ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 12(44), DOI: 10.17485/ijst/2019/v12i44/147850, November 2019*

Anti-Phishing Game Framework to Educate Arabic Users: Avoidance of URLs Phishing Attacks

Ahmed Baiomy[1], Mahmoud Mostafa[1,2]* and Alyaa Youssif[1,3]

[1]Information Systems Department, Faculty of Computers and Information, Helwan University, Helwan, Egypt; ahmed_baiomy@hotmail.com
[2]Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya, Saudi Arabia; mahmoud.mostafa.m@gmail.com
[3]College of computers and information Technology, Arab Academy for Science, Technology and Maritime Transport AASTMT, Cairo, Egypt; aliaay@yahoo.com

Abstract

Objectives: The main objective of this study is to address poor security awareness regarding phishing attack in Middle East by developing anti-phishing educational game to educate Arabic users about phishing URLs. **Methods/statistical analysis:** We start by identifying phishing site URL attributes that help identify phishing sites. Then, we followed a well-established game design framework (EDPE) to develop our anti-phishing game. We performed a study on 56 participants using pre-test and post-test technique to assess the level of phishing awareness among participants before playing the game and after playing the game. We used paired *t*-test and one-way analysis of variance (ANOVA) statistical analysis to identify to what extent anti-phishing game could help users identify and avoid phishing attacks. **Findings:** The results obtained from pre-test proved the clam that security awareness in Arabic region is still immature. While the results obtained from post-test prove that serious educational games in Arabic language could be used to educate Arabic users about security concepts and increase security awareness. In addition, the results reflect that employees need more training (as their performance were the lowest among different demographic participants) to help them correctly identify phishing sites. Moreover, by inspecting participants' responses, we identified that similar and deceptive domains, is the hardest URL phishing category to be correctly identified by users. So, we should pay more attention to this category while performing users training. **Application/improvements:** Our anti-phishing game is the first security educational game in Arabic language. It proves the effectiveness of serious games as a training tool. It is a step towards raising security awareness in Arabic region.

Keywords: Anti-Phishing, Attack, Arabic, Game, Framework

1. Introduction

Phishing is a serious kind of attack that targets many sectors such as financial, retail, cloud computing, and payment systems.[1] In this attack, hackers use social engineering technology and spoofing techniques to deceive users to visit a fake website that similarly appears as a legitimate one. The goal of the hacker is to steal user credential and sensitive data such as user name, password, and credit card data. Previously, hackers used e-mail as a method to disseminate their phishing URLs. While currently, the widespread use of social media networks such as Facebook, Twitter, and Myspace, accompanied with their huge number of users, force hackers to use them as vehicles to spread their phishing URLs.[2]

According to Qabajeh,[3] "phishing" has been defined as "a type of computer attack that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker's benefit". While this definition is general to include all types of phishing our focus here is on fake website phishing. Phishing harms world economy and causes financial loss.[1] To mitigate this kind of attack, many research efforts have been done to detect phishing URLs. But, the proposed solutions have their own limitations.[3]

*Author for correspondence

Some researchers believe that educating end users to detect phishing sites is an effective solution.[4] Some companies such as Symantec and Microsoft provide training materials to educate users about phishing. However, learning how to detect phishing sites through traditional text based materials or tutorials is not effective. Users need more attractive, interactive and entertaining method for education. Moreover, they need to test their gained knowledge in a safe way. To provide such solution some researchers developed educational games.[5,6] Unfortunately, most of these educational materials and games were developed in English language. This puts obstacles for non-English speakers to benefit from these recourses, especially in the Arabic and Middle East region, where security awareness is not mature enough. Aboul-Enein[7] raised the issue of poor security awareness in Middle East. He confirmed that education and awareness are integral to combat cyber threats. In order to raise security awareness in Arabic and Middle East region, we need to develop security training materials and educational games in Arabic language. In this article, we present anti-phishing educational game in Arabic language for the benefits of Arabic users. Figure 1 presents a screenshot of our anti-phishing game website. The Game is publically available for free at: http://antiphishinggame.com. It is the first Arabic website to provide security educational games in Arabic language. Moreover, the website contains additional teaching materials and tutorials in Arabic language. It is a step towards raising security awareness in Arabic region.

