Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and Phishing Attacks.

Premankit Sannd$_1$, David M. Cook$_2$
School of Science
Edith Cowan University
Perth, Australia
d.cook@ecu.edu.au

Abstract—Despite the variety of global research on the identification and proliferation of ransomware and other online scams, there is still a relative vacuum of research with respect to the problem of digitally and socially engineered deception in the form of ransomware on an individual. This is particularly problematic for older cohorts, where life experience in many endeavours sits alongside novice understanding and experience in the use of online technology. This paper examines the indicators that characterize authenticity and deception within ransomware and phishing. A survey of older Australian people over the age of 65 reveals markers and patterns that assist the user to determine likely deception using non-cyber skills. The paper outlines a grammar and syntax-derived framework to assist older users in the ability and awareness to recognize fraudulent emails.

Keywords—elderly, grammar, ransomware, seniors, syntax

I. INTRODUCTION

Older people represent a challenging segment of the online usage demographic in terms of cybersecurity. Older people are developing a growing proportion of the overall population. For over twenty years since 1996 there has been a marked increase in the population growth of people over the age of 65. This trend is expected to further increase with a predicted growth of 15.3% by the year 2026 [1]. In concert with this trend, there is an escalation in the need for digital literacy and digital proficiency with older cohorts [2], [3]. Australian citizens over the age of 65 are digitally less knowledgeable and less erudite than other cohorts, with 34% of older men and 30% of older women having only basic digital skills and capabilities [4].

Due to the increase in cyber fraud, scams and financial crimes, it is challenging for older people to fully trust digital technology [5], [6]. Since older people are limited in their online experience in terms of literacy, digital fluency and security, older people can benefit from an authenticity approach that allows older people to use their generationally superior language skills. Such abilities are evident in terms of grammar, syntax, and socially constructed narratives that appear in the form of offers, requests and commonplace styles of email communication. Despite the extended capabilities of older people, they remain vulnerable to a range of socially constructed offers present in the form of phishing and ransomware attacks [7].

This paper examines the responses from older people regarding their ability to recognize phishing and ransomware offers that are distributed through email and social media. A sample of older adults (*n=63*) reveals two main vectors of concern. The first is in the ability for older adults to differentiate between authentic emails and deceptive emails. This qualitative research considered older adults' perceptions of authenticity based upon grammar, syntax and the associated authenticity of the context. The study examined the role of grammar and syntax in recognizing fraudulent email communications that relate to phishing and ransomware. The second part uses an analysis of a sample of 21 known ransomware and phishing attacks through the lens of grammatical and syntax-related diversity. In some cases, the syntax and associated context might indicate a fraudulent proposition by means of a title or opening statement. In other situations, the key indicators of deception are more closely associated with an inconsistent use of normalized English language. Alternatively, the deception can be more easily identified where email addresses appear to lack corporate organizational credibility. Rather than examine the method of delivery or analyses the payload of different variations of ransomware, this study examines the contextual and grammatically structural indicators in email-based attacks that can assist older adults to make more accurate judgements when opening email communications.

II. BACKGROUND AND LITERATURE

Social engineering is well documented as an effective strategy in the deception of novice technology users [8]. Cohorts of older people universally show susceptibility to fraud and deception using online technology [9]. This is particularly observable in variations of phishing and ransomware [10], [11].

Ransomware represents a subset of malicious software that is diffused through a range of electronic mail and messaging formats. These include file attachments in emails and advertising-supported software. At the moment that the software is triggered, ransomware encrypts the files and scrambles the normal access criteria for the computer. Victims are invited to pay a sum of money in the form of a ransom in exchange for a key that de-crypts the otherwise secured files [12]. Ransomware works by deploying various attacks, most notably as either social engineering or as phishing. In the majority of cases these attacks are delivered by means of a malicious hyperlink [13]. Ransomware attacks are often delivered as part of a scatter-gun approach rather than through pre-determined and specific targeting. Such attacks are commonly linked to an opportunity or chance opening [14]. Online threats using ransoms are known to impact a variety of business areas. IT Security specialist firms including Delloite, McAfee, and Malware bytes, state that the industry effects of ransomware are particularly challenging on industries such as health-care, teaching and learning, and critical infrastructure in the form of utilities such as power, electricity and gas. In the case of the WannaCry ransomware release, more than 300,000 computers were affected within a timespan of less than 24 hours. [15].

