Communications of the IIMA

Volume 12 | Issue 3 Article 4

2012

International Perceptions of Online Banking Security Concerns

Donald R. Moscato
Iona College

Shoshana Altschuller
Iona College

International Perceptions of Online Banking Security Concerns

Donald R. Moscato, Iona College, USA
dmoscato@iona.edu

Shoshana Altschuller, Iona College, USA
saltschuller@iona.edu

ABSTRACT

Concern about security is and always has been one of the major factors affecting the adoption of online banking. It is therefore essential for online banks to not only take proper security measures but to ensure that their customers and potential customers perceive their services as secure. This research highlights the significance of user perceptions of security by examining the content of the security policies of banks throughout the world. The security policy is illustrated as a tool for banks to use to manage their users' perceptions. The investigation also uncovers some notable differences among the expected security concerns within different regions. If banks understand their target audiences' e-commerce backgrounds, they can more effectively manage their potential users' perceptions of security.

Keywords: global banks, online banking, security policy, user perceptions, security concerns

INTRODUCTION

For nearly two decades the banking industry has been evolving in tandem with e-commerce capabilities. During this time, the ability to conduct business online has frequently been viewed as a strategic opportunity for banks, who could save transaction costs, expand their customer market, and improve customer service and cross-selling opportunities (Nath, Schrick, & Parzinger, 2001). In its short history, research activity in the field of Internet banking has directed much effort into understanding the phenomenon of consumer adoption of the new banking channel (Kolodinsky, Hogarth, & Hilgert, 2004; Tan & Teo, 2000; Xue, Hitt, & Chen, 2011). At a time when Internet connectivity was new and uncertain for many people, research findings aided banks in their quest for the best way to ease the market into a new medium for banking transactions. In addition to the expected technology acceptance variables (Lee, 2008) and the growing knowledge of what aspects make Web sites successful (Jarvenpaa & Todd, 1997), studies have, historically, overwhelmingly suggested that in banking in particular, trust of the banking medium and perceived security of the transactions play major roles in customers' decisions of whether or not to adopt Internet banking (Pavlou, 2003; Yousafzai, Pallister, & Foxall, 2009).

While information security practices are crucial to ensure continuity of any business, online banks have approached it with an additional focus. Due to the sensitive nature of their transactions and continuous media reports of security breaches of financial systems (including the recent events at Global Payments (Sidel & Johnson, 2012)), banks are aware that their users' *perception* of transaction security is of equal importance to the security measures themselves as it is a major factor in users' willingness to participate in online banking. To that end, a bank's online strategy ideally includes a full evaluation of its perceived trustworthiness in the eyes of its potential consumers (Yousafzai, Pallister, & Foxall, 2005). Logically, in order to help customers convert to online banking from traditional banking, the bank must actively manage the customers’ perception of the security of doing so.

Today, online banking has gained explosive popularity in the United States (American Bankers Association, 2010 & 2011) and other parts of the world (Anderson, 2010). Statistics reported indicate that the banking landscape has shifted and, for example, in the United States, online banking is practiced by the majority (Zickuhr & Smith, 2012), rapidly becoming the norm. Yet, interestingly, as the banking industry continues to increase its investment in now widely accepted online capabilities (BusinessWire, 2011), security doubts still remain at the forefront of research inquiries (Jain & Kohli, 2009) and banks continue to investigate users' perception of them (Hanzaee & Alinejad, 2012; Yousafzai et al., 2005). Furthermore, some banks are still trying to convince users to participate in online banking – at least in some parts of the world, such as India (Sharma, 2011). Although security is and always has been a major area of concern for online banking customers, the nature of those concerns is not widely discussed. (For exceptions see (Moscato & Moscato, 2004 & 2007)). Therefore, we cannot fully understand the connection between security concerns and banks’ attempts to alleviate them. Furthermore, it is not well understood if these concerns have been the same throughout the world and over the history of online banking.

One tool that online banks commonly use to manage their customers' perceptions of security is the "security policy". The security policy is an explicit description on the bank's Web site of the security measures taken by the bank to protect the personal information of its customers, such as encryption, firewalls, server authentication, and password protection. Inclusion of this statement serves the goal of assuring customers and making them aware of the security of their transactions and thereby enhancing perceptions of security (Yousafzai et al., 2005). Consequently, we expect that an online bank's security policy will portray its security measures in a light that addresses the customers' most likely fears. Thus, the security policy can be used as a proxy to gain insight into the bank's perception of its users' most likely security concerns.

