Migliorare le conoscenze, l'atteggiamento e le pratiche anti-phishing degli infermieri attraverso un intervento educativo e un serious game

Enhancing nurses' anti-phishing knowledge, attitude, and practices through an educational intervention and serious game

Andriana Magdalinou, Athena Kalokairinou, Flora Malamateniou, John Mantas

Department of Nursing, National and Kapodistrian University of Athens, Athens, Greece

Riassunto

Introduzione: le opportunità di E-learning possono migliorare le competenze digitali degli operatori sanitari. Più precisamente, la formazione anti-phising può supportare gli infermieri quando si imbattono in contenuti dannosi su Internet. Questo articolo presenta l'impatto di un intervento educativo potenziato da un serious game sulle conoscenze, gli atteggiamenti e le pratiche degli infermieri riguardo all'uso di Internet.

Materiali e Metodi: questo studio si è basato su un disegno a doppio pre-test ed è la seconda parte di una tesi di dottorato basata su un progetto che valuta le pratiche di Infosec degli infermieri che lavorano in sette ospedali della prima e della seconda regione sanitaria in Grecia. Agli infermieri interessati a partecipare a questa seconda fase del progetto è stato fornito un link per accedere al materiale e al questionario. Il campione di convenienza è stato suddiviso in quattro sottogruppi, di cui solo un gruppo è stato esposto alla formazione anti-phising. Tutti i partecipanti hanno completato lo strumento HAIS Q e la KAP è stata stimata con PSPP 1.6.2. Sono state eseguite statistiche descrittive e ANOVA a una via. L'analisi post hoc di Tuckey è stata condotta per determinare le differenze tra i gruppi.

Risultati: è stato utilizzato un campione di 124 infermieri. I partecipanti che hanno preso parte all'intervento educativo hanno ottenuto risultati migliori nelle voci Conoscenze e Pratiche. La loro consapevolezza totale è stata valutata più alta rispetto a quella dei loro coetanei che non sono stati esposti all'intervento. Non è stata riscontrata alcuna differenza significativa nell'atteggiamento verso l'uso di Internet.

Conclusioni: un intervento educativo multimodale è stato erogato e ha influenzato positivamente le conoscenze, le pratiche e la consapevolezza generale degli infermieri sull'uso di Internet. Tuttavia, i ricercatori sottolineano che la presente versione dell'intervento educativo era uno studio pilota e che potrebbero essere condotte ulteriori ricerche.

Parole chiave: E-learning; valutazione; anti-phising; serious game.

Abstract

Introduction: E-learning opportunities can improve healthcare professionals’ digital competencies. More precisely, the anti-phising training may support nurses when encountering malicious content on Internet. This paper presents the impact of an educational intervention enhanced by a serious game on the nurses’ Knowledge, Attitudes and Practices (KAP) regarding Internet usage.

Materials and Methods: this study was based on a double pre test design and is the second part of a PhD thesis based on a project that assess the Infosec practices of nurses who work in seven hospitals in the first and second Healthcare Region in Greece. Nurses who were interested in participating in this second phase of the project were given a link to access the material and the questionnaire. The convenience sample was divided into four sub groups out of which only one group was exposed to the anti phising training. All participants completed the HAIS Q tool and KAP was estimated in PSPP 1.6.2. Descriptive statistics and one-way ANOVA were performed. Tuckey post hoc analysis was conducted to determine differences among groups.

Results: the sample of 124 nurses was utilized. Participants that took part in the educational intervention performed better in Knowledge and Practices items. Their total awareness was rated higher than that of their peers who were not exposed to the intervention. There was no significant difference in Attitude towards Internet usage.

Conclusions: a multimodal educational intervention was delivered and positively affected nurses' Knowledge, Practices, and general Awareness on Internet usage. Nevertheless, the researchers highlight that the present version of the educational intervention was a pilot study and further research could be conducted.

Key words: E-learning; evaluation; anti-phising; serious game.

Correspondence: Andriana Magdalinou, Department of Nursing, National and Kapodistrian University of Athens, Papadiamantopoulou 123, Athens, Greece. Tel.: +30.210.7461499.

