The impact of short-term memory on phishing detection ability and password behaviour

Joakim Kävrestad[1,2,*], Muhammad Abbas Khan Abbasi[1], Márton Tarczal[1] and Marcus Nohlberg[1]

[1]School of Informatics, University of Skövde, Sweden
[2]School of Engineering, Jönköping University, Sweden

Abstract

Cybersecurity is a socio-technical discipline which is dependent on the interplay between users and devices, and the organizations where this interplay takes place. Previous research has shown that the interplay between users and devices is highly affected by the cognitive abilities of users. This is prominent in cybersecurity, which requires users to make security-aware decisions when, for instance, reading emails and decide which emails are legitimate and which emails constitute phishing. Research further suggests that decision-making is dependent on memory ability, which is the focus of this research. In this study, we investigate the impact of short-term memory on phishing detection ability and password behaviour. A web survey was used to collect quantitative data from a large sample of respondents. The survey was distributed on social media platforms and 93 participants completed the survey. The results indicate a positive correlation between short-term memory scores and both password detection ability and password behavior.

Keywords

cybersecurity, behaviour, memory, phishing, password

1. Introduction

OECD describes that the world is becoming more digital at a rapid pace [1]. As a natural consequence, cybercrime continues to steadily increase [2]. Consequently, individuals and organizations must find ways to protect themselves from cybercriminals. Such protection involves both technical, organizational, and user-oriented methods, called controls. Technical controls include firewalls and authentication procedures that control what devices and control what users can and cannot do. Organizational controls include policies and strategies, and user-oriented controls aim to support users towards secure behavior through, for instance, training. The present research focuses on user-oriented cybersecurity, and the rationale is that the current research reflects that user behavior is extensively exploited by cybercriminals [3, 4]. One example is phishing where an attacker attempts to trick users into doing something users should not do using email. Phishing can be used to trick a user into installing ransomware,

The 9th International Conference on Socio-Technical Perspectives in IS (STPIS'23) 27.-28.10. Portsmouth, UK

*Corresponding author.
joakim.kavrestad@ju.se (J. Kävrestad); muhammad.abbas.khan.abbasi@his.se (M. A. K. Abbasi); tarczal.marton@gmail.com (M. Tarczal); marcus.nohlberg@his.se (M. Nohlberg)
0000-0001-5962-9995 (M. Nohlberg)

giving up sensitive information, etc. Another example is exploiting poor password habits to gain access to a system. This can include, for example, guessing user passwords in hope that a user selected a weak password.

Cybersecurity can be seen as a sociotechnical system that is dependent on technology, users, and the organization. As described by Mumford (2006), a socio-technical approach does not only assume that a system consists of technology, users and an organization, but emphasizes that the interplay between those entities is crucial for the success of the system [5]. In the context of cybersecurity, it is crucial to have a strategic plan, supported by relevant technology and based on the needs of users and organizations. Consider, for instance, user authentication, which is paramount to ensure that only authorized users can access digital resources [6]. An effective authentication system needs to ensure that users can access the resources they need and nothing more, in a timely manner. This requires a strategic plan that outlines the resources that should be made available and to what user groups. Then, technical measures to realize the plan are needed. Finally, users should be educated on how and why to efficiently use the system. For the system to be successful, all those parts must be aligned. Should the plan be too vague, technical implementation becomes difficult. If the technical implementation is difficult to use, the user will struggle to use it correctly [7]. Indeed, a socio-technical approach is argued to lead to increased stakeholder value and user acceptance of technology [8].

The management teams or IT departments are usually in charge of the technical and organizational security aspects, while the users are expected to take on a large responsibility by selecting secure passwords, avoiding phishing, etc. It is well-known that it is difficult to get users to use tools, features, and procedures designed to ensure cybersecurity. Consequently, the usability of such tools has been the focus of much research, and it is evident that the usability of tools, features, and procedures is a factor that determines which tools and features users decide to adopt or not [9, 10, 11, 12]. Furthermore, recent studies describe cognitive workload and fatigue as possible inhibitors of secure behavior [13, 14]. The rationale is that activities such as password creation or phishing detection require reasoning, planning, memory, etc., which demands cognitive resources from the user. When these resources are depleted, users' ability to engage in secure behavior is reduced [15].

The purpose of the present study is to investigate how the ability of users to detect phishing and adopt strong passwords is impacted by short-term memory capacity. Short-term memory is, in this paper, defined as a persons ability to recall information recently presented to them. Phishing and password, while only a subset of user responsibilities were selected in this research, as they are exploited very frequently by cybercriminals [16]. Although different cognitive functions have been discussed in the cybersecurity domain [3], this research is focused on short-term memory. The rationale is that short-term memory has been found to influence decision making, which is believed to be important for cybersecurity behavior [17, 18]. The purpose of this research is to be an initial study on how cybersecurity behavior is impacted by cognitive abilities.

