Behaviour & Information Technology, 2013
Vol. 32, No. 6, 584–593, http://dx.doi.org/10.1080/0144929X.2011.632650

Phishing for phishing awareness

K. Jansson* and R. von Solms

Institute for ICT Advancement, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

(*Received 18 March 2011; final version received 13 October 2011*)

Using various social-engineering techniques, criminals run havoc on the Internet and defraud many people in a number of different ways. This puts various organisational communities at risk. Therefore, it is important that people within such communities should learn how to protect themselves when active in cyberspace, or when dealing with cyber-related technologies. Training can indeed play a big role in this regard, and consequently, assist by altering the insecure behaviour of many people. The objective of this article is to ascertain whether simulating phishing attacks together with embedded training can contribute towards cultivating users' resistance towards 'phishing attacks'. In order to achieve this objective, a phishing exercise at an institution in South Africa was conducted.

Keywords: information security; social engineering; phishing

1. Introduction

Many criminals are currently focusing on attacking users; they do this by using deceptive techniques (social engineering) to carry out electronic fraud (Symantec 2010a). A number of authors refer to this as phishing (Dodge *et al*. 2007, Jagatic *et al*. 2007, Mann 2008, Kumaraguru *et al*. 2009, Aaron 2010, Aburrous *et al*. 2010). The Oxford English Dictionary (2009) defines phishing as: *the fraudulent practice of sending emails purporting to be from reputable companies, in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online*. Thus, phishing electronically deceives a user to conform to some action, subsequently, divulging sensitive information.

Phishing attacks have increased tremendously in recent times and the lack of awareness regarding such attacks can have devastating effects on any organisation or individual (Symantec 2010b). Consequently, it is important that the right phishing countermeasures are implemented. Indeed, most researchers and information security specialists agree that the key countermeasure to mitigate or prevent phishing attacks is security training (Dodge *et al*. 2007, Jagatic *et al*. 2007, Kumaraguru *et al*. 2009, Jansson and von Solms 2010).

Kumaraguru *et al*. (2009) evaluated the effects of simulating phishing attacks together with 'embedded' training on volunteering users. The authors of this article have used this approach in order to conduct an exercise to evaluate whether simulating phishing attacks together with embedded training can indeed contribute towards cultivating users' resistance to phishing attacks. Thus, in this research no volunteers were involved. The exercise was named 'the SERUM exercise' since it was partly based on some aspects of a model, called the Social Engineering Resistant User Model, with the same acronym (Jansson and von Solms 2011).

The remainder of the article is organised as follows: the next section discusses related work including previous phishing exercises. Then, some general principles for conducting phishing exercises were identified and defined. These principles were then reflected in the research methodology used in the exercise. Finally, the findings and results of the evaluation are presented, and the article concluded together with some benefits and drawbacks as well as future research suggestions.

2. Related work

There are many studies and solutions regarding how to protect the users of the Internet from phishing attacks.

One technical solution is to use anti-phishing security toolbars. These connect to a database or list where known phishing websites are blacklisted. Examples include, Websense, McAfee's anti-phishing filter, Netcraft anti-phishing system and Microsoft Phishing Filter (Aburrous *et al*. 2010).

Shahriar and Zulkernine (in press) developed and implemented a technical approach in the form of a tool named PhishTester to automate the process of testing whether a website is a phishing website or a legitimate website.

*Corresponding author. Email: Kenny.Jansson@nmmu.ac.za

Although technical tools can protect a user from falling prey to phishing attacks to a certain extent, it is important that the user does not become too reliant on technology. Thus, it is critical to combine the technical tools with phishing training (Kumaraguru *et al.* 2010).

There are many training solutions with regards to teach a user regarding how to avoid falling prey to phishing attacks. Jansson and von Solms (2010) developed a flowchart employees can follow to identify, mitigate or even prevent social engineering (including phishing) attacks. Srikwan and Jakobsson (2008) used cartoons to convey phishing awareness. Sheng *et al.* (2007) described the design and evaluation of 'Anti- Phishing Phil', an online game that teaches users good habits to help them avoid phishing attacks.

Solutions such as the ones discussed may sometimes be sufficient in mitigating phishing attacks. However, to be ensured whether this is the case, it is essential that the resistance to phishing attacks and its related countermeasures are measured (Jakobsson *et al.* 2008).

2.1. Simulating phishing attacks to measure phishing resistance

Several researchers have used security exercises that simulate real phishing attempts to evaluate the awareness levels of their subjects as well as their countermeasures (Ferguson 2005, Hasle *et al.* 2005, Jakobsson and Ratkiewicz 2006, Dodge *et al.* 2007, Jagatic *et al.* 2007, Steyn *et al.* 2007).

Jakobsson and Ratkiewicz (2006) presented a set of techniques for ethical and safe contractions of experiments to measure the success rate of a real phishing attack and disclosed the results of a number of experiments that adopted this set of techniques. Hasle *et al.* (2005) developed a social engineering metric, called Social Engineering Resistance (SER), to evaluate the resistance to social engineering in an organisation. Furthermore, they conducted an e-mail exercise that involved simulating phishing attacks to 120 subjects, and then measured their resistance.

