Social Networking: A Tool for Effective Cybersecurity Education in Cyber-Driven Financial Transactions

R. Maharaj and R. von Solms

Nelson Mandela University, Port Elizabeth, South Africa
e-mail: s212254189@mandela.ac.za, rossouw.vonsolms@mandela.ac.za

Abstract

Cyberspace technology and cyber-driven services are core in today's modern world. This means that cyber services can be found in many facets of societies and many of the world's industries. This is also true for banking and users of cyber-driven financial transactions. Cybersecurity education is becoming imperative for users to be able to protect themselves better against a wide variety of threats. This is especially true for banking users, who due to the financial nature, are affected by a growing number of cyber-related threats. This paper presents an educational approach using social networking to assist in educating modern users of cyber-driven financial transactions.

Keywords

E-banking, Education, Cybersecurity Education, Social Networking, Cyber-driven financial transactions.

1 Introduction

In modern times, the rise of information technology (IT) can be seen in many facets of industry. IT innovations and developments shape the way end-users interact with traditional industries. These information technologies and their "partner" cyberspace have become intertwined in end-users' lives. Cyberspace and IT can both be seen as critical aspects of end-users' day to day lives. Although cyberspace has brought about numerous benefits, it has also introduced aspects of danger and risks in end-users' modern way of living. As end-users become more and more reliant on cyberspace, the chances of them becoming potential victims of cybercrime increases unless they are made aware and vigilant of the dangers surrounding their cyber activities. Examples of these possible dangers include e-mail hacking, phishing attacks and social engineering attacks. It is essential that end-users are made aware of these potential dangers and how to protect themselves more effectively. This is particularly important for end-users involved in cyber-driven financial transactions. Due to the financial nature of these cyber-driven financial transactions, users of these cyber services are often faced with more threats. According to the Financial Fraud Action UK (Five et al., 2017), financial fraud losses across payment cards, remote banking and cheques totalled £366.4 million between January and June 2017. During that period compromised personal and financial data was seen as a key driver of the financial losses (Five et al., 2017). Criminals utilized attacks similar to the above mentioned. Thus, it is critically important that end-users, specifically when conducting cyber-

driven financial transactions, are made aware of the dangers and risks associated with negligent behaviour when doing so.

This paper attempts to address the lack of education surrounding end-user cyber-driven financial transactions by introducing an alternative education approach utilizing two prominent social networking platforms, Facebook and YouTube. This paper will focus on the introduction of this educational approach as part of a joint research project undertaken with the South African Banking Risk Information Centre (SABRIC).

2 Background

The aim of this section is to provide a sound base and motivation for cybersecurity education, awareness and training to individuals exposed to sensitive personal and organizational cyber, especially users of cyber-driven financial transaction.

2.1 Cybersecurity Education, Awareness and Training

Cybersecurity is comprised of various elements, varying from technical to operational and behavioural security. There is no single solution to address it and therefore a multifaceted approach needs to be taken. Cybersecurity education, awareness and training provide end-users with the ability to recognize related threats where acceptable and act on them appropriately. Traditionally cybersecurity education, awareness and training programs have been targeted at organizations. However, in modern times cyberspace is at a simple "*click*" or "*tap*" away for everyone and thus cybersecurity education should be part and parcel of the lives of all end-users. This includes banking users involved in cyber-driven financial transactions, where end-users are particularly vulnerable.

2.2 Banking and Cyberspace – The shift in responsibility

Banking is one of the oldest industries in the world. As with many long-standing industries, banking has evolved over time, embracing new technologies and markets. This is also true for cyberspace, as many financial institutions and the way they transact are heavily dependent on cyberspace and IT (Horn, 2010). As financial institutions introduced more cyber-related services, it allowed users to take a more active role in their personal financial management. As seen with the introduction of the ATM and in more recent times mobile and internet banking. This shift, puts more responsibility in the hands of users, as they now become a potential point of weakness in the banking process. This statement is echoed in research where end-users are often considered weak links in the information security process (Al Awawdeh & Tubaishat, 2014; Aloul, 2012; Frauenstein & Von Solms, 2014). Thus, as mentioned in the previous section, modern banking users involved in cyber-driven financial transactions are very dependent and will benefit from appropriate education, awareness and training. As this will enable them to conduct personal banking in a more secure and safe manner, giving users peace of mind.

