https://doi.org/10.48009/1_iis_2017_78-86

Issues in Information Systems
Volume 18, Issue 1, pp. 78-86, 2017

AWARENESS OF MALICIOUS SOCIAL ENGINEERING AMONG FACEBOOK USERS

Kevin J. Slonka, Pennsylvania Highlands Community College, kslonka@pennhighlands.edu

ABSTRACT

With the rapid growth of Facebook, the social networking website is becoming a lucrative target for malicious activity. Users of Facebook therefore should be aware of various malicious attacks and know how to identify them. This research analyzed Facebook users' level of understanding in the domain of malicious social engineering on Facebook. The research examined differences in awareness among multiple generational groups; secondary research questions focused on how factors such as age, gender, education, Internet usage, and trust affected users' awareness of malicious activity. Results suggest that the Baby Boomer generation is the least aware of malicious social engineering tactics on Facebook, specifically in regard to the Donation scam category. In addition, education level and educational background are significantly associated with awareness. These findings indicate a need for future work to gain a deeper understanding of Facebook users' awareness of malicious social engineering and generate targeted training in order to increase said awareness.

Keywords: Facebook, Social engineering, Privacy, Awareness

INTRODUCTION

Since its opening to the public, Facebook has been widely adopted. What started as a Harvard-only social networking website became available to any person with an email address at an educational institution (.edu) and currently can be used by anyone. No longer do the users of Facebook strictly represent traditional, college-age students. Instead, multiple generations have adopted it as a communication platform. This widespread adoption by people of vastly different ages introduces two main problems.

The first problem lies with the number of people who use Facebook. Malicious attackers on the Internet do not have unlimited time. Because of this, it is in the attackers' best interest to do as much damage and/or make as much money as they can in the smallest amount of time. Attacking targets with an extremely large user base makes this possible. Were one to check personal email every day, the number of spam email messages seen would make this apparent. Many people use email on a daily basis, thus making it a perfect target for malicious attackers. Performing attacks en masse, only a small number of victims need to be compromised for the attackers to profit greatly. Because of Facebook's growing user base (1.23 billion active users as of December 31, 2013 ("Company Info", 2014)), its popularity as a target for attack rivals email.

The second problem exists because of the varying ages of Facebook users. People from the Baby Boomer generation, Generation X, Generation Y, and the Millennial generation use Facebook. Jorgensen (2003) has argued that those born between 1946 and 1962 belong in the Baby Boomer category and both Jorgensen (2003) and Paula and Dominic (1999) have argued that people associated with Generation X were born anywhere from 1963-1978. Moving forward on the timeline, Goldgehn (2004) has defined Generation Y as those born between 1981 and 2000 while Jorgensen (2003) has suggested the years 1977-1988. For the purposes of this study, in order to keep the generational groups distinct, Generation Y will consist of those born between 1979 and 1992. The last group, Millennials, consists of anyone born after 1992 (Tucker, 2006).

The availability of different technologies during each generational timeframe leads to differences in the understanding and use of technology (Rosen, 2004), and this represents one of the grounds for analyzing Facebook users based on age, and specifically generational group. Facebook, a new, non-physically interactive technology, offers new opportunities for misunderstandings about technology, technology safety, and malicious online behavior. But it is not

only technology that can shape a person. Bennis and Thomas (2002) have suggested that computers and the Internet have had a "profound effect" (p. 11) on those who had access to them during their younger years, but also have advocated another reason for using one's age as an analytical factor; "[a]ll of us come of age in a particular place and time – an era – that shapes us in large and small ways" (p. 2). Though technology is one aspect that Bennis and Thomas explore, other aspects, such as historical events, influence and shape people. As a whole, however, prior research supports using age as an analysis factor.

RESEARCH METHODOLOGY

The overarching methodological framework for this research was a population study. The purpose was to "build an understanding of th[e] population's knowledge, attitudes, and practices (KAP)" (O'Leary, 2010, p. 110) on the topic of malicious social engineering tactics on Facebook. Little data existed on this topic; therefore, primary data was gathered.

