1-1-2011

Seniors language paradigms: 21st century jargon and the impact on computer security and financial transactions for senior citizens

David M. Cook
Edith Cowan University

Patryk Szewczyk
Edith Cowan University

Krishnun Sansurooah
Edith Cowan University

DOI: 10.4225/75/57b52d42cd8b8
9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

SENIORS LANGUAGE PARADIGMS: 21ST CENTURY JARGON AND THE IMPACT ON COMPUTER SECURITY AND FINANCIAL TRANSACTIONS FOR SENIOR CITIZENS

David M. Cook, Patryk Szewczyk, Krishnun Sansurooah
secau Security Research Centre, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
d.cook@ecu.edu.au

Abstract

Senior Citizens represent a unique cohort of computer users insomuch as they have come to the field of computer usage later in life, as novices compared to other users. As a group they exhibit a resentment, mistrust and ignorance towards cyber related technology that is born out of their educational and social experiences prior to widespread information technology. The shift from analogue to digital proficiency has been understated for a generation of citizens who were educated before computer usage and internet ubiquity. This paper examines the language difficulties encountered by senior citizens in attempting to engage in banking and communications that now rely heavily on internet connectivity and computer expression. In particular, this research exposes a generational problem facing senior citizens in the security of their financial assets.

Keywords
Senior novice users, senior citizens, novice users, online security, elderly, phishing, spoofing, patching.

INTRODUCTION

Computer security is rapidly overtaking other cyber disciplines through the need for safe systems, secure banking, and identity protection. Just as internet usage has become ubiquitous, in its shadow the requirement to secure internet usage has similarly expanded. This expansion has brought about a new language of terms that describe and categorise novel areas as they emerge. Acronyms abound, terminology evolves, and the need to keep abreast of emerging terms becomes a necessity for a much wider audience than computer programmers and software developers. This paper will argue that one of the inherent limitations of computer security is its inability to articulate key messages in a manner that can be interpreted and understood by the wider population. At the forefront of the security "gap" is the distance between senior citizens and younger counterparts (Cook, Szewcyzk, & Sansurooah : 2011) .

Novice users such as children share a number of learning characteristics that define their generation. Generation Z citizens quickly absorb new technology. They share technology freely and with very few inhibitions. In terms of security and identity protection they are fearless, often posting large and significant pieces of identity-significant data that can be used by others. Whilst their identity and information may be vulnerable to attack, their (current) nett value and assets is relatively small. In stark contrast, senior novice users (perhaps best categorised as Golden Baby Boomers) are cautious and restrained (Cook et al. 2011). They have significant assets built over a lifetime of employment which in many cases may be vulnerable through online banking and default cyber-technology of financial data and information. Elderly novice users have a different frame of mind, largely shaped by their enforced exposure to new norms such as internet banking, online information services, and computer-reliant communications systems (Ellis & Kurniawan 2000).

Senior citizens represent a unique legion of computer users because in general terms the sum of their occupational and vocational contributions have required significantly less direct interaction with computing systems. At the professional end of the employment spectrum, senior company executives have enjoyed decades of secretarial support, middle management, and hierarchical business structures, many of which have allowed their computer interaction to be fed indirectly, with the support of other workers who have more up to date skills and are more conversant with 21st century computer opportunities. At the vocational end of the employment spectrum, traditional skills in manual employment such as welding, building, and mechanics have been successfully enjoyed by Golden baby boomers in the latter half of the twentieth century without the need for major shifts in retraining or up-skilling in computing. In the retail area, shopkeepers and supermarket workers

have all enjoyed careers that have been largely free for the need to become highly skilled or proficient in computing.

For younger baby boomers and post baby boomers the engagement with, and acceptance of, computing skills has occurred far more easily. Younger users accept cyber systems largely without question. Middle-aged users have been attracted to computing as a means to improve and achieve greater efficiency. Yet senior citizens as a group do not share the same appreciation for computer-facilitated communication. For many, the salad days of the 20th century are largely cyber-free. Seniors who are novice users are more deeply disadvantaged through a range of somewhat obvious issues such as font size, background colour, and language (Ball, 2008). In many instances there is widespread hesitancy, resentment and confusion of computing and cyber-related technology acceptance. Once-relatively simple procedures such as banking and financial transactions were previously made through face to face interactions. Bills were paid in person, money was deposited by queuing in line at banks, and pay packets were delivered in cash inside envelopes. The requirement for cyber-facilitated compliance of everyday financial transactions is a relatively novel aspect for senior citizens.

