TOWARDS THE DESIGN AND EVALUATION OF CLICKBAIT EDUCATION CONTENT: LEVERAGING USER MENTAL MODELS AND LEARNING SCIENCE PRINCIPLES

A. Shrestha, A. Flood, B. Hackler, A. Behfar, M.N. Al-Ameen

Utah State University (UNITED STATES)

Abstract

Clickbait refers to sensationalized or misleading post on social networking sites (e.g., Facebook) that can trick users into clicking on malicious links. Clickbait is often used in cyberattacks, especially to conduct `social engineering attacks' that direct users to malicious websites, resulting in disclosure of users' personal information or installing malicious software (i.e., malware). Thus, clickbait has become a major security concern with the recent boom in social media use. Therefore, security education has become necessary more than ever for the safe and secure use of social media, where there is dearth in security education literature to explore how we could leverage the learning science principles, and the mental models (thought processes about how something works) of users in designing educational contents. We begin to address this gap in our work, where we conducted two online studies over Amazon Mechanical Turk (MTurk), recruiting a total of 834 participants. Our first study aimed to understand the existing mental models of clickbait among social media users; we derived six mental models from our study, which led to the design of security education materials (treatment condition) integrating user mental models with learning science principles. We then conducted our second online study to evaluate treatment condition with the baseline educational content. Our findings denote the efficacy of leveraging user mental models in security education design, and unveil the potentials of integrating learning science principles into the design process. Based on our findings, we provide guidelines for future education research in these directions.

Keywords: clickbait education, mental models, learning science.

1 INTRODUCTION

Social engineering attacks are the most common security attacks primarily performed to exploit the weakest link in online security- humans [1], [2]. Such attacks typically involve some form of psychological manipulation, tricking users into clicking on links that direct them to websites stealing sensitive information or containing malware [3], [1], [2]. In fact, 98% of cyberattacks rely on social engineering, and 90% of data breach incidents target the human element to gain access to sensitive information [4]. Further, 84% of Americans have experienced some form of social engineering attacks [5]. Phishing, a typical social engineering attack, is carried out primarily through email, tricking users to click on links and has caused considerable problems in online security of end-users [6]. While email is still one of the most used online tools, social networking sites have recently become an integral part of life for many people. Clickbait is a social engineering attack primarily performed through social networking sites with the use of sensationalized or misleading posts that trick users into clicking on malicious links [1], [7], [8], [9]. However, a large portion of social media users lack knowledge and awareness about clickbait [10], [11]. In light of the growing social media usage, we focus our research on clickbait education.

In clickbait education, we first look at the learning science principles to guide our designs (see §4.1) [12], [13], [14], [15]. While learning science principles are proven to improve the understanding of a concept, many works have also recommended contextualizing information to a group to enhance understandability while maintaining interest [16], [17]. However, such recommendations have yet to be implemented for security education. One of the reasons may be that the users are inherently tricky to group through methods of demographics (sex, age, location) due to the variance in their understanding of a concept. Therefore, mental models [18] that represent a user's understanding of a concept present a viable method for categorizing users to provide information contextualized to them [19], [20].

We address this gap in our work, where we investigate the following research questions: (**RQ1**): *How can we integrate mental models with learning science principles to build content for clickbait education?* (**RQ2**): *How does mental model-based clickbait education compare to only using learning science principles?*

To integrate mental models with learning science principles (RQ1), we first need to identify the existing mental models of social media users about clickbait. Therefore, we conduct a study with 770 participants on MTurk, asking them about their understanding of clickbait. We derive six mental models from our analysis. The mental model designs contain the same learning science principles used in our baseline design (an article using graphical representation). We evaluate these designs with another online study with 64 participants (based on power analysis for large effect size) on MTurk.

Our findings from the online study show that mental models can be effective in security education and integrate well with learning science principles. Taken together, our findings provide valuable insights into users' mental models of clickbait, the translation of mental models into contextualized education designs, and their effectiveness in enhancing the understanding of concepts by users. Finally, our findings point to a set of recommendations, including exploring mental models as a viable education tool in future research.

2 BACKGROUND

Clickbait is often used in social engineering attacks to trick users into clicking links that direct them to malicious websites, including sites spreading ransomware, viruses, Trojans, adware, and spyware [7], [8], [9]. Clickbait also helps in the propagation of misleading information [21], which has previously led to chaos among the general public and has created tangible problems in public health [22] and safety [23]. In this section, we first discuss why users are still vulnerable to click on clickbait and then discuss our motivation to use mental model-based education in our study.

