Paakat
Revista de tecnología y sociedad

Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios

Awareness and Training to Increase Cyber-Security in University Students

http://dx.doi.org/10.18381/Pk.a8n14.318

Ramón Ventura Roque Hernández*
Universidad Autónoma de Tamaulipas, México

Carlos Manuel Juárez Ibarra**
Universidad Autónoma de Tamaulipas, México

Received: December 29, 2017
Accepted: February 9, 2018

RESUMEN

Este artículo presenta una investigación realizada para explorar las deficiencias en seguridad informática que poseen los alumnos universitarios de licenciatura en informática en sus primeros semestres, y para evaluar preliminarmente el efecto que tendría un programa de capacitación y concientización diseñado para ellos. Se trabajó con un solo grupo de participantes, a quienes se encuestó antes y después de un evento formativo en modalidad de conferencia. Para analizar los datos se utilizó el software SPSS, donde se realizaron pruebas no paramétricas de Wilcoxon para buscar diferencias entre las respuestas recabadas antes y después del evento. Se encontró que los participantes podrían tener mayores niveles de conocimientos y seguridad en sus actividades cotidianas de cómputo, y que el evento logró incrementar indicadores tales como la percepción de conocimientos sobre seguridad informática y la conciencia de realizar respaldos más frecuentemente. Los resultados preliminares muestran un efecto positivo que motiva a implementar un programa permanente de concientización y capacitación.

Palabras clave
Educación superior; tecnología de la información; internet

ABSTRACT

This paper presents a research aimed at: 1) exploring the deficiencies in cyber security that freshman university students of Information Technology (IT) undergraduate programs have, and 2) evaluating the effect that an awareness and training program designed for them would have. In this research, one group of students participated; they were surveyed before and after a training activity that was presented to them as a conference. The responses of the participants were analyzed using the SPSS statistical software, and several Wilcoxon non parametrical tests were performed to find differences before and after the event. It was found that participants could have higher levels of knowledge and safety in their daily activities; also, it was found that the conference increased the perception about cyber-security concepts and the awareness to create information back-ups more often. These preliminary results show a positive effect that encourages to implement a permanent training and awareness program.

Keywords
Higher Education; Information Technology; Internet

INTRODUCTION

Computer security is currently a central issue for all users of computer equipment, whether desktop or mobile, at home, school or within an organization. The popularity of the use of the Internet has brought important security risks. Since its inception, the Internet is used for purposes other than those it was conceived. Initially the Internet was designed to promote connectivity and not security (Jenab and Moslehpour, 2016).

The rapid adoption of the Internet, mobile devices and Cloud applications has hindered companies in rapidly implementing measures that would improve the security to face the threats of today's world (Stanciu and Tinca, 2016). All users of IT resources should be more critical of the activities they perform on their computers, especially for those activities connected to the Internet. However, even today many users seem to overlook cybersecurity.

This article presents a research which objectives were to explore the deficiencies in the area of cybersecurity that the undergraduate computer science students experience in their first semesters, and to preliminarily evaluate the effects that a training and awareness program oriented to increasing the level of cybersecurity of these students would have on their daily computing tasks. As research design, we chose to work with one group of participants only. The latter were surveyed before and after a training program given in conference mode.

This paper is organized as follows: first, we expose the background of the subject, which includes the technical definitions used in this article as well as the previous paper written under the same line of research. Subsequently, we explain the methodology followed for this study, which gives details of the participants, the setting, the collection instrument, intervention, type of study and research design, as well as the conceptual and operational definition of the variables. Next, we present the results obtained in the statistical analysis of the data and the discussion with its implications. Finally, we address the conclusions of this study.

Background

Cybersecurity

Security is a topic that has gained increasing relevance for computer sciences given the growth of the Internet and the volume of data exchanged currently (Forouzan, 2003). Cybersecurity not only seeks to protect equipment and data, but also people.

Therefore, education and awareness must be valued as useful tools against dangerous incidents. For example, users can be trained on preventive measures and good practices that help them understand the meaning of threats and how to protect themselves against them. In doing so, users can be more cautious and hence, increase the level of security they have in their daily computing activities.