The current study utilizes online banks' security policies to investigate how banks across the world perceive their local markets' security concerns. Research has shown that factors that contribute to users’ comfort with security features include level of education and users’ prior experience with the feature (Al Sukkar & Hasan, 2005; Kline, He, & Yaylacicegi, 2011). We therefore expect that given different experiences and knowledge levels across the world, banks will view security concerns differently internationally. Also, considering the varied stages of e-commerce development that exist across world markets (Moscato, Moscato, & Altschuller, 2012), we expect that online banks in different markets perceive different main concerns among their potential customers. While some reflect earlier stages of e-commerce development, others might be perceived as more mature markets. Insight into banks' perceptions of their local e-commerce markets could be an important factor in understanding how banks are and/or should be interacting with their target markets across the world.

METHODOLOGY

As part of a multi-year study by a university research team investigating the security and privacy policies of over a thousand companies engaged in e-commerce activities, the data for this paper was collected by one of the authors during the summer of 2011. It focused on online global banking and involved the review of 275 bank's e-commerce web sites. The areas investigated were as follows: United States (USA), Canada (CA), Mexico (MX), South America (SA), Europe, Australia, Africa, Japan and China. This cluster of global banks provided a representative group from the many regions of the world and allowed for a comparison of stated security policies followed by these banks.

A standardized reporting form was completed for each bank's web site visited. For this paper, data on nine security features were gathered and compared. Results for each feature were reported in tabular form in terms of the percentage of web sites that had the feature explicitly stated as part of the policy versus those that did not report the use of the stated security feature. The following features were used in the global comparison:

1. Was encryption used in the transmission of e-commerce data?
2. Was encryption used in the storage of banking data?
3. Was there any statement on the use of 128 bit encryption?
4. Did the site discuss the use network security or firewalls?
5. Was there a statement on logging, auditing or monitoring?
6. Did the site discuss multi-level sign on for e-commerce activity?
7. Was there a statement included on a glossary of terms?
8. Did the site discuss the use of a timeout feature?
9. Was there a statement on useful security hints?

RESULTS

Encryption During Transmission

Encryption technologies have been around for a very long time. Ingenious methods have been developed to implement the technology. The ultimate purpose is to render clear text data unrecognizable to a third party who has no authorization to read it. Therefore, clear text is converted into crypto text by means of formal algorithms that can be of varying degrees of complexity (Knudson, 2010).

By encrypting transmitted data you are strengthening the security of the data while it is being distributed over any variety of modalities (Kupfer, 2007). Virtually all e-commerce applications employ encrypted transmission using SSL (Secure Sockets Layer) technology (Cole, 2006). Improvements can enhance the transmission process. The DNS Security Extension (DNSSEC) specification enables the addition of encryption validation at the DNS layer (Davis, 2012). SSL also has its critics who contend that SSL has its own unique vulnerabilities (Rashid, 2011a). Table 1 illustrates consistent results of the regions across all classifications. Forty percent state that they use it while 60% make no statement of its use.

Country	Yes %	No %
United States	33	67
Canada, Mexico, South America	41	59
Europe, Australia	48	52
Africa, Japan, China	32	68
Total	**38%**	**62%**

Table 1: Encryption During Transmission.

Encryption in Storage

There is a debate raging regarding how extensive encryption technology should be deployed by organizations (Nelson & O'Conner, 2011). While many companies have implemented encryption in transmission, fewer have felt the need to implement the technology to stored data in company servers (Millard, 2009). The argument stems from the belief that data is at a greater risk while in transmission than it is in the confines of an organization safely nestled behind any firewalls that might be in operation.

The results in Table 2 demonstrate rather emphatically that banks discuss in their security policies their use of encryption for storing data far less than for its transmission. About 15% say they use it, whereas 85% do not mention making use of encryption for data storage. The results are very consistent across all regions studied. Perhaps, the reason is that banks have greater confidence in their internal IT systems than in third party communications providers. The data seem to overwhelmingly support this belief.

Country	Yes %	No %
United States	11	89
Canada, Mexico, South America	21	79
Europe, Australia	18	82
Africa, Japan, China	11	89
Total	**15%**	**85%**

Table 2: Encryption in Storage.

