Mobile Users' Strategies for Managing Phishing Attacks

Rasha Salah El-Din[1], Paul Cairns[1] & John Clark[1]

[1] Department of Computer Science, University of York, York, United Kingdom

Correspondence: Rasha Salah El-Din, Department of Computer Science, University of York, York, YO10 5DD, United Kingdom. E-mail: rsed501@york.ac.uk

Received: April 10, 2014 Accepted: May 12, 2014 Online Published: May 19, 2014

doi:10.5430/jms.v5n2p70 URL: http://dx.doi.org/10.5430/jms.v5n2p70

Abstract

Phishing is the use of electronic media, like emails and SMS messages, to fraudulently elicit private information or obtain money under false pretence. Though there is considerable interest in phishing as a security problem, there is little previous research from the human factors perspective and in particular very little empirical support for what makes phishing effective or successful and therefore how best to defend people from it. In this paper, we report findings of an experimental lab study to investigate individuals' strategies dealing with mobile phishing attacks.

Keywords: decision making, strategies, phishing, mobile security, risk management

1. Aims and Hypothesis

The purpose of this study is to understand the psychological aspects of mobile phishing and to examine the correlation between the individuals' personality traits and their ability to detect phishing. Ideally, we are looking into mobile users' vulnerability. Yet, the nature of the study, as a closed lab experiment, does not allow for measuring if the subjects would fall for the phish or not. Instead, it tests people's capability to correctly identify phishing. That is why this sort of studies is referred to as IQ-tests.

Phishing IQ-tests take the form of screen shots of web sites and/or emails and the users classify which are phishing and which are legitimate ones. Their answers are calculated and according to the ratio of the correct ones, they are given a score. Phishing IQ-tests are widely available to help individuals assess their susceptibility to phishing attacks. Examples of these are Sonic Wall and Mail Frontier.

Hence, Phishing IQ-tests can be used for training purposes, as they are a powerful tool to educate users about phishing attacks and how to spot them. Downs et al (2007) argue that the study of users' behavioural response through IQ-tests is very useful for developing educational methods to teach users about phishing, as well as, guiding the design of warning indicators and security toolbars that users will truly keep an eye on.

However, for research purposes, this type of studies has its limitations and can not replace field studies as each is used for specific purpose. As mentioned above, IQ-tests are performed in a closed-lab environment and accordingly they lack 'context' surrounding real life attacks. A number of researchers believe the artificial context of these studies may skew the tests' results (R. Salah El-Din, 2012; Jakobsson et al., 2008; V.Anandpra, 2007).

A Phishing IQ-test, in this regard, introduces a preconceived notion, as subjects know their detect-ability is being tested. Accordingly, "the knowledge of the existence of the study biases the likely outcome of the study" (Jakobsson et al., 2008, p66). Therefore its results can not be linked to real life situations. In other words, they can not be generalized to the real world as they are not a true representative of it.

However, this type of phishing studies can be effective in certain aspects. First, it can provide insights to what makes phishing messages believable in contrast with naturalistic experiments that have an edge in helping us determine to what extent a certain phishing message is believed (Jakobsson, 2007). Second, Lab studies can help us understand what text messages would typical mobile users react to and why. That is because lab studies allow comparing users' reactions to a sequence of stimuli. This can not be done via naturalistic experiments, or else, a severe increase in the sample size will be needed (Jakobsson, 2007). Third, Lab studies have been proposed as an approach to measure phishing education effectiveness (Downs et al., 2007). Fourth, phishing IQ-Tests have the advantage of assessing the risk of phishing attacks which are not yet in use. Finally, the nature of lab studies permits an opportunity for a

prolonged interview with every participant, through which they can explain what made them react differently to each stimuli / the reason for their interpretations for each stimuli.

2. Method

2.1 Participants

Participants were all graduate students in Computer Science department, University of York. 36 students were recruited in the study of whom 8 were women and 28 were men. The age of the participants ranged from 23 to 45 years old, with the most common age group being between 23 and 30. All participants were mobile users for at least 1 year at the start of the study.

2.2 Design

The study is examining the relationship between personality traits and people's perception of phishing attacks represented in their ability to detect phishing. The predicting variable is the personality traits. The traits of interest are Agreeableness, Conscientiousness, Openness, Extraversion, Neuroticism, Assertiveness and Trust.

The study followed the 'closed-lab' experiment approach. The experiment incorporated a phishing IQ test where real mobile messages were shown to the participants. Half of which were authentic texts while the other half were captured phishing messages. Participants were asked to make a distinction between phishing messages and genuine ones. Every message was followed by 2 questions. In the first question participants were asked to state the reason for their rating. The second question was a behavioural response question that asked the participants what their reaction would be towards the message. Options included; texting back, calling back, ignore or other to be specified by the participants.

2.3 Materials

Respondents' personality was measured using a psychological Personality Inventory; NEO-PI. NEO-PI measures the personality traits mentioned above. IPIP was the questionnaire we used to measure the participants' personality.

