International Journal of
Applied Mathematics,
Electronics and Computers

ISSN: 2147-8228 http://ijamec.atscience.org

Advanced Technology and Science

Original Research Paper

It's all about me! The Influence of Personality on Susceptibility to Mobile Security Attacks#

Rasha Salah El-Din *, Paul Cairns, John Clark

Accepted 15th August 2014 **DOI: 10.18100/ijamec.47036**

Abstract: Mobile phones security is an emerging field of study. As the number of data-centric mobile phones grows, the industry experts expect them to face major security problems. We believe the first step to devise countermeasures for protecting users would be a comprehensive understanding of the mobile users' perception of risk. We report on a qualitative grounded theory study to inspect such perception. The initial thematic analysis identified relationship between level of knowledge and security attitude. However, further grounded theory analysis returned in personality type taxonomy for exposure for mobile attacks in general and phishing attacks in particular. We confirm our findings by conducting the first naturalistic phishing experiment on mobile phones.

Keywords: *Phishing, Personality, the Big-Five, Mobile, Cyber-security, Human Factors, SMS, Text Messages*

1. Introduction

The small size, high connectivity and mobility provided by mobile phones empowered them to be one of the most used devices all over the world. Yet, that at same time let mobile phones subject to different security threats. A recent study by Informa Telecoms [1] had put mobile malware and phishing on top of mobile security threats. Mobile malware has witnessed a rapid evolution since 2004, the number of malware families has trebled causing mobile data damage, disabling mobile operating systems, calling high premium rate paid services and downloading files from the Internet. In 2010, 65.12% more new malicious programs targeting mobile devices were detected than in 2009, and over 17 months they nearly doubled in number [2].

Regarding phishing attacks, mobile phones are vulnerable to new types of phishing; Vishing and Smishing. The former depends on using voice for phishing by phoning the victim and asking her to reveal confidential information. The later uses short message service to mount phishing attacks. Both types of attacks can be performed via context aware phishing that is called 'spear phishing'. Dunham et al. [3] define spear phishing as an attack targeting specific group at specific time. Actually, the relationship of a phishing attack to the time of its delivery and to the time of its interpretation forms a ground for determining whether the attack would work as expected or not. Imagine an email asking you to follow a link for electronic voting when there is no elections currently taking place. It would certainly lose its credibility. On the contrary, if a phishing message, asking the victim to click on a link for car accident insurance claim, hits a person who had just had a car accident, the probability that she would trust the message is extremely high. There is also a technological context concerned. It is related to the technological device on which the victim has received the phishing message. That includes the type of the network, the services provided and possibility of mobility of the victim. The spatial context that mobile phones provide denotes the physical surroundings where the victim is existed at the time of hacking. In principle, that refers to the place at which the victim receives the phishing message but comprehensively, it implies the situation as a whole; the overall atmosphere around the victim, the location, the activity performed, noise and even weather.

Apart from the above mentioned contexts and the high level of persuasion they may add to the phishing message, the mental context remains the decisive factor. To contribute to an understanding of the variables involved in such socially based interaction, we have undertaken an interview study to examine the mobile users' security patterns with regard to the different contexts explained above. We have analyzed their perception, decisions and strategies they used for securing their mobile phones. Our analysis also discussed three different theories to reach the dominant feature responsible for mobile users' security behavior. We confirmed that certain personality qualities are the main factor that guides such behavior.

2. Grounded Theory

The main goal of our investigation was understanding how mobile phones security issues were perceived and experienced by different mobile user groups. Special focus was given to mobile phishing attacks represented in Vishing and Smishing. As our emphasis was not on measuring numbers as much as understanding the qualities of such socially based issues, a qualitative study was conducted. It was highly important to understand what people think and also feel about mobile security, and at the same time relate these concepts to real life social structures. For example, the users' attitudes towards mobile security are provoked by economic, social, psychological and technological drivers. For that reason, it was important to study the users' perspectives not in isolation of their real life security practices.