2.1 Vulnerability of Users towards Clickbait

Users still encounter clickbait regularly despite the several attempts from social media platforms to limit it [24], [25]. Prior literature has provided us with the knowledge regarding why clickbait is effective- clickbait works by creating a curiosity gap where users feel rewarded with answers when they click on it [26]. Studies, however, show that users need education and awareness to identify clickbait and understand the importance of avoiding it [10], [11]. Unfortunately, the effectiveness of clickbait is further enhanced when the clickbait post aligns with the beliefs of the users [27] and when the presented false information is novel [28]. In addition, key findings from several works reported that users are vulnerable to the misleading and sensationalized information provided in clickbait [29], [30]. The vulnerability of the users to clickbait presents a need for clickbait education to help them understand the consequences of clickbait and the criticality of avoiding it.

2.2 Mental Model based Contextualization

Several works have suggested that contextualizing information to users can enhance the understanding of a concept [16], [17], [31], [32]. Many factors may facilitate the contextualization of information, including sex, age, and location. However, users grouped based on such factors may be inherently different due to the variance in their understanding of a concept. However, mental models provide a feasible solution for grouping users to effectively contextualize information based on the user's existing understanding of a concept. To that end, several studies [33], [34], [35] have worked on the identification of mental models about concepts such as the Internet and security tools. The study of Kang et al. [33] explored users' mental models of the Internet, where participants convey how they view and make sense of Internet technology. Another study [34] identified mental models to understand how users perceive the working of encryption. Oates et al. [35] revealed users' mental models of privacy from the illustrations created by users about what privacy means to them. However, little study to date explored the method of leveraging mental models to develop educational content contextualized to the users based on their understanding of a concept. To the best of our knowledge, our study is the first to identify users' mental models of clickbait and leverage it to create contextualized educational content.

3 MENTAL MODEL STUDY

In line with our *RQ1*, we first conducted a study to understand the existing users' mental models of clickbait. The study was approved by the Institutional Review Board at our university. We then leverage the identified mental model and integrate it with learning science principles to create our educational content (see §4).

3.1 Method

We conducted a study with 770 participants through Amazon Mechanical Turk, asking them, "What do they understand by the term Clickbait?". Participants had to be 18 or older and live in the United States or Canada to participate in our study. We removed 48 responses from our analysis due to three reasons- 1) lack of understandability (For instance, "Clickbait is the important is a post."), 2) extreme shortness (For instance, "clickbait"), and 3) irrelevance (For instance, "I think it is a tv show"). We performed thematic analysis on the responses of the remaining 722 participants [36], [37], [38]. Two independent researchers coded each response, developed codes, and assigned a mental model. The inter-coder reliability in the thematic analysis was 88.78%.

Our participant pool included 434 male, 326 female, and 19 non-binary users. The age range of the participants varied from 18-24 years old to above 65 years old. Five hundred ninety-eight of our participants were white, 56 were Asian, 41 were African American, 21 were Hispanic or Latino, and 57 were mixed or other.

3.2 Mental Model Identification

Based on our analysis, we extracted the users' mental models of clickbait. We observed that users' mental models overlap partially, whereas new ideas may be added to this partial overlap. Therefore, we conducted a mental model decomposition to derive the basic building blocks of the users' mental models (termed decomposed mental models). We found that users make sense of clickbait in terms of how it works and what it aims to achieve. Our in-depth analysis revealed a set of mental models under each sensemaking category.

We identified three decomposed mental models on users' perceptions of how clickbait works. 52.63% of users believed that clickbait worked by exaggerating either the thumbnail or the headline, which is termed as *Sensationalization of Information*. 64.95% of users believed that there is some trickery, lying, or non-factual information involved in clickbait. Such an understanding of clickbait is termed as *Deception Mechanism*. 9.14% participants thought clickbait works by hiding the most critical information from the users, which we termed as *Information Camouflage*.

We identified three mental models under the users' sensemaking of a clickbait's goal. 58.72% of participants believed clickbait's goal is to get more users to visit a website to generate traffic, which we termed as *Traffic Increment*. 13.69% of participants thought that clickbait's goal was to get financial benefit either by getting clickthrough traffic or showing ads on the websites they lead to. Such a mental model was termed as *Financial Benefit*. 8.86% participants believed that the goal of clickbait was to harm the users by introducing malicious software to their devices which we termed as *Detrimental Effect*.

These mental models are not mutually exclusive as users may have a combination of them. Users made sense of clickbait through multiple lenses creating an aggregated mental model formed based on some combination of the six mental models. For instance, a user may believe that clickbait works by both exaggerating information and presenting non-factual information.

