E-commerce and the Media – Influences on Security Risk Perceptions

Pita Jarupunphol[1],Chris J. Mitchell
Information Security Group, Royal Holloway, University of London, London, England
P.Jarupunphol@rhul.ac.uk, C.Mitchell@rhul.ac.uk

Abstract: Security is clearly a very important factor governing the size of the e-commerce market. E-commerce security concerns include payment confidentiality, payment integrity, and payment authorisation for Internet transactions. Currently, many potential e-commerce participants are reluctant to participate in Internet e-commerce because of these concerns, not least because many users perceive Internet shopping as the riskiest shopping method by comparison with other methods of payment. In this paper we consider the influence of the mass media, including television and newspapers, on e-commerce consumer perceptions. Given that cases of security breaches are often sensationalised by these media, we observe that the mass media may actually be unduly increasing e-consumer concerns, and thereby adversely affecting the e-commerce marketplace.

Key words: Credit card fraud, e-commerce end-users, actual risk, risk perception, security breaches, risk perception gap.

1. INTRODUCTION

The emergence of e-commerce provides consumers with an alternative method of payment via the Internet. According to Whiteley [15], e-commerce reduces both the complexity and the time spent in traditional shopping methods. For example, there is no need for consumers to go to retail premises in order to purchase goods. This non face-to-face shopping method permits fraudsters to exploit the lack of any inbuilt authentication in

[1] Pita Jarupunphol was sponsored by the Rajabhat Institute of Phuket

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35616-7_23

W. Cellary et al. (eds.), *Internet Technologies, Applications and Societal Impact*

the Internet to perform illegal operations, such as use of credit card numbers without the consent of the valid cardholder [7]. This threat deters consumers from purchasing goods online by credit card and also reduces the commercial potential of e-commerce, since the credit card is the most popular method of payment for e-consumers (see Treese and Stewart [14], and Survey.Net[2]).

According to Miyazaki and Fernandez [10, p.27], 'Many involved in online retailing assume that time alone will dissolve consumer concerns regarding the privacy and security of online shopping, yet others argue that greater Internet experience and more widespread publicity of the potential risks of online shopping will lead to increased risk perceptions'. Thus, the fact that breaches of Internet security are reported with great frequency means that there is a danger that potential users will remain reluctant to engage in e-commerce because of fears about security. This means that user trust is a key enabler for the growth of the e-commerce market. This is supported by Friedman et al. [6], who argue that lack of financial and security confidence are reducing consumer acceptance of this innovative online shopping technology.

The relationships in e-commerce transactions can be categorised into business to business (B2B), business to consumer (B2C), consumer to consumer (C2C), and public/private sectors to government [8]; we focus on B2C transactions in this paper.

2. CURRENT ISSUES IN E-COMMERCE

Consumer perceptions of e-commerce security appear to be very negative [9]. Many Internet users are currently unwilling to participate in Internet shopping because of fears about the compromise of their financial information when submitted to e-commerce web sites.

Where the true levels of risk are unclear to users, e.g. in the context of non face-to-face shopping, recommendations from other members of a social system, such as friends, relatives, and neighbours, have an important effect on consumer participation [11]. This is supported by Roger [12, p.5], who argues that information about an innovation 'is communicated through certain channels over time among the members of a social system'.

Prior to their adoption of Internet e-commerce, consumers may learn of its advantages and disadvantages via social interactions, e.g. with friends or relatives. Reports on television, newspapers and other mass media arguably play a very important role in user adoption of e-commerce, since this is

[2] Survey.Net (http://www.survey.net)

likely to be the prime source of information regarding security breaches for the majority of domestic users. As argued by Rosenbloom [13], how the media interprets a social experience influences individual trust.

In the e-commerce context, how the broadcaster interprets a social experience can be either beneficial or damaging to the adoption of e-commerce given that consumer understanding of, and trust in, e-commerce is very fragile. Some aspects of particular criticality to consumer perceptions of e-commerce are as follows (see also Figure 1).

