Teaching Phishing-Security: Which Way is Best?

Simon Stockhardt, Benjamin Reinheimer, Melanie Volkamer, Peter Mayer, Alexandra Kunz, Philipp Rack, Daniel Lehmann

Teaching Phishing-Security: Which Way is Best?

Simon Stockhardt, Benjamin Reinheimer, Melanie Volkamer, Peter Mayer,
Alexandra Kunz, Philipp Rack, and Daniel Lehmann

Technische Universität Darmstadt
firstname.lastname@secuso.org
https://secuso.org

Abstract. Ever more processes of our daily lives are shifting into the digital realm. Consequently, users face a variety of IT-security threats with possibly severe ramifications. It has been shown that technical measures alone are insufficient to counter all threats. For instance, it takes technical measures on average 32 hours before identifying and blocking phishing websites. Therefore, teaching users how to identify malicious websites is of utmost importance, if they are to be protected at all times. A number of ways to deliver the necessary knowledge to users exist. Among the most broadly used are instructor-based, computer-based and text-based training. We compare all three formats in the security context, or to be more precise in the context of anti-phishing training.

Keywords: IT-security training, user study, computer-based training, instructor-based training, text-based training, phishing

1 Introduction

As our daily lives increasingly shift into the digital world, the number and variety of security threats the average user faces on a daily basis increases as well. Technical measures are in place to mitigate these security threats, but they do not offer sufficient protection [17]. One example that demonstrates this insufficiency is phishing: it takes on average 32 hours until automated phishing detection identifies and blocks malicious websites. During that time frame users will remain unprotected if not taught how to protect themselves [11,21,16]. Security training is widely accepted as one of multiple components for achieving higher end-user IT-security [2]. Corresponding training approaches exist in different formats, all offering different advantages and disadvantages. Especially instructor-based training, computer-based training, and text-based training have been proposed for delivering all kinds of IT-security knowledge to average end-users [13,14,20].

Instructor-based training describes training situations in which an instructor teaches the participants. Due to the presence of the instructor, this situation allows for real-time feedback, questions and answers, as well as shifting the focus of the training to suit the learners' needs [8]. The term computer-based training describes training that is necessarily aided by technology (e.g. computers, tablets, smartphones). The learner can train individually at the most convenient times and can always stop learning to return at a later point in time. Like the instructor-based training it also allows for direct

feedback on the users performance. Text-based training is based on reading material (e.g. printouts, PDF, etc.). Analogously to computer-based training, text-based training offers self-paced, individualized learning of the content. However, due to the static nature of the format text-based training does not offer the possibility for individual feedback or other interactive elements. In its basic form it does not require an instructor or electronic devices (though some forms of text delivery, e.g. through PDFs or websites, obviously necessitate a respective device). While the formats have been compared in empirical evaluations, the existing literature lacks studies comparing all three formats in the phishing context, when delivering the same content with each format.

The goal of this work is to comparatively evaluate the three formats instructor-based training, computer-based training, and text-based training when delivering the same content through each format. For this purpose we conducted a user study researching the following aspects: (1) effectiveness of transferring the knowledge to the user, (2) user satisfaction, (3) confidence, and (4) efficiency of the training formats. Our results indicate that instructor-based training transfers knowledge significantly more effectively than any other format. Instructor-based training also achieves the highest scores in user satisfaction and confidence. Furthermore, text-based training is the most efficient format (time spent with this format leads to more correct answers in comparison to the same amount of time spent with any other format).

2 Training Material

For our evaluation we use the anti-phishing training NoPhish (secuso.org/nophish), as it exists in all three different delivery formats: instructor-based, computer-based and text-based training. Also NoPhish has previously undergone research delivered as computer-based and instructor-based training and has iteratively been improved [5,4].

2.1 NoPhish Content

The NoPhish training content is based on findings from different academic disciplines. Firstly it is based on learning principles [22] such as practice, effect, repetition and direct feedback in order to deliver an effective learning experience. Secondly it is based on a user-centered design [1].

