PRIVATNOST I SIGURNOST U ELEKTRONIČKOM POSLOVANJU

PRIVACY AND SECURITY IN E-COMMERCE

UDK 658.8:004.738.5
Pregledni rad
Review

Milan Mandić, M. A. Art Design and Internet technologies
Creative Director
Exit Centar
Vojvode Momčila 16, 78000 Banja Luka, BOSNIA AND HERZEGOVINA
Phone: ++387 66 165 486
E-mail: mail@milanmandic.com

Ključne riječi:
elektroničko poslovanje, e-sigurnost, e-privatnost, e-povjerenje

Keywords:
electronic commerce, e-security, e-privacy, e-trust

SAŽETAK

Glavna je prepreka za elektroničko poslovanje nepovjerenje kupaca prema internetu. Ono proizlazi iz činjenice da su zabrinuti kako se koriste njihovi osobni podaci, ali i zbog rizika od izlaganja prijevari na internetu. Ovaj rad analizira neke od najvažnijih aspekata povjerenja u e-poslovanju, osobito pitanje sigurnosti i privatnosti. Uz sav potencijal koji e-poslovanje pruža svim sudionicima u ovom procesu, u interesu je poduzeća da steknu povjerenje svojih potrošača. Analizirani su i neki od najčešćih oblika kriminala na internetu, a date su i upute kako steći povjerenje u internetskom okruženju.

ABSTRACT

Consumer distrust and concerns, mainly in regards to the protection of their private information and risk of being exposed to online frauds, have been the main obstacles in online commerce. This paper analyzes some of the most significant aspects of trust in e-commerce, with a focus on online security and privacy issues. With all the potential that e-commerce provides to both companies and consumers, it is in the interest of the company to increase trust among its online users. Some of the most common online crimes are analyzed and practical guidelines to achieving trust in the online environment are provided.

1. INTRODUCTION

A number of industries nowadays recognize the Internet as one of the most important communication tools and, perhaps, the most significant technological development. Computers have had an enormous impact on communications and its potential for business growth has certainly been widely recognized.

Numerous companies have, at the very least, a website to enhance the company's brand though many have recognized the potential the Internet provides that goes beyond just having a website. The Internet can help a company establish and build better relationships with its customers to the benefit of both the company and its clients. The customers are offered an improved service while companies can achieve better targeting in their marketing communications campaigns by gathering more precise information through a vast range of applications, such as data warehousing and data mining.[1]

Electronic commerce (e-commerce) is the second most widely used retail channel and the number of individuals who purchase goods online keeps rising.[2] Even though this sounds very promising, one must take into consideration that there are many different estimations about the growth of e-commerce, some not very optimistic, due to a different use of methodology and definitions.[3] However, there is no doubt that this is an important area for research.

E-commerce is a concept that goes beyond just buying online – "it is a holistic strategy of redefining dated business models, with the aid of technology, in order to gain benefits for the consumer and a maximum profit".[4] This definition implies two significant aspects of e-commerce: firstly, the importance of a strategic focus, since just using the Internet will not in itself provide the company with a competitive advantage, but only when companies use the available technology strategically. This view has clearly been demonstrated by the number of online companies which went bankrupt at the end of 1990s. Secondly, e-commerce should benefit both the company and its customers, equally. Consequently, when applied correctly, e-commerce has the potential to provide convenient means of communications, more interactivity and a more cost-effective way of presenting information,[5] which leads to loyalty towards a company and improved profitability in the long term.

Along with all the opportunities come challenges as well. In case of e-commerce, one of the challenges has been in finding a successful business model to follow, as the expectations of e-commerce failed to materialize as dramatically as it was hoped for in the beginning.[6] While it is important to research potentially successful online business models, this paper will focus on another issue that is highly related to the Internet: the concerns and challenges regarding customers, mainly the question of security and privacy in the online environment.

2. PUBLIC CONCERNS REGARDING E-COMMERCE

Technology, alongside all the potential and promises for a business, also has a negative aspect. Technological innovations, as potentially positive as they might be, also provide ways of gathering consumer data without detection and there is a risk that absolutely anyone from anywhere might be able to intercept such data from a user.[7]

Public concerns regarding e-commerce have emerged from a vast range of potential threats present on the Internet. Due to its nature, the Internet is very different from a traditional "off-line" environment. The most prominent of these differences is the lack of a person to communicate to, face-to-face.[8] In regards to the purchase of products, one does not have a chance to assess goods as one would in a store,[9] or even worse, purchased goods might not be delivered as promised or delivered at all. These problems only get worse if an individual is dealing with a foreign company without a head office in the country from which goods are purchased, or if there are no offices in the first place.[10]

It must be noted that the publicity about various online crimes has led to more of a concern that might be justified. Fear has increased in particularly when publicity involved better-known companies.[11] Even though the risks involving e-commerce might at times be perceived more strongly than they are in reality, it still must be acknowledged that they truly are out there, and they must be communicated to the public and prevented whenever possible.