Most perpetrators of ransom-based attacks invite victims to pay using an untraceable crypto-currency (eg: Bitcoin), in order to evade identification by financial banking systems and online currency gateways [16]. Single victims are repeatedly asked for payments in the range of two hundred to eight hundred dollars, however much larger ransom payments have been recorded, usually in concert with specific deadlines that force the victim to believe they need to make immediate payments so as to prevent the access to their files from being permanently lost [17].

Older people rely on online systems in order to take control of their day to day bills, banking, and financial management. With an increasing dependency on online banking, coupled with low levels of digital literacy, older adults are primary targets for cyber-based scams that prey upon a collective perception of security and trust in others [18]. The challenge of reducing the number of older adults from becoming targets of ransomware is growing alongside the proliferation of social engineering, Sybil accounts, and fake emails from seemingly trustworthy firms and institutions [19]. The entrapment of older people by means of fraud and deception is driven by the human participation in the emotions of anticipation, blame, curiosity distress and greed [20], [21], [22]. The majority of ransomware events are distributed through electronic mail and online messaging. Email deception is based on fake images, non-authentic logos, and technical data such as dates, serial numbers, and validation codes. Despite these tactics, ransom-based email attacks are widely known to include grammar, syntax, and spelling errors [23]. A 2016 report from the United Kingdom identified that 53% of older people are predisposed to falling victim to fraudulent email stings [24].

Ransomware attacks and social engineering events are known to have a significant impact on the victims of cybercrime. The 2017 Veda Banking report characterizes the impact of such incidents as far greater than simply incidents of financial loss, with known impacts extending to psychological and emotional concerns, with victims suffering from reputational fears, and ongoing anxieties about identity loss [25], [26]. The Australian Crime Commission (ACC) has concluded that many older Australians remain unaware of their victimization, whilst others recognize elements of a deception but without the ability to understand the online method by which they have been electronically defrauded. This has far-reaching consequences, not least of which are issues of reputation, and subsequent reluctance to report ransomware by either individuals or institutions. Mental and emotional anguish from these attacks has been associated with episodes of misery, apprehension, worry, and personal and familial injury suffered by victims and their associates. Further distress can arise from the emergence of spam and perceived addition threats that may re-emerge from the hardware and software of a victim's computer network [27], [28], [29].

III. METHOD

This research came about in two parts. The first part centres on a survey of 63 people (*n = 63*) and their responses to known examples of phishing and ransomware. The project aimed to examine whether people could recognize examples of phishing and or ransomware as malicious through the recognition of syntax, grammar, spelling, formatting and their associated contextualized irregularities. Participants were shown examples of email-based ransomware and asked their opinion about its validity as a genuine communication.

The second part of the research involved the collection of known images of ransomware and phishing attacks directed at older people. A sample of 21 images was collated and analyzed. The images were examined for the positioning and prominence of irregular markers in the form of grammar, spelling, syntax and associated contextualization. These markers were then further segmented to determine indicators of influence and easy recognition. The markers were divided into four subcategories. as follows: title, the body of text, distinguishing between errors in Titles, in email addresses, in the body of the text, or in closing statements. (Table I)

TABLE I. INDICATOR SEGMENTS OF DECEPTION

	Indicator segments within Likely Fraud and Deception
1.	Title
2.	Body of Text
3.	Closing Statements
4.	Email Addresses / URLs