Data were obtained using an online survey that measured the participant's ability to identify phishing emails, password behavior, and short-term memory. The results indicate a positive correlation between short-term memory scores and both phishing detection ability and password behaviour. To the best of our knowledge, this is the first study that explicitly measures the impact of short-term memory capacity on cybersecurity behavior. Although the sample size in this study (n = 93) is a limitation, it is a first step that researchers can build on in continued investigations into how cybersecurity behavior is affected by cognitive abilities.

The next section will describe the research methodology used for this research. Then, the results of the survey will be presented before they are discussed and concluded with suggestions for future work.

2. Methodology

With the purpose of collecting quantitative data from a large sample of respondents, a web-based survey was used. The following section will, in turn, discuss the hypotheses developed in this research, describe how the survey was developed and distributed, and how the collected data were analyzed.

2.1. Hypothesis development

Recent research describes password behavior and phishing as two key areas of user behavior with respect to cybersecurity [19, 20]. Industry reports provide a similar view, where phishing is commonly discussed as the most common cyberattack [16, 21, 22]. Likewise, exploiting weak passwords is a common practice used by attackers seeking to gain unauthorized access to computer systems [23, 24]. Consequently, password behavior and phishing are two critical areas of investigation.

There are several previous studies which suggest that cognitive abilities have an impact on cybersecurity behavior [13, 14]. Cognitive ability includes the ability of a person to reason, plan, solve problems, etc. [25]. It also affects a person's memory and ability to concentrate [26]. This research has chosen to focus on short-term memory with the motivation that it affects a person's memory [18].

Given the justification above, two sets of hypotheses were developed. The first hypothesis and corresponding null hypothesis are:

> **H1**: A person with higher memory ability will display a better ability to identify phishing emails.
> **H1$_{\mathbf{null}}$**: Memory ability is not associated with the ability to detect phishing emails.

The second hypothesis and corresponding null hypothesis are:

> **H2**: A person with higher memory ability will display better password behavior.
> **H2$_{\mathbf{null}}$**: Memory ability is not associated with password behaviour.

2.2. Instrumentation

A survey was developed for this research and consisted of four blocks of questions each containing five questions:

- Block 1: Questions about the participants' background.
- Block 2: Questions measuring the participants' ability to identify phishing.

- Block 3: Questions measuring the participants' password behavior.
- Block 4: Question measuring the participants' short-term memory.

The questions in block one, which intended to introduce the survey with a few demographic questions, appeared to the participants in a fixed order. Blocks two to four were presented in fixed order, but the question order within those blocks was randomized to minimize question order bias [27].

In block 2, each question displayed an email and the participants were asked to decide if it was legitimate or phishing. The survey was designed so that participants could hover over links to display link targets and interact with the email as they would in a webmail client. An example is provided in Figure 1. All emails were phishing and the five phishing scenarios included an email regarding a SWEDBANK transaction alert redirecting to a malicious link, a Netflix account-related email with a malicious link, an iCloud account storage issue email with a malicious link, the University finance office email regarding payment of a fee containing a malicious attachment, and a Firefox account login alert with a malicious link. Te were selected to represent phishing of medium difficulty.

In Block 3, the questions were presented as account registration forms to the following five websites:

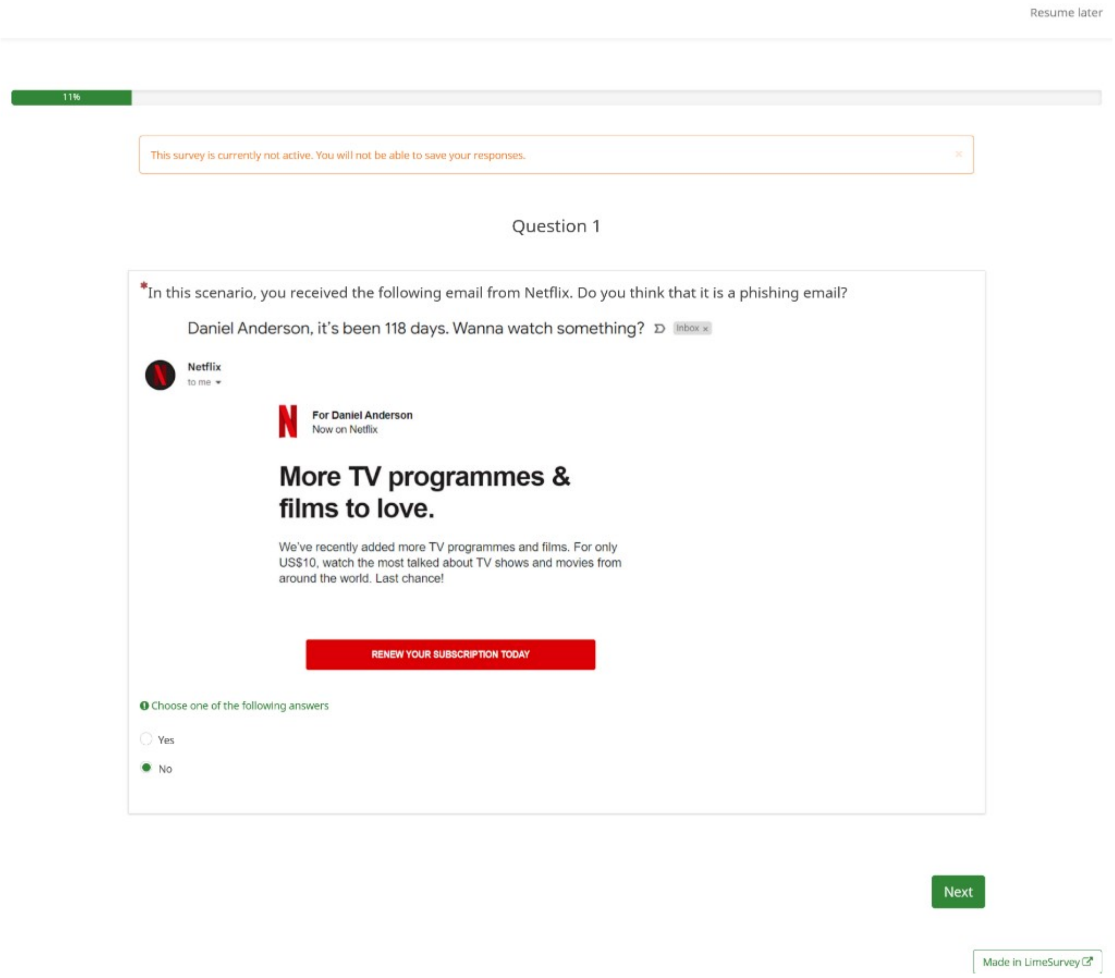
- Citibank
- Google
- Instagram
- LinkedIn
- 7-eleven