Within cybersecurity there are many terms and problems that users should know. In our research, we have focused our attention on the following: *hackers, crackers*, worms, Trojans, *spyware, phishing* and information backups. Next, we will address each of these terms.

Hackers y crackers

According to Magazine (2009), a hacker is a person with a high level of technical knowledge who uses a computer to access a computer or network with the object of carrying out unauthorized activities. Some experts argue that *hackers* have ethical principles and that their actions do not carry any malicious intent. On the contrary, a *cracker*, while doing the same as a *hacker*, does have implicit malicious objectives to his behavior.

Worms, Trojans and Spyware

A malicious code is any program written to produce inconveniences to the user (Miguel-Pérez, 2015). Its effects may include data destruction, misuse of resources and information theft. Worms, Trojans and *spyware* are examples of this type of code.

Jenab and Moslehpour (2016) define worms as malicious programs that can replicate themselves, and can be transmitted from different places, for example on the internet through instant messaging, or sharing files on networks. Although worms are widely known to users, they still continue to infect computers successfully due to the security vulnerabilities of current systems.

Trojans are programs that cannot replicate themselves, but offer the user an apparently useful functionality such as removing viruses from their system. Once these programs are run, they infect the computer with viruses that can send information, provide remote access or disable protection options. Trojans are difficult to detect since they are disguised as useful programs; however, they are just the opposite and slow down the operations of the computer.

The term *spyware* refers to programs that gather information from an end user without his knowledge. These programs can be used to show contents relevant to the user or to install other programs that can siphon information from the keystrokes and thus, steal passwords or record the search history of a user. A *spyware* does not replicate itself to other computers.

Phishing

Phishing is a way of stealing information through an email that seems to come from a legitimate organization (Aston, 2016). The email includes a link that leads to a fake site, which is a copy of the original and is responsible for tricking the user in order to steal passwords, personal information or credit cards.

Until a few years ago it was easy to identify these types of threats since they contained elements that were visibly suspicious. For example, their design was simplistic or their writing poor. Today it is more difficult to identify if an email is legitimate or not, because the quality of the falsifications has increased notably.

Information Backups

Information is an important asset for companies and for people (Rhodes-Ousley, 2013), thus, it is necessary to safeguard it; one way of doing so is through backups. A backup is a copy of the important files of a computer system made in order to prevent possible loss due to *hardware*, *software* errors, or virus infections to mention only a few causes.

Backups can be complete, that is, of all the files, or incremental or only of the files that have changed since the last backup. The decision to perform a full or incremental backup can accelerate or lengthen considerably the file copying process (Stier, 2015).

Backups should be made periodically and stored in places other than the computer equipment in order to prevent loss due to physical disaster. In this way, the cloud is a good option to save backups since their servers are geographically distant from the equipment that is being backed up.

Awareness and training programs

Wiseman (2017) and Peterson (2017) highlight the importance of training users, regardless of their good intentions or the new technologies they use. Human beings are always the weakest link in the chain of data protection. Wiseman also believes that awareness is key in the battle against intruders and advises periodic evaluations among users to determine if they recognize potential vulnerabilities in order they act accordingly and improve the cybersecurity of an organization.

According to Rhodes-Ousley (2013), cybersecurity awareness programs are useful tools to educate users on computer media about the behaviors expected of them, the actions they must perform in certain scenarios and the consequences of not following the established rules.

An awareness program also helps people understand the importance of following the rules and the benefits when taking measures that help increase the security of their data. The main objective of an awareness program is to change behaviors, habits and attitudes. Some resources used to achieve this include seminars, online trainings, videos, emails, posters and games. This objective must be met through a long-term continuous process and must be careful not to saturate users with too much information at once.

These programs address some of the following topics: information privacy, *software* and *hardware* vulnerabilities, malicious codes such as viruses, worms, trojans, *spyware* and the damage they can cause. Rhodes-Ousley mentions that an awareness program may fail for several reasons such as the lack of incentives to motivate user's participation, as

well as the lack of measurements to ensure that users understand the material and to evaluate its behavior in predetermined scenarios.