In addition to numerous issues that might arise from the fact that the Internet as a medium is different from other, more traditional, retail channels, there are problems that are naturally only associated with this particular medium.

2.1. Fraud

Online fraud occurs through deception or through data interception[12] and takes many forms on the Internet. We have already mentioned the common frauds of non-delivered goods, which is often related to the issue of non-existent companies, as it is rather simple to make a website posing as a company. Companies lacking in moral standards might charge for the services which they have advertised as free or hide costs (such as delivery costs). Such issues might never be resolved for some individuals as official bodies, assigned to these problems, may lack the resources to deal with every encountered matter.[13]

The more frightening examples of fraud include credit card frauds and identity theft, but as scary as these are, it must again be highlighted that these issues are not as common as it is often thought[14] and are most often dealt with in a timely and efficient manner. Of course, whoever has encountered these problems might not care about statistics but might only emphasize the point that security and privacy must be a responsibility of any e-retailer. To add to the problem, it is well-known to the public that the malicious use of user information is not always a result of fraudulent online crime but of companies that gather data in order to refer or sell it to third parties.

2.2. Malicious software

Online criminals use a variety of tools to commit online fraud. These are constantly changing as various forms of protection are being developed, and some security experts find this fact very alarming. To give an example, in 2000, 81% of the detected malware were viruses, which accounted for only 1% six years later.[15] It would be almost impossible to review all the techniques used by online criminals but we will briefly explore perhaps the most common one: „Trojan horses". Trojan horse is, according to the Texas State Library and Archives Commission, „An apparently useful and innocent program containing an additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data."[16]

The characteristics of „Trojan horses" are that they are not visible, have a variety of ways of stealing data and do not require any action by the user in order to be launched. A banking „Trojan horse", for instance, will remain inactive until the user tries to log in on the banking website and it will then steal data by either capturing keystrokes or copying the filled out page.[17]

A more frightening example of a fraudulent technique is the HTML injection. It modifies the HTML code before the user is presented with the page. The main issue here is that this threat does not break the protection measures of a website because it manipulates with the code of the page and not with security (which is separate from the HTML code). This way the URL (Uniform Resource Locator) does not change and the user is not being redirected to another page, giving the attacker opportunity to obtain data.[18]

Two Swiss Ph.D. students conducted an interesting study and discovered a way of recognizing the typed keystrokes remotely. Every keyboard key sends out a specific electromagnetic wave, regardless of the type of the keyboard (wireless or not). The students explored this property on twelve different keyboards and discovered that they were vulnerable to at least one of the four different ways the keystrokes can be recognized. The distance at which they captured the

signals reached up to twenty meters and it was possible to recognize the keystrokes even with a physical barrier present, such as a wall between the keyboard and the keystroke recognizer.[19]

3. E-TRUST

Angriawan and Thakur (2008) define online trust as "when a consumer has confidence in an e-merchant's reliability and integrity to perform online transactions successfully."[20]

Having established the many potential threats present in the online business environment, it is clear that the lack of trust perceived with e-commerce may be the largest obstacle to companies. Though consumers are sometimes dissatisfied with some of the characteristics of the Internet as a medium (the lack of a physical store, for instance), the main issues regard that associated with a lack of trust in the online security and privacy.[21]

Though general skepticism towards companies might appear off-line as well, this feeling may only be enhanced when there is a lack of trust cues, such as personal communication and a concrete feeling of actually seeing the product purchased.[22] Because of these features that are absent in an online environment, trust becomes a fundamental aspect of online commerce.[23] Some industries, such as the banking industry, are especially vulnerable to this fact, as the service itself is one which requires a trusting relationship. Giving away one's funds is always a sensitive activity, which becomes even more so when this activity is done electronically. This requires the user not only to give their trust to the company in question but also to the technology itself. The complication of this, as we will explore later on, lies in the fact that trust, inherently, is a feeling that is usually cultivated by interpersonal relations,[24] and hence, for companies doing business online it is even more difficult to gain this reaction from customers.

The importance of trust in general is widely acknowledged, thought of as a foundation of commerce[25] and it is a highly significant concept in the creation of relationships with consumers. In marketing communications literature, it is at the core of the relationship marketing theory, which highlights the importance of customer retention. Given the vast competition taking place especially on the Internet, retaining clients may only be achieved through trust, reinforcing the feeling of safety with regard to each of the transactions taking place.[26]

Most of the empirical research has shown that lack of trust will discourage customers from making a purchase online,[27] though there have been contradictory results in this area as well. Ribbink et al.[28] did not find that e-trust had a crucial role in e-commerce but, nevertheless, discovered that it did have a significant effect on loyalty. The link between e-trust and loyalty has been supported by later studies as well.[29]

It should clearly be acknowledged that e-trust is an important factor in relation to e-commerce, in spite of some differences in opinion regarding its effects. The concept of trust has been widely researched through many different disciplines, such as psychology, sociology and marketing communications. From this, diverse theories and dilemmas have emerged, all focusing on different aspects depending on the area of research. Trust as a concept is complex and what makes it even more complicated is that, to date, not enough empirical data has been presented to give us complete answers to the question of how to achieve this trust. Trust in relation to the online environment is even more under-researched.[30]

The research that has been conducted has instead pointed to many factors that might be influencers of e-trust: honesty, benevolence,[31] integrity, trustworthiness, competence, openness,[32] perceived good reputation of the company as well as personal trust disposition, familiarity with online purchasing[33] and usability,[34] including elements such as design quality, easy navigation etc.