The remainder of this article is organised as follows: related work is introduced in Section 2. Section 3 presents game design framework. Then, section 4 gives details of used evaluation methodology. Obtained results are discussed in Section 5. Then, Section 6 presents the originality and limitations of the study. Finally, Section 7 draws up our conclusions and future work.

Figure 1. Screenshot of anti-phishing game website.

2. Literature Survey

Video games are "interactive play that teaches us goals, rules, adaptation, problem solving, interaction, all represented as a story. They give us the fundamental needs of learning by providing – enjoyment, passionate involvement, structure, motivation, ego gratification, adrenaline, creativity, social interaction, and emotion.[8] All these features of video games force researchers to use them for training and educational purposes. The term serious games appeared to describe the use of video games for purposes rather than entertainment.[9] Other terms such as educational games, gamification, and game-based learning are used to refer to the use of video game for educational purposes. Many serious games have been developed to educate users about security concepts and practices. Cyber Protect is the first security educational game appeared in the literature.[10] Cyber CIEGE is the most popular cyber security game.[11] It was the focus of many research studies. However, our focus here is on anti-phishing games. In Ref.[5] from Carnegie Melon University developed Anti-Phishing Phil game. The purpose of the game is to provide a training tool to educate users about phishing attacks. The game takes place in the Interweb Bay. A little phish named Phil lives there, with his father. There are a lot of worms in the bay where some are normal worms and the others are fake worms used by phishes to trick fishes. Each worm is associated with an URL. The father gives advices to Phil to educate him how to differentiate between benign and phishing worms. When Phil comes near to the worm, the URL appears and he must take a decision either to eat the worm if he finds that the associated URL is benign or reject the worm if he identifies that the URL is phishing one. Taking the right decision results in an increased score while the wrong decision reduces player's life.

They performed a user study to evaluate the effectiveness of Anti-Phishing video game compared to other teaching materials such as reading anti-phishing tutorial or reading existing text based online training materials. The obtained results reflected the effectiveness of Anti-Phishing game as a teaching tool. However, the concern is that they used a small sample in their study. In Ref.,[6] Arachchilage and

Love developed the game for Mobile devices and evaluated its effectiveness. In addition, the obtained results prove that Anti-Phishing game plays a significant role in training users how to detect and avoid phishing attacks.

We followed the same approach of.[5] However, we developed our game in Arabic language, because, our focus is on Arabic users. Moreover, we developed a different game story and followed a well-established game design framework. In addition, we used large sample size in our user study to be statically significant. We decided to develop web-based game to reach large number of audiences. The website is accessible from any kind of computing devices, including smart phones and personal computers.

3. Game Design Framework

Many researches have been conducted to identify the most suitable way of designing serious games.[12] In order to develop our game, we have chosen Extended Design, Play, and Experience (EDPE) Framework.[13] As presented in Figure 2, EDPE framework consists of three iterative phases. It presents a process to effectively design learning games; it includes a methodology to analyse the design by playing the game and to assess the effect on preset user experience goals. A feedback is given to enhance the design in an iterative manner. EDPE has four layers: learning, storytelling, game play, and user experience. These layers influence each other. In the following subsections, we describe these layers.

3.1. Learning Layer

In this layer, we set the learning objectives and identify the contents. According to the learning sciences theory,[14]

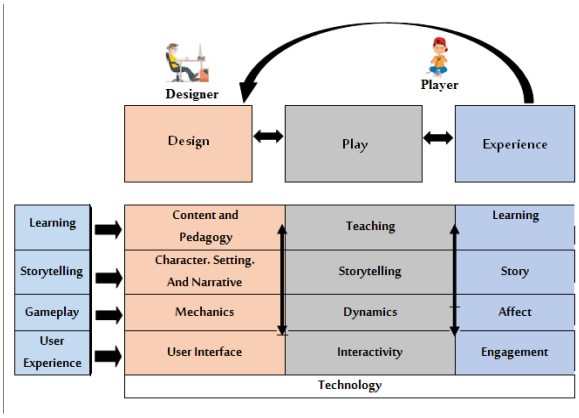

Figure 2. Extended design, play, and experience (EDPE) framework.[13]

educational game should be goal oriented. Our game consists of four levels and each level focuses on certain type of phishing URL. The goal is to increase user awareness regarding phishing attack. According to Ref.,[15] the user interface is the right place to solve phishing. A well-trained user can inspect websites URLs – in browser's address bar – using their naked eyes and identify phishing one. To provide the appropriate training material, we inspected phishing URLs attributes and identified three main categories of phishing URLs.

