Identity Theft – Empirical evidence from a Phishing exercise

T Steyn, HA Kruger, L Drevin
Computer Science & Information Systems
North-West University, Private Bag X6001, Potchefstroom, 2520
South Africa
{Tjaart.Steyn, Hennie.Kruger}@nwu.ac.za, ldrevin@acm.org

Abstract. Identity theft is an emerging threat in our networked world and more individuals and companies fall victim to this type of fraud. User training is an important part of ICT security awareness; however, IT management must know and identify where to direct and focus these awareness training efforts. A phishing exercise was conducted in an academic environment as part of an ongoing information security awareness project where system data or evidence of users' behavior was accumulated. Information security culture is influenced by amongst other aspects the behavior of users. This paper presents the findings of this phishing experiment where alarming results on the staff behavior are shown. Educational and awareness activities pertaining to email environments are of utmost importance to manage the increased risks of identity theft.

Keywords: Identity theft, phising, security awareness, education.

1 Introduction

"Beware, don't be caught!" These words serve as a warning on the website of one of the major banks in South Africa. Clients are reminded that a financial institution will never request a customer to complete personal details on a webpage-link in an email. They use the term 'phishing' to warn against this type of fraudulent emails that are most often used in conjunction with a fake website [1]. The term 'identity theft' is then used to show how the information obtained by the phishing attack can be used in fraudulent transactions. Identity theft is not a new type of crime. It has been used

Please use the following format when citing this chapter:

Steyn, T., Kruger, H., and Drevin, L., 2007, in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 193–203.

for centuries to impersonate someone and thereby obtaining a way of committing a crime anonymously.

The term phishing originates in the hacker community in 1996 where customer account information was stolen from AOL users. Hacked accounts were called 'phish' and were a type of electronic currency used between hackers to swap user account information for pieces of hacked software. It is a variant of the term fishing (fishing for passwords) and it is influenced by the term phreaking (exploitation of telephone systems). The meaning of the term phishing expanded over the years and the technique became more sophisticated with the resulting damages also escalating. Fake websites, key-loggers via Trojan horses and other malicious attempts are also now part of the phishing attacks [2].

One definition of phishing is given as "it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication" [3]. Another comprehensive definition of phishing, as quoted by Granova and Eloff [4] states that it is "the act of sending an email to a user falsely claiming to be an established legitimate enterprise into an attempt to scam the user into surrendering private information that will be used for identity theft". The conduct of identity theft with this acquired sensitive information has also become easier with the use of technology and identity theft can be described as "a crime in which the impostor obtains key pieces of information such as Social Security and driver's license numbers and uses them for his or her own gain" - four common types of identity theft crime include financial ID theft, criminal ID theft, identity cloning and business identity theft [5].

According to a study done in 2004 by the Gartner group an estimated 57 million US adults received a phishing email and almost 11 million online adults have clicked on a link in phishing attacks [6]. Around 1.78 million Americans remembered giving out personal information and many more could have but did not realize it. Financial losses suffered by US financial institutions in 2003 were nearly $1.2 billion as a direct consequence from identity theft and the accompanying phishing attacks.

Awareness and training programs, technical controls and new legislation are all possibilities to handle the growing number of phishing incidents. To address ICT security awareness in an academic environment, a project was started during 2005 where a value focused approach was used to identify key areas of importance - the objective was to develop a measuring instrument for ICT security awareness levels based on the identified key areas [7]. One of the key areas identified by managers and users was the responsible use of email and the Internet. This includes awareness on phishing and identity theft. As part of the broader project, it was envisaged that system data be obtained on users' behavior regarding ICT security. To this end a practical test was designed to firstly test users' awareness levels pertaining to phishing and identity theft and secondly to make users aware of the risks of responding to these attacks. The use of such practical tests is frequently carried out by organizations and academic institutions. An example can be found in Dodge and Ferguson [8] where they described a successful exercise to evaluate students' propensity to respond to email phishing attacks.

The aim of this paper is to present a practical phishing experiment, including the planning, execution and results. The remainder of the paper is organized as follows: In section 2 the background to the exercise and the methodology used are discussed, while section 3 details the results from the experiment. Section 4 concludes the paper with a summary and possible future work.