4 THEORETICAL FRAMEWORK BEHIND DESIGNS

We evaluate two design variations for security education in our study. First, the baseline design is an article about clickbait based on learning science principles. Second, the treatment design is the integration of mental models with the same learning science principles. Below, we will first discuss the learning science principles we have used in both baseline and treatment design and then the integration of mental models with these learning science principles in the treatment design.

4.1 Learning Science Principles

Principle of *dual code effects* [39], [13] states that information is remembered better when delivered in multiple modes. Our designs use graphical presentations, textual explanations, and examples to provide multiple delivery modes. Since computer security topics often involve abstract concepts, graphical representations are particularly powerful for security education [14], [40]. They are also easier to remember than text because of the *picture superiority effect* [14], [41]. Therefore, we use graphical presentation in the two design variations that we use in our study (see Fig. 1). Since we are using multiple modes of delivery, we follow the principles of *segmentation* [12] to present the information in segments in both the baseline article and the treatment designs (see Fig. 1). The segmentation of

information aligns well with *cognitive load reduction* [15], [42] as the difficulty in processing the provided information by a person is considerably reduced.

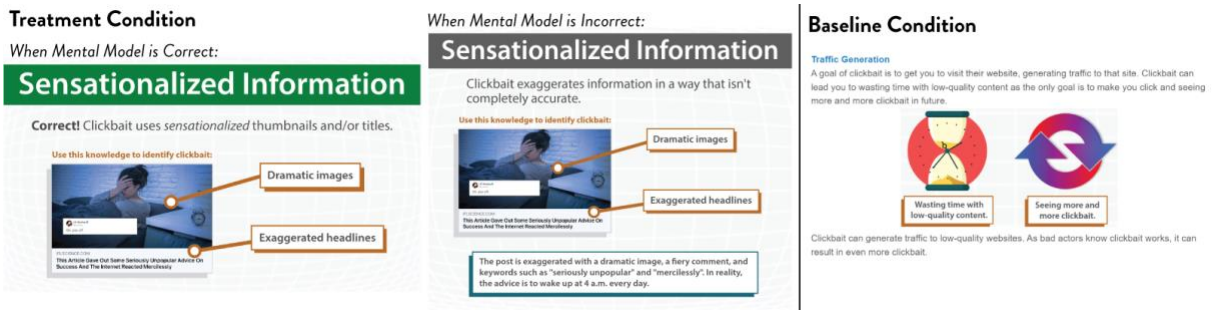

Figure 1. Treatment and Baseline conditions used in the study

To arrange the information provided in the designs, we connect related text and graphics together to adhere to the *contiguity effect* [39] for better learning (see Fig. 1). The presentation of associated ideas contiguously complements the *coherence effect* [43] as a well-connected representation of the concept is formed through contiguity. Further, the principle of *discovery learning* [44] states that people have trouble discovering important principles on their own without careful guidance. Therefore, we provide guidance in our designs to use the knowledge they acquire in a step-by-step approach. We provide users with knowledge about how clickbait works (e.g., through deception) and then guide them in using that knowledge to identify clickbait (e.g., by looking for unbelievable thumbnails and headlines) (see Fig. 1}). In doing that, we also combine the *conceptual and procedural learning* as we provide the users with the correct concepts of clickbait and explain the procedural steps of applying that to identify clickbait.

4.2 Integrating Mental Models into Education Content

We use the six identified mental models in §3 to create a total of 12 educational designs. Since users lose interest when provided information is contained within their mental models, we develop two variations of the educational design for each of the six mental models (see Fig. 1). If a user has correct knowledge about a mental model, we provide a short summary and applicability of that knowledge (Variation 1). In contrast, if a user does not have the correct knowledge, we provide detailed conceptual information along with its applicability (Variation 2). Such an approach contextualizes the education content allowing the participants with the correct mental model to get affirmation while quickly going through the educational material without losing interest. In contrast, the participants with the incorrect mental model will be provided with detailed education on clickbait's working and goal.

5 DESIGN EVALUATION STUDY

In line with our *RQ2*, we conducted an online study comparing our treatment design using mental models with our baseline design to understand the impact of mental models on online security education. The study is approved by the Institutional Review Board at our university.

5.1 Method

We conducted a study with 64 participants (32 for treatment and 32 for baseline) through Amazon Mechanical Turk. For our study, we designed a survey in Qualtrics. Participants were first asked to read an Informed Consent Document (ICD). After agreeing to the ICD, the participants were first given a quiz on clickbait to understand their existing knowledge (mental model). They were then either presented with the baseline design- an article about clickbait using learning science principles without contextualization through mental models, or the treatment design- contextualized educational designs based on their responses to the clickbait quiz (mental models), which used the same learning science principles.