Research Question

What are the differences in awareness of malicious social engineering tactics on Facebook between people associated with the Baby Boomer generation, Generation X, Generation Y, and the Millennial generation?

Population

This research studied members of multiple generational groups who used the social networking website Facebook. These generational groups were the Baby Boomer generation, Generation X, Generation Y, and the Millennial generation. Surveying multiple generational groups allowed for greater participation due to the larger number of possible participants as well as allowed for greater generalizability of the results across the population of all Facebook users.

In order to access the population, the researcher sent the survey electronically to members of his multiple social graphs. Due to the non-use of protected classes, no special permission was required in order to access the population. In addition, the survey was not distributed via corporate means, which removed the necessity of permission for distribution. Social graphs, such as Facebook, other online communities, such as Twitter and Reddit, and friends and colleagues, who were reachable via email, were utilized. Accessing personal connections provided a convenience sample, making the generalizability of the results unknown. In order to gain access to a more meaningful sample the researcher asked those participants in the convenience sample to forward the survey link to members of their social graphs. This is known as snowballing (Brickman-Bhutta, 2009).

There was no set minimum number of participants for this research. The survey remained available until a reasonable amount of participation was gained. In addition, statistical significance is possible with uneven groups; therefore, the number of participants belonging to each generational group can be uneven.

Selecting the Tactics

It would have been possible to administer a survey to the population with open-ended questions in order to create the initial list of tactics; however, this approach was not used due to time constraints. Instead, the most common malicious social engineering tactics were gathered from literature due to the existence of many websites that have aggregated the most common tactics over the years. The data from these websites was used in order to generate a list of tactics. Next, those tactics were coded and grouped according to content. Finally, a pilot test of the survey instrument was conducted and the results guided the revisions of the instrument (Fink, 2002).

A list was created of some of the most common tactics used on Facebook ("5 dangerous", 2017; Fernandes, 2011; Hayley, 2012; Jelea, 2012). Many of these tactics were extremely similar to other tactics in the list; some were duplicated. For this reason, it was necessary to code these tactics by category in order to determine which were the most commonly occurring. In order to code, or themeatize, these tactics, a small group of industry professionals (IP) was surveyed. Given the list of tactics, they were asked to assign an appropriate category to each. Upon completion

of the coding, the researcher compared each of the IPs' themes with his own list in order to derive the final categorization.

The four responses for each tactic were analyzed for frequency and the most frequently appearing category was chosen to represent the tactic, as demonstrated in Table 1.

Table 1. Categories of the Most Common Tactics

Tactic	Category
Add Facebook Functions: new buttons (dislike, love, etc.)	Alter Facebook
Altering the Facebook Layout	Alter Facebook
Change Your Facebook Background	Alter Facebook
Facebook will start charging beginning with [date]; Facebook will close beginning with [date]	Alter Facebook
See who viewed your profile, and its countless variants	Alter Facebook
[Celebrity x] dies / is caught doing scandalous act	Celebrity
Celebrity Death Rumors	Celebrity
Marika Fruscio Spam	Celebrity
OMG Can't Believe Justin Beiber Did This To A Girl Spam	Celebrity
Ryan Dunn's LAST WORDS EXCLUSIVE Video	Celebrity
See sex tape/naked photos of [celebrity x]	Celebrity
Sharing a Picture Results in Donations	Donations
Fake Events	Events
Free Gift Cards and Vouchers	Free Items
Gift Card/Cool Gadget Giveaways	Free Items
[huge percent] of people cannot watch this video for more than x number of seconds	Sensational
Girl Killed Herself After Dad Posted On Wall Scam	Sensational
I Can't Believe You Are In This Video Scam	Sensational
Like and share schemes using atrocious images (maimed animals, suffering children)	Sensational
To see [hot topic of the day] install browser extension/add-on or youtube/flashplayer update	Sensational
You won't believe what she does!! Scam	Sensational

After coding the tactics based on content, a frequency table for the group of scams as a whole was extrapolated. The coding of the tactics allowed six themes to emerge. In descending order of frequency, those themes were celebrity, sensational, alter Facebook, free items, donations, and events. Because the survey needed to present the participant with an actual malicious social engineering tactic, not simply a category, specific tactics were chosen. The method for choosing the specific tactics to present to the participant was based on the pilot test of the survey instrument.

