**JOURNAL OF DIGITAL SYSTEM DEVELOPMENT**

*https://e-journal.uum.edu.my/index.php/jdsd*

How to cite this article:
Ismail, N.N.S., Fammy Rikzan, F.I., Katuk, N. Hashim, N.L. & Mohd Zulkefli, N.A. (2023). Enhancing Information Security Awareness on Phishing Among IT Students: A Pilot Test Case Study at Politeknik Tuanku Syed Sirajuddin. *Journal of Digital System Developments*, *1*, 12-23. https://doi.org/10.32890/jdsd2023.1.2

# ENHANCING INFORMATION SECURITY AWARENESS ON PHISHING AMONG IT STUDENTS: A PILOT TEST CASE STUDY AT POLITEKNIK TUANKU SYED SIRAJUDDIN

**[1]Nor Naematul Saadah Ismail, [2]Fatin Izzati Fammy Rikzan, [3]Norliza Katuk, [4]Nor Laily Hashim & [5]Nurul Akhmal Mohd Zulkefli**

[1]Human Resource Department, Ministry of Higher Education, Malaysia
[2,3&4]School of Computing, Universiti Utara Malaysia, Malaysia
[5]College of Arts and Applied Science, Dhofar University, Oman

*[1]Corresponding author: naematul@ptss.edu.my*

Received: 17/9/2023 Revised: 21/9/2023 Accepted: 1/10/2023 Published: 31/10/2023

## ABSTRACT

Students engage with the core operations of university business processes, making them potential targets susceptible to significant cyberattack risks due to their limited experience and knowledge in information security. Consequently, IT students must gain awareness and competence in information security to mitigate potential threats and attacks, including those related to Information Technology (IT) security threats and the loss of valuable information and intellectual assets. This paper aims to assess the Phishing Awareness Program implemented at the Department of Information Technology and Communication (ITC) in Politeknik Tuanku Syed Sirajuddin (PTSS) and its students' awareness level. The significance of this study is focusing on students' weaknesses and educating them about being cyber victims. Thirty students were involved in participating in this survey. They were given a set of questionnaires and performed pre-test and post-tests. After that, they were given three videos related to phishing and, later, three videos related to the consequences of phishing. Their awareness evaluation was performed after video training had been completed. Even though the score results of the post-test were increased and got positive feedback from respondents, several respondents still got the medium-level score. Suggestion for improvement was obtained to improve the current video content and its implementation. This work contributes to the information security awareness domain, where managers at higher learning institutions can replicate similar processes as proposed in this work in conducting similar training awareness with their students.

**Keywords:** Student awareness, Cybersecurity, Training awareness, Phishing Awareness.

## INTRODUCTION

Politeknik Tuanku Syed Sirajuddin (PTSS) is a public higher-learning institution with approximately 500 academic and 200 administrative staff. It has six academic departments with two supportive academic departments with several programs offered. A group of students from the Department of Information Technology & Communication (ITC) were involved in this study. Since Malaysia was affected by the Corona Virus Disease in 2019, also known as COVID-19, all educational institutions were asked to run classes online during and several months after the lockdown. Besides that, some institutions still run the course in a hybrid mode, either face-to-face or via the online learning platform. Thus, students and lecturers are dependent a lot on the Internet. With the tremendous usage of the Internet nowadays, students and lecturers face many possible cybersecurity threats.

Students are amongst the largest groups in PTSS. They have a significant role in determining the PTSS's data security successfully. The students have more opportunities to initiate information security problems than other PTSS populations, such as lecturers, office workers, or upper management. Students relate to the entire main activities of business processes at the university. Because of that, a student could be the target and bring high-risk impacts in any cyber-attacks based on their lack of experience and knowledge about information security. Therefore, students must understand and perform information awareness to avoid potential threats or attacks by understanding Information Technology (IT) security threats, loss of information and knowledge assets (Gandhi, 2017).

Phishing is one of the threats that students may face. Phishing attacks can dupe targeted victims into sharing their personal or vital information. This attack is commonly accomplished through emails that got and shared counterfeit links that portray trustworthy or well-known third-party websites (CJ et al., 2018). It can also happen via phone call, which is voice phishing (vishing). However, the latest sophisticated technique has been raised in phishing attacks. The link is hidden behind a QR code. Using QR codes for malicious purposes was relatively uncommon before COVID-19, but that all changed when the QR code was introduced. QR codes became a valuable intermediary for sharing URLs, including malicious ones. This creates an appealing new method of phishing as QR codes are now widely used (Sharevski et al., 2022).

