NovoVerse Undergraduate eJournal

Volume 1 · Issue 1 · June 2018

The Fight Against Fraud: An emphasis on the role of people and processes over technology achieved through the incorporation of Gamification

Authors:

Gary Roche: g.roche7@nuigalway.ie
Niall Keane: n.keane9@nuigalway.ie
Katie Keaney: k.keaney1@nuigalway.ie
Daire Flanagan: d.flanagan16@nuigalway.ie
Conor Hoy: c.hoy1@nuigalway.ie

Supervisor:

Dr Eoin Whelan

Business Information Systems, J.E. Cairnes School of Business & Economics, National University of Ireland, Galway

Abstract

New threats and hacking methods emerge every day, proving the online consumer is an increasingly growing target. In the age of multi-million-euro data leaks and thefts, to voluntarily giving away personal information on social media, users must be educated on how they are unwittingly putting themselves at risk to be fraudsters next victim. Banking customers are at the ultimate risk of having their personal information stolen in ways no one thought was possible such as covert channel attacks or the stealing of data through hackers use of mobile sensor data. This paper provides insights into the latest hacking threats, and how the use of biometrics and multi-factor authentication can help users to combat these issues. The project also explores human psychology, the consumers brain, and how gamification can be used to nudge users towards a safer online lifestyle. Ultimately, the aim of this report is to prove that no matter how much prevention technology is in place, education is paramount in order to fully secure a user and their data.

Keywords: *Cyber-security, Biometrics, Multifactor authentication, Gamification, Online Banking.*

Introduction

This paper is structured as follows: The first section of the report includes a literature review. Such details and evaluates the various existing sources of information which were utilised to draw the findings of the report in the areas of emerging future threats, the importance of "people and processes over technology", biometrics and gamification. There then follows a section on the methodologies used in this research. This section describes the data gathering processes involved throughout the projects course. Following such, a findings section details the information derived from the project research. Finally, a discussion section provide insight regarding the solution provided on the basis of the research conducted, data gathered and finding derived.

Literature Review

Future Threats

Several forms of future threats were considered as part of the research conducted. Drawing on the work of (Mordechai Guri, 2017) and (Elovici, 2017), we explored two forms of covert channel attacks, namely DisFiltration and Magneto. This research conducted at the Ben-Gurion University of the Negev in Israel based on experiments carried out at their Cyber Security Research Centre. These experiments which they conducted show the real possibility of how easily sensitive data can be exfiltrated from an infected computer or server to a hackers device through acoustic and magnetic signals. Additionally, research conducted by (Bhasin, 2017) at the Nanyang Technological University, Singapore details how user login credentials can be stolen from their phone via the motion sensors embedded within it. This is definitely something that constitutes a future potential banking security threat so information from this source was referenced in the final project. The current study also examined a report by (Newlin, 2016) of the Bastille research team. This report outlines how it is possible for hackers to intercept the radio frequency between some wireless keyboards and their USB dongles enabling hackers to eavesdrop on unsuspecting users and see what they are typing. This new form of threat has the potential to cause serious security concerns for those affected.

People and Processes over Technology

The people and process over technology section in the report looks to emphasise a possible key area of weakness in data security by iterating the point that the people who interact with the system may prove the easiest point of access for a breach in the system in the gaining of sensitive data to carry out malicious transactions. The report illustrates this point by drawing on the findings of (Shey, 2013) which explain how the greatest volume of security breaches at "36%" comes from insider negligence in that they inadvertently misuse data. It continues to outline of how it is common practice amongst employees to unwittingly share sensitive data or information carelessly. Employees casually share confidential highly sensitive information inappropriately online often giving the ids and login credentials to other employees either out of necessity or to make work collaboration easier without realising the detrimental effect this could have on keeping data secure.

Waugh (2013) lays out tips for end users or customers of online banking apps as well listing some examples of some of the latest techniques and phishing techniques of hackers to gain customers information. The article continues by detailing the lengths cybercriminals will go in order to carry out their fraudulent activities as well the correct course of action in staying safe online. Finally, it details how to recognise behaviour and the tell-tale signs to look out for when attempting to catch out fraudsters and phishers in the act.

Biometrics

The extant research on Biometrics is extensive, a significant percentage of which argue why such technologies should be considered as a primary source when attempting to secure a user's personal data. The review of this research conducted for this study lent credence to the theory that biometrics should be used as part of Multi-Factor security in order to guarantee additional security. Although many claim Biometrics is fully secure, our report explores the idea that biometrics should be used as only part of a higher standard security method. One noteworthy study in this space is a study carried out by the Institute of Electrical and Electronics Engineers, named "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems (Roy, Memon, & Ross, 2017). This study explores the possibility of Master prints which can bypass any fingerprint scanner and the threat partial fingerprint readers pose to the user.