Participants were then asked to rate the provided education content on a 7-point Likert scale (-3: strongly disagree, 3: strongly agree). They were explicitly asked to evaluate the design based on its *Perspicuity*, *Efficiency*, and *Usefulness* [45] using a validated scale (UEQ+ [46]). We also asked them about the effectiveness of design in grabbing their attention (*Attention*) by adding custom questions similar to prior studies [47], [48]. In order to understand the knowledge gained by the participants, we added additional custom questions about applying their understanding in the future (*Application*), making them cautious (*Cautious*), increasing their knowledge on clickbait (*Knowledge*), and increasing their ability to identify

clickbait (*Identification*). Then, the participants were asked an open-ended question to provide their thoughts and feedback on the presented content. This was followed by the identical quiz the participants took before the educational content was presented to them to measure their knowledge gain. They then answered a set of demographic questions and were compensated with USD 2.0 for completing the study, which took an average of 10-12 minutes.

Table 1. Demographic Information of Participants in the Evaluation Study (N=Number of Participants)

Demographic	*Demographic Group*	*N*
Gender	Male	25
	Female	39
Age range	25-29 years old	1
	30-34 years old	10
	35-39 years old	14
	40-44 years old	14
	45-49 years old	6
	50-54 years old	6
Age range (continued)	55-59 years old	6
	60-64 years old	4
	Above 65 years old	3
Race	White	56
	Asian	1
	Black/African American	2
	Native American	1
	Mixed Race	4

The demographic information of the 64 participants who took part in the study is available in Table 1.

We used non-parametric Mann-Whitney U-test for the analysis since our study was between subjects and our data was not normally distributed. We also report the parameters in our study as above average or below average based on the recommendations from the UEQ handbook. We performed thematic analysis [36], [37] on open-ended responses from participants. The inter-coder reliability in the thematic analysis was 89.06%.

5.2 Design Evaluation Results

We start this section with an evaluation of knowledge gained by the participants from the education content and then compare the treatment and baseline designs based on the parameters described in §5.1. For consistency, we use these terms throughout this section based on the frequency of comments in participants' responses: *a few* (0-10%), *several* (10-25%), *some* (25-40%), *about half* (40-60%), *most* (60-80%), and *almost all* (80-100%).

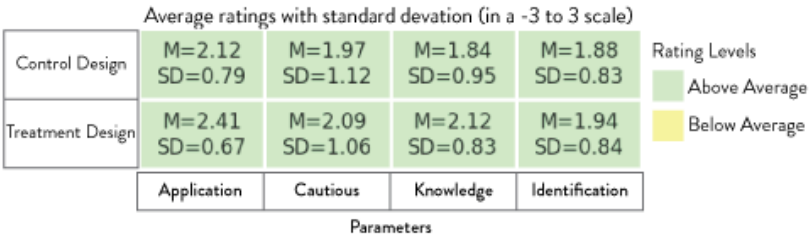

Figure 2. Average ratings in knowledge parameters for the treatment and the baseline designs

5.2.1 Knowledge Gain from the Educational Content

Since the baseline and the treatment designs both used learning science principles for clickbait education, they effectively increased users' knowledge about clickbait. For the baseline condition, the average score on the quiz increased from 19.68 to 23.06 points (+1 for correct answers and -1 for incorrect) before and after presenting the educational article. The average improvement on the quiz was 3.37 points. For the treatment condition, the average score on the quiz increased from 18.09 to 21.68 points before and after presenting the designs. This resulted in an average improvement of 3.59 points. When comparing the quiz scores before and after showing educational content, both baseline and treatment designs significantly improved the knowledge gained by the users (p<.001 for both conditions). This is supported by the average ratings for *Knowledge, Identification,* and *Application*, as both of these conditions were rated above average (see Fig. 2). As the knowledge increased, the participants also rated the two conditions above average in the *Cautious* parameter (see Fig. 2). The

average scores for all these four parameters are around two on a -3 to 3 scale, which is considered an excellent rating.

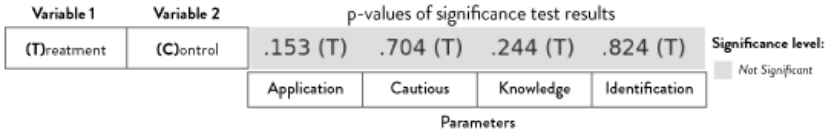

Figure 3. Significance test results comparing treatment and baseline designs in knowledge parameters

When comparing the knowledge gained between treatment and baseline condition, there was a lack of significant difference (p=.745) even though the average improvement was higher for treatment designs. We see similar results in *Knowledge, Identification, Application,* and *Cautious* parameters, as all scores are higher for the treatment design. However, no significant difference exists for any of the measures (see Fig. 3).