Therefore, in collaboration with the ITC Department of PTSS, a Security Awareness Programme has been implemented to assess students' awareness and behaviour toward IT threats that have been decided to be performed, such as Phishing Attacks. The awareness programme will analyse awareness and behaviour based on the questionnaire. This paper aims to present a phishing Awareness Programme at PTSS and evaluate the awareness among students. This paper is shown as follows. Section 2 contains related work and is followed by the methodology section. Section 4 presents the results and discussion. This paper ends with a conclusion section.

## RELATED WORKS

Higashino (2019), in his work, has designed a system that can share information about targeted attack emails quickly and perform anti-phishing training between multiple organisations. This semi-auto system automatically detoxifies and anonymises attack emails an organisation receives and transmits them with various organisations. Each organisation can complete semi-automatic and continuous anti-phishing training using current attacking information. This system will simulate phishing messages via email.

In their project, CJ et al. (2018) developed a serious game to train enterprise users on phishing awareness called PHISHY. They chose this severe game because Serious Games is purposely designed to train users on a specific skill set. However, it is a computer-based game category mainly designed for training users

on a particular skill set. They are an essential opportunity for improving education. The primary goal of PHISHY was to provide phishing awareness training to enterprise users. There are three points that they focus on while educating the enterprise users, which are: - inspection as the method to identify phishing URLs, short URL familiarisation and brand name online searching to determine whether the website is legitimate or not.

Qasaimeh et al. (2021) investigated the variety of phishing email messages characteristic among Jordanians and determined Jordanian Internet users' awareness and knowledge about these threats. They performed an experiment based on an online survey. Demographic details like gender, age, education, Internet usage, and online banking social media accounts were collected. Besides that, information about perceptions towards message appearance to decide whether the message is trusted or not is also stored. Table 1 below describes the message criteria that have been used.

**Table 1**

*Description of message criteria*

| Message Criteria | Description |
|---|---|
| Known sender | The message body indicates the name of a specific individual that a recipient could attempt to contact |
| Unknown sender | The message body does not indicate the name of a specific individual that a recipient could attempt to contact |
| Images/ logos | The message includes graphical content that could help improve the appearance and emphasise brand identity, etc. |
| Untidy layout | The message is presented in an unprofessional manner (e.g. line breaks in the middle of sentences) |
| Language errors | The message contained spelling mistakes or grammatical errors. |
| URL/ link | The message seeks to encourage the receiver to follow a hyperlink. |

Burda et al. (2020) empirically studied human-computer interaction. They performed a tailored phishing technique. The tailored phishing technique is a single-stage attack of a 'hit-or-miss' nature. There are 747 respondents targeted in universities and large international companies. The user notification has been well established and exploited to attack delivery techniques. Then, the success rate of their phishing campaign evaluated how that technique affected them. As a result, the effect of 'traditional' attack techniques is widely mitigated in highly tailored phishing settings, suggesting that current user training and detection techniques may be off-target for more sophisticated attacks. However, they discovered that the method by

which the attack is delivered to the victim matters and can significantly increase up to three times the effect of the base attack.

Sykosch et al. (2020) introduced a framework that captures user responses to artefacts like phishing tests. They performed user behaviour analysis in response to controlled stimuli for IT security awareness assessment stimuli is something causing or regarded as causing a reply. The methodology to analyse the user behaviour is artefact, user reaction, ethics, framework, intervention design, and study design. The concept of real-world phishing tests is broadened to include artefact-based IT security awareness assessment. A framework capable of implementing this concept is introduced. A field study is conducted using this framework to investigate the behaviour of 259 people in response to 13 different artefacts in their familiar work environment. An intervention impact assessment of a standard intervention and a direct reliability assessment demonstrates the validity of generalised phishing tests to measure IT security awareness.

