The *Phishing Master* Anti-Phishing Game*

Heike Dietmann, Tobias Länge, Philipp Matheis, Aleksandra Pawelek, Benjamin Berens, Mattia Mossano, Maxime Veit, Peter Mayer, Melanie Volkamer
{mattia.mossano,tobias.laenge9,philipp.matheis9,benjamin.berens,maxime.veit,peter.mayer,melanie.volkamer}@kit.edu
Karlsruhe Institute of Technology
Germany

ABSTRACT

Games are one type of measure developed to raise security awareness. We present the design of a anti-phishing game for public events or for public spaces. We collected feedback on the game and got an impression of individuals' interaction with it, through a small user study with a convenience sample at a public event. Participants left overall positive feedback on the game. Our anti-phishing game seems to be a good alternative to classical anti-phishing measures – in particular for public security awareness events. However, further work is required to integrate the received feedback and then evaluate the game in a controlled study.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; • **Software and its engineering → Interactive games**.

KEYWORDS

Phishing, Gamification, Human Factors

1 INTRODUCTION

Sending phishing messages – be it as email or otherwise – is a popular method of online fraud. The FBI [1] rated phishing as the most widespread cybercrime in 2020 and IBM [3] rated it as the second most costly attack. While many email providers use technical measures to automatically detect phishing emails, these technical measures are not 100% effective. As attack methods continue to improve, phishing messages become more difficult to detect. In turn, continuing improvements to filter rules might lead to a higher accuracy in the detection of phishing messages, but they are likely to result in false positives. Moreover, keeping filters relevant and consistent across communications mediums might prove hard.

One way to support users is to increase their awareness of the problem and teach them how to distinguish legitimate and phishing messages. Accordingly, a large number of phishing awareness measures have been developed in recent years, such as texts (e.g., [5]), e-learning platforms (e.g., [4]), videos (e.g., [2]), and games or quizzes (e.g., [7]). Typically, these measures are used as part of a mandatory security training for employees and/or by individuals motivated to learn more about anti-phishing security. However, individuals who are completely unaware of phishing or who are not yet motivated to learn about it might be left out. Our work tries to address this issue. We present the design of an anti-phishing game and a first study at a public event in Germany.

2 PHISHING MASTER

The anti-phishing game we propose, *Phishing Master*, is in first-person perspective. The anti-phishing content is based on the awareness measures proposed by Reinheimer et al. [6] which have been previously evaluated in different formats and shown to significantly increase the phishing detection ability of individuals. We adapted the content and evaluation materials to fit a shooting game. The game was developed using an iterative approach, integrating feedback from potential players.

In the game, players are taken to a virtual office where they are positioned in front of a desk with a monitor, a keyboard, and a mouse (see Figure 1). The design idea at the base of the anti-phishing game is that messages fly towards the player for a period of 30 seconds, one after the other, and only the phishing ones should be shot at. If the message is legitimate, points are awarded only if the players shoot at the "Legitimate" button on the desk. Additional points are earned the more quickly and accurately a player acts. Accuracy is defined as hitting the malicious part of the message, e.g., hitting the malicious e-mail address, URL, or attachment. If several messages are answered correctly in a row, the gained points increase through a "combo" system. At the end, the players are shown the number of points they have achieved and their position on the leader board (they can enter a name or continue anonymously).

Phishing Master has sound and visual effects (e.g., firework explosions for correct decisions) to increase its appeal. It can be played with either a gamepad or with keyboard and mouse. The main purpose of Phishing Master is to support organizers of security

Figure 1: Our anti-phishing game in score mode.

*An extended version of this poster abstract is available at: https://publikationen.bibliothek.kit.edu/1000153329

ACSAC 2022, December 05–09, 2022, Austin, TX, USA
2022. ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Figure 2: The study setup.

awareness events in making security awareness more attractive – in particular for individuals in favor of video games. To that end, it is freely available as a stand-alone application for Windows and as a web application[1]. After playing through the game in the web version, players can also invite friends and compete directly by sharing a specific URL to the game.

3 USER STUDY – METHODOLOGY

To gain insights into individuals' interaction with Phishing Master and to collect feedback on it, the game was made available at an event in Germany for three hours a day, over three days. Following COVID-19 regulations, to guarantee the safety of the participants each surface was disinfected after each participant and masks were mandatory the whole time. The setup of the study consisted of an armchair in front of a large monitor next to a table with a PC, a gamepad, feedback forms, a yellow mailbox and pens (see Figure 2). The station was constantly supervised by one of the authors. The participants were recruited with convenience sampling. If the station was free, many were immediately interested on their own or quickly agreed to test the anti-phishing game after being approached; few said they didn't have the time or interest.