IV. DISCUSSION AND FINDINGS

A. *Identify the Brand Recognition and Associated Misguided Trust and Acceptance*

Older adults over the age of 60 participated in research to reveal their awareness and understanding of ransomware, as well as each participant's ability to recognize ransomware, phishing, and online deception and fraud. The findings revealed that older adults placed greater trust in an email displaying a well-known brand, than in their own reading of the same email to check for context-based grammar and syntax errors (Table II). In one example, participants reviewed an email containing ransomware that used an Australian trusted brand "Australia Post". By using a brand that is regarded as trustworthy, cybercriminals can establish a sense of trust that allows some participants to overlook any grammatical or syntax-based errors. In isolation, errors such as spelling, and grammar are useful indicators of likely phishing, often indicating that the composer of the phishing is writing from a second or third language, rather than using their mother tongue. Approximately one third (32%) of participants indicated that they trusted the brand "Australia Post" but were suspicious of grammatical awkwardness within the written text of the email message. Additionally, 46% of older participants acknowledged that they could identify grammar and syntax errors, but still felt that they could trust the email (see Table II).

TABLE II. GRAMMAR AND SYNTAX INDICATORS

Concern over Grammar and Spelling mistakes in emails with a known brand.	
Percentage of Participants with Concerns over grammar and spelling mistakes	16%
Percentage of Participants with No Concerns over grammar and spelling mistakes	38%
Percentage of Participants who could see the grammar and Spelling mistakes but decided to ignore the errors.	46%

The results show that older people are capable of misjudging phishing and ransomware deployments through emails. Some older people allow their recognition of a well-known brand to override their normal evaluation of emails, in this case, to reveal grammar and spelling errors, and to subsequently treat the email with a greater level of trust that if it were evaluated in a stand-alone mode. Many of the participants could identify and acknowledge something wasn't quite right, and that elements of the email seemed awkward and clumsy.

> *"I'm fairly sure this is a scam. I can't quite work it out for sure. But it doesn't seem quite right. The words don't seem right. The first line that says "thus the receiver was absent" isn't right. I mean the post office wouldn't say that. They certainly shouldn't use the word "thus" – it's the wrong context."*

B. *Knowledge and Experience by Themselves or Others*

The results showed that many participants had either previous knowledge themselves, or they knew of others who had an experience with ransomware or phishing attacks. 30% of participants knew of someone who had been scammed through a "request for update" PayPal email. In contrast, participants were asked to explain what they knew about ransomware. The results indicate a low level of understanding about the danger or recognition of ransomware (see Table III).

TABLE III.AUTHENTIC KNOWLEDGE OF RANSOMWARE

Authentic Knowledge about Ransomware	
High Level of Knowledge about Ransomware.	5%
Participants with Some / Limited knowledge about ransomware	24%
Participants who had no Idea what Ransomware was, or if could affect them	51%
Participants who believed that they knew what Ransomware was, but were incorrect in their understanding.	19%

Participants were also asked to indicate what they thought people should do to deal with ransomware. Some participants gave specific advice explaining the need to delete emails from unknown sources that contained messages that contained errors in spelling, grammar and syntax. Others gave responses that would be of no assistance in identifying, removing, or managing ransomware in email correspondence (see Table 4).

TABLE IV APPLICABLE / USEABLE KNOWLEDGE ABOUT DEALING WITH RANSOMWARE

Applicable / Useable Knowledge about dealing with Ransomware	
Useful Advice regarding Ransomware	32%
General / Vague advice regarding ransomware	41%
Unhelpful advice (likely to cause severe financial loss and / or deception	27%

C. Knowledge Location and Evaluation of context, grammar, syntax, and spelling errors in phishing and ransomware attacks.

A review of 21 different previously known images of phishing and ransomware showed many examples of where the message contained spelling and grammar errors and identified different segments within standard email messages where such errors occurred (See Table V). The review showed that many phishing and ransomware threats contained errors in terms of grammar, spelling, syntax, and overall context and awkwardness.