3.1.1. Group (A): Using IP Address Instead of Domain Name

If an IP address is used instead of domain name in the URL, such as **"http://125.98.3.123/fake.html"**, users can be sure that, this is a phishing website.[16] In addition, sometimes, phishers write URL in hexadecimal format like http://0x58.0xCC.0xCA.0x62/2/ fake.eg/index.html to deceive their victims.

3.1.2. Group (B): Sub Domain Phishing

In this phishing technique, scammers write the real domain first followed by phishing domain.[17] For example, "www.helwan.edu.eg" is a real domain and "hacker.com" is a phishing domain. To deceive users, scammers concatenate the two domains putting the real domain first to appear as real domain while it became a subdomain in phishing URL. The resulting URL becomes "www.helwan.edu.eg.hacker.com". Clearly, this URL will lead users to phishing site. The right most domains in the URL is the top level domain. So, the user should inspect URL from right to left searching for the real domain. The real domain is the one just precedes the last dot in the URL. To make URL hard to be detected, scammers use long URLs – hoping you will lose the will to bother looking for the dots. To make URL longer they put sub directories using "/" or use long query string.

3.1.3. Group (C): Similar and Deceptive Domains

This group contains all deceptive techniques:

3.1.3.1. URL's having "@" Symbol

Using "@" symbol in the URL leads the browser to ignore everything preceding the "@" symbol and the phishing address follows the "@" symbol.[16]

3.1.3.2. *Redirecting using "//"*

The existence of "//" within the URL path means that the user will be redirected to another website. An example of such URL's is: **"http://www.legitimate.com//http://www.phishing.com"**. User should examine the location where the "//" appears.[17]

3.1.3.3. *Adding Prefix or Suffix Separated by (-) to the Domain*

The dash symbol is rarely used in legitimate URLs. Phishers tend to add prefixes or suffixes separated by (-) to the domain name so that users feel that they are dealing with a legitimate webpage.[18] For example, "http://www.nbe-eg.com/" is phishing URL.

3.1.3.4. *Deliberated Typing Mistakes*

In this phishing URL, phishers deliberately write domain names with typo mistakes to make it looks like legitimate one. The authors in Ref.[19] identified possible typo-generation models used for typo squatting. These deliberated typo mistakes include the following: missing-dot typos, character-omission typos, character-permutation typos, character-substitution typos, and character-duplication typos.

Users will learn the above phishing concepts and techniques during game play. This definitely will affect their experiences and increase their awareness regarding phishing attack.

3.2. Storytelling Layer (Anti-Phishing Game)

Here, we describe the story of the game. In our game, we use the analogy of mines. This gives the player the feelings of the real danger as trusting phishing URL may result in catastrophic consequences like stepping on mines. As depicted in Figure 3, we have two main characters: the soldier (game hero) and the commander. The role of the commander is to give instructions to the soldier to let him know the details of the required mission at the beginning of each level. These instructions definitely include the knowledge that must be taught. The soldier's role is to apply the given instructions in each level to accomplish the required mission. This allows the player to practice the knowledge in an interactive way and learn from his both successful and failure trails while avoiding the bad consequences that might occur in real-life situations.[9]

Figure 3. Anti-phishing game main characters.

Our game consists of four levels. Each level takes place in a different environment. As shown in Figure 4, the first level takes place in a dessert Mines field. When the player becomes near to the mine a URL appears and he should determine if it is phishing or legitimate one. All URLs in this level belong to class (A) IP address phishing URLs.

In the second level, the soldier exists in a garage and must inspect cars and remove mines. This level focuses on phishing URLs of type (B) subdomain phishing URLs. Figure 5 presents a snap shot of level 2.

While in the third level, the soldier should go to train station and inspects train vehicles for mines. This level deals with category (c) which includes similar and deceptive phishing URLs. Figure 6 shows a snap shoot of level 3.