Many of these concepts are interrelated themselves and, again, the question of how to achieve these in the context of the Internet remains unclear. There are,

however, two factors that seem to be the main features leading to consumer distrust: the issue of security and privacy, a point we will review more closely shortly.

Based on the literature, any definition of e-trust should highlight the aspects of trust in both the company and the Internet as a medium;[35] as well as the degree of consumer confidence in the company's potential to reduce the uncertainty[36] regarding the cues that users associate with a safe relationship on the Internet, leaving users reasonably secure about the good intentions of the company and the measures it is taking to provide a protected and pleasant experience to them.

3.1. Main factors of distrust – security and privacy

Despite the fact that the literature on e-trust has proposed numerous possible influencers of e-trust, we have mentioned the fact that security and privacy are the two factors mostly associated with customer distrust.[37] As we have established previously, these are also the features that are most likely to be associated with all concrete online threats, such as online fraud. Also, many of the other factors, such as perceived honesty and trustworthiness, have their grounds in these concepts.

Industry surveys constantly demonstrate that distrust of a website's security and privacy is significant in customer purchase behavior. In 2004, TRUSTe and Taylor Nelson Sofres found that 69 percent of online shoppers from the United States would limit their purchases due to concerns about online privacy.[38] European Commission also found that only 23 percent of European online users truly trusted the Internet as a purchasing medium, security being stated by 48 percent as the main concern.[39]

Empirical data supports these views as well. Angriawan and Thakur[40] found strong correlations between e-trust and the issue of security and privacy. Online users are increasingly insecure about the treatment of their data on the Internet.[41] They become cautious about websites asking for personal information due to fears about this information being misused.[42] Online security, or a perceived lack of it, has been found to be one of the primary reasons why online users are not engaging in e-commerce.[43]

Given these results, e-trust could be achieved by applying both secured online technology and appreciation of customer privacy.[44] If this trust is achieved, customers are much more likely to engage in e-commerce and establish a relationship with a company.[45] If customers can trust the company in terms of privacy, they will not only be more willing to make a purchase but will also reveal truthful information about themselves, as the only kind of information that will be useful for a company in order to achieve its goal of more targeted marketing communications efforts.

4. PRIVACY

As with the concept of trust, privacy has grounds in various disciplines, such as philosophy, anthropology, politics and law.[46] Broadly speaking, privacy is the protection of personal information. In e-commerce especially, it is related to a company's policies on the use of user data[47] – to put it simply, what the intentions of this use are or whether the customer can restrict the use of personal information.

An important factor of privacy is the consumer consent – whether the consumer is given a choice to decide what the information can and can not be used for.[48] Usually, when the proper security systems are in place, the user will not mind sharing the information necessary for a transaction to take place (needless to say, some information about the user is simply required in e-commerce, such as a delivery address, card details and name and customers are aware of this). But the consent will relate to whether this information can be further exploited.

Companies have different views on the management of user data. There is an increasing number of companies which recognize the importance of privacy and

will provide the users with the choice in deciding what the company can do with the information, and will in addition provide an opt-out clause. On the other hand, some firms feel that the information users have shared now belong to them and feel no moral obligation not to make a profit by using such data.[49] These companies usually fall into the category of those that will utilize the user data without asking for permission or, more discreetly, the ones that will ask for data but will not give an opt-out option.[50] As mentioned at the beginning of this paper, companies do benefit from the possibilities of gathering data about their customers, and restricting them in doing so might reduce the profit sought from the Internet as a medium as well as the potential to provide customers with a better service due to increased knowledge about them. Also, in order to offer an efficient payment system to customers, companies sometimes need to use the data already given by those same customers. For instance, Amazon makes the brand experience a more pleasant one as the user does not always need to re-enter all the information and, thus, goes through the purchase more easily and quickly. It is therefore not argued that companies should in every way be restricted from collecting user data but, rather, that they should address the issue of security and privacy of their online business. Companies should take into consideration the fact that consumer trust is far more profitable in the long term and breaching this trust will have a more negative impact on loyalty and repeat purchase. Accordingly, even if a company does not recognize its ethical and moral duties, but focuses solely on its potential for improved profitability, the solution is still the same: to address the concerns customers have regarding privacy and e-commerce.

