business or interpersonal payments (Shih ,2004).

5-Lack of efficiency: Payments via the Internet can be too small to be handled by existing payment systems, because of expenditure included in the processing of payments and transaction. Credit cards are too expensive for effecting small payments and not appropriate for small transactions. The minimum fixed fee charged to the retailer for processing a transaction could even go beyond the value of the goods sold, (Guttmann ,2003).

Web Security

Web security define the ability of the web to maintain and keep the personal sensitive information from any changing, waste, disclosure, destruction or taken by unauthorized people such as Internet interlopers and hackers. Furthermore the web security system must prevent unauthorized users to use the computer system and control access to the network block from inside and outside the corporation (Hopwood ,2001) Security is the heart of E-Commerce and it has become the most significant issue for its advance (Jun & Punit, 2011)However the two most important areas avoiding the successful execution of E-Commerce globally are the Internet and E-Commerce communications security.

According to (Efraim ,2006) the security requirements of E-Commerce can be considered in a number of ways:

1- The authentication of the partner.

2- The confidentiality of the transactions data.

3- The integrity of the transactions data.

4- The reliability of the E-Commerce system.

According to (Chellappa & Pavlou, 2001) they stated that through the transactions by the Internet, E-commerce transactions must be considered secure just when all consumers' sensitive information reaches at its destination without any modification. Basically Internet transactions are dangerous because the Internet was initially given to the public for sharing information between each other and not for business aims. For that reason there were no security tools to support significant business transactions. Therefore without appropriate security mechanisms to control E-Commerce transactions, customer's sensitive information become susceptible to web risks such as hackers and Internet interlopers.

The Internet security emphases more on security characters such as, access control, authenticity, confidentiality, and data integrity. These characters also support to sustain the security during the transactions process; as a result these characters can aid to minimize Company's transactions security risks and contribute toward improving perceived web security of trading partners as well as the general customers. Furthermore there are particular basic

security requirements for E-Commerce security, which contains authentication, integrity, confidentiality, availability and privacy (Yam ,2011).

According to (Hsiao ,2003) they observed that firms are still worried about their information through transfer from one port to another via the Internet network. This is because the Internet security is still at the rising stage. so it is very significant to sustain the security reputation in the network and it is based on security perceptions between the transaction parties.

ELECTRONIC PAYMENT SYSTEMS (EPS)

The favourite e-payment service seems after e-commerce shaped (et al ,2010) E-Payment is defined as "the transfer of an electronic value of payment from a payer to a payee through an e-payment tool" (Weir, 2006). Prior researcher categorize the instruments used for e-payment as shown in Fig (1).

Figure 1. Categorization of electronic payment systems
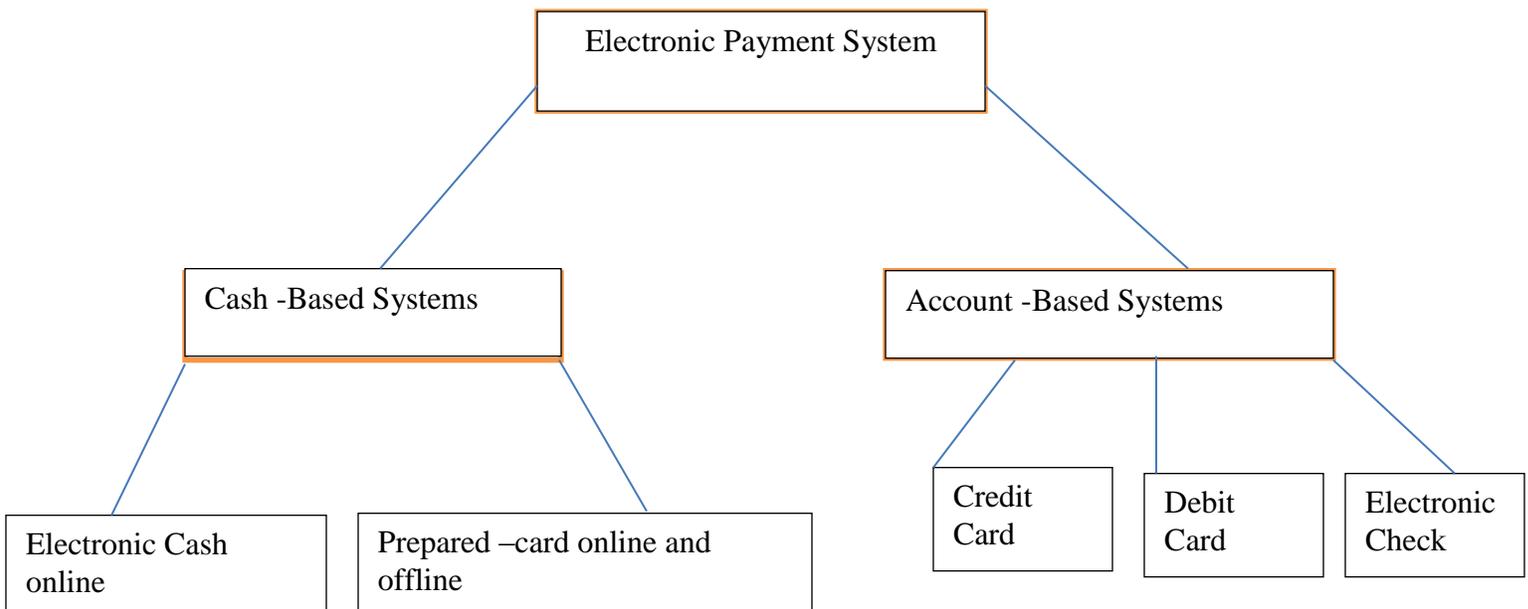
Kemp ,2013 defined E-money as "Broadly, e-money is defined subject to exclusions as financial value represented via claim on the issuer that is:

