Spearing High Net Wealth Individuals: The Case of Online Fraud and Mature Age Internet Users

Nigel Martin, Research School of Accounting and Business Information Systems, The Australian National University, Canberra, ACT, Australia

John Rice, Department of International Business and Asian Studies, Griffith University, Southport, QLD, Australia

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. Alarming, 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

DOI: 10.4018/jisp.2013010101

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\$1.4 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,

1997). Over time, studies show that the use of Information and Communications Technologies (ICT) results in several important benefits, including the ability to stay socially connected; email friends and family; seek government information; conduct electronic commerce and shopping; plan travel and leisure activities; execute internet banking transactions; and, undertake self-improvement training and education (Cameron, Marquis, & Webster, 2001; Osman, Poulson, & Nicolle, 2005; Russell, Campbell & Hughes, 2008; Selwyn, 2004; Sum, Mathews & Hughes, 2009). Also, other studies in this area have examined the types of factors that engender the adoption of ICT by mature age persons, including the capacity to be innovative, relevance to lifestyle, and connection to everyday activities (Haukka, 2011; Reisenwitz, Iyer, Kuhlmeier, & Eastman, 2007; Selwyn, Gorard, Furlong, & Madden, 2003); and some of the common barriers to ICT adoption, including low levels of computer skills; social vulnerability; perceived risky online transactions; and, ICT complexity (Cameron, Marquis, & Webster, 2001; Haukka, 2011; Reisig, Pratt & Holtfreter, 2009). On balance, we note that mature age people have embraced the use of ICT in daily life.

However, with this movement to internet channels, there comes a need to understand the types of risks and threats; build confidence and skills; and, remain aware and informed of current and emerging issues (Dodge, Carver, & Ferguson, 2007; LaRose, Rifon & Enbody, 2008; UK Office of Science & Technology, 2004; Wagner, Hassanein & Head, 2010). These protective behaviors are important when we consider that mature internet users (many vulnerable high net wealth individuals) are 'typically disproportionately targeted' for internet crime and fraud (Hough, 2004); often vulnerable due to misplaced trust in internet information (Grimes, Hough, Mazur, & Signorella, 2010); and, regularly use structured, step-by-step online instructions (Cook, Szewczyk, & Sansurooah, 2011). When we factor in their lifetime accumulation of wealth and assets, mature age people make prime targets (Zagorsky, 1999; Sylvester, 2004).

In summary, we support legal studies that call for increased protection of mature age people who extensively use the internet (Adams, 1996; Carlson, 2006; Martin, 2009; Mouallem, 2002; Sylvester, 2004; Temple, 2007). It should be highlighted that the legal fraternity is not just seeking regulatory enforcement and criminal prosecution but also asserts the need for adequate training and awareness; technological tools such as anti-virus software, encryption, digital signatures, and public key infrastructure; community support programs; and dedicated monitoring and surveillance initiatives (such as the US Elder Watch Program) (Carlson, 2006; Hough, 2004; Martin, 2009; Mouallem, 2002; Sylvester, 2004). Hence, a multi-safeguard approach to online fraud protection is strongly advocated. Importantly, in this respect, our study builds into the emerging tradition of literature that blends the use of ICT by mature age persons with the discipline of online security (Carlson, 2006; Cook, Szewczyk, & Sansurooah, 2011; Grimes, Hough, Mazur, & Signorella, 2010; Hough, 2004; Reisig, Pratt & Holtfreter, 2009; Sylvester, 2004).

METHOD

The study's research method used qualitative analysis techniques to collect and code the data (Bauer & van Eeten, 2009; Denzin & Lincoln, 2005; Freeman, Wicks & Parmar, 2004; Miles & Huberman, 1997). The stakeholders' opinions are subjected to a structured coding analysis in order to determine the types of risks (and potential negative impacts) that mature internet users' face, and what safeguards may assist in countering these hazards. This form of qualitative analysis is well suited to an exploratory investigation (Creswell, 2003; Denzin & Lincoln, 2005), and follows other research programs in the field of computing security where qualitative and human behavioral analyses have been successful (Albrechtsen, 2007; Jain, 2005; Schultz, 2004, 2005; Stanton, Stam, Mastrangelo, & Jolton, 2005).

Data Collection and Processing

The 29 individual and organization stakeholder submissions (written) and a public hearings transcript were collected over the period January to April 2012 from the Parliament of Australia web pages that were established for the Inquiry into Cyber-Safety for Senior Australians (Commonwealth of Australia, 2011). Noting that 'internet fraud' was the most prevalent form of personal fraud committed against Australians (Australian Bureau of Statistics, 2012), the inquiry was tasked to investigate and report on the nature, form, implications and impacts of internet risks and threats to mature age users; and, the adequacy of current and future internet security safeguards (Commonwealth of Australia, 2011). Importantly, the scope of the inquiry provided a useful base of stakeholder data for our analysis.

A summary of the stakeholders and their inputs is presented below (see Appendix). The majority of inputs came from fourteen large to medium government agencies covering policy, program and crime prevention and policing functions. Ten Non-Government Organizations (NGOs) represented the views of older people (older age activities focus), charities and community organizations, libraries and information dissemination bodies, and healthcare consumers. eBay and Telstra Corporation provided statements from the perspective of internet and telecommunications service provider firms. Importantly, two individual stakeholders in the 80 years plus age group came forward to report family members (60 year old son and 98 year old mother) who had been the victims of internet enabled advance fee fraud (over A\$1.5 million in accumulated losses). Stakeholder submissions were provided on a voluntary basis, and all submissions were included in the analysis to maximize the results output.