THE SECURITY PERILS OF MODERN BANKING

For senior citizens, the shift from traditional banking arrangements to modern de-regulated assets management represents a significant threat through previously non-existent vulnerabilities. For senior citizens, the shift from a tangible passbook savings account to online banking has left large numbers of elderly people afraid and uncertain about financial matters. Incorporating even a four digit password for account access can be a daunting change for experienced bank customers who have committed a lifetime to saving and spending their money using transactions that required their personal and physical presence. The shift to pin codes, passwords and online transactions is misunderstood by seniors whose lifetime experiences are built on a foundation of face to face encounters, written and signature-endorsed communications, and the physical interaction of ink on paper, handshake commitments, and personal trust. Novice users of online systems are prone to navigate web-based systems by means of a superficial approach where ease of use takes prominence over thorough methodical interaction (Ciampa, 2010). The shift to modern banking therefore asks significantly greater normative demands of many senior citizens than is anticipated. Security protocols and procedures may take a back seat to connectivity at whatever the cost. The shift towards efficiency of time and effort is a problematic feature of all internet usage. (Dodge, Carver, & Ferguson, 2007). The acceptance of online banking is, however, a two way street. The pathway to protecting one's financial assets as well as one's identity and security now require senior citizens to embrace technology or ignore it at their own peril (McCloskey, 2006).

Online Instructional Banking Security Literature

In order to establish an understanding of the security issues facing Senior Citizens, a review of the big four banks (Murdoch 2009) known as: National Australia Bank (NAB); Commonwealth Bank; Westpac; and Australia and New Zealand Banking Group (ANZ), was undertaken. The review focused on the language and terminology used to describe the necessary procedures for secure online banking. All four of the banks used the ten terms: Virus, Spam, Worm, Trojan, Phishing, Hypertext, HTTPS, Patches, Spoofing and Cookies. Each bank incorporated the terms into their online information portals using different approaches. The Commonwealth Bank (Commonwealth Bank 2011a) used a conversational approach to security information by means of a series of short videos. Whilst the language used was straightforward, some terms were explained whilst others were assumed. National Australia Bank (NAB) used more technical language and did not explain any terms. Words such as "Spoof" and "Spoofing" were used alongside words such as "Hoax" so as to imply a meaning, even though no specific meaning was given (NAB 2011). The ANZ bank was slightly more comprehensive with clearer explanations of the words "Phishing, Viruses, Worms and Trojans" and a simple drop down tab to explain some key terms (ANZ 2011b). Westpac had no direct explanation of key terms, but instead relied on customers searching via the "ask an expert" link (Westpac 2011). None of the four big banks explained all ten terms in a manner that would allow for consistent understanding of the terms as used in ordinary conversation.

Whilst it is possible to infer a meaning from many of the terms used in each of the four banks' online information pages, the use of these terms is deployed from the assumption that readers already understand their meaning. In some cases the meaning may be obvious, whilst in others there is a lack of intuitive or instinctive connotation. It is possible to search and reveal meanings to each of the terms, but they are used under an expectation that the reader already has a clear understanding of their implications and importance. No distinct

solution has materialised to put forward reliable direction for novice users, nor ‘golden’ baby boomers who present in novice form (Lusardi & Mitchell, 2007).

An understanding of the key cyber issues for Senior Citizens therefore needs to look beyond existing informational offerings about online banking and consider some past perspectives in determining security vulnerabilities that are born out of both governance and social norms and values. Prescriptive language may command less respect, especially where a dogmatic approach assumes understanding rather than assuming that for some people, specific terms and acronyms that have not been used in common language with their current meaning. The most secure financial encryption of an online banking system is worthless if the customer using it does not trust it to replace their own personal stance on finance security. Similarly, if a user finds it difficult to remember passwords, he or she may resort to keeping confidential password information nearby to computers, or where they are vulnerable to acquisition and use by someone other than themselves. In terms of online banking and bill paying, personal security is now much more heavily reliant on self-awareness, personal comprehension of computing security issues, and systems comfort (Dickinson, Newell, Smith, & Hill, 2005). In part, this mistrust of systems is accompanied by ignorance and confusion. The use of terminology that is both new and linguistically different, is depicted by the following pilot study of Senior Citizens.