Peltier's work (2002) emphasizes that an effective program of awareness in cybersecurity will allow users to understand the reasons why they should take cybersecurity seriously; the gains they will obtain from implementing it and how it will help them in their daily tasks.

Peltier also mentions that a program of this nature should seek to reduce losses associated to the intentional or accidental disclosure of information as well as the modification or destruction of data; then, the users would improve the efficiency and productivity in their tasks.

Peltier recommends that the training sessions last less than fifty minutes, and be prepared with the vocabulary appropriate to the audience to maintain the attention and interest of the attendees. The sessions can be scheduled during the users' everyday activities, but taking care of not interfering with their busiest hours.

Previous works

According to Dunn Cavelty (2014), the approaches used to provide cybersecurity seem to be failing, as security levels instead of increasing are decreasing even more. The reason for this decrease is that security is a multidimensional phenomenon which is often conceived as a technical aspect and separated from the human elements of computing. Awareness about the safety requirements could help get better results.

North and Pascoe (2016) indicate that cybersecurity is a topic of growing concern, especially for private sector companies, since they are the ones that are most frequently victims of expensive computer attacks. In their work, North and Pascoe highlight the importance of conceiving safety as a topic of interest for the entire organization and not just for the technology department.

Company officers have a very important task in regard to this process, since they should provide the necessary means to promote a continuous culture of awareness about cybersecurity. Furthermore, they must ensure that there are financial resources to implement a permanent program that supports this culture among the staff.

Awareness, at university level, plays an important role in creating an acute perception of cybersecurity risks among students. They are future professionals who will soon face computer threats as part of their professional lives. Some researches have identified the importance that security be fostered and researched at university level.

The work of Stanciu and Tinca (2016) highlights the urgent need to implement training and awareness programs on cybersecurity, especially at university level, since students' knowledge is usually more technical and specific to their field of study and less oriented towards security aspects. It is emphasized that people's attitude, coupled with their behavior, represents a very important weakness. For example, human errors committed

unintentionally and the misuse of systems by the staff has led to serious security incidents.

In his work, Kiani (2016), studies the perception the students of a specific university have of cybersecurity. Said university offers online academic programs and addresses the influence of individual characteristics such as age, sex and marital status as well as aspects of social trust on the perception of cybersecurity. In this study, we found that the greater the social trust, the higher the perception of cybersecurity, while at a greater age, the lower is the perception of security

Case and King (2013), in their research, carried out a longitudinal study on the perceptions and the habits related to cybersecurity in undergraduate students. They found that the number of emails with *spam* and *phishing* received by students had decreased in recent years; so had their level of concern about attacks and theft identity.

On the other hand, it was found that the students at that university reported a safer computer behavior in recent years than at the beginning of the research. This positive change in their habits is attributed to the proactive training that students have been receiving on security in their regular classes.

Whitty, Doodson, Creese and Hodges (2015) studied more specifically the bad practices of people in regard to passwords. They found that people know the recommendations for the proper use of passwords; however, they are optimistic in believing that it is unlikely that they will experience negative incidents, therefore, they do not value the negative consequences of their bad practices.

They also found that young people are more likely to share their passwords with others, and that educational programs on security should target young people as their primary objective. They also stress that in this context, knowledge dos not suffice to change the dangerous behaviors related to cybersecurity, and that the evidence shows that if bad practices are to be eliminated, the training should also promote awareness and not only technical knowledge.

Methodology

Participants

Six second-semester students of the Bachelor's Degree in Computer Sciences (LI, [Spanish acronym]) of the Faculty of Commerce, Administration and Social Sciences (FCACS [Spanish acronym]) of the Autonomous University of Tamaulipas (UAT [Spanish acronym]), in Nuevo Laredo participated in this research. The study was conducted in the 2017 spring class period, with 27 students registered in the second semester of the Bachelor's Degree in Computer Sciences at the FCACS.