2 Background and Methodology used

2.1 Background

As mentioned in the introduction, a project to propose a framework to measure the security awareness levels of staff was initiated in 2005. The proposed framework consists of the following phases which are described in more detail in [9]. Firstly, the key areas on which measurements will be taken need to be identified - this would form the basis of the actual measurements. Secondly, knowledge, attitude and behavior of staff, pertaining to the identified key areas, will be surveyed to determine their awareness levels. In addition to the employee surveys, it was suggested that appropriate system generated data should also be used as input to the final model as system data is expected to be more reliable (not subjective or human dependent) and fairly easy to obtain. Finally, the data should then be combined with appropriate importance factors to construct a final model to be used for improving the overall information security culture. One of the specific aspects that was identified in the initial project as an issue that should be tested by system generated data was identity theft. The verification of awareness levels that relates to identity theft would assist in covering one of the key areas viz. the responsible use of email and the Internet. These initial project phases were conducted in an academic environment [7] and it was therefore decided to design a phishing test to evaluate staff at the same academic institution.

The use of the Internet and email facilities at universities implies that universities are subjected to the same threats and vulnerabilities as other organizations. In a sense it can be argued that certain universities use electronic communication more intensively as an ordinary business because, apart from the normal communication functions, it is also used in the teaching function – both as a subject of study as well as a tool and an aid to perform teaching activities. There are a number of risks attached to the use of electronic communication systems in both organizations and universities such as spreading of viruses, using the facilities to conduct private business, routing chain emails, impersonation, eavesdropping and certainly one of the most important aspects that is dealt with in this paper, identity theft.

The university where the phishing test was conducted is a South African university that consists of three different campuses located in three different cities of which one was selected for the exercise. The selected campus is the largest of the three with eight divisions (academic faculties) and more than 26000 students. The campus is served by approximately 3400 staff members of whom about 550 are full-time academic staff. The ICT infrastructure at the campus is one of the best and staff are linked to a central network that gives access to the full spectrum of electronic communication as well as Internet access. Although a high level of security is

maintained, the university has no official security awareness program in place and staff did not receive any ICT security awareness training. A general notice on where to find certain security policies are displayed during sign-on to the network. Warnings against disclosing or misuse of passwords are included in these documents.

The phishing exercise was designed with the definition of phishing in mind. An email, that claims to be legitimate, had to be constructed, sent to users and tried to convince them to surrender private information that could be used for identity theft. This explains the objective of the exercise. The reason for the test was, in the first place to obtain system generated data for the overall ICT security awareness model. Secondly, the aim was simply to gauge the reaction of staff when confronted with possible identity theft as well as to get an indication of how easy staff would give away sensitive information. Finally, the exercise itself would serve as a tool to raise security awareness and make staff aware of the dangers and risks surrounding phishing scams. All personnel were aware of a recent implementation of new systems at the university and this created the ideal opportunity to construct a credible email that most staff would be interested in opening and reading. The email asked employees to confirm their details which were necessary because of the implementation of the new administrative systems. They were then asked to click on an html link that would take them to a fake university web page that asks for their personnel number, network identification and network password. One of the advantages of asking for a password was that the usual phishing email content such as financial details were avoided – however, the password and other details requested are sufficient to commit identity theft. The implication is that adequate information would be available to get access to facilities, services, systems, etc. that could have direct adverse financial or possible other effects for the respondent, his/her division or for the university.

The design and the execution of the phishing test appear to be straightforward but there were a number of issues that needed clarification before the test could be regarded as legitimate, both from an organisational view and a research perspective. The first requirement was that the necessary permission from the appropriate level of management had to be obtained. An official request that includes a research motivation was prepared and presented to the Institutional Director (Human Resources, Students and Innovation and Research), the Institutional Director (Finance and Facilities) and the Manager Information Technology. They gave permission for the exercise on the condition that no individual staff member would be identified and that actual passwords may not be recorded during the exercise. The condition was seen as a reasonable condition that would also address possible ethical consequences such as protecting the privacy and identity of staff. The phishing program was therefore designed in such a manner that the only information recorded was whether a user opened the email, deletes it, follows the link and whether or not something was entered in the required data fields – actual data such as passwords entered was not recorded. Therefore no passwords were compromised during the exercise. The assumption was made that respondents entered their real passwords when prompted for it, however, this could not be verified. This assumption was supported by enquiries regarding passwords. Although no staff details were divulged, the results can be used by management.

