Information Security Awareness & Training

H.Al-Ghatam and P.S.Dowland

Network Research Group, University of Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

This paper identifies users' weaknesses regarding information security awareness, based on a survey which was conducted to assess security awareness. The survey showed that it is often the actions of users which makes them vulnerable, and that many are aware of the problems but continue to compromise themselves. The survey result shows that training and education do benefit users, and there is a clear difference between trained users and the rest – demonstrating that education, and training can work. The survey results have been used to help develop a training tool, to provide resources and interactive learning tools for users. These tools have been assessed and demonstrated to help promote information security awareness.

Keywords

Security awareness, training, tutorial.

1. Introduction

Computer Security is something that all organisations want to achieve, and a problem which has been rising more and more, without a real solution being developed. A problem that all have, since the moment many got involved with the computer technology, and being part of the world global network, which is the internet. Organisations, and users started to complain about applications they use, and IT professionals for not providing much protection. Most of them do not know that the actual protection is in their hands. By having a level of security awareness themselves, security can be more realistically achieved. It is important to have a security awareness, and by using the right way to promote security awareness, the real security can be achieved.

A survey which been conducted to support this research, and which provided evidence that users which had previously training related to information security in the past, do have a better security awareness. After proving evidence of the problem existence, it became important to find a way to help to solve it. Training seems to be the best way to do that, that's why a security assessment and training tool been designed, and implemented. The tool provides users with the information and resources needed. In addition, the online assessment tool provides, allows users to assess themselves and provide them with a feedback, and supportive information. This paper has all the details, and information regarding the security awareness tool, the survey and other information related to the research.

2. Contexts

Having security awareness is very important to have for computer users, and employees. It is as important as having the latest firewalls, anti-virus, and security hardware. Aware computer users are the gate which attackers getting throw at the moment. Attackers trying to get the most from user's awareness, to try trick them, and get as much sensitive and confidential information as they can. To avoid that, computer users should be more aware about security aspects, and they should know that they are in the danger zone if they do not. Security is like a chain, and computer users are the largest link on this chain. Being the biggest link do not always means that it's the strongest one, actually computer users appear to be the weakest link on that chain. The reason of that is that users do not think that it have anything to do with their action and use of systems. 435 senior college and university administrators participated in a research for EDUCAUSA (Kvavik, 2004), which shows that user awareness and other cultural factors are the second major problem in US institutions, and it presents 42%, which shows how much awareness needed to prevent any security failures in our organisation.

3. Aim & Objectives

The project aims to prove the need of security awareness, and to help to produce a tool which provide normal computer users at home and at work with the basic knowledge they need to know in order to increase the security awareness level, so they can be more robust against computer security threats which targets computer users. The idea is to have a tool that have the ability to assess users, and provide employers to have an idea about the knowledge that their employee have. The tool will makes it easier for users to find their weaknesses, and will advice, and provide users with the appropriate materials, and tutorials that they have to look at depending on their assessment. The tool will help computer users to enhance their security knowledge, and gives them an idea about how they can avoid being trapped by their own mistakes, especially in a time when everybody connected to internet, the place where users get very vulnerable to security thetas without their knowledge.

4. The User Awareness Problem

A survey about users attitude and awareness, which been carried out in UK (Dowland *et al* 1999), about public attitudes and awareness. Aimed to assess the attitude and awareness of general public about the computer crime, and abuse. The research shows that most people have the wrong idea about where the danger is coming from, and the people who is responsible. The research showed that the media have a very big effect on computer users, where media always tend to put the blame on computer hackers on any breach of computer security, and the way that media defining hackers as a very skilled people in IT which nothing can stop them from backing into your system. The research shows that 30% of respondents think hackers are lonely, young, male and lacking social skills, which do not really refract the real image of hackers. This is just an example of how people are really unaware about what's really happening and what is the danger. Lack of security education, and the media way of presenting the problem is driving computer users to the wrong way.

But at the other hand, Media doing a great job by getting people to understand that there is a big danger of been attacked, and showing them the type of crimes that might happen using computers. The research shows that 80% of respondents felt that computer crime and abuse was a problem, and most people highly consider computer crime as a serious concern.

5. Promoting Security Awareness

Most organisations do understand that are security problem, but they are not fully understanding what to do about it. Most the time they end with doing the wrong things to solve the problem, or they try to do the right thing, and some do the first right step, but they stop there (Furnell *et al*, 2002). Like obtains guidelines like ISO 17799, and British standard 7799, but they do not really do what these guidelines says. Organisations have to understand that these guidelines are all about insuring security and responsibilities with the organisation to be highlighted and reinforced, by doing number of steps, like having a security officer within the organisation to handle security issues, and to determines what need to be done to reinforce the organisation security at the right time and by using the right tools. Promoting security awareness among organisation members, during day-to-day activities, and not forgetting the most important thing, which is ensuring that organisation members to take training courses.

Training is an essential part to ensure the security of your organisation, by teaching all members the right way to use they systems securely. Training is not meant to be just for key staff members, or just IT staff, but it should include all type of members. Different type should be placed for all types of members.