Finally, in the fourth level, which is the hardest level as shown in Figure 7, the player has to inspect parachutes and try to destroy parachute mine that bear phishing URL, in the sky before reaching the ground. While letting benign parachutes that bear legal URLs form landing

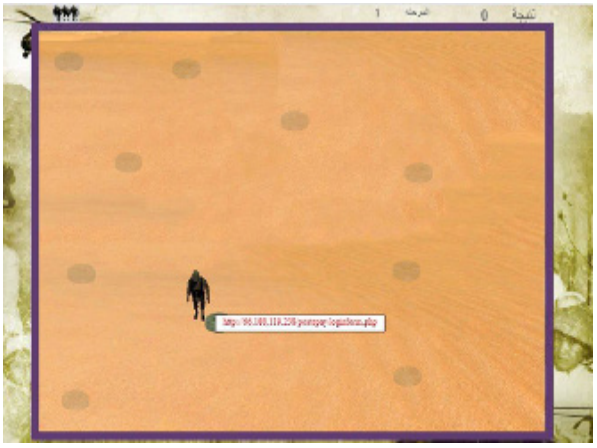

Figure 4. First level of anti-phishing game.

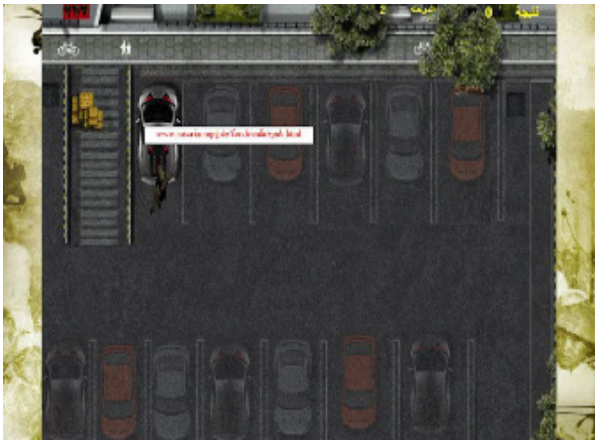

Figure 5. Second level of anti-phishing game.

Figure 6. Third level of anti-phishing game.

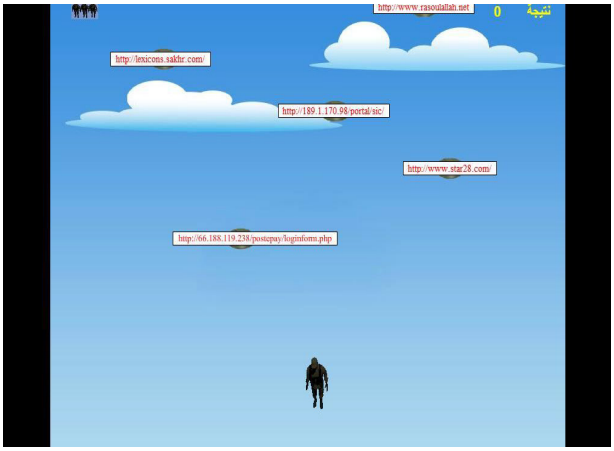

Figure 7. Fourth level of anti-phishing game.

safely. This level presents a mix of all previous phishing URLs techniques. Clearly, game levels start from easy to hard in order to increase user engagement and deliver learning contents in a progressive way.

3.3. Game-play Layer

This layer uses the original Mechanics, Dynamics, and Aesthetics (MDA) framework,[20] but they changed the word Aesthetics into Affect. Mechanics describe the rules governing the game and the goals that must be achieved. In this game, phishing URLs resample mines and the role of the player is to inspect (URL) to determine if it is a mine (phishing) or not. Correct identification will result on mine removal and increased score. The challenge is that, incorrect identification will result in mine explosion and loss of live. As depicted in Figure 8, at the beginning of each level there is an introductory screen presents rules governing the game and the goals that must be achieved. Feedback from users helped modify the design. In the initial development stages, members of our team played the role of users and tested the game to provide necessary feedback to enhance the design.

Dynamics is the resulting behavior produced by the player interacts with game. As shown in Figure 9, at the beginning of the game the allowed user actions are described. User can move right, left, up, and down using the arrow keys. In addition, he will press (K) key in the keyboard to accept benign URL and press the (B) key to destroy phishing URL. Moreover, in level 4, he could use E button to shot fire. We iteratively tested the game to fine tune movement speed and fire shooting speed and balancing the difficulty of each level.

Affects (Aesthetics) are resulting experiences, or emotions: disturbance because of loud explosion and sadness in case of misidentification, loss of life, and lost score. Happiness in the case of successful identification due to increased score, overcome challenge, and mission completeness.

