Human Factors in Training, Education, and Learning Sciences, Vol. 231, 2026, 77–87
https://doi.org/10.54941/ahfe1007998

A Bridge Too Far: Low Literacy and Cybersecurity Materials

Mary L. Still, Jeremiah D. Still, and Hagar E. Baruch

Old Dominion University, Norfolk, VA 23529, USA

ABSTRACT

Accessibility is emerging as the third dimension of cybersecurity design, addressing the growing concern that dependence on digital services is creating disparities in vulnerable populations. While many factors influence the effectiveness of cybersecurity materials, most materials providing security advice are written at a high school or college level. This means over 30% of the United States adult population would struggle to understand them. To explore how the gap between standard materials and the average reading level might be bridged, we contextualized guidelines for low-literacy design in the cybersecurity domain. Three main considerations – text characteristics, focused content, and graphic design – were used to redesign text-based cybersecurity materials. A mixed factorial design was used to evaluate the effectiveness of the redesigned materials for university students at higher and lower literacy levels. The study found that participants with lower literacy levels scored lower on cybersecurity knowledge tests and tended to rate all cybersecurity materials (standard and redesigned for low literacy) less favorably than participants with higher literacy levels. Surprisingly, although materials were redesigned to objectively improve the communication of cybersecurity information, those materials did not impact post-test measures of cybersecurity knowledge and the materials were rated as less effective. These findings suggest that changes intended to simplify content may have unintended consequences, potentially limiting the design's effectiveness.

Keywords: Inclusive design, Instructional materials, Cybersecurity, Literacy

INTRODUCTION

Accessibility is emerging as the third dimension of cybersecurity design, extending beyond the traditional dual focus on technical security and usability (Renaud and Coles-Kemp, 2022). There is growing concern about dependence on digital services for essential needs (e.g., banking, healthcare, education) and the widening disparity in access to these services. The online world requires greater inclusivity for vulnerable populations. To mitigate these risks and enhance inclusivity, we recommend shifting from a human-as-problem approach to a human-as-solution approach (c.f., Still, 2016; Zimmermann and Renaud, 2019). This human-centered perspective focuses on strengthening factors that contribute to positive outcomes and to user resilience against cybersecurity threats.

Received January 21, 2026; Revised March 28, 2026; Accepted April 17, 2026; Available online July 20, 2026

NEED FOR ACCESSIBLE CYBER HYGIENE

Cyber hygiene is defined as personal cybersecurity behaviors and conditions that support security and minimize threats (Clemente, 2021). The importance of effective individual cyber hygiene practices continues to increase. For example, in its 2023 Global Data Breach Investigations Report, Verizon estimates that 74% of breaches were associated with ineffective human interactions with cyber systems. As home computing environments have shifted from casual entertainment to higher-stakes activities such as working from home, managing finances, and accessing and understanding medical care (Morris and Still, 2023), it has become critical that everyone have the opportunity to learn how to protect themselves. Unfortunately, it is a significant challenge to disseminate cybersecurity information effectively and to develop materials that lead to actual changes in cybersecurity behavior (e.g., Bada, Sasse, and Nurse, 2015; Chowdhury and Gkioulos, 2021; Kävrestad, Rambusch, and Nohlberg, 2024; Renaud and Coles-Kemp, 2022).

A similar situation has unfolded in the context of health literacy. Bodie and Dutta (2008) identified a variety of factors that may affect health disparities between groups and how these disparities might be mitigated through access to online information. In their review, they emphasize that several factors impact the effectiveness of online materials, including experience and proficiency with computer and internet use, ability to identify reliable sources, preferences in information sources (e.g., text-based material, videos, friends and family), pre-existing health knowledge, attitudes about health, motivation to engage in the materials, and literacy levels. In short, providing access to information is only part of the solution; situational factors associated with the population of interest and the materials themselves must be considered to develop effective designs.

In cybersecurity, one of the most straightforward ways to improve the effectiveness of online materials is to ensure they are understandable to the general public. Although explicitly designed to convey cybersecurity risk and best practices to the public, current guidance materials can be challenging to understand. In their examination of online security advice documents, Redmiles et al. (2018) found that the average document was written at a high school or college level. In contrast, only 22% were written at middle school or lower levels. The Web Content Accessibility Guidelines 2.0 recommend that content above the middle school level include a simplified version; this recommendation is seldom followed. Furthermore, Wu et al. (2020) found that technical terms negatively affect comprehension and 65% of their participants reported that they would benefit from a dictionary of relevant terms. Therefore, even if individuals are motivated to locate materials and implement the guidance provided, they may still be unable to do so because they do not understand the material. Because cybersecurity information is often written at a high literacy level, individuals with lower literacy levels will be disadvantaged in their cybersecurity knowledge.