Introduction

A survey conducted in Greece revealed that the Internet usage is the most vulnerable security area in hospitals.[1] More precisely, nurses have average knowledge on Internet usage and apply average practices when accessing the Internet. Thus, the need for a self-regulated training that is designed to improve Knowledge, Attitude, Practices (KAP) aspects when accessing Internet and ameliorate phishing awareness is urgent.[2] A study of healthcare professionals' Infosec practices in organizations in the Mediterranean region supported that educational interventions could mitigate cyber-attacks and such interventions should become a priority in organizations, especially in cases that limited resources and funding restrains could make the installation of upgraded software and hardware impossible.[3]

Educational initiatives

E-learning can be perceived as an inspirational way of learning which may result in enhancing knowledge background,[4] improving skills and competencies, and encouraging active learning and participation.[5] A considerable number of interactive educational applications can be found in literature utilizing multimodal content and tools such as text, graphics, comics, games or videos.[6] A plethora of educational interventions are dedicated to train users about the Internet usage and phishing phenomena. It is considered that interactive games can be an effective way to educate users in avoiding cyber-attacks and support users in dealing with phishing incidences.[7] Phishing as a common attack technique that can be encountered in web sites or emails is based on social engineering and attempts to extract personal information from Internet users.[8,9] Users should be aware of phising and be cautious about its complications when accessing the Internet. According to a survey, participants achieved higher mean scores when detecting anti-phising scams and reported increased level of confidence.[10] Another study revealed that multimodal interactive trainings are more helpful than traditional ones.[11] Similar interventions showed that participants who were trained on an anti-phising serious game demonstrated significant performance and were able to recognize malicious sites.[12] On the contrary, a study supports that educating users about phishing can only increase the user's suspicion and fear.[13]

Aim

The aim of this study is to evaluate the impact of an anti-phishing educational intervention enriched with a serious game on the mean scores of the nurses' Knowledge, Attitudes and Practices when dealing accessing the Internet.

Materials and Methods

A Double Pre-test Design was envisioned and applied as a variation of the Quasi Experimental One Group Pre-Test/Post-Test Design methodology. This design demonstrates improved validity according to Knapp.[14] Two groups were formed, intervention group A and control group B, and each group was divided into two sub-groups. There were four sub-groups in total. Each of the intervention and control groups was given the questionnaire to complete (Pre-Test). Sub-group A2 continued with the intervention and completed the questionnaire after exposure (Post-Test), while control sub-group B2 completed the questionnaire (Post-Test) without being exposed to the intervention. The educational intervention was carried out online and participants could access Moodle platform to complete the training. The estimated time for completion was 30-40 minutes. Participants were required to be nurses working in the first and the second Healthcare Region in Greece AND use Internet regularly during their shift. Exclusion criteria were nurses working in other sectors and the limited use of Internet in order to perform their duties.

Hypothesis

The first hypothesis we intended to test was that the mean score of nurses' responses who received training in Internet usage Knowledge should be better that the responses given by nurses who were not exposed to the educational intervention, while the second hypothesis was that the mean score of nurses' responses who received training in Internet usage Attitude should be better that the responses given by nurses who were not exposed to the educational intervention. The third hypothesis was that the mean score of nurses' responses who received training in Internet usage Practices should be better that the responses given by nurses who were not exposed to the educational intervention. Finally, the fourth hypothesis was that the educational intervention should have improved participants' Internet usage Awareness compared to those who were not exposed to the educational intervention.

Tools

To estimate the effect of the educational intervention on the participants' responses, the HAIS-Q questionnaire was used. The researchers who developed it originally were informed and consented to its use.[15] From the HAIS-Q questionnaire, the category that refers to the use of the internet was extracted which was consisted of 9 items on a Likert scale from 1-5 (1 - Strongly disagree, 2 - Disagree, 3 - Neither Agree nor Disagree, 4 - Agree, 5 - Strongly Agree) concerning the Knowledge, Attitude and Practices of the respondents regarding the Internet usage.

Sample

This study is the second phase of a PhD thesis based on a project that estimate the Infosec practices of nurses who work in seven hospitals in the first and second Healthcare Region in Greece. Nurses who were interested in participating in this phase of the project were given a link to access the material on Moodle and fill in the questionnaire on Google Forms. This study was based on a double pre-test design thus the convenience sample was divided into four sub-groups out of which only one group was exposed to the anti-phishing training. The sample was divided into group A and control group B. Then, each group was sub divided into two sub-groups. Sub-group A1 (30 people) and B1 (32 people) completed the questionnaire. Sub-group A2 (29 people) completed the educational intervention and completed the questionnaire afterwards while control sub-group B2 (33 people) completed the questionnaire without being exposed to the intervention. The subgroups were divided and defined as shown in Figure 1.

