How Vulnerable is the Average Population?
Advocating for Cybersecurity Awareness Education in People's Private Lives

DANIEL KÖHLER[*], WENZEL PÜNTER[*], and CHRISTOPH MEINEL, Hasso-Plattner-Institute, Germany

Cybersecurity attacks cover countries, institutions, companies, employees, and private persons. Companies can protect against known threat vectors through technical or organizational measures. Organizational measures, such as education of the employees, have shown to yield success in securing companies' perimeters. It is often assumed that knowledge and experiences from a person's professional life impact their private life. As such, (security) awareness should translate between a person's leisure and work life.

We performed a phishing study across more than 4,700 participants in Germany. Our study did not observe significant positive correlations between previously participating in cybersecurity programs and phishing susceptibility. Quite contrary, we observed that participants of classroom-based training performed worse than the average population. A more significant effort is required to be put into the education of laypersons for online cybersecurity threats in their private life.

CCS Concepts: • **Security and privacy** → **Phishing**; *Social aspects of security and privacy*; • **General and reference** → Experimentation.

Additional Key Words and Phrases: phishing, cybersecurity awareness, private, education

ACM Reference Format:
Daniel Köhler, Wenzel Pünter, and Christoph Meinel. 2024. How Vulnerable is the Average Population? Advocating for Cybersecurity Awareness Education in People's Private Lives. In . ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION AND RELATED WORK

Ongoing digital transformation leads to a continuous increase in attack surfaces exposed to the internet. While attacks against companies, users, and laypersons are nothing new, the internet allows them to be executed faster, easier, and against a broader range of targets. The dangers imposed by the omnipresent cyberspace need to be observed and, to some extent, understood by everybody. Currently, education on cybersecurity mainly happens in one of three contexts: (1) Optional study content in universities and schools, (2) Professional training programs for employees, or (3) Voluntary education programs, such as online courses.

Educating for cybersecurity, however, is part of a greater psychological problem space. People do not necessarily apply their knowledge or act accordingly [6]. Hence, previous research has presented various models to foster different dimensions of cybersecurity awareness. In 2006, the Knowledge, Attitude, Behavior (KAB) model by *Kruger and Kearney* [9] provided a first foundation for analyzing the learning curve connected to cybersecurity awareness, in which a focus on the behavior is required. In the past years, the KAB model has been further developed [3], and other researchers developed alternative models [7]. All models agree that knowing a threat does not directly result in appropriate security behavior. Hence, quizzes on cybersecurity threats are insufficient to assess security awareness.

With that knowledge, organizations are moving towards evaluating their employees' knowledge and behavior. One opportunity for assessing an employee's behavior is by performing phishing tests. Extensive research has been conducted in this context throughout the past years, with studies covering more than 10,000 participants [12, 14] or spanning more than a year [14]. With their work, fellow researchers identified, e.g., cues in the email design

[*] Both authors contributed equally to this research.

leading to improved susceptibility of recipients [1, 13, 16, 17], or psychological vectors influencing a phishing mail's success [2, 14, 15]. Researchers similarly studied various (socio-) demographic vectors of targets which potentially impact susceptibility [5, 8, 12, 14]. However, researchers are inconclusive on the impact of many of the underlying vectors throughout the different studies. Further, all previous work has been conducted in professional or academic contexts. No previous work has targeted private persons, e.g., in a phishing study. We, therefore, investigate how findings on phishing susceptibility translate from research in professional contexts to the previously unstudied private context.

2 CONTRIBUTIONS FROM OUR CURRENT RESEARCH

In a recent (10/2022 – 01/2023) study [10], we sent more than 14,000 phishing emails to approximately 4,700 German-speaking participants. We recruited participants for our research through consent for email communication on our online education platform openHPI[1]. To ensure unbiased results, we did not inform the participants of the explicit goal of the research. Instead, we approved the study with the Institutional Review Board of the University of Potsdam. Participants hence did not know in advance that they would receive phishing emails.