Jagatic *et al.* (2007) studied the vulnerability of a university community towards a phishing attack that pretends to come from somebody in their own social network. Dodge *et al.* (2007) conducted a number of exercises over a couple of years on the United States Military Academy (USMA) – in order to evaluate the success of their awareness programmes.

2.2. Simulating phishing attacks with embedded training

Wash (2010) has modelled how users make security-decisions. Wash (2010) argues that in order for a user to defend against a threat, the user must first be exposed to the threat. Kumaraguru *et al.* (2010) argues that a user can learn how to defend against phishing attacks if the user pays adequate attention to the learning material.

Kumaraguru *et al.* (2009) has studied the principles of simulating phishing attacks together with embedded training on volunteers. Their 'embedded' training system teaches users to avoid falling prey to phishing attacks. To do this, this system sends simulated phishing e-mails to the users and records their action. Users who react 'insecurely' receive a 'training message' when falling for the attack. Each simulated phishing e-mail acts not only as a mechanism to deliver training, but also as a test to determine whether the user has learned how to distinguish legitimate messages from phishing messages. Therefore, one can identify and present training interventions only to those users who continue to fall for simulated phishing attacks. This principle is similar to what is often referred to as 'education on-demand' (Gordon and Pawlowski 2002).

Kumaraguru *et al.* (2009) sent 515 volunteers a series of three legitimate and seven simulated phishing e-mails over the course of 28 days and trained these subjects with the embedded training system. Results of this study show that users trained with the embedded training system retain knowledge even after 28 days. Additionally, adding a second training message to reinforce the original training decreases the likelihood of people giving information to phishing websites. Their results also show that training does not decrease users' willingness to click on links in legitimate messages and most participants enjoyed receiving training during their normal use of e-mail.

The authors of this article have used the principles of a phishing 'embedded' training system as proposed by Kumaraguru *et al.* (2009) to conduct a phishing exercise to conclude whether users' phishing resistance can be cultivated through simulating phishing attacks together with embedded training. It must be noted that the study by Kumaraguru *et al.* (2009) only involved volunteers and that the exercise in this article involved no volunteers. Thus, the subjects had no knowledge of any research exercise in advance. Additionally, the geographical location for the research in this article is different from Kumaraguru *et al.* (2009) as the study was conducted in South Africa.

3. Principles of the SERUM exercise

There are many principles to be considered when conducting phishing exercises. The following principles were identified and followed with regard to the SERUM exercise:

3.1. Before designing the exercise

Before the exercise was designed, the objective of the exercise was clearly defined (Dodge *et al.* 2007). Additionally, ethical clearance was obtained from the institution, as it is essential that phishing studies obtain ethical clearance (Jakobsson and Ratkiewicz 2006, Kumaraguru *et al.* 2009).

3.2. Before conducting the exercise

Before conducting the real exercise, the exercise was 'tested' on a focus group. The reason for this was to ensure that the simulated phishing e-mails had passed through spam filters, and that 'anti-phishing tools' in the web-browsers had not identified the 'phishing scam' (Kumaraguru *et al.* 2009).

The test population was recorded as 25,579 subjects (Hasle *et al.* 2005) and the timing of the exercise was such that the test could accurately assess the defined objective (Dodge *et al.* 2007). Thus, the exercise was conducted towards the end of the year, to allow all the subjects the necessary time to familiarise themselves with the e-mail system in use.

No information on the research exercise was disclosed to any subjects in advance, as this might well result in distortion or invalidation of the test data (Hasle *et al.* 2005). Furthermore, system administrators were alerted in regard to the exercise, and were provided with a predetermined response which they could use to respond to any enquiries from the subjects. This minimised the chance of the administrators distributing warnings regarding the simulated phishing e-mails (Kumaraguru *et al.* 2009).

3.3. During the exercise

During the exercise, each subject was exposed to a phishing attack (Hasle *et al.* 2005) and the subjects were provided with an e-mail message that they were invited to open. However, if they read the message carefully, they should have realised that it was not valid (Dodge *et al.* 2007). To make the subjects aware of their 'insecure' behaviour, the subjects received both immediate notification and delayed notification – after such behaviour (Dodge *et al.* 2007).

Users' user-ids and e-mail addresses were collected and stored to cross-reference data between the two cycles and to gather statistics. These were also compared with the e-mail-system's log to ensure that they were valid. Although the subjects were requested to divulge their password in a form field, no passwords or other sensitive information were collected and/or stored (Kumaraguru *et al.* 2009).

The outcome of an attack was either disclosure of sensitive data (user's name, e-mail address with a related password) or no disclosure of sensitive data (Hasle *et al.* 2005). Although the passwords were not verified, users' user-ids and e-mail addresses were considered to be sensitive data, since these could be sold on the black market and used for spam (Symantec 2010a).

The institution's computer security staff were not referred to in any e-mail message, since this might compromise the trust between them and the subjects (Dodge *et al.* 2007). Furthermore, subjects were not allowed to access the link in a message, or to open an attachment outside the institution. This minimised the chance that personal information was leaked outside the institution (Dodge *et al.* 2007).