Another aspect that needed careful planning was the content of the email message. The message had to be credible but the official contact details of the IT department (who normally sends out general email messages to all staff) may not be used – the reason for this was that management was of the opinion that a good relationship between users and the IT department exists and there may be a possibility of doing harm to the existing relationship by sending out fake email messages on behalf of the IT department. The authors' own contact details (phone numbers) were then added to the message. The final content of the message and the web page was again presented to the Manager Information Technology as well as the Human Resources department for approval.

Finally, a decision had to be made on whether all staff at the selected campus will receive the phishing email or whether a sample should be used. The exercise forms part of a bigger research project and it was agreed that in future there would be other exercises where it might be necessary to test users' awareness via email messages again. To prevent all staff from regularly receiving questionable email messages it was decided to use only a sample of staff members – these staff members may then be excluded in future tests. The sampling process is described in section 2.2.

2.2 Methodology used

The process followed to conduct the exercise was handled in three phases – two test runs and a final test. As an initial test, the email was sent to the authors who performed all possible actions e.g. open the message without following the link, open the message and follow the link but without entering any information, delete the message without opening it etc. The objective was purely to test the technical working of the program and to verify whether the statistics were recorded correctly.

The second test was a small pilot run where messages were sent to 20 randomly selected staff members – the aim was to determine if everything operates correctly when sending the message outside of the technical test environment and also to try and determine what reactions or enquiries could be received. An important aspect identified during the pilot run was that provision had to be made for collecting data from those people who phone or directly reply to the email message.

The final test was conducted a few days after the pilot run. As stated earlier, it was decided to send the message to a sample of staff and to assist with the sampling process the electronic campus address book, which is publicly available to all staff, was used as the population. There were approximately 2400 useable records in the address book and the sample size, n, was determined as $n = e^{-2}$, where e is the accuracy of the estimated proportion with a 95% confidence [10]. For the purpose of this study, e was chosen to be 0,05 which resulted in a sample size of 400. Once the sample size was determined, it was decided to select staff by making use of the systematic sampling method [11]. Sampling begins by randomly selecting the first observation. Thereafter subsequent observations are selected at a uniform interval relative to the first observation. The ratio N/n, where N is the population size and n the sample size, provides the interval length – for this study, N was approximately

2400 and $n = 400$ which means that every 6th element (staff member) was chosen to receive the email message.

The email message was sent to the 400 randomly selected staff members and provision was made to receive phone calls from staff. Personnel of the Help Desk were also alerted to be prepared to assist where necessary. A facility was also created to capture direct email replies. After seven days the exercise was declared closed and the recorded statistics were analysed. A discussion of the results follows in the next section.

3 Results

A response rate of 80% was received. To determine the response rate, the email messages that were not opened was ignored – these email messages were regarded as analogous to paper questionnaires that were not returned. Fourteen of these unopened email messages were immediately deleted by the recipients.

Figure 1 shows the major activities performed by all staff on the phishing email. The categories in figure 1 indicated the percentage of staff members who entered their passwords on the fake web page; the percentage of staff that reacted to the email in the form of a direct reply to the phishing email or telephonically; the percentage of staff members who opened the email, but did not follow the html link; and the percentage of staff who opened the email, followed the link but did not enter a password. It can be seen that more than half of the employees (53.4%) were willing to give their passwords away. It should be noted that the percentages do not add up to 100 as there may be overlaps between the "Replied" category and the others e.g. someone may have replied to the email but also may have entered his/her password on the web page.