TABLE V. GRAMMAR AND SYNTAX ERRORS IN PHISHING AND RANSOMWARE MESSAGES

Type of Error	**Grammar**	**Spelling**	**Syntax**	**Context Awkwardness**
Email Address identity	0	3	0	0
Title or message	1	0	1	2
Body of Text	4	7	12	1
Closing Statement	2	1	1	2

A large percentage of older adults were prepared to accept email and ransomware content, even though they could recognize grammar and syntax errors. These errors are prominently recognizable across different segments of a standard email message, yet they consistently exist within the body of the text in most threat messages.

A. CONCLUSIONS

From the results, we make three conclusions. The first is that significant numbers of older adults are inadequately capable to recognize fundamental indicators in emails such as grammar, spelling and syntax. People over the age of 60 show the propensity to place greater faith and trust in a known brand, irrespective of whether the known brand is in the form of a copied logo in an email that contains multiple grammatical and spelling errors. Trust and discernment of grammar and syntax are low in adults aged 60 and over. The second conclusion is that participants are poorly educated in the awareness, recognition and treatment of phishing and ransomware emails. Some adults will see and acknowledge errors in emails but accept grammar and syntax errors as normative. The third conclusion is that poor or unusual grammar, syntax, spelling and any associated context within a message can be a useful indicator of likely illegal activity, older people remain less likely to recognize the indicators with enough consistency to expect a mitigation of ransomware and phishing attacks. We conclude that despite the increased proliferation of phishing and ransomware attacks directed at older adults, they continue to remain at high risk of attack.

REFERENCES

[1] Australian Bureau of Statistics, Population by Age and Sex, Australia, States and Territories, Abs.gov.au. Retrieved from: http://www.abs.gov.au/AUSSTATS/abs@.nsf/Previousproducts/3101.0 Feature%20Article1Jun%202016, 2017.

[2] S.E. Peacock and H. Kunemund, Senior Citizens and Internet Technology. *European Journal of Ageing*, Volume 4, Issue 4, pp 191 – 199, 2007.

[3] PEW Research Center, Older Adults and Technology Use, available from: http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/, 2014.

[4] J. Thomas, C. Wilson, J. Barraket, J. Tucker, E. Rennie, S. Ewing, and T. MacDonald, Measuring Australia's Digital Divide: *The Australian Digital Inclusion Index*, 2017. Melbourne: RMIT University, 2017. From: http://www.dx.doi.org/10.4225/50/596473db69505, 2017.

[5] A. Oxendine, E. Borgida, J.L. Sullivan, and M.S. Jackson, The importance of trust and community in developing and maintaining a community electronic network. *International Journal of Human-Computer Studies,* Volume 58, Issue 6, pp 671-696, 2003.

[6] H. Wu, A.A. Ozok, A.P. Gurses, and J. Wei, User aspects of electronic and mobile government: results from a review of current research. *Electronic Government, an International Journal,* Volume 6, Issue 3, pp 233-251, 2009.

[7] J.L. Richet, From Young Hackers to Crackers. *International Journal of Technology and Human Interaction (IJTHI),* Volume 9, Issue 3. pp 53-62, 2013.

[8] D.M. Cook, P.S. Szewczyk, and K. Sansurooah, Seniors Language Paradigms: 21st Century Jargon and the Impact on Computer Security and Financial Transactions for Senior Citizens. *Proceedings of the 9th Australian Information Security Management Conference.* Perth, Western Australia, 2011.

[9] D.M. Cook, P.S. Szewczyk, and K. Sansurooah, 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, Western Australia 2011.

[10] D.M. Sarno, J.E. Lewis, C.J. Bohil, M.K. Shoss, and M.B. Neider, Who is the Phishers luring? A Demographic Analysis of those susceptible to Fake Emails, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* Volume 6, Issue 1. SAGE Journals, 2017.