2.3 Cyber-Driven Financial Transaction Education

Cyber- driven financial transactions can be regarded as any transaction that occurs involving cyberspace. Examples of cyber-driven financial transactions include ATM usage, online purchases and credit card usage. As such, it can be seen that the majority of transactions that occur in modern banking can be regarded as cyber-driven financial transactions. As stated in the Ombudsman's Annual Report for Banking Services South Africa (2016), a large number of users are negatively affected by cyber-crime. Human error or, as mentioned previously, negligence is a large contributor, in financial loss experienced by users during cyber-driven financial transactions. Human error can be as a result of inexperience, improper training, the making of incorrect assumptions and other circumstances (Whittman & Mattord, 2013). Therefore, it can be argued that there is a need for proper education, awareness and training among users of cyber-driven financial transactions. Education and training are literally 'placed' between users and the cyberspace or systems utilized (Whitman & Mattord, 2012). It is through proper education, awareness and training that it is possible to foster a cyber-culture of secure cyber usage towards conducting safe cyber-driven financial transactions. It is thus clear that users may be self-responsible for malicious cyber-driven financial incidents due to their lack of related education, awareness and training or ignorance on the subject matter. Further, that education plays an important role in cyber-driven financial transactions to ensure that users are knowledgeable about utilizing cyber services in a secure manner. Through proper education, that increases their awareness, it reduces their inherent negligence and ignorance and therefore assists in mitigating the related risks associated with cyber-driven financial transactions.

Financial institutions, offering these cyber-driven financial services, do offer some educational material and services to educate their clients and therefore helping to mitigate the associated risks. Even though the educational content is correct, the content may be challenging to locate and also, the material is not necessarily presented in a manner that appeals to the average user. The following section will discuss an alternative educational approach that aims to educate users of cyber-driven financial transactions allowing them to conduct these cyber services safely and securely.

3 Instrument Implementation

It is clear from the foregoing sections that users of cyber-driven financial transactions are extremely vulnerable. This is due to the increased threats they face and the lack of appealing education surrounding the subject matter. This section will provide insight into how an alternative educational approach was created in partnership with the South African Banking Risk Information Center (SABRIC).

3.1 Research Approach

This research resides in the problem-solving domain and follows a mixed methods approach. The research approach followed is that of an experiment, utilizing an instrument within the social media domain to gather data. The instrument in this context is the cybersecurity education tool utilizing a social media quiz and video combination created in order to raise awareness and educate users of cyber-driven financial transactions.

The structure of the following sections and subsections will firstly provide the context and environment in which the instrument will be implemented; secondly to describe the instrument and its content, thirdly to describe the research agent and finally to describe the instrument's implementation.

3.2 Context of Implementation

Cyber usage and cybersecurity is a topic often addressed in the South African banking industry. The majority of security-related efforts resides in the technical space. However, technical security safeguards are only as secure as the users involved in the process at hand. As stated in literature, hardware and software security mechanisms are widely used to strengthen information systems (IS) against attacks, however, these systems are still vulnerable because of user's undesirable behaviour (Öğütçü, Testik, & Chouseinoglou, 2016). As cyber services and technology has integrated into the daily lives of many people, including those involved in cyber-driven financial transactions, it has become critical to ensure that users are educated about threats and dangers related to their cyber services. The context in which this study occurs is at a national level, using social networking platforms as an educational tool. A fun social networking quiz (to raise awareness) and a related informative video (to educate) therefore had to be created. This two-fold approach and the use of social networking form the basis of the instrument. The design of the instrument was carefully considered and is discussed in the next subsection.