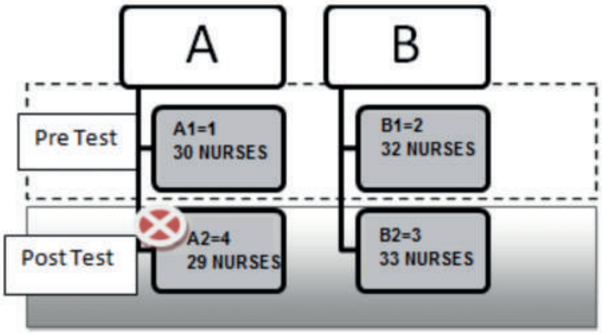

Figure 1. Division of sub-groups.

Analysis

To identify the reliability of the tool, the Cronbach's alpha coefficient was determined and received a value above 0.7. Thus, the tool was considered reliable and was administered to the participants. After the questionnaires being completed, all questionnaires were monitored for correct completion and the answers and were stored to an Excel spreadsheet. For the correct statistical analysis, some sentences were reversed so that all sentences are worded negatively. Therefore, an answer close to 1 is considered optimal. Pearson's correlation, Chi square, descriptive statistics and one-way ANOVA were performed. Tuckey post hoc analysis was conducted to determine which groups showed a difference in mean responses.

Ethics and confidentiality issues

The selected nurses were informed about the topic of the research, the institution that coordinated the research and the researchers that designed and performed the study. They were also notified about their right to participate voluntarily and their right to withdraw any time. Anonymity of the participants was maintained, and the collected data was used for research purposes only. This study is part of a PhD candidature project and is accepted and coordinated by the department of Nursing in the National and Kapodistrian University. The Research Boards of seven hospitals in the first and the second Healthcare Region accepted the research proposal and facilitated the conduct of the PhD thesis.

Results

The sample consisted of 124 nurses was composed by 85.5% women and 14.5% men. The age of the participants was recorded for all sub-groups. The 9.7% of the respondents were aged between 18 and 28 whilst 29% were in the age group between 29 and 39. A percentage of 35.5% was between 40 and 50 and 23.4% between 51 and 61. A minority of 2.4% was over 61 years old. The duration of their employment in the same organization was estimated as following: 12.9% was employed less than one year, 9.7% from 1 to 5 years, 23.4% from 6 to 10 years, 21% from 11 to 15 years, and 33.1% have been employed for more than 15 years. The percentage of the participants who have been notified about Infosec issues was calculated and was polarized into 53.2% who had not been notified and 46.8% who had been notified for related issues.

First of all, the initial step of the analysis was to examine whether the sub-groups differed significantly in age, gender, length of employment and Information Security notifications received from other sources. For this task, Chi square was performed, and Pearson Chi square was estimated. It was deducted that there is no statistically significant difference between the sub-groups (Gender: CI=95%, p=0.993>0.05, Age: CI=95%, p=0.352>0.05, Duration of employment: CI=95%, p=0.515>0.05, Notifications received: CI=95%, p=0.635>0.05).

The mean, standard deviation, maximum and minimum of the Knowledge, Attitude, and Practices (KAP) constructs and total Awareness of the participants in the area of Internet usage were recorded for all sub-groups as per Table 1. Results showed that all groups demonstrated average KAP and Awareness.

The Table 2 shows that the mean score of the responses in each area under study (Awareness on Internet usage, Knowledge on Internet usage, Attitude towards Internet usage and Internet usage Practices) by sub-group. The results demonstrate that sub-group 4 gave good responses (Knowledge = 2.15 ± 0.40, Attitude = 2.37 ±

Table 1. Descriptive statistics: knowledge, attitude, practice and awareness.

Item	N	Mean	St. Dev.	Min	Max
Knowledge	124	2.89	0.82	1.33	5.00
Attitude	124	2.55	0.68	1.00	4.33
Practices	124	2.77	0.82	1.33	5.00
Awareness	124	2.74	0.64	1.56	4.44

Table 2. Mean of responses in each area of interest.