Statement on the Use of 128 Bit Encryption

Building on our earlier discussions of encryption, we measure with this question, the specific strength of the encryption method employed by banks in their online operations. Using a 128 bit encryption algorithm makes it significantly more difficult to break the code than it is with a 64 bit procedure. With the advent of quantum computers, even this encryption standard is being questioned (Wood, 2011). The obvious goal is to increase the cost and effort required for a prospective perpetrator to compromise a bank’s e-commerce initiative. By explicitly stating that a 128 bit encryption system is being deployed, the bank creates the impression of a more secure banking platform in the mind of the consumer.

Table 3 again shows a very consistent set of results among all of the regions with about 36% stating that they use 128 bit encryption and 64% not stating that it is employed. A spread of about 20% exists between the USA banks and those from Africa and Asia.

Country	Yes %	No %
United States	45	55
Canada, Mexico, South America	41	59
Europe, Australia	34	66
Africa, Japan, China	24	76
Total	**36%**	**64%**

Table 3: Statement on 128 Bit Encryption.

Use of Network Security or Firewalls

A firewall is an appliance used to enhance security by acting as a filter through which all network traffic must pass before it reaches a bank's server(s) that contains customer financial data. Any given firewall implementation can provide a wide range of screening capability that has its goal the acceptance of only valid, authorized customer transactions. In one of its more secure forms, it becomes the centerpiece of a VPN (Virtual Private Network). A bank will comment publically about its use of a firewall in order to raise customer confidence in the security of its e-commerce network (Kapner, 2012).

Table 4 presents results that show that there is a 20% difference between the behaviors of the representative banks. The overall percentage of yes responses was 43% for stating the existence of a firewall and 53% for not stating that it uses them.

Country	Yes %	No %
United States	52	48
Canada, Mexico, South America	55	45
Europe, Australia	34	66
Africa, Japan, China	27	73
Total	**43%**	**57%**

Table 4: Network Security or Firewall Statement.

Statement on Logging, Auditing, Monitoring

The results of Table 5 indicate that an overwhelming number of global banks across all categories do not state that they use these processes as part of their security disclosure policies. Twenty three percent of banks use them, while 77% do not explicitly state that they use them.

One can consider controls implemented on an e-commerce network to consist of both real time and after-the-fact approaches. A bank can monitor live the activity on its network and make any requisite real time changes it deems necessary to maintain its targeted level of security (Dolezalek, 2011; Vanhorn, 2007). These processes capture attacks as they occur possibly by deploying intrusion detection systems (IDS).

However, a bank can also perform periodic analyses of transactions and/or incident reporting logging systems (Strom, 2007). Using these methods, security analysts can investigate the data for patterns of attacks in order to prevent and/or deter the impact of future attempts to breach the security of their online banking application (Peterson, 2008). By stating explicitly on their web sites that one or more of these approaches are used, the bank can gain the confidence of their clients to use the online banking environment.

Country	Yes %	No %
United States	32	68
Canada, Mexico, South America	13	87
Europe, Australia	28	72
Africa, Japan, China	19	81
Total	**23%**	**77%**

Table 5: Statement on Logging, Auditing, Monitoring.

Multi-level Sign on for E-Commerce Activity

Passwords have been the staple of online identification and authentication for many years. Unfortunately, passwords have severe limitations if used alone (Rashid, 2011b; Traynor, 2012). A paramount concern for online banks is identity theft and its rapid rise across the e-commerce landscape (McMillan, 2011). Regulating authorities across countries have come to realize that a multi-layered sign on process adds to the ability of a bank to identify and authenticate who their valid customers are (Stephenson, 2012). The use of biometrics has also been proposed as part of the multi-factor approach (LaRoche, 2008). With the rapid rise of key loggers and skimmers, banks are using very creative methods to have their clients interact with their systems (Cohen, 2011; Hulme, 2011). FFIEC, in the United States as of 2005, mandates the use of multi-layered sign on techniques (Armstrong, 2011). It is now common to provide a customer with a user name, a password and a security question in order to gain access to a bank's online transaction system. Herein, lays the classic confrontation between enhanced security and ease of use. Most banks have recognized the need for this form of security and try to make it as least intrusive as is possible.

Table 6 presents the results for this security feature. The results come the closest to an even split across all geographic regions of global banks. 49% state that they use this approach while 51% do not. However, the U.S. banks along with those from Europe and Australia mention utilizing multi-factor sign-ons more than do banks from the other regions.