1- Electronically saved.

2- Issued on receipt of moneys for the purpose of creating payment transactions.

3- Accepted as payment via someone other than the issuer.

New mechanisms discussed by (Tsai ,2010) in deeply which called Web ATMs. By this new technology the payment of operation can gain and send right in numerous seconds. Additionally they argued that "With Web ATMs and Web 2.0, we now have a chance to make compensation.

Recent electronic financial services will be more flexible and modular, allowing capabilities to be added as and when needed on Web. Such secure payment services will not only spread their sales chances but also benefit to the whole economic advantages, cost-effective of banking trade. Most significantly, this does mean that there is a big break through on the advanced payment device of money flow of e-commence".

KEY INFERENCES AND SUGGESTIONS

(Ma'aitah and shtat, 2011) agreed that Significance of Authorization and Significance of encryption effect the perceived security of E-finance transactions; these characteristics can impact toward enhancing the perceptions of the users that the web and online transactions including E-Finance transaction are safe, and inspire them to use the online system and do financial transactions electronic.

Some Suggested steps by (Kennedy, 2011) that have to be taken via companies to keep personal information in the specific security dangers with in organizations. In determining suitable security measures, companies should:

1- Identify the security threats to the personal information that is being held.

2- Create policies and procedures to decrease those identified threats.

3- Utilise appropriate IT security settings governing system access.

4- Monitor and calculate performance anti related Australian and International criteria.

Tsiakis and Sthephanide (2005) argued the concept of security and trust in electronic payments. Though they discussed some of requirement and properties essential to construct positive automatic payment systems as listed follow:

1- Integrity: trust that information has not been altered after the data was sign up.

2- Authentication: The process via which one person proves that another entity is who they request to be.

3- Cheat avoidance and allowance: prevention of parties from cheat and from economic damages in the case the system damage or the network declines.

4- Privacy: information must not be exposed to not license people.

6- Transferability: expenditure of symbolic without the need to connection the issuer.

7- Payment anonymity: the payee will recognize only penname of the payer.

REFERENCES

A.Herbst, "E-finance Promises kept, promises unfulfilled, and implications for policy and research", Global Finance Journal, Vol.12, pp. 205– 215.

A.Michel, "The future of e-money: main trends and driving forces, the journal of futures studies", Strategic Thinking and Policy, Vol.03, No.5, 2001.p.429-451.

AL-ma'aitah, M. and Shatat, A. "Empirical Study in the Security of Electronic Payment Systems ", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No (2011).

B.Lietaer, "The Future of Payment Systems", 2002 Unisys Corporation.

C.Goldfinger and J. Perrin, "E-finance and small and medium enterprises (SMEs) in developing and transition economic", UNCTAD conference, Geneva, pp.45-78.