Survey Instrument

The instrument was delivered electronically, via a well- established online survey company, SurveyMonkey. Due to the electronic nature of the survey, this study was not location-bound and accepted participants from any location with Internet access. Its impersonal nature (i.e., being delivered to the participant without the presence of the researcher) made the survey more likely to produce honest results as any immediate perceived embarrassment was removed.

DATA ANALYSIS

The generation of indices is a supported method of providing a better understanding of the data through the use of different statistical analyses (von Lengerke & Mielck, 2012; Moore, Murphey, & Bandy, 2012; Moore, Vandivere, Lippman, McPhee, & Block, 2007; Royuela, Lopez-Tamayo, & Surinach, 2009; Zullig 2010). They are normally

generated when one lacks a unit of measurement and, instead, creates a surrogate based upon indicators of that which is to be measured (Arsham, 1994). Two indices were created in order to generate scale data, which allowed the researcher to run more detailed analyses than those available for use with the original nominal data. The decision to create these indices stemmed from the three-step process of index creation suggested by Lalloue et al. (2013).

The first index was the total gullibility index, the sum of the answers to the malicious survey questions. The value of this variable was calculated using SPSS's sum() function on the variables for survey questions 11, 13, 19, 25, and 31, which were the Facebook Timeline Remover, Baby, Justin Beiber, Ebay, and Girl Video Scams, respectively (the other scam questions were the placebo questions; i.e., non-online and non-malicious). The second index, the average gullibility index, was calculated using the mean() function on the same variables. In all tests where gullibility was used as a measure, the tests were run once using total gullibility and once using average gullibility. The inclusion of the average gullibility measure was based on Fisher (1922), who suggested that indices should "fairly represent, so far as one single figure can, the general trend of the many diverging ratios from which it is calculated" (p. 10). They should be a "just compromise" (p. 10) or a "fair average" (p. 10) that eliminates extreme dispersion among the index values. The mean of the values satisfied this requirement.

Overview of the Population Sample

Descriptive statistics and frequencies were used in order to gain a broad understanding of the sample used in this research. The majority of the participants were members of Generation Y, as shown in Table 2. The smallest group, at only 1.4% of the sample, was the Millennial generation.

Table 2. Frequency Distribution for Generation

	Frequency	**Percent**
Millennial	4	1.4
Generation Y	163	57.4
Generation X	77	27.1
Baby Boomer	40	14.1
Total	284	100.0

The total participation for this study was 284, which is small when compared to the total number of registered users on Facebook but is more than enough for statistical analysis.

Research Question Analysis

In order to answer the research question, both the parametric tests (ANOVA) and non-parametric tests (Kruskal-Wallis) were run on the gullibility indices by generation in addition to crosstabs on each individual malicious scam by generation. The ANOVA test compared the variance of the means between the different groups (generations) with the variance within each group. This allowed the researcher to determine whether the variability of the dependent variable (awareness score) was due to the independent variable (the generations) or simply due to chance. A significant finding ($p < .05$) means that the null hypothesis can be rejected (i.e., the means of the groups are not equal and the variability is due to the independent variable).