The undeniable importance of dual and multifactor was supported by research papers such as "Why You Should Start Using Two-Factor Authentication Now" (Chipurci, 2016) and "The Importance of Two-Factor Authentication" by (Powers, 2017) stating that without using at least dual-factor authentication, a user is putting themselves and their data at a larger risk. Given the substantial number of risks faced by end users of banking applications and the internet daily, it is critical that the optimum number of varying security features are set in place to protect each of those potential fraud victims, which may very well include the incorporation of Biometrics.

Psychology

An important aspect of this study aimed to increase customer awareness regarding the existence of security threats online. The research conducted to date proved that little awareness existed in this problem area and so, the question was posed, "How can banking institutions attempt to intrinsically motivate end-users of their banking applications (both web and mobile) to make their online banking applications more secure?".

With such questions posed, the project team investigated the "Stages in Consumer Decision Making Process". Written by (Juneja) and reviewed by the Management Study Guide Content Team, this study outlines a generic five step decision making journey regularly repeated by consumers during the process of purchasing goods and services.

The consumer decision-making journey study outlined the following to our project team: It was found that the influence of external factors often initiates a consumer to engage in a decision-making journey. With that in mind, this study attempted to identify external factors that could possibly lead to banking customers becoming more aware of current fraud trends and in turn, the steps that can be taken to mitigate the risk of falling victim to fraudulent activity. Research online proved that two possible external methods could be applicable to this use case, digital nudging and gamification. Both digital nudging and gamification are similar in that they incorporate technology and an in-depth knowledge of human behaviours in their attempt to heavily influence consumer decisions and behaviours.

While researching different methods of digital nudging, members of the project team discovered an article composed by (Ariely, 2008) called "3 Main Lessons of Psychology". It discusses the "opt-in vs opt-out" method which proves that consumers are more inclined to opt into a service when the use of double negative language is present. An example: The Netherlands have a high rate of organ donation in comparison to other EU countries. This is because individuals in the Netherlands are asked to "opt-out" if they would *not* like to have their organs donated. This can be compared to countries who have low rates of organ donation, whereby individuals are asked to "opt-in" if they would like to donate their organs.

An additional study helped to reiterate the notion that digital nudging and gamification should be considered as possible external factors for influencing consumer decision. The study in question is "The Big Donor Show", written by (Harrebye, 2012). Again, this study proved to our project team how human psychology can be used as a tool to encourage preferred human behaviours.

Gamification

Gamification is concerned with the application of "video game elements in non-gaming systems to improve user experience (UX) and user engagement", (Deterding, 2011), as well as attempting to steer users' behaviours toward preferred outcomes. Gamification can often be misinterpreted as being solely associated to the gaming world. After being transferred from the Gartner Technology to Educational Hype Cycle in 2014, it is now apparent for gamifications potential to improve society practices and behaviours in the attempt to reduce the levels of cybercrimes and online financial fraud. The gamification model canvas, (GameOnLab, n.d.), has enabled the formulation of the gamified application proposed by the project team. Included are the proposed game components, mechanics, dynamics and their resulting aesthetics, behaviours and simplicities. It also outlines the platforms, players and costs required as well as the resulting revenues. The objectives, game design elements, IT-based gamified enhancing services and core offerings of the proposal too are illustrated using a widely cited gamification framework, (Leimeister & Blohm, 2013). The use of such a framework helps to illustrate how gamification can be successfully incorporated into banking institution applications globally to successfully combat against online banking fraud. The possibility of Gamifications successful incorporation is achieved through its ability to educate and raise awareness via gamified elements incorporated into end-user applications, whereby rewards are generated for the end user's active participation.

Methodology

With a goal of determining a list of information security concerns that are important in practice a "belief elicitation" process was begun (Limayem & Hirt, 2003), involving professionals in the field. This process took the form of a series of interviews and meetings with experts /practitioners in the field, which informed the design of two subsequent surveys.

Interviews and phone calls were designed to be exploratory so that the general perception surrounding online banking security and fraud could be explored as well as providing an opportunity to gain some insight into the thoughts of experienced professionals in the security and banking industries. Building on the findings from these interviews, two separate surveys were constructed to further examine some of the key themes that emerged. The purpose of such aimed to help research identify where areas of improvement could be made as well as possible solutions that could be implemented. These two methods of data gathering were chosen for specific reasons. Interviews and phone calls provided the opportunity to gather information in the most personal and adequate manner so that this current study could reap as many benefits as possible from the data gathering. Also, surveys represented the most effective way to get information from real consumers in a sufficient quantity while interviews formed the best.

Interview with Fraud Prevention Manager, an Irish banking institution.

After an arising opportunity was identified, the decision was made to interview the Fraud Prevention Manager of an Irish banking institution who wishes to remain anonymous. The Fraud Prevention Manager was considered an expert in his field and therefore a vital contributor to the projects field research. The interview sought to provide feedback regarding his thoughts on the potential future threats in the area of online fraudulent activity as well as

his thoughts on potential technologies that could combat against such future threats. Developed by the project team, an interview protocol was used throughout the course of the interview. The interview itself was conducted over a mobile phone call, of which lasted a total duration of 28 minutes.