Respondents' ability to detect phishing was measured via an IQ-test that was composed of 12 mobiles messages. The messages were presented to the recruits in paper format. The phishing messages were collected from a pool created and archived by the author over a year period. Normally in phishing lab studies, the stimuli are gathered from phishing archives available online such as (Millersmiles, 2012, Scamdex, 2012). However, to the best of our knowledge, no 'mobile' phishing archives exist. For that reason, the author built her own database of real mobile phishing messages by collecting texts from the public and friends. A Face Book page has been created for this purpose. The messages were then validated, analyzed and archived by the author.

As for the genuine messages, these were collected from real mobile texts. The messages were chosen to cover different types of authentic service providers' messages. As the grounded theory suggested that mobile operators are very trusted by mobile users, two messages were included in this regard. One was sent be a mobile company promoting an offer to its clients and the other was a notification message of service suspension. Two messages were sent by big institutions, well known to the participants, their University and NHS (National Health Service). The administration office of University of York used to send mobile messages to remind the students to enrol online every semester. The NHS is the system that provides health care for all the UK citizens and one of its clinics resides with in the University campus. It sends frequent feed back surveys to the students to fill in. The two other genuine messages were selected from messages sent by other service providers: British Gas company and a local dentist clinic.

The table below summarizes the main features of the messages.

Table 1. Lab study messages features

SMS	Legitimacy	Main Features
Government Debt Relief	Phishing	• Incentive to text back
Accident Compensation	Phishing	• Incentive to text back a Claimed free number
University of York	Legitimate	• Enrolment Alert • Link:www.york.ac.uk/enrol • Warning of late fee of £30
Friend Missed Call	Phishing	• Using familiar Names • International Number
Gas Reading	Legitimate	• Gas Reading Alert • Link: www.britishgas.co.uk/meterreads • Notice period of 5 days.
Pepsi	Phishing	• Lucky Winner of £1 Million Pepsi Award 2011 • Email:markjose65@hotmail.com
Bank Account	Phishing	• Closed Bank Account for unusual activity • Sender: Unknown number • Requiring a Call Back
ATM Card	Phishing	• ATM Reactivation • Sender: Unknown number • Requiring a Call Back
Dentist	Legitimate	• Routine dental check-up • Sender: 'Dentist @' • Requiring a Call Back
NHS	Legitimate	• Patient Survey • Sender: Known • Link:www.dr.priceandpartners.co.uk • Wenlock.terrace.nhs.net
TalkMobile	Legitimate	• Mobile Internet Offer: 30p per day • Link:www.talkmobile.co.uk
Mobileworld	Legitimate	• Mobile Service Suspension Alert • Link:talkmobile.co.uk • Code: MW010

2.4 Procedures

The participants were recruited via advertising by email to the department of Computer Science students. The respondents were offered an Amazon voucher of five pounds and a free personality report. The experiment took place at the Human Computer Interaction Lab study. The recruits filled the IPIP personality questionnaire in a paper form. This was followed by a phishing IQ-Test.

For the IQ-test, an introductory briefing was given to the participants about the nature of the study and the meaning of 'phishing'. It was defined as a fraudulent attempt to acquire money and confidential information from people by impersonating legitimate entities. Participants were presented each message in a separate paper. Each message was composed of two parts; the message sender (either in a form of a number or in a form of an ID) and the message content. For every message, the participants were asked to rate the authenticity of the message over a 7 point Likert scale ranging from Definitely Phishing to Definitely Genuine.

After finishing with the 12 messages, the participants filled in a survey that investigated their habits regarding security and how they view messages with either grammar or spelling mistakes.

After that, the participants were thanked and their personality reports were sent to them by mail.

3. Results

The process of detecting which are phishing messages and which are genuine can be regarded as a binary detection problem (Wickens, 2002). The four possible outcomes are summarized in Table 2 where True Negative is when a participant correctly detects a text message as a phishing one. True Positive is when a participant correctly detects a

text message as a genuine one. Hence, false negative would be when a participant mistakenly detects a phishing text as a genuine message. This means the participants have fallen for the phish. Finally, False Positive is when participant mistakenly detects a legitimate text message as a phishing one. This indicates the participant is excessively watchful.

Table 2. Phishing binary detection

		Participants think the message is:	
Actually the message is		Genuine	Phishing
	Genuine	True Negative	False Positive
	Phishing	False Negative	True Positive

Table 3. Descriptive statistics of participants" response

		Participants think the message is:	
		Genuine	Phishing
Actually the message is:	Genuine	Mean=4.06 SD=1.286	Mean=1.25 SD=1.251
	Phishing	Mean=0.50 SD=0.775	Mean=4.75 SD= 1.105

Table 3 shows the mean number of the texts correctly detected in each category. It shows that the participants were more accurate in detecting phishing messages (mean = 4.75) than genuine ones (mean= 4.06).