Gandhi (2017) examined whether informatics students have adequate information security awareness (ISA). The quantitative assessment used to demonstrate the measurement has three dimensions: knowledge, attitude, and behaviour. He employs 66 criteria: 30 classified as High, 26 as Medium, and the remaining as Low. The author also provides all dimensions in the medium category based on their overall average scores. These results are only partially satisfying because High is not the most dominant category. Using the detailed scores, the university can predict critical issues for information security in the future. University administrators can use these findings to provide relevant ISA programmes for informatics students. Six parameters have been used to determine the ISA among students. The parameters are Password management, Email use, Internet use, social media use, Laptop and mobile device and Information handling.

Moul (2019) is a User Service Department staff member at The Dickinson College. He indicated that the team has been working hard to educate the campus community on identifying and eliminating phishing traps. They initiated annual phishing quizzes with prizes, developed a phishing alerts page, held Cyber Security Awareness Month events, chose to give a "Avoid Phishing Alerts" presentation, added a warning banner to external incoming emails, and began implementing Microsoft Multi-Factor Authentication (MFA), primarily through the Microsoft Authenticator app.

## METHODOLOGY

The methodology is a necessary process to be implemented in any research that comes with more detail about the materials, procedure and respondents involved while completing and fulfilling the objectives of this pilot test for the awareness program. The focus of this methodology is on the phishing awareness level of the students being measured by the questionnaire provided. The central flow diagram of this PTSS Phishing Awareness is shown in Figure 1 below.

**Figure 1**

*PTSS Phishing Awareness Main Flow*


## Materials

Several materials are used in this test to identify awareness levels among the students. The primary materials were awareness videos containing the consequences of phishing and a Google form used for the pre-test and post-test questionnaires. The video awareness content was referred to and taken from videos based on the YouTube platform. Then, the chosen videos were edited by the Capcut application to improve the awareness content and included subtitles for better delivering phishing awareness to the respondents. There were twenty-two multiple-choice questions delivered to the respondents.

## Youtube

YouTube is a social media platform that allows people to share and watch videos. This research used the YouTube platform to search for related video content about phishing attacks. Three videos were selected and edited to make it straightforward to play with the respondents during the awareness program. The YouTube logo is shown in Figure 2 below.

**Figure 2**

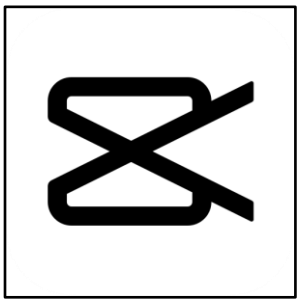
*The YouTube logo*


## Capcut application

In this pilot test, the videos downloaded from the YouTube platform were edited using the Capcut application—this Capcut application, commonly known as the video editor application that is easy to use by smartphone. The videos were cut into the crucial points and combined as one complete video about the Phishing attack. Figure 3 below shows the Capcut application logo.

**Figure 3**

*The Capcut logo*



## Google Form

Google Forms is one of the most effective online platforms for creating surveys, quizzes or questionnaires without any software or coding needed. Mobile or web browsers can make it. In this awareness project, Google Forms created the pre-test and post-test questions and shared them with the respondents. The pre-test and post-test questions were the same, excluding the demographic questions in the pre-test. This was to measure their understanding and knowledge level about Phishing. The Google Form logo is shown in Figure 4 below.

**Figure 4**

*The Google Form Logo*


The questions were created based on the video phishing awareness shown to the respondents. The list of questions implemented into the Google Form is shown in Table 2 below.

**Table 2**

*List of Questions*

| No. | Demographic Questions | Questions Based on Phishing Awareness Video |
|---|---|---|
| 1 | Please indicate your gender. | Select the correct definition for phishing. |
| 2 | How long do you spend your time using the Internet daily? | How does a Phishing attack work? |
| 3 | Do you install any virus protection software on | What is the incorrect purpose of the |