2.1. Research Methodology

The methodology we used was grounded theory. The rationale behind choosing such methodology is that we view the topic of

* *Corresponding Author: Email:* rsed501@york.ac.uk

 # This paper has been presented at the International Conference on Advanced Technology&Sciences (ICAT'14) held in Antalya (Turkey), August 12-15, 2014.

mobile phones security as a complex interaction between technology and way of life. Yet, it is a much under researched area. And as grounded theory methodology is suited to complex phenomena where little is known [4]; we believed grounded theory would be practical to our research. We went into this research unequipped with a predefined set of hypothesis, though, the absence of a predefined theory helped broadening the research and allowed the data to be tested and retested to identify any source of initial contradictions. Using grounded theory, we were able to break down the data, conceptualize it and then put it back together in new ways. Besides, grounded theory iterative way of research helped to identify valid and complex relationships in shorter time frames. Moreover, grounded theory permits the concept of Reflexivity and hence allowed our influence to be improved gradually as the theory was developed step by step throughout the study.

Our research has gone into three types of cycles of data gathering, analysis and theorizing. We stopped when we felt the theory reached saturation. Three signs indicated such saturation. First, each new item of data was perfectly fitting into existing theory. Second, the theory rightly was justifying the data. And third, the theory was successfully engaged in different types of mobile security-related interaction such as Internet browsing, mobile authentication and phishing attempts handling.

Our method of research was interviews. Face-to-face semi structured interviews helped developing a second version of survey questions in later stages of the study.

2.2. Sampling

The process through which the interviewees were selected was theoretical sampling. In theoretical sampling, the required participants are deliberately chosen [4]. The reason for using such sampling technique is that our interest was not to cover all possible variations as much as proving or refuting our tentative theory that will be explained later on. The grounded theory needed to be tested at all times. Hence, we had to choose the sample knowingly to test each theory. The whole process was iterative, thus it was validated by continual comparisons with the raw data. When gaps were identified in the framework, they were filled by further investigation using theoretical sampling. 15 mobile users were interviewed. We are quite aware there has been a debate among the HCI community regarding the ideal sample size. While some researchers encourage using large size samples, others led by Nielson [6] support sizes of between five and ten participants.

Since the appropriate sample size is the one that adequately leads to comprehensive interpretation of the studied phenomena [7], and as generalization was not the goal of our investigation; we considered interviewing 15 participants would be sufficient. This number was not decided in advance, on the contrary, as our methodology was rounded theory, an interview after another was conducted until we felt that our theory had reached saturation then we discontinued our interviewing process. Regarding the sample nature, directed by grounded theory methodology, sample selection went on three phases. In the first phase, the initial interviews suggested interviewing users with disturbing history of security-related incidents would be useful for the research. Therefore, following interviewees were selected according to their past security experience either with mobile phones, or in general. Further analysis recommended interviewing users with different levels of security awareness. Hence, the sample, in the second phase, covered people with little to average level of knowledge such as housewives and undergraduate students, people with high knowledge level represented in Computer Science postgraduate students and university staff of the security group in a Computer Science department.

The sample included both male and female participants. Being over 18 years of age and being a UK mobile phone user for at least 1 year at the start of the study, were the prerequisite factors for selecting participants.

2.3. Research Findings

In this section, we introduce the findings of our research represented in the grounded theory we reached through analyzing our data followed by a detailed interpretation of our results. In our methodology, no hypothesis was set in advance; instead the process of our research formulated our theory. Here we explain our grounded theory from the point where it started as a tentative theory, passing by its development as the data was collected and ending up with the final mature theory.

3. Tentative Theory

The initial interviews conducted led to the following theory: "Users' history and previous experience with security related issues formulates their security attitude and shapes their future behaviour". This theory was founded on an observation made while conducting the interviews that several participants exhibited desirable security behaviour in their real life such as insuring their mobiles, backing up their data on another media and updating their antivirus software frequently. The common criterion among those participants was that they all had a history of upsetting security-related incidents such as getting their phones stolen, losing their mobiles while travelling or being infected by a virus in the past. These unpleasant memories affected the way they felt and acted in later incidents. For example, one of those participants got a virus on her computer as soon as her anti-virus software got expired. Accordingly, she related her bad security attitude 'delay in updating the antivirus program' to the consequence of getting her PC infected. “It expired and then I got 2 detections of viruses”, she said. That caused reliable future security practices. For example, she said she had never forgotten to upgrade her antivirus software since then.” And now I scan my entire computer all the time”, she added.