To interpret the results of the binary detection, two measures were calculated: Accuracy and precision. Accuracy refers to the percentage of correct answers out of the total answers. Precision refers to the percentage of correct positives of all the positive responses. Below is how each was calculated.

Accuracy= (Number of True Positives + Number of True Negatives) / (Number of all possibilities).

Precision= (Number of True positives / Number of all positives (True and False)

A linear regression analysis was conducted to investigate the relation between the participants' personality traits and their accuracy and precision scores. Linear regression predicts on one variable from one or more independent variables. Accordingly, multiple regression was suited for our analysis as it helps answering the following questions: Do the predicting variables (personality traits) predict which of the two categories on the dependent variable, the person falls into? Question 2: Are all the independent variables or only part of them predicting the participants' response? Question 3 is related to the relative importance of the independent variables, as it answers the question which of these independent variables is most useful in predicting phishing response?

An alpha level of 0.05 was used. As can be seen in table 1, the outcome variable, Accuracy, was significantly correlated with the predictor variable Extraversion, with high accuracy in phishing detection being associated with high Extraversion scores.

Analysis of the data using multiple linear regression revealed that the combined predictors explained 13 % of the variance in phishing detection accuracy, R2=.129, F (1, 34) =5.015, p <0.05. Extraversion was the only significant individual predictor, β=.359, p<.05, neither Agreeableness β= -.091 nor Assertiveness β= -.364, nor Trust β=-1, nor Conscientiousness β=-1.08, nor Openness β=.002, nor Anxiety β=.119 were significant individual predictors in the final model.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.359a	.129	.103	11.566

a. Predictors: (Constant), Extraversion

Coefficients a

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
Extraversion	.148	.066	.359	2.239	.032

a. Dependent Variable: Accuracy

Excluded Variables a

Model		Beta In	t	Sig.
1	Agreeableness	-.091b	-.559	.580
	Assertiveness	-.364b	-1.719	.095
	Trust	-.100b	-.575	.569
	Con	-.108b	-.654	.517
	Neur	.206b	1.097	.280
	Opp	.002b	.010	.992
	Anxiety	.119b	.652	.519

To sum up the results indicated a correlation between Accuracy and the personality trait Extraversion with significance=.032. No correlation was found between Precision and any personality trait.

Analysis of Messages:

Table 4. Suspicion about phishing and legitimate messages

MSG	Legitimacy	Phish	Genuine	Do not know	Percent Expressing Suspicion
1-DEBT	PHISHING	33	2	1	91%
2-Accident	PHISHING	34	-	2	94%
3-Uni	LEGITIMATE	4	30	2	11%
4-Friend	PHISHING	19	7	10	52%
5-Gas	LEGITIMATE	5	27	4	14%
6-Pepsi	PHISHING	36	-	-	100%
7-Bank	PHISHING	24	3	9	67%
8-ATM	PHISHING	25	6	5	69%
9-Dentist	LEGITIMATE	3	31	2	8%
10-NHS	LEGITIMATE	8	27	1	22%
11-MobileAd	LEGITIMATE	6	22	8	17%
12-Mobile	LEGITIMATE	19	9	8	53%

Table 4 summarizes the number of participants per message according to how they view it (a Phish, a Genuine message, or Do not know). The last column represents the respondents' suspicion of every message in a form of a percentage. Phishing messages are the shaded ones.

Everyone expressed suspicion in at least two of the 12 messages (with this participant suspect only the Accident and the Pepsi award messages) and a maximum of 11 messages (with this participant suspect all the messages except the talk mobile advertisement message).

A) The phishing Messages:

For the phishing messages, as the table shows, no single participant trusted the Pepsi award message. On the contrary, the phishing message that got the least percentage of suspicion was *'the Friend'* message. It was also the most message that caused confusion among the participants. 28% of the participants were confused and did not know whether to rate the message as a genuine or a legitimate message.

Below, we will go quickly over each message and discuss the participants' behavioral responses and the messages cues that informed their decisions.

For the first phishing message, 'The Debt', almost all the participants regarded it is a phishing attempt, except two recruits who thought it might be a legitimate message. It is not clear why these two participants believed such message. And we can not attribute them being unable to detect the message to their personality scores (Both scored low in Neuroticism and Anxiety). Despite previous research suggested that individuals with high scores in

Neuroticism are more likely to fall for phishing. We believe that emotionally stable users can fall for such kind of message, as it was not targeting anxious users. It was not associated with any loss nor did it threaten the users by any means. It was just an opportunity for those who have problem paying their debt. The participants stated they would not call back to investigate more, yet they thought such offer may exist in reality.

As for the second phishing message, no single participant fell for it. Only two recruits felt confused about 'The Accident' message and were unable to make a decision.