| | | |
|---|---|---|
| | your mobile phone? | Phishing attack? |
| 4 | Do you install any virus protection software on your laptop or computer? | Choose which statements lead to a Phishing attack. (Choose 3) |
| 5 | Have you heard of "Phishing?" Phishing is spelled with a "p h." | Is email a medium for Phishing attacks? |
| 6 | Have you ever received any message or email containing a link that said you are receiving something for free for any branded things discounted? | Select the correct option to detect a phishing attack. |
| 7 | Have you responded to the received link? | Ahmad received an email from his bank telling him that someone had his debit card information and that he needed to replace the card via a given link. What should Ahmad do? |
| 8 | Do you scroll over the link in the email and view the address before responding? | If you receive a message and realise it is a Phishing attack, is deleting the message correctly? |
| 9 | Do you search for information about the topic in a received message or email before responding? | If you fall for a phishing scam, what should you do to limit the damage? |
| 10 | How carefully do you read the email or message before responding? | What would you do if you got an email asking to reset your account password? |
| 11 | If you can remember, can you indicate why you clicked on the link? | The bank will email an appropriate link asking you to update your details, including online banking login credentials. |

The questions came with optional answers for the respondents to choose from. The results of this questionnaire were directly saved into the host of the Google Form as the respondents submitted their answers.

## Procedure

This pilot test was conducted face-to-face among participants gathered in a computer laboratory. Thirty respondents participating in this pilot test for the phishing awareness program were informed earlier about the test objectives to give them a rough visualisation of this test. The students or respondents were in the same class to ensure the integrity of the answers, as they were required to answer independently.

Firstly, they were given the Google Form link for the pre-test questions. All of them were given around 10 minutes to answer the questions without any discussion. Next, after completing the pre-test, the video on phishing awareness was played in that class by the projector on the screen provided, and they were asked to focus on the critical points in that video. The video explained phishing attacks, how to avoid phishing and what action needed to be taken if we got phishing. This video took 4 minutes to finish. After that, the

post-test link was given to the respondents, who needed to complete the question within 10 minutes. The questionnaire results are automatically recorded into the Google Form to be analysed. The outcomes from the pre-test and post-test were analysed and studied to measure the awareness level amongst the students about phishing attacks. In conclusion, this pilot test took less than 15 minutes to complete the session with participants.

### Respondents

The participants or the respondents in this pilot test were recruited from a similar educational background level, and their age range is 19 to 22 years old. Thirty respondents were involved in this phishing awareness pilot test of thirteen men and seventeen women. They joined this test as volunteers, and they had been informed of the confidentiality of these questionnaires. The respondents were given the links to the Google Form to answer the pre-test and post-test questions; they were advised to answer the test honestly.

## RESULT AND DISCUSSION

In this section, the results from the pre-test and post-test through the Google Form amongst selected respondents were discussed to measure their awareness level about phishing attacks through the scores they got. The total score for the test is 15 marks. Each question had different effects based on the question's difficulty. The demographic questions were neutral and did not count the score. The scores were calculated and then visualised into a suitable chart or diagram for analysis.

### Pre-test and Post-test Score

A pre-test is a test created to measure the general knowledge of the respondents at the initial state about phishing attacks. Because of that, they were required to answer without referring to any materials. The post-test is then used to measure the understanding or awareness level of the respondents after watching the video about phishing awareness. Both tests had ten different questions with a total score of 15 marks. The post-test results could also be the benchmark of the material effectiveness during the awareness program. The detailed results score of the pre-test and post-test are shown in Table 3 below. The respondents' identities were labelled in numbering.

**Table 3**

*Pre-test and Post-test Result Score for Each Respondent*

| Respondent No. | Pre-Test Score | Post-Test Score |
|---|---|---|
| 1 | 6 | 8 |
| 2 | 12 | 15 |
| 3 | 7 | 13 |
| 4 | 7 | 14 |
| 5 | 10 | 11 |
| 6 | 5 | 15 |

| | | |
|---|---|---|
| 7 | 15 | 13 |
| 8 | 7 | 7 |
| 9 | 6 | 6 |
| 10 | 8 | 12 |
| 11 | 2 | 10 |
| 12 | 4 | 10 |
| 13 | 5 | 13 |
| 14 | 6 | 12 |
| 15 | 5 | 13 |
| 16 | 10 | 14 |
| 17 | 8 | 15 |
| 18 | 6 | 11 |
| 19 | 15 | 15 |
| 20 | 6 | 13 |
| 21 | 9 | 14 |
| 22 | 11 | 15 |
| 23 | 11 | 15 |
| 24 | 3 | 6 |
| 25 | 11 | 14 |
| 26 | 9 | 11 |
| 27 | 15 | 15 |
| 28 | 4 | 12 |
| 29 | 5 | 10 |
| 30 | 14 | 15 |

Based on Table 3 above, the pre-test and post-test scores were visualised in the column chart in Figure 5 above. The x-axis is classified as the respondent's identities, and the y-axis belongs to the score values. Table 4 below shows the score level for every respondent categorised into three groups.