In the study, we observed average click rates of 10-15% per email throughout the four iterations of emails sent to the participants. With survey feedback, we identified a significant ($\chi^2 = 4.75, p = 0.029 < \alpha$) correlation between gender and susceptibility, with males being slightly more susceptible. Further, we observed that particularly young (<20 years) and older (70+ years) recipients are significantly ($\chi^2 = 27.241, p = 0.0001 < \alpha$) more prone to fall for phishing attacks. We validated the finding from previous research that having fallen victim to a past phishing email is a good indicator for future susceptibility [4, 12].

However, we observed contrasting findings to previous research when investigating if previous training programs are beneficial. Most previous training programs, such as phishing tests and video- or computer-based training, did not significantly correlate with phishing susceptibility. Classroom-based training, on the other hand, even negatively impacted the recipient's phishing susceptibility ($\chi^2 = 4.44, p = 0.035 < \alpha$). Of the 114 participants who participated in classroom-based training, 41,2% clicked on a link in any of our emails, while only 30,7% from all other participants reacted. We further evaluated the impact of an online course on cybersecurity, which we provided during the first two months of the study. 15% of our study participants ($N_{MOOC} = 693$) participated in the course targeting private persons. We observed a significant correlation between course participation and phishing susceptibility (only) with the fourth email of our study (2 months after course end), with course learners performing slightly, but significantly, better ($\chi^2 = 0.333, p = 0.021 < \alpha$, click rate of $C_M = 10,4\%$ compared to $C_{!M} 13,8\%$).

3 DISCUSSION AND POSITION

Our findings on the helpfulness of education programs contrast with most previous research. However, this finding might be strongly impacted by the differing context of the study. As such, while we investigated the reactions of private people to phishing emails which they did not expect, other authors investigated educational programs included in the security concepts of companies. However, professional education programs target different threat vectors than those imposed through our phishing emails.

An initial conclusion could be that specific training for private persons is beneficial. However, our online course only significantly impacted participants' susceptibility for one of the four emails sent during our study. Qualitative analysis

[1] openHPI is a research and education platform by the Hasso-Plattner-Institute which provides cost-free Massive Open Online Courses.

of the results of our research as well as feedback provided in our final survey shows that learners aim to investigate the emails they receive. Some of those learners even perform dangerous actions during their investigation, such as clicking on links sent to them. We conclude from our study and corresponding analysis:

C1 Awareness in private contexts is not implicitly enabled through awareness programs and measures from people's professional life.

C2 People want to understand and investigate their threats themselves, which can be dangerous if done inconsiderately.

As training and awareness apparently do not translate from the professional context into private life as expected, other accessible resources and programs are required. However, the training programs for private people we have observed so far (including our course) lack the skills needed to investigate (potential) cybersecurity incidents securely. Educators hence need to re-evaluate the skills taught in programs for private people.

ACKNOWLEDGMENTS

The results partly presented in this work are part of a study performed between October 2022 and January 2023 on user phishing susceptibility. One manuscript on this study has been published at the ACNS 2024 [11], the second manuscript is currently under review at SOUPS 2024 [10].

(Updated: March 2024)

REFERENCES

[1] Sadia Afroz and Rachel Greenstadt. 2011. PhishZoo: Detecting Phishing Websites by Looking at Them. In *2011 IEEE Fifth International Conference on Semantic Computing*. IEEE, Palo Alto, CA, USA, 368–375. https://doi.org/10.1109/ICSC.2011.52 http://ieeexplore.ieee.org/document/6061361/.

[2] Zinaida Benenson, Freya Gassmann, and Robert Landwirth. 2016. Exploiting curiosity and context: how to make people click on a dangerous link despite their security awareness. https://www.blackhat.com/us-16/briefings.html.

[3] Bilal Khan. 2011. Effectiveness of information security awareness methods based on psychological theories. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT* 5, 26 (Oct. 2011). https://doi.org/10.5897/AJBM11.067 http://www.academicjournals.org/AJBM/abstracts/abstracts/abstracts2011/28Oct/Khan20et20al.htm.