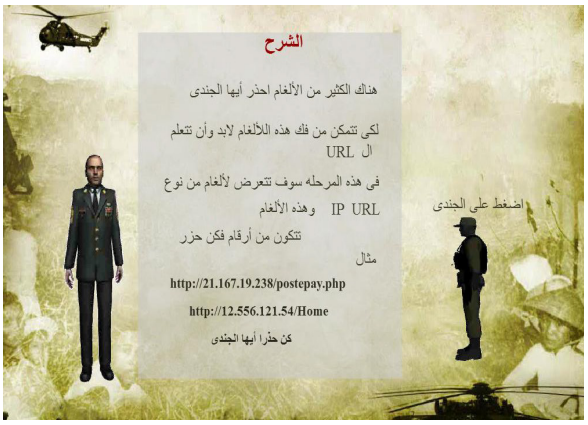

Figure 8. Mechanics for level one of anti-phishing game.

Figure 9. Anti-phishing game dynamics.

3.4. User Experience Layer

This layer focuses on user interface, interactivity, and engagement. Attractive and accessible game will increase user interaction with the game. Interactivity is one of the most important aspects of educational games. A well-designed game will result to user engagement which affects the learning process positively.

We tried to make our game attractive by adding high quality sound effects. Also, as a part of user experience we provide feedback to the user about his answers at the end of each level. Figure 10 depicts the feedback for level one.

As shown in Figure 11, at the beginning of the game, the user must have his/her login name and password. This is necessary for him/her to continue after the level that has been passed previously, and give him/her the opportunity to complete from where he/she has stopped. In addition, this helps us save each player profile for further analysis.

Figure 10. Feedback for level one.

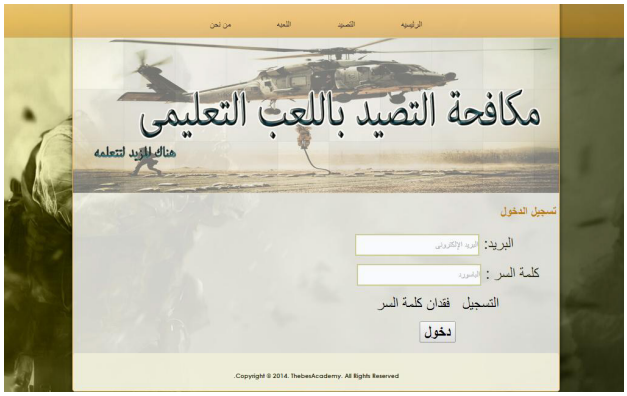

Figure 11. User log in page.

3.5. Used Technology

We used Adobe Flash and its Action script programming language. Our choice of Flash is due to its ability to produce high-performance games, console-quality games in 2D and 3D and to leverage the ubiquity of Flash Player and Adobe AIR that can reach the web, desktop, mobile, and TV audiences.[21]

Also, we used My SQL to develop a game database to store user profile, including obtained result for each level.[22]

4. Evaluation Methodology

In this part, we describe the methodology used to test the game for its effectiveness in training users.

4.1. Subjects Recruitment and Demographics

We published an announcement on Helwan university campus and used Facebook and Twitter social media sites to reach large audiences. We called for volunteers to participate in the study. We asked for participants from high schools, university undergraduates, postgraduates (age under 30) and employees (age over 30). We filtered volunteers to exclude those having Information Technology experience. We used the same technique used by the authors[23] for participants' selection. We decided that participants should be evenly demographically distributed. Table 1 shows participants and their demographics. We have a total of 56 participants equally distributed into 4 categories and each category has 7 males and 7 females. We thought that this distribution would give more unbiased representation of results.

Table 1. Show participant recruitment and demographics

	Number and percentage
Gender	
Male	28 (50%)
Female	28 (50%)
Education and age	
High school (15–18)	14 (25%)
College under grade (19–23)	14 (25%)
Post graduate (24–30)	14 (25%)
Employee (>30)	14 (25%)
Total	**56 (100%)**

4.2. Study Design

We designed two tests: pre-test and post-test. Each test contains twenty URLs; eight legitimates and twelve phishing sites. The fishing URLs were selected to represent all phishing groups (A, B, and C) described in section 3.1 above. We used four URLs for each group. Table 2 presents the used URLs for both pre-test and post-test. However, in real tests, URLs were randomly distributed. We refer to legitimates URLs by group D. We used well-known sites for Egyptians and Arabic Users.