**Table 4**

*Score Level for Every Respondent*

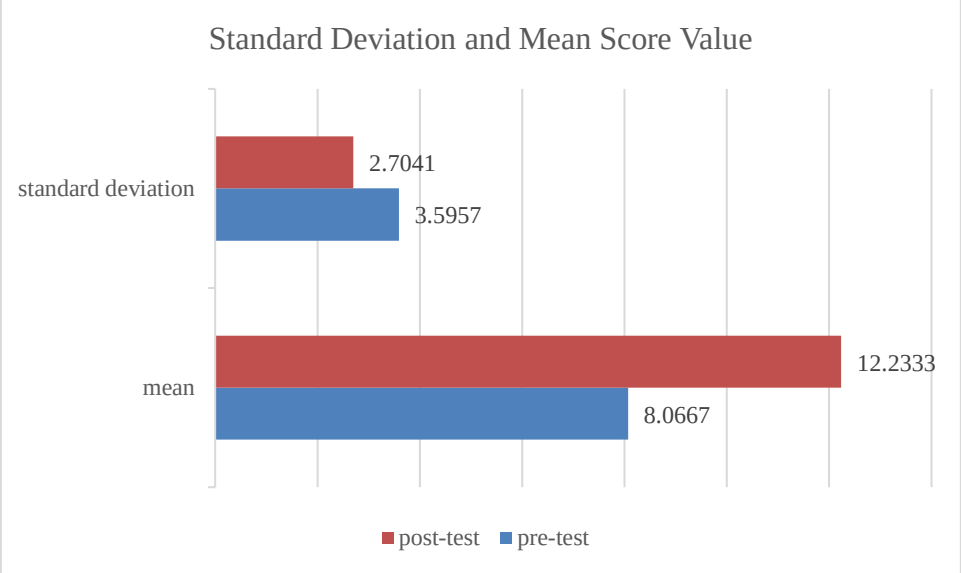
| *Score Level for Each Respondent* | Score Ranges | Number of Respondents in Pre-test | Number of Respondents in Post-test |
|---|---|---|---|
| Low | 0 - 5 | 8 | 0 |
| Medium | 6 - 10 | 14 | 7 |
| High | 11 - 15 | 8 | 23 |

The results were analysed into three different score ranges, which were 0 to 5, 6 to 10, and 11 to 15, to categorise their score level. 0 to 5 was classified as a low level of awareness, 6 to 10 was medium, and 11 to 15 labelled as a high level of awareness about phishing. The results are shown in Table 4 above.
For pre-test results, the highest score gained was 15 marks, and the lowest was 2. The highest respondents' score ranges between 6 to 10 marks, with fourteen respondents. In the post-test, the highest score gained 15 marks, and the lowest was six. For the score ranges, the highest number of respondents was between 11 and 15 marks, with twenty-three respondents. This showed the increment of respondent numbers in a high level of awareness and zero number of respondents under a low level. The chart showed that each respondent's score increased in the post-test compared to the pre-test. These results concluded that 90% of the respondents improved after being enlightened about phishing through the materials, as they could answer better in the post-test.

The mean calculated from the pre-test was 8.0667, and the post-test was 12.2333. For standard deviation, it was 3.5957 on the pre-test, and the post-test was 2.7041. This calculated mean and normal deviation value is visualised in a chart in Figure 6 below. Mean and standard deviation were crucial to analyse the pattern of overall results between the pre-test and post-test. The mean score was the average value of the awareness level gained from the respondents and the standard variation used to calculate the concentration of the results on means. The higher the mean leads to lower standard deviation values. Based on the mean value in Figure 6, the mean value became higher during the post-test compared to the pre-test, and the standard deviation became lower compared to the pre-test results. This proved that the post-test means and standard deviation improved awareness level scores.