For each question, participants were asked to pick the password that was closest to the one they would personally create for the website in question. An example question is provided in Figure 2. The participants could choose from the following passwords:

- 1YellowCatCrossedTheRoad?
- aZtG@497$/#
- KYbeR1&
- 1986March8!
- Password123!

The first two passwords are considered secure in this research since they are sufficiently long and/or complex [28]. The other passwords are considered insecure because they are too short or easy to guess.

Block four intended to measure the participants' short-term memory by presenting five questions about what the participants had experienced during block 3. This approach mimics a free recall test which is a popular measurement of explicit memory [29]. The survey was developed by the research team and validated in a pilot test intending to ensure that participants interpreted the survey in the intended way and that all participants interpreted the survey in the same way [30]. During the pilot, nine participants were asked to do the survey monitored by a member of the research team and asked to speak out their thoughts. The survey was updated following insights from the pilot.



This survey is currently not active. You will not be able to save your responses.

Question 1

*In this scenario, you received the following email from Netflix. Do you think that it is a phishing email?

Daniel Anderson, it's been 118 days. Wanna watch something?

For Daniel Anderson
Now on Netflix

More TV programmes & films to love.

We've recently added more TV programmes and films. For only US$10, watch the most talked about TV shows and movies from around the world. Last chance!

Choose one of the following answers

○ Yes

● No

Figure 1: Example of a phishing scenario used in the survey.