Research Model and Data Structure

In order to maintain sufficient analytical rigour, and high levels of traceability between the data points and the research aims, we were advised to

establish an integrated research model (using a column format) and data structure for our study (Corley & Gioia, 2004). This required the close linkage of the data (stakeholder statements) provided to the government with the aims, and the structural capacity to axially collapse the coded data into integrated summaries that accurately portray the results (see Figure 1). This data structure supported the careful coding and interpretation processes and allowed us to draw connections between the statements within, and across, the data sub-structures (Corley & Gioia, 2004).

Research Procedure Using Content Analysis Software

A data structure for the study (Corley & Gioia, 2004) was created using the NVIVO Version 8 software (Walsh, 2003). Stakeholder written statements and the public hearing transcript were collected and placed in the internal documents folder for the project. The project's tree node structure assigned safeguarding mature internet users as the apex node, and the four major data sub-structures (i.e. serials 1 to 4 in Figure 1) were assigned as the major branch nodes. Stakeholder statements (661 in total) were coded within the sub-branch node to maintain and assure issue or construct integrity. Statements were separately coded by each researcher, with any differences resolved through cyclic review and revision. Example statements, noting the stakeholder, submission number and date are presented in the results. The coded statements were then axially collapsed into summaries (Denzin & Lincoln, 2005; Miles & Huberman, 1997).

DISCUSSION

Internet Risks and Threats: Nature and Form

The major risk event or threat identified by the stakeholders is financial and investment fraud (63% of the coded statements) (see Table 1). In addition, personal data and identification theft from social network and electronic transac-

Figure 1. Data structure for the study

tions accounted for a further 26% of the coded responses. Stakeholders responded that spear phishing e-mails (i.e. mature high net wealth internet users as prime targets) for the theft of user names, access passwords, credit card numbers and financial institution account details; and

associated malicious software (malware) attacks on computer networks and mobile devices (e.g. tablet computers, smartphones), were the main forms of risks and threats encountered.

The results show that several types of online financial fraud, and the potential for personal

Table 1. Internet risk and threats: nature and form

Serial 1	Results	Coded Statements	
A. Nature of internet risks and threats	Internet fraud - Finance and Investment scams - Superannuation Account and Retirement Savings theft - Charity Donation theft - Advance Fee fraud - Internet Dating and Romance scams	68	63%
	Theft of Personal Data	17	16%
	ID Theft (for reuse and resale)	14	12%
	Other (cyber stalking, offensive materials, crime networks)	10	9%
	<i>Total</i>	109	100%
B. Form of internet risks and threats	Spear Phishing email scams	29	57%
	Malware Attacks (computer networks and mobile devices)	22	43%
	<i>Total</i>	51	100%

data and identification theft (for the purposes of conducting further criminal activities), present as areas of high risk in the broader community. As an example, the AIC submission highlighted this issue “If (online) victimisation were to occur, the impact on seniors could be substantial. They may lose all, or part, of their superannuation retirement savings, and having a limited ability to recover financially, could impose an additional burden on welfare agencies. In addition to the financial impacts, victimization can lead to a loss of trust, fear and anxiety” (AIC, sub. 12, February 16, 2012).

Further, these types of losses were put in a harsh and real perspective by the first two individual stakeholders (sub. 17, February 22, 2012; and sub. 21, March 2, 2012) who revealed that family members had been the victims of internet advance fee fraud to the value of over A\$1.5 million. Additionally, the analyzed statements show that the steady growth in spear phishing attacks on ‘high net wealth individuals’, sometimes known as ‘whale phishing’, appears highly visible to community stakeholders (Anti-Phishing Working Group Inc., 2010; RSA, 2012). As we noted from other studies, this risk-laden environment leaves mature internet users, with large accumulated wealth and assets, significantly vulnerable to internet fraud and crime (Sylvester, 2004; Temple, 2007).

Internet Risks and Threats: Implications and Impacts

The main implication arising from higher rates of spear phishing and malware attacks was the need for practical internet security skills, and increased awareness for mature internet users (see Table 2). The Australia’s largest telecommunications firm, Telstra, strongly emphasized security skills requirements “When it comes to using the internet, users of any age need to know how to stay safe online at all times. The lack of adequate skills and training can result in a negative online engagement amongst senior Australians, and can discourage online participation. A lack of understanding, ICT skills and awareness of online safety risks contribute to a negative experience and perception of the internet amongst senior Australians, thus impacting on the uptake of online engagement, and a lack of participation in the digital economy” (Telstra, sub. 22, February 24, 2012).

Stakeholders also raised the issue of trust arguing that the apparent legitimacy of these scams and frauds (many originating from other countries), left mature age users at a significant disadvantage in knowing ‘who to trust and what to believe’. Certainly, the results of this and other studies show that when we combine a lack of practical internet security skills with unresolved trust issues, the potential for significant material losses is heightened (Australian Institute of

Table 2. Internet risk and threats – implications and impacts

Serial 2	Results	Coded Statements	
A.Implications of internet risks and threats	Requirement for internet security skills and awareness	53	58%
	Uncertainty over who to trust and what to believe	26	28%
	Support for digital inclusion	13	14%
	Total	92	100%
B. Impacts of internet risks and threats	Substantial financial wealth, assets and reputation losses	28	39%
	Loss of confidence and fear of ICT	28	39%
	Emotional trauma and family related distress	16	22%
	Total	164	100%

Criminology, 2012; Mansell & Collins, 2005; Ross & Smith, 2011; Smith & Budd, 2009).