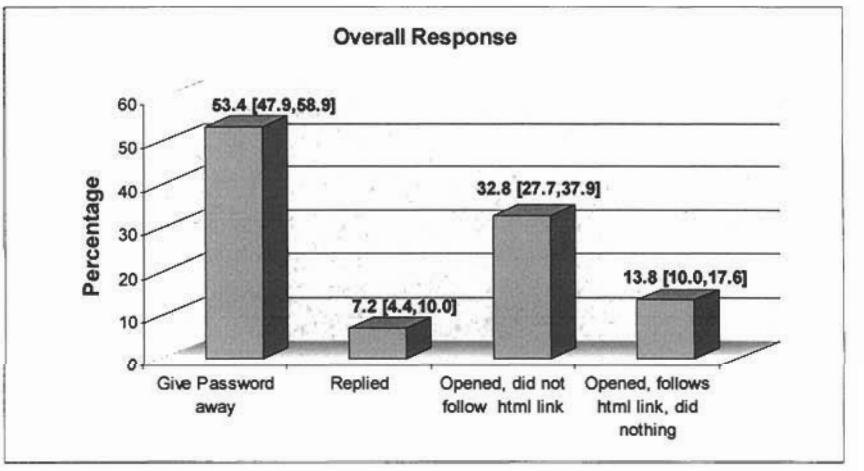

Fig. 1. Overall response

At the top of each bar in the histogram in figure 1, a 95% confidence interval for the true population proportion is given. The formula used for constructing these confidence intervals is given by $p \pm 1.96\sqrt{p(1-p)/n}$ where p is the single sample proportion and n the sample size [11]. There is therefore a 95% chance that the actual percentage of all staff on the campus that would be willing to give their passwords away is between 47.9% and 58.9%.

Figure 2 presents the distribution of the staff who responded over the different divisions, e.g. Natural Sciences, Economic and Management Sciences, etc. The graph shows that the systematic random sampling method resulted in a reflection of the proportional division sizes. There are eight divisions plus a ninth one called 'non-academic' which include all staff not working in an academic faculty e.g. student administration, human resources, technical staff, etc. Due to the protection of privacy and identity of staff it was not possible to distinguish between academic and non-academic staff within divisions – numbers per division therefore include all staff working in that specific division. Characteristics of the divisions are not disclosed due to the ethical and confidentiality considerations. The results were meaningful and could be used internally by management in training efforts to improve ICT security awareness.

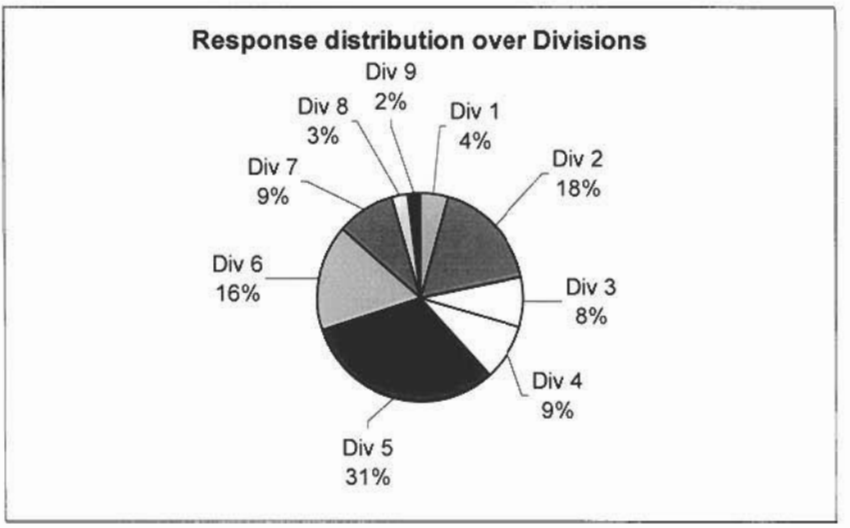

Fig. 2. Response distribution

Figure 3 shows the distribution of staff per division that was willing to give their password away, e.g. from the 171 respondents who gave their passwords away, 2% was in division 9 as opposed to the 36% in division 5. More detailed figures per division are presented in table 1.