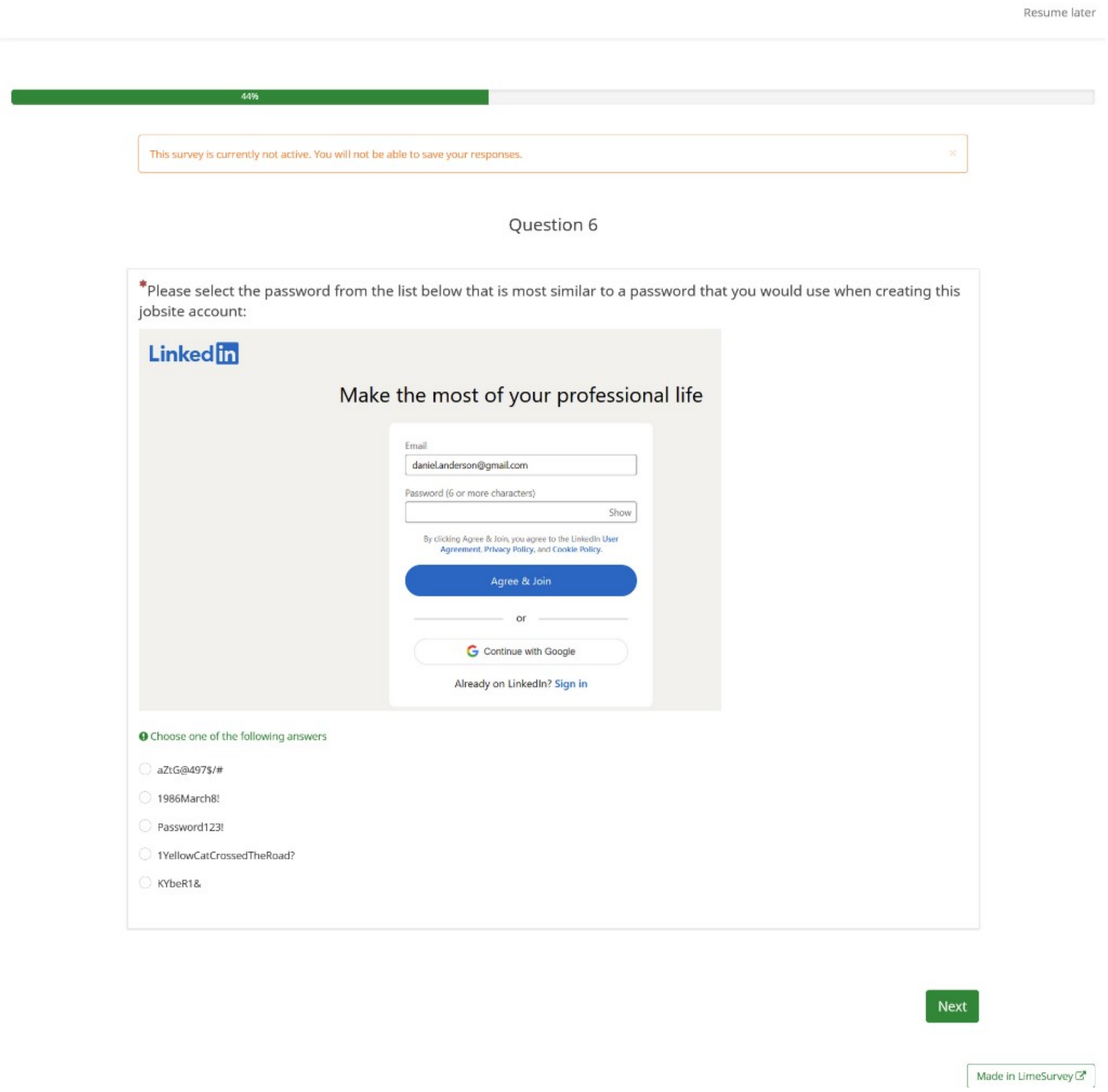
2.3. Execution

The survey was anonymous and was preceded by an informed consent form. Ethical approval was not necessary for this research according to Swedish regulations [31]. The online survey platform Limesurvey was used to conduct the survey[1].The survey was distributed using social media platforms.

2.4. Data Analysis

The gathered data was analyzed using SPSS version 27. Responses to demographic questions are presented to provide an overview of the data sample. The questions in blocks two to four are used to create index variables that are used for further analysis. Each question had correct

[1] https://www.limesurvey.org/



This survey is currently not active. You will not be able to save your responses.

Question 6

*Please select the password from the list below that is most similar to a password that you would use when creating this jobsite account:

Make the most of your professional life

Email: daniel.anderson@gmail.com

Password (6 or more characters)

By clicking Agree & Join, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.

Already on LinkedIn? Sign in

Choose one of the following answers

- ○ aZtG@497$/#
- ○ 1986March8!
- ○ Password123!
- ○ 1YellowCatCrossedTheRoad?
- ○ KYbeR1&

Figure 2: Example of a password scenario used in the survey.

and incorrect response options. Each participants index variable was computed as the number of correct answers within each block.

Index variables were used to test the established hypotheses using correlation tests. Correlation tests measure the correlation between two variables and return a value between 1 and -1. A positive value indicates a positive correlation, while a negative value indicates a negative correlation [32]. Pearson's rank correlation was used for variables with normal distribution, and Spearman's rho was used in other cases [32, 33]. Normality was assessed using the Shapiro-Wilk test [34]. In this study, the conventional 5% significance level was used.

3. Results and Analysis

A link to the survey was distributed on social media platforms and 93 participants completed the survey. This section will provide an overview of the characteristics of the sample before describing the responses to the questionnaire. It ends with testing of the established hypotheses.

3.1. Sample characteristics

Out of the 93 respondents 45 identified as female while 48 identified as male. 53 respondents lived in Pakistan, 21 lived in Sweden, and the remaining 19 were spread between another ten countries. As seen in Table 1, the age distribution in the sample is skewed toward younger adults with only a handful of respondents over the age of 45.

Table 1
Age distribution among respondents

Age	Participants
18-24	34
25-34	28
35-44	21
45-54	6
55-64	2
65+	2

Participants were asked to rate their own IT competence by selecting one of four levels of competence. Most of the participants rate themselves as good IT users, as seen in Table 2 which also presents the description of the levels as presented to the participants.

Table 2
IT competence among respondents

Skill level	Participants
Below Average user - I always have problems with IT, and always seek help from someone in IT matters	9
Average user - I often have problems with IT, and feel that I need help with things that others can do on their own	25
Expert user - I use IT without any larger problems, but need help time-to-time	31
Professional - Works within, has a degree within, or studies within IT	28

3.2. Descriptives

Following the demographic questions, the participants received five emails and asked if the email was legitimate or not. The five phishing scenarios included an email regarding a SWEDBANK transaction alert redirecting to a malicious link, a Netflix account-related email with a malicious link, an iCloud account storage issue email with a malicious link, the University finance office email regarding payment of a fee containing a malicious attachment, and a Firefox account