The training is split into two parts: the *introductory part* and the *main part*. The introductory part of the training material contains general information about phishing. This includes possible consequences of phishing attacks to emphasize the risks. It is based on the fact, that the URL is the only reliable indicator when it comes to deciding whether or not a website is a phish. As shown by [10] and [15]. Afterwards, it explains where to find the URL, which is especially important when using a mobile device. Users are more vulnerable to phishing when using a mobilve device [9]. How the URL is structured is also explained.

The main part is split into four different lessons, which cover the most common URL spoofing tricks [21]. Each lesson explains a specific spoofing trick, namely 1) *IP/Random URL*, 2) *Subdomain/Path* (e.g. facebook.login.com, login.com/facebook),

Fig. 1: Structure of the URL.

3) *Name Extension* (e.g. facebook-login.com) and 4) *Spelling* (e.g. facebok.com). Information about the spoofing trick contains detailed explanations on the type of attacks as well as a number of legitimate and fraudulent examples. Examples increase in complexity during the course of the training to challenge learners. The number of examples per newly introduced spoofing trick increases with later lessons.

2.2 Training Formats

The training formats differ from each other in terms of how the training is delivered to the participants. We explain the differences in this section.

Fig. 2: Example taken from NoPhish PDF.

Instructor-Based Training: The exercises are given to the participants to be classified as phishing or legitimate in a plenary session. Answers are to be openly discussed in the audience. The audience is encouraged to give feedback and helpful advice if an example was answered incorrectly. During the exercises the instructor moderates the discussion and answered questions to clarify misunderstandings.

Computer-Based Training: The computer-based training format is delivered via an Android application and is self administered by the participants. The application gives direct feedback on correctness of answers. The exercise part was designed in a playful

manner containing gamification elements like lives and “levels” (see Figure 3). The purpose of using gamification elements was to motivate users. Progress in the game is granted only if a predefined number of phishing and legitimate URLs has been identified correctly.

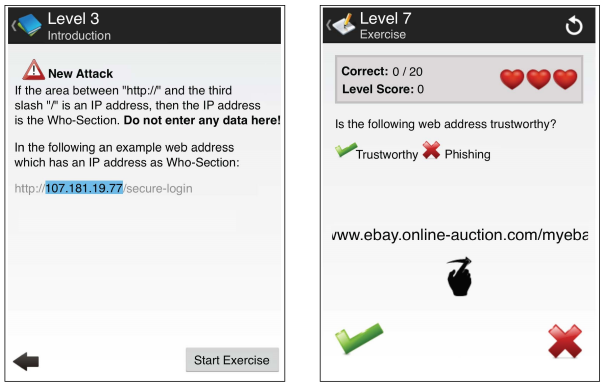


Fig. 3: Example screenshots taken from NoPhish Android Application.

Text-Based Training: The text-based training issues participants with the same NoPhish PDF used in instructor-based training. This training format precludes provision of feedback. Participants can take as much time as they wanted in reading through the Material.

3 Methodology

We conducted a user study to answer the following research questions:

Research Question 1 - Effectiveness: a) How effective are the formats in transferring knowledge to the participants? b) Are there significant differences between the three formats?
Research Question 2 - User satisfaction: a) How satisfying is it to learn with each format? b) Are there significant differences between the three formats?
Research Question 3 - Confidence: a) What impact do the training formats have on people’s confidence regarding their own abilities in correctly identifying legitimate and fraudulent websites attacks? b) Are there significant differences between the three formats?
Research Question 4 - Time efficiency: a) How much does a training group increase in correctly recognizing phishing and legitimate URLs per minute spent with the training? b) Are there significant differences between the three formats?

3.1 Study design

A between subject design was used to answer our research questions. The instructor started by informing all participants about the purpose of the study and emphasized the aim of evaluating the material rather then the individual students knowledge. We obtained the consent of every student. For minors we obtained the consent of their parents. The study was run in Germany. For answering our research questions we send an instructor into the partaking school to administer the different training formats to the participants. The instructor had an active part in instructor-based training and was passive in computer-based training as well as text-based training. The course of the user study was split into the following phases:

Pre-Questionnaire: Participants were asked to fill out a pre-questionnaire which contained 16 screenshots of webpages in a randomized order. Eight of these screenshots had been altered to show a phishing URL in the adress bar while the other eight screenshots showed legitimate URLs. Every URL spoofing category was used twice. Participants were asked the following questions for each screenshot: 1) Is the screenshot showing a phishing website or the legitimate website? 2) How certain are you with your decision?