Interview with Dell

As part of an attempt to gain some new primary information that was not available online, we were given the opportunity to visit and interview a cybersecurity expert, Richard Parker and his team in Dell, Limerick. This meeting gave us the opportunity to get first-hand information on the steps companies are actively taking to combat new security threats. The meeting was one hour long and consisted of talking openly with 5 team members and asking them about the measures they take to protect their customers. The interview was semi-structured, based loosely around an interview protocol but moved deeper into some areas when appropriate. Contemporaneous notes were taken by all group members for analysis following the interviews conclusion.

Dell Threat Hunters

Following on from the site visit to Dell that consisted of a meeting with their cybersecurity team, an opportunity presented itself to arrange a video conference call with Dells Threat Hunter team based in Romania. Because this opportunity was anticipated as a rich source of understanding regarding the subject matter, a meeting was set up with the contact Paul Ivan. Paul is a senior support engineer of strategies and techniques based in Bucharest and his experience and knowledge base proved an invaluable addition to the current study. The purpose of this meeting was to try and determine what the latest fraud trends that he has seen in his line of work are and also if he predicts any new emerging threats becoming prominent in the future as technology advancements continue. The conference call included Richard Parker, Paul Ivan as well as our team and lasted 35 minutes in total. We had a structured interview with Paul aided by set of questions that one team member posed to while the rest of the team members took notes on his responses.

The following is a table detailing the time spent collecting primary data through interviews, and the total duration of such interviews. This phase of the project lasted a total of 123 minutes which enabled for the sufficient collection of information that was not available online.

Interview	**Length (in minutes)**
Fraud Prevention Manager	28
Dell	60
Threat Hunters	35
Total time spent interviewing:	123
Average Interview Time:	41

Table 1: Interviews conducted and their duration

Findings

In this section, the report discusses the results derived from the project field research conducted as well as from two compiled surveys as completed by a total of one hundred and

thirty-four members of the public. The first survey complied looked to identify the general public's opinion on banking security while the second aimed to gain insight into the current state of fraud awareness amongst the general public.

The conducted field research provided some very useful results that helped in the decision-making process for choosing a project vertical. From meetings conducted with Dell, the Irish banking institution fraud prevention manager and the Dells Threat Hunter team, a common trend was identified. All interviews conducted similarly outlined that as the technology to combat online fraudulent activity advances/ changes, so too will the technology used to commit those online fraudulent activities. Data collection from the field research identified that the adaptation of new technologies as a means of combatting against online fraudulent activity will only result in winning a battle against online fraud, but not the war. Therefore, in the long run battle against online fraud, technology alone will not produce any significant decreases in the overall level of fraudulent activities committed. This pointed out to the project team that technology as a primary tool is insufficient and therefore should be used in collaboration with other key combatting tools and/ or strategies. On the contrary, all fraud experts clearly outlined that in the long run, an emphasis should be placed on the people and processes rather than technology when attempting to combat against online fraudulent activity. It was identified that the people and/ or processes are often the weak link and therefore the primary target when fraudulent activities are attempted. Rather than abandoning technology and focusing solely on people and processes, it was decided to explore how technology, people and processes can work together in an intertwined fashion and therefore in an innovative way to combat against online fraudulent activities.

Based on the main finding from the qualitative aspect of our research that people and processes are the most vulnerable and therefore the primary target for fraudsters, a survey was compiled for the general public that set to prove this point further. The results of this survey clearly aligned with the opinions of field experts we had engaged with via the various meetings. In particular, a significantly large portion (65.1%) of those who completed the survey outlined that convenience of web surfing was superior to their concern regarding a free public Wi-Fi networks source (as can be seen in Figure 1).