Yet these sound practices performed by those users were missed in the rest of the interviewees who did not have such memories of bad security related incidents. Hence, we were satisfied that users' upsetting memories affect their future decisions or as Ingvar [8] called it 'memories of the future' where people's past experiences program their future actions by forming the basis for anticipation and expectation for both short term and long term future.

Accordingly, our theory suggested that new situations and events can trigger disturbing memories leading the person to believe the danger will occur again if they maintain their bad security habits. This belief would lead them to take a defending action by becoming more cautious and behaving more securely. Consequently, the perceived usefulness of their new healthy behaviour will turn into confirmed usefulness. In order to examine our theory, further interviews were conducted. Our main goal was collecting more data to enhance and expand our theory.

However, the analysis of the collected data rejected the tentative theory. Some users who had suffered from displeasing security-related history continued acting in poor security manner. Examples of which are having no antivirus software on their PCs, having no password for their laptops or their phones and taking no back up for their data. They have passwords only for their PCs at work but not at home. When asked who taught them to set their

passwords they answered: “Technical support did, if he didn’t, I would not”. Same answer was given regarding antivirus software. Those participants seemed to be more susceptible to mobile phishing specially vishing and smishing attacks. Concerning Vishing, when those participants were asked if they would give their passwords to their mobile company support over the phone, they said “Yes, if I got it from an unknown number”. For Smishing, we wanted to measure how easily they can be deceived by a forged message pretending to be from their bank. Half of those participants expressed 100% level of trust. The other half said they would trust such message with 70% level of trust. This proves that their disturbing history did not give them sufficient alarm to become more alert in future. These results prove that 'Disturbing experience' is not the dominant feature that guides users' attitude. Accordingly, the tentative theory was refuted.

4. Second Theory

To identify the dominating feature that caused certain participants to act securely and others to act the opposite, our research went into two phases. In the first phase, a thematic analysis has been carried out for the purpose of identifying concepts in the existing data. The second phase, that involved further data collection, was reflexive to the thematic analysis results. The interpretation of the analysis performed in the first phase suggested that similar concepts were leading to joint category with relation to each participant's level of education and security awareness. Hence, the second phase was concerned with more data collection with specific attention to this category. The analysis of the data revealed that security patterns of the participants, whose expertise was security, were more guided rather than haphazard. Here are some examples. The participants’ selection process of antivirus software was not influenced nor constrained by the products already downloaded on their PCs or the ones available for free, as was the case for other participants. Instead, they consciously chose the program according to its efficiency. They were aware of the special characteristics that distinguish mobile phones from other devices. For instance when asked about the way they look at mobile phones threats, they said " not different than those of PCs, however the handsets have less computational power and energy so they have weak encryption algorithms". When discussing the level of privacy concerning one's SMSs, their answers reflected they realized the level of encryption provided. It was "SMS is not encrypted while being transferred so if someone has a special device, he can easily read it". They felt confident to deal with security problems of their mobile phones. Unlike other participants with lower levels of knowledge, when asked whom to contact in case they encountered a mobile security problem, their answer was "I will reset the mobile settings". Moreover, their assessment for the risk involved with certain data connections through mobile phones such as Bluetooth or Internet was wise, balanced and based on their knowledge. An example of which was their answer when asked about ranking the mobile services from a security perspective. "Bluetooth is not that harm, it's a mutual process it requires security digit code from both sides", they said.

Accordingly, the following source for data collection was interviewing people with different information technology backgrounds and various levels of security awareness. Hence, university staff whose major was security, Computer Science postgraduate students, non-Computer Science undergraduate students and house wives, were interviewed.

The further we went in our analysis the more positive we became regarding our theory. People who got enough awareness regarding mobile phones security, either through their education or from their mobile operator or bank, made more rational mobile security decisions. They were more alert about responding to vishing or smishing attacks on their mobiles and compared it to the information provided to them by the concerned authorities. On the contrary, for people with low knowledge levels, security came last of their priorities. They felt no harm can ever come through short message service. They even declared they would trust an SMS pretending to come from their bank and some tried to be more watchful and said: "I would only answer security questions like what's your mother's maiden name". They did not know that by answering such questions they are simply helping the attacker to steal their identity. “if it was written that the message sender is my bank, I would trust it 100%", they said. Thus, their lack of knowledge about the easiness of spoofing an ID on a mobile phone, and about the kind of information that should remain confidential, increase their vulnerability to mobile phishing. The theory was almost shaped; the level of awareness and amount of knowledge transferred to the mobile users constitute the dominant factor that indicates whether the user will follow a desirable security pattern or not. Yet, there were three gaps that did not fit between the data and our interpretation and would question the validity of our theory.