4.3. Study Procedures

At the beginning, participants are given 15 minutes to solve pre-test by inspecting each URL and determine if it is phishing or legitimate sites. Moreover, for each URL, participant should tell us to what extent he was confident with his answer. Answers were based on a five-point Likert scale[24] ranging from 1 to 5, where 1 means strongly confident and 5 means strongly unconfident. After evaluation the twenty URLs, participants were given twenty minutes to play our anti-phishing game

Table 2. URLs used in pre-test and post-test

Group	URL for "pre-test"	URL for "post-test"	Phishing/legitimate
A	193.227.34.45/nbe.com	193.227.34.45/elwatannews.com/	Phishing
A	212.111.46.12/akhbarak.net/	212.11.64.16/banquemisr.com/ar	Phishing
A	132.122.12.134/youm7.com/	214.232.12.17/alexbank.com	Phishing
A	214.215.14.23/youth.gov.eg	214.26.34.32/moh.gov.eg/	Phishing
B	www.fifas.gega.com	ar.fifa.com.tam.com	Phishing
B	cu.edu.eg.camd.com	www.asu.edu.eg.140.bit	Phishing
B	www.cbe.org.eg.customer.srv	www.hsbc.com.eg.users.log	Phishing
B	twitter.com.login.lang.eg	www.facebook.com.gg.com	Phishing
C	www.helwan-un.edu.eg	www.nbe-com.eg	Phishing
C	www.almasrialyoum.com/	https://twiter.com	Phishing
C	https://ar.islamway.net//free.web	www.whyislam.org//greating.eg	Phishing
C	mail.google.com@myaccount.com	login.yahoo.com@secure.eg	Phishing
D	https://www.elwatannews.com/	www.nbe.com.eg/	Legitimate
D	www.banquemisr.com/ar	http://www.akhbarak.net/	Legitimate
D	www.yallakora.com	https://www.youm7.com/	Legitimate
D	www.eulc.edu.eg/	https://cu.edu.eg/	Legitimate
D	www.alexbank.com	www.helwan.edu.eg	Legitimate
D	www.moe.gov.eg	www.almasryalyoum.com/	Legitimate
D	https://www.facebook.com/	www.arabbank.com.eg/ar	Legitimate
D	www.moh.gov.eg/	www.eulc.edu.eg/	Legitimate

that educate them in four levels how to detect phishing site. After finishing game play, participants were asked to answer post-test in the same way as they did in the pre-test.

5. Results

In this section, we discuss the results obtained from a user study. Actually, the use of pre-test was for two purposes. First, to assess the level of phishing awareness among participants before playing the game. Second, to compare the results of the pre-test with post-test and identify to what extent anti-phishing game could help users identify and avoid phishing attack. Table 3 presents the obtained results classified by participants' demographics. The paired *t*-test analysis shows a significant increase in participants' performance from pre-test to post-test ($\mu1 = 6.9$, $\mu2 = 8.77$, $p = 0.01$). These results confirmed by one-way analysis of variance (ANOVA $F(1, 110) = 164.51$, $p < 0.01$). It is clear that users' awareness regarding phishing attack was low before playing anti-phishing game. This is evident by the obtained average score and average confidence. However, all participants did better in post-test. The average score increased. Also, their confidence regarding their answers significantly increased. These results reflect the effectiveness of anti-phishing game as a training tool.

The Spearman statistical analysis reflect that there is no correlation between participants post-test performance and gender (rho = 0.027, $n = 56$, p(2-tailed) = 0.84). However, there is a correlation between post-test performance and four education and demographic categories (rho = −0.28, $n = 56$, p(2-tailed) = 0.039). These results confirmed by one-way analysis of variance (ANOVA $F(3, 52) = 6.459$, $p < 0.001$). Postgraduates have the best results for both tests, followed by higher schools and undergraduate students successively and finally employees get least scores. This reflects that employees may need to spend more time playing anti-phishing game to raise their skills in correctly detecting phishing URLs.

Moreover, to identify which phishing group is most difficult to be detected by users, we measured percentage of correct answers (True Positives (TP) and True Negatives (TN)) and percentage of wrong answers (False Positives (FP) and False Negatives (FN)) for each group of tests' URLs.