3.4. After the exercise

After the exercise, logs were examined in order to find the number of active users (an active user is one who has read his/her e-mail) (Hasle *et al.* 2005). Additionally, all private data were deleted after the exercise in order to maintain privacy (Kumaraguru *et al.* 2009).

A week after the exercise, a general e-mail was distributed to all the subjects, making them aware of the exercise, and providing them with the contact details for questions or feedback (Kumaraguru *et al.* 2009).

The next section describes the methodology utilised during the SERUM exercise.

4. Methodology

Using the principles described in the previous section for conducting the phishing exercise, a software implementation was developed. The software implementation was tested on a small focus group – in order to find flaws within the software implementation. For example, it was found that it is difficult to determine whether a user has actually read through the content of the associated awareness programme. Therefore, an evaluation component consisting of three multiple-choice questions was included in the online training programme. After testing the prototype carefully, the formal phishing exercise was conducted. The exercise methodology is illustrated in Figure 1.

The total number of users on the e-mail system was found to be 25,579. These users belonged to one of seven faculty groups. Although Faculty group 2 may have consisted of more 'computer comfortable' users than other faculty groups, this group also involves other departments unrelated to information

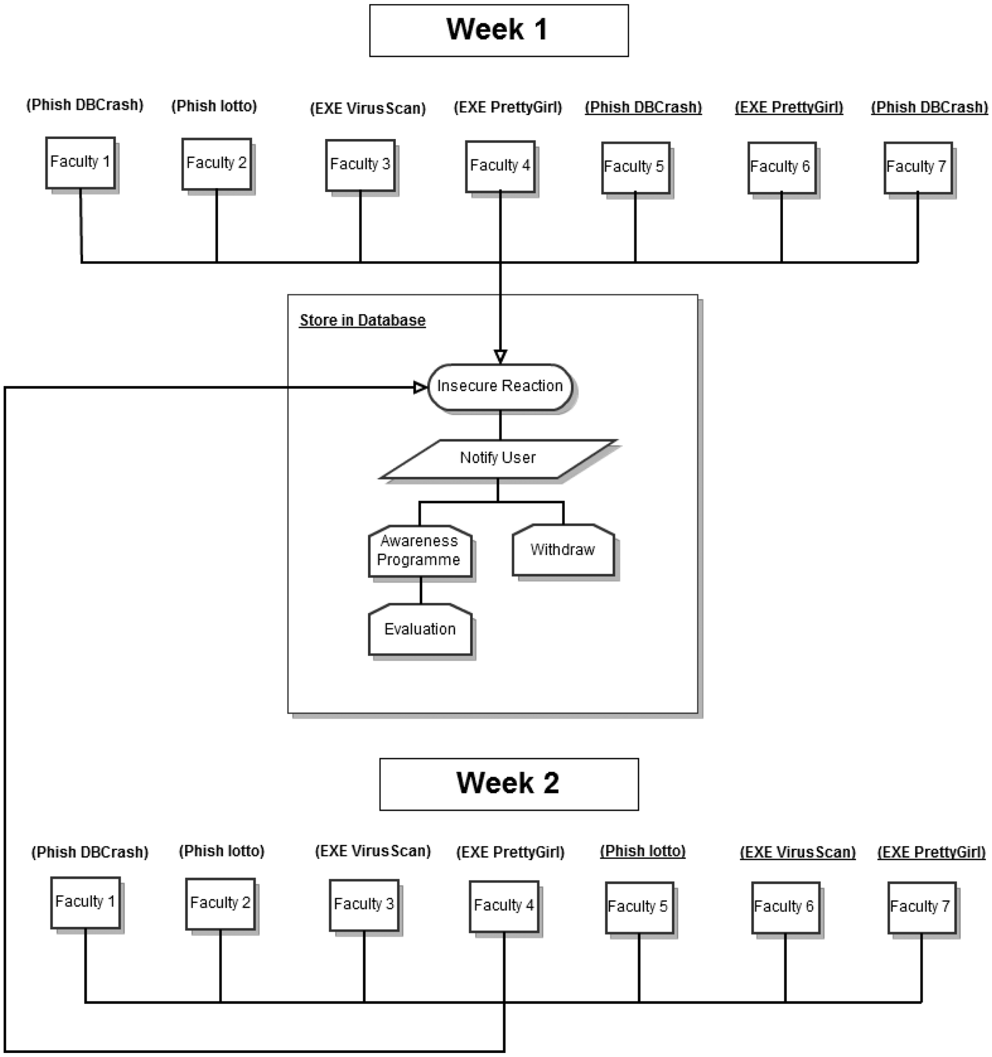


Figure 1. SERUM exercise methodology.

technology. Therefore, it is very difficult to have sound data regarding which group has the most 'computer comfortable' users in this study.

The type of simulated phishing attack a user received depended on the faculty group where the user was registered, as well as the week when the phishing attack was distributed. As illustrated in Figure 1, there were, in total, four different types of phishing attacks.

