Email Security Awareness – a Practical Assessment of Employee Behaviour

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

Abstract: Email communication is growing as a main method for individuals and organizations to communicate. Sadly, this is also an emerging means of conducting crime in the cyber world, e.g. identity theft, virus attacks etc. The need for improving awareness to these threats amongst employees is evident in media reports. Information security is as much a people issue as a technology one. This paper presents a description and results of an email awareness experiment that was performed amongst staff from a South African university. It is shown how management can use these results to focus and improve ICT awareness.

Keywords: Email security, identity theft, security awareness, employee behaviour

1 Introduction

The value of information in today's business environment has become increasingly important – information is regarded as an asset [1] and as such, is exposed to a wide variety of threats and vulnerabilities that are usually addressed by a combination of technical and procedural controls. Technology and the associated technical solutions are necessary to address certain vulnerabilities such as viruses, denial of service attacks etc. However, information security is about more than technology; it also includes people. Dark [2] stated that the "people" piece of the security puzzle is perhaps the most critical. The lack of understanding security issues coupled with the pervasive and growing use of computers, makes people a critical factor in the information security equation.

One way to develop and motivate employees in an organisation to counter information security threats properly is through the implementation of security awareness programs. With appropriate knowledge, staff can better prevent information security breaches, detect malicious activities of other staff members and efficiently and effectively respond to security incidents [2]. To address information security awareness in an academic environment, a project was recently initiated to try and develop a measuring instrument for security awareness levels [3]. Key areas were identified to form the basis of the instrument and one of the key areas was the responsible use of email and the Internet. As part of the development of a measuring instrument it was also de-

Please use the following format when citing this chapter:

Kruger, H., Drevin, L., Steyn, T., 2007, in IFIP International Federation for Information Processing, Volume 237, Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer), pp. 33–40.

cided to make use of certain system data to evaluate users' behaviour in certain situations. To this end, four practical email tests were designed to test employees' awareness levels and behaviour when confronted with questionable email messages. The use of such practical tests has been used before. Dodge and Ferguson [4] described similar tests that were used to evaluate students' propensity to respond to email attacks.

The objective of this paper is to present a brief overview of the planning and execution of four email tests that were performed at a university to evaluate employees' behaviour. Results of the exercise will also be presented. The remainder of the paper is organised as follows: In section 2 the background to the exercise and the methodology used are discussed. Section 3 details the results of the four tests while section 4 presents some concluding remarks.

2 Background and Methodology used

2.1 Background

During 2006 a framework to evaluate ICT security awareness levels amongst employees was suggested [5]. The framework was based on the identification of key areas on which measurements can be taken. It was also suggested that, where appropriate, actual system generated data be used as measurements. System data is expected to be more reliable (not subjective) and fairly easy to obtain as opposed to data obtained by using questionnaires. One of the specific aspects that was identified as a key area to be measured and where system data could be useful to evaluate knowledge and behaviour, was the responsible use of the Internet and email facilities. The initial framework was developed at a university in an academic environment [3] and to obtain unbiased and objective data for this important area, four tests were designed to evaluate the same university's staff actions pertaining to certain email activities. All the tests were unannounced and distributed by means of email messages that requested staff to perform certain questionable actions – responses to these requests were then recorded and analysed. One of the tests aimed at identity theft, has already been described in detail in another article [6] but will be referred to again in this work for completeness sake.

As described in [6], the university where the tests were conducted is a South African university. The campus selected for the tests consists of 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. 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.

The design and execution of the four tests raised a number of issues to be solved before the actual tests could take place. Permission was obtained from senior management on the condition that no individual staff member would be identified during

the exercise. Another aspect that needed careful planning was the content of the email messages. The messages had to be credible, not harming existing relationships and approved by the Manager Information Technology and the Human Resources department.

The design and motivation for the four tests can be summarized as follows:

Test 1 - The main idea was to send a questionable email to users and request them to click on a HTML link. The aim was to determine if users read and interpret what they receive and not automatically do what is requested. The message used in the email tried to convince users to follow a web link to obtain certain information that would be beneficial for their personal finances. The source of the email as well as the contents contained enough obvious questionable information to raise the suspicion of users and the correct, expected action of users should be to delete the message without following the link.

Test 2 - A questionable email was sent to users to try and trick them into opening a strange attachment with the objective of testing their reaction when confronted with attachments from an unknown source. The basic message was to invite users to get a free virus checker when clicking on the attachment and, as in test 1, the contents contained questionable information that should have caused users not to click on the attachment.