Country	Yes %	No %
United States	59	41
Canada, Mexico, South America	47	53
Europe, Australia	60	40
Africa, Japan, China	35	65
Total	**49%**	**51%**

Table 6: Multi-Level Sign-on for E-commerce.

Statement on a Glossary of Terms

Many computer security features are shrouded in technical jargon that can be very frustrating to potential customers of online banking. At the same time, there can be a subset of clients that can be very computer savvy. This latter segment prefers that banks communicate their security levels to interested customers so that they can make a more informed decision about selecting one bank over another one to do their online banking. This practice would enable a side by side comparison of security features being employed.

Several banks have discovered that by providing a glossary of terms as part of their web site both constituencies can be satisfied in their ability to evaluate and compare the security features of various web sites. A review of Table 7 illustrates that the vast number of banks have chosen not to include a glossary of terms for their customers. Only 22% of the global banks include a glossary whereas 78% do not. It is interesting to note that African, Japanese and Chinese banks used a glossary the least number of times.

Country	Yes %	No %
United States	23	77
Canada, Mexico, South America	32	68
Europe, Australia	28	72
Africa, Japan, China	8	92
Total	**22%**	**78%**

Table 7: Glossary of Terms Included.

Does the Site have a Timeout Feature?

When using any computer system, much more so in an e-commerce banking environment, there is always the possibility that a customer leaves the premises without engaging in a proper sign-off activity. This action results in an exposed system that can be co-opted by a predator. In order to protect both the bank's computer network as well as the customer, after a specified period of no keyboard activity, the application will forcibly terminate. Clearly, most banks have this protective feature in operation but far more choose not to disclose it to their clientele.

The results are illustrated in Table 8 and, at best, are mixed. Overall, 42% of the global banks use and disclose a timeout feature while 58% do not. The results are fairly consistent across all of the banking regions.

Country	Yes %	No %
United States	37	63
Canada, Mexico, South America	59	41
Europe, Australia	36	64
Africa, Japan, China	33	67
Total	**42%**	**58%**

Table 8: Timeout Feature on Web Site.

Is There a Statement on Useful Security Hints?

As the technology underpinning computer crime has increased, there has been a commensurate need for more security countermeasures. For the typical online banking customer, he/she might not have the expertise to operate successfully in an online e-commerce banking environment. Some banks have opted to explain how the customer can navigate the online banking application with a higher level of confidence that good security practice is being followed. For example, some topics might include guidelines for the following: frequency of changing passwords, the robustness of certain password choices, recognizing the presence of key loggers and/or skimmers, etc.

Table 9 depicts the results that show that 60% of global banks do include a statement containing useful security hints while 40% do not. Interestingly, the African and Asian banks have results that show the converse while all of the other regions are more consistent with the overall totals.

Country	Yes %	No %
United States	71	29
Canada, Mexico, South America	75	25
Europe, Australia	66	36
Africa, Japan, China	32	68
Total	**60%**	**40%**

Table 9: Statement on Useful Security Hints.

DISCUSSION AND CONLUSIONS

Examining the results presented, we can make a number of observations about banks' portrayal of their online services to their customers. Firstly, analysis of the results regarding encryption in Tables 1 and 2 indicates that banks in fact seem to be concerned with users' *perception* of security as a key element of their trust. Across the board, banks are found to be more vocal in their security policies about their transmission encryption than about their storage encryption. Transmission is the part of the transaction that the user experiences and takes part in. Storage happens behind the scenes in the purview of the bank and out of the sight of the customer. Seemingly, banks would like to draw users' attention to the things that they can actually see during the transaction, bolstering the perception that security exists. This seems to be a main goal in portraying an online bank's security policy. This finding is consistent with previous research that has indicated that Web users are influenced more by the security measures that are apparent during the transactions (such as a lock icon in the browser) than by those that are not visible (such as a digital certificate) (Kline et al., 2011). While users' level of concern about security is very high, their level of technical knowledge does not necessarily match. Therefore, peer evaluation, reputation, and visual cues indicating security (such as the "hacker-tested badge" icon) are most effective in producing the users' perception that the Web-based transaction is indeed safe (Kline et al., 2011; Post & Walchli, 2010). This finding is further supported in our dataset by examining the overall levels of the other security features. For example, multi-level sign-on is a security feature that is by definition interactive and obvious to the user. Not surprisingly, it is mentioned by nearly half of the security policies overall - comparatively, one of the most prominent of all the features studied. Additionally, multi-level sign-on is one of the most widely addressed concerns within each region.