4.1. Techniques for establishing e-privacy

The most common means of providing users with privacy information are privacy statements. In this way companies inform the website users what their policy is regarding data protection, and provide the information about who is collecting data and what it will be used for.[51]

However, any Internet-savvy user will know that these privacy policies are often long documents, written in small fonts and are full of legal and technical terminology. Surveys have shown that even when companies had privacy statements, they were often difficult to read and seemed to be written for the companies' benefit – to protect them against litigation rather that to protect customer data.[52] Companies face another dilemma here – if they do provide their consumers with more choice regarding the use of personal information, the customers are more likely to restrict its use; on the other hand, by failing to provide this choice, they will run an increased risk of consumer distrust, which might even undermine purchase behavior. Again, the importance of e-trust should be highlighted here and research has shown that a stronger privacy policy leads to a higher perceived trustworthiness of a company,[53] which should in turn benefit the company more in the long run than the possibility of passing on information to affiliate companies.

Another way of increasing trust in online privacy of a website is to use privacy seal verifications. These trust-marks are usually links to the organizations that work towards a safer online environment by establishing whether a website follows an accredited privacy policy. If the website is verified by these companies, the user will be more comfortable with providing personal information.[54] These seals might not be sufficient enough to provide the consumer with a trusting attitude towards the company but will reduce some of the uncertainty with regard to a website's credibility and reinforce trust.[55] There are several categories of seals, such as reliability, vulnerability, security and privacy seals[56] – the one relevant to this section is the privacy seal, which shows that a company respects personal information and that this fact is monitored on a regular basis.

4.2. Contradictory feelings about privacy

It would be useless to discuss online privacy issues without raising the question that many companies might ask themselves: if people are so concerned

about privacy, why are they sharing their information on almost any website they encounter? This would be a valid question. Researches themselves have highlighted the fact that one needs to distinguish between privacy concerns and privacy practices: individuals tend to rate their privacy concerns higher than they might seem to when viewing their online behavior.[57]

When we refer to the issues of online privacy, it often seems that people are reluctant to provide any of their private information at any given time. But this is certainty not the case – we need only to consider the phenomenon of Facebook to see that Internet users are often more than happy to give out personal data even when it is not required by the host website. This is so too when we sign up for newsletters and similar promotional opportunities – it is simply the case of sometimes actually being happy to exchange some data in order to receive something we wish to obtain. Online users do this on a daily basis, despite their deep concerns about privacy issues.

One of the reasons for this could be that online users are essentially aware of the fact that there is always a risk of data being violated due to not only privacy protection but security issues as well.[58] Both the company and the user understand that there is never a full guarantee of safety online but as much as the consumer understands this, if and once their privacy has been violated, they will turn to the company with their complaint.

5. SECURITY

Before going further into details about online security, a note must be added about the perceived similarity between the concepts of security and privacy. People inevitably tend to group these concepts together. This is an important note for the context of this paper, as online users seem to be more familiar with security technologies and thus, tend to perceive these as more important in an online framework.[59] Although they are interrelated, there are clear distinctions between the two concepts: While privacy is linked to legal requirements and good practices regarding the management of personal data, security refers to the technical aspects of this management and protection.[60] Protecting user data from online fraud can not be achieved without proper security. Nevertheless, consumers, companies and even official legislative bodies often view these concepts as very similar, and some authors have therefore proposed that they are two dimensions of a construct called SHPD: security in the handling of private data.[61] Customers, however they view these concepts, will usually care mostly about their data being protected, whether this is done by security measures or a company's policies.

Security, as we have seen, relates to the ability of a company to protect its consumers online and prevent online fraud through security measures. Security involves both managerial and technical measures: the organizations' limitations of who can access the data within the organization and the purpose of this access. The technical measures include elements, such as encryption in the handling of the data, data storage on secure servers and the use of passwords.[62] Security is achieved if the information reaches the person without data being observed, altered or destroyed.[63] In more detail, this means that the transmitted or stored data can not be modified by third parties without permission; data can only be seen by authorized individuals; and certain actions can only be undertaken if proper authentication has taken place.[64]

As with privacy, online users are usually aware of the fact that a company can never fully guarantee security. Non-expert users will not fully comprehend the scope of the technological measures on a website but will react to the perceived strength of a website's security.[65] The perceived security refers to the consumer belief that their personal data, including financial details, will not be abused. Though there are still many threats online, the technologies of e-security have advanced to the level where security breaches have been reduced.[66]

5.1. Techniques for establishing e-security

There are many different methods of e-security, such as statements about data protection and firewalls (protection) as well as familiar and verifiable domain names (verification). Encryption, usually marked by an unbroken lock or key,[67] refers to the encryption of the content and protects sensitive data when it is transmitted through open channels. Encryption scrambles the information with a numeric key that is added to the computer code and can only be read by the user with the key to unscramble the document. Any unauthorized person without the key can only see an unreadable document.[68]

Digital certificates from trusted third parties, as is the case with privacy, validate the probable credibility of the website. These certificates confirm whether the company is taking measures to secure their users or not; for instance, whether they have SSL (Secure Socket Layer) protection.[69]

One of the principal methods of e-security includes the techniques involving user identification.[70] The authentication usually follows two steps: providing a login or user ID; and then proving authenticity by providing a password. This two-step process is inherently a somewhat weak option,[71] as the authentication is performed only at the one end – the user's computer – which is vulnerable to attacks, such as the "Trojan horses" mentioned above. Concern over the insufficient security of this process have been raised by official bodies, such as the Federal Financial Institutions Examination Council,[72] which urge industries, especially the banking industry, to adopt improved authentication methods. These methods might be fraud detection, the capacity to recover transactions in a fast way,[73] smart-card technologies,[74] one-time passwords or USB plug-ins[75] etc. Numerous companies and banks have adopted these new practices but there are still some instances of the two-way authentication process in e-commerce.