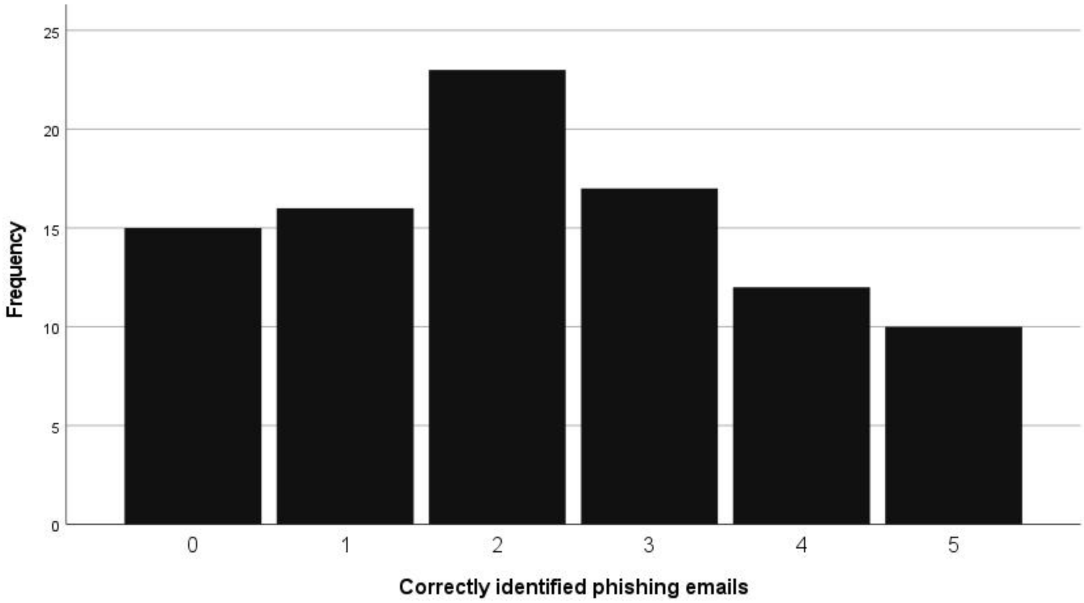


Figure 3: Participant scores for phishing email identification (out of five)

login alert with a malicious link. Table 3 shows how many participants who correctly identified each email as phishing.

Table 3
Participant results for phishing questions

Phishing scenario	Correct answers (count)	Correct answers(%)
Swedbank transaction alert	41	44%
Netflix account email	39	42%
iCloud storage issue	37	40%
University fee email	47	51%
Firefox login alert	47	51%

Furthermore, an index variable reflecting how many correct answers each participant had was computed. As seen in Figure 3, only 10 (11%) participants correctly classified all emails as phishing, and the median result was two correct responses.

The participants were then presented with different account registration pages and asked to pick which password, out of five provided examples, most closely resembled one that they would choose for a new account on the website in question. Two passwords were considered strong and three were considered weak. Table 4 lists the included websites and the number of participants who selected one of the strong passwords for each website.

An index variable was created and reflects the number of secure passwords each participant selected. The median value was 2 and, as shown in Figure 4, the data demonstrate that a large number of participants selected only good (n=19(20%)), or only bad (n=26(31%)). However,

Table 4
Participant results for password questions

Website	Participants selecting strong passwords (count)	Strong passwords(%)
Citibank	45	48%
Google	42	45%
Instagram	38	41%
LinkedIn	39	42%
7-eleven	33	35%

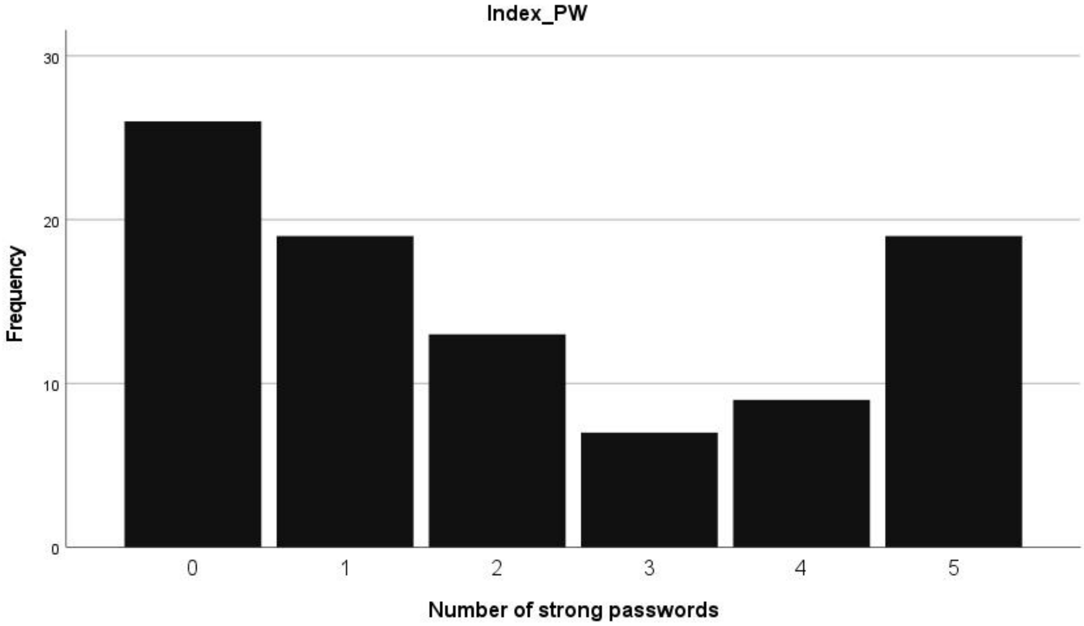


Figure 4: Participant scores for password behaviour (out of five)