D. McCloskey, "The importance of ease of use, usefulness, and trust to online consumers: an examination of the technology acceptance model with older consumers", Journal of Organizational and End User Computing, Vol. 18 No. 3, 2006, pp. 47-65.

D.Abrazhevich, D, "Electronic Payment Systems: A User-Centered Perspective and Interaction Design", PHD thesis Technische Universiteit Eindhoven, Eindhoven, 2004.

E. Lawrence, Newton, S., Corbitt, B., Braithwaite, R. and Parker, C. Technology of Internet Business, Brisbane: John Wiley and Sons Australia Publishing 2003a.

F.Allen, J. McAndrews, and P.Strahan, P, "EFinance: An Introduction", Journal of Financial Services Research, Vol.22, No.2, 2002 , pp. 5-27.

F.Shamim, "The ICT environment, financial sector and economic growth: a cross-country analysis", Journal of Economic Studies, Vol. 34, No. 4, 2007, pp. 352-370.

G. Schneider, "Electronic Commerce", Thomson Course Technology, Canada, 2007.

H. Shih, "An empirical study on predicting user acceptance of e-shopping on the web", Information& Management, Vol.41, No. 3, 2004, pp. 351-68.

K.C. Laudon, and C.G.Traver, "E-commerce: Business, Technology, Society", London: Addison Wesley.

Kemp., R. "Mobile payments: Current and emerging regulatory and Contracting issues", computer law & security review Vol.2, No.9, (2013), pp: 175:179.

Kim., C., Tao., Wang , and Shin, N. "An empirical study of customers' perceptions of security and trust in e-payment systems", Electronic Commerce Research and Applications, Vol. 9, (2010), pp: 84–95.

L.B. Yam, W. Marco, L.L. DALE,"Consumers' perceptions of online ethics and its effects on satisfaction and loyalty", Journal of Research in Interactive Marketing Vol. 5 No. 1, 2011 pp. 71-89.

P.Ratnasingham, "Internet-based EDI trust and security", Information Management & Computer Security, Vol. 6 Issue 1, 1998, pp.33 – 39.

R.Guttmann, "Cybercash: the coming era of electronic money", Basingstoke: Palgrave, 2003.

R.K.Chellappa, and P.A. Pavlou, "Perceived information security, financial liability and consumer trust in electronic commerce transactions", Logistics Information Management, Vol.15, No.5, 2001, pp. 358-368.

R.L. Hsiao, "Technology fears: distrust and cultural persistence in electronic marketplace adoption" The Journal of Strategic Information System", Vol.12 No.3, 2003, pp. 169-199.

S. Manuchehr, 2008, "E-finance: status, innovations, resources and future challenges", Managerial Finance,Vol. 34 No. 6, 2008, pp. 365- 398.

S.Guan and F.A.Hua, "Multi-agent Architecture for Electronic Payment", International Journal of Information Technology and Decision Making, Vol.2, No.3, 2003, pp. 497–522.

S.Jun, and A.Punit, "The more secure the better? A study of information security readiness", Industrial Management & Data Systems, Vol.111 Issue: 4, 2011, pp.570-588.

T. Efraim, C.H. Michael and L.K.Jae, Electronic Commerce: A Managerial Perspective, Prentice Hall, 4th Ed, 2006.

Tsai., W, Huang. B, Tsaur. T, and Lin., S. "The application of Web ATMs in e-payment industry: A case study", Expert Systems with Applications, Vol.37, (2010), pp: 587–597.

Tsiakis, T., and Sthephanides, G. "The concept of security and trust in electronic payments", Computers & Security, Vol.24, pp: 10-15.

W. Samsudin and M. Khaled, 'The influence of perceived privacy on customer loyalty in mobile phone services: An Empirical Research in Jordan", IJCSI, Vol. 8, Issue 2, 2011, pp.45-52.

W. Tao, N. Shin, and K.S. Kim, "An Empirical Study of Customers' perceptions of security and trust in e-payment systems", Electronic Commerce Research and Applications, Vol.9, Issue 1, 2010, pp.84–95.

W.Hopwood, "Security in a Web-Based Environment, Managerial Finance", Vol.26, 2001, pp.42-52.

X.Dai and J.Grundy, "NetPay: an off-line, decentralized micro-payment system for thin-client applications" Electronic Commerce Research and Applications, Vol.6, 2007, pp.91–101.