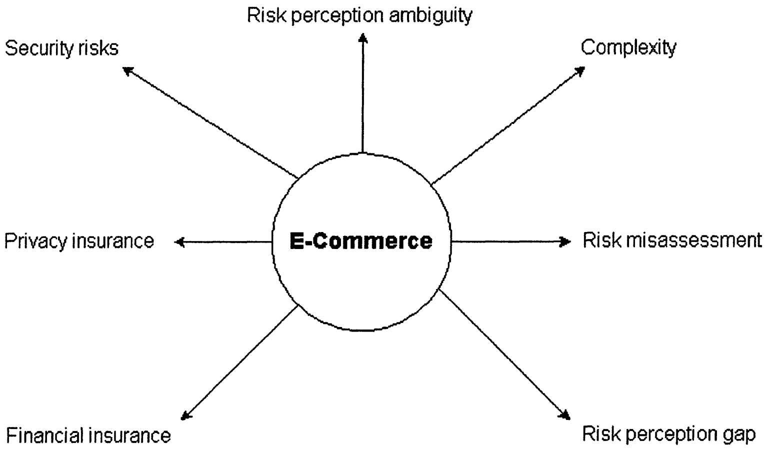

Figure 1. Current issues in e-commerce

- E-commerce complexity—consumers need to perform several different procedures in order to participate in e-commerce.
- Financial insurance requirements—consumers need contractual or legal protection to ensure that they will not lose financially.
- Privacy insurance requirements — consumers need contractual or legal protection to ensure that the confidentiality of their personal information will be protected.
- E-commerce security risks — consumers perceive e-commerce as the riskiest shopping method.
- E-commerce risk misassessment — consumers perceive data transmission as the most vulnerable aspect of an e-commerce

transaction although in fact many, if not most, security breaches occur at merchant web sites.

- E-commerce risk perception ambiguity—consumer risk perceptions are still ambiguous, since it is difficult to find out what aspects of credit card fraud in e-commerce are of most concern to consumers.
- E-commerce risk perception gap—consumers are particularly concerned about online credit card fraud, whereas many studies indicate that the risks are no greater than for conventional credit card use.

We now examine these issues in more detail.

2.1 The complexity of e-commerce

For inexperienced e-commerce consumers, shopping over the Internet can present problems, as several categories of information are presented via a typical e-commerce website. In addition, there are a number of stages involved in completing a transaction, from searching and selecting products to the receipt of an order confirmation from the merchant.

A variety of payment methods may be accepted by e-commerce merchants (e.g. debit/credit card, cheque, money transfer, etc.) [8], and consumers may be confused over which payment methods are most reliable for ensuring the secrecy and integrity of their order and payment information. In fact, payment by credit card is arguably the most appropriate method for e-commerce consumers, because of the speed of transaction clearance and the fraud insurance offered by credit card companies.

2.2 Requirements for financial protection

According to Friedman et al. [6, p.38], 'Insurance refers to social arrangements in which there is a promise to compensate individuals for future harm if it occurs'. Bhatnagar et al. [1] claim that e-commerce consumers require contractual protection or insurance to ensure that their financial information will not be used fraudulently by an unauthorised party when participating in e-commerce.

Currently, many consumers are very concerned about online credit card fraud, even though they are covered by their credit card issuers who will reimburse them for the value of any disputed or fraudulent transactions conducted over the Internet [3]. In fact, in some legal jurisdictions, e.g. England and Wales, credit card companies are legally obliged to reimburse credit account card holders in the event of fraud. However, despite this level of protection against fraud, e-consumers are in many cases still reluctant to participate in e-commerce.

2.3 Requirements for privacy protection

If consumer personal information is misused, e.g. if it is sold by merchants or other parties involved in a transaction, consumers may have difficulty in establishing who is responsible. Merchants can always deny having sold consumer personal information. On the other hand, if merchant fault in such cases is always assumed, then the merchant may be reluctant to engage in e-commerce transactions because of the risk of unfairly being given the blame for compromises of consumer information.

2.4 The security risks of e-commerce

Many consumers perceive e-commerce as the riskiest method of payment by credit card in comparison with other shopping methods, such as shopping in the High Street and telephone shopping [5], [9]. However, as argued in [9], in practice the reverse is true. E-commerce transaction messages are typically protected using SSL or TLS, making the probability of successful interception very small. Also, as long as merchants protect their e-commerce servers, the risk of credit card number compromise at any point in the e-commerce transaction path is probably rather small.