Adult Literacy Levels and Comprehension

While many factors contribute to an individual's ability to understand written material, this study focuses on reading level. The Program for the International Assessment of Adult Competencies (PIAAC) data indicate that literacy levels in the United States declined from 2017 to 2023. In 2017, approximately 19% of the adult population was predicted to have Level 1 or lower literacy; this figure increased to 28% in 2023 (NCES, 2024). Individuals with Level 1 proficiency can find information on a page but may be distracted by irrelevant information. They can also locate specific information in the text but are most successful when the question specifies what to look for. By comparison, adults with Level 2 literacy can make inferences about the text and can find information across multiple pages, even with distracting information included. Based on these numbers, in a population of approximately 265 million adults, over 74 million adults would be at or below Level 1 literacy; they would struggle to understand text describing an unfamiliar or technical topic.

Revising complex cyber hygiene materials to present information in plain language may improve comprehension among individuals with low literacy or intellectual disabilities. However, designing materials that are easier to read does not always improve individual outcomes (Buell et al., 2020; Chinn and Homeyard, 2017). In their review of medical information designed for easy reading, Chinn and Homeyard (2017) explain that the target populations for the redesigns identified new issues, such as simplified language that is too generic to be useful, and images intended to improve accessibility were too abstract to be useful. Therefore, it is always possible that new designs introduce new complexities, inadvertently hindering the very population they aim to help.

Designing Cybersecurity Materials for Lower Literacy

Although there has been limited research examining literacy-related concerns in cybersecurity materials, an extensive body of parallel research exists in the medical field. In their seminal work, *Teaching Patients with Low Literacy Skills*, Doak, Doak, and Root (1996) consider the scope of adult low-literacy levels and the implications for effective communication of medical information to that population. In terms of text, Doak et al. recommend using accessible language, accomplished in part by using shorter sentences, shorter words, and avoiding jargon. The authors note that low literacy is more than just an issue with vocabulary; individuals may have difficulty making inferences based on the text, missing important contextual cues and interpreting text literally. In terms of the content, it should be focused, minimizing repetition and using concrete examples. Relevant images should be used to supplement the text, while irrelevant images should be avoided. Doak et al. also consider factors beyond readability. For instance, designers should consider users' self-efficacy. Does the information look difficult to read? Individuals with lower literacy may be discouraged when they see a solid page of text or when it appears several concepts or facts are addressed in one paragraph. From this perspective, the layout of the material (e.g.,

providing white space, using visual grouping principles) is also important for motivating lower-literacy users.

Recommendations from the cybersecurity domain are consistent with Doak et al. (1996). For example, Kävrestad, Rambusch, and Nohlberg (2024) examined how cybersecurity training might be designed for individuals with cognitive disabilities. After an iterative design process for their cybersecurity training tool, Kävrestad et al. present design principles to reduce the cognitive effort required to understand and implement cybersecurity guidelines. Specifically, they recommend designing with a focus on relevance and applicability (i.e., providing information in the context it is used, presenting only the most important topics, and avoiding irrelevant design features) and by providing options for access (e.g., visual and auditory modalities). In further support for providing specific and contextualized cybersecurity information, Reeves, Calic, and Delfabbro (2023) note that users express frustration when cybersecurity information is too general, abstract, or vague; instead, they value specific, actionable advice.

We developed design guidelines for accessible literacy in cybersecurity, drawing on the literature on common cybersecurity threats to personal computing, the complexity of cybersecurity instructional materials, the characteristics of low-literacy adult readers, and design guidelines for low-literacy materials in the medical field. Three primary considerations organize the guidelines: 1) Text Characteristics, 2) Focused Content, and 3) Graphic Design.

Text Characteristics. Minimize the total amount of text; use short sentences (10–15 words); use short paragraphs (50 words or less); use short words instead of words with multiple syllables when possible; avoid jargon; create materials to be lower than a 7th-grade reading level.

Focused Content. Only present one idea per paragraph; minimize repetition; exclude irrelevant information; use concrete examples; provide actionable advice.