Training: We followed with the specific training format. The duration of text-based training and computer-based training differed between participants. While instructor-based training took exactly 45 minutes the other two formats differed between participants. When participants had finished they received the Post-Questionnaire.

Post-Questionnaire: The post-questionnaire contained 32 screenshot of webpages (see Table 1) in a randomized order with 16 already shown in the pre-questionnaire and 16 new ones. As in the pre-questionnaire we added eight legitimate and eight phishing screenshots again using every URL spoofing category twice. Therefore we ended with 16 phishing, 16 legitimate screenshots and utilized every URL spoofing category four times.

General Survey: Following the post-questionnaire, participants were asked to answer socio-demographic questions. We also included three statements based on the system usability scale (SUS) [3] that were to be answered via a 5 point Likert scale, namely:

- I enjoyed learning about phishing the way I did.
- I think I learned a lot.
- What I learned will help me protecting myself in the future.

3.2 Recruitment

We recruited our participants at a school. School settings offer access to groups of participants that are homogenous in terms of sociodemographic factors like age and educational level. For this purpose we contacted a vocational0 school which has over one thousand students in total split over different professionalisation branches. The school management valued our study as complementary to the schools curriculum and cooperated with us by allowing us to use school hours of 90 minutes to carry out both the

	Pre and Post Questionnaire	Post Questionnaire only
Original	https://www.chefkoch.de/login.php	https://www.amazon.de/Angebote/b/...
	https://www.ebay.de/rpp/Deals/reisen-...	https://epaper.bild.de/
	https://www.gmx.net/produkte/mail/...	https://secure.ikea.com/webapp/wcs/...
	https://plus.google.com/u/0/me	https://touch.linkedin.com/login.html
	https://www.m.spiegel.de/panorama/...	https://www.stepstone.de/5/index.cfm...
	https://www.blumen.tchibo.de/login...	https://tagesschau.de/frontpage:.
	https://www.t-online.de/wetter/....	https://www.welt.de/sonderthemen/...
	https://blog.xing.com/category/german/	https://de.yahoo.com/...
Phishing	IP/Random URL	
	https://www.lhjwrpik.com/signin/Raum...	https://www.lesen.de/abo/digital
	https://130.83.162.6/signup/	https://198.176.23.15/Ip/pw/login
	Subdomain/Path	
	https://badcat.com/mobile.twitter.com/...	https://events-ma.de/www.gutefrage.net...
	https://web.de.emailclient.com/	https://login.live.dub123.com/login.srf...
	Name Extension	
	https://www.paypal-sicher.com/web...	https://www.zalando-zahlungsarten.de/...
	https://www.shopping-esprit.de/cgi/h2/...	https://de.wikipedia-login.org/index....
	Spelling	
	https://www.maxdorne.de/?fwe=true&...	https://www.0tto.de/damenmode/...
	https://www.windows.mircosoft.com/de...	https://id.sueddeutsche.de/login

Table 1: Legimitate and Phishing URLs used in Pre/Post-Questionnaires.

training as well as the evaluation. This had an impact on students motivation, it can be expected to make the results more transferable to education in other contexts where participants are obliged to take part in IT-security trainings (e.g. company context). The user study was carried out in three different classes which were randomly assigned to one of the three training formats. All participants taking part in this study were recruited from the branch of information assistants.

4 Results

In total, 81 participants participated. We recruited all participants from the same school and 33 participants had a secondary school leaving certificate, 45 had a high school qualification and three participants had a university degree. The group that took part in instructor-based training had 30, computer-based training 25 and text-based training 26 participants. The instructor-based training group had 2 female and 28 male participants with a mean age of 17.33 (± 1.06) and the computer-based training group had 10 female and 14 male participants with a mean age of 20.48 (± 4.82). The text-based training group had 2 female and 24 male participants with a mean age of 21.62 (± 5.177).