[4] Matthew Canham, Clay Posey, Delainey Strickland, and Michael Constantino. 2021. Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards. *SAGE Open* 11, 1 (Jan. 2021), 2158244021990656. https://doi.org/10.1177/2158244021990656 https://doi.org/10.1177/2158244021990656.

[5] Frank L. Greitzer, Wanru Li, Kathryn B. Laskey, James Lee, and Justin Purl. 2021. Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility. *ACM Transactions on Social Computing* 4, 2 (June 2021), 1–48. https://doi.org/10.1145/3461672 https://dl.acm.org/doi/10.1145/3461672.

[6] Tapiwa Gundu. 2019. Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security*. 94–102.

[7] Norman Hänsch and Zinaida Benenson. 2014. Specifying IT security awareness. In *2014 25th International workshop on database and expert systems applications*. IEEE, 326–330.

[8] Daniel Jampen, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. 2020. Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences* 10, 1 (Aug. 2020), 33. https://doi.org/10.1186/s13673-020-00237-7 https://doi.org/10.1186/s13673-020-00237-7.

[9] H.A. Kruger and W.D. Kearney. 2006. A prototype for assessing information security awareness. *Computers & Security* 25, 4 (June 2006), 289–296. https://doi.org/10.1016/j.cose.2006.02.008 https://linkinghub.elsevier.com/retrieve/pii/S0167404806000563.

[10] Daniel Köhler, Wenzel Pünter, and Christoph Meinel. 2024. Fishing for Non-Professional Answers: Quantitative Study on Email Phishing Susceptibility in Private Contexts. https://doi.org/10.13140/RG.2.2.21865.47201/1 In Review.

[11] Daniel Köhler, Wenzel Pünter, and Christoph Meinel. 2024. How Users Investigate Phishing Emails that Lack Traditional Phishing Cues. In *Applied Cryptography and Network Security (Lecture Notes in Computer Science, Vol. 14585)*, Christina Pöpper and Lejla Batina (Eds.). Springer, Cham, Abu Dhabi, UAE, 381–411. https://doi.org/10.1007/978-3-031-54776-8_15

[12] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. 2022. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. In *2022 IEEE Symposium on Security and Privacy (SP)*. 842–859. https://doi.org/10.1109/SP46214.2022.9833766 ISSN: 2375-1207.

[13] Kathryn Parsons, Marcus Butavicius, Malcolm Pattinson, Agata McCormac, Dragana Calic, and Cate Jerram. 2015. Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails? (2015). https://aisel.aisnet.org/acis2015/90.

[14] Florian Quinkert, Martin Degeling, and Thorsten Holz. 2021. Spotlight on Phishing: A Longitudinal Study on Phishing Awareness Trainings. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, Lorenzo Cavallaro, Leyla Bilge, Giancarlo Pellegrino, and Nuno Neves (Eds.). Vol. 12756. Springer International Publishing, Cham, 341–360. https://doi.org/10.1007/978-3-030-80825-9_17 https://link.springer.com/10.1007/978-3-030-80825-9_17.

[15] Prashanth Rajivan and Cleotilde Gonzalez. 2018. Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Frontiers in Psychology* 9 (2018). https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00135.

[16] Hossein Siadati, Sean Palka, Avi Siegel, and Damon McCoy. 2017. Measuring the Effectiveness of Embedded Phishing Exercises. https://www.usenix.org/conference/cset17/workshop-program/presentation/siadatii.

[17] Emma J. Williams and Danielle Polage. 2019. How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. *Behaviour & Information Technology* 38, 2 (Feb. 2019), 184–197. https://doi.org/10.1080/0144929X.2018.1519599 https://www.tandfonline.com/doi/full/10.1080/0144929X.2018.1519599.

Received 23 February 2023; Revised 18 April 2023; Updated References 25 March 2024