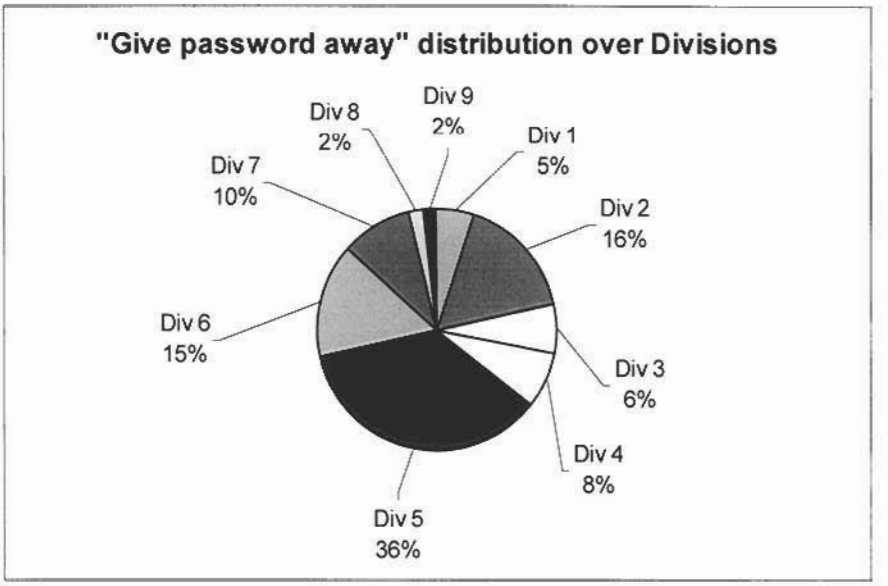

Fig. 3. "Give password away" distribution

Table 1. Information per division

Division	Number of responses	Give password away (Percentage)	Give password away (Number)	Replied	Opened, did not follow html link	Opened, follows html link, did nothing
1	13	69.2	9	1	2	2
2	56	50.0	28	3	19	9
3	25	44.0	11	1	11	3
4	29	44.8	13	3	12	4
5	101	60.4	61	11	26	14
6	52	50.0	26	3	17	9
7	30	56.7	17	0	12	1
8	8	37.5	3	1	3	2
9	6	50.0	3	0	3	0
Totals	**320**		**171**	**23**	**105**	**44**

Figure 4 shows the detailed figures from table 1 in graph form.