4.1. First Gap

Participant D had an advanced level of knowledge about mobile phones security; she is a research student in computer science department, she had read many articles about mobile security. Additionally, her sister is studying phishing attacks and many times had warned her against fake phone calls and messages. Nevertheless, D was the worst participant in terms of security behaviour; she had no password for her laptop nor her mobile phone, no anti-virus software for either of them, no backup for her data and moreover, she said she would respond to a phone call from her mobile operator and give away her password without a doubt. She said she might be reluctant if bank details were required.

4.2. Second Gap

Participant H represented the opposite case to participant D. She had false information regarding the security about mobile phones short messages. For example, she believed that her short messages were private and no one has access to them even in the mobile operator databases. She was also quite confident that SMS is very safe. She stated that she may trust a message pretending to be from her bank if the message sender ID confirms that. According to her perception, any message she receives on her mobile phone should be trusted because it has passed through the mobile operator network.

In spite of the wrong knowledge she acquire, her security attitude can be described as 'perfect'. She had set passwords and installed antivirus programs for all her PCs, she had backed up for her mobile phone contacts and she insured her handset. And although she did not know that mobile messages' headers can easily be spoofed, she pointed out that she would never give her password, bank details or any confidential information over the phone.

4.3. Third Gap

Participant J was a member of the staff at the University, his major was security. So his knowledge was more than enough to deal with security attacks attentively. Yet, his belief that he is not a target for mobile attacks caused a lax security attitude. When asked about scanning mobile files against possible virus infections, he said "I know I should but no time for that". And

when asked what his reaction would be if he received a Vishing attack pretending to be from his bank, he said "I will ask them that I will call the number myself". Phoning the same number will not solve the ID problem if the caller was a phisher. Additionally if the phisher was using a premium number, our participant might become a fraud victim.

The results from these three gaps were quite confusing because they contradicted with our theory. They led us to wonder: if knowledge was not the factor that guides security behaviour, where knowledgeable people behave insecurely and ignorant ones behave ideally, then what was the dynamic that made each group behave as such?

5. Final Theory

Further data breakdown directed us to examine inside the personality of each participant. For that, a new version of interviews questions was designed. The findings endorsed that personal characteristics were the main factor that guided the participants' security patterns of behaviour. Accordingly, our thorough analysis of the data suggested the following theory: "There are two traits of personality that shape human security attitude; these are Agreeableness and Conscientiousness. The former influences situational decisions while the later formulates frequent security strategies". Agreeableness is related to person's intensity of suspicion whereas Conscientiousness refers to self-discipline [10].

How we reached our theory

The research at this stage has gone through two levels. In level one, an in-depth analysis was performed not just for participants' actions but for their feelings and reactions as well. In level two, we carried out a further investigation to compare the diagnostic criteria of each personality trait against the users' behaviour not only regarding their security habits but for their daily life practices too. That led to sorting participants into the following categories.

- Low Agreeableness, High Conscientiousness
- High Agreeableness, Low Conscientiousness

Participants' Classification

While conducting the interviews, it was clear that some participants had high sense of worry and fear that guided their security attitude. On contrary, others could not care less. We were positive that individual differences play a role. Our confidence was supported by the dissimilarity in security behaviour among people with same level of awareness yet varied security history. Below, we give a brief layout of the Big Five and their definitions and provide explanation of our theory. Psychiatrics currently prefer to use personality traits rather than personality types in the field of psychology research for the reason that it is hard to restrict varieties of human personality in small number of types [9]. Personality Traits nowadays are considered a representation for the higher order super-factors of personality [10]. For these reasons, we will be using the Big Five personality traits.

The Big Five factors:

• **Openness**. It describes imagination, appreciation of arts and creativity levels

• **Conscientiousness**. It is concerned with self-discipline and the way individuals control their life and direct their impulses.