Table 4 presents the obtained results. It is clear that users have no difficulty identifying normal URLs; however, in some limited cases, they may accidently identify benign URL as phishing.

Table 3. Tests results classified by participants' demographics

	Pre-test					Post-test				
	Minimum	**Maximum**	**Average**	**STDV**	**Average confidence**	**Minimum**	**Maximum**	**Average**	**STDV**	**Average confidence**
Gender										
Male	5.5	8.5	6.91	0.81	3.68	7.5	10.0	8.79	0.70	4.54
Female	5.0	8.5	6.89	0.90	3.63	7.0	10.0	8.75	0.69	4.51
Education and age										
High School (15–18)	6.0	8.0	7.00	0.71	3.76	8.5	9.5	9.07	0.47	4.63
College under grade (19–23)	5.5	7.5	6.57	0.65	3.79	7.5	9.5	8.57	0.65	4.46
Post graduate (24–30)	7.0	8.5	7.79	0.47	3.93	8.0	10.0	9.14	0.60	4.72
Employee (>30)	5.0	7.0	6.25	0.67	3.15	7.0	9.0	8.29	0.67	4.32

Table 4. Percentage of total correct answers and wrong answers for each URLs group

Test	Pre-test						Post-test					
Group	% Correct answers			% Wrong answers			% Correct answers			% Wrong answers		
	TP	TN	Total Correct	FP	FN	Total wrong	TP	TN	Total Correct	FP	FN	Total wrong
A	72.1	0	72.1	0	27.9	27.9	92.7	0	92.7	0	7.3	7.3
B	68.4	0	68.4	0	31.6	31.6	87.6	0	87.6	0	12.4	12.4
C	60.8	0	60.8	0	39.2	39.2	74.9	0	74.9	0	25.1	25.1
D	0	75.4	75.4	24.6	0	24.6	0	95.6	95.6	4.4	0	4.4

As shown in Figure 12, regarding phishing URLs for both pre-test and post-test, Group (C) similar and deceptive domains, was the hardest category to be correctly identified by participants. While Group (B) subdomain phishing has medium level of difficulty and Group (A) IP address phishing, was the easiest phishing type to be detected.

6. Originality and Limitations

The article presents the design, implementation, and evaluation of anti-phishing game to educate Arabic users about phishing attacks. It is the first security educational game in Arabic language. In addition, we identified phishing site URL attributes that help identify phishing sites and used them to build anti-phishing game. Moreover, we performed a study to assess the level of awareness regarding phishing attack in Egypt and Middle East. Furthermore, we trained 56 users using the developed anti-phishing game and evaluated the effectiveness of this approach. Finally, we identified that similar and deceptive domains (Group C) is the hardest category of URL phishing to be detected by users. Therefore, users need more practices to accurately, detect this phishing category. While the study used pre-test and post-test to assess the effectiveness of anti-phishing game as an instructional tool. It would be better if the game group performance was compared with a controlled group that uses traditional lessons and tutorials. This would help identifying, to what extent the presented anti-phishing game is more effective than traditional lessons and tutorials.

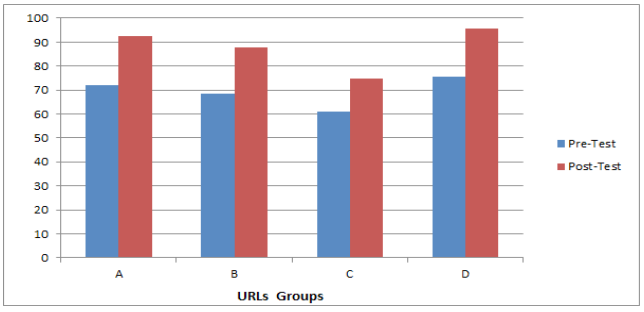

Figure 12. Percentage of correct answers for each group in pre-test and post-test.

7. Conclusions and Future Work

In this article, we addressed the problem of low security awareness regarding phishing attacking Egypt and Middle East. We developed anti-phishing game to educate Arabic users about phishing URLs. In order to reach this goal, we used a well-established framework to design and implement our game. Then we tested our implementation to assess its effectiveness as a training tool.