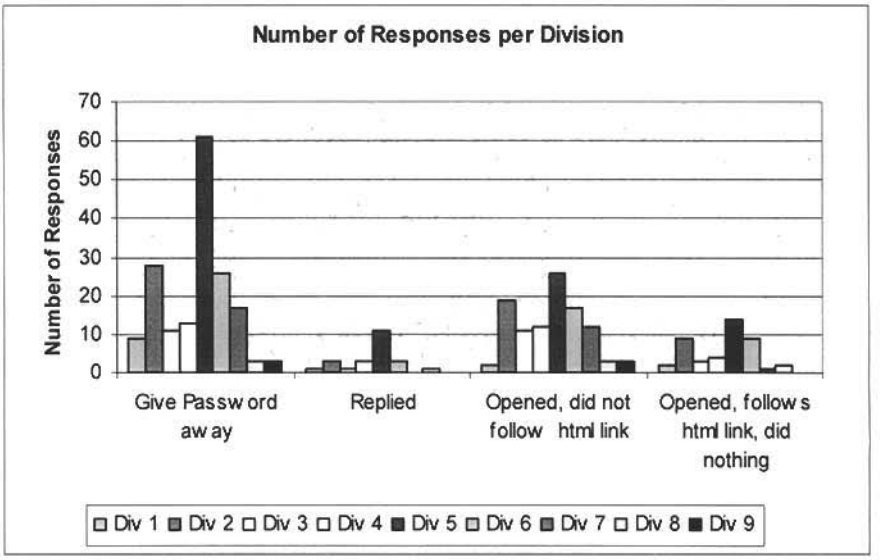

Fig. 4. Number of responses per division

The results of the experiment have indicated that the current ICT security awareness level that relates to phishing, identity theft and good management of passwords, may not be adequate with more than 50% of staff who gave their passwords away when asked for it. This figure should be considered high given the environment and the above average level of computer literacy of staff. Formal computer literacy programs for staff are in place but it is clear that these programs do not sufficiently address the ICT security risks and dangers found in the workplace. The relative low number of enquiries (replies) received (7.2%) may also be an indication of a lack of understanding on how to handle security incidents – users should be aware of *how to recognise* a security incident such as a phishing scam; be *willing to report* it and *know where to report* it. One should also expect the fourth category in Figure 1 – follows the html link but did not enter any data – to be much higher than the current 13.8%. The ideal is that when respondents see the request for personal and private information, more of them should have refused to provide it. It should therefore be worthwhile for management to consider some form of awareness training for staff or to consider the distribution of awareness material to make employees aware of the risks and dangers of phishing scams and what to do when they suspect irregularities. The statistics per division should also enable a focused and phased approach by targeting those divisions with the highest percentage of staff giving their passwords away, first. Finally, the results provided measurements that will be used in the development of a comprehensive ICT security awareness model.

4 Conclusions

In this paper a successful phishing exercise was conducted as part of an existing research project to measure ICT security awareness levels of staff in an academic environment as to raise the overall information security culture. An email message was sent to users to try and convince them to surrender their private network passwords. The results indicated that more than 50% of employees were willing to surrender their passwords – a clear indication that some form of awareness exercise may be needed.

One practical test can only provide partially insight into the awareness levels of those tested; however, the results do provide a baseline measurement for a more comprehensive measuring model as well as an opportunity for management to focus existing security awareness programs or to establish new ones. The test in itself was also useful as a tool to raise awareness amongst employees. It was shown by these results that employees are prone to phishing attacks. Therefore, potential identity theft incidents have to be managed and security awareness in email environments must be addressed in educational activities.

The intention is to expand the exercise to include the other two campuses of the university as well. The test will also be repeated after a certain period of time to determine if there was any change in awareness levels. Another possibility that is investigated is to extend the exercise in future to include the students from the different campuses.

Acknowledgement

The authors would like to thank Mr. C Muller for the technical support during this experiment. We would also like to thank the three anonymous reviewers for their useful feedback.

References

1. ABSA. Security Centre (October 25, 2006); http://www.absa.co.za/.
2. G. Ollman, The Phishing guide: Understanding & Preventing Phishing attacks, (October 25, 2006); http://www.ngssoftware.com/research/papers/.
3. Wikipedia. (October 25, 2006); http://en.wikipedia.org/wiki/Phishing.
4. A. Granova and J.H.P. Eloff, A legal overview of phishing, *Computer Fraud and Security,* 6-11, (July 2005).
5. Identity Theft Resource Center. (October 24, 2006); http://www.idtheftcenter.org/cresources.shtml.
6. A. Litan, Phishing attack victims likely targets for Identity Theft, (October 24, 2006); http://www.gartner.com 4 May 2004.
7. L. Drevin, H.A. Kruger and T. Steyn, Value-focused assessment of ICT security awareness in an academic environment, *In: IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-*

Hubner, S., Ranneberg, K., Yngstrom, L., Lindskog, S. (Boston: Springer, 2006), pp. 448-453.

8. R.C. Dodge and A.J. Ferguson, Using Phishing for User Email Security Awareness, *In: IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Ranneberg, K., Yngstrom, L., Lindskog, S.* (Boston: Springer, 2006), pp. 454-459.
9. H.A. Kruger, L. Drevin, and T. Steyn, A framework for evaluating ICT security awareness, *In: Proceedings of the 2006 ISSA Conference, Johannesburg, South Africa*, (5-7 July 2006, on CD).
10. A.G.W. Steyn, C.F. Smit, S.H.C. Du Toit and C. Strasheim, *Moderne Statistiek vir die Praktyk*, (Sesde uitgawe. JL van Schaik. Pretoria, 1998).
11. T. Wegner, *Applied Business Statistics*, (Juta & Co, Ltd. Kenwyn, 1993).