By contrast, in a high street transaction the retailer has access to a user's credit card for a short period of time, and therefore has the opportunity to copy all the information on the card. Moreover, the retailer will also have a copy of the transaction details, as needed for clearing and settlement, which again will contain most of the information on the card. Similarly, in a telephone transaction the retailer has access to a user's credit card number because this information must be passed to the retailer over the telephone in order to complete the transaction.

Apart from credit card fraud risks arising from data transmission and data storage, the fraud risk from fraudulent merchants is also an issue of concern to potential e-commerce participants, since it is often difficult for the consumer to differentiate between a legal e-commerce web site and a web site created for fraudulent purposes. A fraudulent merchant can create a seemingly secure web site by providing convincing contents. In addition, the merchant can also set up a secure link to the consumer, e.g. using SSL, to further convince the consumer of the security of the web site. By this means, consumer financial information may be stolen by the fraudster.

2.5 Incorrectness of consumer risk perceptions

Currently, many consumers not only have a negative attitude to Internet shopping, but also wrongly perceive that the compromise of credit card numbers is most likely to occur during data transmission. However, most cases of compromised credit card information are due to weaknesses at merchant web servers [13]. This is supported by Caldwell [2], who states that the compromise of sensitive information in e-commerce in not likely during transmission, but is much more likely to occur through insufficient protection of merchant web servers.

Of course, if SSL/TLS is used, then the communications channel will be protected, and hence the risks during data transmission will be effectively minimised.

2.6 Ambiguity of consumer risk perceptions

As has already been mentioned, numerous consumers are concerned about e-commerce credit card fraud. This concern, however, has a variety of different causes. For example, consumers may worry about credit card fraud because the credit card clearing procedure is allegedly insecure or they may be concerned because they simply do not exactly know what happens when the credit card number is cleared.

2.7 The risk perception gap

From eMarketer[3] of November 2000 we learn that Visa and MasterCard report overall rates of credit card fraudulent transactions of 0.08% and 0.09% respectively. As far as e-commerce credit card transactions are concerned, eMarketer from January 2001 reports that of 60,320,000 online B2C transactions in 1999, only 18,600 (i.e. 0.03%) were fraudulent. These credit card fraud rates are consistent with a survey of credit card fraud among Internet users in the UK conducted by MORI[4], in which 3% of Internet users claimed to have experienced fraudulent online transactions, whereas 5% of them had experienced credit card fraud in conventional transactions. This means that consumer perceptions of security risks for Internet shopping are at variance with the genuine levels of risk.

[3] eMarketer (http://www.emarketer.com)

[4] MORI (http://www.mori.com/polls/2001/dti-e-commerce.shtml)

3. MEDIA REPORTING AND E-COMMERCE RISK PERCEPTIONS

As mentioned above, consumer risk perceptions regarding e-commerce are out of line with reality. This naturally leads to the question 'How can this perception gap be reduced?' One way is by learning from media reports, i.e. the media can have a beneficial effect in reducing the gap between actual and perceived level of risks [9]. Potentially beneficial roles of the media include the following.

- Media reports can provide consumers with guidelines for safe shopping via e-commerce.
- Media reports can inform consumers regarding the most secure methods of payment over the Internet.
- The media can inform potential e-commerce participants regarding the actual rate of fraud for both online and offline transactions, as well as providing information about relative security risks.
- The media can help to reduce consumer negative perceptions about e-commerce by informing consumers about the protection offered by credit card companies.

As well as educating consumers about e-commerce and its security, the media also has the potential to discourage potential e-commerce participants. According to the e-commerce resource centre [4], 'Reports about fraud on the Internet are frequently contradictory. Some reports claim that the Internet is an extremely safe place to transact business; other studies indicate that fraud is a clear and present danger; and some studies make it sound as if cybercrime is ubiquitous'.