Research question 1 - Effectiveness: Starting with a) the effectiveness in knowledge transfer of the different formats and b) the differences in effectiveness between the formats, we measured effectiveness as the number of correct answers for both phishing URLs, legitimate URLs and overall.

a) First of all we look at the general effectiveness in knowledge transfer. Therefore we evaluated the mean difference between pre-questionnaire and post-questionnaire. A repeated measures ANOVA determined that the mean correct answers differed statistically significant between pre- and post-questionnaire ($F(1, 78) = 3918.92$, $P < 0.001$, $\eta^2 = .98$).

b) Likewise to the general effectiveness in knowledge transfer the training format (see fig. 4) showed a statistically significant difference for the mean differences ($p < .001$, $\eta^2 = .255$).

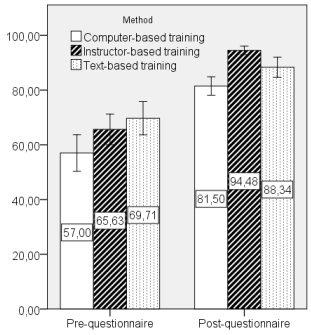


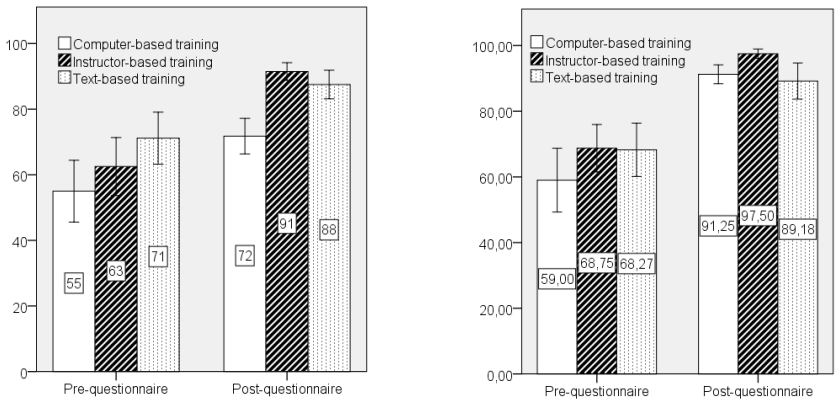
Fig. 4: Mean correct answers for pre & post legimitate and phishing URLs with 95% confidence interval (in %).

Post-hoc tests for overall correct answers using the Games Howell correction, for different number of participants per group and violated homogeneity of variance, revealed that the difference between computer-based training and instructor-based training is statistically significant ($p < .001$). The same goes for computer-based training and text-based training ($p = .004$). Whereby instructor-based training and text-based training do not differ significantly from each other ($p = .445$).

Looking at the results of the repeated measures ANOVA, every training showed a significant improvement in detecting both phishing and legitimate URLs as their representative part. Taking this into account post-hoc tests showed further significant differences between the three formats. The instructor-based training achieved both the highest post score for correct answers and the highest improvement in score from pre-questionnaire to post-questionnaire. Nevertheless only looking at the correct answers they do not score significantly better than the text-based training.

Further analyzing the results separated into phishing (fig. 5a and legitimate (fig. 5b) URLs, there is a change. While the results for phishing URLs remain the same, as computer-based training differs statistically from instructor-based ($p < .001$) and text-based training ($p < .001$) and instructor-based training does not differ significantly from text-based training ($p = .997$), this is not the case for legitimate URLs. Only considering these computer-based training remains significant below instructor-based training ($p = .009$). This time there is no statistical significant difference between

text-based training and both computer-based ($p = .843$) and instructor-based training ($p = .108$).



(a) Phishing URLs

(b) Legitimate URLs

Fig. 5: Mean correct answers for pre & post split into phishing and legimitate with 95% confidence interval (in %).