Test 3 - An email, that appeared to be legitimate, was sent to users, requesting them to follow a web link where they were asked to disclose private information (e.g. passwords) that could be used for identity theft. The aim was simply to gauge the reaction of staff when confronted with a possible email identity theft situation.

Test 4 - An apparently legitimate email was send to users to convince them to run an executable file. The users were given bait in the form of a message that invited them to run an executable file that will improve their computers' performance. This was an unfamiliar named file and the aim was to determine if users reacted responsibly by not executing strange files.

2.2 Methodology used

The process followed to conduct the exercise is described in [6] and is briefly repeated here. The complete process, including all four tests, was handled in three phases – two test phases and the final test. As an initial test, the email messages were sent to the authors to test the technical working of the program and to verify whether the statistics were recorded correctly. The second phase was a small pilot run where messages were sent to a small number of randomly selected staff members – the aim was to determine if everything operates correctly when sending the messages outside of the technical test environment and also to try and determine what reactions or enquiries could be received.

For the final test 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, for each one of the four tests, was determined as $n = e^{-2}$, where e is the accuracy of the estimated proportion with a 95% confidence [7]. For the purpose of this study, e was chosen to be 0,05 which resulted in a sample size of 400 for each of the four tests. Once the sample size was determined, it was decided to select staff by making use of the systematic sampling method [8]. 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 6^{th} element (staff member) was chosen to receive the email message for each of the tests.

The email messages were sent to the 1600 (400 per test) randomly selected staff members and provision was made to receive phone calls and direct email replies from staff. After seven days the exercise was declared closed and the recorded data was analysed. A discussion of results follows in the next section.

3 Results

The main result of interest was to determine how many employees in each of the four tests were trapped. The term "trapped" is used for those cases where the users' reaction was not in line with expected behaviour, e.g. to give a password away as opposed to not give it away.

Table 1 shows the main outcome of how many employees were trapped in each of the four tests. For example, in test 1, the message on personal finances, 295 (73.8%) from the sample of 400 users opened the mail message; of these, 148 (50.2%) were not trapped (did not follow the HTML link) and 147 (49.8%) were trapped by following the link. Figure 1 is a graphical representation of the figures.

Table 1. Behaviour data

Tests	Emails opened	Opened not trapped	Opened and trapped
Test 1	295	148 (50.2%)	147 (49.8%)
Test 2	213	160 (75.1%)	53 (24.9%)
Test 3	320	149 (46.6%)	171 (53.4%)
Test 4	265	148 (55.8%)	117 (44.2%)

It is interesting to note that tests 1 and 3 (personal finances and personal information), were more readily opened. There were also a fair number of employees who opened the message of test 4 (computer performance) while less users opened the message from test 2 (virus checker). The fact that only 53 of the 213 users were trapped with the virus checker message may indicate that there is a certain degree of awareness related to virus threats. At the same time it is disappointing that 50% of us-

ers were trapped in test 1 and more than half was willing to give their passwords away in test 3. These figures should be considered high given the environment and the above average level of computer literacy of staff.

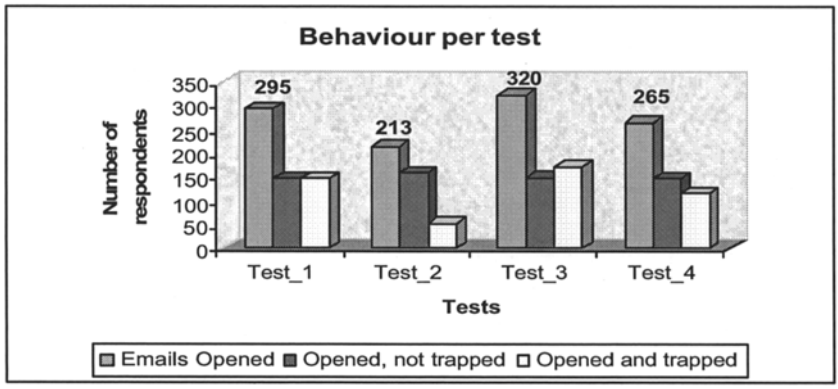

Fig. 1. Behaviour per test

Figure 2 presents the sample distribution of staff for all four tests over the 8 different divisions, e.g. Natural Sciences, Economic and Management Sciences etc., as well as a ninth one which represents the non-academic component.