Graphic Design. Avoid large blocks of text; supplement ideas with relevant images; use white space to reduce visual crowding; use visual indicators of grouping and organization.

The objective of this study was to test the effectiveness of inclusive design guidelines applied to cyber hygiene materials. We hypothesized that redesigned materials would improve knowledge acquisition relative to conventional materials (the control), particularly among low-literacy participants. Redesigned materials should also be rated as more effective than conventional materials.

METHOD

Participants were recruited through introductory psychology courses at Old Dominion University. Students received course credit for their participation. All data were collected via Qualtrics, and no identifying information was collected, ensuring the data were anonymous.

Participants

A total of 106 adults from Virginia participated in the study. The sample was comprised of university students (*M* age = 23.54, ranging from 18 to 53 years of age) living in urban locations. The majority of participants were

women (79 women, 23 men, two non-binary, two prefer not to disclose) with a household income under $100,000 per year (77%). Participants' self-reported race indicated that the sample was primarily Black or African American (42%), White (35%), or Asian (15%). Participants report regular and diverse interactions involving the internet and internet-connected devices. Ninety-three percent access the internet or an internet-enabled program daily; 5.6% access it multiple times each week. The most common devices used on a weekly basis were smartphones (96%) and personal computers (95%), followed by tablets (43%), smartwatches (41%), smart appliances (28%), and smart speakers (28%). Further, most participants reported using multiple connected devices each week.

Materials

Literacy Assessment. A four-item literacy assessment was used to classify participants as having lower or higher literacy levels. The assessment was intended to be as brief as possible while still being useful in providing an overall characterization of participants' reading comprehension. The assessment was not intended to quantify an individual's specific literacy levels. The four items were selected from the 2022 National Assessment of Educational Progress (US Department of Education, 2024) fourth-grade reading assessment; based on NAEP data, two items were easier, with over 60% of 4th graders answering correctly, while two items were more difficult, with less than 40% of 4th graders answering correctly (US Department of Education, 2013). For purposes of this study, participants were categorized as having lower literacy levels if they scored 0–50% on the assessment (n = 30). Those scoring 75–100% were categorized as having higher-literacy levels (n = 76).

Cybersecurity Materials. Two sets of cybersecurity materials were developed in accordance with guidelines for creating accessible materials for low literacy (see Figure 1). The materials needed to be appropriate for the general population. Accordingly, cybersecurity topics had to be those important for maintaining personal cybersecurity hygiene. Eighteen critical cyberhygiene behaviors were identified as common recommendations in academic reviews of cyberhygiene best practices and industry guides for safe home computing. Those behaviors correspond with six general topics: 1) phishing, 2) password management and authentication, 3) app and social media privacy, 4) system/software updates, 5) data storage and encryption, and 6) safe computing outside of the home network.

Development began with the *conventional* (control) condition. Cybersecurity materials were obtained from the publicly available CISA Cybersecurity Awareness Program Toolkit (CISA, 2021). Four guides - *Mobile Payments and Banking Tip Card*, *Phishing Tip Card, Cybersecurity while Traveling* guide, and *5 Steps to Protecting Your Digital Home* - were selected based on their focus on important cyber hygiene topics and relevance for personal cyber hygiene for adults. The materials feature a conventional presentation style characterized by blocks of text, a formal tone, and a higher density of technical jargon. These guides averaged 399 words and an 8.4-grade Flesch-Kincaid reading level. To ensure appropriate comparisons, we limited each guide to one page, primarily

by removing redundant information across the materials. For instance, nearly every document included guidance for creating strong passwords. Because participants would be exposed to all four documents, they would encounter password guidelines four times, whereas other critical information may be encountered only once. Removing information that repeated across guides reduced redundancy and kept the document length to one page.

Our *redesigned* (experimental) materials mirrored the conventional materials but were redesigned to promote inclusive literacy. Modifications included leading with a clear rationale, reducing redundant information, removing jargon where possible, reducing text complexity, reducing word count, including relevant graphics to aid comprehension, creating shorter sections of text, increasing white space around text, and integrating specific examples of cybersecurity scenarios. These guides averaged 363 words and a Flesch-Kincaid reading level of 6.4.