3.3 The Instrument (Social Networking Game Quiz and Video)

The instrument is targeted at the majority of South African banking clients - the majority of which make use of cyber-driven financial services. Therefore, considerations in the design of the instrument include; audience-appropriate content, delivery mechanism, ease of use and understanding. Existing educational instruments used by South African banks were considered as a basis for the instrument. However, the current state of awareness and education is lacking and unappealing. During an initial discussion with the South African Banking Risk Information Center (SABRIC), a two-fold approach, a combination game-type quiz and an accompanying video, was decided upon. This approach served as the basis for the instrument for two major reasons. Firstly, social networking, particularly Facebook and YouTube are growing rapidly in South Africa and allow for a far wider audience to be reached. Secondly, a social networking game and video approach lower the audience preconceived notions about typical education, which can be seen as dull and unappealing. This makes the

instrument more mass marketable. The design and content will be discussed in the following subsections.

3.3.1 Design

This subsection will address the reasons why a social networking game quiz and video combination was chosen as the most suitable instrument to raise awareness and educate users of cyber-driven financial services. The focus of this section will, therefore, be the design of the instrument.

Firstly, the instrument's approach must cater to a wide audience. Due to SABRIC's involvement, the instrument had to be designed to reach a national audience. This was achieved by making use of social networking (Facebook and YouTube) as the platform for which the instrument would be hosted. Facebook, as of the fourth quarter of 2017, has 2.2 billion active users, with a significant amount being South African (Statista, 2017). This allowed the instrument to be reached by many users of cyber-driven financial transactions, accomplishing the goal of being able to reach a wide audience. Secondly, the design of the instrument had to be "fun" and interactive. This allowed, as previously mentioned to lower the preconceived notions of traditional learning. This was achieved by using a high score type quiz format. The quiz served as an awareness-raising tool. Using a quiz format allowed for the instrument to be interactive and have that "fun" factor. This interactive approach appeals to many social networking users as quizzes are typically popular with some quizzes seeing an average of 60 000 user engagements (Boland, 2017). Thirdly, the instrument had to allow for users to be educated in an alternative manner. This was done by a short, suitable video. Once the user completed the quiz (raising awareness) they were then prompted with a video on the subject matter. Video was used due to its ease of use and lack of effort required by the user to educate themselves. Videos produced were short as this enables a user to keep focus throughout the duration of the video, enabling them to better concentrate.

An element of educational reinforcement is also incorporated in the instrument. This is done by introducing a message after a user selects an answer. The message relates to the question, after a participant, answers the quiz questions the message is displayed. This enables the user to learn (reinforcing), alongside the "fun" quiz.

In order for the user to benefit, the content of the quiz and video is very important to ensure focused and relevant learning takes place. The content found in both the video and quiz are obviously of particular importance.

3.3.2 Content

Five quizzes with five related videos were created. Topics were chosen following close liaison with SABRIC regarding what affects the typical cyber-driven financial transaction user most. Examples of topics include online shopping, malware, card fraud, cyber hygiene and mobile banking. Online shopping will be used as an example in this paper.

The questions asked in the quizzes were topic related and pertaining to safe and secure online shopping. Table 1 represents the online shopping quiz questions and answers.

Question: Which of the following contribute to unsafe online shopping?	
Answer A:	Saving of payment information in web browsers
Answer B:	Using a well-known online merchant
Answer C:	Making use of 3-D secure payment
Answer D:	Looking for the closed padlock symbol
Correct Answer Text: Right answer! Never save payment information in your web browser as it may be used if someone gets a hold of your device.	Incorrect Answer Text: Wrong answer! Some sites (as well as all browsers) offer to "remember" your payment information (e.g. password) for your convenience upon subsequent purchases. Never accept to have your "financial information" stored on any website/web browser.

Table 1: Online Shopping Sample Question

As in the above table, quiz questions were structured as multiple-choice questions with four possible answers. The video that relates to the quiz is roughly 1 minute and 30 seconds long. As mentioned previously, the videos were kept short in order to hold the user's attention. The online shopping video comprises of the following five pointers for safe and secure online shopping. These five pointers are;

1. Look out for the padlock followed by HTTPS next to the URL when transacting online – the 'S' indicates that you are connected to a secure and encrypted website.
2. When registering on a secure site, choose a strong password and do not save your login details on any computer or mobile device. Never re-use the same password on multiple domains.
3. Avoid sharing your personal information, online merchants don't need your ID number or date of birth to process your order, but cybercriminals can use this to steal your identity.
4. Check your bank balance after making any online shopping payments. Report any fraudulent transactions to your bank as soon as possible.
5. For added online shopping verification, register your bank card with 3D Secure.