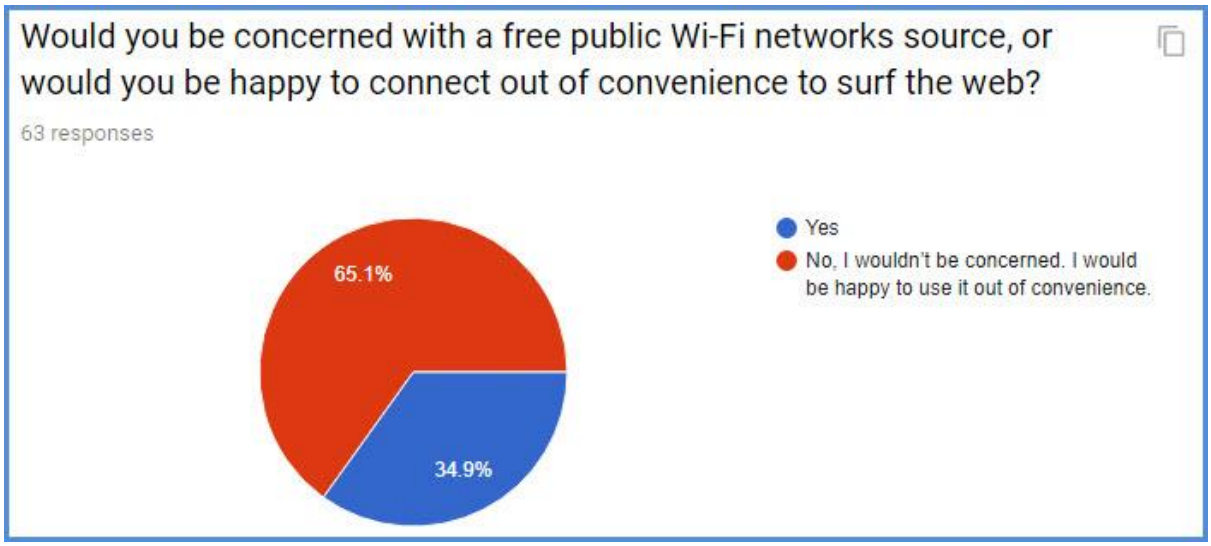

Figure 1: Survey response on free public Wi-Fi connections concerns

Additionally, 71.4% of survey participants admitted to accessing personal information such as online banking or other personal details when connected to a public Wi-Fi network (as can be seen in Figure 2). These two findings have not only support the experts point that an emphasis should be placed on people and processes, but also helped to highlight the significance of the current problem and need for absolute prioritisation of investigating people and processes in depth in a bid to understand what can be done to significantly reduce the number of online fraudulent activities resulting from bad people and process practices.

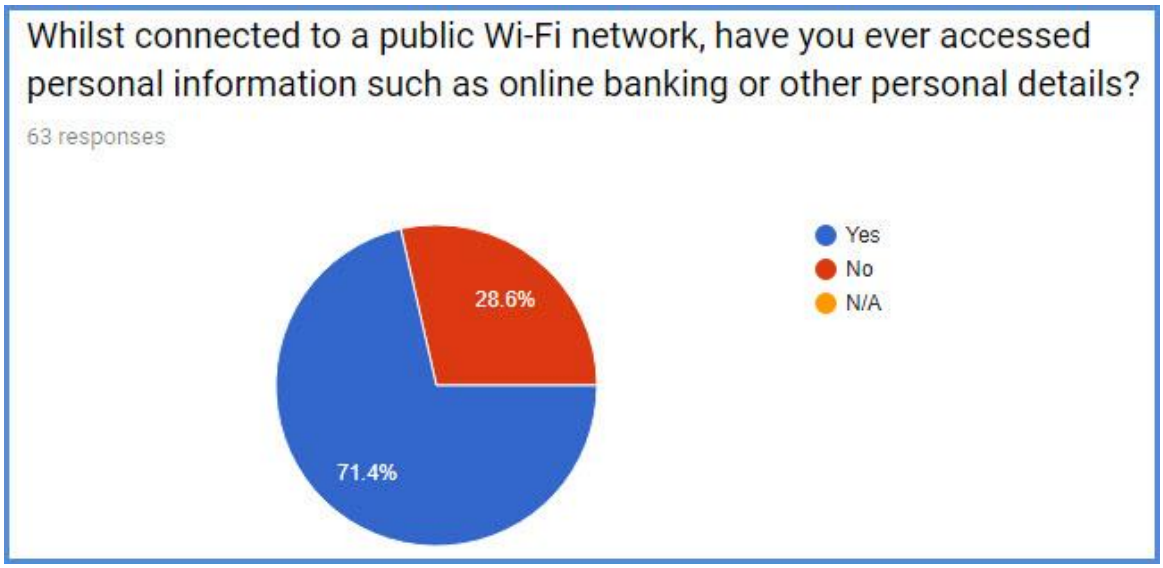

Figure 2: Survey response regarding the accessing sensitive information via public Wi-Fi networks.

In a bid to reiterate the significance of the people and process problem present for banking institutions worldwide, 50.8% of survey participants replied "no" when asked whenever they are browsing the web on a public Wi-Fi network whether they check to see if a website is HTTPS secured. A further 15.9% of replied "I don't know what this is" in relation to the term "HTTPS" (as can be seen in Figure 3). It cannot be emphasised how vulnerable people and processes are when analysing online fraudulent activities and steps that can be taken to combat against such criminal activity. By including these findings within the report and highlighting the associated severity, it helps to formulate the basis for the need to urgently address the issue as well as the need to devise a plan which aims to effectively tackle the issue.