A very interesting response was that of the third phishing message 'The Friend missed call', which tricked the participants the most. 71% of the respondents who fell for it scored low in Extraversion and Assertiveness. Despite that this taxonomy supports the quantitative analysis results that introvert individuals are bad in detecting phishing, and despite that most research attributes that to lack of knowledge of introverts that resulted from having low social engagement persons, we believe the recruits' participants response, to this message in specific, has an emotional aspect.

What we meant by the 'emotional aspect' is that because of their introvert nature, the participants who fell for this message are thirsty for online relations. Modical and Leal reached the same conclusion, they suggest that introvert people are more vulnerable to scams due to their preference for internet communication rather than face to face interaction. Similar deduction was reached by research conducted in Exeter University on people's judgment on scams (Exeter, 2012). They suggested that people who are socially isolated are more likely to fell for phishing scams.

Putting into consideration that the recruits were all computer science students, they were all knowledgeable about phishing attacks. Moreover, those who fall for this message in specific, scored high in Conscientiousness, all of them. This is an indicator that, not only do they know about phishing but they also care about their safety and that their behavior is normally planned. Another proof for our conclusion is that 100% of these same users declared that they would never call the number provided by the other phishing messages, and they preferred to 'ignore' even the bank messages. Yet, they all decided to 'call back' the sender of the 'Friend' message despite the number was international.

As for the fourth phishing message 'Pepsi Award', there was no difference in the participants' response towards it as it was detected by all the participants.

Regarding the fifth phishing message 'The closed Bank Account', only three participants fall for it. They all scored low in Extraversion which supports the statistical analysis that extrovert individuals are better at detecting phishing.

It is also worth mentioning that 100% of those users scored low in Conscientiousness and high in Neuroticism and Anxiety.

This additionally supports our observation that people with low Conscientiousness scores are susceptible for this kind of phishing attacks that are of financial nature. Also, it is in line with previous research that suggests that Neuroticism has an effect on individuals' vulnerability to phishing attacks, which is expected especially for users with high levels of Anxiety in specific as a facet under the personality trait Neuroticism. It is logical that individual with high levels of fear and concern and with low ability to control their impulse, will fall easily for phishing attacks that are related to their banking activities and pose a threat to their financials. Those individuals are expected to be impulsive and behave spontaneously. This ends in the attacker's benefit.

However, we stress again that is observation was not statistically supported in our research. Accordingly, we advise that it be tested in studies with bigger sample size.

More users fell for the last phishing message 'The ATM Suspension'. In fact it got double the response rate than the 'Bank Account' message. 67 % of the respondents who fell for this message scored low in Extraversion and Conscientiousness. 83% scored high in Anxiety. These results are again in line with our statistical results, where introvert people fall for phishing more easily than extroverts. Yet, there is a possibility that the effect is doubled if the individuals score high levels on Anxiety.

We can also conclude from comparing the participants' response here to their response to the 'Bank Account' message, that people pay great attention to their ATM cards. They mentioned 'I'll call immediately', 'This message is more convincing than the bank one'. Some mentioned they might go to the bank to enquire for his ATM status, yet for the bank message, they said they may search the sender phone number on the internet.

B) The Genuine Messages:

For the genuine messages, all of them were suspected by at least one participant. The least suspected message was the Dentist message and the most suspected one was that sent by Mobile World.

The first genuine message 'The University' message was a real message sent every semester by the University of York administration to all the students on their mobile phones to remind them to enroll to the University system.

Ironically, 11 % of the recruits rated it as a phishing attempt and said they have to check their emails first and contact the University administration for assurance. Others said ' Currently the Uni contact me through mail or emails, they have not used mobile messages for billing issues', They all scored low Extraversion, which confirms our conclusion that Introverts are bad detectors. For their other personality traits, 75% of these users scored low in Trust, and high in both Neuroticism and Anxiety. This may explain why they were over cautious when analyzing the message. People who score low in Trust, are generally pessimistic and view others as suspicious, dishonest, or dangerous (McCrea, 2006).

The participants' responses also pose a doubt on the University method of communication with its students and whether they are aware of it.

For the second genuine message, it was rated as a phishing attempt by only 3 participants. No significant relation to their personality traits was found. Yet, those who scored low in trust said: ' My Dentist calls me, they do not text'.

The third genuine message was from 'British Gas' company asking its clients to send their meter reading by mobile message or via their website. 13% of the participants rated it as a phishing attempt. Some said ´According to the role play, I'm a customer of British Gas, yet, still I would not use the number provided in the message', 'I'll wait for the company to send someone to take the reading, I'll not contact them', 'British Gas always estimate alternate bills and I'm sure they would NOT make things convenient for their customers', 'The link is probably to download malware onto my computer'. Those participants' scores low on Extraversion.

A surprising result came from the fourth genuine message 'The NHS survey'. 22% of the participants rated it as a phishing message despite almost all the university students are members of NHS via the surgery mentioned in the message. Students are used to receive such messages. 88% of the over cautious participants scored low to average in Extraversion, and 63% of them scored low in Trust, which supports the conclusions of the previous messages.