In analyzing the results related to the impacts of spear phishing and malware attacks, we observed a somewhat unusual outcome with stakeholders giving equal emphasis to (1) the losses of wealth and personal assets, and (2) the loss of personal confidence and fear of using online systems. The results suggests to us that these types of online fraud can deliver a mix of economic and social losses, where victims may suffer from electronic or digital isolationism as a consequence of internet crime (Jain, 2005; Schmallegger & Pittaro, 2009; Sharpe, 2004). Arguably, in our haste to pursue criminals, recoup lost assets and seek legal remedies, we may fail to adequately deal with these important social impacts (Reisig, Pratt & Holtfreter, 2009). Hence, while online fraud might be a crime of financial opportunity, it could also be characterized as having a large measure of social abuse and damage.

Internet Security Safeguards: Current Adequacy

In assessing the current adequacy of internet safeguards we found that protections against spear phishing and malware attacks are ‘partially adequate’ at best, and do not provide the required level of support for mature internet users (note, in relation to national advisory services for internet fraud, stakeholders rated this

as inadequate) (see Table 3). The results show that internet security skills programs, awareness and information campaigns; internet security technologies; legal and consumer protections; and national advisory services are in need of significant improvements.

As an example, the peak body for senior citizens, National Seniors Australia (NSA), made firm recommendations on improving safeguards “National Seniors (Australia) proposes more targeted government-sponsored online security and safety campaigns for senior people; more government-sponsored training courses and materials which allow for and address the lack of basic skills; and, a hotline and website for senior people providing information on online safety issues, such as virus protection, scams and privacy protection” (NSA, sub. 29, March 20, 2012).

Further contemporary studies reinforce the importance of the results. As an example, the international study of Connolly, Maurushat, Vaile and van Dijk (2011) showed that, across 11 jurisdictions and over 68 different internet security education and awareness programs, ‘none focused solely on mature age computer users’, and ‘only 12% contained some materials tailored to the needs of older internet users’. Similarly, other studies call for the changing and strengthening of inadequate consumer laws to support internet fraud victims (Martin, 2009).

Table 3. Adequacy of current internet security safeguards

Serial 3: Current Safeguard	Adequacy Rating and Reasoning	Coded Statements	
Internet security skills development and community awareness campaigns	Partial – not specific to mature age internet users	45	49%
Technical measures and technology	Partial – highly complex, difficult to understand and often expensive	18	20%
Expert internet fraud advisory services	Inadequate expert advisory services for internet users	16	17%
Criminal law and consumer protections for internet users	Partial – weak and ineffective; continually changing to adapt to new criminal threats	13	14%
	<i>Total</i>	92	100%

**Internet Security Safeguards:
Future Best Practices**

The results from this section of the study are not necessarily unexpected. While stakeholder responses were largely concentrated in and around the areas of skills and awareness development, security information services, enhanced laws and enforcement, protective technologies (see Table 4), we would draw out several important issues. First, while ICT security skills and awareness initiatives have been proven to be effective in addressing various phishing and malware threats (Johnson, 2006; Spurling, 1995; Thomson & von Solms, 1998; Wooding, Anham, & Valeri, 2003), technical studies show that they are singularly ineffectual (Sheng, Holbrook, Kumaraguru, Cranor & Downs, 2010). Importantly, skills and awareness must form part of a larger suite of safeguards (e.g. mix of security skills, awareness, information, laws, and technologies) (Parmar, 2012). Hence, none of the proposed future safeguards should be considered, or deployed, in isolation.

Second, external evidence highlights the importance of providing increasing levels of internet safety and security resources to support mature age internet users (Johnson, 2003; Sharpe, 2004; UK Office of Science & Technology, 2004). Therefore, the high priority assigned to publicly available internet security and point-of-sale information by the stakeholders is arguably well positioned. The Brotherhood

of St Laurence social welfare organization captured this issue as follows “Funding and subsidies could be extended. Currently, the quantum of government funding to support the development of internet understanding, skills and confidence is minimal in comparison with the large and increasing population of senior Australians lacking internet experience or competence” (Brotherhood of St Laurence, sub. 13, February 17, 2012).

Also, we would argue that resources will need to grow markedly as the community observes a combination of steady increases in mature age internet user activity (Australian Bureau of Statistics, 2011), and heightened levels of email and internet fraud, particularly against those older high net wealth citizens (Australian Bureau of Statistics, 2012).

Third, while the importance placed on laws and legal instruments is understandable, online fraud, spear phishing and the deployment of high grade malware are typically transnational and highly transformative in nature (Schmallegger & Pittaro, 2009). Our analysis of the Australian Federal Police submission provided a measure of realism in relation to online law enforcement “The Commonwealth legal and regulatory framework is under constant review. Law reform in this area presents a number of challenges due to the rapidly changing digital environment and the transnational and highly adaptable nature of online criminality. Online crime is borderless and evidence can be transi-

Table 4. Future best practice internet security safeguards

Serial 4 – Future Best Practice Safeguard	Coded Statements	
Internet security skills and awareness development	57	37%
Public information and point-of-sale resources	36	24%
Improved criminal laws, consumer law and protections, and cooperative law enforcement (cross-jurisdictions)	20	13%
Widespread use of protective technologies and socio-technical support systems	20	13%
Improved business codes of practice, industry-government agreements and business and technical standards	12	8%
Increased research on internet practices of high net wealth individuals	8	5%
Total	153	100%

tory, highly volatile and located overseas. As a result a key legislative issue for law enforcement is an effective and efficient legal framework for the exchange of information and evidence with overseas agencies. Reforms to the Mutual Assistance in Criminal Matters Act 1987 in the Cybercrime Legislation Amendment Bill 2011 presently before Parliament will enable greater sharing of information between Australian and foreign law enforcement agencies” (Australian Federal Police, sub. 20, February 23, 2012).