The effectiveness of both baseline and treatment designs in increasing user knowledge about clickbait can be attributed to the learning science principles, as evidenced by the open-ended responses. Some participants liked the examples and the information provided through multiple modes (text and graphics) in the explanation of clickbait. One participant talking about baseline said, *"I thought it gave great examples and a detailed description of why it was clickbait. It was easy to follow."* Similarly, the combination of conceptual and procedural knowledge worked well, as several participants found the knowledge about the identification of clickbait useful. One participant mentioned, *"There was a lot to learn from the article. It had specific examples and gave me guidelines to identify clickbait. I will save it to refer to in the future."* Another participant said, *"They pointed out specific things from clickbait article/ads which made me more aware and confident when trying to identify clickbait. I thought the designs were clear and easy to understand."*

Moreover, the segmentation and contiguous presentation of information were effective, as about half of the participants found the educational content concise and organized. One participant said, *"I think the article was quick and easy to understand. I liked that it included images and would still be useful to someone who wanted to scan the article and get information quickly because of how it is organized and the important information is prominent."*

5.2.2 Impact of Integrating Mental Models with Learning Science

Open-ended responses highlighted the effectiveness of contextualizing the designs based on the mental models. Some participants liked the provision of education based on their quiz answers. One participant mentioned, *"I liked that it took my answers from the test and put them into an easy-to-understand format. I like that it showed the headlines from earlier as an example of what clickbait is."* Some participants also liked the affirmation provided when their answers were correct. One participant said, *"I thought the icons and check marks, along with the examples, were useful in helping to hold my attention."*

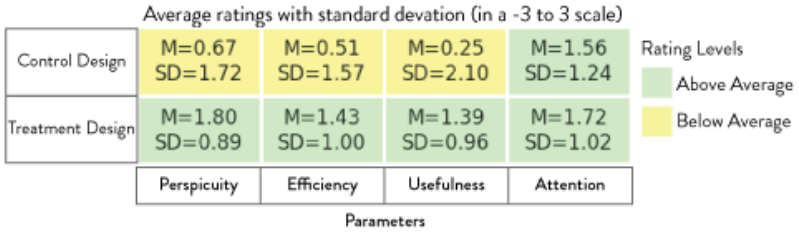

Figure 4. Average ratings in user experience parameters for the treatment and the baseline designs

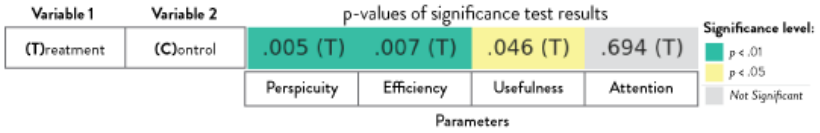

Figure 5. Significance test results comparing treatment and baseline designs in user experience

Further, the treatment designs integrating the mental models with learning science principles were rated above average on four out of five parameters- *Perspicuity, Efficiency, Usefulness,* and *Attention* (see Fig. 4). However, the baseline was rated above average only in terms of *Attention* (see Fig. 4). While both treatment and baseline performed well in increasing users' knowledge, treatment performed

significantly better than the baseline in terms of *Perspicuity* (p<.01), *Efficiency* (p<.01), and *Usefulness* (p<.05) (see Fig. 5).

Regarding *Perspicuity*, the treatment design was rated more than one point higher than the baseline on average (see Fig. 4). Open-ended responses support that mental model-based education leads to higher understandability of the content as users can focus on the information that they do not already know. About half of the participants mentioned the clarity and simplicity of the treatment design and how it helps convey critical points they need to understand. One participant said, *"I think they are pretty simple and easily get across the information they intend to. This would be a good way to introduce clickbait to someone that may not be aware of what it is like school kids or non-technically adept people. I thought the images were straightforward, making the concept easy to understand and spot."*

For *Efficiency*, treatment scored almost a point higher than the baseline on average (see Fig. 4). While both designs used images to improve the speed of gaining information, providing information based on mental models helped the users gain only the relevant information, increasing the overall speed. In the open-ended responses, some participants mentioned pinpointing information in the treatment design. One participant said, "I felt they were clear and concise. Not too much information nor too little. The pinpointed info at the main parts of the articles were very helpful."