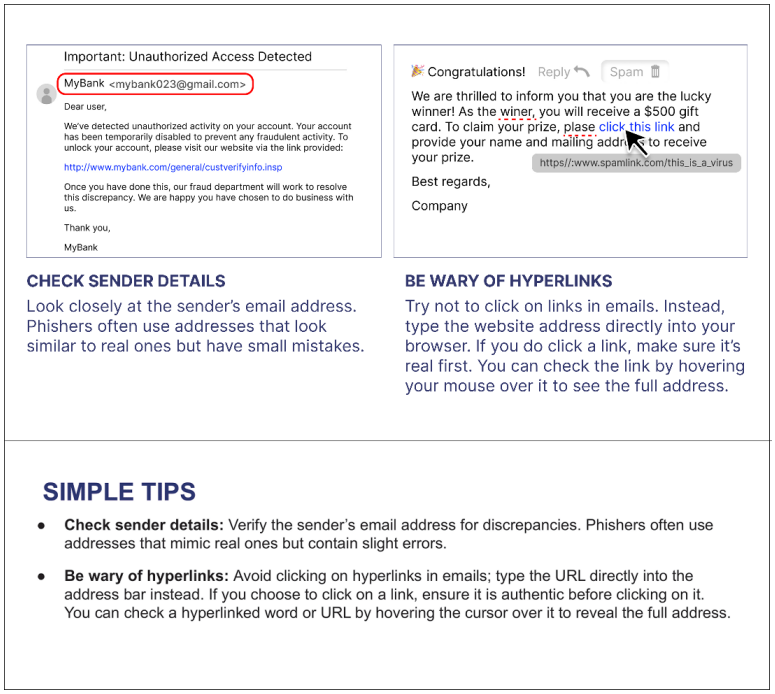

Figure 1: Example of redesigned (top panel) and conventional materials (bottom panel).

Cybersecurity Knowledge Test. Two versions of a cybersecurity knowledge test were developed for this study. Topics on the tests included protecting oneself through software updates, home network security, device management, public Wi-Fi use, phishing and social media attacks, application permissions settings, and authentication. The tests were written at a 6th-grade reading level.

A 10-item multiple-choice pretest and 10-item multiple-choice post-test indexed knowledge scores. Both pre- and post-tests were matched for cybersecurity topics. For example, both tests contained a question about updating software (Version A – Why is it important to update the software on

your home devices? Version B – How often should you update your software and operating system?). Participants were randomly assigned to take one version of the test as the pre-test and the other as the post-test.

Procedure

Participants accessed the study online and provided informed consent. The survey began with items regarding age and county/city of residence. Participants under 18 or residing outside the state of Virginia were excluded.

Eligible participants completed the 4-item literacy measure, followed by a pre-test of personal cybersecurity knowledge. They were then randomly assigned to the conventional (control) or redesigned cybersecurity materials condition, each consisting of four documents. After reading each document, participants rated it on a 1–5 Likert scale for (a) ease of understanding and (b) usefulness for learning protection strategies. Document presentation order was randomized for each participant. Participants then completed a 10-item post-test of cybersecurity knowledge and provided demographic data related to age, gender, race, household income, and internet and technology use. Finally, participants were debriefed and provided links to CISA personal cybersecurity materials.

A mixed factorial design was employed. The between-subjects factors were Condition (Conventional vs. Redesigned materials), which was randomly assigned, and Literacy level (High vs. Low), which was a quasi-independent variable. The within-subjects factor was Test (Pre vs. Post).

RESULTS

Knowledge Scores

Participant pre- and post-test scores were used to measure cyber hygiene knowledge and to test the impact of the cybersecurity materials. One test item related to protecting oneself when using public Wi-Fi, performed significantly worse than all other items (approximately 43% answered it correctly, whereas other items ranged from 79 to 96%). To ensure this item did not confound the pre-test/post-test comparison, the public Wi-Fi questions were excluded from both versions of the test leaving 9 items in each pre- and post-test score.

A repeated-measures ANOVA revealed a significant main effect of literacy level, $F(1,102) = 38.91$, $p < .001$, $\eta^2_p = .276$. Participants with higher literacy levels demonstrated greater cyber hygiene knowledge ($n = 76$, $M = 8.59$, $SE = .26$) than participants with lower literacy levels ($n = 30$, $M = 6.68$, $SE = .26$).