The message behind this video is to educate the users to perform online shopping in a safer and more secure manner. The video itself is an animated production, with a 'look and feel' that should appeal to users.

As discussed, this study focuses on five topics, namely; online shopping, malware, card fraud, cyber hygiene and mobile banking. However, the topic of online shopping will be discussed as an example in this paper. The instrument was designed to meet the following goals. Firstly, the instrument had to reach a wide audience. Secondly, it had to be "fun" and interactive. This was done through the creation of a social media game quiz and related video. all quizzes comprise of five, close-ended questions and are linked to the video. After a user selects an answer, regardless if it is a correct or incorrect answer, an educational message is displayed. This, as previously mentioned, adds an element of educational reinforcement.

The effectiveness of this instrument as a cybersecurity educational tool will be determined by the research agent, to be discussed in the next section.

3.4 Research Agent

The research agent consists of two parts. The initial part of the research agent constitutes the quiz. The quiz, alongside raising user awareness, has been used to capture statistical data about the level of awareness and knowledge that users of cyber-driven financial transactions possess. The quiz questions are close-ended, multiple-choice questions which relate to the most prominent threat situations users face concerning cyber-driven financial transactions. This allows for some approximation of users' awareness levels and knowledge to be rated per quiz. The primary data gathered from the quiz includes; correct and incorrect answers, while additional data captured and calculated includes; average score, number of participants, participant country, participant device, gender and average elapsed time. The ratio of correct and incorrect answers gives some indication of the users' level of awareness and knowledge on the specific topic. Incorrect answers indicate that users might lack awareness and knowledge to conduct these cyber services in a safe and secure manner.

The second part of the research agent consists of a single question asked at the end of each video. The question asked, attempts to determine if the user feels more positive and assured of the level of knowledge on the subject matter acquired. Users are only asked this question, once they complete both the quiz and the video.

Both parts of the research agent, therefore, form part of the instrument and is applied in the context of this study. The combination of both parts of research agent, indicates the level of awareness and education before and after the instrument has been used. All five quizzes and related videos follow the research agent outlined in this section. The instrument's implementation will be presented in the following section.

3.5 Implementation (Experiment)

The research agent was distributed through social media channels in the form of the final instrument. The distribution took place primarily through a Facebook campaign which took place in partnership with SABRIC. This allowed for a wider audience to be reached, as SABRIC is an authority in the local banking environment. The initial campaign began on the 27th of March 2018. SABRIC released a media statement alongside a sponsored Facebook campaign. The sponsorship consisted of promoting the associated videos themselves through paid adverts on YouTube and promoting the quizzes via sponsored adverts on Facebook directly. This sponsorship allowed for a greater target audience to be reached. While the campaign was being run, the quizzes were also shared from other sources. These sources included, the researcher's own Facebook and any participants that opted to share the quizzes themselves. At present the social media campaign is still ongoing, as such participants are still taking part in quizzes and viewing the educational videos.

The following section will discuss the results of the research agent with the focus being on the topic: online shopping.

4 Analysis and Results

As mentioned previously, there are five quizzes with five related videos. Quizzes are based on topics most prevalent to users of cyber-driven financial transactions, according to SABRIC. This section will discuss the results of a single quiz, namely; online shopping, as the social media campaign is still ongoing and part of a larger research project.

At present, the online shopping quiz has 420 participants of which 86% fully completed the quiz. This results in a total of about 389 participants. 57% of participants were female and 43% were male. A small number of participants accessed the quiz via a mobile device (37%) while the majority of participants accessed it via their desktop machine (63%). Due to social media being accessed worldwide, participants were not only from South Africa. At present 92.2% of participants are South African, while 1.8% are United States citizens, 2.4% are United Kingdom citizens, 3% are Icelandic citizens and 0.6% are from other countries.