For example, users registered in Faculty 1 received a 'Lottery-Win' message (Figure 3) for both week one and week two. However, users within Faculty 7 received a 'Database Crash' message (Figure 2) in week one and a 'PrettyGirl' message (Figure 5) in week two. This method was integrated – to conclude whether the simulated phishing attack together with embedded training was effective in training users regarding different phishing attacks.

The types of phishing attacks are discussed in the following subsections.

4.1. *Database crash*

The Database Crash e-mail (illustrated in Figure 2) claimed that some database has crashed and, therefore, the user was requested to submit his/her username and password. This message used the following social engineering techniques (Twitchell 2009):

- Urgency: The message requested the user to update his/her credentials 'ASAP'.
- Legitimacy: The message appeared to originate from within the institution, since the institution's e-mail domain was used.

The user should have doubted whether the message was valid because the message requested the user to update his/her credentials. This is one of the most common methods 'phishers' use to gain sensitive information (Mann 2008).

4.2. *Lottery win*

This message (illustrated in Figure 3) requested the user to submit his/her username and password in order to claim a 'price' (notice the misspelling). This message used the following social engineering techniques (Twitchell 2009):

- Legitimacy: The message appeared to originate from within the institution, since the institution's e-mail domain was used.
- Strong affect: The user may have felt a strong sense of surprise.
- Curiosity: The user may have been tempted to witness what he/she had won.

The user should have doubted whether the message was valid for the following reasons:

(1) The message was sent to every student inside the faculty group. Thus, the 'to address' was Faculty@domain.com and not user@domain.com.
(2) The word 'price' was misspelled.
(3) The message was not addressed to an individual.

4.3. *Virus scanner*

This message (illustrated in Figure 4) claimed that the attached file vscan.exe would remove a dangerous virus. The message requested the user to open the ZIP file and launch the .exe file residing inside the ZIP file. This message used the following social engineering techniques (Twitchell 2009):

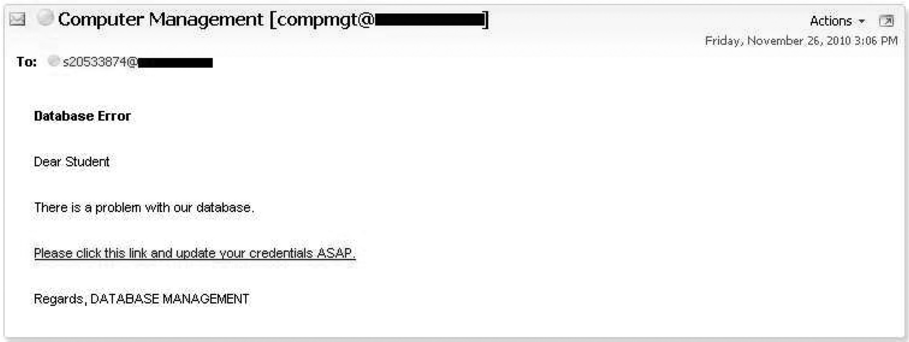
- Fear: The user may have feared that the virus that was detected may harm the user's computer.
- Legitimacy: The message appeared to originate from within the institution, since the institution's e-mail domain was used. The message also refers to 'COMPUTER MANAGEMENT'.

The user should have doubted whether the message was valid for the following reasons:

(1) The message was sent to every student inside a Faculty group. Thus, the 'to address' was Faculty@domain.com and notuser@domain.com.
(2) Installing software (including anti-virus software) should be done by computer staff only.

4.4. *PrettyGirl*

This message (illustrated in Figure 5) claimed that the attached file 'PrettyGirl.exe' promised pictures of 'hot'



Computer Management [compmgt@[redacted]]

Friday, November 26, 2010 3:06 PM

To: s20533874@[redacted]

Database Error

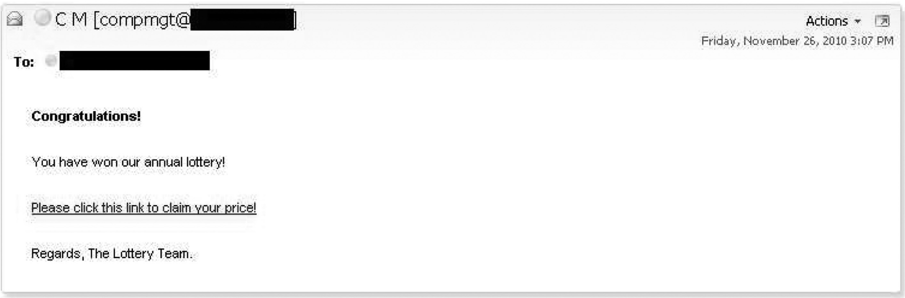
Dear Student

There is a problem with our database.

Please click this link and update your credentials ASAP.

Regards, DATABASE MANAGEMENT

Figure 2. Database crash.



