Chapter 7

Scams and the Australian E-Business Environment

Michelle Sofo
University of Canberra, Australia

ABSTRACT

This chapter highlights the risks and benefits of transacting business within a virtual environment. It becomes evident that e-business has changed the face of consumer/business interactions. Substantial competitive advantage can be gained by a business engaging in well-managed e-business transactions, while consumers can receive benefits such as cheaper prices, a wider range of products, and more convenient shopping via the internet. The chapter commences with a review of the current literature on scams and online fraud, including an introduction to the role that social networking sites can play in facilitating online scams. Statistics regarding e-business transactions for small and medium-sized Australian enterprises are presented followed by the exploration of two specific types of scams: overpayment scams and online shopping scams. Reported financial loss within Australia during 2010 as a result of these scams totalled AUS$29,710,420. The chapter concludes with the identification of some preventative measures to ensure the transactions occurring in any e-business environment are legitimate, followed by some directions for future research.

INTRODUCTION

The Internet has generated countless benefits for societies and particularly businesses, with commercial transactions requiring only an internet connection and the ability to conduct financial movements. A key aim of using e-commerce within a business environment is therefore to gain a competitive advantage. As noted by Roman (2010), competing businesses are now only a mouse-click away from each other, thus it is essential for retailers to gain a sound understanding of the factors affecting both customer satisfaction and loyalty. E-commerce can bring innumerable

DOI: 10.4018/978-1-4666-1619-6.ch007
conveniences to both businesses and consumers, and by expanding into an e-business environment the trader can increase their customer base to all individuals – regardless of location – who are connected to the internet. Physical stores require significant financial outlays for property, personnel and inventories. In contrast, e-businesses can be quite cost effective as the entry costs involved in establishing an online store are low. Of course, the downside to such low entry barriers is that the online retailer may bring with it some uncertainty regarding longevity (Mavlanova & Benbunan-Fich, 2011) and whether it will stay in business long enough to honour the statutory and express warranties that would typically accompany the products being purchased by consumers.

Beyond the concerns over longevity, there are numerous other downsides to e-business, as shown by Dinna, Leau, Habeeb and Yanti (2007) who suggest that the internet has destroyed traditional business transactions in a number of ways. E-commerce brings with it a number of risks, including the risk of becoming the victim of a scam and the risk of either online fraud or other cyber crime occurring. The Australian Government’s Department of Broadband, Communications and the Digital Economy (DBCDE, 2010) note that fraudulent online transactions can result in numerous losses for a business including lost revenue, damaged reputation and the frustration of having to deal with credit card charge-backs on behalf of aggrieved consumers. Further, entering into an e-business environment can expose business systems to unauthorised access and theft of consumer information such as credit card details or other personal identifiers. All these incidences are types of cyber crime.

It has been estimated that 65% of the world’s 2 billion internet users have fallen victim to some form of cyber crime (Coopes, 2010). Dinna et al (2007) suggest that the complexity, frequency and severity of online phishing attacks have escalated to the point where offenders are regarded as the ‘street muggers of the digital era’. ‘Phishing’ in this context is defined as an email that fishes for specific information such as credit card numbers, account names, passwords or other personal information (Australian Federal Police, n.d.). When the Australian Bureau of Statistics conducted the National Personal Fraud Survey, it was found that AUS$980 million dollars were lost in a 12 month period as a result of credit/bank card fraud, identity theft, and scams such as fake lotteries, pyramid schemes, phishing incidents, chain letters and advance fee fraud (Australian Bureau of Statistics, 2007b). Many of these incidences occurred online and were facilitated through interpersonal and financial transactions. Although this monetary loss is reported on a personal level, it can be extrapolated that there is a significant proportion of financial loss affecting small, medium and large enterprises operating within the Australian e-business environment. Scams can also be costly in ways that extend beyond monetary value. As noted by Stajano and Wilson (2011), some people have gone bankrupt while others have committed suicide as a result of being scammed.

The purpose of this chapter is to highlight the risks and benefits of transacting business within a virtual environment and to raise awareness amongst organizations, manufacturers and vendors about the vulnerabilities that arise when conducting business online. Perry (2002) identifies several factors that make the electronic environment so attractive to criminal activity, including the borderless and global nature of the Internet, the affordability, accessibility, anonymity, speed and immediacy of online transactions, and the lack of readily accessible evidential material such as documents or fingerprints. Regulations that relate to e-commerce and e-business transactions tend to be incomplete and inconsistent (Zaharia, Zaharia, Tudorescu & Zaharia, 2010), and it is common for jurisdictional challenges to arise when law enforcement agencies in one country discover cyber-criminals operating out of another country.

The structure of the chapter includes four main sections. First, the chapter commences with
Related Content

A Socio-Cultural Analysis of the Present and the Future of the M-Commerce Industry
[www.igi-global.com/chapter/socio-cultural-analysis-present-future/19511?camid=4v1a](www.igi-global.com/chapter/socio-cultural-analysis-present-future/19511?camid=4v1a)

IT Governance as Resource Mobilization
[www.igi-global.com/chapter/governance-resource-mobilization/8734?camid=4v1a](www.igi-global.com/chapter/governance-resource-mobilization/8734?camid=4v1a)

Organisational Challenges of Implementing E-Business in the Public Services: The Case of Britain's National Mapping Agency
[www.igi-global.com/article/organisational-challenges-implementing-business-public/1868?camid=4v1a](www.igi-global.com/article/organisational-challenges-implementing-business-public/1868?camid=4v1a)

User Interface Design and E-Commerce Security Perception: An Empirical Study
[www.igi-global.com/article/user-interface-design-commerce-security/66051?camid=4v1a](www.igi-global.com/article/user-interface-design-commerce-security/66051?camid=4v1a)