Research question 2 - User satisfaction: We looked at a) the satisfaction for each format and b) the differences between the three formats.

a) As shown in table 2 all formats achieve high results for overall satisfaction (from 4.09 to 4.46). Split into the questions, starting with the first one, instructor-based training achieved the highest mean score with ($4.57 \pm .568$), followed by text-based ($4.38 \pm .637$) and computer-based training ($4.2 \pm .764$). For question two instructor-based training again achieved the highest mean score with ($4.34 \pm .814$), this time next is computer-based ($3.88 \pm .971$) and text-based training (3.65 ± 1.198). For the third question the order is instructor-based training with a mean score of ($4.47 \pm .776$), text-based (4.31 ± 1.011) and computer-based training ($4.20 \pm .816$).

Format	1. Enjoyed?	2. Learned?	3. Protection?	Overall
Instructor-based training	4.57 (.57)	4.34 (.81)	4.47 (.78)	4.46
Computer-based training	4.2 (.76)	3.88 (.97)	4.2 (.82)	4.09
Text-based training	4.38 (.64)	3.65 (1.2)	4.31 (1.0)	4.11

Table 2: User satisfaction split into three questions and overall per format.

b) Starting with the differences for the three training formats over all three questions the one-way ANOVA suggest that there is no statistically significant differences between the training formats ($F(2, 80) = 3.023, p = .51$)

Divided into the three questions, starting with "I enjoyed learning about phishing the way I did.". The results of the one-way ANOVA showed no statistically significant difference between the training formats ($F(2, 80) = 2.138, p = .125$).

Next participants had to rate the sentence "I think I learned a lot.". The results of the one-way ANOVA showed a statistically significant difference between all formats ($F(2, 79) = 3.433, p = .037$). A Games-Howell post-hoc test showed that participants from the text-based training answered significant lower compared to the computer-based training ($p = .74$) and to those in the instructor-based training ($p = .045$). There was no statistically significant difference between the instructor-based training and the computer-based training ($p = .153$).

Finally participants had to rate the sentence "What I learned will help me protecting myself in the future.". The results of the one-way ANOVA showed no statistically significant difference between formats ($F(2, 80) = .658, p = .521$).

Research question 3 - Confidence Level: We looked at a) the impact the training formats have on peoples confidence regarding their own abilities in correctly identifying legitimate and fraudulent websites attacks and b) differences between the three formats?

a) Therefore we analyzed the confidence level for all formats in between the pre- and post-questionnaire. A repeated measure ANOVA determined that the mean correct answers differed statistically significant between pre- and post questionnaire (F$(1, 71) = 150.71$, $P < 0.001$, $\eta^2 = .68$).

b) Just as the difference between the pre- and post-questionnaire the training formats (see table 3) showed a statistically significant difference for the mean differences ($p = .002$, $\eta^2 = .16$).

Format	Pre	Post	Difference
Instructor-based training	3.22(.80)	4.73(.27)	1.51
Computer-based training	3.58(.79)	4.58 (.52)	1.00
Text-based training	4.12(.50)	4.67(.31)	0.55

Table 3: Average user confidence pre-questionnaire and post-questionnaire per format.

Post-hoc tests using the Games Howell correction revealed that the difference between text-based training and instructor-based training is statistically significant ($p < .001$). Whereby computer-based training and instructor-based training do not differ significantly from each other ($p = .76$), as well as computer-based and text-based training ($p = .098$).

Looking at the results of the repeated measures ANOVA, every training showed a significant improvement in confidence. Post-hoc tests showed further significant differences between the three formats. The instructor-based training achieved both the highest post confidence, the highest improvement in confidence and achieved a significant higher confidence than the text-based training.