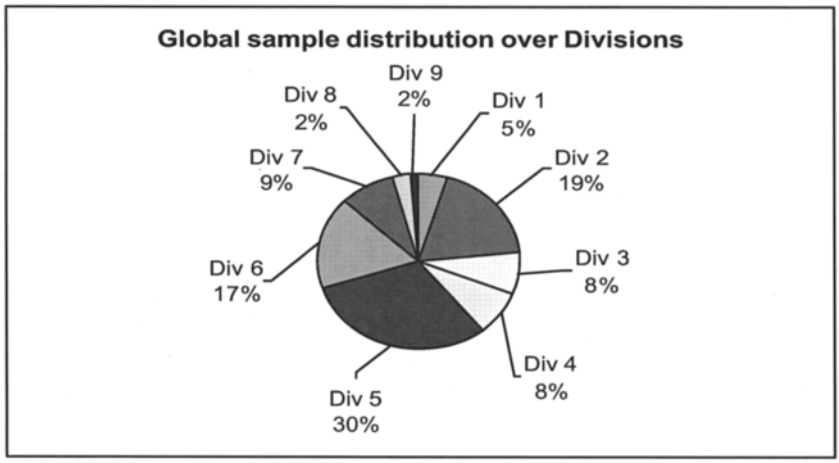

Fig. 2. Sample distribution over divisions

The distribution of employees, who were trapped in all four tests, is shown in figure 3. Although it is strongly related to the sample distribution in figure 2, it does provide certain insight into possible higher risk groups. For example, division 5 had 30% of the employees that were sampled (fig 2) and 35% of the employees that were

trapped (fig 3). Clearly division 5 is a higher risk group than, for example, division 6 where the proportions were 17% and 14% respectively.

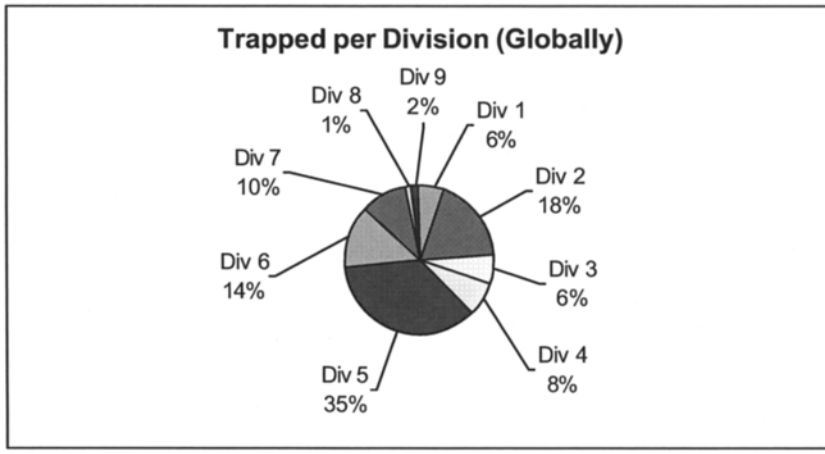

Fig. 3. Behaviour per division

The statistics so far are on a fairly high level. However, the design of the experiment and the data obtained made it possible to drill down into specific tests and specific divisions to such a level where the information becomes very significant and meaningful to management. The constraints of a conference paper prohibit a detailed presentation and explanation of such drill down activities and the following short example should suffice.

Table 2. Drill down data for test 2

Test 2	Sample size	Opened (%)	Delete - Not Opened (%)	Trapped (%)
Div 1	19	13 (68.42)	5 (26.32)	4 (30.77)
Div 2	76	39 (51.32)	16 (21.05)	11 (28.21)
Div 3	34	12 (35.29)	11 (32.35)	5 (41.67)
Div 4	29	14 (48.28)	7 (24.14)	3 (21.43)
Div 5	120	69 (57.50)	27 (22.50)	19 (27.54)
Div 6	69	39 (56.52)	19 (27.54)	6 (15.38)
Div 7	37	20 (54.0)	9 (24.32)	5 (25.00)
Div 8	9	3 (33.33)	5 (55.56)	0 (0.00)
Div 9	7	4 (57.14)	1 (14.29)	0 (0.00)
Total	**400**	**213 (53.25)**	**100 (25.00)**	**53 (24.88)**

Detailed figures per division for specific tests can be constructed. In table 2 such figures for test 2 are presented.