If perception of security is a key focus and the security policy is an indication of how banks address and manage those perceptions, then it makes sense that the security policies will differ from bank to bank. The security policy represents a bank's deliberate appeal to the perceptions of bank users rather than only an objective description of security measures. Each bank, in including features in its security policy, makes a judgment about its users and potential users. Since the users are different worldwide, security policies will reflect banks' expectations of the users in a particular part of the world. This is evident in the above data analysis as well. By comparing the frequency of the features in security policies by region, we observe that banks are portraying a very different security profile in different parts of the world. 128-bit encryption and logging and monitoring, for example, are being highlighted by banks in the United States more than anywhere else in the world. At the same time, glossaries and security hints are mentioned significantly less in Africa, Japan, and China than in any of the other regions. Clearly, as banks manage their users' perceptions of security, the characteristics of the regions' e-commerce environment dictate in part how a bank will communicate its security efforts to the public.

Differences that have been studied among e-commerce users have included experience, education, culture and language (Al Sukkar & Hasan, 2005; Kline et al., 2011; Miyazaki & Fernandez, 2001), all contributing to unique "e-commerce cultures" (Moscato et al., 2012). In addition, e-commerce markets have been described based on their stage of development ranging from underdeveloped (such as Africa) to hyper-developed (such as Europe) (Moscato et al., 2012). Differences among security features profiled in security policies around the world could be a result of banks' perceptions of the different e-commerce cultures within which they are operating. Examining the security features that are addressed in different world regions can lend support to this proposition and reveal insight into how banks relate to their various markets. For example, the security profile that we've observed portrayed in the United States might reflect a more sophisticated e-commerce market where users' perceptions extend beyond just seeing that encryption is being used. They would like to see signs of proactive control on the part of the banks where they are using the strongest encryption, they are actively monitoring activity, and ensuring authentication. It is possible that in the United States more banking customers understand and perhaps have experienced security breaches and need to have the perception that security measures are in place to prevent them. In addition, perhaps the banking customers in Africa, Japan, and/or China, with their shorter e-commerce history and leaner experience, are less proactive about their security than in other parts of the world. They might be less likely to be looking to take part in the process of ensuring security by obtaining definitions and security hints. Rather, their perceptions might be more suitably informed by mention of the existence of standard security measures.

Despite perceived differences among e-commerce regions, security is a concern for all users of online banking. The current analysis also lends insight into the types of concerns that are being addressed in various markets. By examining the most seemingly important security features within each region we can illustrate what types of concerns are being addressed at different stages in e-commerce development. For example, the most frequently mentioned security feature in each of the regions except for the one that includes Africa is security hints. This might be an indication that in many of these areas, e-commerce experience and security awareness has developed to such an extent that users are becoming actively involved in assuring their own security. In a similar vein, in the United States and Europe, the next most important feature is multi-level sign-on whereas in Canada, Mexico, and South America the more prominent concern seems to be about a timeout feature. In both cases, banks suspect that their users are worried about fraud but in the United States and Europe perhaps users are advanced enough to be trusted to take their security into their own hands and not leave a session without signing out.

It is interesting to note that in Europe and Australia, transmission encryption is the third most prominent of all the features with 48% of banks mentioning it. In Africa, Japan and China this feature is also the third most prominent compared to all the other features in the same region. In the United States and Canada/Mexico/South America, there is a moderate percentage of mentions of this feature. Europe and Africa are at opposite extremes in terms of e-commerce. A recent Forrester research report indicates that Western Europeans are the most advanced in terms of online banking adoption (Anderson, 2010) while Africa has been known to lag due to lack of infrastructure support (Mensah, Bahta, & Mhlanga, 2005). Surprisingly, concern over transmission security is prominent in both. Perhaps this can be explained again by the level of e-commerce development. While Africa is largely at the beginning of its e-commerce journey and still needing to be convinced of online security during financial transactions, Europe is perhaps at a point where they are embracing mobile technology and renewing their concerns for transmission security in this new medium.

Looking at a cumulative percentage of security features mentioned, the United States, the Americas, and Europe/Australia range from 352-384% whereas in China, Japan, and Africa these features were only cumulatively 221%. In future research it would behoove us to examine what other security features are being addressed in these markets other than the ones under examination here. In addition, future such examinations should open up the regional categories and inspect each of the markets individually in attempt to learn more about what security perceptions are occurring in each of the regions individually.