[11] K. Coronges, R. Dodge, C. Mukina, Z. Radwick, J. Shevchik, and E. Rovira, The Influences of Social Networks on Phishing Vulnerability. Paper presented at the 45th Hawaii International Conference on System Science (HICSS), on 4th January 2012.

[12] D. Winder, Ransomware. *PC Pro Issue* Volume 261, Issue 107, 2016.

[13] B. Kenyon, and J. McCafferty, Ransomware recovery. *It Now,* Volume 58, Issue 4, pp 32-33. doi:10.1093/itnow/bww103. 2016.

[14] Delloite, Ransomware holding your data hostage. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/.../risk/us-aers-ransomware.pdf, 2016.

[15] McAfee, McAfee Labs Threat Reports. Retrieved from https://www.mcafee.com/au/resources/reports/rp-quarterly-threats-sept-2017.pdf, 2017.

[16] J. Bohannon, The bitcoin busts. *Science,* Volume 351, Issue 6278, pp 1144-1146. doi:10.1126/science.351.6278.1144, 2016.

[17] S. Kirchheimer, New Threats in Ransomware. *Bulletin Today.* Retrieved from https://blog.aarp.org/2016/05/06/new-threats-in-ransomware/, 2016.

[18] H. Care, Two-Thirds of Seniors Have Been Scammed Online, Prnewswire.com, Retrieved from https://www.prnewswire.com/news-releases/two-thirds-of-seniors-have-been-scammed-onlinesurvey-300408178.html, 2017.

[19] C. Everett, Ransomware: To pay or not to pay? *Computer Fraud & Security*, Volume 4, pp 8-12. 2016. doi:10.1016/S1361-3723(16)30036-7, 2016.

[20] K. Mitnick, and W. Simon, The art of deception: Controlling the human element of security. Indianapolis, Ind.: Wiley, 2002.

[21] P. Lichtenberg, L. Stickney, and D. Paulson, Is Psychological Vulnerability Related to the Experience of Fraud in Older Adults? Clinical *Gerontologist,* Volume 36, Issue 2, pp 132-146. doi: 10.1080/07317115.2012.749323, 2013.

[22] G. Kirwan, and A. Power, Cybercrime: The psychology of online offenders. Cambridge University Press, 2013.

[23] J.R. Nino, E. Enstrom, and A.R. Davidson, Factors in Fraudulent Emails that Deceive Elderly People, *Human Aspects of IT for the Aged Population, Aging, Design and User experience,* Springer pp360 – 368, https://link.springer.com/chapter/ 10.1007/978-3-319-58530- 7_28, 2017.

[24] The Age UK, Only the tip of the iceberg: Fraud against older people. Retrieved from https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-andbriefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf, 2016.

[25] Veda, Banking, Veda picks top 5 Fraud trends for 2017, https://www.rfigroup.com/australian-banking-and-finance/news/veda-picks-top-five-fraud-trends-2017

[26] Kirchheimer, S. (2016). New Threats in Ransomware. *Bulletin Today*. Retrieved from https://blog.aarp.org/2016/05/06/new-threats-in-ransomware/, 2016.

[27] Australian Crime Commission, Inquiry into Cyber safety for Senior Australians Retrieved on March 20th 2018 from: https://duckduckgo.com/?q=Australian+Crime+Commission.+Inquiry+into+Cyber+safety+for+Senior+Australians+&t=ffnt&ia=web, 2013.

[28] P. Lichtenberg, L. Stickney, and D. Paulson, Is Psychological Vulnerability Related to the Experience of Fraud in Older Adults? *Clinical Gerontologist,* Volume 36, Issue 2, pp 132-146. doi: 10.1080/07317115.2012.749323, 2013.

[29] R. Tzezana, High-probability and wild-card scenarios for future crimes and terror attacks using the internet of things, *Foresight,* Volume 19, Issue 1, pp 132 – 148, 2017.