An unexpected three-way interaction was observed among Test, Condition, and Literacy, $F(1, 102) = 6.26$, $p = .014$, $\eta^2_p = .058$. There was no impact of Condition for participants with higher literacy levels as pre- and post-test scores were near ceiling: redesigned materials ($n = 39$, Pre-test $M = 8.51$, $SE = .24$; Post-test $M = 8.49$, $SE = .25$), conventional materials ($n = 37$, Pre-test $M = 8.73$, $SE = .25$; Post-test $M = 8.62$, $SE = .26$). But, participants with lower literacy levels had mixed results. Those who read conventional

materials improved from pretest (n = 15, M = 6.13, SE = .39) to post-test (M = 6.73, SE = .41) while those who read the redesigned materials showed decreased performance from pre-test (n = 15, M = 7.27, SE = .39) to post-test (M = 6.60, SE = .41). This interaction may be driven by the high pre-test score in the low-literacy Redesign group.

Subjective Ratings

A Multivariate ANOVA was conducted on the subjective ratings for 1 - *how easy it was to understand the information in the guide*, and 2 - *how much the guide helps them understand how to protect themselves*. When considering both ratings, a main effect of Literacy was found, $F(2,101) = 4.91$, $p = .009$, $\eta^2_p = .089$; participants with higher literacy levels tended to rate all materials more favorably (n = 76, M = 4.6, SE = .08) than the ratings provided by those with lower literacy levels (n = 30, M = 4.2, SE = .13). There was also a main effect of Condition, $F(2,101) = 3.93$, $p = .023$, $\eta^2_p = .072$. The conventional guides were rated more positively (n = 52, M = 4.6 SE = .11) than the redesigned guides (n = 54, M = 4.3, SE = .11). There was no interaction between Literacy and Condition.

DISCUSSION

The results of this study challenge the assumption that reducing the reading level, creating visual segmentation, and adding relevant graphics will naturally improve accessibility for populations with lower literacy levels. Unfortunately, in this sample, the redesigned materials may have caused these individuals to score lower on their cybersecurity knowledge post-test than on the pre-test. Further, while it might be assumed that everyone would appreciate easy-to-read materials over conventional materials, that was not the case; the redesigned materials were consistently rated less favorably than traditional, conventional materials.

Text Characteristics vs. Individual Characteristics

In their review, Chinn and Homeyard (2017) note that presenting health information at an appropriate level has the potential to contribute to positive outcomes (e.g., increased understanding, improved decision-making, improved health). However, there is no consistent evidence of positive outcomes. They note that variability in materials, measurement techniques, and stakeholders contribute to the mixed results. Further, they suggest that most studies identify readability as a critical factor in making information accessible but often fail to consider factors beyond that. It is possible that participant characteristics are more important to consider than text characteristics. For example, Buell et al. (2020) asked adults with intellectual disabilities to read health information and then answer questions about it. The paragraph was easy to read (4th-grade level) or difficult to read (university-level, 14th-grade level). No difference in comprehension was found based on text grade level. Instead, individual participant vocabulary and reading comprehension scores were the best predictors of performance.

An analogous pattern was observed in our data. Making cybersecurity information easy to read did not benefit our participants who had lower literacy levels. Even so, our data show that participants with lower literacy levels also had lower cybersecurity knowledge. Thus, while literacy level and cybersecurity knowledge are correlated, it may be that literacy level is not predictive of who will best learn from text-based cybersecurity materials. It is possible that more nuanced measures of individual reading ability would be more predictive.

User Expectations

Another unexpected outcome of this study was that the subjective ratings were consistently higher for conventional materials than for redesigned materials. Although ratings were generally good, the dense, jargon-heavy materials were rated as easier to understand and to use for protective action than the simplified materials that included concrete examples and relevant graphics. By objective design measures the redesigned materials should be easier to understand. Why weren't they rated that way?

It is possible that participants' expectations regarding the difficulty and technicality of cybersecurity, in general, impacted their subjective experience with the materials. A finding similar to this was reported by Park et al. (2016). In their study, participants rated the quality, security, and convenience of a web browser after reading an easy-to-understand description or one containing jargon and technical abbreviations. Participants who read the jargon-filled, technical description rated the web browser as more secure than those with the easy-to-read description. Park et al. suggested that the difficulty of reading the technical text led participants to infer that the browser was more technologically sophisticated and therefore more secure. A similar inference may have occurred in the present study (i.e., cybersecurity is technical, so difficult-to-read materials are better).

It is also possible that expectations regarding educational materials – how they should be formatted and how technical they should be – contributed to participants' subjective ratings of the materials. The design of the conventional materials aligns with standard schemas for "official" or "educational" documents. This congruence between the design and individual expectations for technical materials may have contributed to the higher ratings for conventional materials.