6. GUIDELINES FOR COMPANIES

It is not just consumers who are concerned about online security and privacy. Companies which respect these issues, or at least recognize the financial gains in addressing these problems, are faced with a problem of how to gain consumer trust online. As the relevant literature has shown, despite widespread concerns, there are not so many solutions to these problems. Sometimes, the solutions are apparent (such as giving a choice to users of how their data may be used) but are in direct conflict with the company's objectives (for instance, to gather information for marketing communications purposes). Nevertheless, analysis of the empirical data and industry studies has clearly demonstrated the importance of taking these issues in consideration when dealing with online commerce. As perceived security and privacy might be the most significant factors in influencing e-trust, there are several steps a company might take in order to address these influencers.

A considerable amount of online fraud may be prevented by the users themselves, and consumers should take more responsibility for their online security and information privacy.[76] This is the fact that the companies committed to online security and privacy can and should educate their users about. Not only would it actually prevent online fraud but would also reduce user uncertainty about the company's reputation and credibility while increasing trust as well.

In addition to the already mentioned techniques for establishing e-privacy and e-security, each company should include a privacy statement, which clearly states its security and privacy policies. TRUSTe, whose seal demonstrates a company's compliance with privacy best practices, recommends that a comprehensive privacy statement should include the aspects, such as: notice (the use of collected information) and choice (provide users with a choice or whether the information may be collected and used); access (provide users with access to their own information).[77] Internally, organizations should restrict employees' access to sensi-

tive data, unless it is absolutely necessary in doing their job. As regards security, the content should include a description of how the registration process works; how the website uses cookies and contact information.[78] Providing company's contact information and photographs of the employees and physical premises[79] will enhance the initial trust, especially with less known companies. Being given the chance to visit or speak directly to employees will reduce the anxiety the users associate with the remote nature of the Internet.

Providing more information on products and services, following usability guidelines, should also greatly influence e-trust.[80] The company should make sure that consumers understand that it will never send e-mails asking for personal financial information, and should also discourage them from opening links from an e-mail in order to prevent phishing-frauds. When a company requires user authentication, it should include more that the simple two-way process of user ID and password whenever possible. If online fraud does occur, the company should deal with the matter as efficiently and quickly as possible to prevent further loss in terms of reputation damage.

7. CONCLUSION

The growth of Internet technologies has provided various business opportunities with a potential to benefit both companies and consumers. However, e-commerce has not been as successful as expected, due to a number of problems that consumers encounter in the online environment. Security and privacy, or more specifically lack thereof, are both rooted in the issue of trust. These are the issues companies must address in their strategic plans and with their online presence. E-commerce is undoubtedly widespread in the world; therefore, the significance of studies on this topic is huge. Moreover, as technology changing constantly, this subject is always highly topical and research should keep up with any changes as well. This is particularly important for developing countries, where technology is more or less just being introduced. Further research should focus on security of the systems operating in these countries, since the main objective of businesses operating in them should be to get people to use the Internet. The importance of e-privacy must not be neglected; however, the trust in security is the first step in achieving a higher percentage of online users.

Even though all participants in e-commerce recognize that there is no full guarantee of online safety, companies are still in a position to increase trust among their online consumers and should do so in order to achieve the full potential of e-commerce.

LITERATURE

1. Acohido, B.: Hackers barrage bank accounts, **USA Today**, 2009, [Online] Available on: http://www.usatoday.com/money/industries/banking/2009-02-22-bank-accounts-hackers_N.htm (29.05.2009.)
2. Angriawan, A., Thakur, R.: A Parsimonious Model of the Antecedents and Consequence of Online Trust: An Uncertainty Perspective, **Journal of Internet Commerce**, Vol. 7, No. 1, 2008, pp. 74-94.
3. Arcand, M., Nantel, J., Arles-Dufour, M., Vincent, A.: The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust, **Online Information Review**, Vol. 31, No. 5, 2007, pp. 135-161.
4. Benamati, M., Serva, J.: Trust and distrust in online banking: Their role in developing countries, **Information Technology for Development**, Vol. 13, No. 2, 2007, pp. 161-175.