In the "Sample size" column, the number of employees per division, selected in the sample is shown. This is followed by the number and percentage of employees per division that opened the message. The "Delete (Not opened)" column indicates the number and percentage of people who deleted the email message, during the 7 days of the experiment, without opening it. It should be noted that the numbers in this column and the numbers in the "opened" column do not necessarily add up to the sample size. This is due to the fact that there were certain cases where overlapping of reactions were possible e.g. staff who was on leave during the exercise and who did not open or delete the messages. The last column indicates those that were trapped per division. From this table it is easy to see, for test 2, that an awareness campaign should not be a high priority in divisions 8 and 9 but rather be focused on divisions 3, 1, 2, and 5. Figure 4 shows the detailed figures from table 2 in graph form.

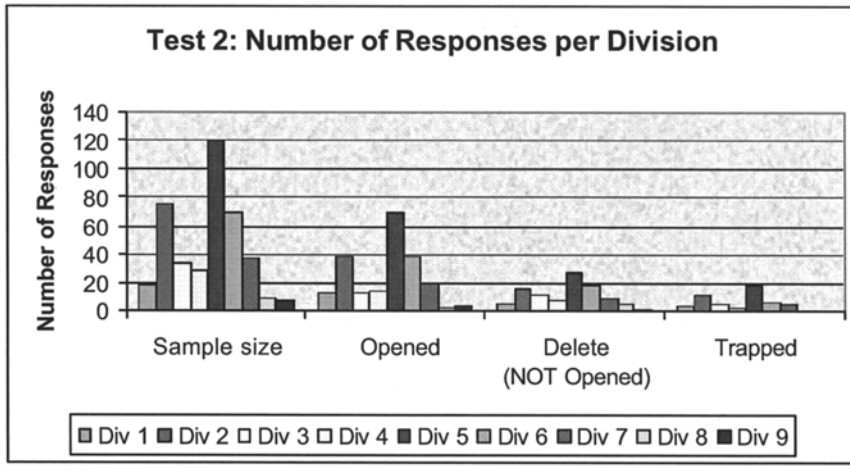

Fig. 4. Number of responses per division for test 2

The reported figures and data presentations in this paper are by no means a comprehensive report on the email awareness assessment and more detailed analyses and interpretations are possible. An important lesson from this assessment, however, was the confirmation that a significant number of users are irresponsible in certain situations. The temptations should be identified and acted upon and the results from the reported exercise should be helpful to indicate whereto and on what level awareness campaigns can be considered. The next section concludes the paper.

4 Conclusion

This paper has described a practical assessment of employees' awareness pertaining to responsible email usage. The experiment was performed as part of a bigger ICT se-

curity awareness project to obtain objective system data on users' behaviour. The results have shown that users generally acted irresponsibly in some of the tests, e.g. most users were trapped by emails regarding their personal finances and personal information. More than 50% of employees were willing to disclose their passwords. On the positive side employees appear to be more aware of virus threats.

The data obtained in these tests can be used for educational and training purposes in security awareness programmes. Not only can divisions be identified where guidance is needed but the specific types of threats that users are exposed to can also be identified. These results are made available to IT management and they are in a position now to address specific problem areas.

Future work will include the incorporation of the results obtained here with other system generated data. These tests can also be extended to other campuses or companies for comparative research purposes.

Acknowledgements

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

References

1. Pipkin, D.L.: *Information Security. Protecting the Global Enterprise.* Prentice-Hall Inc., (Upper Saddle River, NJ, 2000)
2. Dark, M.J.: Security Education, Training and Awareness from a Human Performance Technology Point of View, *In: Readings and Cases in Management of Information Security, Whitman, M.E., Mattord, H.J.* (Thomson Course Technology, 2006), pp. 86-104.
3. Drevin, L., Kruger, H.A. & Steyn, T.: 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.
4. Dodge, R.C. & Ferguson, A.J.: 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.
5. Kruger, H.A., Drevin, L. & Steyn, T.: A framework for evaluating ICT security awareness, *In: Proceedings of the 2006 ISSA Conference, Johannesburg, South Africa,* 5-7 July 2006 (on CD, 2006).
6. Steyn, T., Kruger, H.A. & Drevin, L.: Identity theft – Empirical evidence from a Phishing exercise, *In: Proceedings of the 2007 IFIP Conference, Sandton, South Africa,14-16* May 2007 (Accepted, to be published, 2007).
7. Steyn, A.G.W., Smit, C.F., Du Toit, S.H.C. & Strasheim, C.: *Moderne Statistiek vir die Praktyk*. Sesde uitgawe. (JL van Schaik. Pretoria, 1998).
8. Wegner, T.: *Applied Business Statistics*. (Juta & Co, Ltd. Kenwyn, 1993).