Research question 4 - Time efficiency: For the fourth and final research question we wanted to know a) how much the training formats increase the correctly recognition of

phishing and legitimate URLs per minute spent with the training and b) the differences between the three formats.

a) Table 4 shows the mean time efficiency for the formats. Furthermore, it shows that on average for every minute that the instructor-based group spent with the training, they were able to increase the amount of correct answers given by 0.64 on average. For computer-based training it is on average 0.92 more correct answers per minute and for text-based training on average 1.03 more correct answers

Format	Mean time (minutes)	Improvement per minute
Instructor-based training	45	0.64
Computer-based training	26.5	0.92
Text-based training	18	1.03

Table 4: Time taken and time efficiency per format. Improvement per minute = percentage of improvement of correct answers divided by mean time.

b) A Kruskal-Wallis H test showed that there was a statistically significant difference in time spent between the different trainings, $\chi^2(2) = 35.01, p < 0.001$.
Median in formats computer-based training and text-based training were 26.5 and 18 minutes; the distributions in the two formats differed significantly ($U = 55.5, Z = -3.17, p = 0.002, \eta^2 = .26$).

Regarding our time efficiency although the instructor-based training had the biggest improvement (+28.85%) it is only an improvement of 0.64 correct answers per minute spent. The second best improvement was achieved by the training that took part in computer-based training (+24.5%) which results in an improvement of 0.92 correct answers per minute spent. Finally the text-based training training achieved lowest general improvement (+18.63%). Considering the time spent for the training they achieve the highest score with an improvement of 1.03 correct answers per minute spent.

5 Discussion

All training methods improve participants ability in phishing detection and their ability in identifying legitimate webpages significantly. Furthermore, they felt significantly more confident in judging webpages after the training. However, the results of the user study show significant differences between the different training formats. Considering efficiency, user satisfaction and confidence, instructor-based training format achieved the best results. It performed significantly better than the other two formats. At the same time it achieved the lowest time efficiency. This result is in line with the findings in [7]. The authors showed that a social situation and a familiar context like for the pupils in our instructor-based group has a positive learning effect. While the improvement in confidence differs, all three formats achieve a very high score around 4.7 of 5. Not surprisingly, instructor-based training takes more time. While we decided to go for 45 minutes, in a company instructor-based training requires more time, e.g. as participants need to reach the class room and get back to their offices. Thus, while the security

level in the company would increase more than with the other levels, it might not be chosen because of the time (and maybe the costs and the lack of flexibility to decide when to learn and to take breaks).

Interestingly, text-based training performs better than computer-based training. With respect to efficiency, user satisfaction and confidence it achieves the second best results. The results of research question 4 indicate that spending some more minutes with the material is likely to improve the results even further. Thus, if time is a limited resource text-based training is the best training format as it clearly achieves the best results in time-efficiency. Furthermore, participants improved also significantly in making proper decisions as well as in detecting phishing webpages.

A possible explanation for this results is that participants were able to chose their own pace when going through the training. While one can miss important messages when lacking concentration during instructor-based training this cannot happen with text-based training. Participants could go back and read earlier explanations again. Furthermore, it might be easier reading the URL letter by letter when the PDF is displayed at the screen right in front of them other than displayed by a projector on the wall. What would be interesting but has not been tested is the effect it would have if people do not learn the entire content at once but would start one day and come back at a later time.

The results of the computer-based training group indicate, that this method is not particularly more effective or satisfying than the other two formats; however more expensive, as it needs to be developed. The unexpectedly low improvement of the computer-based training group might possibly be affected by the small screen size of the smartphones. Reading through educational material via a small smartphone screen might not be the best way to partake in security training. While on the other hands it offers a potential for even more interactive training formats. Our results for computer-based training are inline with the results in [19]. However, the authors of [12] got a greater effect than instructor-based training. It needs to be studied further, why their results differ.

Limitations: Participants saw a high amount of phishing examples in a short time frame. Such a high frequency exposure to phishing URLs would likely never happen in a real scenario. While this is the typical problem of phishing studies, this is not a major concern for our study as we compare which format performs better in communicating the content of the NoPhish training concept.

While the text-based training and computer-based training usually have the innate option of pausing at any convenient moment, our study design precluded this possibility. Which effort pausing has to the results needs to be studied in future.

The training was given by a motivated instructor. It is possible that the very positive results of the instructor-based training group can in part be attributed to this fact. But this is a limitation with instructor-based training in general that does not specifically apply to our study design.