Within the quiz, six questions relating to online shopping were asked. These questions were asked before mention was made to the associated educational video. Only once a participant has completed the initial quiz, they can view the associated video. Once the video was watched, a follow-up question was asked, in order to assess if the participant felt he/she learned something from the quiz and related video. The overall results show that participants, regardless of their score, felt as though they had learned something and that they could conduct their cyber-driven financial transactions in a more safe and secure manner. The table below shows the results for the online shopping quiz.

Question Number	Correctly Answered (%)	Incorrectly Answered (%)
1	89.0	11.0
2	51.4	48.6
3	94.4	5.6
4	79.6	20.4
5	61.9	38.1
6	75.4	24.6

Table 2. Online Shopping Participant scores

As seen in the above table, participants scored well in the quiz. Due to the videos being promoted separately from the Facebook quizzes, the online shopping video was viewed at present 38 141 times. One hundred percent of the users that answered the poll, responded positively to the question whether the video was indeed useful and added value. It can be seen from the number of views recorded that users preferred to go directly to the video rather than following the quiz-video route. This might be interpreted that a large number of users are already aware they lack proper knowledge to deal with the cyber threats they face. Irrespective of the standalone YouTube video views, results show that a combination of both the quiz and video can be a successful educational combination. In general, this study confirms that participants gained relevant knowledge and confidence on how to conduct online shopping safely and securely in cyberspace, through a social networking educational approach.

5 Conclusion

Cyber-based services are found in many businesses and industries today. This is particularly true in the banking sector, where users make use of ATMs, internet and mobile banking. These users of cyber-driven financial transactions pose a great risk to themselves, through negligent or ignorant behaviour. Therefore, relevant cybersecurity education and awareness is a must for these users. Social media and social networking can indeed be used as an educational tool towards effective cybersecurity education, under the following conditions: firstly, the material can be accessed with ease, secondly, the material is appealing to users and thirdly, that the material is not too data and time-consuming.

This study has shown that if implemented correctly and made appealing, users can be made more aware and educated through the means of social media. Allowing them to conduct their cyber-driven financial transactions in a more safe and secure manner. It is therefore concluded that, social networking and social media in general and specifically in the format used in this study, can be a possible option for the education of users of cyber-driven financial transactions. However, further research should be done to improve the process.

6 Future Work

The results shown in this paper is part of a larger ongoing study. The next stage will be to complete the social media campaign and verify all quiz results to show statistical significance. This will allow for the educational approach of utilizing social networking for cybersecurity education to be verified.

7 Acknowledgements.

The South African Banking Risk Information Center (SABRIC) is acknowledged for their contribution towards this research project.

8 References

Al Awawdeh, S., & Tubaishat, A. (2014). An information security awareness program to address common security concerns in IT unit. *ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations*, 273–278. https://doi.org/10.1109/ITNG.2014.67

Aloul, F. a. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, *3*(3), 176–183. https://doi.org/10.4304/jait.3.3.176-183

Boland, G. (2017). What to know about quizzes on social in 2017 - NewsWhip. Retrieved March 2, 2018, from http://www.newswhip.com/2017/04/know-quiz-content-2017/

Five, T., Campaign, S. F., Office, H., Taskforce, J. F., Fraud, F., Uk, A., & Five, T. (2017). 2017 half year fraud update : Fraud : January to June 2017, (September).

Frauenstein, E. D., & Von Solms, R. (2014). Combatting phishing: A holistic human approach. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*. https://doi.org/10.1109/ISSA.2014.6950508

Horn, S. (2010). *Cyberville: Clicks, Culture, and the Creation of an Online Town*. Grand Central Publishing. Retrieved from https://books.google.co.za/books?id=7VGZCwAAQBAJ

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Ombudsman Annual Report for Banking Services. (2016). Ombudsman Annual Report 2016 for Banking Services.

Statista. (2017). Worldwide 2017 | Statista. Retrieved March 2, 2018, from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security*. *Course Technology*. https://doi.org/10.1016/B978-0-12-381972-7.00002-6

Whittman, M. E., & Mattord, H. J. (2013). Management of Information Security Fourth Edition, 545. https://doi.org/2013945552