48 (52%) participants selected different passwords for different sites, suggesting that they are selecting passwords based on how important they think it is to keep the respective accounts secure.

Finally, participants were asked five questions about the previous questions in the survey. The purpose of these questions was to see how much of the survey the participants remembered. The number of correct responses was collected in an index variable that is the measure of the short-term memory of the participants used in the remaining analysis. An overview of the results is presented in Figure 5.

3.3. Hypothesis testing

The last step in the analysis was to test the hypotheses previously developed to test for correlations between short-term memory and the ability to identify phishing and password behavior. The index variables were subjected to Shapiro-Wilks normality test, which suggested that the

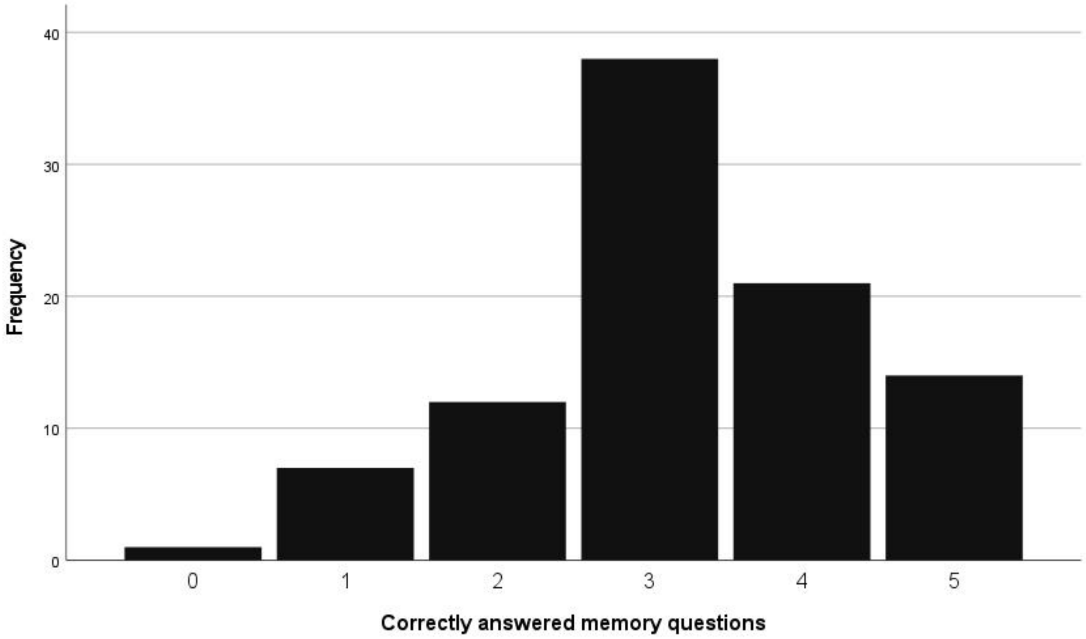


Figure 5: Overview of answers to memory questions (out of five)

data do not follow a normal distribution. Consequently, Pearson's rank correlation was not appropriate to use and Spearman's rho was used instead.

The correlation between short-term memory and the ability to identify phishing was first tested. Spearman's rho returned a correlation coefficient of .238, and a p-value of .022. Thus, the tests show a statistically significant correlation between the variables and the following hypothesis is supported by the data:

> **H1**: A person with higher memory ability will display a better ability to identify phishing emails.

The correlation between short-term memory and password behavior was then tested. Spearman's rho returned a correlation coefficient of .207, and a p-value of .046. Thus, the tests show a statistically significant correlation between the variables and the following hypothesis is supported by the data:

> **H2**: A person with higher memory ability will display better password behavior

4. Conclusions and Future Work

This research aimed to investigate whether the ability of users to detect phishing and adopt strong passwords is impacted by short-term memory capacity. Data was collected using an online survey, and subjected to statistical analysis that showed a correlation between the ability of users to detect phishing and short-term memory capacity as well as password behavior and short-term memory. It could be seen that the correlation coefficients, while significant, were around 0.2 which signifies quite weak correlations [32]. In light of previous research, this is quite unsurprising. Both phishing detection ability and password behavior are affected by numerous factors such as previous training [35], the use of other security functions [36], and risk perception [37]. However, this research suggests that short-term memory is a predictor of the ability to identify phishing and password behavior. This information can, for example, be useful in developing tailored cybersecurity awareness efforts and policies. For instance, care could be taken to evaluate policies from a memory-requirement perspective. One could perhaps limit how password behavior is impacted by memory by allowing for passphrases without complexity requirements or implement multi-factor authentication and allow for simpler password. Such an approach has been suggested to improve users password behaviour in previous research [38].