C M [compmgt@[redacted]]

Friday, November 26, 2010 3:07 PM

To: [redacted]

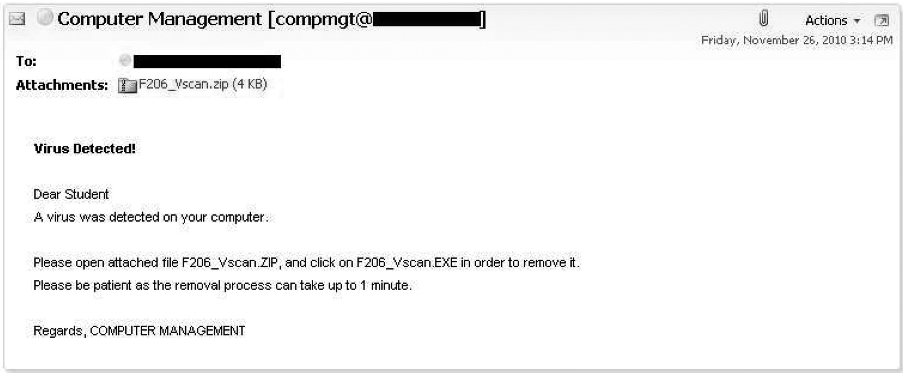
Congratulations!

You have won our annual lottery!

Please click this link to claim your price!

Regards, The Lottery Team.

Figure 3. Lottery win.



Computer Management [compmgt@[redacted]]

Friday, November 26, 2010 3:14 PM

To: [redacted]

Attachments: F206_Vscan.zip (4 KB)

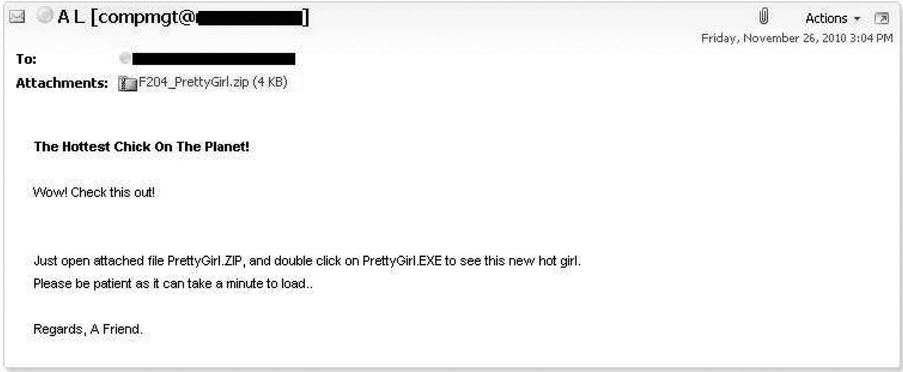
Virus Detected!

Dear Student
A virus was detected on your computer.

Please open attached file F206_Vscan.ZIP, and click on F206_Vscan.EXE in order to remove it.
Please be patient as the removal process can take up to 1 minute.

Regards, COMPUTER MANAGEMENT

Figure 4. Virus scan.



A L [compmgt@[redacted]]

Friday, November 26, 2010 3:04 PM

To: [redacted]

Attachments: F204_PrettyGirl.zip (4 KB)

The Hottest Chick On The Planet!

Wow! Check this out!

Just open attached file PrettyGirl.ZIP, and double click on PrettyGirl.EXE to see this new hot girl.
Please be patient as it can take a minute to load..

Regards, A Friend.

Figure 5. PrettyGirl.

girls. This message used the following social engineering techniques (Twitchell 2009):

- Curiosity: Many users may have been enticed into opening the attachment, as it promised pictures of 'hot girls'.

The user should have doubted whether the message was valid for the following reasons:

(1) The message was sent to every student inside a Faculty group. Thus, the 'to address' was Faculty@domain.com and not user@domain.com.
(2) No name regarding the sender of the message was included in the message. Only, 'A Friend' appeared.

5. Sequence of the SERUM exercise

The sequence of the SERUM exercise is illustrated in Figure 6. The exercise was conducted in two cycles over a period of two weeks, as follows: each user on the e-mail system received an e-mail that invited them to react insecurely – by responding with private information through a link to a website, or opening an exe attachment. The 'phishing website' or the exe attachment recorded the users who reacted 'insecurely'. These users then receive 'embedded training' in the form of a red warning screen, alerting them of their 'insecure' behaviour, as well as another e-mail message, making them aware of their 'insecure' behaviour. This message also provided a hyperlink to the online training programme, giving the user the option to participate in this programme. After reading through the content in the online training programme, the user also had the option to be evaluated by a number of short questions.

Users who did react insecurely did not receive any notification. Neither was their behaviour recorded. However, by comparing the e-mail log of each week with the exercise log of each week, it was possible to extract the users who had logged in on the e-mail system during each week but did not react to the simulated phishing attack. This concluded whether a user actually ignored (or did not notice) the phishing attack. Consequently, it was possible to deduce whether a user had behaved 'securely'.