Although all the students were present at some point in the training event, the responses of eleven participants were rejected since they did not answer the questionnaire in any of the two periods in which the measurements were taken. The reason for this rejection

is that they arrived late, they retired before finishing the event or they were absent for a few moments.

Setting

This study was conducted during a cybersecurity training event that lasted fifty minutes and was addressed to the FCACS LI students. The event was held at the facilities of a computer center located within the same faculty, and was scheduled during the students' regular class hours, but separately from the subjects they were studying during that semester.

The professors proposed this training given the deficiencies they had observed in the students of the first semesters on the subject of cybersecurity. Hadn't they done so, they would have overseen severe risks for the students and for the computer resources they use on a regular basis at the university. The topics proposed for the training included: vulnerabilities, viruses, worms, Trojans, *spyware*, *phishing*, means of prevention, diagnosis and recovery of incidents, as well as the *firewall, hackers* and *crackers* concepts.

These contents were taught free of charge by an external professional expert. This expert had a bachelor's degree in Computer Sciences and a Master's Degree in Computer Technology. Besides having teaching experience, he owns a *software* development and technical support business, which has a significant number of clients in the locality.

The students had the opportunity to listen to the topics presented with a pleasant, practical and applied approach. They could also interact with the expert by asking him questions and making comments. The room was well equipped with sufficient seating for all the attendees, air conditioning and a video projector to show any electronic presentation.

Instrument

The Table 1 questionnaire was used to gather data. Questions P1 to P5 were to be answered by using a scale from 0 to 10, where zero represented: "absolutely none / nothing" and ten, "a lot". Question 6 was presented with the following possible answers with their numerical codes indicated between parentheses: today (0), tomorrow (1), this week (2), in two weeks (3), in three weeks (4), in one month (5), in more than a month (6).

In this question, the greater the numerical value of the answer, the more distant the date for the student to carry out his next backup. It is important to note that the version of the questionnaire shown in Table 1 is the result of a couple of refinements that consisted of the evaluation of experts and the application of a pilot test. These procedures allowed adjusting the wording and the order of the questions, as well as the scales for the answers.

Table 1. Questions asked to students

Identifier	Question
Q1	What level of security do you have in your daily computing activities?
Q2	What level of knowledge do you have about security?
Q3	How clear are the differences between *hacker* and *cracker*?
Q4	How clear are the differences between worm, Trojan and *spyware*?
Q5	How much do you know about *phishing*?
Q6	When will the next backup of your information be?

Source: Developed by the author.

Intervention

First, the students were surveyed just before the training. Subsequently, the guest expert presented the topics and immediately afterwards the students were surveyed again with the objective of knowing the effect of the training offered to them. On both instances, the questionnaires were handed out to the students on a whit half letter sheet of paper with the questions and possible printed answers. The participants marked their answers with the pens that were provided.

Type of study and research design

A pre and post-test experimental study of a single group was conducted. This research design offers the possibility of making a comparison of the same individuals before and after a treatment. The difference observed in both instances is the measure of the influence of the experimental treatment (Zikmund, Barry, Carr and Griffin, 2013).

Conceptual and operational definition of variables

Table 2 shows the variables studied in this research, as well as their conceptual definitions and the questions associated to the questionnaire used:

Table 2. Conceptual and operational definition of variables

Variable	Conceptual Definition	Operational Definition and Questions
Applied security	Students' perception of the level of cybersecurity applied in his daily tasks	Q1
Knowledge on security	Student's perception of the level of security knowledge he has	Q2
Knowledge on attackers	Student's perception of the level of knowledge he has to make the difference between a *hacker* and a *cracker*	Q3

Knowledge on *software* threats	Students' perception of the level of knowledge he has to make the difference between a worm, a Trojan or a *spyware* program	Q4
Knowledge on *phishing*	Student's Perception of the level of knowledge he has on *phishing*	Q5
Time to carry out information backups	Time in which the student plans to make his next information backup	Q6

Source: Developed by the author.

Analysis of data

The students' answers were gathered before and after the conference, and were organized and captured using the SPSS *software* version 22 (Wagner, 2014). By using this statistical package, the data descriptive values were obtained and non-parametric Wilcoxon tests were conducted (Anderson, Sweeney and Williams, 2011).