In addition to the results discussed in the previous paragraph, this paper provides data about users' ability to detect phishing and password behavior. Looking at the participants' ability to detect phishing, presented in Figure 1, it can be seen that only ten out of 93 participants correctly classified the five emails presented as phishing. In fact, the mean result was two correctly identified phishing emails out of five, which means that the median participant was tricked in three out of five attempts. Consequently, this paper adds to the existing body of research which states that users struggle to correctly identify phishing [39]. A possible limitation, however, of the study design is that the participants are presented with constructed phishing emails rather than faced with actual phishing attempts as part of their daily life. In a real life situation, it is likely that a lot of phishing is simply not relevant to the recipient and therefore discarded as spam. In example, a user who is not a LinkedIn user would not be likely to be tricked by a LinkedIn related phishing attempt. The results of this research reflects the participants ability to detect phishing when forced to do that for every email included in the study and should be interpreted as such.

The common approach to phishing detection has historically been training and awareness [40]. Training does, however, only focus on improving one socio-technical dimension, the user. A socio-technical approach to phishing detection should perhaps also consider how organizational and technical aspects can be changed to help users detect phishing, possibly with better results. Organizational culture has, fro instance, been associated with cybersecurity behaviour in the past [41]. The results regarding password behavior suggest that there are three groups of users; one group that always creates strong passwords, one group that never creates strong passwords, and one group that uses different levels of password strength for different accounts.

The purpose of this research was to be a first step in the investigation of how user cognitive abilities impact cybersecurity behavior. The main limitation in this work comes from the data sample, which was acquired using social media and was of a limited size (93 participants), and the results should be interpreted with this in mind. The rationale for this sampling method was that sampling using social media is easy and cost efficient. Nevertheless, the results in this research motivate further research in the area. Such research could be survey-based and then include larger samples gathered using non-probability sampling techniques. Future research could also look at other aspects of cybersecurity behavior and / or other cognitive abilities.

References

[1] OECD, Hows Life in the Digital Age?, 2019. URL: https://www.oecd-ilibrary.org/content/publication/9789264311800-en.

[2] CyberEdge, 10th annual Cyberthreat Defense Report, 2023. URL: https://cyber-edge.com/cdr/.

[3] S. Chaudhary, V. Gkioulos, S. Katsikas, Developing metrics to assess the effectiveness of cybersecurity awareness program, Journal of Cybersecurity 8 (2022) tyac006.

[4] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, H. N. Basim, Cyber security awareness, knowledge and behavior: A comparative study, Journal of Computer Information Systems 62 (2022) 82–97.

[5] E. Mumford, The story of socio-technical design: Reflections on its successes, failures and potential, Information systems journal 16 (2006) 317–342.

[6] C. P. Pfleeger, S. L. Pfleeger, J. Margulies, Security in computing, fifth edition ed., Prentice Hall, Upper Saddle River, NJ, 2015.

[7] R. Shay, S. Komanduri, A. L. Durity, P. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, L. F. Cranor, Designing password policies for strength and usability, ACM Transactions on Information and System Security (TISSEC) 18 (2016) 1–34.

[8] G. Baxter, I. Sommerville, Socio-technical systems: From design methods to systems engineering, Interacting with computers 23 (2011) 4–17.

[9] R. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, M. Savvides, Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption., in: USEC'15: Workshop on Usable Security, 2015, pp. 1–10.

[10] A. Whitten, J. D. Tygar, Why johnny can't encrypt: A usability evaluation of pgp 5.0., in: USENIX Security Symposium, volume 348, 1999, pp. 169–184.

[11] B. Liu, J. Lin, N. Sadeh, Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?, in: Proceedings of the 23rd international conference on World wide web, 2014, pp. 201–212.

[12] K. M. Ramokapane, A. C. Mazeli, A. Rashid, Skip, skip, skip, accept!!!: A study on the usability of smartphone manufacturer provided default features and user privacy, Proceedings on Privacy Enhancing Technologies 2019 (2019) 209–227.

[13] R. Gutzwiller, J. Dykstra, B. Payne, Gaps and opportunities in situational awareness for cybersecurity, Digital Threats: Research and Practice 1 (2020) 1–6.

[14] A. Reeves, P. Delfabbro, D. Calic, Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue, SAGE Open 11 (2021).

[15] A.-M. Horcher, G. P. Tejay, Building a better password: The role of cognitive load in information security training, in: 2009 IEEE International Conference on Intelligence and Security Informatics, IEEE, 2009, pp. 113–118.

[16] A. Sfakianakis, C. Douligeris, L. Marinos, M. Lourenço, O. Raghimi, ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends, ENISA, 2019.

[17] M. R. Hatfield-Eldred, R. L. Skeel, M. P. Reilly, Is it random or impulsive responding? the

effect of working memory load on decision-making, Journal of Cognitive Psychology 27 (2015) 27–36.