Students in the school setting are primed for instructor-based training. This is different from a company setting. Thus, using the instructor-based approach in companies may perform less good than in a school.

Our sample is not representative of the general population, as participants were all students in the professionalisation branch of information assistants. Such they brought

an above average general knowledge of IT related problems. However, it shows that also those people lack knowledge in phishing security. Furthermore, earlier evaluations on NoPhish showed significant improvements also for lay people.

6 Related Work

In our study, we used the NoPhish training materials, which are freely available in the three formats in question (instructor-based, computer-based, and text-based). All of the formats provide the same content to the user. In the following, we present similar research comparing different IT-security training formats.

Sheng *et al.* [20] compared the effectiveness of different educational materials to identify phishing websites. Their study included two groups using text-based training and one group using computer-based training. They did not include instructor-based training in their comparison. For their text-based solutions they used "three consumer oriented educational web pages from the first page of Google search results using the search query *phishing*" and the cartoon PhishGuru. The computer-based training used the Anti-Phishing Phil game. The formats used in their study provided different content to the users and not all of them are freely available. The authors did not find any difference in the number of users that fall for phishing between the different formats.

Kumaraguru *et al.* [14] reports on the comparison of three formats for improving the users' skills in terms of detecting phishing attacks. They developed two embedded training designs (computer-based training) and another format consisting of simple email security notices (text-based training). The embedded training designs consisted of regularly sent phishing emails. The results of their study indicate that the embedded training designs (computer-based training) were more effective than simple security notices (text-based training).

Khan *et al.* [13] compared different education material formats based on psychological theories, including instructor-based training, computer-based training (traditional and video games), and text-based training (newsletter articles and posters). They categorize instructor-based training as efficient but unattractive. In their opinion, computer-based training has the advantage of allowing users to learn at their own pace, while being resource-extensive and relatively expensive. For the text-based materials they summarize that these are efficient ways to deliver information, but that it cannot be verified if the information was actually read by the user.

Schilliger and Schmid [19] discuss multiple formats from a theoretical point of view. They see advantages in computer-based training. It can efficiently serve to big groups, due to its support of time and location independent learning. Furthermore, it is much easier to track the learners' success. With regard to text-based training, the authors believe that it is best used to remind people of content they already learned before. Concerning instructor-based training, they argue that it should be as short and as memorable as possible to increase the effectiveness.

Reid [18] developed a software program that supports the delivery of important information. He used a commercial set of knowledge level questions and measured the success of his computer-based technique. The results indicate that frequent repetition of training activities increases knowledge retention.

Canova *et al.* [6] did a small scale lab and retention study of the NoPhish android application. They found significant effects of the application when it comes to transferring the information to the participants both immediately after the study aswell as five months after the participants had taken part in the study.

7 Conclusion and Future work

We conducted a user study comparing the three different training formats computer-based training, instructor-based training and text-based training with respect to their effectiveness, user satisfaction, confidence and time efficiency. We note that every format lead to a significant improvement of participants IT-security knowledge and confidence in handling the tasks. Also, participants of all groups were satisfied with their respective training format. Instructor-based training created the most promising results regarding three of our four research questions (effectiveness, user satisfaction, confidence). However it performed the worst in our fourth research question (time efficiency). The text-based training format performed slightly worse than instructor-based training. However it has applications in scenarios where time is the most pressing matter as it is the most time efficient formats. Though computer-based training performed worse than the other two formats it still provided for a significant improvement in URL detection. Computer-based training via smartphones enables users to learn whenever they want, wherever they want and for any duration they seem fit and it has benefits when it comes to flexibility in application.

While our study focused on the possible gains of different formats of security training we did not evaluate how the required expenditures differ. A realistic cost assessment including creation and maintenance of the materials remains an area of future work. Also we plan the evaluate the retention of the transmitted knowledge in the future. A comparative analysis of the effect small screensizes have on training effectiveness also remains a topic for further research. Another open issue for future work will be to evaluate whether the rules can be implemented into a usable security tool that automatically addresses incoming E-Mails.