In summary, this investigation of security policies has shed light on the prominence of security perceptions in a bank's formation of its online image. It further indicates that the security policy is a tool that banks can and do use to manage the perceptions of their security. Examination of the security policies in different regions has shown how banks might be tailoring their security communications based on their perceptions of their target markets, perhaps in terms of their culture, history, or levels of development and awareness. While the specific conclusions drawn about the different regions are not empirically tested here, this analysis highlights that by understanding the needs of a customer base in order to feel secure, a bank can highlight the security features that will help their customers perceive their services as secure.

REFERENCES

Al Sukkar, A., & Hasan, H. (2005). Toward a model for the acceptance of internet banking in developing countries. *Information Technology for Development, 11,* 381-398. doi: 10.1002/itdj.20026

American Bankers Association. (2010). *ABA survey shows more consumers prefer online banking*. Retrieved from http://www.aba.com/Press/Pages/093010PreferredBankingMethod.aspx

American Bankers Association. (2011). *ABA survey: Popularity of online banking explodes*. http://www.aba.com/Press/Pages/090811ConsumerPreferencesSurvey.aspx

Anderson, J. (with Reitsma, R., Ensor, B., & Sorensen, E.). (2010). *How global consumers are adopting online banking.* Cambridge, MA: Forrester Research.

Armstrong, I. (2011, December). Paying dividends: Financial services roundtable. *SC Magazine,* 30-31.

BusinessWire. (2011). *Novarica research finds banks investing in online capabilities, profiles online banking providers* [Electronic Version]. Retrieved from http://www.businesswire.com/news/home/20110728005501/en/Novarica-Research-Finds-Banks-Investing-Online-Capabilities

Cohen, S. (2011, November 23). Task force cracks down on ATM ‘skimmers” in Westchester; 5 arrested, more sought. *Journal News,* p. 9A.

Cole, E. (2006). Transit safety. *Information Security,* 9(4), 56-59.

Davis, M. (2012, February 12). Data encryption: Piling on. *InformationWeek.com,* 27-32. Retrieved from http://reports.informationweek.com/abstract/15/8647/risk-management/data-encryption-piling-on.html

Dolezalek, H. (2011, July 29). Monitoring user activity Keep your data secure & your network humming along safely. *Processor.com,* p. 23. Retrieved from http://www.processor.com/articles//P3315/28p15/28p15.pdf?guid=

Hanzaee, K. H., & Alinejad, S. (2012). An investigation about customers perceptions of security and trust in e-payment systems among Iranian online consumers. *Journal of Basic and Applied Scientific Research, 2,* 1575-1581. Retrieved from http://www.textroad.com/pdf/JBASR/J.%20Basic.%20Appl.%20Sci.%20Res.,%202(2)1575-1581,%202012.pdf

Hulme, G. V. (2011). Drone fleet keylogger infection: How’d it happen? *CSOonline,* 9-10.

Jain, V., & Kohli, S. (2009). Exploring the security of e-banking systems: Questions of theft, fraud, jurisdiction and the shifting sands of time. *International Journal of Electronic Finance*, *3*(4), 339-352.

Jarvenpaa, S. L., & Todd, P. A. (1997). Consumer reactions to electronic shopping on the world wide web. *International Journal of Electronic Commerce, 1*(2), 59-88.

Kapner, S. (2012, January 10). Banks unite to battle online theft. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB1000142405297020343690457715123059891 9896.html

Kline, D. M., He, L., & Yaylacicegi, U. (2011). User perceptions of security technologies. *International Journal of Information Security and Privacy, 5*(2), 1-12. doi: 10.4018/jisp.2011040101

Knudson, J. (2010, December 17). The latest security developments: End-to-end protection & cloud security are among the trends that are picking up stream. *Processor.com, 32*(26), p. 13. Retrieved from http://www.processor.com/editorial/article.asp?article=articles%2Fp3226%2F22p26%2F22p26.asp

Kolodinsky, J. M., Hogarth, J. M., & Hilgert, M. A. (2004). The adoption of electronic banking technologies by US consumers. *International Journal of Bank Marketing, 22*(4), 238-259.

Kupfer, S. (2007). Connect to an encrypted wireless network. *PCToday, October*, 72-73.