Comparing the individual user behaviours between the two cycles made it possible to conclude whether the

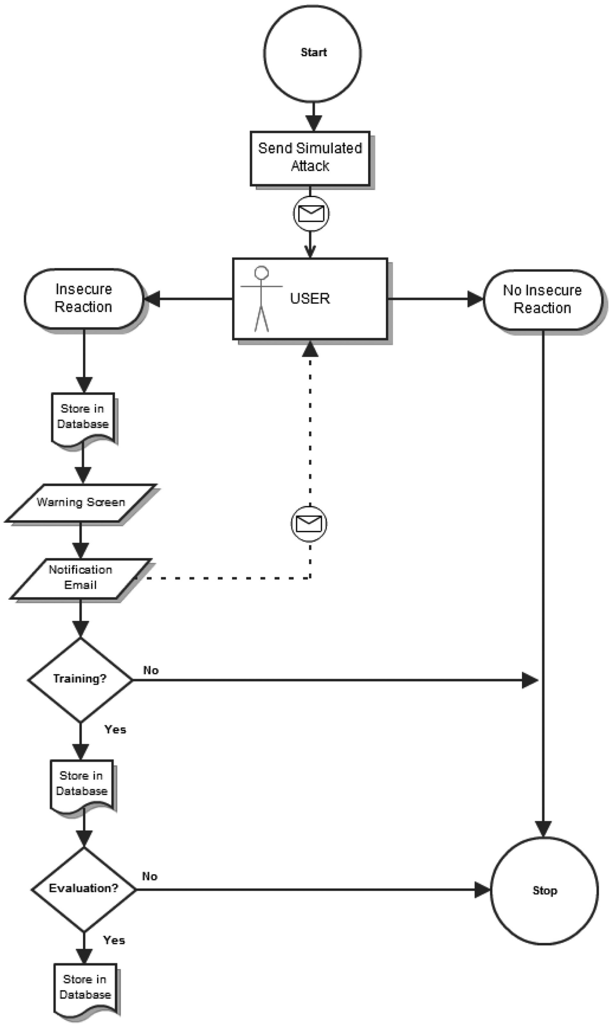


Figure 6. SERUM exercise flowchart.

individual users had learnt to act more securely regarding phishing attacks in the second cycle. Subsequently, this concluded whether the users' phishing resistance can be cultivated by simulating phishing attacks together with embedded training.

6. Findings and results

The following subsections include the findings and results of the research exercise.

6.1. *Week one*

A total of 9,273 (36.25% of all the users) checked their e-mails during week one (active users). A total of 1,304 users reacted incorrectly, while 165 of the reacting users took part in the awareness programme. Additionally, 108 of the reacting users evaluated themselves after the awareness programme. Thus, 14.06% of all the users who had logged in during week one reacted; 12.65% of these users took part in the awareness programme, and from these users, 65.4% evaluated themselves. In addition, PrettyGirl was the most enticing e-mail message during this week (Figure 7). It can also be argued that 7,969 users ignored the e-mail, as these were active on the e-mail system but did not react to the attack.

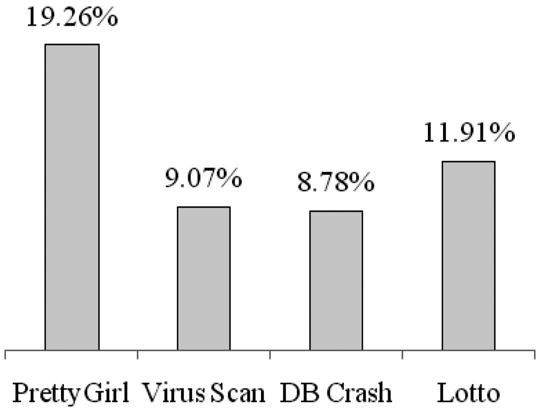


Figure 7. Reactions of active users per phishing type in week one.

6.2. *Week two*

In week two, 8,231 (32.18% of all the users) checked their e-mails (active users). A total of 664 users reacted, while 62 of these users took part in the awareness programme. Additionally, 35 users evaluated themselves afterwards. Thus, 8.06% of all the users who had logged in during week two reacted; 9.3% of these users took part in the awareness programme, and from these users, 56.4% evaluated themselves. In addition, PrettyGirl was also the most enticing e-mail message during week two (Figure 8). It can also be argued that 7,567 users ignored the e-mail, as these were active on the e-mail system but did not react to the attack.

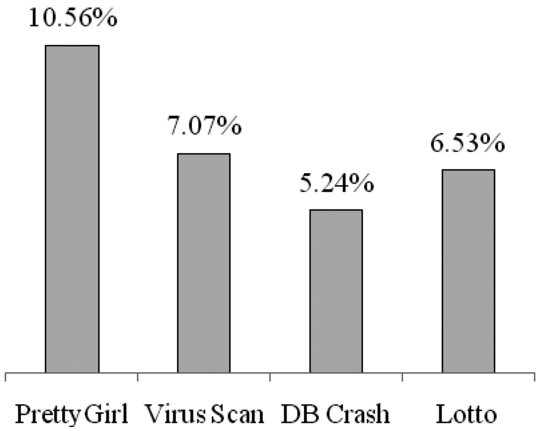


Figure 8. Reactions of active users per e-mail type in week two.