Hence, while criminal statute exists to protect us from internet fraud (Commonwealth of Australia, 1995, 2001), it remains unlikely for the foreseeable future that we could depend on legal instruments to protect high net wealth individuals from transnational internet based crimes (Carlson, 2006; Clough, 2010; Hammond, 2003; Hough, 2004; Martin, 2009; Milhorn, 2007; Mouallem, 2002; Schell & Martin, 2004; Sylvester, 2004).

Fourth, benchmarking surveys and studies shows us that the volume and density of online attacks is increasing exponentially (e.g. 286 million online threats detected in 2010, A\$2 billion losses (42% internet fraud related) in Australia in 2012) (Norton, 2012; Sophos, 2013; Symantec, 2011). Since 2004, the financial and

payment services industries have suffered the highest rate of phishing attacks on a global basis (see Figure 2) (Anti-Phishing Working Group Inc., 2013). Accordingly, technology safeguards in the form of SPAM email filters, anti-virus software, blacklisting and white listing technology, and intrusion detection and prevention systems play a valuable role in deterring spear phishing and malware attacks (Fire Eye, 2012a, 2012b; Gragido & Pirc, 2011; Luo & Guan, 2007; Masud, Khan, & Thuraisingham, 2007; RSA, 2012).

However, it must be acknowledged that many of our protective technology safeguards will have temporal and technical limitations (Gragido & Pirc, 2011; Heyman, 2007; Jakobsson & Myers, 2007). Therefore, these safeguards might be complemented by social service monitoring and surveillance programs, like the US Elder Watch Program (Sylvester, 2004) and the Older Persons Abuse Prevention Referral and Information Line (APRIL) operated by the Australian Capital Territory Government (ACT Government, 2012). In this respect, socio-technical solutions provide multi-layer deterrents against spear phishing and malware attacks.

Figure 2. Phishing attack volumes on financial and payment services (2004-2012)

Finally, the use of cooperative agreements, business codes of practice, and corporate and technical standards may offer further opportunities to protect mature age internet users from online fraud. As an example, the Australian iCode is a voluntary code of practice for Internet Service Providers (ISPs) that provides a business framework for internet users and ISPs. These types of safeguards have found favour in the literature (Bauer & van Eeten, 2009; Clough, 2010; Sharpe, 2004) and, as noted in the Australian context (Bauer & van Eeten, 2009), will likely form part of an ongoing joint work program targeted at improving internet safety and security.

CONCLUSION

In concluding our study, we would argue most strongly that developing a greater understanding of the internet risks, threats and safeguards related to mature high net wealth users is very important. We duly acknowledge the limitations of research that uses a small sample of voluntarily provided statements obtained from a range of different organizations and individuals in Australia (few private businesses and individual citizens elected to participate in the inquiry). That said, we took expert methodological advice and applied the maximum level of rigour possible using an automated content analysis and coding software tool.

In the context of this study, the confluence of emerging events now leaves us facing what we would see as 'the perfect storm'. The latest international reporting and data on phishing and malware attacks presents a sobering view to the future. First, since 2004, financial and payment services, including banking, investment, superannuation and brokerage accounts, have been the number one target for spear phishing criminals and organized crime (Anti-Phishing Working Group Inc., 2013). Second, the use of spear phishing campaigns against high net wealth citizens in Australia achieved an infection rate of 25% in 2012 (in the top 25 countries in the world for phishing attacks) (Anti-Phishing

Working Group Inc., 2013). Third, the use of Remote Access Trojan (RAT) malware has reached the 78% level contributing to an estimated A\$0.9 Billion in internet fraud related financial losses in Australia (Norton, 2012; Trend Micro, 2012; Sophos, 2013). Hence, when we combine these facts with limited internet security skills and awareness, limited publicly available internet security information, weak consumer laws and complex technology safeguards, the problems become largely magnified.

Our analysis shows that a broad based multilayered combination of safeguards is preferable. Importantly, stakeholders opined that many safeguards are only partially effective at best, with some under-resourced and ineffective. Hence, the capacity to singularly rely on training and awareness, public information, protective technologies, or consumers laws for protection is manifestly inadequate. In sum, the nature and form of evolving spear phishing and RAT malware risks and threats, including the associated financial losses and social impacts, provides public and private organizations with strong incentives to construct and continually improve a range of internet safeguards (RSA, 2012).

In closing, the security and safety issues and problems that confront our wealthy internet users are growing with each passing day. Statistics clearly show that phishing attacks are reaching pandemic proportions (Anti-Phishing Working Group Inc., 2013). Contemporary national surveys show that the highest growth rate of Internet usage occurred in the 55 to 64 year old age bracket with over 70% of these older Australians accessing the internet environment (Australian Bureau of Statistics, 2011). When we combine these trends with Australia's aging population, (Australian Bureau of Statistics, 2010), it is difficult not to conclude that this presents as a significant problem for ours and other global communities. Accordingly, there is a hope that this research stimulates the creation of further programs, technologies, standards and laws that are aimed at protecting this expanding generation of wealthy internet users.