**Figure 6**

*Standard Deviation and Mean Score Value*




Based on the tables and charts analysis, the score of most respondents increased, and one respondent's score remained the same in post-test results compared to the pre-test results. The respondent who got full marks in the pre-test was predicted to know about the phishing attack. The rest of the respondents could be classified as unfamiliar with the phishing attack. However, in post-test results, they were improved in choosing correct answers after watching the video. The number of respondents who got full marks also increased from one to two people in the post-test. These pre-and post-test results showed that the material used for the phishing awareness program was adequate based on improving their score in answering post-test questions.

Even though the score results of the post-test were increased and got positive feedback from respondents, several respondents still got scores below 10, which was medium level. This could be a factor of time given for the respondents to understand the video was too short as the video explanation was too fast, and some of them may have problems understanding English subtitles. The lack of time could cause the respondents to face difficulties interpreting the new information effectively. Other than that, the language barrier could be one of the problems for them to digest the video content quickly. As a recommendation, the material can be improved by doing another test with the addition of other language subtitles based on respondents' background or by increasing the duration time for them to understand the video by playing the video twice or slowing the speed. However, overall, the results prove that the current material used was generally effective based on the score gained in the post-test results. In conclusion of this discussion and effects, the higher the score earned, the higher the respondents' understanding of the phishing attacks concept based on the video context shared.

## CONCLUSION AND FUTURE WORKS

Referring to the observation and analysis of the results obtained from the pre-test and post-test respondents, there was positive feedback as the test scores improved. The test score improvement can be summarised as the objectives of this pilot test are achieved. The awareness about phishing created was effective and successful in identifying and evaluating student awareness. Thus, this program can be launched to

determine the awareness of all Politeknik Tuanku Syed Sirajuddin (PTSS) students about phishing attacks. Several improvement ideas can be given for this awareness program for future work. Each student's awareness and behaviour level in PTSS can be measured according to suitable timing. Besides that, in this pilot test, we can gather input from respondents at a similar average age, but in the future, it is hoped to get feedback from various ageing levels and add up staff awareness. The number of respondents can also be added from 30 to 60 to get more accurate test results. As for this study, the material provided for the respondents is using video. For enhancement in the future, we would suggest implementing a phishing simulation using either email or a messaging system to determine students' behaviour towards phishing. Reinforcement of knowledge also should be made frequently so that students will not forget about the possible threats to occur. The impact of an awareness program can be measured based on these criteria. An example of awareness level is that students must be able to identify phishing emails, while the example of behaviour level is that students must detect and report phishing emails to the appropriate personnel or department.

## ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

## REFERENCES

Burda, P., Chotza, T., Allodi, L., & Zannone, N. (2020). We are testing the effectiveness of tailored phishing techniques in industry and academia. Proceedings of the 15th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3407023.3409178

CJ, G., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018). PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness. Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play. https://doi.org/10.1145/3270316.3273042

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Computing Surveys, 54(8), 1–35. https://doi.org/10.1145/3469886

Gandhi, A. (2017). Quantitative Assessment of Information Security Awareness on Informatics Students in a University. Proceedings of the 2017 International Conference on Information Technology - ICIT 2017. https://doi.org/10.1145/3176653.3176728

Higashino, M. (2019). A Design of an Anti-Phishing Training System Collaborated with Multiple Organizations. Proceedings of the 21st International Conference on Information Integration and Web-Based Applications & Services, iiWAS2019. https://doi.org/10.1145/3366030.3366086

Moul, K. A. (2019). Avoid Phishing Traps. 2019 ACM SIGUCCS Annual Conference on - SIGUCCS '19. https://doi.org/10.1145/3347709.3347774

Qasaimeh, M., Al-Manaseer, H., Al-Manaseer, H., & Alghanim, F. (2021). Status Update on Phishing Emails Awareness: Jordanian Case. The 7th International Conference on Engineering & MIS 2021. https://doi.org/10.1145/3492547.3492565

Sharevski, F., Devine, A., Pieroni, E., & Jachim, P. (2022). Phishing with Malicious QR Codes. 2022 European Symposium on Usable Security, EuroUSEC '22. https://doi.org/10.1145/3549015.3554172

Sykosch, A., Doll, C., Wübbeling, M., & Meier, M. (2020). You are generalising the phishing principle. Proceedings of the 15th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3407023.3409205