In terms of perceived *Usefulness*, treatment scored more than one point higher than the baseline (see Fig. 4). Some participants found the selective provision of information based on their mental models more valuable than the baseline article. One participant said, *"They were easy to understand and helpful. I always thought clickbait was annoying but harmless, but this helped to educate me. Overall, I appreciated it. There's not much to say. The designs were clear and informative, so that was great."* Another participant mentioned, *"I thought it was really informative and useful. I liked the presented designs and I think they would be useful and help people avoid clickbait."*

6 DISCUSSION

Our findings show the effectiveness of integrating mental models with learning science principles in clickbait education. Based on these findings, we discuss the possible implications of our study and provide considerations to take into account in future designs.

Learning Science Principles in Education. Prior works point to the vulnerability of users in identifying and understanding the importance of avoiding clickbait [10], [11]. However, using learning science principles to educate users about clickbait can help increase user knowledge. The effectiveness of learning science principles is apparent from the above average ratings for the knowledge parameters and significant knowledge gain for both baseline and treatment designs (see §5.2.1). The study of Al-Ameen et al. [49] analyzed online security training modules through the lens of learning science and recommended strategies (e.g., graphical presentation and user interaction) for an online training module to comply with the principles of learning science. Our study and literature together point to the direction that learning science principles can be an effective tool in security education in the future.

Mental Models: Avenues for Exploration. Prior studies [33], [34], [35] argue that a system should be adapted to varying mental models. However, there is a need to explore contextualizing educational content based on users' mental models. To this end, our findings show promise in leveraging users' mental models for online security education in general. However, mental models are not a standalone principle and must be incorporated with theories and principles for effective education. In this study, we used learning science principles together with the mental models of clickbait. The positive findings from our study highlight that such an approach can be fruitful, leading us to recommend future works to explore incorporating mental models beyond the learning science principles used in our study. Further, our work also provides directions for future studies to explore the use of mental models in broader educational contexts, including password creation and sharing, phishing, and malware.

Limitations and Future Work. Our study was limited to participants from the U.S. and Canada. Recent HCI studies [23], [50], [51], [52], [53] highlight the importance of looking beyond Western contexts, where the societal and cultural background, literacy rate, public policy, economic condition, and infrastructural support could impact users' perceptions and behavior. Since mental models have worked well in the Western context, future studies should involve participants from diverse geographic regions, including developing countries, to understand and design personalized and effective mental model based educational content for online security concepts.

7 CONCLUSION

The designs we presented in the study provide the directions for future works in creating educational content for online security concepts, in general, to support users through awareness and education in following a safer and more secure behavior. Based on our recommendations, there are still multiple avenues for future work incorporating a mental model-based education approach. We conclude our work by highlighting our positive findings on the effectiveness of our treatment design approach in increasing the educational content's understandability, efficiency, and usefulness.

ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1949699.

REFERENCES

[1] H. Aldawood and G. Skinner, "Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal," *International Journal of Security (IJS)*, vol. 10, no. 1, pp. 1, 2019.

[2] F. A. M. Khiralla, "Statistics of cybercrime from 2016 to the first half of 2020," *Int. J. Comput. Sci. Netw.,* vol. 9, no. 5, pp. 252–261, 2020.

[3] Social engineering (security), Accessed 20 December, 2023. Retrieved from https://en.wikipedia.org/wiki/Social_engineering_(security).

[4] Understanding and Preventing Social Engineering Attacks, Accessed 20 December, 2023. Retrieved from https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engineering-attacks.

[5] Report: 84% of U.S. citizens have experienced social engineering..., Accessed 20 December, 2023. Retrieved from https://venturebeat.com/security/report-84-in-us-have-experienced-social-engineering-attacks.

[6] Phishing, Accessed 20 December, 2023. Retrieved from https://en.wikipedia.org/wiki/Phishing.

[7] K. Rides, Clickbait Malware Sites, Accessed 20 December, 2023. Retrieved from https://www.linkedin.com/pulse/clickbait-malware-sites-kris-rides.

[8] E. M. Redmiles, N. Chachra and B. Waismeyer, "Examining the Demand for Spam: Who Clicks?," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pp. 1-10, 2018.

[9] J. Avery, M. Almeshekah and E. Spafford, "Offensive deception in computing," in *International Conference on Cyber Warfare and Security*, pp. 23, 2017.

[10] Y. L. Huang, K. Starbird, M. Orand, S. A. Stanek and H. T. Pedersen, "Connected through crisis: Emotional proximity and the spread of misinformation online," in *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*, pp. 969-980, 2015.