ACKNOWLEDGMENT

The authors acknowledge the support and assistance of the Australian Government and the Federal Minister for Broadband, Communications and the Digital Economy, Senator Stephen Conroy. We also wish to thank Professor Denny Gioia for his helpful advice on the conduct of robust and rigorous qualitative research.

REFERENCES

- Adams, J. (1996). Controlling cyberspace: Applying the computer fraud and abuse act to the internet. *Santa Clara Computer and High-Technology Law Journal*, 12(1), 403-434.
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289. doi:10.1016/j.cose.2006.11.004.
- Anti-Phishing Working Group. (2010). *APWG phishing attacks trend report 4th quarter 2009*. San Francisco, CA: APWG Inc. Retrieved October 7, 2011, from <http://www.apwg.org/resources/apwg-reports/>
- Anti-Phishing Working Group. (2013). *APWG phishing attacks trend report 3rd quarter 2012*. San Francisco, CA: APWG Inc. Retrieved March 2, 2013, from <http://www.apwg.org/resources/apwg-reports/>
- Australian Bureau of Statistics. (2010). *Population by age and sex, Australian states and territories, December 2010, Cat No. 3201.0*. Canberra, Australia: ABS.
- Australian Bureau of Statistics. (2011). *Household use of information technology, Australia 2010-2011, Cat. No. 8146.0*. Canberra, Australia: ABS.
- Australian Bureau of Statistics. (2012). *Personal fraud, Australia 2010-2011, Cat. No. 5428.0*. Canberra, Australia: ABS.
- Australian Capital Territory (ACT) Government. (2012). *Elder abuse prevention and assistance*. Canberra, Australia: Department of Community Services. Retrieved December 18, 2012, from http://www.dhcs.act.gov.au/wac/ageing/elder_abuse_prevention_and_assistance
- Australian Institute of Criminology. (2012). *Australia crime; facts and figures 2011*. Canberra, Australia: Australian Institute of Criminology.
- Bauer, J., & van Eeten, M. (2009). Cybersecurity: Stakeholder incentives, externalities and policy options. *Telecommunications Policy*, 33(1), 706-719. doi:10.1016/j.telpol.2009.09.001.
- Cameron, D., Marquis, D., & Webster, B. (2001). Older adults perceptions, experiences and anxieties with emerging technologies. *Australasian Journal on Ageing*, 20(1), 50-56. doi:10.1111/j.1741-6612.2001.tb00399.x.
- Carlson, E. (2006). Phishing for elderly victims: As the elderly migrate to the internet fraudulent schemes targeting them follow. *The Elder Law Journal*, 14(2), 423-452.
- Cassini, J., Medlin, B., & Romaniello, A. (2008). Laws and regulations dealing with information security and privacy: An investigative study. [IJISP]. *International Journal of Information Security and Privacy*, 2(2), 70-82. doi:10.4018/jisp.2008040105.
- Clough, J. (2010). *Principles of cybercrime*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511845123.
- Commonwealth of Australia. (1995). *Criminal Code Act*. Canberra, Australia.
- Commonwealth of Australia. (2001). *Cybercrime Act*. Canberra, Australia.
- Commonwealth of Australia. (2007). *Older Australians at a glance*. Australian Institute of Health and Welfare. Canberra, Australia. Retrieved September 8, 2011, from <http://www.aihw.gov.au/WorkArea/DownloadAsset.aspx?id=6442454209>
- Commonwealth of Australia. (2011). *Inquiry into cyber-safety for senior Australians*. Joint Select Committee on Cyber-Safety. Retrieved August 25, 2012, from http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jsc/senior_australians/index.htm
- Connolly, C., Maurushat, A., Vaile, D., & van Dijk, P. (2011). *An overview of international cybersecurity awareness raising and educational initiatives*. Galexia Research. Retrieved March 13, 2012, from http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf
- Cook, D., Szewczyk, P., & Sansurooah, K. (2011, August 1-2). Securing the elderly: A developmental approach to hypermedia-based online information security for senior novice computer users. In the *Proceedings of the 2nd International Cyber Resilience Conference*, Perth, Australia (pp. 20-28).