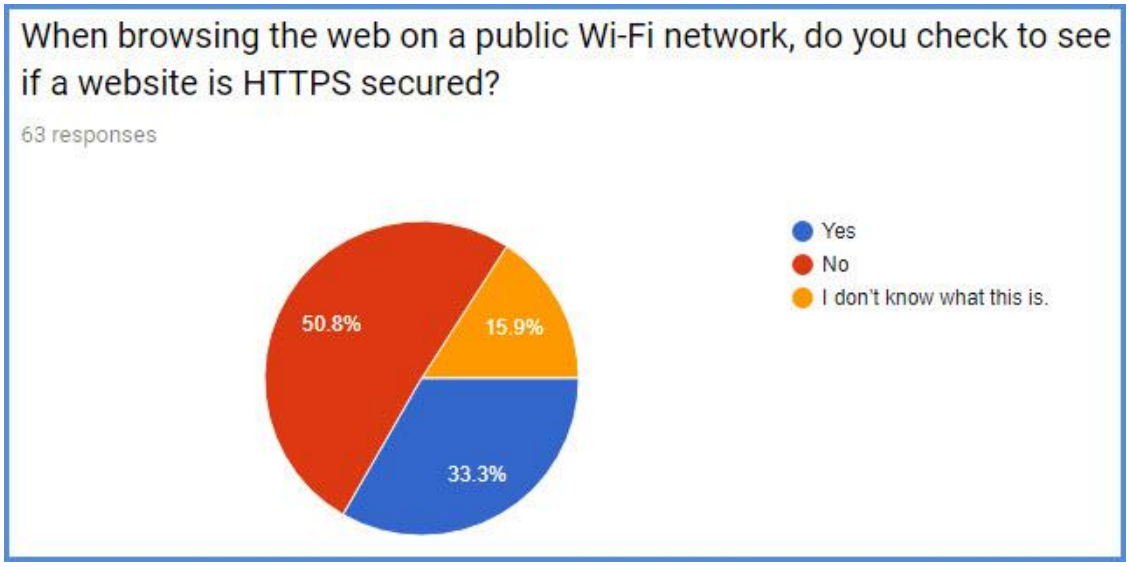

Figure 3: Survey response to public knowledge regarding HTTPS and its importance

Further research conducted by the project team via the internet proved a significant increase in the number of consumers who engage in online banking, (as can be seen in Table 2).

	Europe	**North America**	**Asia/ Pacific**
2013	35.4	46.5	102.1
2014	44.6	60.9	120.8
2015	54.1	75.5	141.4
2016	64	90.7	163.6

Table 2: *Number of mobile payment users from 2013 – 2016, by region (in millions),* (Statista, 2017).

Statista (2017) state a significant increase in the use of mobile payment users in Europe, North America and Asia/ Pacific regions. Particularly the Asia/ Pacific region, which over a short three years has seen the number of mobile payment users increase by 61.5 million. It is now evident that a significant increase regarding the number of mobile payment users exists as well as the vivid understanding relating to the vulnerability of people and/ or processes in the eyes of fraudulent activity and cybersecurity concerns. Furthermore, it establishes the need for developing a strategy necessary to help reduce the overall level of fraudulent activities that occur annually due to bad practices in relation to both processes and people.

With regard to biometrics, the survey has indicated that 47.2% of people find fingerprint authentication a more convenient method of login while 36.1% find it to be both more convenient and more secure (as can be seen in Figure 4). Consequently, our project team believe it is necessary to focus on incorporating more unusual biometric authentication features as a means of enhancing security login requirements as well as customer satisfaction.

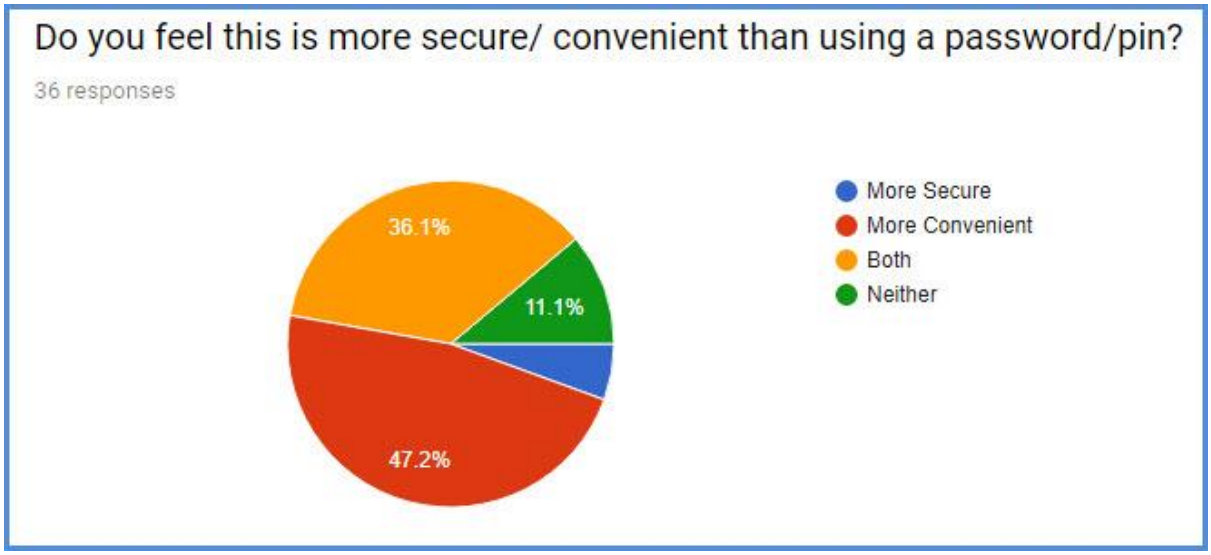

Figure 4: Fingerprint authentication responses

As previously stated, the total response rate to both survey conducted was one hundred and thirty-four people, which gave the project a true insight into how consumers behave in certain circumstances. Survey participants were contacted through social media channels such as LinkedIn, and emails were sent out to students of NUI Galway.