Table 3. Parametric Analysis of Total Gullibility by Generation

Analysis	**Significance (p)**
ANOVA	.005

Analysis	**Significance (p)**	**Group 1**	**Group 2**
Tukey's HSD	.008	Baby Boomer	Generation X
Tukey's HSD	.014	Baby Boomer	Generation Y

Analysis	**η^2**	**Size**
Effect Size	.04	Medium

The ANOVA of total gullibility by generation, shown in Table 3, suggested a significant difference between the generations, which, as Pallant (2010) explained, suggested that the difference didn't occur by chance. In order to see between which groups the difference laid, Tukey's Honestly Significant Different (HSD) test was performed. Tukey's HSD test was chosen because it was a post-hoc comparison, designed to protect against Type I errors (rejecting the null hypothesis when it is actually true). Post-hoc tests are used because they "guard against the possibility of an increased Type I error due to the large number of different comparisons being made" (p. 209) by using more stringent rules for achieving significance. Furthermore, no planned comparisons of groups were made; this made Tukey's HSD test the best choice because it would test all groups. The result of Tukey's HSD test suggested significant differences between the Baby Boomer generation with both Generation X and Generation Y, as also demonstrated by Table 3.

In addition to statistical significance, Pallant (2010) urges researchers to assess the "strength of association" (p. 210) by calculating the effect size. Effect size is a necessary calculation because statistical significance does not imply practical significance (i.e., just because a statistic is significant doesn't mean that a human will be affected or even notice the difference). In order to assess whether this finding had any practical significance (i.e., detectable by a human), the eta squared value was computed using the equation eta squared = sum of squares between groups / total sum of squares. According to Cohen (1988), an eta squared value of .01 corresponds to a small effect size, .06 is a medium effect size, and .14 is a large effect size. The effect size was .04, noted in Table 3, a medium effect size, which suggested that the effect would be "apparent to the naked eye of a careful observer" (Cohen, 1992, p. 99). This effect size suggested that the finding was practically significant.

Table 4. Parametric Analysis of Average Gullibility by Generation

Analysis	Significance (p)
ANOVA	.005

Analysis	Significance (p)	Group 1	Group 2
Tukey's HSD	.008	Baby Boomer	Generation X
Tukey's HSD	.014	Baby Boomer	Generation Y

Analysis	η^2	Effect Size
Effect Size	.04	Medium

The ANOVA of average gullibility by generation, shown in Table 4, suggested a significant difference between the generations. In order to see between which groups the difference laid, Tukey's HSD test was performed. This suggested significant differences between the Baby Boomer generation with both Generation X and Generation Y. The effect size was .04, a medium effect size, which suggested that the effect would be "apparent to the naked eye of a careful observer" (p. 99).

Table 5. Non-Parametric Analyses

Analysis	Significance (p)	Variable
Kruskal-Wallis	.007	Total Gullibility
Kruskal-Wallis	.007	Average Gullibility

Analysis	Significance (p)	Generations vs.
Chi-Square	.007	Baby Scam

Analysis	Significance (p)	Value	Effect Size
Cramer's V	.007	.206	Medium

Both non-parametric (Kruskal-Wallis) tests corroborated the results of the parametric (ANOVA) tests, as demonstrated by Table 5, suggesting a significant difference between the generations. As previously stated, the Kruskal-Wallis tests were run due to the possible non-normality of the data; their purpose was to support/contradict the findings of the parametric tests, thus confirming/discrediting their validity.

Because the indices were constructed from nominal data, crosstab analysis and the Chi-square test for independence were run on said nominal data in order to determine if there was further support of the previous findings. Crosstab analysis of the generations and scams yielded a single significant scam between the generations. The Chi-square test for independence indicated a significant difference between the generations and the Baby Scam, $\chi 2=12.086$, $p=.007$, Cramer's $V=.206$. The Cramer's V value, used when the crosstab analysis produces a table larger than 2x2, suggested a medium effect size (Pallant, 2010), which was aligned with the results of the ANOVA test. These results suggested that the Baby Boomer generation is the least aware of the malicious tactics.

DISCUSSION

This study primarily focused on exploring one's awareness of malicious social engineering tactics employed on Facebook. The study collected quantitative data in order to address the research question. The data was examined using SPSS. In all cases where parametric and non-parametric tests were available given the specific types of data, both were run due to the apparent non-normality of the data. The results from the research question provided valuable insight into the problem.