Item	Group	Mean	St. Dev.	St. Err.	95% CI of mean (Lower upper)
Knowledge	1	2.89	0.53	0.10	2.69/3.09
	2	3.24	0.91	0.16	2.91/3.57
	3	3.21	0.79	0.14	2.93/3.49
	4	2.15	0.40	0.08	2.00/2.30
	Total	2.89	0.82	0.07	2.75/3.04
Attitude	1	2.48	0.55	0.10	2.27/2.68
	2	2.64	0.90	0.16	2.31/2.96
	3	2.68	0.54	0.09	2.48/2.87
	4	2.37	0.63	0.12	2.13/2.61
	Total	2.55	0.68	0.06	2.43/2.67
Practices	1	2.62	0.57	0.10	2.41/2.84
	2	3.04	0.94	0.17	2.70/3.38
	3	2.98	0.65	0.11	2.75/3.21
	4	2.40	0.91	0.17	2.06/2.75
	Total	2.77	0.82	0.07	2.63/2.92
Awareness	1	2.66	0.41	0.07	2.51/2.82
	2	2.97	0.85	0.15	2.67/3.28
	3	2.96	0.48	0.08	2.78/3.13
	4	2.31	0.47	0.09	2.13/2.49
	Total	2.74	0.64	0.06	2.62/2.85

Table 3. ANOVA Comparison of knowledge, attitude, practices and awareness regarding safe internet use in sub-groups.

Item	Sum Sq Total	Mean Sq.	F	Sig.
Knowledge	81.90	7.75/0.49	15.85	0.000
Attitude	56.07	0.63/0.45	1.39	0.250
Practices	82.12	2.80/0.61	4.55	0.005
Awareness	49.76	2.97/0.34	8.71	0.000

0.63, Practices = 2.40 ± 0.91). To investigate whether the sub-groups differed significantly in the mean of the responses regarding Knowledge, Attitude, Practices and Awareness on the safe use of the Internet, ANOVA was performed as shown in Table 3. It was inferred that there is no statistically significant difference between sub-groups in the Attitude of participants towards the safe use of the Internet. However, there is a statistically significant difference between at least two sub-groups regarding the Knowledge (CI=95%, $p=0.000<0.05$), the Practices (CI=95%, $p=0.005<0.05$), and the Awareness on the safe use of the Internet (CI=95%, $p=0.000<0.05$).

To determine exactly which sub-groups show a statistically significant difference in the mean scores in the areas of interest and to what extent the mean scores differ, Tuckey post hoc analysis was performed. Below are the results of Tuckey Multiple Comparison test comparing the sub-groups regarding the nurses' Awareness, Knowledge and Practices on safe Internet usage. Attitude was omitted as there was no statistically significant result.
Knowledge: Groups 1 and 4: CI=95%, $p=0.01<0.05$, Groups 2 and 4: CI=95%, $p=0.000<0.05$, Groups 3 and 4: CI=95%, $p=0.000<0.05$.
Practices: Groups 2 and 4: CI=95%, $p=0.10<0.05$, Groups 3 and 4: CI=95%, $p=0.023<0.05$.
Awareness: Groups 2 and 4: CI=95%, $p=0.000<0.05$, Groups 3 and 4: CI=95%, $p=0.000<0.05$.

Discussion

The findings suggest a statistically significant difference in Knowledge on Internet usage between sub-groups 1 and 2, 1 and 3 and 1 and 4, and in Internet security Practices between sub groups 2 and 4 and 3 and 4. Nevertheless, there was no significant difference in the sub groups' responses related to the Attitude towards the safe Internet usage. The evidence highlighted that the educational intervention improved the mean of the responses regarding nursing staff's Attitude towards the safe Internet usage, but according to Statisticians the available data may be not sufficient to draw a clear conclusion about the effect of the training on the Attitude.[16] Additional factors such as self-efficacy or organizational climate could be taken into account when developing educational interventions to improve the Attitude towards safe Internet usage.[17-20]

Conclusions

A comprehensive anti-phising training enriched with an educational game was developed and its effect on participants' responses was analyzed. The evidence support that the training positively affected nurses' knowledge, practices, and general awareness on safe Internet usage. The researchers point out that a future version of the educational intervention could focus on improving aspects that influence Attitude towards the safe Internet usage.