[11] J. Urakami, Y. Kim, H. Oura and K. Seaborn, "Finding Strategies Against Misinformation in Social Media: A Qualitative Study," in *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pp. 1-7, 2022.

[12] R. E. Mayer and R. Moreno, "Nine ways to reduce cognitive load in multimedia learning," *Educational psychologist*, vol. 38, no. 1, pp. 43–52, 2003.

[13] R. Moreno and A. Valdez, "Cognitive load and learning effects of having students organize pictures and words in multimedia environments: The role of student interactivity and feedback," *Educational Technology Research and Development*, vol. 53, no. 3, pp. 35–45, 2005.

[14] A. Paivio, *Mind and its evolution: A dual coding theoretical interpretation*, Mahwah, NJ: Lawrence Erlbaum Associates, Inc, 2006.

[15] F. Paas and L. Kester, Learner and information characteristics in the design of powerful learning environments, *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition*, vol. 20, no. 3, pp. 281–285, 2006.

[16] M. Kaptein, P. Markopoulos, B. De Ruyter and E. Aarts, "Personalizing persuasive technologies: Explicit and implicit personalization using persuasion profiles," *International Journal of Human-Computer Studies*, vol. 77, pp. 38–51, 2015.

[17] B. Liu, M. Schaarup Andersen, F. Schaub, H. Almuhimedi, S. Zhang, N. Sadeh, A. Acquisti and Y. Agarwal, "Follow my recommendations: A personalized privacy assistant for mobile app permissions," in *SOUPS 2016-Proceedings of the 12th Symposium on Usable Privacy and Security*, pp. 27-41, 2016.

[18] Mental Models and User Experience Design, *Nielsen Norman Group*, Accessed 20 December, 2023. Retrieved from https://www.nngroup.com/articles/mental-models.

[19] P. N. Johnston-Laird, *Mental models: Towards a cognitive science of language, inference, and consciousness*, Harvard University Press, 1983.

[20] I. Young, *Mental models: aligning design strategy with human behavior*, Rosenfeld Media, 2008.

[21] E. Zeng, T. Kohno and F. Roesner, "Bad news: Clickbait and deceptive ads on news and misinformation websites," in *Workshop on Technology and Consumer Protection*, pp. 1-11, 2020.

[22] Y. Zhang, N. Suhaimi, N. Yongsatianchot, J. D. Gaggiano, M. Kim, S. A. Patel, Y. Sun, S. Marsella, J. Griffin and A. G. Parker, "Shifting Trust: Examining How Trust and Distrust Emerge, Transform, and Collapse in COVID-19 Information Seeking," in *CHI Conference on Human Factors in Computing Systems*, pp. 1-21, 2022.

[23] F. Vasudeva and N. Barkdull, "WhatsApp in India? A case study of social media related lynchings," *Social Identities*, vol. 26, no. 5, pp. 574–589, 2020.

[24] Y. Roth and D. Harvey, How Twitter is fighting spam and malicious automation, 26 June, 2018. Retrieved from https://blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.

[25] N. Gleicher, Removing coordinated inauthentic behavior from China, 19 August, 2019. Retrieved from https://about.fb.com/news/2019/08/removing-cib-china.

[26] K. Scott, "You won't believe what's in this paper! Clickbait, relevance and the curiosity gap," *Journal of pragmatics*, vol. 175, pp. 53–66, 2021.

[27] J. Allen, C. Martel and D. G. Rand, "Birds of a feather don't fact-check each other: Partisanship and the evaluation of news in Twitter's Birdwatch crowdsourced fact-checking program," in *CHI Conference on Human Factors in Computing Systems*, pp. 1-19, 2022.

[28] S. Wineburg and S. McGrew, "Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information," *Teachers College Record*, vol. 121, no. 11, pp. 1–40, 2019.

[29] C. Geeng, S. Yee and F. Roesner, "Fake news on Facebook and Twitter: Investigating how people (don't) investigate," in *Proceedings of the 2020 CHI conference on human factors in computing systems*, pp. 1-14, 2020.

[30] G. Pennycook, J. McPhetres, B. Bago and D. G. Rand, "Beliefs about COVID-19 in Canada, the United Kingdom, and the United States: A novel test of political polarization and motivated reasoning," *Personality and Social Psychology Bulletin*, vol. 48, no. 5, pp. 750–765, 2022.

[31] P. Dumaru, A. Shrestha, R. Paudel, C. Haverkamp, M. B. McClain and M. N. Al-Ameen, "'… I have my dad, sister, brother, and mom's password": unveiling users' mental models of security and privacy-preserving tools," *Information & Computer Security*, 2023.