- Corley, K., & Gioia, D. (2004). Identity ambiguity and change in the wake of a corporate spin-off. *Administrative Science Quarterly*, 49(2), 173–208.
- Creswell, J. (2003). *Research design: Qualitative, quantitative, and mixed method approaches*. Thousand Oaks, CA: Sage Publications.
- Denzin, N., & Lincoln, Y. (2005). *The handbook of qualitative research* (3rd ed.). Thousand Oaks, CA: Sage Publications.
- Dodge, R., Carver, C., & Ferguson, A. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73–80. doi:10.1016/j.cose.2006.10.009.
- Fire Eye. (2012a). *Spear phishing attacks: Why they are successful and how to stop them*. Milpitas, CA: Fire Eye.
- Fire Eye. (2012b). *Top words used in spear phishing attacks to successfully compromise enterprise networks and steal data*. Milpitas, CA: Fire Eye.
- Freeman, R., Wicks, A., & Parmar, B. (2004). Stakeholder theory and “the corporate objective revisited”. *Organization Science*, 15(3), 364–369. doi:10.1287/orsc.1040.0066.
- Friedman, M. (1992). Confidence swindles of older consumers. *The Journal of Consumer Affairs*, 26(1), 20–46. doi:10.1111/j.1745-6606.1992.tb00014.x.
- Gragido, W., & Pirc, J. (2011). *Cybercrime and espionage: An analysis of subversive multi-vector threats*. Rockland, MA: Syngress Media.
- Grimes, G., Hough, M., Mazur, E., & Signorella, M. (2010). Older adults’ knowledge of internet hazards. *Educational Gerontology*, 36(3), 173–192. doi:10.1080/03601270903183065.
- Hammond, R. (2003). *Identity theft: How to protect your most valuable asset*. Franklin Lakes, NJ: Career Press.
- Haukka, S. (2011). *Older Australians and the internet* (June). Brisbane, Australian: Creative Workforce Program, Australian Research Council Centre of Excellence for Creative Industries and Innovation (CCI).
- Heyman, K. (2007). New attack tricks antivirus software. *Computer*, 40(5), 18–21. doi:10.1109/MC.2007.179.
- Hough, M. (2004). Exploring elder consumers interactions with information technology. *Journal of Business and Economics Research*, 2(6), 61–66.
- Internet Crime Complaint Center. (2010). *ICCC annual report 2010*. Washington, DC: Bureau of Justice Assistance/Federal Bureau of Investigation.
- Jain, A. (2005). *Cyber crime issues, threats and management*. Delhi, India: Isha Books.
- Jakobsson, M., & Myers, S. (2007). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Hoboken, NJ: Wiley and Sons.
- Johnson, E. (2006). Security awareness: Switch to a better programme. *Network Security*, (Feb): 15–18. doi:10.1016/S1353-4858(06)70337-3.
- Johnson, K. (2003). *Financial crimes against the elderly. Trends and issues in crime and criminal justice, office of community oriented policing services, problem specific guide series No. 20*. Washington, DC: US Department of Justice.
- LaRose, R., Rifon, N., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3), 71–76. doi:10.1145/1325555.1325569.
- Lee, J., & Geistfeld, L. (1999). Elderly consumers’ receptiveness to telemarketing fraud. *Journal of Public Policy & Marketing*, 18(2), 208–217.
- Luo, X., & Guan, T. (2007). Defeating active phishing attacks for web-based transactions. [IJISP]. *International Journal of Information Security and Privacy*, 1(3), 47–60. doi:10.4018/jisp.2007070104.
- Lusardi, A., & Mitchell, O. (2007). Baby Boomer retirement security: The roles of planning, financial literacy, and housing wealth. *Journal of Monetary Economics*, 54, 205–224. doi:10.1016/j.jmoneco.2006.12.001.
- Mann, W. (1997). Common telecommunications technology for promoting safety, independence, and social interaction for older people with disabilities. *Generations (San Francisco, Calif.)*, 21(3), 28–29.
- Mansell, R., & Collins, B. (2005). *Trust and crime in information societies*. Cheltenham, UK: Edward Elgar.
- Marshall, A., & Tompsett, B. (2005). Identity theft in an online world. *Computer Law & Security Report*, 21(2), 128–137. doi:10.1016/j.clsr.2005.02.004.
- Martin, N. (2009). Consumer scams and the elderly: Preserving independence through shifting default rules. *The Elder Law Journal*, 17(1), 1–30.