For the mobile operator advertisement message, about 6 participants' doubted its credibility. They rationalized their belief by saying: 'Price unrealistic', 'never heard of them',' arbitrary company with no credentials'. No specific personality trait justified this behavior, yet, this behavior can be attributed to two things; the type of the message itself, and the type of the study. The message was an advertisement message which is relevantly new to the mobile environment. The study nature as a closed- lab study has a bias that users know from the beginning they are performing a phishing detection task. That made them so alerted.

In the same way, the users dealt with the last genuine message, 'Mobile world', with suspicion. It was the most genuine message rated as a phish by 53% of the participants. The users suspected the message for many reasons; the brand was not known to them 'I've never heard of a UK operator called mobileworld', 'no legitimate trust behind the URL'. They also doubted the method itself 'suspension usually sent by mail or phone call'. The urgency of the message sent a false message that it is a phish 'urgent messages tend to be spam', 'just trying to force users to a URL to install an exploit'.

Participants'-Stimuli Evaluation

Thematic analysis was used for the analysis of the behavioural responses of the participants. Patterns through the data, which were related to the participants' personality and at the same time associated to our research question, were pinpointed. The analysis produced themes in two categories: First category was concerned with themes identified by the 'Detectors' behavioural responses. Second categories isolated themes by those who 'Fall' for the phishing messages. Key excerpts appearing to inform the recruits' decision were included.

4. Discussion

Below we discuss the different themes that resulted out of the analysis:

1). Themes of the Detectors

A) Impossibility

B) Non Relevance to the victim

C) Message Media

D) Sender ID

E) Awareness of Implications

F) Publicizing

G) Logic

H) Message Style

I) Common Attacks

2). Themes of the Failed

A) Confusion

B) Lack of Knowledge

C) Conviction

D) Stubbornness

E) The use of Familiar Names

1). Themes for Phishing Detectors

There were common themes among the participants who were able to correctly detect the phishing messages.

A) Impossibility

Phishing messages that were conveying generous offers such as a debt cancellation or a prize awarding were regarded, by the participants, as implausible.

One of the grounds, the participants based their judgement upon was the impossibility of the offer. "Complete debt write-off is impossible" They said. Or "*The message does not make any sense, so must be ignored*". Others described these messages as *"Too good to be true" or "Unbelievable"*.

They were hesitated to believe that legitimate institutions would put forward such offers *"I doubt the government would come up with such a deal"* or *"No government ever wiped off its citizens debts"*.

Impracticality was one of the reasons why the detectors suspected the authenticity of the messages is the easiness of the process claimed and the lack of any course of actions required, *"Wiping off debts without official procedures is not convincing at all"*, they said.

Doubting the Intension of the sender was another cause for the successful detection of phishing messages "No one would offer that without wanting something in return". They said. "Definitely phishing, why would anyone dole out 1 Million pounds without even buying a lottery ticket?".

Hopelessness was one of the factors that helped some participants in discovering the phish. They showed *"Nothing in the world is free*", *I'm not lucky enough*", they said.

B) Non Relevance to the victim

Participants were inclined to mistrust the messages that were not applicable to them either for being not related to them *"I do not have any debt*", *"No debt in hand*", *"I didn't have any accident"*, for special precautions they set in advance with their service providers that made them confident the message is fake *"I don't allow mobile banking messages*", or for certain life style they accustomed to *"I don't participate in this kind of prize draw*", they said. Others refused to accept the message as a whole, for short they said: "*The message is based on 100% wrong information*".

In this, mobile users' judgment was not different than that of internet users who judge relevance before authenticity (Jakobsson, 2007) as they evaluate the content of the stimuli not the signs of legitimacy.

This observation may pose a problem for service providers sending either alerts or advertisements to their clients over mobile phones as these are likely to be considered as phishing attempts by the mobile users.

C) Message Media

The channel through which the message was communicated to the participants affected the opinion they formed towards it. For example, they expected the government would communicate with the public by means of letters of correspondence rather then by mobile short message services "*Government does not send sms, they send official letters*", "*Text message is not an official way to inform me, the gov should have other means to inform me"*, they said. They also questioned the reliability of banks messages if sent via mobile phones *"Banks do not normally send text regarding account management, more formal methods like letters or message to the internet banking inbox"*, they said.

D) Sender ID

Several text messages were dismissed based on their sender, especially for the financial messages that claimed to be sent from their banks. Participants cited the absence of the bank name from the sender ID, instead it was a number unknown to them. *"Unknown number", "normal number not hsbc2",* they said. Messages purported to be from

mobile operators got the same remark. The participants expected to see the name of their mobile company as the sender, they said: *"normal number not O2"*.