5. Chen, Y., Barnes, S.: Initial trust and online buyer behaviour, **Industrial Management & Data Systems**, Vol. 107, No. 1, 2007, pp. 21-36.
6. Durkan, P., Durkin, M., Gillen, J.: Exploring efforts to engender on-line trust, **International Journal of Entrepreneurial Behaviour & Research**, Vol. 9. No. 3, 2003, pp. 93-110.
7. European Commission, Commission Staff Working Document: Report on cross-border e-commerce in the EU, 2009, Available on: http://ec.europa.eu/consumers/strategy/docs/com_staff_wp2009_en.pdf (2.6.2009.)
8. Flavián, C., Guinalíu, M.: Consumer trust, perceived security and privacy policy, Three basic elements of loyalty to a web site, **Industrial Management & Data Systems**, Vol. 106, No. 5, 2006, pp. 601-620.
9. Fraumeni, B.M.: E-Commerce: Measurement and Measurement Issues, **The American Economic Review**, Vol. 91, No. 2, 2001, pp. 318-322.
10. Hooper, T., Vos, M.: Establishing business integrity in an online environment: An examination of New Zealand web site privacy notices, **Online Information Review**, Vol. 33, No. 2, 2009, pp. 343-361.
11. Hsu, C.J.: Privacy concerns, privacy practices and web site categories: Toward a situational paradigm, **Online Information Review**, Vol. 30, No. 5, 2006, pp. 569-586.
12. Jaikumar, V.: Security Concerns Cloud Online Shopping, **Computerworld**, Vol. 39, No. 49, 2005, pp. 8.
13. Kalakota, R., Robinson, M.: **E-poslovanje 2.0**, MATE, Zagreb, 2001.
14. Kolsaker, A., Payne, C.: Engendering trust in e-commerce: a study of gender-based concerns, **Marketing Intelligence & Planning**, Vol. 20, No. 4, 2002, pp. 206-214.
15. Martins, N.: A model for managing trust, **International Journal of Manpower**, Vol. 23, No. 8, 2002, pp. 754-769.
16. McRobb, S., Rogerson, S.: Are they really listening?: An investigation into published online privacy policies at the beginning of the third millennium, **Information Technology & People**, Vol. 17, No. 4, 2004, pp. 442-461.
17. Mohatar, O.D., Sierra Cámara, J.M.: New Directions in Online Fraud. **AIP Conference Proceedings**, Vol. 963, No. 2, 2007, pp. 973-976.
18. Nielsen, J.: Trust or Bust: Communicating Trustworthiness in Web Design, 1999, Available on: http://www.useit.com/alertbox/990307.html (20.06.2009.).
19. Pennanen, K., Tiainen, T., Luomala, H.T.: A qualitative exploration of a consumer's value-based e-trust building process: A framework development, **Qualitative Market Research: An International Journal**, Vol. 110, No. 1, 2007, pp. 28-47.
20. Ramnath, K., Chellappa, P., Pavlou, A.: Perceived information security, financial liability and consumer trust in electronic commerce transactions, **Logistics Information Management**, Vol. 15, No. 5/6, 2002, pp. 358-368.
21. Regnier, P., Sahadi, J.: Thwart the ID Thieves, **Money**, Vol. 35, No. 12, 2006, pp. 124-125.
22. Ribbink, D., van Riel, A.C.R., Liljander, V., Streukens, S.: Comfort your online customer: quality, trust and loyalty on the Internet, **Managing Service Quality**, Vol. 14, No. 6, 2004, pp. 446-456.
23. Roberts, P.F.: FFIEC report pans passwords, **eWeek**, Vol. 22, No. 42, 2005, pp. 19.
24. Roca, J.C., Garcia, J.J., de la Vega, J.J.: The importance of perceived trust, security and privacy in online trading systems, **Information Management & Computer Security**, Vol. 17, No. 2, 2009, pp. 96-113.
25. Shalhoub, Z.K.: Trust, privacy, and security in electronic business: the case of the GCC countries, **Information Management & Computer Security**, Vol. 14, No. 3, 2006, pp. 270-283.
26. Smith, A.D.: Cybercriminal impacts on online business and consumer confidence, **Online Information Review**, Vol. 28, No. 3, 2004, 224-234.

27. Thakur, R., Summey, J.H.: E-trust: empirical insights into influential antecedents, **Marketing Management Journal**, Vol. 17, No. 2, 2007, pp. 67-80.
28. Thomas, L., Xiaodong, D.: Building online trust through privacy practices, **International Journal of Information Security**, Vol. 6, No. 5, 2007, pp. 323-331.
29. TRUSTe, Online Privacy - A Tutorial for Parents and Teachers, Available on: http://www.truste.org/pdf/parent_teacher_tutorial.pdf (2.06.2009.)
30. Udo, G.: Privacy and security concerns as major barriers for e-commerce: a survey study, **Information Management & Computer Security**, Vol. 9, No. 4, 2001, pp. 165-174.
31. Wirtz, J., Lwin, M.O., Williams, J.D.: Causes and consequences of consumer online privacy concern, **International Journal of Service Industry Management**, Vol. 18, No. 4, 2007, pp. 326-348.