- Masud, M., Khan, L., & Thuraishingham, B. (2007). e-Mail worm detection using data mining. [IJISP]. *International Journal of Information Security and Privacy*, 1(4), 47–61. doi:10.4018/jisp.2007100103.
- Metropolitan Life Insurance. (2011). *The Metlife study of elder financial abuse: Crimes of occasion, desperation and predation against America's Elders* (June). Metlife, New York, NY. Retrieved March 10, 2012, from <https://www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf>
- Miles, M., & Huberman, A. (1997). *Qualitative data analysis – An expanded case book* (2nd ed.). Thousand Oaks, CA: Sage Publications.
- Milhorn, H. (2007). *Cybercrime: How to avoid becoming a victim*. Boca Raton, FL: Universal Publishers.
- Mouallem, L. (2002). Oh no grandma has a computer: How internet fraud will take the place of telemarketing fraud targeting the elderly. *Santa Clara Law Review*, 42(1), 659–687.
- Norton. (2012). *The 2012 cybercrime report*. Mountain View, CA: Symantec Corporation.
- Osman, Z., Poulson, D., & Nicolle, C. (2005). Introducing computers and the internet to older users: Findings from the care onLine project. *Universal Access in the Information Society*, 4(1), 16–23. doi:10.1007/s10209-005-0111-8.
- Parmar, B. (2012). Protecting against spear phishing. *Computer Fraud & Security*, 1, 8–11. doi:10.1016/S1361-3723(12)70007-6.
- Rabiner, D., O’Keeffe, J., & Brown, D. (2006). Financial exploitation of older persons. *Journal of Aging & Social Policy*, 18(2), 47–68. doi:10.1300/J031v18n02_04 PMID:16837401.
- Reisenwitz, T., Iyer, R., Kuhlmeier, D., & Eastman, J. (2007). The elderly’s internet usage: An updated look. *Journal of Consumer Marketing*, 24(7), 406–418. doi:10.1108/07363760710834825.
- Reisig, M., Pratt, T., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior*, 36(4), 369–384. doi:10.1177/0093854808329405.
- Ross, S., & Smith, R. (2011). *Risk factors for advance fee fraud victimization, Paper No. 420 (August)*. Canberra, Australia: Australian Institute of Criminology.
- R. S. A. (2012). *RSA 2012 cybercrime trends report*. Bedford, MA: RSA Inc..
- Russell, C., Campbell, A., & Hughes, I. (2008). Research: Ageing, social capital and the Internet: Findings from an exploratory study of Australian ‘silver surfers’. *Australasian Journal on Ageing*, 27(1), 78–82. doi:10.1111/j.1741-6612.2008.00284.x PMID:18713197.
- Schell, B., & Martin, C. (2004). *Cybercrime: A reference handbook*. Santa Barbara, CA: ABC-CLIO.
- Schmallegger, F., & Pittaro, M. (2009). *Crimes of the internet*. Upper Saddle River, NJ: Prentice Hall.
- Schultz, E. (2004). Security training and awareness – fitting a square peg in a round hole. *Computers & Security*, 26(1), 1–2. doi:10.1016/j.cose.2004.01.002.
- Schultz, E. (2005). The human factor in security. *Computers & Security*, 24(6), 425–426. doi:10.1016/j.cose.2005.07.002.
- Selwyn, N. (2004). The information aged: A qualitative study of older adults’ use of information and communications technology. *Journal of Aging Studies*, 18(4), 369–384. doi:10.1016/j.jaging.2004.06.008.
- Selwyn, N., Gorard, S., Furlong, J., & Madden, L. (2003). Older adults’ use of information and communications technology in everyday life. *Ageing and Society*, 23(1), 561–582. doi:10.1017/S0144686X03001302.
- Sharpe, C. (2004). *Frauds against the elderly*. Jefferson, NC: McFarland & Co..
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010, April 10–15). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the 28th Conference on Computer-Human Interaction, CHI 2010: Imagine all the People*, Atlanta, GA. New York, NY: ACM Press.
- Smith, R., & Budd, C. (2009). *Consumer fraud in Australia: Costs, rates and awareness of the risks in 2008, Paper No. 382 (September)*. Canberra, Australia: Australian Institute of Criminology.
- Sophos Ltd. (2013). *Security threat report 2013*. Boston, MA: Sophos.
- Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security*, 3(2), 20–26. doi:10.1108/09685229510792988.
- Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. *Computers & Security*, 24(2), 124–133. doi:10.1016/j.cose.2004.07.001.

- Sum, S., Mathews, R., & Hughes, I. (2009). Participation of older adults in cyberspace: How Australian older adults use the Internet. *Australasian Journal on Ageing*, 28(1), 189–193. doi:10.1111/j.1741-6612.2009.00374.x PMID:19951340.
- Sylvester, E. (2004). Identity theft: Are the elderly targeted. *The Connecticut Public Interest Law Journal*, 3(2), 371–401.
- Symantec. (2011). *Internet security threat report volume 16*. Mountain View, CA: Symantec Corporation (April).
- Temple, J. (2007). *Older people and credit card fraud. Trends and issues in crime and criminal justice, Paper No. 343 (August)*. Canberra, Australia: Australian Institute of Criminology.
- The Association of Superannuation Funds of Australia. (2013). *Superannuation statistics* (February). Retrieved March 1, 2013, from <http://www.superannuation.asn.au/resources/superannuation-statistics/>
- The Financial Services Roundtable. (2010). *Protecting the elderly and vulnerable from financial fraud and exploitation* (April), BITS. Retrieved July 27, 2011, from <http://www.bits.org/publications/fraud/BITSProtectingVulnerableAdults0410.pdf>
- Thomson, M., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, 6(4), 167–173. doi:10.1108/09685229810227649.
- Trend Micro Inc. (2012). *Spear phishing email: Most favored APT attack bait*. Cupertino, CA: Trend Micro Inc..
- Tueth, M. (2000). Exposing financial exploitation of impaired elderly persons. *The American Journal of Geriatric Psychiatry*, 8(2), 104–111. PMID:10804070.
- UK Office of Science and Technology. (2004). *Cyber trust and crime prevention project: Gaining insight from three different futures*. London, UK: Crown.
- Vacca, J. (2003). *Identity theft*. Upper Saddle River, NJ: Prentice Hall.
- Wagner, N., Hassanein, K., & Head, M. (2010). Computer use by older adults: A multi-disciplinary review. *Computers in Human Behavior*, 26(5), 870–882. doi:10.1016/j.chb.2010.03.029.
- Walsh, M. (2003). Teaching qualitative analysis using QSR NVivo. *Qualitative Report*, 8(2), 251–256.
- Wooding, S., Anham, A., & Valeri, L. (2003). *Raising citizen awareness of information security: a practical guide. eAware Program*. Berlin, Germany: RAND Europe.
- Zagorsky, J. (1999). Young Baby Boomer's wealth. *Review of Income and Wealth*, 45(2), 135–156. doi:10.1111/j.1475-4991.1999.tb00325.x.

Nigel Martin is a senior lecturer of information systems and management, and a senior researcher at the National Centre for Information Systems Research (NCISR) at the Australian National University (ANU), Canberra, Australia. He received his PhD in enterprise and security architecture at the ANU, while holding several executive level roles in the Department of Defense. His current research interests include privacy and security, and IT management and strategy. His previous publications appear in journals such as Information Technology and People, Behavior and Information Technology, and Computers and Security.