Others took a broad view and treated all messages from an unknown sender the same whether they were sent by banks, service providers or individuals, *"I ignore numbers I don't know"*, I don't trust unknown numbers", they said.

E) Awareness of Implications

One of the reasons why participants ignored phishing messages was their awareness of the implications resulted if they responded to the mobile text. Some were worried the sender was trying random numbers and that their reply will encourage the sender to keep annoying them in the future. *"I'll ignore because no matter what text I send, the scammers will record my number as 'active' and continue sending messages", "Possibly sent to random numbers, So, I'll ignore to avoid further attention",* they said. Others were afraid their numbers will be sold for potential attacks. *"If I replied, they would know my number is real and they would sell it"*, they said.

F) Publicizing

Participants believed that some of the offers conveyed by certain messages lacked proper broadcasting. The fact that they were not made public elsewhere raised the participants' doubts about the messages' legitimacy. They were suspicious the claimed offers were kept under wraps rather than being advertised.

They were expecting the government would seek praises from the public if a decision has been made to remove debts from individuals' shoulders. *"Government does not wipe out debt with out a lot of press",* they said. They were positive such declarations should have been published widely in more official manner. *"If it were true, It would be announced through the media, not through text to me*", "*If there was any such scheme, it must have been in the news"*, they said.

This suggests that while people may become better at detecting phishing attacks that take the form of governmental communication, yet, they may be predisposed to respond to disaster scammers. Those are cybercriminals who make use of real national or international events specially disasters. An example of that was the phishing scams that used Japan earthquake in 2011 and Hurricane Sandy in 2012 to steal money under the cover of donations' appeals.

G) Logic

Thinking rationally was a notable feature that characterized the participants' analysis for the messages. They strongly observed essential factors such as the content of the message, the peculiarity of the sender number and also the way through which the sender possessed their mobile numbers, *"The number to call looks fishy",* "*Why would the government have my number*", *" why do they need us to follow certain steps, there may be some trap*" , they said. For the messages that proposed prizes, they evaluated the amount of money awarded. An example is the one Million pounds award, where the participants commented *"The value is too big!*" More over, they criticized the ambiguity of the messages that was too general for the purpose of drawing attention of as many people as possible: *"It does not mention anything about which account and why"*, message is Vague", *"it's not specific"*. They said. The participants were also clever and could spot that the email addresses used in the phishing messages were not official ones. This occurred for both the lottery and the prize purported to be offered by PEPSI, *"The email address does not sound professional; it does not carry the signature of the organization organizing the lottery", "it's a Personal email address", "Markjose56@hotmail =not Pepsi"*.

The subjects also stated that one of the main reasons they ignored some phishing messages was that they did not address them by their names. The individuals' names brought in the massages were unknown to them personally*: "I don't know the names mentioned that's why I ignored it*". This last remark warns us that spear phishing may have high probability of success.

H) Wording and Style

Poor grammar and shoddy style of the messages were discerned by the participants. These made it clear for them that the messages were faked. *"Sloppy grammar"*, they said. Even the wording of the messages irritated them. Words like "*Winner*" and "*Free message*" let them believe, the message is a phishing attempt. "*WINNER: every thing about the message is dodgy", "Why they said FREEMSG?!! This creates doubts. That's why I consider it phishing*", *"The word FREEMSG indicates that something tricky*", they said. The participants explained how the language used added an unofficial character to the messages. *"Language has an informal tone*", they said.

These findings are in line with jakobsson's results (Jakobsson, 2007) that viewed spelling and design as *"the number one*" aspect that participants consider in evaluating phishing messages. However, a study conducted by Blythe et al. (2011) suggested that phishing is getting harder to detect and that we should not rely on spelling and grammar to spot phishing. They based their opinion on a five day analysis of phishing messages archived in MillerSmiles (2012).

They found 38% of the phishing messages were spelled correctly and 68% used identical logos from the original websites. These resulted in more convincing phishing emails and websites.

I) Common Attacks

Individuals were skilful in recognizing common attacks like '*winning an award*' message: *"This is a classic 419 scam"*, they said referring to defrauding the victims for monetary gain. For the message that offered compensating them for the claimed accident, they commented: *"I do not trust these messages"* and *"I know loads of people who receive these messages despite having no accidents"*. This suggests that people may be better at detecting attacks of generally occurring forms.

2). Themes of Those Who Fell for the Phish

There have been some trust indicators that were common among the participants who fell for the phishing stimuli. Below is a discussion of those.

A) Confusion

Some of the participants who fell for the phishing messages stated that they were actually confused and were not sure the messages were authentic. Yet they preferred to respond anyway in an attempt to remove their confusion.