References

[1] Wirtz, J., Lwin, M.O., Williams, J.D.: Causes and consequences of consumer online privacy concern, **International Journal of Service Industry Management**, Vol. 18, No. 4, 2007, pp. 327.
[2] European Commission, Commission Staff Working Document: Report on cross-border e-commerce in the EU, 2009, Available on: http://ec.europa.eu/consumers/strategy/docs/com_staff_wp2009_en.pdf (2.6.2009.)
[3] Fraumeni, B.M.: E-Commerce: Measurement and Measurement Issues, **The American Economic Review**, Vol. 91, No. 2, 2001, pp. 318.
[4] Kalakota, R., Robinson, M.: **E-poslovanje 2.0**, MATE, Zagreb, 2001, pp. 5.
[5] Kolsaker, A., Payne, C.: Engendering trust in e-commerce: a study of gender-based concerns, **Marketing Intelligence & Planning**, Vol. 20, No. 4, 2002, pp. 206-214.
[6] Pennanen, K., Tiainen, T., Luomala, H.T.: A qualitative exploration of a consumer's value-based e-trust building process: A framework development, **Qualitative Market Research: An International Journal**, Vol. 110, No. 1, 2007, pp. 28.
[7] Arcand, M., Nantel, J., Arles-Dufour, M., Vincent, A.: The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust, **Online Information Review**, Vol. 31, No. 5, 2007, pp. 136.
[8] Ramnath, K., Chellappa, P., Pavlou, A.: Perceived information security, financial liability and consumer trust in electronic commerce transactions, **Logistics Information Management**, Vol. 15, No. 5/6, 2002, pp. 358.
[9] Flavián, C., Guinalíu, M.: Consumer trust, perceived security and privacy policy, Three basic elements of loyalty to a web site, **Industrial Management & Data Systems**, Vol. 106, No. 5, 2006, pp. 603.
[10] Ibid.
[11] Durkan, P., Durkin, M., Gillen, J.: Exploring efforts to engender on-line trust, **International Journal of Entrepreneurial Behaviour & Research**, Vol. 9. No. 3, 2003, pp. 98.
[12] McRobb, S., Rogerson, S.: Are they really listening?: An investigation into published online privacy policies at the beginning of the third millennium, **Information Technology & People**, Vol. 17, No. 4, 2004, pp. 443.
[13] Flavián, C., Guinalíu, M.: op. cit., pp. 612.
[14] Regnier, P., Sahadi, J.: Thwart the ID Thieves, **Money**, Vol. 35, No. 12, 2006, pp. 124-125.
[15] Mohatar, O.D., Sierra Cámara, J.M.: New Directions in Online Fraud, **AIP Conference Proceedings**, Vol. 963, No. 2, 2007, pp. 973.

[16] Texas State Library and Archives Commission Web Site, 2009, Available on: http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html (13.10.2009.)

[17] Acohido, B.: Hackers barrage bank accounts, **USA Today**, 2009, [Online] Available on: http://www.usatoday.com/money/industries/banking/2009-02-22-bank-accounts-hackers_N.htm (29.5.2009.)

[18] Mohatar, O.D., Sierra Cámara, J.M.: op. cit., pp. 974.

[19] Vuagnoux, M., Pasini, S.: Compromising Electromagnetic Emanations Of Wired And Wireless Keyboards, 2009 - Available on http://lasecwww.epfl.ch/keyboard/ (13.10.2009.)

[20] Angriawan, A., Thakur, R.: A Parsimonious Model of the Antecedents and Consequence of Online Trust: An Uncertainty Perspective, **Journal of Internet Commerce**, Vol. 7, No. 1, 2008, pp. 76.

[21] Durkan, P., Durkin, M., Gillen, J.: op. cit., pp. 93-110.

[22] Thakur, R., Summey, J.H.: E-trust: empirical insights into influential antecedents, **Marketing Management Journal**, Vol. 17, No. 2, 2007, pp. 74.

[23] Kolsaker, A., Payne, C.: op. cit., pp. 208.

[24] Benamati, M., Serva, J.: Trust and distrust in online banking: Their role in developing countries, **Information Technology for Development**, Vol. 13, No. 2, 2007, pp. 164.

[25] Arcand, M., Nantel, J., Arles-Dufour, M., Vincent, A.: op. cit., pp. 138.

[26] Angriawan, A., Thakur, R.: op. cit., pp. 74-94.

[27] Roca, J.C., Garcia, J.J., de la Vega, J.J.: The importance of perceived trust, security and privacy in online trading systems, **Information Management & Computer Security**, Vol. 17, No. 2, 2009, pp. 96-113.

[28] Ribbink, D., van Riel, A.C.R., Liljander, V., Streukens, S.: Comfort your online customer: quality, trust and loyalty on the internet, **Managing Service Quality**, Vol. 14, No. 6, 2004, pp. 446-456.

[29] Flavián, C., Guinalíu, M.: op. cit., pp. 601-620.

[30] Thakur, R., Summey, J.H.: op. cit., pp. 67-80.; Pennanen, K., Tiainen, T., Luomala, H.T.: op. cit., pp. 28-47.

[31] Flavián, C., Guinalíu, M.: op. cit., pp. 601-620.

[32] Martins, N.: A model for managing trust, **International Journal of Manpower**, Vol. 23, No. 8, 2002, pp. 754-769.