The objective of every question in Table 1 was to find significant statistical differences between the students' perceptions at the two instances of the study. A reference confidence level of 95% was used. In this way, any bilateral QValue (significance) inferior to .05 in the hypothesis tests was interpreted as an indicator of the existence of the differences between the students' perceptions before and after the conference.

Results

Table 3 shows the answers obtained in applying the questionnaire before the conference. Table 4 shows the summary of the answers provided by the students after the conference. Table 5 shows the result of the non-parametric Wilcoxon test.

Table 3. Descriptive Data of the Answers to the Questions before the Conference

	P1	**P2**	**P3**	**P4**	**P5**	**P6**
Media	6.25	6.63	4.50	5.75	2.31	3.44
Desv. est.	2.463	1.360	2.449	2.769	2.869	2.529
Mediana	7.00	7.00	5.00	6.00	.50	4.00
Rango intercuartil	3	2	5	5	5	5

Source: Developed by the author.

Table 4. Descriptive Data of the Answers to the Questions after the Conference

	P1	**P2**	**P3**	**P4**	**P5**	**P6**
Media	7.00	8.06	9.25	8.63	7.75	1.75
Desv. est.	2.129	1.389	.931	1.544	2.380	1.390
Mediana	8.00	8.50	9.50	9.00	8.00	3.00
Rango intercuartil	4	2	1	2	3	4

Source: Developed by the author.

Table 5. Results of the Wilcoxon Non-parametric Test to Find Differences between the Answers Before and After the Conference

	P1	P2	P3	P4	P5	P6
Z	-1.170	-3.096	-3.529	-3.022	-3.433	-2.547
PValor bilateral	.242	.002	.000	.003	.001	.011

Source: Developed by the author.

Discussion

Discussion of the results of the statistical tests

When performing the non-parametric Wilcoxon test, no significant statistical differences were found in question 1. This was expected as it refers to current practices in daily computing activities, which would not be modified immediately after a training session, but rather after some time.

Significant statistical differences were found in question 2 (what level of knowledge do you have about security?). The highest score was obtained after the conference. This indicates that the students perceived that their knowledge had increased thanks to the content that was addressed in the seminar.

Significant statistical differences were also established in question 3 (how clear are the differences between *hacker* and *cracker*?), question 4 (how clear are the differences between worm, Trojan, and *spyware*?), and question 5 (How much do you know about *phishing*?). These questions referred to concepts that were directly addressed during the training; therefore, it is understandable that the higher scores were recorded after said training.

It is striking that most students reported knowing little about the *phishing* term before attending the event. These findings are in agreement with those of Stanciu and Tinca (2016), who, in their research, found that the students did not know anything about *phishing* and its consequences even though this type of attacks are on the rise.

Question 6 (when will the next backup of your information be?), also shows differences between the students' answers. It is noteworthy that before the conference the students had planned to backup their information further in time, but immediately after the conference the students' perception was modified and they said that they would backup their information at a closer date.

Discussion of the implication of the results

The results obtained showed that the participants, in spite of being students from the bachelor's degree in Computer Sciences, could have a higher level of security in their daily computing activities. This is especially important at a time when networks and the Internet are used very frequently and the connectivity they offer bears within latent threats that the users must recognize in order to protect themselves adequately.

It was noted that the training event increased students' perception of their cybersecurity knowledge, and it also raised their awareness to take immediate measures to protect their data. This was interpreted as a positive effect that must be constantly strengthened with activities aiming at improving the security of the students and of their information.

While it is true that our research exposes the need to offer cybersecurity training and awareness programs at university level, and reveals the benefits of this type of resources, the limitations of our study must be taken into account.

This investigation, while being a preliminary evaluation, focuses on the students' perceptions and does not measure their knowledge or evaluate the effect of the training event after some time. Both of these activities remain proposals for pursuing this study.