At the end of the interaction with the anti-phishing game, the participants were invited to fill out a questionnaire for evaluation and feedback. On the questionnaire, the anti-phishing game could be rated in terms of design (7-point Likert, from "Very good" to "Very bad") and understandability (7-point Likert, from "Very understandable" to "Very incomprehensible"). It was also asked to what extent they agreed that the high score is an incentive to play again (7-point Likert, from "I strongly agree" to "I strongly disagree"). The participants were then asked for any suggestions for improvement. At the end, they were asked if they would recommend the anti-phishing game to others. All the data was collected on paper and was anonymous (no demographics). We neither had nor requested any information about the people invited to this event.

4 USER STUDY – RESULTS

Many stopped to try out our game, despite its availability not being advertised. The majority of individuals (52 out of 57) filled out the questionnaire. A total of 49 out of 52 (almost 95%) participants gave Phishing Master a positive rating, 33 (63.5%) selected "Good", 11 (21.2%) "Very good" and 5 (9.6%) "Partially good". When asked how easy it was to understand how to play Phishing Master, almost all players (96.2%) felt that the anti-phishing game was generally easy to understand (rating it very easily, easily or partially understandable). Regarding the high score being an incentive to play it again, 36 (69.2%) participants generally agreed, with 13 (25.0%) simply agreeing, 3 (5.8%) fully agreeing and 20 (38.5%) partially agreeing. 45 participants said they would recommend the anti-phishing game to others.

From the feedback, the following improvements could be derived:
Context: Provide more context on the messages to be judged as most senders are unknown. This issue is mainly caused by the design decision to not use real service providers in [6].
Overview page: Improve the overview page by (a) focusing on the messages which were judged as legitimate although they are phishes and (b) providing general hints how to improve the phishing detection skills (in particular when the wrong answers are above a threshold or for a particular type of phishing).
Interaction: Shooting anywhere outside the email could be considered as legitimate and improving the unzoomed messages' visibility.

5 CONCLUSION & FUTURE WORK

Our results suggest that Phishing Master might be a good alternative to well-known awareness measures. The main limitation is that our goal is to find an appropriate measure for security awareness events while in our study setting the main event was not on security. Thus, the future work is twofold: (1) integrating the feedback we received and (2) an evaluation in a controlled setting with a larger and more balanced participant sample at a security event.

ACKNOWLEDGMENTS

This research is supported by the topic Engineering Secure Systems, topic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by KASTEL Security Research Labs, as well as by the ministry of Science, Research and the Arts Baden-Württemberg as part of the DIGILOG@BW - joint research project with funds from the digilog@bw State Digitization Strategy.

REFERENCES

[1] FBI. 2021. 2020 Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[2] Vaibhav Garg, L Jean Camp, Lesa Mae, and Katherine Connelly. 2011. Designing risk communication for older adults. In *Symposium on Usable Privacy and Security (SOUPS '11)*. USENIX, USA, 1–10.
[3] IBM. 2021. Cost of a Data Breach Report 2021. https://www.ibm.com/security/data-breach
[4] Masatoshi Kawakami, Hiroshi Yasuda, and Ryoichi Sasaki. 2010. Development of an E-Learning Content-Making System for Information Security (ELSEC) and Its Application to Anti-Phishing Education. In *Proceedings of the 2010 International Conference on E-Education, e-Business, e-Management and e-Learning (IC4E '10)*. IEEE Computer Society, USA, 7–11. https://doi.org/10.1109/IC4E.2010.63
[5] Stephan Neumann, Benjamin Reinheimer, and Melanie Volkamer. 2017. Don't Be Deceived: The Message Might Be Fake. In *Trust, Privacy and Security in Digital Business*. Springer, Cham, 199–214.
[6] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana Von Landesberger, and Melanie Volkamer. 2020. *An Investigation of Phishing Awareness and Education over Time: When and How to Best Remind Users*. USENIX, USA, 259–284.
[7] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. 2019. What.Hack: Engaging Anti-Phishing Training Through a Role-Playing Phishing Simulation Game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300338

[1] https://phishing-master.secuso.org