John Rice is a senior lecturer in international business at Griffith University, Queensland, Australia. He is also a researcher at the National Centre for Information Systems Research (NCISR) at the Australian National University (ANU), Canberra, Australia. His PhD was undertaken at Curtin University, Western Australia studying international strategic alliances adopted in the Finnish telecommunications industry (particularly Nokia). His current research interests include strategic management, technology innovation, and knowledge and information management. His previous publications appear in journals such as Research Policy, Training and Education, Behaviour and Information Technology, Computers and Security, and the Journal of Business Ethics.

APPENDIX

Table 5. Summary of stakeholders (Commonwealth of Australia, 2011)

Stakeholder Group	Stakeholder/s Function and Description/Scope
Government organizations (GOs) (14)	<p>GO1. Australian Communications and Media Authority – responsible for the regulation of broadcasting, the internet, radio communications and telecommunications (659 staff; Services cost A\$110 million, 2011).</p> <p>GO2. Australian Crime Commission – coordination services for domestic crime prevention (628 staff; Services cost A\$96 million, 2011).</p> <p>GO3. Australian Department of Broadband, Communications and the Digital Economy – policy agency for telecommunications, broadcasting and the digital economy (692 staff; Services cost A\$126 million, 2011).</p> <p>GO4. Australian Department of Health and Ageing – health and ageing policy and program delivery and regulation (4,500 staff; Services cost A\$45.5 billion, 2011).</p> <p>GO5. Australian Department of Veteran's Affairs – policy and program delivery and regulation for retired and past defence force members (2,051 staff; Services cost A\$12.3 billion, 2011).</p> <p>GO6. Australian Federal Police – federal level law enforcement and diplomatic protection (6,500 staff; 3,000 police officers; Operating budget A\$1.8 billion, 2011).</p> <p>GO7. Australian Human Rights Commission – legal protection of the human rights of all Australians (126 staff; Services cost A\$14.6 million, 2011).</p> <p>GO8. Australian Institute of Criminology – informed policy research on crime and criminal justice (52 staff; Services cost A\$9 million, 2011).</p> <p>GO9. Frankston City Council – supporting city of 120,000 people of which approx. 20% are over the age of 50 years (1,108 staff; Operating income A\$137 million, 2011). Views from the Older Persons Reference Group.</p> <p>GO10. Hobart City Council – supporting city of 50,000 people of which approx. 15% are over the age of 65 years (600 staff; Operating revenue A\$96 million, 2011). Views from the Older Persons Reference Group.</p> <p>GO11. National eHealth Transition Authority – rollout/support electronic health initiatives and solutions (257 staff; Retained funds A\$56 million, 2011).</p> <p>GO12. National People with Disabilities and Carer Council – government advisory body for disability and caring relationships (29 independent members)</p> <p>GO13. Tandara Lodge Community Care Inc – 41 permanent and palliative care older persons in Northern Tasmania region.</p> <p>GO14. Western Australia State Government – deliver state policy and programs for Western Australia (Over 100,000 staff; Operating revenue A\$25 billion, 2011).</p>
Non government organizations (NGOs) (10)	<p>NGO1. African Seniors and Elders Club Australia Inc. – promotion of community services for older African persons living in Brisbane, Queensland. Over 300 older age members.</p> <p>NGO2. Australian Library and Information Association – promotion and delivery of library/information services (over 6,000 members; Operating revenue A\$3.5 million).</p> <p>NGO3. Australian Seniors Computer Clubs Association – encourage older people to adopt IT and computing for quality of life enhancement. Over 45,000 older age computer/Internet users.</p> <p>NGO4. Brotherhood of St Laurence – non-government social welfare and charitable community organization (over 600 staff and 1,300 volunteers; Operating revenue A\$62 million). Aged and older persons services.</p> <p>NGO5. Centre for Internet Safety, University of Canberra – thought and policy leadership for Internet safety (2 staff from the area of policing and law enforcement).</p> <p>NGO6. Consumers Health Forum of Australia – peak advocacy body for healthcare services consumers and industry (15 staff; Operating revenue A\$0.5 million).</p> <p>NGO7. Legacy Australia Council – supporting over 100,000 family members of deceased/incapacitated military service staff. Over 6,100 volunteer staff in 49 clubs.</p> <p>NGO8. Life Activities Clubs Victoria Inc. – over 5,000 members/older persons in 22 clubs (incl. computer/Internet clubs).</p> <p>NGO9. Moorooka (Queensland) Neighbourhood Watch – small suburban crime prevention cooperative. Population of 8,600 citizens.</p> <p>NGO10. National Seniors Australia – social, benefit and advocacy support for people 50 years and over in Australia. Membership of approx. 250,000 citizens.</p>
Public and private companies (PPCs) (2)	<p>PPC1. eBay (incl. PayPal) – Internet business with operating revenues over US\$11.6 billion and over 27,800 staff.</p> <p>PPC2. Telstra – Australian media and telecommunications firm with operating revenues over A\$25 billion and over 35,700 staff.</p>
Individuals (IND) (3)	<p>IND1. 81 year old adult male with mother who is a victim of over A\$200,000 advance fee fraud over the Internet.</p> <p>IND2. 83 year old adult male with son who is a victim of over A\$1,300,000 advance fee fraud over the Internet.</p> <p>IND3. 70 year old adult male who is a victim of a A\$250 advance fee fraud (Russian dating scam) over the Internet.</p>