[32] R. Paudel, A. Shrestha, P. Dumaru and M. N. Al-Ameen, ""It doesn't just feel like something a lawyer slapped together." Mental-Model-Based Privacy Policy for Third-Party Applications on Facebook," in *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing*, pp. 298-306, 2023.

[33] R. Kang, L. Dabbish, N. Fruchter and S. Kiesler, ""my data just goes everywhere:" user mental models of the internet and implications for privacy and security," in *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, pp. 39-52, 2015.

[34] J. Wu and D. Zappala, "When is a tree really a truck? exploring mental models of encryption," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS)*, pp. 395-409, 2018.

[35] M. Oates, Y. Ahmadullah, A. Marsh, C. Swoopes, S. Zhang, R. Balebako and L. F. Cranor, "Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 4, pp. 5–32, 2018.

[36] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[37] R. E. Boyatzis, *Transforming qualitative information: Thematic analysis and code development,* sage, 1998.

[38] A. Shrestha, R. Paudel, P. Dumaru and M. N. Al-Ameen, "Towards Improving the Efficacy of Windows Security Notifier for Apps from Unknown Publishers: The Role of Rhetoric," in *International Conference on Human-Computer Interaction,* pp. 101-121, 2023.

[39] R. E. Mayer, *Introduction to multimedia learning*, Cambridge University Press, 2014.

[40] L. Zhang-Kennedy, S. Chiasson and R. Biddle, "The role of instructional design in persuasion: A comics approach for improving cybersecurity," *International Journal of Human-Computer Interaction*, vol. 32, no. 3, pp. 215–257, 2016.

[41] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor and J. Hong, "Teaching Johnny not to fall for phish," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, pp. 1–31, 2010.

[42] J. J. G. Van Merriënboer, L. Kester and F. Paas, "Teaching complex rather than simple tasks: Balancing intrinsic and germane load to enhance transfer of learning," *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition,* vol. 20, no. 3, pp. 343–352, 2006.

[43] R. Kozma, "Reflections on the state of educational technology research and development," *Educational technology research and development*, vol. 48, no. 1, pp. 5–15, 2000.

[44] P. A. Kirschner, J. Sweller and R. E. Clark, "Why minimal guidance during instruction does not work: An analysis of the failure of constructivist, discovery, problem-based, experiential, and inquiry-based teaching," *Educational psychologist*, vol. 41, no. 2, pp. 75–86, 2006.

[45] M. Schrepp, A. Hinderks and J. Thomaschewski, "Applying the user experience questionnaire (UEQ) in different evaluation scenarios," in *International Conference of Design, User Experience, and Usability*, pp. 383-392, 2014.

[46] M. Schrepp and J. Thomaschewski, "Handbook for the modular extension of the User Experience Questionnaire," in *Mensch & Computer*, pp. 1-19, 2019.

[47] L. Zhang-Kennedy, S. Chiasson and R. Biddle, "Password advice shouldn't be boring: Visualizing password guessing attacks," in *2013 APWG eCrime Researchers Summit*, pp. 1-11, 2013.

[48] V. Zimmermann, K. Marky and K. Renaud, "Hybrid password meters for more secure passwords–a comprehensive study of password meters including nudges and password information," *Behaviour & Information Technology*, vol. 42, no. 6, pp. 1–44, 2022.

[49] M. N. Al-Ameen, E. A. Watkins, B. Lowens, F. Roesner, S. Mcgregor and K. Caine, "Evaluating Online Security Training for Journalists Through the Lens of Learning Science," in *Advances in Security Education (ASE) 2017 Workshop, USENIX,* 2017.

[50] M. N. Al-Ameen, H. Kocabas, S. Nandy and T. Tamanna, ""We, three brothers have always known everything of each other": *A Cross-cultural Study of Sharing Digital Devices and Online Accounts," Proceedings on Privacy Enhancing Technologies*, vol. 2021, no. 4, pp. 203–224, 2021.

[51] A. Shrestha, T. Sharma, P. Saha, S. I. Ahmed and M. N. Al-Ameen, "A first look into software security practices in Bangladesh," *ACM Journal on Computing and Sustainable Societies*, vol. 1, no. 1, pp. 1–24, 2023.

[52] R. Paudel, P. Dumaru, A. Shrestha, H. Kocabas and M. N. Al-Ameen, "A Deep Dive into User's Preferences and Behavior around Mobile Phone Sharing," *Proceedings of the ACM on Human-Computer Interaction*, vol. 7, no. 1, pp. 1–22, 2023.