In the same way as Wiseman (2017), Peterson (2017) and Rhodes-Ousley (2013), we consider that training and awareness are important as means of prevention and as agents of change of students' behaviors, habits and attitudes. We recommend that these training actions be for all areas and not only aimed at students of professional technological careers, thus agreeing with North and Pascoe (2016). Finally, we highlight the need not to isolate these actions but rather to enrich university studies through permanent programs that address the multiple dimensions of cybersecurity.

Conclusions

In this article we presented the results of a study that highlights the importance of cybersecurity awareness and training programs. It was found that the knowledge of the students of the first semesters of a professional career in computer science could be increased for their own benefit, and it was observed that a training event had a positive effect on the participants.

We conclude that the implementation of a permanent program with the objectives of training and raising awareness among university students about computer security issues would be beneficial to create safer communities with more protected users and with greater awareness of their actions.

REFERENCES

Anderson, Sweeney y Williams (2011). *Estadística para negocios y economía*. México, México: Cengage Learning.

Aston, G. (2016). Who is phishing for your data? *Trustee*, 69 (2), 8-11.

Case, C. J. and King, D. L. (2013). Cyber Security: A Longitudinal Examination of Undergraduate Behavior and Perceptions. *American Society of Business Behavioral Sciences eJournal*, 9 (1), 21-29.

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, 20 (3), 701-715.

Forouzan, B. A. (2003). *Introducción a la ciencia de la computación.* México: Thomson.

Jenab, K. and Moslehpour, S. (2016). Cyber Security Management: A Review. *Business Management Dynamics*, 5 (11), 16-39.

Kiani, M. (2016). Internet Security Feeling of Students. Study of Payame Noor University. *Trakia Journal of Sciences*, 14 (3), 230-235.

Magazine, A. (2009). Unveiling the misterious world of an ethical hacker. *SiliconIndia*, 36-37.

Miguel-Pérez, J. C. (2015). *Protección de datos y seguridad de la información.* México: Ra-Ma.

North, J. and Pascoe, R. (2016). Cyber security and resilence - it's all about governance. *Governance Directions*, 68 (3), 146-151.

Peltier, T. R. (2002). *Information Security, Policies, Procedures and Standards: Guidelines for Effective Information Security Management.* USA: CRC Press LLC.

Peterson, A. (2017). One negligent employee: Ensure security training raises employees' awareness of threats. *Credit Union Magazine*, 10.

Rhodes-Ousley, M. (2013). *Information Security - The Complete Reference.* USA: McGraw-Hill.

Stanciu, V. and Tinca, A. (2016). Students' awareness on information security between own perception and reality - an empirical study. *Accounting and Management Information Systems*, 15 (1), 112-130.

Stier, K. (2015). Data backup in the age of the cloud. *University Business*, 49-51.

Wagner, W. (2014). *Using IBM SPSS Statistics for Research Methods and Social Science Statistics.* USA: SAGE Publications.

Whitty, M., Doodson, J., Creese, S. and Hodges, D. (2015). Individual Differences un Cyber Security Behaviors: An Examination of Who is Sharing Passwords. *CyberPsychology, Behavior, and Social Networking*, 18 (1), 3-7.

Wiseman, C. (2017). Accounting Firm Cybersecurity: Training Your Staff and Protecting Your Business. *CPA Practice Advisor*, 27.

Zikmund, W., Barry, B., Carr, J. and Griffin, M. (2013). *Business Research Methods.* Mason, Ohio, USA: Cengage Learning.

* Ramón Ventura Roque Hernández (Autonomous University of Tamaulipas, Mexico) is an engineer in Computer Systems, a Master of Science in Electronic Engineering, a Doctor of Telematics Engineering and a Doctor of Education. He is currently a research professor at the Universidad Autónoma de Tamaulipas, Mexico. His research interests include software engineering, applied computing and educational technology.
** Carlos Manuel Juárez Ibarra (Autonomous University of Tamaulipas, Mexico) has a degree in Computer Science and a Master in Academic Communication. He is currently a professor at the Universidad Autónoma de Tamaulipas, Mexico, and a professional website developer. His research interests include computer security, educational technology and software development.