Survey	**Response Rate (in people)**
Banking Security	71
Publics fraud awareness	63
Total survey responses:	134

Table 3: *Number of survey participants.*

Discussion

The common theme that emerged from the project research findings was that people are often the root cause of the problems relating to online and mobile banking security. Even as technology advances and hackers learn new techniques it is human error that remains centric to allowing attacks to occur. This project focuses on highlighting this issue and determining an effective way to educate customers on security issues without negatively impinging on their banking experience.

In order to get through to customers in a way that would successfully encourage them to engage with the security material provided it was necessary to examine the psychology behind how customers choose options placed in front of them. The goal is to have the bank's customers safe online. Educating customers as to why they should have security settings in place and keeping them up to speed with the latest forms of attacks is how to do this. If these settings are forced on people the bank could have bad publicity and even lose customers. Also, it was shown that just making the security material available is not enough to make customers take head of it. Consequently, it was necessary to find a way to have a balance between making every customer secure within the system but without making them feel like they were doing something against their will and feeling dissatisfied towards their banking experience as a result.

The solution proposed in the project to tackle this issue is Gamification. This study identified gamification as a means of creating a way in which banking customers would be happy and willing to educate themselves and improve their overall banking security by engaging with material provided and enabling various login features. In order to do this a "Protect and Reward" model was conjured which essentially gamifies the online and mobile banking security experience so that customers are offered incentives in return for educating themselves to become more security conscious. Based on the survey conducted as part of the project research it was discovered that over 94% of people do not actively check their banks website security section but 89.6% would be willing to do this in return for a free gift e.g. coffee (as can be seen in Figures 5 & 6). The proposed "Protect and Reward" model would facilitate this. Customers would be able to earn points by engaging with security content provided within their online or mobile banking which they could save up in exchange for gifts. Also, the more points they earn enables them to progress through the levels of the secure consumer scale.