CONCLUSION

To achieve digital equity, cybersecurity materials must be designed with a rigorous evidence-based approach. This study demonstrates that "inclusive" design guidelines may not be practical if they inadvertently violate user expectations. The simplified materials likely failed because their format lacked the stylization users associate with credible security advice. Future work should explore how to leverage the perceived validity of traditional design elements while simplifying and contextualizing the content.

ACKNOWLEDGMENT

This work was supported in part by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. For more information about CCI, visit www.cyberinitiative.org.

REFERENCES

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). 'Cyber security awareness campaigns: Why do they fail to change behaviour?', In *Proceedings of the 1st International Conference on Cyber Security for Sustainable Society,* pp. 118–131.

Bodie, G. D. & Dutta, M. J. (2008). 'Understanding health literacy for strategic health marketing: eHealth literacy, health disparities, and the digital divide', *Health Marketing Quarterly*, 25(1–2), pp. 175–203.

Buell, S., Langdon, P. E., Pounds, G., & Bunning, K. (2020). 'An open randomized controlled trial of the effects of linguistic simplification and mediation on the comprehension of "easy read" text by people with intellectual disabilities', *Journal of Applied Research in Intellectual Disabilities*, 33(2), pp. 219–231.

Chinn, D. & Homeyard, C. (2017). 'Easy read and accessible information for people with intellectual disabilities: Is it worth it? A meta-narrative literature review', *Health Expectations*, 20(6), pp. 1189–1200.

Chowdhury, N. & Gkioulos, V. (2021). 'Cyber security training for critical infrastructure protection: A literature review', *Computer Science Review*, 40, 100361.

CISA Cybersecurity Awareness Program Toolkit. (2021) https://www.cisa.gov/resources-tools/resources/cisa-cybersecurity-awareness-program-toolkit

Clemente, D. (2021). 'Personal protection: "Cyber Hygiene"', in *The Oxford handbook of cyber security*, ed P. Cornish, Oxford University Press, Oxford, pp. 361–376.

Doak, C.C., Doak, L.G., & Root, J.H. (1996). *Teaching patients with low literacy skills,* 2nd edn, J.B. Lippincott, Philadelphia, PA.

Kävrestad, J., Rambusch, J. & Nohlberg, M. (2024). 'Design principles for cognitively accessible cybersecurity training', *Computers & Security*, 137, 103630.

Morris, T.W., & Still, J.D. (2023). 'Cybersecurity hygiene: Blending home and work computing', in *New perspectives in behavioral cybersecurity,* ed W. Patterson, CRC Press, Boca Raton, FL, pp. 107–119.

Park, Y.-W., Herr, P. M. & Kim, B. C. (2016). 'The effect of disfluency on consumer perceptions of information security', *Marketing Letters*, 27, pp. 525–535.

Redmiles, E. M., Morales, M., Maszkiewicz, L., Stevens, R., Liu, E., Kuchhal, D., & Mazurek, M. L. (2018). 'First steps toward measuring the readability of security advice', in *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*, pp. 89–108.

Reeves, A., Calic, D., & Delfabbro, P. (2023). '"Generic and unusable": Understanding employee perceptions of cybersecurity training and measuring advice fatigue', *Computers & Security*, 128, 103137.

Renaud, K., & Coles-Kemp, L. (2022). 'Accessible and inclusive cyber security: A nuanced and complex challenge', *SN Computer Science*, 3(5), 346.

Still, J. D. (2016). 'Cybersecurity needs you!', *Interactions*, 23, pp. 54–58.

U.S. Department of Education (2013). 'National Assessment of Educational Progress (NAEP), 2013 Reading Assessment', *Institute of Education Sciences, National Center for Education Statistics.3*

U.S. Department of Education (2024). 'Highlights of the 2023 U.S. PIAAC Results Web Report (NCES 2024–202)', *National Center for Education Statistics*. Washington, DC. https://nces.ed.gov/surveys/piaac/2023/national_results.asp.

Wu, T., Zhang, R., Ma, W., Wen, S., Xia, X., Paris, C., Nepal, S., Xiang, Y. (2020). What risk? I don't understand. An empirical study of users' understanding of the terms used in security texts. ASIA CCS '20: In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, pp. 248–262.

Zimmermann, V. & Renaud, K. (2019). 'Moving from "human-as-problem" to a "human-as-solution" cybersecurity mindset', *International Journal of Human-Computer Studies*, 131, pp. 169.187.