Chapter 49
Online Scams
Case Studies from Australia

Michelle Berzins
University of Canberra, Australia

ABSTRACT

The adoption of new technologies presents a risk that inexperienced users may become immersed in a virtual world of cyber-crime featuring fraud, scams, and deceit. In addition to the societal benefits of social interaction technologies (SIT), the adoption of social software tools brings a range of security issues. The chapter highlights the "darker" side of SIT in which online safety and interpersonal trust become tangible commodities and where fraudsters prey on unsuspecting netizens; it demonstrates that an assortment of technological tools and psychological practices may be used to gain the confidence and trust of unsuspecting consumers. The author argues that consumer education can be successfully utilized to enhance the ability of Internet users to detect and avoid fraudulent interactions and safely enjoy the many benefits afforded by the emerging social interaction technologies.

INTRODUCTION

Online experiences, such as shopping, gambling, and dating, are vivid examples of social interaction technologies (SIT). Using Internet-based applications, consumers can perform interactive transactions within the seemingly anonymous comforts of their own home or office. Essentially, all that is required is a credit card and Internet access, and consumers are able to freely interact with others during the purchasing of goods or the creation of personal attachments. Whilst the Internet has generated countless benefits, it has also provided new opportunities for criminal behaviour (Savona & Mignone, 2004), including fraudulent solicitations, fraudulent transactions, and the transmission of the proceeds of crime (Davila, Marquart, & Mullings, 2005). The use of new technologies therefore brings a risk that inexperienced users may become immersed in a virtual world of cyber-crime featuring scams, fraud, and deceit.

Emerging social interaction technologies can be used as tools through which crimes can be planned

DOI: 10.4018/978-1-60566-368-5.ch049

or implemented (Savona & Mignone, 2004). Wall (2004) defines *cyber-crime* as criminal acts that are transformed by networked technologies. They are crimes that are traditionally executed by other means yet are now being executed via the Internet or some other technological computing advancement. There are so many benefits to Internet-based services: e.g., cost effectiveness, timeliness, accessibility, speed, and convenience (Krone & Johnson, 2007). However, there are also innumerable scams transmitted via the Internet everyday; these include: get rich quick schemes, romance scams, requests to launder money under the guise of a legitimate offer of employment, and offers to purchase cheap products (such as pharmaceuticals).

Digital versions of traditional fraud readily target Internet users regardless of their location, age, or level of education. They are scams conducted by computer-savvy individuals who know how to instill confidence in consumers by manipulating an online situation to produce the type of behaviour that they desire. Even people who are confident that they would not fall victim to a scam may be at risk, particularly given the seemingly legitimate appearance of many scams. This is called *unconscious manipulation* and occurs when a consumer perceives an illegitimate offer or situation to be legitimate due to the specific information and artificial reality created by the scammer. The proliferation of online scams comes from this apparent legitimacy which results in people failing to independently evaluate the authenticity of an online offer or situation.

This chapter aims to highlight the dangers of SIT in exposing unwitting participants to fraudulent activity in Australia. By exploring specific cases of online shopping and online dating scams, significant risks are demonstrated that consumers and everyday users of SIT should be aware. Greater attention to consumer education could possibly reduce the risk of SIT users falling for online scams and go some way towards keeping SIT users alert to new forms of Internet deceit.

BACKGROUND

Scams, confidence tricks, and other types of fraudulent activity have existed for a long time. Some of the earliest scams were advance fee frauds where individuals pretended to sell something that they did not have, while taking money in advance from their victims. While these types of scams were initially transmitted via mail and facsimile, the early 1990s saw their existence proliferate due to the speed and ease with which they could be transmitted via the Internet by individuals around the globe (Holt & Graves, 2007). This proliferation has had two noticeable effects: first, a decline in consumer confidence levels, and second, increased reports of monetary loss as a result of scam activity.

With regard to a decline in consumer confidence levels, the e-business report released in May 2007 by Sensis, an advertising subsidiary of a major communications provider in Australia – Telstra, used the results of telephone interviews with 1,800 small and medium businesses to assess their attitudes towards, and experiences with, e-business (Sensis, 2007). The study found that 42% of small to medium enterprises were concerned about the risk of people hacking into their computer system, and 12% noted that their customers were not prepared to carry out their financial transactions over the Internet due to security concerns (Sensis, 2007). These types of concerns are not uncommon, nor are they unfounded as shown by the Sensis consumer report (Sensis, 2008). This study involved the surveying of 1,500 people to measure their consumer confidence and expectations. The March 2008 consumer report indicates that consumers reported an average of 5.49 when asked to rate their concerns about Internet security on a scale between 1 and 10. The highest level of concern on this issue was among those in the 65+ age bracket (5.77). These concerns ranked 15th behind other issues such as: the price of gasoline, the environment, the cost of living, drought, health, and education (Sensis, 2008).