References

1. Magdalinou A, Kalokairinou A, Malamateniou F, Mantas J. Assessing Internal Consistency of HAIS-Q: A Survey Conducted in Greek Hospitals. Stud Health Technol Inform 2022;295:24-7.
2. Chaudhary S, Gkioulos V, Katsikas S. Developing metrics to assess the effectiveness of cybersecurity awareness program. J Cybersec. 2022;8:tyac006.
3. Georgiadou A, Michalitsi-Psarrou A, Gioulekas F, et al. Hospitals' Cybersecurity Culture during the COVID-19 Crisis. Healthcare 2021;9(10):1335. Doi: 10.3390/healthcare9101335.
4. Kim SY, Kim SJ, Lee SH. Effects of online learning on nursing students in South Korea during COVID-19. Int J Environ Res Public Health 2021;18:8506.
5. Chandross D, Decourcy E. Serious Games in online learning. Int J Innovat Online Educ 2018;2(3).
6. Argyri T, Zoulias E, Liaskos J, Mantas J. Use of Scratch as ICT educational tool in Health. Studies Health Technol Informat 2022:341-344.
7. Kumaraguru P. PhishGuru: A system for educating users about semantic attacks. Carnegie Mellon University, Pittsburgh PA. 2009.
8. Sheng S, Magnien B, Kumaguru P, et al. Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In: Usable Privacy and Security SOUPS 2007, Pennsylvania, USA. 2007.
9. National Cyber Security Authority 2020-2025. Accessed on 6/3/2023. Available from: https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf
10. Arachchilage N, Love S, Maple C. Can a mobile game teach computer users to thwart phishing attacks? Int J Infonomics 2013:720-730.
11. Jampen D, Gur G, Sutter T, Tellenbach B. Don't click: towards an effective anti-phishing training. A comparative literature review. Hum Cent Comput Inf Sci 2020:1-41.
12. Sumner A, Yuan X, Anwar M, McBride M. Examining factors impacting the effectiveness of anti-phishing trainings. J Computer Informat Systems 2021:1-23.
13. Anandpara V, Dingman A, Jakobsson M, et al. Phishing IQ tests measure fear, not ability. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg; 2007:362-366.
14. Knapp T. Why is the one-group pretest–post test design still used? Clin Nurs Res 2016;25:467–472.
15. Parsons K, McCormac A, Butavicius M, et al. Determining employee awareness using the human aspects of information

security questionnaire (HAIS-Q). Computers Security 2014;42:165-76.
16. Lane D, Scott D, Hebl M, et al. Introduction to statistics. Lane D. (Ed). Online Edition.
17. Ajzen I, Fishbein M. The influence of attitudes on behavior. The handbook of attitudes. Albarracín D, Johnson BT, Zanna MP (Eds). Mahwah, NJ: Lawrence Erlbaum Associates; 2005:173-221.
18. Chan M, Woon I, Kankanhalli A. Perceptions of information security at the workplace: linking information security climate to compliant behavior. J Informat Privacy Security 2005;1:28-41.
19. Zainal N, Puad M, Sani N. Moderating effect of self-efficacy in the relationship between knowledge, attitude and environment behavior of cybersecurity awareness. Asian Soc Sci 2022;8:55-64.
20. Fabrigar LR, MacDonald TK, Wegener DT. Structure of Attitudes from: The Handbook of Attitudes, Routledge. 2005.

Conflicts of interest: the Authors declare no conflict of interest.

Ethics approval and consent to participate: this project is part of a PhD thesis which is approved by the scientific and ethical board of the National and Kapodistrian University of Athens, the department of Nursing (Regulation 3685/2008, ID 153, 27/9/2017)

Informed consent: not applicable.

Patient consent for publication: not applicable.

Availability of data and materials: all data generated or analyzed during this study are included in this published article.

Acknowledgments: the authors would like to acknowledge the nursing staff who participated in this study.

Received for publication: 15 March 2023. Accepted for publication: 27 April 2023.

Licensee PAGEPress, Italy (on behalf of ANIARTI, Italy).
Scenario 2023; 39:540
doi:10.4081/scenario.2023.540

Publisher's note: all claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article or claim that may be made by its manufacturer is not guaranteed or endorsed by the publisher.