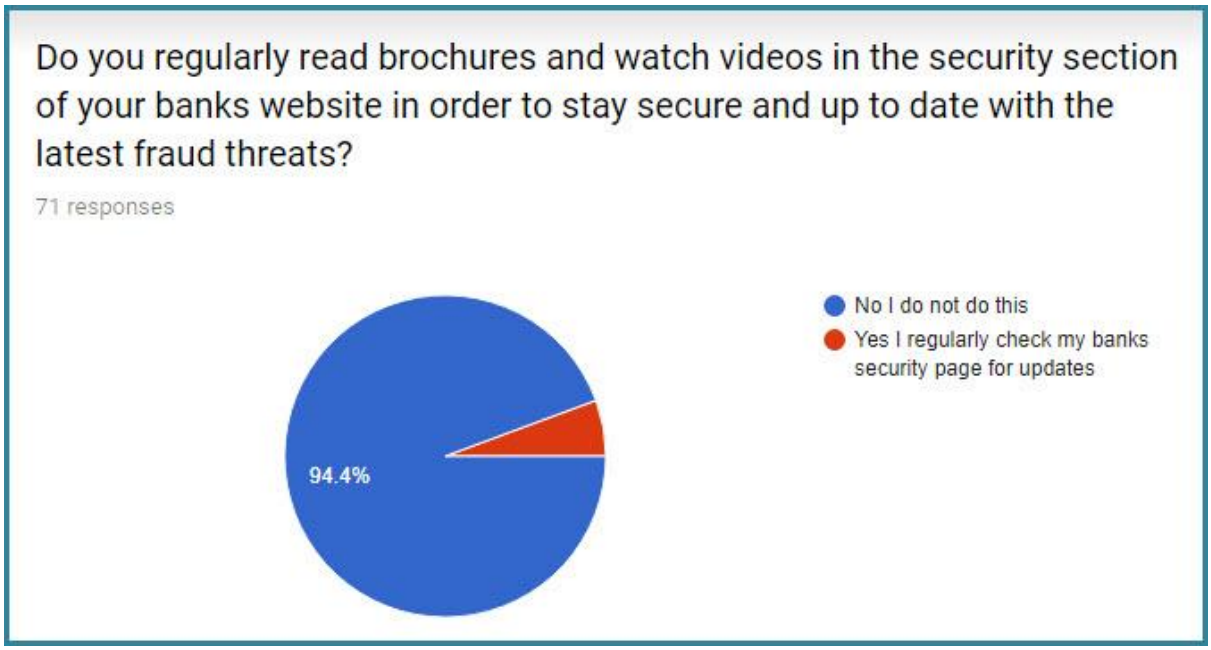

Figure 5: Current security education

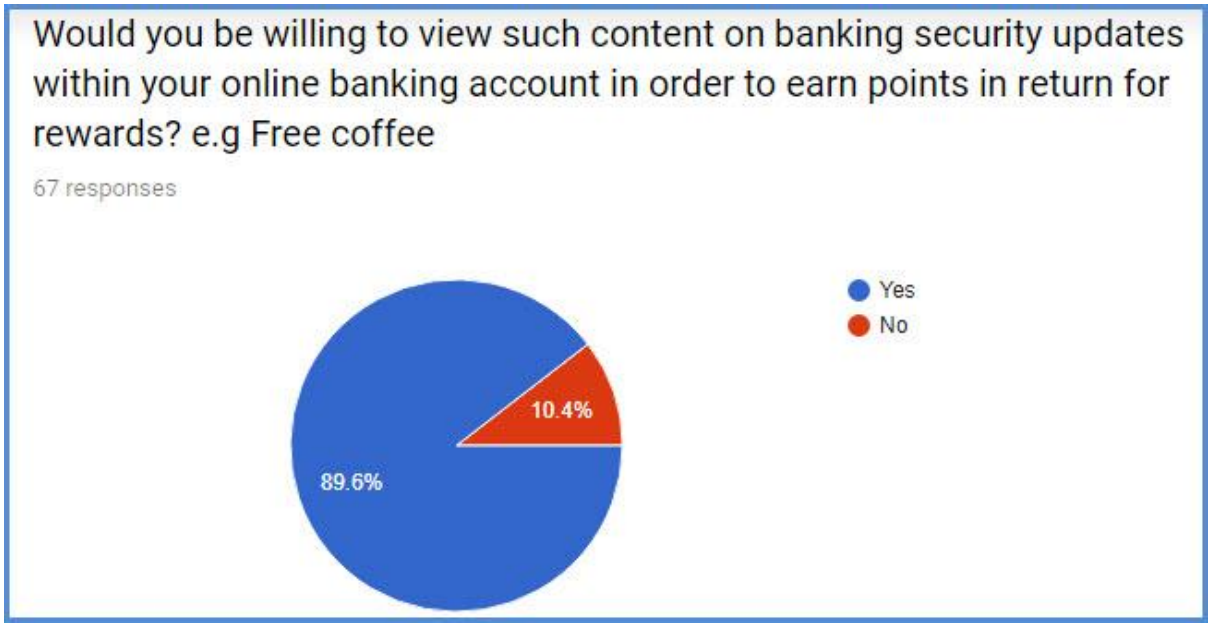

Figure 6: Potential popularity of implementing gamification

While studying the psychology behind what encourages end-users to engage with gamified applications, the project team identified a number of motivating factors. The first of these motives could be curiosity. This is something that the vast majority will never have experienced on a banking website. As a result, our team feel that customers would be motivated by their own curiosity to engage with mobile banking applications and their associated websites if such motivators were to be incorporated successfully. Secondly, a sense of achievement could prove to be a factor in encouraging consumers to engage with the new gamification process. People will get a sense of accomplishment from achieving higher levels on the secure consumer scale which will also make them feel positive about their banking experience as a whole. Finally, the rewards themselves will prove to be the main factor in getting consumers on board with the gamification. Consumers will be more than happy to become more secure and educate themselves further on security if they are receiving rewards in return. Based on these factors it was evident that the "Protect and Reward" model met the required criteria to attract customers to the gamification process in this instance, so this is what was proposed.

Also derived from our findings in relation to password and biometric authentication was the requirement to introduce multi-factor authentication. It was clear from the findings that passwords alone or a singular form of biometrics does not suffice in offering secure enough customer accounts. It is much better to incorporate both password and at least one form of biometric authentication if not more and that is what the project proposes. The research also recognises that added security measures can be a cause of hindrance for customers when logging in and that is why this study homes in on biometric authentication and the relative ease of use that it poses to the login procedure. Biometrics offer an easier and more secure means of logging in and the project identifies this.

Conclusion

In conclusion, the research this project entails has allowed us to come to the following realisation.

Firstly, the research has outlined the potential for future threats that may very well be used in the attempt to commit fraudulent crimes. By identifying such potential future threats, this report has succeeded in outlining that the technology used to combat against fraudulent activity alone will not suffice due to the constant unknown alterations of the technology used in the attempt to commit such crimes. Indeed, the current technologies set in place to combat against fraudsters lack in their capabilities to prevent against attacks such as covert channel attacks or data hacks through mobile sensors. This project attempts to raise awareness in relation to these potential future threats by highlighting their existence so that the appropriate safety measures can be implemented.