Using the newly created gullibility indices, a significant difference arose between one's generation and their gullibility. The effect size of this difference was medium, meaning the difference could be seen by the naked eye. This is important to note, as a significant difference could have been found with a small effect size, which makes the finding less actionable because it could not be detected by the naked eye. Examining the difference more closely, Tukey's HSD test revealed the key difference between the Baby Boomer generation and both Generation X and Y. This suggested that Baby Boomers have a different understanding of maliciousness on Facebook than the younger generations and thus need to be educated differently. These findings were in line with the work of Drennan, Mort, and Previte (2006), Heaney (2007), and Lehtinen, Näsänen, and Sarvas (2009), who all found that there are differences between generations and their understanding of online privacy.

Although determining that a significant difference exists is a crucial first step, one must look further for information describing the structure of the difference. Examining the descriptive statistics revealed that the mean gullibility of the Baby Boomer generation is more than double that of Generation X or Generation Y. In addition, Crosstab analysis showed that Baby Boomers have a higher click rate on four out of the five malicious scams. Baby Boomers are vastly less aware of malicious social engineering than younger generations.

The data, however, does not imply a reason as to why Baby Boomers are much more susceptible to social engineering attacks. Instead, credence is given to Rosen's (2004) and Bennis and Thomas' (2002) findings, where they offered technology availability as a reason for differences in understanding. The case can be made that technology as it existed during the formative years of Generation Y participants more closely resembled the current technology than the technology available during the formative years of the Baby Boomers. Due to this massive shift in technology, it is possible that current technology is unknown and/or confusing to the Baby Boomer generation, who did not have the same technology available to them as the younger generations did during their formative years. Determining the root cause for this difference in awareness is an area for further research. What is clear, however, is that there is a crucial need for customized awareness training. This research suggested that Baby Boomers have much less of an understanding of malicious social engineering tactics on Facebook than other generations; however, with future research one might be able to further define this awareness divide and produce training that specifically targets each generational group.

Although the Millennial generation was included in this study, any significant results that include the group should be suspect due to the extremely low number of participants belonging to that generation. With such a small number it is not possible to say, with any amount of certainty, that a result including the Millennial generation is meaningful or repeatable. For example, with a higher amount of Millennial participation the first research question may have shown that Baby Boomers are significantly different from the Millennials as well. However, for the purposes of this study, no conclusions can be made about the Millennial generation.

Limitations

Various items could have been different in order to produce better results with this research. First, the number of participants in the Millennial generation limited the results. With only four participants in that age range, no conclusions could be made about this generation. An initial assumption of the researcher was that generation would have played a significant role in one's gullibility, especially with the younger generations. This assumption could not be fully fleshed out due to the extremely low number of Millennials who responded to the survey.