Whilst loss of personal data confidentiality during transmission is an overriding concern for consumers, there is an associated factor causing negative consumer perceptions of e-commerce, namely sensationalised reporting of computer security incidents in the popular press. For example, instances of credit card fraud involving Internet use are often given very wide press coverage, out of proportion to their importance [7]. According to the MORI survey mentioned above, 44% of Internet users have heard about online credit card fraud from press reports. Of course, it is inevitable that the press gives coverage to e-commerce security issues, since it is a subject of enormous potential public interest. Meanwhile, this public interest in security breaches is explicitly exploited by the mass media in order to increase sales. In the next section we consider how media coverage can be used to the best advantage. Figure 2 illustrates how consumer perceptions of e-commerce can be influenced by media reports.

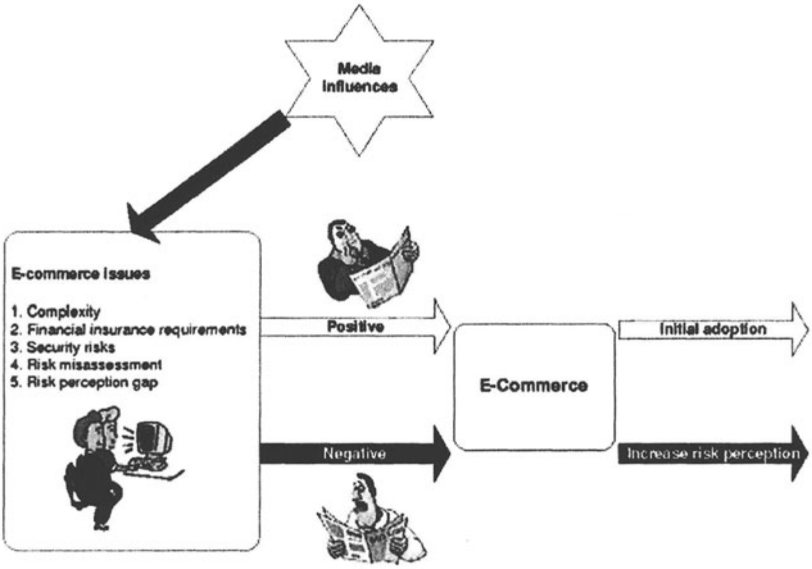

Figure 2. Media influences on consumer perceptions of e-commerce

4. INTERPRETING MEDIA REPORTS OF E-COMMERCE SECURITY BREACHES

Farrell et al. [5] claim that, in a number of cases, security breaches described in newspaper headlines may not be genuine threats to e-commerce participants. Given that media reporting probably affects consumer perceptions to Internet e-commerce, it is crucial for consumers to try to evaluate whether the sources are reliable, and consistent with the real threats to e-commerce.

4.1 Broadcaster technical knowledge

Since most broadcasters are not likely to be e-commerce experts, reports regarding e-commerce security breaches are likely to be somewhat unreliable. Furthermore, it seems that broadcasters do not always analyse carefully the reasons for security breaches; this is perhaps not surprising as there are many possible sources of online frauds involving credit cards. In addition, some of the fraud cases blamed by the media on e-commerce may have little or nothing to do with electronic transactions. As a result, the media may unwittingly be maintaining the gap between consumer perceptions of e-commerce risks and the reality.

4.2 Exaggerated media reports

There is an inevitable tendency for the media to sensationalise news reports – after all, their main job is to attract readers/listeners/viewers. Any compromise of credit card numbers resulting from breaches in e-commerce security receives much public attention, since consumers are already very concerned about the intrinsic security of the e-commerce transaction process. Thus there is a tendency for both the media to exaggerate any e-commerce security breach stories, and also for the e-consumers to over-react to them, potentially maintaining an excessive degree of end-user caution with respect to this new technology. This is a potentially important factor limiting the growth of e-commerce, since the growth of this innovative shopping method is presumably dependent upon public perceptions. If consumers perceive e-commerce negatively, it will clearly reduce the future use of this new technology.

4.3 Reasons for credit card fraud

Because of a lack of technical understanding, the media seems to interpret all e-commerce frauds as being due to security weaknesses. In fact, this is not the case. Such fraud is just as likely, if not more likely, to arise for other reasons. One possible source of frauds is that, through ignorance, consumers may choose to use insecure and unauthorised web-sites, e.g. because of the bargain prices offered. If the site turns out to be completely fraudulent, and consumers lose money as a result, it is perhaps unfair to blame this on the authorised sites. Other frauds, e.g. those involving unreliable merchants, may be just as relevant to conventional offline transactions, and hence it is again unfair to blame the frauds on e-commerce security weaknesses. It is therefore important for the media to try and identify the real reasons for frauds.