[33] Chen, Y., Barnes, S.: Initial trust and online buyer behaviour, **Industrial Management & Data Systems**, Vol. 107, No. 1, 2007, pp. 21-36.

[34] Nielsen, J.: Trust or Bust: Communicating Trustworthiness in Web Design, 1999 - Available on: http://www.useit.com/alertbox/990307.html (20.06.2009.)

[35] Ribbink, D., van Riel, A.C.R., Liljander, V., Streukens, S.: op. cit., pp. 448.

[36] Shalhoub, Z.K.: Trust, privacy, and security in electronic business: the case of the GCC countries, **Information Management & Computer Security**, Vol. 14, No. 3, 2006, pp. 270.

[37] Flavián, C., Guinalíu, M.: op. cit., pp. 601-620.; Chen, Y., Barnes, S.: op. cit., pp. 21-36.

[38] Jaikumar, V.: Security Concerns Cloud Online Shopping, **Computerworld**, Vol. 39, No. 49, 2005, pp. 8.

[39] European Commission, Issues relating to Business and Consumer E-commerce, 2004 - cited in: Flavián, C., Guinalíu, M.: op. cit., pp. 605.

[40] Angriawan, A., Thakur, R.: op. cit., pp. 74-94.

[41] Pennanen, K., Tiainen, T., Luomala, H.T.: op. cit., pp. 28-47.

[42] Roca, J.C., Garcia, J.J., de la Vega, J.J.: op. cit., pp. 96-113.

[43] Udo, G.: Privacy and security concerns as major barriers for e-commerce: a survey study, **Information Management & Computer Security**, Vol. 9, No. 4, 2001, pp. 165-174.

[44] Thomas, L., Xiaodong, D.: Building online trust through privacy practices, **International Journal of Information Security**, Vol. 6, No. 5, 2007, pp. 323-331.

[45] Udo, G.: op. cit., pp. 165-174.

[46] Hsu, C.J.: Privacy concerns, privacy practices and web site categories: Toward a situational paradigm, **Online Information Review**, Vol. 30, No. 5, 2006, pp. 570.

[47] Angriawan, A., Thakur, R.: op. cit., pp. 79.

[48] Shalhoub, Z.K.: op. cit., pp. 271.

[49] Thomas, L., Xiaodong, D.: Building online trust through privacy practices, **International Journal of Information Security**, Vol. 6, No. 5, 2007, pp. 323.

[50] Kolsaker, A., Payne, C.: op. cit., pp. 209.

[51] Ramnath, K., Chellappa, P., Pavlou, A.: op. cit., pp. 361.

[52] Hooper, T., Vos, M.: Establishing business integrity in an online environment: An examination of New Zealand web site privacy notices, **Online Information Review**, Vol. 33, No. 2, 2009, pp. 355.

[53] Thomas, L., Xiaodong, D.: op. cit., pp. 323-331.

[54] Durkan, P., Durkin, M., Gillen, J.: op. cit., pp. 99.

[55] Kolsaker, A., Payne, C.: op. cit., pp. 208.

[56] TRUSTe, Online Privacy - A Tutorial for Parents and Teachers - Available on: http://www.truste.org/pdf/parent_teacher_tutorial.pdf (2.6.2009.)

[57] Hsu, C.J.: op. cit., pp. 572.

[58] Thakur, R., Summey, J.H.: op. cit., pp. 76.

[59] Roca, J.C., Garcia, J.J., de la Vega, J.J.: op. cit., pp. 107.

[60] Flavián, C., Guinalíu, M.: op. cit., pp. 604.

[61] Ibid., pp. 605.

[62] Shalhoub, Z.K.: op. cit., pp. 272.

[63] Ramnath, K., Chellappa, P., Pavlou, A.: op. cit., pp. 359.

[64] Flavián, C., Guinalíu, M.: op. cit., pp. 604.

[65] Arcand, M., Nantel, J., Arles-Dufour, M., Vincent, A.: op. cit., pp. 152.

[66] Ibid., pp. 135.

[67] Ramnath, K., Chellappa, P., Pavlou, A.: op. cit., pp. 361.

[68] Smith, A.D.: Cybercriminal impacts on online business and consumer confidence, **Online Information Review**, Vol. 28, No. 3, 2004, pp. 230.

[69] TRUSTe, op. cit.

[70] Smith, A.D.: op. cit., pp. 230.

[71] Mohatar, O.D., Sierra Cámara, J.M.: op. cit., pp. 976.

[72] Roberts, P.F.: FFIEC report pans passwords, **eWeek**, Vol. 22, No. 42, 2005, pp. 19.

[73] Mohatar, O.D., Sierra Cámara, J.M.: op. cit., pp. 976.

[74] Smith, A.D.: op. cit., pp. 231.

[75] Roberts, P.F.: op. cit., pp. 19.

[76] Hsu, C.J.: op. cit., pp. 584.

[77] TRUSTe, op. cit.

[78] Ibid.

[79] Durkan, P., Durkin, M., Gillen, J.: op. cit., pp. 106.

[80] Thakur, R., Summey, J.H.: op. cit., pp. 74.