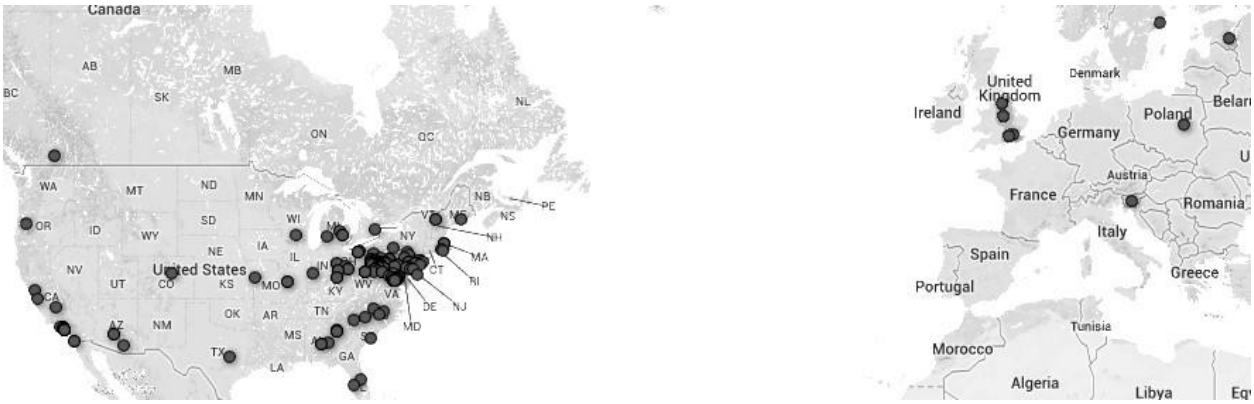

Figure 1. Map of Participant Locations

Second, as depicted in Figure 1, the majority of the participants were from the Eastern side of the United States of America (USA), with few in other locations such as the Western USA and Europe. While the results of this study may be applicable to Facebook users from the USA, there is no guarantee they will be applicable outside of that particular part of the world. In order to have more meaningful results, effort should be put into getting the survey into the hands of participants from all parts of the world where Facebook is used.

Lastly, it must be noted that the data was collected about electronic scams using an electronic survey. It is possible that a large number of people simply ignored the request to take the survey because they have already been trained not to click on links in emails, on Facebook, etc. This survivor bias means that some less gullible Facebook users simply ignored the survey, and as such their non-gullibility would not be accounted for in the data set.

Recommendations for Future Studies

In addition to further studies implementing the suggestions from the previous section, various other studies can be conducted using this research as a starting point. In order to gain a better understanding of not just of what people are unaware but why they are unaware, analysis of the reasons why participants would click on certain scams should be conducted. These reasons were elicited as part of this study's survey, however the data did not directly apply to the research question and as such was not used. A study should be created in order to fully utilize the existing data set.

On the opposite end of the spectrum, the literature review revealed that no data currently exists about malicious social engineering in the realm of psychoanalysis. While this study answered the question of to "what" people are unaware it did not answer the question of "why." The previously suggested future study provided a point at which to begin, however completely answering this question would entail a more thorough analysis of the human mind. This study is crucial since Facebook is also used as a means to find romantic relationships. Deception in one's love life can have lasting negative effects (Toma, 2017). An expert in the field of psychology should be contracted to participate in the conducting of this research.

Conclusion

The purpose of this study was to analyze the level of understanding of Facebook users in the area of malicious social engineering on Facebook. Analysis of the quantitative data drew a picture of the general Facebook population that

yielded some interesting results. These results were assumed but are now backed by research and, as such, more reliable.

The results of this study can be used by a wide array of parties. First, as previously mentioned, this study can serve as a base on which future researchers can create new, improved studies. Second, educational institutions should heed the warnings of this research. Some sort of awareness training needs to be integrated into post-secondary curricula. Third, businesses who offer Internet access to their employees must also offer awareness training, as the integrity of their corporate infrastructure lies in the ability of their employees to ignore their gut and not help a dying baby. Last, social networking companies, such as Facebook, Google, etc., should offer awareness training that is built into their platform. Since all companies have access to demographic data, targeting specific training based on age, education, etc. should be trivial.

This study adds to the limited body of knowledge in this domain and creates a base on which to conduct future studies in order to better understand this problem and make substantial strides in mitigation of the risks. People are the weakest link. We can train them; we have the technology.

REFERENCES

5 dangerous Facebook scams spreading like fire now. (2017). Retrieved from http://www.komando.com/tips/12190/5-dangerous-facebook-scams-spreading-like-fire-now/all

Arsham, H. (1994). Statistical thinking for managerial decisions. Retrieved from http://home.ubalt.edu/ntsbarsh/Business-stat/opre504.htm

Bennis, W. G. & Thomas, R. J. (2002). *Geeks & geezers*. Boston, MA: Harvard Business School Publishing.

Brickman-Bhutta, C. (2009). Not by the book: Facebook as sampling frame. Retrieved from http://www.thearda.com/workingpapers/download/Not%20by%20the%20Book%20-%20Bhutta.doc

Cohen, J. (1992). Statistical power analysis. *Current Directions in Psychological Science, 1*(3), 98-101.