4.4 Promoting public understanding

We have seen that lack of technical knowledge and an inherent tendency to sensationalise reporting of security incidents present a long-term obstacle to the adoption of e-commerce. Perhaps the only way in which this issue can be addressed is by active efforts from the e-commerce industry to promote greater understanding.

It is incumbent on all those who stand to benefit from e-commerce (including merchants, banks and third parties) to make positive efforts to educate both the media and the public at large regarding e-commerce and its security. This will probably involve some combination of detailed press releases and open workshops. Above all else, there is almost no chance of the, rightly suspicious, media being convinced of the soundness of e-commerce security provisions without a greater openness by all the involved parties in honestly presenting both the strengths and weaknesses of existing solutions. One-sided 'advertising puffs' are unlikely to convince the media or the public.

5. CONCLUDING REMARKS

Given the public perception of e-commerce security is somewhat negative, the role of the mass media is likely to be very important to the adoption of e-commerce. Potential e-commerce participants are likely to be influenced by information about online credit card frauds reported on television, radio, and in the press. The information provided can be either beneficial or damaging to the acceptance of e-commerce by educating the public about it or exaggerating e-commerce fraud, respectively. It is therefore crucial to the future success of e-commerce that broadcasters carefully evaluate the real reasons for online credit card fraud before reporting to the public. If the reason for an e-commerce fraud is because a consumer used an unreliable payment method, then it would be enormously helpful if that was made clear in the media reports. Achieving the necessary level of media awareness will require a major effort from all the involved parties, combined with a greater commitment to openness.

References

[1] A. Bhatnager, S. Misra, and H. R. Rao. On risk, convenience, and internet shopping behaviour. *Communications of the ACM*, 43(11):98–106, November 2000.

[2] K. Caldwell. Global electronic commerce—moving forward. *CommerceNet: The Public Policy Report*, 2(11):2–17, December 2000.

[3] Department of Trade and Industry. *A Guide for Business to The Consumer Protection (Distance Selling) Regulations*, October 2000.

[4] The E-Commerce Resource Center. *Net Deception: The Impact of Consumer Perceptions of Fraud*, December 2000. Available at http://www.ecomresourcecenter.com/ecom_connection/net description.html.

[5] V. Farrell, Y. Leung, and G. Farrell. A study on consumer fears and trust in internet based electronic commerce. In *Proceedings of 13th International Bled Electronic Commerce Conference*, June 2000. Avaliable at

http://www.it.swin.edu.au/centres/cicec/ECTrust/Bled2000.pdf.

[6] M. Friedman, P. H. Kahn, and D. C. Howe. Trust online. *Communications of the ACM*, 43(12):34–40, December 2000.

[7] A. K. Ghosh. *E-Commerce Security, Weak Links, Best Defences*. John Wiley and Sons, 1998.

[8] V. Hassler. *Security Fundamentals for E-Commerce*. Artech House, 2000.

[9] P. Jarupunphol and C. Mitchell. Actual and perceived levels of risk in consumer ecommerce. In *Proceedings of 2nd International We-B Conference*, pages 207–216. Edith Cowan University Press, November 2001.

[10] A. D. Miyazaki and A. Fernandez. Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, 35(1), November 2001. Available at http://special.northernlight.com/ecommerce/ perceptions.htm.

[11] K. B. Murray. A test of services marketing theory: Consumer information acquisition activities. *Journal of Marketing*, 55:10–25, January 1991.

[12] E. Roger. *Diffusion of Innovation*. New York: The Free Press, 3rd edition, 1983.

[13] A. Rosenbloom. Trusting technology. *Communications of the ACM*, 43(12):31–32, December 2000.

[14] G.W. Treese and L. C. Stewart. *Designing Systems for Internet Commerce*. Massachusetts: Addison-Wesley, 1998.

[15] D. Whiteley. *E-Commerce: Strategy, Technologies and Applications*. Berkeley: McGraw-Hill, 2000.