METHOD

This research specifically looks at the interactions of novice elderly computer users. It asks "how do novice elderly computer users engage with computing and can their differences enable a better approach to personal computer security within this cohort?" Researchers interviewed 183 senior citizens from the northern suburbs of Perth as part of a series of information and discovery sessions on computer security for seniors. The information sessions were held between June and September 2011. Attendees at the sessions were present because they wanted more information about computer security, identity theft, and online banking security. Participants came from: two non-profit groups; four local branches of the National Seniors Australia organization; and three public libraries under the State Library of Western Australia. This was a total of seven distinct groups totaling 183 contributors. Attendance at the sessions was free and voluntary, and participants answered interview questions within the information sessions as part of the group interactions and discussions. Participants came to the sessions expecting to learn how to increase their computer security and how to deal with identity theft.

Initial discussions attempted to encourage participants to think about their current computing interactions and experiences (Riva 2001). Participants were asked “Are you keen to know more about computing, or do you feel “forced” into having to use computers or computerized systems?”. In group discussions there was a range of answers to this question that reflected a diversity of opinion in regards to how keen people were to embrace computing. All participants were keen to learn about computing, whilst every discussion group had several contributors who cited difficulty in understanding new words that appeared to be a new language. For some, there was concern about why there was a need for such confusing terms and acronyms.

After the general group discussions regarding computer usage and security issues of concern, participants were asked to respond individually to specific questions about how they used computers. They were then asked questions in regards to specific terms and acronyms that were used in explaining a range of security strategies that could be used to reduce their personal vulnerability to computer security breaches with particular emphasis on identity theft and financial banking. Of the 183 participants 145 (79%) responded to the effect that they felt compelled to use computing systems. The most common response was in regards to banking, and the direction of financial institutions to accept online banking, online statements, and the need to pay bills online in order to minimize fees and charges. Of the 145 respondents who felt compelled, 128 (70%) felt that they had little choice, but that they held concerns for the security of their finances. Notably 13 (7%) participants stated that even though they did not own a computer, they felt that they needed a computer if they were to retain control over their banking and finances. A further 22 participants (12%) explained that they relied on some assistance from family and friends to either access banking or make financial transactions.

Participants were asked to explain what their main concerns were regarding security. Again, a variety of responses were recorded. The most frequent response was regarding identity theft. A common theme across all information sessions and discussion groups was that whilst many participants attempted to understand computer security, they were constantly faced with a problem of understanding computer terminology. Many participants spoke of confusion when reading online banking information regarding computer security and identity theft. Of

the 183 participants 155 (84%) responded that they did not understand some of the computer terms and acronyms. Each group information session agreed that there were several words that appeared new, or that they assumed must have a new meaning. The chart (Table.1) below indicates the level of understanding of 10 key terms that the respondents were asked in order to indicate their level of understanding about computer security terms.

Table 1. Understanding of Computer Security Terms and Acronyms by Senior Citizens

Key Terms and Acronyms	Has a Clear Understanding of Term	Unsure but some understanding	Does not understand term at all
Virus	35 (19 %)	71 (39%)	77 (42%)
Spam	32 (17.5%)	85 (46.5%)	66 (36%)
Worm	24 (13%)	34 (18.5%)	125 (68.5%)
Trojan	31 (17%)	33 (18%)	119 (65%)
Phishing	11 (6%)	30 (16%)	142 (78%)
Hypertext	0 (0%)	5 (3%)	178 (97%)
HTTPS	0 (0%)	5 (3%)	178 (97%)
Patches	5 (3%)	22 (12%)	156 (85%)
Spoofing	3 (1.5%)	29 (16%)	151 (82.5%)
Cookies	12 (6.5%)	60 (32.5%)	111 (61%)

DISCUSSION

In all of the discussion groups there was widespread agreement that individuals thought that using computer-based banking systems appeared to be riskier than face to face banking and bill paying. Most participants were defensive in regards to their ability to understand financial banking systems. Seniors groups demonstrated a high level of financial understanding in group discussions. However all groups pointed to the security of their identity, and to a lack of understanding of certain words and terminology used to describe methods for protecting computer security. Groups also collectively raised concerns regarding the security of financial information that they could access online.

Of the ten terms and acronyms presented to respondents, the most understood terms appeared to be the terms “virus” and “spam”. Yet even with these terms less than one in five respondents felt that they had a clear understanding of how a virus could impact upon the security of their identity information and the security of their financial transactions. Many of the groups showed a general understanding regarding the propensity for a computer to become infected, yet significant numbers of individuals were hesitant to relate virtual concepts to physical concepts with any great conviction.