6. User Security Awareness Survey

It's important to know the level of security awareness users have, before taking any actions. In order to determine that, a survey has been conducted to help find some of the common security mistakes that users do, and how user normally reacts to some common can faces in their daily use of internet and computer, along with some other electronic devices like mobile phones. Users normally unaware of the danger that surrounding them while they are using internet, or even a computer connected to a privet network. Users tend to get them self in trouble by the action they do while using computer, and internet. Most users are unaware that the actions they are taking, makes them so vulnerable to security threats. One of the important question that this survey tries to answer is whether the level of awareness that users have does reflects their actions while using internet and computer, and if an computer security awareness campaign needs to be taken in mind, and if that can help increase the security level among all computer users.

The survey distributed online, and it was linked to the University of Plymouth's Network Research Group site, and to the British Computer Society's south west branch site which allowed visitors from both sites to participate and take part of the survey, which titled User Security Awareness. To get the best results from the survey, and not just from computer professionals, people from different

backgrounds, ages, and education levels been invited to participate as well. and The survey has been conducted for a period of 2 months, between March and May 2006, with 135 participants taken part in the survey.

When respondents quizzed about their actions regarding internet pop-up, by presenting them with an internet pop-up messages. The right action to take is to ignore the pop-up, and that to avoid the possibility of clicking on a link which can lead to virus infection or security attack on your computer. 77.78% of respondents said that they will ignore the message if it come up, while the remaining 22.22% of respondents said that they will response to the pop-up message.

It may sound positive that most of respondents had chosen to ignore the pop-up message, but 22.22% still a big number, especially taken in mind that 80% of the respondents who chosen to respond to the pop-up message are using the internet more than once every day. You can imagine the security threat that can face those who responds to those kind of pop-up, especially with the increase of malware threats, and pop-up on the internet. The survey shows as well that most of the respondents who responded to the pop-up message are at the age of 17 to 29 with 70%, with 30% for respondents at the age of 30 to 59. That give you an idea about the importance about educating young internet users about the safe use of computer and internet in particular, knowing that 88.8% of respondents whose aged 17 to 29 do use internet more than once every day, which shows how important is to consider training and educating users about the safe use of computer and internet, not only for employee, but also for young users as they make the majority of users at the present time.

Passwords is very important to keep personal information safe from others, and for passwords to be effective, they need to be used correctly. First of all, participants asked whether they use the same password for more than one application and e-mail. 55.5% said that they use the same password for more than one application and e-mail, where the 44.4% claim that they do not. Then participants asked about what do they do to remember their passwords. 73.3% of respondents stated that they do not have any problem memorising passwords. 6.6% said they do write their passwords down and keep them in a safe place, while 6.6% of respondents said they will do the same and write it down, but they will keep it somewhere close to the computer, or stick it on the computer monitor. 4.4% of respondents do save their passwords in their computers, by writing it in a text document, which is saved in the computer. Other 4.4% of respondents said they will use a password management software to keep their password in a safe place in case they need it to have a look to them, in case they forget them. 2.2% of respondents said that they save their passwords in their mobile phones. The remaining 2.2% of respondents said that they have another way to remember their passwords, but without stating what is that way they using.

The respondents, who said that they do not have any problem in memorising their passwords with 73.3% of respondents. It appears that 81.8% of them are at the age of 17 to 29 years old, which can make since because normally old people have less ability to memories things than young people. In fact, the reason why 73.3% of respondents do not have problem memorising their passwords, isn't because their age and ability to remember, but because that 51.5% of those who do not have problem

memorising (73.3%), are actually use the same password for more than one e-mail and application, which explain a lot why those do not have problem memorising, or they think they do not have problem. Memorising password always is the best option, but using the same password for more than one application will take the advantage from memorising the password, and users will have the disadvantage of making themselves very vulnerable, once your password get discovered by someone. In fact, the amount of lose can be more greater than, if user using different passwords for different applications, because who have the password will be able to access any system that user use, specially that the user use the same password for the different applications.

When participants asked about if they do open e-mails from unknown senders, 44.4% said they do not. 20% of participants said it depends on the e-mail subject whether they open it or not. 17.7% said they do sometimes open e-mails from unknown senders, with 8.8% not sure. Some minority of respondents with 6.6% say they do open e-mails from unknown senders. One of the respondents gave an interesting answer, by declaring that he use the university computers to open any suspicious e-mails messages he receives.

What's more, is that 66.6% of respondents who do open e-mails from unknown senders, do not check file extension, when they download files from the internet. In contrast, 90% of respondents who do not open e-mails from unknown senders, do check file extension before they download any file from the internet. Also, 66.6% of respondents who do open e-mails from unknown senders, never do back-up their computer files. To make matter worse for those who open e-mails from un-known senders, 33.3% of them said they would use the computer and internet normally, and will not care about if there is a virus attack going to struck soon, and they even will not take any action to prevent their computers get attacked. In fact, most of those respondents (84.2%) do use the internet more than once every day.