One of the incidents that triggered confusion was the mixed signals the messages gave. An example of that was the message that asked the participants to call back to reactivated their blocked account as the message claimed. The participants agreed the message was indefinable and they were in doubt it may be phony. However, many of them decided to respond to it. *"Tricky!! It does not specify which account has been closed. So it could be poorly-expressed legitimate message or a clever attempt at phishing"*, they said. The same observation occurred with other messages like those asking the participants to call back. This gave a false sense of security. Participants could not help wondering why a bogus message would ask them to call back rather than requiring confidential information. *"Giving the number to call in the message raises the alarm bells, but giving complete control details also remove the doubts!"*, *"It gives me a number to call, which I can check against my bank. But it should give the bank name though"*, they said. Again the last comment refers to spear phishing as it implies that mentioning the bank name instills trust in the message. That is the reason why attackers bombard victims with emails or text messages hoping their messages would reach the right target whose bank is the same stated in their phishing messages.

B) Lack of Knowledge

Some participants fell for the phish and texted back. They were under the impression that texting is safe. They did not know that one text to the sender can cost them up to 5 pounds per message if the calling number is a premium rate one. In their response to the message purported to be from a person who would like to contact them, some of the answers we got were: *"So, I will text back. This sounds the logical approach as a sinister motive might be behind making me call and charge me unwittingly"*. Others seem not aware of the premium rate numbers at all. They decided to follow the attacker request and ring back despite the number provided was an international number. *"If the message is not genuine, then i can find out on calling the number", "I'll call and ask"*, they said. Similar attitude accompanied the bank messages. *" May be correct & may be wrong since there are no account details in the text"*, *" I'll call back to find out how true is the text by requesting them provide my details by giving my phone number then after I know from which bank they are calling, I'll go directly to my bank"*, they said. This implies that individuals may be vulnerable to attacks that use new deceit techniques. Same concern was raised by jakobsson but for email phishing. He stated that:" as soon as a new psychological twist is developed, there is reason to believe that it will become successful"(Jakobsson, 2007).

C) Conviction

Some participants responded to the message either by calling or texting back the message sender out of persuasion. For message number four, they truly believed they missed an actual phone call. *"I am not expecting any call from J.Paige or Paul Clark & I don't know any of those. But it might be genuine, I'll call back to find out what are they calling for"*, *" Not sure about the number and the name, I'll text him back, I think it might be important to me to check the person name and the reason of the call"*, they said. They were really keen not to miss the call that may be important: *"Could be someone trying to reach me"*, *"I'll call back to check if the caller really has something important"*.

The participants' response to other messages, like those claimed to be from their bank, was attributed to their conviction of the message content. An example of this is the message that claimed unusual activity in the participant's account. Here some participants believed the message and went further to the extent that they undertake clarifying the situation, *"I'll call back, I have to be sure that this is true, and I did not do any unusual activity"* and

"My ATM card is with me & in these occasions, they usually call me not text. I'll send them a text to ask for the reason to reactivate the ATM card", they said.

D) Stubbornness

The persistence of the attacker is one of the reasons that may encourage the individuals to interact with him. The respondents of the study declared that they are more likely to respond to the phishing message only if the message sender was insisting and sent another message, otherwise, they would ignore the whole issue. *"As long as this is the first time, I'll ignore it"*, *"Only, if they call again"*, they said. Individuals were also looking for cues from the attacker to prompt them to respond. One of these signals was a call from the attacker, *"If I found a missed call, then it may be genuine, otherwise it's definitely not"* or *" I'll wait for them to call again"*, they pointed out.

E) The Use of Familiar Names

The employment of well-known names that could be easily recognized was very effective at gaining the trust of the recruits. In the stimulus that purported to be from a person who was trying to communicate the victim without success and asked her to call back, familiar names like ' Paul' and 'Clark' gave an authenticity to the message. Many recruits did not even notice that the number was international. Some actually believed the message to the extent they imagined it as real. They used the same persona the attacker used, *"I'll call Mr.Paul Clark"*, they said. Others went further to say that they knew the people who tried to contact them earlier as per the message allegation. *"I recognize the names, I'll call back"*, they said. This suggests that using familiar English names and drawing on casual tone, played a big role in convincing the mobile users there is a social acquaintance between them and the caller.

Individual strategies

Interestingly, we found that people think strategically when deal with mobile phishing attacks. The following section contributes the first investigation of mobile users' strategic patterns of thinking in reaction to phishing attacks. These strategies can be very useful in protecting individuals from phishing attempts, as they can feed anti-phishing training and educational materials.

These strategies are discussed below.

A) Google it

Many participants stated they would individually verify the phone numbers proposed in the messages by goggling it via the internet to make sure they are the correct numbers.

B) Use own contacts

Very few said they would call the phone numbers they already have, either for they banks or other service providers such as their mobile operators, gas or electricity company. This applied as well for websites.