The least understood term was “HTTPS”. No group contributors knew that HTTP stood for Hypertext Transfer Protocol (Stallings 2007), and none of the participants understood that HTTPS included encrypted communication and secure identification of a network webserver. Since in the review of online bank literature all four major banks in Australia referred to the term HTTPS as important in establishing secure links to online banking, the finding that senior computer users do not understand the term HTTPS indicates a problem with regard to secure banking connections. In all of the discussion groups there was widespread acknowledgement that no one understood any significant difference between HTTP and HTTPS for online banking. Only after repeated instruction regarding the need to connect using a secure connection was there any indication within groups that HTTPS was a necessary identifier for more secure online banking conditions. Many contributors cited their difficulty with HTTP and HTTPS as such similar terms that confusion was likely, especially since no one could remember the full meaning of the acronyms, or assign any real understanding to their terms. Every group asked a similar question along the lines of “why can’t we simply replace the terms HTTP and HTTPS with terms such as “Secure Connection” and “Unsecure Connection?”.

The terms “Worms”, “Trojans’ and “Cookies” all met with limited understanding. All three terms had more than 60 percent of respondents admitting that they did not understand these terms at all. There was some discussion surrounding the connection to a Trojan Horse, and the idea of a threat hiding inside a piece of downloadable software, but for the terms “Worms” and “Cookies’ the general consensus of opinion was that these terms held little meaning or value for seniors.

The term that generated the most active discussion was 'phishing', with 78% of the respondents claiming that they did not understand the term at all. A further 16% said that they had some understanding whilst only 6% of respondents claimed to have a clear understanding of the term. Many participants described the terms as a nonsense word. Several went further to describe it as a term not to be found in the English dictionary. Most agreed that when they saw the term they were either confused or likely to disregard the informationt.

The term 'Patches' was deemed by 85% of the respondents to have little meaning to them. Despite this, in the group discussions, all of the groups spoke repeatedly about the need to update their software and to update their computer against threats. Very few (3 percent) of the respondents made a clear connection between the term 'Patching' and the need to fix software bugs and to update using software add-ons. Again, the concept of updating computers was understood, but the key supporting terminology was largely misunderstood.

As with "Patching", the term "Spoofing" held little significance. More than 82% of respondents did not understand the term. In most of the group discussions, each time the word "Spoofing" was used, several participants claimed disapproval at the use of vulgar terminology. For at least some participants, the connection between spoofing and computer technology was that it represented something offensive. Less than 2 percent of the participants understood that spoofing related to forged sender addresses for the purpose of social engineering.

Throughout each of the group discussions, the underlying theme that recurred was that certain terms and acronyms appeared new, invented, or simply not normal terms that one might expect to use in the conversation. Many Senior Citizens felt that they had a better than average understanding of the English language, and that the introduction of certain terms represented a collection of jargon that was unhelpful in gaining a clearer understanding of safe and secure online computing. The range of feelings was diverse, however the premise of jargon terminology was consistent amongst all participant groups. Terms that were meant to convey serious meaning and prevent or reduce threats to computer security were more commonly regarded as lingo, jargon, and gobbledygook.

Ambiguity over "Confidential" Information

In addition to the discussions of key terms, many of the participants spoke of confusion arising from understanding what is classed as confidential information. Group discussions made reference to online information from banks citing that they would never ask for confidential information in an email or phonecall to customers. Yet many respondents mentioned confusion when communicating by phone with banks.

Respondents cited instances where they were required to reveal date of birth, mother's maiden name and recent transaction history in order to continue telephone communications with some banks. The Commonwealth Bank in its "Online Security" video states that it will never ask for confidential information in an email. It further states that any attempt to gain this information from a customer is clearly a scam. Yet in group discussions seniors claimed difficulty in knowing what is "confidential information". In contrast to the Commbank video, the Commonwealth Bank will ring and ask to confirm some details before proceeding with a telephone call. Other major banks follow a similar practice of customer verification over the phone. All of the seven discussion groups declared confusion in determining the difference between confidential information and what is deemed as necessary information to establish identity.

The paradox about information for computer security users of poor understanding is that senior novice computer users represent the intended target of those engaged in phishing, social engineering, and scamming (Pfleeger and Pfleeger, 2007). A vicious circle of under-awareness, confusion and ambiguity prevails. Computer fluency and understanding has settled into two major conduits. On the one hand, younger novice users swiftly attain skills and become adept at navigating web-based media and online systems. Older novice users become increasingly cautious about financial online interactions with severe consequences. Both pathways attract more frequent use as the popularity of social media coupled with the inherent usefulness of the internet evolves.