8 Acknowledgement

This work has been developed within the project ‘KMU AWARE’ which is funded by the German Federal Ministry for Economic Affairs and Energy under grant no. BMWi-VIA5-090168623-01-1/2015. The authors assume responsibility for the content.

References

1. Abras, C., Maloney-Krichmar, D., Preece, J.: User-centered design. Bainbridge, W. Encyclopedia of Human-Computer Interaction. 37(4), 445–456, Sage Publications (2004)
2. Bada, M., Sasse, A., Nurse, J.R.C.: Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In: International Conference on Cyber Security for Sustainable Society. pp. 118–131. Global Cyber Security Centre (2015)

3. Brooke, J.: SUS-A quick and dirty usability scale. Usability evaluation in industry 189(194), 4–7, Taylor and Francis (1996)
4. Canova, G., Volkamer, M., Bergmann, C., Borza, R.: NoPhish: an anti-phishing education app. In: STM, pp. 188–192. Springer (2014)
5. Canova, G., Volkamer, M., Bergmann, C., Borza, R., Reinheimer, B., Stockhardt, S., Tenberg, R.: Learn to Spot Phishing URLs with the Android NoPhish App. In: Information Security Education Across the Curriculum, pp. 87–100. Springer (2015)
6. Canova, G., Volkamer, M., Bergmann, C., Reinheimer, B.: NoPhish App Evaluation: Lab and Retention Study. USEC 2015, Internet Society (2015)
7. Das, S., Kim, H., Dabbish, L.A., Hong, J.I.: The effect of social influence on security sensitivity. In: SOUPS. vol. 14. ACM (2014)
8. Desai, M.S., Richards, T., Eddy, J.P.: A field experiment: instructor-based training vs. computer-based training. Journal of Instructional Psychology 27(4), 239, George Uhlig Publisher (2000)
9. Felt, A.P., Wagner, D.: Phishing on mobile devices. USEC 2011, Internet Society (2011)
10. Garera, S., Provos, N., Chew, M., Rubin, A.D.: A framework for detection and measurement of phishing attacks. In: ACM workshop on Recurring malcode. pp. 1–8. ACM (2007)
11. Greg, A., Rasmussen, R.: Global Phishing Survey: Trends and Domain Name Use in 2H2014 (2015), http://internetidentity.com/wp-content/uploads/2015/05/APWG_Global_Phishing_Report_2H_2014.pdf Accessed 13 March 2016
12. Harrington, S.S., et al.: A comparison of computer-based and instructor-led training for long-term care staff. The Journal of Continuing Education in Nursing 33(1), 39 (2002)
13. Khan, B., Alghathbar, K.S., Nabi, S.I., Khan, M.K.: Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management 5(26), 10862–10868, Academic Journals (2011)
14. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E.: Protecting people from phishing: the design and evaluation of an embedded training email system. In: CHI. pp. 905–914. ACM (2007)
15. Ma, J., Saul, L.K., Savage, S., Voelker, G.M.: Beyond blacklists: learning to detect malicious web sites from suspicious URLs. In: SIGKDD international conference on Knowledge discovery and data mining. pp. 1245–1254. ACM (2009)
16. Ng, B.Y., Kankanhalli, A., Xu, Y.C.: Studying users' computer security behavior: A health belief perspective. Decision Support Systems 46(4), 815–825, Elsevier (2009)
17. Ramzan, Z.: Phishing attacks and countermeasures. In: Handbook of Information and Communication Security, pp. 433–448. Springer (2010)
18. Reid, D.: Knowledge retention in computer-based training. University of Calgary (2001)
19. Schilliger, B., Schmid, R.: Entwickeln einer Awareness-Kampagne für einen sicheren Umgang mit dem Internet an mittelgrossen Berufs-oder Maturitätsschulen. Ph.D. thesis, Hochschule Luzern, Wirtschaft (2010)
20. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J.: Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In: CHI. pp. 373–382. ACM (2010)
21. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E.: Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In: SOUPS. pp. 88–99. ACM (2007)
22. Thorndike, E.L.: The fundamentals of learning. Teachers College Bureau of Publications (1932)