• **Extraversion**: It is marked by distinct engagement with the external world. Extrovert enjoy being with people, are full of energy and often experience positive emotions. Introverts lack energy and activity levels of extroverts. They tend to be quiet, low-key, deliberate, and disengaged from the social world.

• **Agreeableness**: It reflects social harmony and cooperation with others. It indicates individuals' level of trust, morality, altruism and sympathy.

• **Neuroticism**: It concerns mental distress, unpleasant emotions and the tendency to experience negative feelings.

The new version of the survey questions developed reflecting on the second theory results, has measured different aspects of the five personality domains. Analysing the participants' answers to those new questions resulted in isolating two traits as being particularly relevant. Those traits are Agreeableness and Conscientiousness. The former was chosen as the individual with high level of Agreeableness assumes that most people are fair, honest and have good intentions. This facet is closely related to phishing susceptibility. The latter personality domain was selected as it is concerned with individuals' self-efficacy and sense of duty and obligations. These characteristics are strongly correlated with maintaining responsible security behaviour.

Low Agreeableness, High Conscientiousness

Some of the participants were ideal users of both computers and mobile phones; security wise. They had passwords for their laptops, used to update their anti-virus frequently and no one outside this group had password for their mobile phones. Testing their tendency to become victims of phishing attacks, they stated they would never respond to any message or voice call asking for information. They held themselves responsible for protecting their own mobile phones even if other party would handle this issue. They refused lending their mobile phones to others even friends. And the 'only' interviewee who has plans to download anti-virus software for her mobile was among them. Comparing their answers to their reactions and expressions recorded while being interviewed, suggested low level on agreeableness and high level on conscientiousness. These findings were supported by matching up the results of those participants to the diagnostic criteria for the two personality traits mentioned above.

Here is a detailed explanation for that: Some of those participants had no previous idea about the existence of mobile phone viruses. In the middle of the interview, we informed them that mobile viruses do exist. Afterwards, their answers and reactions during the other half of the interview were totally remarkable. First, they looked disturbed and 'terrified' when being told and their responses to the following questions reflected their fears. For example, when asked if they had experienced a virus on their mobile, unlike other participants, their answers were neither 'yes' nor 'no'. Some said 'Not yet' while others said 'May be'. They also declared an intention to install mobile antivirus software as soon as we finish the interview. And when asked if they ever had security concerns when connecting to the Internet via their mobile phone, some said 'Now I Do'. Moreover, some stated their happiness that their current mobile does not have the ability to connect to the Internet. "Luckily this phone does not have Internet on it", they said.

In questions examining their general security attitude, their answers showed their worries. An example of such was their reaction when their antivirus expired and they got detections of viruses. We got answers like: 'I got really scared'. Additionally, their responses were exaggerated. Not only did they update their antivirus but also some deleted all their laptop files, others uninstalled the operating system. Literally, they said 'Every Thing'. They kept scanning the entire computer 'All the Time', they said.

Concerning texting, some used to write in a way that no one except the person they were communicating with, would

understand. Regarding the handset itself, some said 'I always have the fear that I'll lose or forget it somewhere'. Concerning mobile phishing attack, it was clear that they will not be an easy phishing victim. Explaining the reason behind their refusal to respond to the phishing SMS and the extent to which they confide messages they receive on their mobile, some said: 'People are really creative these days'. Others said: 'You can't trust anything these days'.

These findings show excessive sensation of digital danger and high level of suspiciousness. We were in doubt whether that refers to low level of agreeableness, particularly low trust, or indicates a personality that could be characterized as paranoid. This issue has always been a debate among psychologists; to consider personality disorders (such as paranoid) just a form of normal behaviour but a special extreme of it or qualitatively different from it [11]. What is of importance to our research is the security attitude such personality reflects and whether it can be regarded as a desirable one or not. In spite that some forms of Paranoid have been considered accepted or even successful in business such as narcissistic or obsessive compulsive personality disorders [10], we believe that we might not get the same result concerning mobile phone security. Yes, we care for promoting sound security behaviour for mobile phones, yet we do not want security actions to stem from a personality disorder. Our explanation is that even if this disorder produced an acceptable attitude, the loss brought up will most probably be greater than the benefits gained. Firstly, the person himself, by ignoring mobile messages in order to avoid viruses or phishing attacks, may miss a legitimate message from his bank. Secondly, the service provider itself will lose profits from clients ignoring its advertisements on their mobile phones. Thirdly, the user himself wastes his time worrying about extra security checks that are not necessary such as uninstalling the operating system and installing another one. Fourthly, the user is sacrificing losing uninfected files by deleting them for more additional assurance.