CONCLUSION

Although only a small representation of Senior Citizens, this small pilot study reveals significant and stark divisions in the understanding and acceptance of key terminology relating to computer security, online banking, and trust. Each group of participants had a direct interest in computer security, online banking and identity theft, however an extremely low proportion across all groups of contributors were intuitively positioned to make

sense of key terms and acronyms. In some cases the lack of understanding meant a significant disconnect from the key security message behind each term. In other cases the problem extended to mistrust and ignorance. Given the severe lack of comprehension and identity with key terms, the researchers intend to extend this study into a much wider section of the Seniors community. There is a clear difference between the uptake of key security descriptors by senior citizens when compared to general online computer users. Senior citizens may be ignoring critical information regarding the safety and security of their identity and their financial assets when exposed to online transactions and online banking.

REFERENCES

ANZ (2011a) Ways to Banking; internet Banking, retrieved on September 13th at http://www.anz.com.au/personal/ways-bank/internet-banking/?sourcecode_1=ref_ppc_bs09_brand_google_1070&s_kwcid=TC|21211|a%20n%20z%20online%20banking||S|e|6284722084

ANZ (2011b) Internet Security Threats, retrieved on September 13th at http://www.anz.com.au/personal/ways-bank/internet-banking/protect-banking/security-threats/

Ball, S. (2008) Design for all – how web accessibility affects different people. In Craven (Ed.) *Web accessibililty: practical advice for the library and information professional*. London: Facet publishing.

Ciampa, M. (2010) Security Awareness: Applying Practical Security in your world, Third Edition, Boston: Cengage

Commonwealth Bank (2011a) Security and Privacy, retrieved on September 13th at http://www.commbank.com.au/security-privacy/

Commonwealth Bank (2011b) Online Security, retrieved on September 13th at http://www.commbank.com.au/security-privacy/videos/online-security.aspx

Cook, D.M., Szewcyzk, P., & Sansurooah, K. (2011) Securing the Elderly: A Developmental Approach to Hypermedia-Based Online Information Security for Senior Novice Computer Users, Proceedings of the 2nd International Cyber Resilience Conference, Perth, Australia: Edith Cowan University August 1st and 2nd 2011.

Dickinson, A., Newell, A.F., Smith,M.J., and Hill, R.L. (2005) Introducing the Internet to the over-60s: Developing an email system for older novice computer users, *Interacting with Computers*, Vol 17 Issue 6 pp 621-642.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Ellis, R. D., & Kurniawan, S.H. (2000) Increasing the Usability of Online Information for Older Users: A Case Study in Participatory Design, *International Journal of Human-Computer Interaction*, Vol 12 Issue 2, pp 263-276.

Lusardi, A & Mitchell, O.S. (2007) Baby Boomer retirement security: The roles of planning, financial literacy, and housing wealth, Journal of Monetary Economics, Volume 54 Issue 1 pp205 - 224, Retrieved March 25th, 2011 from http://www.sciencedirect.com/science

McCloskey, D.W. (2006) The Importance of Ease of Use, Usefulness, and Trust to Online Consumers: An Examination of the Technology Acceptance Model with Older Consumers, *Journal of Organizational and End User Computing*, Vol 18 No.3

Murdoch, S (2009) The Big Four banks have joined the Global Elite, Business with the Wall Street Journal, retrieved on August 3rd 2011 from http://www.theaustralian.com.au/business/breaking-news/big-four-join-global-elite/story-e6frg90f-1111118663656

NAB (2011) Three Tips for Online Security, retrieved on September 13th at http://www.nab.com.au/wps/wcm/connect/nab/nab/home/personal_finance/12/3/11/nab_article_098103

Pfleeger, C. P. and Pfleeger, S. L. (2007) Security in Computing, Fourth Edition, Boston: Pearson, Prentice Hall

Riva, G. (2001) The Mind over the Web: The Quest for the Definition of a Method for Internet Research, *CyberPsychology and Behaviour*, vol4, No.1. pp7-16.

Stallings, W. (2007) Network Security and Essentials: Applications and Standards, 3rd Edition, New Jersey: Pearson Education International

Westpac (2011) Personal Banking: Online Security, retrieved on September 13th at http://www.westpac.com.au/personal-banking/westpac-online/security/