Secondly, the biometrics research conducted illustrates that multifactor authentication is the future of online banking. Users are unaware that they are putting themselves at risk every day of falling victim to fraud. The use of multifactor authentication should be a minimum requirement in terms of steps end-users should take to protect their mobile banking accounts. A combination of both password and biometric protected accounts is recommended for sufficient security measures as we have uncovered that when both methods act as standalone security measures breaches are a real possibility.

In addition, from the findings from all aspects of the research, it was identified that most people are not sufficiently educated regarding their potential to fall victim to online fraudulent activities. That is why it all comes down to the people and processes over the technology when looking at ways to significantly reduce the losses banks incur from online related fraudulent activities. This project concludes that technology alone is insufficient as a primary tool to combat against fraudulent activity, but rather an emphasis should be placed on educating customers to become more secure.

Finally, from our realisation that the root of online banking fraud is people-centric, the clear solution that emerged was gamification. The “Protect and Reward” model that is outlined in the project addresses the need to effectively educate consumers and encourage them to engage with the security material. Gamification provides a way to educate consumers without impinging negatively on their banking experience. It would appear from the research conducted for this study that this is a model that could easily adopted by banking institutions and allow them to reap the rewards their more secure customer base would bring them.

These are the outcomes which this project has brought to the attention of the authors included. It is recognised that this research has implications for research and practice. A particular implication being that the proposed solution is yet to be proven in practice to successfully reduce fraudulent activity levels. The project team believe that future studies have the potential to build on the findings of this research. It is also recognised that advancements in gamification design may very help to improve the success potential associated with the proposed application.

Bibliography

Ariely, D. (2008). Retrieved from 3 Main Lessons of Pyschology: http://danariely.com/2008/05/05/3-main-lessons-of-psychology/

Bhasin, S. (2017). *There Goes Your PIN Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting.* Singapore: Nanyang Technological University.

Chipurci, C. (2016). *Why You Should Stop Using Two- Factor Authentication Now .* Retrieved from Hemidal Security: https://heimdalsecurity.com/blog/start-using-two-factor-authentication/

Deterding, S. (2011). *Gamification: Using Game Design Elements in Non-Gaming Contexts.* Vancouver.

Elovici, M. G. (2017). *Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise ('DiskFiltration').* Oslo: ESORICS: European Symposium on Research in Computer Security.

GameOnLab. (n.d.). *Gamification Model Canvas*. Retrieved from http://gecon.es/wp-content/uploads/2016/04/gamification_model_canvas_v02.pdf

Harrebye, S. (2012). *Beautiful Trouble: A Toolbox for the Next Generation, 2012.* OR Books. Retrieved from Case Study: The Big Donor Show: http://beautifultrouble.org/case/the-big-donor-show/

Juneja, P. (n.d.). *Consumer Decision Making Process.* Retrieved from Management Study Guide: https://www.managementstudyguide.com/consumer-decision-making-process.htm

Leimeister, P. D., & Blohm, D. I. (2013). *Design of IT-Based Enhancing Services for Motivational Support and Behavioral Change.*

Limayem, M., & Hirt, S. (2003). Force of Habit and Information Systems Usage: Theory and Initial Validation (4:1), . *Journal of the Association for Information Systems*, 65-97.

Mordechai Guri, A. D. (2017). *MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU Generated Magnetic Fields.* Oslo.

Newlin, M. (2016). *www.keysniffer.net.* Retrieved 03 19, 2018, from https://www.keysniffer.net/technical-details/

Powers, A. (2017). *The Importance of Two Factor Authentication .* Retrieved from CORE: https://www.helpmecore.com/two-factor-authentication/

Roy, A., Memon, N., & Ross, A. (2017). *MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems.* Retrieved from IEEE Explore: http://ieeexplore.ieee.org/document/7893784/

Shey, H. (2013). *Understand The State Of Data Security And Privacy: 2013 To 2014.* Forrester.

Statista. (2017). *Number of mobile payment users from 2009 to 2016, by region (in millions)*. Retrieved from Statista: https://www.statista.com/statistics/279957/number-of-mobile-payment-users-by-region/

Waugh, R. (2013, September 12). *A scam-spotters guide: Ten things your bank will NEVER do – but cybercriminals will.* Retrieved from www.welivesecurity.com:

https://www.welivesecurity.com/2013/09/12/a-scam-spotters-guide-ten-things-your-bank-will-never-do-but-cybercriminals-will/

Authors Biography

The authors of this report consist of five final year Business Information systems students enrolled in the National University of Ireland, Galway. Their key interests reside in the areas of Cyber security, Project Management, Gamification and User Experience Design. These interests have been derived through their active involvement and participation in Business Information Systems throughout the four years of the course. All authors have contributed significantly to several projects throughout their time at University, projects of which aimed to create value through the use of innovative and creative technologies. Outside of the authors participation in the course, each of them has keen interests relating to current affairs surrounding emerging technologies and hacking breaches which proved very relevant to the project research. All authors can be reached through the emails provided above.