High Agreeableness, Low Conscientiousness

Other participants were representing the opposite case. They had high level of security awareness yet poor security attitude. They defended not having a password for their laptops by saying: "I'd like quick, just turn it on and you know" or by saying "I am not taking it anywhere, no one else can use it". They justified not securing their mobiles by saying "No one would attack me". Users within this group were the totally aware and highly educated regarding mobile security issues, especially phishing attacks. However, applying weak security strategies and showing high tendency to fall for mobile phishing attacks, they preserved the poorest security behaviour of all participants.

Relating their results to the criteria that distinguish each personality trait, their personality matched the characteristics of low Conscientiousness such as: leaving their belongings around, forgetting where they had put their house keys, and losing the keys of their cars. Same applies for their handbags. Those users showed low self-discipline and are considered careless individuals. That was obviously reflected on their security behaviour.

Balanced Personality

Some users had stable security behaviour and rational level of trust. Their security attitude reflected a balanced personality with high level of Conscientiousness and average level of agreeableness. Their life is an example of high self-discipline as they act devotedly towards their responsibilities. That was very much revealed in the way they deal with mobile security issues. In their frequent strategies, they used healthy security plans; passwords, antivirus software, frequent checks and updates, insurance and data backup for all their devices; PCs, laptops and mobile phones. Regarding phishing attacks, their answers indicated a careful attitude. Some seemed to question the credibility of Smishing attacks pretending to be from their banks, others were quite confident they would never fall for a Smishing attack on their mobile phone.

Grounded theory completed

Consequently, our grounded theory is completed: "There are two traits of personality that shape human security attitude; these are Agreeableness and Conscientiousness. The former influences situational decisions while the later formulates frequent security strategies. Awareness from concerned parties affects person's communication style with phishing attacks being neither passive nor aggressive but assertive ".

5.1. Grounded Theory Confounds

The methodology used to reach the grounded theory was interviews. This type of correlational research has its own problems. We list some below.

1- **The researcher effect**: This problem occurs where interviews are used. Here the participants want to impress the researcher. Accordingly, they may claim to do something, regarding their security practices, while in reality they do something else. The results the researcher obtains may be affected by her age, race or gender.

2- **The evaluation apprehension:** This is a special type of anxiety that occurs when the participants think the study is testing their abilities. Clearly, this affects the results of such studies.

In order to confirm the results of our grounded theory and at the same time avoid the drawbacks of correlational research, we moved to experimental research.

5.2. Phishing Experimental Study

The methodology used to reach the grounded theory was interviews. This type of correlational research has its ownAn experimental field study to examine the grounded theory results was conducted. Below we detail the procedures and results of this field study.

A. Method

Participants were recruited to take part, ostensibly, in an experiment to assess their personality. In reality the experiment was designed to acquire their mobile phone numbers in order to subject them to a later simulated phishing attack. Participants were told that their personality is to be assessed by a standard personality questionnaire. Each participant completed the questionnaire individually on paper. Participants were asked to give the researcher their mobile number to contact them to receive their personality results at a later meeting. Few weeks later, the researcher sent a phishing message to each of these participants' mobile phones. The message pretended to be from a bank and asked the participants to ring back to confirm an internet banking activity. The participants' responses to the phishing message were dealt with in a confidential manner that was explained to all participants individually after the experiment was completed.

B. *Design*

The study adopted an independent measure design approach. There is one condition (exposure to a phishing message) corresponding to one independent variable; Personality traits, with five levels; Agreeableness, Conscientiousness, Openness, Extraversion, Neuroticism. The dependant variable the study

measured was phishing vulnerability. The main Hypothesis of the study was that Personality Traits affects People's Vulnerability to phishing attacks'.

