ABSTRACT

Every day dangerous criminals are targeting high net wealth members of our community as they venture onto the internet. Statements from twenty-nine community organizations and mature age internet users were analyzed using structured coding techniques in order to identify the major criminal risks and threats, and key protective safeguards. The study warns that mature users, particularly those with high net wealth, are critically vulnerable to internet fraud, and personal data and identification theft through spear phishing email and remote access trojan malicious software attacks. The major implication for countries with aging populations, and rising numbers of mature internet users, is the urgent need for ongoing development and resourcing of internet security skills and awareness programs; consumer protection laws and law enforcement assistance; affordable protective internet technologies and complementary support schemes; and the strengthening of online business codes and standards, particularly in dealings with older people.

Keywords: Criminal, Fraud, Internet, Mature, Phishing, Spear

INTRODUCTION

While we might think that internet-based crime is typically perpetrated against the younger and more tech savvy parts of our community, mature users are emerging as vulnerable targets for criminals. Alarmingly, there is a steady growth in opportunities for criminals to exploit the mature segment of our communities. As an example, reports of information theft, malicious software (malware) attacks, and online financial scams in the 40 to 59 year old age bracket represented the largest group of complaints (Internet Crime Complaint Center, 2010). In addition, a more recent study highlights the multi-billion dollar losses suffered by older people due to financial scams and exploitation (estimates up to US$2.9 Billion in the US alone) (Metropolitan Life Insurance, 2011). Critically, government authorities and legal experts now acknowledge...
that past fraudulent telemarketing and financial scam attacks have now firmly transitioned to the internet (Mouallem, 2002; Sylvester, 2004).

While several studies examine the benefits and barriers related to internet use by older people (Haukka, 2011; Reisig, Pratt, & Holtfreter, 2009; Russell, Campbell & Hughes, 2008; Selwyn, 2004), we present a case study that investigates the types of risks and threats, and safeguards related to internet use by mature high net wealth individuals. Our reasoning is based on two important points. First, in the Australian context this is extremely important with the median net wealth of those in the 55 to 74 year old age bracket ranging from A$743,000 to A$824,000 (Commonwealth of Australia, 2007). In addition, Australians’ retirement savings in superannuation accounts exceeds A$1 Trillion, with the highest value accounts held by 60-64 year old members (i.e. A$199,000 in 2010) (The Association of Superannuation Funds of Australia, 2013). Hence, the high volumes of accumulated wealth and financial assets in the mature segment of our community (Lusardi & Michell, 2007) provide an inviting target for criminals and scams. Second, over 54% of Australians over the age of 60 years use the internet extensively to access government services, purchase goods and services, and undertake financial transactions (Australian Bureau of Statistics, 2011). These rising rates of online activity provide increasing opportunities for internet fraud and theft (Australian Bureau of Statistics, 2012). Accordingly, our research was motivated by the aims to: (1) understand the types of risks and threats to mature internet users; and (2) focus on the safeguards that reduce online fraud and financial losses. Our investigation analyzed the combined views of community stakeholders using a rigorous data structure and content analysis to examine the risks, threats and safeguards (Corley & Gioia, 2004; Freeman, Wicks & Parmar, 2004). The stakeholder approach is well-suited to the detailed analysis of differing and unified community views, particularly when considering a confluence of behavioral and technological issues.

The balance of the paper is developed as follows. First, we review some of the extant and contemporary literature that addresses internet enabled crimes against mature users, the use of the internet by mature high net wealth members of the community, and the associated internet security issues. Next, we briefly describe our research method, including the data collection and processing procedures; and the analytical steps using the data structure and automated content analysis. This is followed by a presentation and discussion of the results obtained during the study. The paper concludes with a summary of key issues and advisory remarks.

LITERATURE REVIEW

In a sad indictment on modern society, several studies show a propensity for systemic abuse and exploitation of mature age people in communities (Friedman, 1992; Johnson, 2003; Sharpe, 2004). Past research shows that mature age people were identified by criminals and organized crime gangs as wealthy ‘easy targets’ for the perpetration of identity theft, telemarketing and consumer based fraud (Cassini, Medlin, & Romaniello, 2008; Johnson, 2003; Lee & Geistfeld, 1999; Marshall & Tompsett, 2005; Martin, 2009; Rabiner, O’Keeffe, & Brown, 2006; Sharpe, 2004; Tueth, 2000; Vacca, 2003; Zagorsky, 1999). Also, specific to this study, research conducted by the Australian Institute of Criminology (AIC) found that card based identity theft and consumer fraud in Australia targeted at the 65 years and older age group was likely to rise by 20% in the near term (Temple, 2007). So while these more traditional channels have been used to exploit the older segment of our community, the emergence of internet pathways provides criminals with yet another potential avenue for illegal activities (Carlson, 2006; Sylvester, 2004; The Financial Services Roundtable, 2010).

Studies of the internet dating back to the late 1990s asserted that the online environment offered many exciting and important ‘quality of life’ opportunities for mature age users (Mann,
Privacy-Preserving Transactions Protocol Using Mobile Agents with Mutual Authentication
Song Han, Vidyasagar Potdar, Elizabeth Chang and Tharam Dillon (2007).
*International Journal of Information Security and Privacy* (pp. 35-46).
[www.igi-global.com/article/privacy-preserving-transactions-protocol-using/2455?camid=4v1a](www.igi-global.com/article/privacy-preserving-transactions-protocol-using/2455?camid=4v1a)

Information Security for Situational Awareness in Computer Network Defense
*Situational Awareness in Computer Network Defense: Principles, Methods and Applications* (pp. 86-103).
[www.igi-global.com/chapter/information-security-situational-awareness-computer/62377?camid=4v1a](www.igi-global.com/chapter/information-security-situational-awareness-computer/62377?camid=4v1a)