6.3. Discussion

Based on the results, it may be concluded that the number of reactions had decreased by 640 in week two (Figure 9). However, it must be noted that the number of active users was 1042 less in week two. Therefore, based on the difference between the active users during the weeks, it may be concluded that there were 42.63% less reactions in week two.

A group of 976 users reacting in week one did not react in week two. However, these users were logged in (active) on their e-mail during week two. This implies that 976 users (11.85%) learnt from the first attack in week one, since they had logged in on the e-mail system during both week one and week two, but did not react in week two. Out of these 976 users, 129 users participated in the awareness programme, and 80 of these users evaluated themselves. Thus, it may be assumed that 13.21% of the users who learnt had learnt from the awareness programme, while 8.19% of the users who learnt had probably learnt by evaluating themselves.

As illustrated in Figure 1, Faculties 5–7 received a different simulated phishing message in the second cycle (week two) compared with the first cycle (week one). Since a total of 201 users in these faculties 'learnt' from the exercise (Figure 10), this implies that simulating phishing attacks together with embedded training can indeed be effective in mitigating different types of phishing attacks.

From the data and findings discussed above, it may reasonably be concluded that users can learn and positively adapt their e-mail behaviour – as a result of simulated phishing exercises – together with embedded training. Therefore, it may be deduced that simulating phishing attacks together with embedded training can, indeed, contribute towards cultivating users' resistance to phishing attacks.

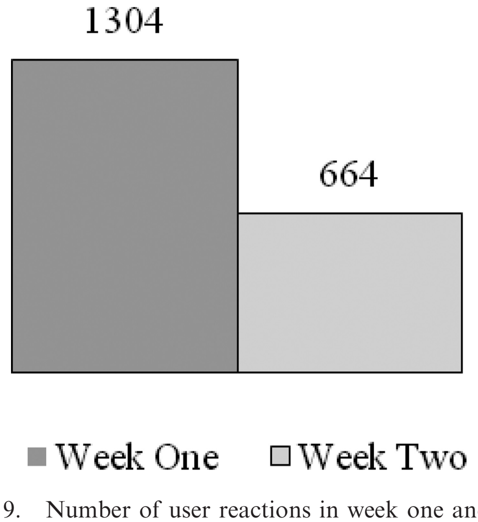


Figure 9. Number of user reactions in week one and week two.

7. Conclusion

With an increase in phishing attacks on the Internet (Symantec 2010b), it is essential that users learn how to protect themselves in cyberspace. This article has evaluated whether simulating phishing attacks together with embedded training can contribute towards cultivating user's resistance to phishing attacks. To do this, such an exercise was conducted on the e-mail system of an institution in South Africa.

Based on the exercise, it can be concluded that a simulated phishing attack together with embedded training can contribute towards cultivating users' phishing resistance as this approach reduces the user's risk of becoming a victim to any future phishing attack. This can be argued because many users reacted 'insecurely' in the first week but after receiving the embedded training in the form of a warning screen, notification email and the option to participate in the online training programme, several of these users reacted 'securely' in the second week.

It must also be noted that the amounts of reactions were 42.63% less in the second week. One contributing factor to this drop in reactions may have been because the users influenced each other and, thus, 'spread the word' that simulated phishing attacks were distributed on the e-mail-system. This could have made many users more vigilant.

There were also some other interesting findings. For instance, a user is most likely to fall victim to an enticing 'pornographic scam'. Another interesting finding is that a user can learn to behave securely towards phishing attacks that are different in nature. For example, some users were exposed to a request to divulge sensitive information in week one and exposed to a malicious exe attachment in week two. Since some of these users reacted in the first week but did not react in the second week, it was possible to conclude that a user can learn to behave securely towards different phishing attacks.

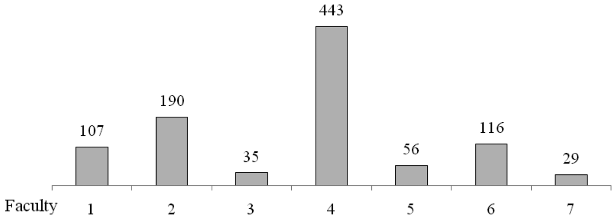


Figure 10. Amount of users that have learnt per faculty (in total 976 users have learnt).

7.1. *Benefits and drawbacks*

Because of the findings in this article, it can be concluded that simulating phishing attacks together with embedded training can provide the following benefits for the organisation. Firstly, the security of the system of an organisation can be enhanced, as many users may refrain from opening suspicious e-mail attachments, or responding to criminals with sensitive information. Secondly, by being able to spot vulnerable users, the idea of 'education on-demand' can reduce the costs of training employees, as the education takes place automatically and continuously. Finally, since the users come to acknowledge to themselves that they are vulnerable, they may often choose themselves to be trained regarding related attacks.

Although there can be many benefits with simulating phishing attacks with embedded training, it must be noted that there may be some drawbacks. For instance, a user may develop 'too much resistance' and ignore important 'non-fraudulent' requests since the user may believe that these are fraudulent. For this reason, it is important that an organisation conduct a phishing exercise with caution and design a simulated phishing attack to be as realistic as possible.