C.*Apparatus*

The study used the personality inventory NEO-PI. The apparatus consisted of standard personality instrument; IPIP and a new 'Pay as You Go' SIM card.

1- IPIP Questionnaire

The IPIP questionnaire is a standard questionnaire. It stands for International Personality Item Pool. It was created by Lewis Goldberg. The questionnaire is composed of 120 self-descriptive sentences on a five point scale, ranging from "strongly disagree" to "strongly agree". The questionnaire assessed the participants' personality of the Big Five Factor Model; Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness to Experience.

The IPIP questionnaire can be filled in and administered online, however, for the following reasons it was printed out and participants filled it in paper form:

- To avoid any filling errors that might occur (eye illusion that might be caused by computer). That may refute the experiment internal validity, as any changes in the scorers may produce changes in the obtained measurements.
- To save participants answers for analysis purposes as the web version of the IPIP does not permit that.
- IPIP web version shows the results on screen as soon as all questionnaire items are answered which will not give the researcher an excuse for second appointment with the participants to complete the experiment steps as will be explained below.

2- New SIM Card

In order for the participants' data to be safe and the researcher's personal number not to be revealed, a new 'Pay. As You Go' SIM card was used for the experiment and was fully dedicated to it. This new mobile was kept secure throughout the study to ensure no one else had access to the replies. This SIM was discarded as soon as the study was completed.

D. Procedures

As the study involved a phishing experiment, an approval from the Physical Sciences Ethics Committee has been applied for before conducting any stage of the study. Mainly, the study consisted of two stages; personality assessment and phishing experiment.

E. Participants

The study has been conducted over 63 participants. The participants were employees in a Microsoft golden partner.

F. Results

53% of the participants responded to the simulated phishing message. In-depth analysis was performed of the personality traits of all participants. Then a comparison to their response to the phishing attack was made. The results confirmed the grounded theory partly. Personality influences individuals' vulnerability to phishing. Yet, Agreeableness and Conscientiousness are not the responsible traits. Instead, it is the individuals' assertiveness that affects their susceptibility to phishing. Participants with high score in Assertiveness fell for the phishing attack. Their tendency to take charge and direct activities encouraged them to respond to the phishing message while participants with low scores did not fall for the phishing attack as they did not have same desire to take control. Assertiveness is a facet under the personality trait; Extraversion.

G. Future Work

We are planning to conduct another field study to examine people response to phishing messages that ask them to reveal confidential information, not only to ring back, as done in the study presented in this paper. We will compare individuals' personality traits against their responses to see if any change will occur as a result of the modification in the message content.

Acknowledgements

This research was sponsored by the Arab Republic of Egypt. These studies were conducted by the author under supervision in University of York.

References

[1] Informa Telecoms & Media report, London: Informa Telecoms & Media. 2009

[2] D. Maslennikov. Mobile Malware Evolution: An Overview, Part 4". RetrievedJanuary , 2014 Available: http://securelist.com/large-slider/36350/mobile-malware-evolution-an-overview-part-4/

[3] K. Dunham. Mobile Malware Attacks and defense. Syngress. 2008.

[4] P. Cairns and A.L. Cox. Research Methods for Human-Interaction. Cambridge University Press. 2008.

[5] J. Preece, Y. Roger and H. Sharp. Interaction Design beyond Human Computer Interaction, USA: John Wiley and Sons. 2002.

[6] S. Love. Understanding mobile human computer interaction. ElSevier Ltd. 2005.

[7] M. N. Marshall. Sampling for qualitative research. Oxford University Press. 1996

[8] DH. Ingvar. Memory of the future": an essay on the temporal organization of conscious awareness. 1985

[9] R. R. McCrae, A. Terracciano, P. T. Cost, and D. J. Ozer. Person-factors in the California adult Q-set: Closing the door on personality types? European Journal of Personality, 20, 29-44. 2006

[10] A. Furnham, J. Crump. Personality Traits, Types, and Disorders: An Examination of the Relationship between Three Self-Report Measures. European Journal of Personality. 2005

[11] L. Clark and D. Watson. Personality, disorder and personality disorder towards a more rational conceptualization. Journal of Personality Disorders, 13, 142–151. 1999

[12] R. West. The psychology of security. Communications of the ACM 51(4). Pages 34-40, 2008.