The results obtained from pre-test proved the clam that security awareness in Arabic region is still immature. While the results obtained from post-test prove that serious educational games in Arabic language could be used to educate Arabic users about security concepts and increase security awareness. As a future work, we will develop more serious games to raise Arabic users' awareness about other security areas such as social engineering and malwares.

References

1. APWG phishing activity trends report second quarter 2018. [cited 2019 Sep]. http://docs.apwg.org/reports/apwg_trends_report_q2_2018.pdf.
2. Phishing and countermeasures: understanding the increasing problem of electronic identity theft. [cited 2006 Dec]. https://www.wiley.com/en- us standing+th

e+Increasing+Problem+of+Electronic+Identity+Theft-p-9780471782452.
3. Qabajeh I, Thabtah F, Chiclana F. A recent review of conventional vs. automated cyber security anti-phishing techniques. Comput Sci Rev. 2018;29:44–55.
4. Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. [cited 2007 Jan]. https://www.researchgate.net/publication/221462241_Getting_users_to_pay_attention_to_anti-phishing_education_Evaluation_of_retention_and_transfer.
5. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. [cited 2007 Jan]. https://www.researchgate.net/publication/221166422_Anti-Phishing_Phil_The_design_and_evaluation_of_a_game_that_teaches_people_not_to_fall_for_phish.
6. Arachchilage NAG, Love S. A game design framework for avoiding phishing attacks. Comput Hum Behav. 2013;29(3):706–14.
7. Cybersecurity challenges in the Middle East. [cited 2017]. https://www.gcsp.ch/publications/cybersecurity-challenges-middle-east.
8. Serious games. [cited 1970]. https://books.google.co.in/books/about/Serious_games.html?id=J2NqAAAAMAAJ.
9. Le Compte A, Elizondo D, Watson T. A renewed approach to serious games for cyber security. In: 7th International conference on cyber conflict: architectures in cyberspace (CyCon); 2015. P. 203–16.
10. Twitchell D. Security Com: a multi-player game for researching and teaching information security teams. J Dig Forensics Sec Law. 2007;2:9–18.
11. Irvine CE, Thompson MF, Allen K. Cyber CIEGE: gaming for information assurance. Secur Priv Mag. 2005;3(3):61–64.
12. Amory A. Game object model version II: a theoretical framework for educational game development. Educ Technol Res Develop. 2007;55(1):51–77.
13. Winn B. The design, play, and experience framework. In: Handbook of research on effective electronic gaming in education; 2008. vol. 3:1010–24.
14. Engaging learning: designing e-learning simulation games. [cited 2005]. https://www.amazon.com/Engaging-Learning-Learning-Simulation-2005-05-13/dp/B01JXOR2KE.
15. Fighting phishing at the user interface. [cited 2006]. https://dl.acm.org/citation.cfm?id=1293151.
16. Mohammad RM, Thabtah F, McCluskey L. An assessment of features related to phishing websites using an automated technique. In: 2012 international conference for internet technology and secured transactions; 2012. P. 492–7.
17. Intelligent phishing URL detection using association rule mining. [cited 2016 Jul 10]. https://hcis-journal.springeropen.com/articles/10.1186/s13673-016-0064-3.
18. Ahmed AA, Abdullah NA. Real time detection of phishing websites. In: 2016 IEEE 7th annual information technology electronics and mobile communication conference (IEMCON); 2016. P. 1–6.
19. Spaulding J, Upadhyaya SJ, Mohaisen A. The landscape of domain name typosquatting: techniques and countermeasures. In: 11th international conference on availability, reliability and security (ARES); 2016. P. 284–9.
20. MDA: a formal approach to game design and game research. [cited 2004]. https://users.cs.northwestern.edu/~hunicke/MDA.pdf.
21. Reimers S, Stewart N. Adobe Flash as a medium for online experimentation: a test of reaction time measurement capabilities. Behav Res Meth. 2007;39:365–70.
22. New riders. [cited 1999]. http://www.peachpit.com/imprint/index.aspx?st=61074.
23. Protecting people from phishing: the design and evaluation of an embedded training email system. [cited 2017 Jan]. https://www.researchgate.net/publication/221518419_Protecting_people_from_phishing_The_design_and_evaluation_of_an_embedded_training_email_system.
24. Likert R. *A Technique for the measurement of attitudes. Arch Psychol. 1932;140:1–55.*