[18] J. A. Dykstra, S. R. Orr, Acting in the unknown: the cynefin framework for managing cybersecurity risk in dynamic decision making, in: 2016 International Conference on Cyber Conflict (CyCon US), IEEE, 2016, pp. 1–6.

[19] A. A. Moustafa, A. Bello, A. Maurushat, The role of user behaviour in improving cyber security management, Frontiers in Psychology 12 (2021) 561011.

[20] F. B. Fatokun, Z. A. Long, S. Hamid, J. O. Fatokun, C. I. Eke, A. Norman, Gamifying cybersecurity knowledge to promote good cybersecurity behaviour, Journal of Computing Technologies and Creative Content (JTec) 7 (2022) 25–34.

[21] techopedia, 50+ Cybersecurity Statistics for 2023 You Need to Know – Where, Who What is Targeted, 2023. URL: https://www.techopedia.com/cybersecurity-statistics.

[22] CompTIA, Top 50 Cybersecurity Statistics, Figures and Facts, 2023. URL: https://connect.comptia.org/blog/cyber-security-stats-facts.

[23] D. O. Dastane, The effect of bad password habits on personal data breach, International Journal of Emerging Trends in Engineering Research 8 (2020).

[24] onelogin, Six Types of Password Attacks How to Stop Them, 2023. URL: https://www.onelogin.com/learn/6-types-password-attacks.

[25] M. Karwowski, J. C. Kaufman, The creative self: Effect of beliefs, self-efficacy, mindset, and identity, Academic Press, 2017.

[26] K. Oberauer, H.-M. Süß, R. Schulze, O. Wilhelm, W. W. Wittmann, Working memory capacity—facets of a cognitive ability construct, Personality and individual differences 29 (2000) 1017–1045.

[27] D. J. Mingay, M. T. Greenwell, Memory bias and response-order effects, Journal of Official Statistics 5 (1989) 253–263.

[28] L. A. Loos, M. E. Crosby, Cognition and predictors of password selection and usability, in: Augmented Cognition: Users and Contexts: 12th International Conference, AC 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, July 15-20, 2018, Proceedings, Part II, Springer, 2018, pp. 117–132.

[29] H. L. Roediger, J. D. Karpicke, Learning and memory, in: K. Kempf-Leonard (Ed.), Encyclopedia of Social Measurement, Elsevier, New York, 2005, pp. 479–486. URL: https://www.sciencedirect.com/science/article/pii/B0123693985005405. doi:https://doi.org/10.1016/B0-12-369398-5/00540-5.

[30] N. H. Chowdhury, M. T. Adam, G. Skinner, The impact of time pressure on cybersecurity behaviour: a systematic literature review, Behaviour & Information Technology 38 (2019) 1290–1308.

[31] S. R. Council, Good Research Practice, 2017. URL: https://www.vr.se/english/analysis/reports/our-reports/2017-08-31-good-research-practice.html.

[32] H. Akoglu, User's guide to correlation coefficients, Turkish journal of emergency medicine 18 (2018) 91–93.

[33] M.-T. Puth, M. Neuhäuser, G. D. Ruxton, Effective use of spearman's and kendall's correlation coefficients for association between two measured traits, Animal Behaviour 102 (2015) 77–84. URL: https://www.sciencedirect.com/science/article/pii/S0003347215000196. doi:https://doi.org/10.1016/j.anbehav.2015.01.010.

[34] K. R. Das, A. Imon, A brief review of tests for normality, American Journal of Theoretical and Applied Statistics 5 (2016) 5–12.

[35] K. Singh, P. Aggarwal, P. Rajivan, C. Gonzalez, Training to detect phishing emails: Effects of the frequency of experienced phishing emails, in: Proceedings of the human factors and ergonomics society annual meeting, volume 63, SAGE Publications Sage CA: Los Angeles, CA, 2019, pp. 453–457.

[36] J. Kävrestad, J. Zaxmy, M. Nohlberg, Analyzing the usage of character groups and keyboard patterns in password creation, Information & Computer Security (2020).

[37] K. Parsons, A. McCormac, M. Butavicius, L. Ferguson, Human factors and information security: individual, culture and security environment, Technical Report, 2010.

[38] J. Kävrestad, M. Lennartsson, M. Birath, M. Nohlberg, Constructing secure and memorable passwords, Information & Computer Security 28 (2020) 701–717.

[39] M. Alsharnouby, F. Alaca, S. Chiasson, Why phishing still works: User strategies for combating phishing attacks, International Journal of Human-Computer Studies 82 (2015) 69–82.

[40] B. Reinheimer, L. Aldag, P. Mayer, M. Mossano, R. Duezguen, B. Lofthouse, T. Von Landesberger, M. Volkamer, An investigation of phishing awareness and education over time: When and how to best remind users, in: Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), 2020, pp. 259–284.

[41] G. Bansal, Got phished! role of top management support in creating phishing safe organizations, MWAIS 2018 Proceedings 6 (2018).