Cohen, J. W. (1988). *Statistical power analysis for the behavioral sciences*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Company Info. (2014). Retrieved from http://newsroom.fb.com/company-info/

Drennan, J., Mort, G. S., & Previte, J. (2006). Privacy, risk perception, and expert online behavior: An exploratory study of household end users. *Journal of Organizational and End User Computing, 18*(1), 1-22.

Fernandes, J. (2011). Most actively spreading Facebook scams. Retrieved from http://techie-buzz.com/social-networking/most-actively-spreading-facebook-scams.html

Fink, A. G. (2002). *The Survey Handbook 2nd Edition*. London, England: SAGE Publications, Inc.

Fisher, I. (1922). *The Making of Index Numbers*. Cambridge, MA: Houghton Mifflin Company.

Goldgehn, L. A. (2004). Generation who, what, Y? What you need to know about Generation Y. *International Journal of Educational Advancement, 5*(1), 24-34.

Haley, C. C. (2012). Top 5 trending hoaxes and scams on Facebook 2012. Retrieved from http://thatsnonsense.com/blog/?p=496

Heaney, J. (2007). Generations X and Y's internet banking usage in Australia. *Journal of Financial Services Marketing, 11*(3), 196-210.

Jelea, I. (2012). Top 10 scams and hoaxes on Facebook you should recognize in 3 seconds. Retrieved from http://www.hotforsecurity.com/blog/top-10-scams-and-hoaxes-on-facebook-you-should-recognize-in-3-seconds-1313.html

Jorgensen, B. (2003). Baby boomers, generation X and generation Y?: Policy implications for defence forces in the modern era. *Foresight : The Journal of Futures Studies, Strategic Thinking and Policy, 5*(4), 41-49.

Lalloue B., Monnez, J., Padilla, C., Kihal, W., Le Muer, N., Zmirou-Navier, D., & Deguen, S. (2013). A statistical procedure to create a neighborhood socioeconomic index for health inequalities analysis. *International Journal for Equity in Health, 12*(1), 21.

Lehtinen, V., Näsänen, J., & Sarvas, R. (2009). Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: *"A little silly and empty-headed": Older adults' understandings of social networking sites*. Swinton, UK: British Computer Society.

von Lengerke, T. & Mielck, A. (2012). Body weight dissatisfaction by socioeconomic status among obese, preobese and normal weight women and men: Results of the cross-sectional KORA Augsburg S4 population survey. *BMC Public Health, 12*(1), 342.

Moore, K. A., Murphey, D., & Bandy, T. (2012). Positive child well-being: An index based on data for individual children. *Maternal and Child Health Journal, 16*, S119-S128.

Moore, K. A., Vandivere, S., Lippman, L., McPhee, C., & Block, M. (2007). An index of the condition of children: The ideal and a less-than-ideal U.S. example. *Social Indicators Research, 84*(3), 291-331.

O'Leary, Z. (2010). *The essential guide to doing your research project*. London: SAGE Publications Ltd.

Pallant, J. (2010). *SPSS survival manual: A step by step guide to data analysis using SPSS*. Open University Press.

Paula, M. P., & Dominic, L. L. (1999). Generation X: Is its meaning understood? *Newspaper Research Journal, 20*(4), 28-36.

Rosen, L. (2004). Understanding the technological generation gap. *The National Psychologist, 13*(2), 18.

Royuela, V., Lopez-Tamayo, J., & Surinach, J. (2009). Results of a quality of work life index in Spain. A comparison of survey results and aggregate social indicators. *Social Indicators Research, 90*(2), 225-241.

Toma, C. L. (2017). Developing online deception literacy while looking for love. *Media, Culture & Society. 39*(3), 423-428.

Tucker, P. (2006). Teaching the millennial generation. *The Futurist, 40*(3), 7-7.

Zullig, K. J. (2010). Creating and using the CDC HRQOL healthy days index with fixed option survey responses. *Quality of Life Research, 19*(3), 413-424.