LaRoche, G. (2008, March). Fingering transactional strong authentication. *Security*. Retrieved from http://www.securitymagazine.com/articles/fingering-transactional-strong-authentication-1

Lee, M. -C. (2008). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, *8*(3), 130-141. doi:10.1016/j.elerap.2008.11.006

McMillan, R. (2011). Cops Arrest 11, Break up 5 ID theft Rings in One Swoop. *CSOonline,* p. 15.

Mensah, A. O., Bahta, A., & Mhlanga, S. (2005). *E-commerce challenges in Africa: Issues , constraints, opportunities*. Paper presented at the World Summit on the Information Society, Tunis. Retrieved from http://www.uneca.org/aisi/docs/PolicyBriefs/E-commerce%20challenges%20in%20Africa.pdf

Millard, E. (2009, March 13). Full-disk encryption: The use of FDE is growing—is it right. *Processor.com,31*(10), p. 35. Retrieved from http://www.processor.com/editorial/article.asp?article=articles/P3110/34p10/34p10/34p10.asp

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *The Journal of Consumer Affairs, 35*(1), 27-44. doi: 10.1111/j.1745-6606.2001.tb00101.x

Moscato, E. D., Moscato, D. R., & Altschuller, S. S. (2012). *A longitudinal comparison of global banks' security policies.* Paper presented at the Academic Business World International Conference, Nashville, TN.

Moscato, D., & Moscato, E. (2004). An assessment of privacy and security policies of U. S., European, Asian and Latin American banks. *Proceedings of the Third International Business and Economy Conference*. Retrieved from http://userwww.sfsu.edu/ibec/papers/48.pdf

Moscato, D., & Moscato, E. (2007). Pursuing trust in an internet banking environment: The U.S. experience. *Proceedings of the 2007 International Business and Economy Conference*.

Nath, R., Schrick, P., & Parzinger, M. (2001). Bankers' perspectives on internet banking. *e-Service Journal, 1*(1), 21-36. doi: 10.1353/esj.2001.0004

Nelson, T., & O'Conner, M. (2011). Self-encrypting drives and other mobile security options Don’t leave home or the office without them. *PCToday, April, 9*(4), 39-41.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Peterson, C. (2008, March 24). Unlock the value of logs. *Network World,25*(12), p. 22.

Post, G. V., & Walchli, S. B. (2010). Consumer perception of web site security attributes. *Journal of Information Privacy & Security, 6*(4), 3-27.

Rashid, F. Y. (2011a, April 18). Comodo attack highlights issues in SSL certificate security. *eWeek,* p. 31.

Rashid, F. Y. (2011b, June 20). Password security remains the weakest link even after big data breaches. *eWeek*, pp. 38-39.

Sharma, H. (2011). Bankers' perspectives on e-banking. *National Journal of Research in Management, 1*(1), 71-85. Retrieved from http://www.publishingindia.com/uploads/samplearticles/njrim-sample-article.pdf

Sidel, R., & Johnson, A. R. (2012, March 30). Data breach sparks worry: Hack attack at card processor compromises potentially thousands of accounts. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB20001424052702303816504577313411294908868.html

Stephenson, P. (2012, January 3). Multifactor authentication. *SC Magazine,* 38-39.

Strom, D. (2007, October). Log wild. *Information Security*, 45-49.

Tan, M., & Teo, T. S. H. (2000). Factors influencing the adoption of Internet banking. *Journal of the Association for Information Systems*, *1*(1), 5.

Traynor, S. (2012, February). The evolution of authentication. *SCOonline*, 32.

Vanhorn, T. (2007, October 2). Activity monitoring and database security. *Network World,* 26.

Wood, L. (2011, March 21). The clock is ticking for encryption: Today's secure cipher-text may be tomorrow's open book. *ComputerWorld,* 32-36.

Xue, M., Hitt, L. M., & Chen, P. -Y. (2011). Determinants and outcomes of internet banking adoption. *Manage. Science., 57*, 291-307. Retrieved from http://mansci.journal.informs.org/content/57/2/291.full.pdf

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2005). Strategies for building and communicating trust in electronic banking: A field experiment. *Psychology and Marketing, 22*(2), 181-201.

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2009). Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal*, *29*(5), 591-605. Retrieved from http://carbsdrupal.hosting.cf.ac.uk/sites/default/files/Multidimensional_role_of_trust_ in_Internet_banking_adoption.pdf

Zickuhr, K., & Smith, A. (2012). *Digital differences*: Pew Research Center.