To see how training is effective, if it's been given to users, participants been asked whether they had IT security training or not. 66.6% of respondents said that they didn't have any training, while the other 33.3% said they did have IT security training. As well as having training, 53.3% of respondents said they get reminded time to time about computer and internet security. The positive thing, that 73.3% of the respondents who had training, do have a strong passwords, which is a combination of characters, words, and numbers. In addition, 60% of them, do change their passwords every one to three months. On the other hand, 53.3% of respondents who had training, do open e-mails from unknown senders.

Having a computer and internet security training is very important, but not all kind of training can be beneficial to computer users. But it seems that many respondents who had training in the past, and benefited from it, would recommend having training to other computer users. In fact, 41.9% of respondents who had training in the past, thinks that computer users should have training, related to computer and internet security.

7. Why Do We Need A Training Tool

Having a training tool at your organisation can get you a great benefit, and it can be a starting point for all members to know about IT security. Each organisation has to ensure that their members have got at least the basic knowledge of security, and know what to do in some circumstances. And training tools can be used as a security assessment tool at the same time, where organisations can assess their member of staff, and train them at the same time. The training tool make it easy for organisation to ensure all members have the minimum amount of security information required, which will make their future work more easier, as it going to be about keeping members updated at all time, and reminding them about what already know.

8. Security Awareness Assessment & Training Tool

A training tool has been designed in a way which makes it accessible by everybody from everywhere, that's why it been designed as an online application, with an easy navigation, and an easy way to use. The main part of the tool been designed using flash which can provide a nice, and easy interactive interface, with multimedia. The tool offers assessment, and tutorials for users to take.

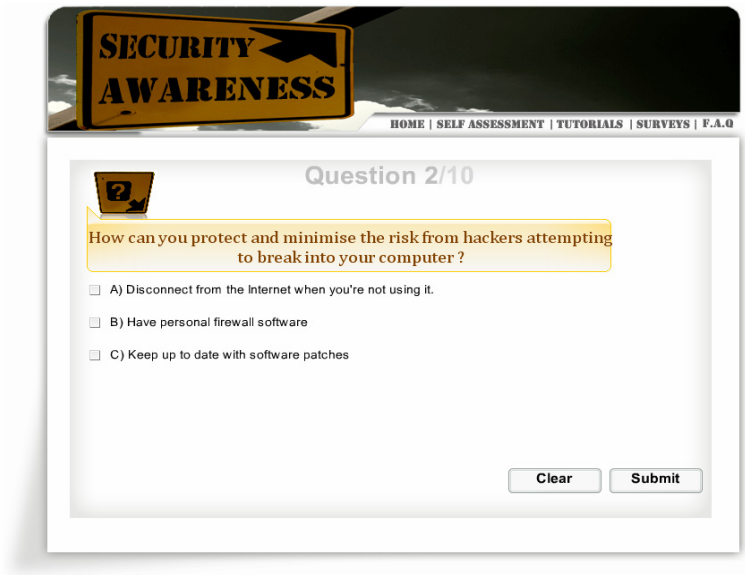

Figure 1: The assessment tool

When users access the assessment tool, they will be presented with number of questions, and they going to be assessed upon their answer to the questions (See figure 1). The users will be able to hear the question as well as reading it from the screen, which will provide a better level of interaction between user, and the application. If the user gives the right answer then will be presented with the next question or case. If the answer was wrong then he will be shown the right answer and why his question is wrong, before taking the user to the next question. That will help

providing users with just the information they do not know, while answering the right question will prevent giving them information they already know.

The online assessment tool will provide users with their assessment's result, by the end of the assessment. After users finish their assessment, and by the end of it, users will see the score they have got, and a short description what that score mean. In addition, users going to be provided with a list of tutorials which they can take to improve their security knowledge. In addition, the online tool will provide users with number of tutorials, which they can access and use any time. These tutorials can be found on the tutorials section, which can be accessed easily from anywhere in the tool. When users click on the tutorial they want to take, the tool will load the tutorial they are looking to take. Tutorials will display a question and an answer, to allow users to understand what the given information solves, and how they can they benefit from it.

9. Conclusion

The initial idea of this project is to develop a user awareness assessment and training tool, which been implemented and designed upon the survey result. The survey which been conducted for a period of two months, did provide some valuable information. The survey did prove that most computer users do have unsafe computer practices, which make users, and the computers they work on very vulnerable. In fact, it's been proven by the survey, that users who had previously training, have a better, and safer computer practices. They do have stronger passwords, do back-up regularly, and have a better idea how to protect their computers. In addition, educated users are more difficult to be tricked my malware writers.

10. References

Dowland P.S, Furnell S.M, Illingworth H.M and Reynolds P.L (1999). "Computer crime and abuse: A survey of public Attitude and awareness", Computers & Security, vol. 18, no. 8, Pages 715-726, 1999

Furnell S.M, Gennatou M, Dowland P.S (2002)"prototype tool for information security awareness and training", International Journal of Logistics Information Management, vol. 15, no. 5, Pages 352-357, 2002

Kvavik B.R (2004). "Information Technology Security: Governance, Strategy, and Practice in Higher Education", EDUCAUSE Centre for applied research at University of Minnesota, Available: http://www.educause.edu/ir/library/pdf/ecar_so/ers/ERS0305/ECM0305.pdf, [Accessed January 2006]