C) Ignore it

Most of the participants chose to ignore messages that were either not related to them or messaged they had doubts are phish. Some of them stated they ignored the messages to save their time. "no time to waste on these", they said. Other reason was despair that an action could be made against the attacker, "I'll ignore, bcz, there is no use of reporting it to my operator", "Even if they manage to block this msg from now on (which I doubt), Attackers will just come up with other phishing messages.", they said. Feeling that the attackers have many ways to attack, was another reason for despair, "I may consider contacting my operator to block the number, but I'm fairly sure the phisher could simply switch to another number", they said. Others simply felt it is sensible enough to ignore such texts, "There is no point of replying to a phishing message", they commented. Some recruits chose to ignore the messages as a rational respond to a communication they did not even asked for, " I donot know how the company got my mobile number, and, it seems wrong that I tell them to 'stop' given that I never asked them to send me adverts in the first place", frustratingly they said.

D) Waiting Policy

Some recruits chose not to respond to messaged they were not sure are legitimate, but instead wait for the phisher to take the next step either by calling or texting them again.

E) Respond

In responding to the stimuli, the participants chose either to call back or text back the number sending the messages.

5. Limitations

The conclusions of this study were reached in the context of a closed-lab environment where the recruits knew that they were performing phishing detection task. Accordingly, these results express the participants' abilities rather than

their tendency to behave in real life situation.

6. Conclusion

The purpose of this study was to identify the individual factors responsible for detecting for phishing as well as to understand the psychological aspects of revealing a mobile phishing attack. In this regard, the quantitative analysis helped the understanding of the dominant personality trait of phishing detectors: Extraversion (high levels of this trait). The qualitative analysis helped explaining how this trait manifests itself in the detection process. The pattern of results emerging from this study suggests that individual differences do play a role in falling for phishing and that introvert people are more likely to fall for phishing. The risk in attending to phishing messages for introverts is higher for socially based messages that seemed to attract socially isolated individuals who prefer online communication over face to face communication.

Although no measure of Anxiety was statistically significant as a main effect in predicting the vulnerability for phishing, further analysis revealed several indicators that anxious people are more likely to fall for phishing especially for messages that are of financial nature. Conscientiousness trait also was of an effect when the stimulus was of a financial nature. Individuals of Low levels of Conscientiousness were bad detectors of phishing attacks.

In general, the participants were better at detecting commonly occurring mobile texting messages. Most of these offered monetary rewards such as Government Debt Relief, Accident compensation or The Lucky Winner of a Million Pounds messages. None of the participants indicated a willingness to act in response to these stimuli. There was a census among all the recruits to ignore such messages, even if they doubt its authenticity.

Regarding the phishing messages that succeeded in deceiving the participants, these can be divided into two branches. Branch one was pressing the social relations button by pretending the victim has missed an important phone call and asked her to call back. The stimulus used very familiar names so it is likely that the victim has either heard of or know them in person. This stimulus got the highest rate of response among the recruits, 25% of them stated they would respond to the message either by calling or texting back. Branch two focused on the participants' finances by warning them of a closure of their bank account or a suspension of there ATM card. For these, participants showed their interest to call back who preferred to text the sender back.

This suggests that individuals were keener to avoid loss than to gain benefit. They ignored the monetary reward stimuli, yet, they responded to the stimuli that threatened them with bank closure or ATM card deactivation. The analysis also revealed that people mix between phishing and advertisements. This poses a risk for commercials and announcements from legitimate service providers.

References

J. S. Downs, M. Holbrook, & L. F. Cranor. (2007). Behavioral Response to Phishing Risk. Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit. ACM.

M. Jakobsson, P. Finn, & N. Johnson. (2008). Why And How To Perform Fraud Experiments. *Security & Privacy, IEEE, 6*(2), 66-68.

M. Jakobsson. (2007). The Human Factor In Phishing. *Privacy & Security of Consumer Information, 7*, 1-19.

MailFrontier Phishing IQ Test – UK Edition. Retrieved March 2012, from http://survey.mailfrontier.com/survey/phishing_uk.html

R. R. McCrae, A. Terracciano, P. T. Costa, & D. J. Ozer. (2006). Person-factors In The California Adult Q-set: Closing The Door On Personality Types? *European Journal of Personality, 20*(1), 29-44.

R. Salah El-Din. (2012). To Deceive or Not to Deceive! Ethical Questions in Phishing Research. In HCI Research in Sensitive Contexts: Ethical Considerations Workshop at HCI 2012. September 10-14, 2012, Birmingham, UK.

Retrieved March 2012, from Available: http://www.millersmiles.co.uk/

SonicWALL Phishing IQ Test. Retrieved March 2012, from http://www.sonicwall.com/furl/phishing/

T.D. Wickens. (2002). *Elementary Signal Detection.* New York: Oxford University Press.

The Email Scam Resource. Retrieved June 2012, from http://www.scamdex.com/

University of Exeter, School of Psychology. The psychology of scams: Provoking and Committing Errors Of Judgment. Retrieved June 2012, from http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf

V. Anandpara, et al. (2007). Phishing IQ Tests Measure Fear, Not Ability. In Proceedings of the 11th International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, Berlin. pp.362-366.