8. Future research

Researchers are urged to conduct further research based on simulating phishing attacks together with embedded training; in particular, whether giving feedback to users, after behaving securely towards a phishing attack, can contribute to making users more resistant towards phishing attacks. Furthermore, measure whether a user deletes a phishing e-mail or not. Additionally, research on other mediums, such as mobile messaging, could result in valuable findings.

References

Aaron, G., 2010. The state of phishing. *Computer Fraud & Security*, 2010 (6), 5–8.

Aburrous, M., *et al.*, 2010. Intelligent phishing detection system for e-banking using fuzzy data mining. *Expert systems with applications*, 37 (12), 7913.

Dodge, J., Carver, C., and Ferguson, A.J., 2007. Phishing for user security awareness. *Computers & Security*, 26 (1), 73–80.

Ferguson, A.J., 2005. Fostering e-mail security awareness: The West Point Carronade. *EDUCAUSE Quarterly*, 28 (1), 54–57.

Gordon, J.A. and Pawlowski, J., 2002. Education on-demand: the development of a simulator-based medical education service. *Academic Medicine*, 77 (7). Available from: http://journals.lww.com/academicmedicine/Fulltext/2002/07000/Education_On_demand__The_Development_of_a.42.aspx [Accessed 4 November 2011].

Hasle, H., *et al.*, 2005. Measuring resistance to social engineering. *In*: *Information security practice and experience: first international conference, ISPEC 2005*, 11–14 April 2005, Singapore. Berlin: Springer-Verlag, 132–143.

Jagatic, T.N., *et al.*, 2007. Social phishing. *Communications of the ACM*, 50, 94–100.

Jakobsson, M., Finn, P., and Johnson, N., 2008. Why and how to perform fraud experiments. *Security & Privacy, IEEE*, 6 (2), 66–68.

Jakobsson, M., and Ratkiewicz, J., 2006. Designing ethical phishing experiments: a study of (ROT13) rOnl query features. *In*: *Proceedings of the 15th international conference on world wide web*, 23–26 May 2006, Edinburgh, Scotland. New York: ACM Press, 513–522.

Jansson, K. and von Solms, R., 2010. Social engineering: towards a holistic solution. *In*: *Proceedings of the South African information security multi-conference (SAISMC 2010). South African Information Security Multi-Conference*, 17–18 May 2010, Port Elizabeth. Plymouth: Plymouth University.

Kumaraguru, P., *et al.*, 2009. School of phish: a real-world evaluation of anti-phishing training. *In*: *Proceedings of the 5th symposium on usable privacy and security SOUPS '09*. New York: ACM, 3:1–3:12.

Kumaraguru, P., *et al.*, 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10 (2), 7.

Mann, I., 2008. *Hacking the human: social engineering techniques and security countermeasures*. Aldershot, UK: Gower Publishing, Ltd.

Oxford English Dictionary, 2009. *Oxford English dictionary* [online]. Available from: http://dictionary.oed.com/cgi/entry/00323586/00323586se1?single=1&query_type=word&queryword=Neurolinguistic+programming&first=1&max_to_show=10&hilite=00323586se1 [Accessed 1 November 2011].

Shahriar, H. and Zulkernine, M., in press. Trustworthiness testing of phishing websites: a behavior model-based approach. *Future Generation Computer Systems*. Available from: http://www.sciencedirect.com/science/article/B6V06-5265S47-1/2/71cf3b73da4bff9605cf1733114e0bb6 [Accessed 4 November 2011].

Sheng, S., *et al.*, 2007. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. *In*: *Proceedings of the 3rd symposium on usable privacy and security*, 18–20 July 2007, Pittsburgh. 88–99.

Srikwan, S. and Jakobsson, M., 2008. Using cartoons to teach internet security. *Cryptologia*, 32 (2), 137–154.

Steyn, T., Kruger, H., and Drevin, L., 2007. Identity theft–empirical evidence from a phishing exercise. *In*: H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. Von Solms, eds. *New approaches for security, privacy and trust in complex environments*. IFIP International Federation for Information Processing. Boston: Springer, 193–203.

Symantec, 2010a. *Symantec intelligence quarterly: global report (July–September 2010)* [online]. Symantec Corporation. Available from: http://www.symantec.com/content/en/us/enterprise/white_papers/b-symc_intelligence_qtrly_july_to_sept_WP_21157366.en-us.pdf [Accessed 16 February 2011].

Symantec, 2010b. *Symantec report shows no slowdown in cyber attacks*. Symantec [online]. Available from: http://www.symantec.com/business/resources/articles/article.jsp?aid=20100527_report_shows_no_slowdown_in_cyber_attacks [Accessed 31 August 2010].

Twitchell, D., 2009. Social engineering and its countermeasures. *In*: M. Gupta and R. Sharman, eds. *Handbook of research on social and organizational liabilities in information security*. Hershey, PA: IGI Global, 228–242.

Wash, R., 2010. Folk models of home computer security. *Symposium on usable privacy and security (SOUPS)*. New York: ACM, 16.