Impact of the Cyber Hygiene Intelligence & Performance (CHIP) Interface on Cyber Situation Awareness and Cyber Hygiene

Janine D. Mator, Jeremiah D. Still

Old Dominion University, Norfolk, VA 23507, USA
{jmator,jstill}@odu.edu

Abstract. A common theme across cybersecurity solutions is a lack of transparency for end-users. Our prototype, Cyber Hygiene Intelligence & Performance (CHIP), was purposefully designed to improve end users' cyber hygiene and cyber situation awareness. We begin by addressing current cybersecurity training solutions, their inability to continuously impact user cyber hygiene and cyber situation awareness (CSA), and how end users' needs for transparency are overlooked. We then illustrate the major stages of our design process for the medium-fidelity CHIP prototype, including defining, ideation, prototyping, and analysis. For each design stage, we describe our methodologies, major decision points, design considerations, and outcomes. We then highlight our between-groups survey experiment that measured cyber hygiene and CSA for an experimental group, who received CHIP notifications while completing web-based tasks, compared to a control group, who completed the same tasks without any notifications. Our findings show promise for a web application-based solution like CHIP to increase cyber hygiene and CSA for specific cyber threats.

Keywords: Human-centered design, Cyber situation awareness, Cyber hygiene.

1 Introduction

End users have been simultaneously recognized as the frontline defense and the weak point of cybersecurity systems [1,2]. Consequently, cybersecurity training has become an essential and often mandatory task for users. However, traditional training is infrequent and only tests theoretical knowledge, which translates poorly to cyber hygiene (e.g., complying with dangerous website warnings) in the real world [3,4]. Users typically complete cybersecurity training once a year through 30-minute modules [4]. This assumes that brief, infrequent, and impersonal training is sufficient to improve user cyber hygiene.

Clearly, cyber hygiene remains a prominent and costly concern [5]. Approximately 90% of cyberattacks are preventable through basic cyber hygiene and best practices [6]. Common examples of poor cyber hygiene decision points include answering account security questions with information that is readily available online (e.g., a mother's maiden name) [7,8], complying with phishing emails [9], proceeding to

dangerous websites [10], and saving/auto-filling passwords in a web browser [11]. Cybersecurity training modules typically discourage these behaviors but fail to prevent them in practice [12]. Organizations may attempt to increase compliance with good cyber hygiene practices by enforcing "Big Brother" software that monitors and reports employees' online behavior. However, these programs are mainly intended for IT administrators to oversee large networks, rather than help end-users increase their awareness of cyber threats.

Even for those with good cyber hygiene, cyber situation awareness (CSA) is another concern. CSA refers to perception, comprehension, and outcome projections of a cyber threat [13]. Conventional cybersecurity tools like firewalls and anti-virus software fail to promote CSA, as they primarily operate in the background (e.g., desktop applications) and only provide information retroactively. Future solutions will need to ensure users not only possess practical knowledge of cyber threats, but how to apply their knowledge [14].

Current cybersecurity solutions lack transparency, leaving end-users out-of-the-loop. For interface designers, transparency refers to how well an interface shows users what they can do, how they can access these functions, and why the system responds as it does [15]. Therefore, transparency in a cybersecurity interface should enable users to understand the nature of a threat, the behavior that triggered it, and its intended consequences. There is a need for solutions that promote good cyber hygiene and CSA. This paper proposes a prototype interface called Cyber Hygiene Intelligence and Performance (CHIP) designed to meet these needs.

2 Overview

In the previous section, we introduced cyber hygiene, cyber situation awareness, and how both have been neglected in the implementation of current cybersecurity solutions for end-users. In the following section, we narrate the design process of our mid-fidelity CHIP prototype. The main stages in our iterative design process are summarized into the four subheadings Define, Ideate, Prototype, and Analyze. In each section, we illustrate design considerations, methodologies implemented during development, and outcomes revealed during that stage. We also discuss our between-groups survey experiment findings that assessed the impact of CHIP notifications on cyber hygiene and CSA compared to a control group. Finally, we discuss our goals, findings, and challenges while designing CHIP.

3 Design Process

3.1 Define

In the first stage of our design process, we defined our goals, stakeholders, and user requirements. Our goals were twofold: to provide users with digestible notifications that increase CSA and further their understanding of cyber hygiene. Uniquely, end-users will learn as they complete daily computing activities.

Requirements gathering from context experts narrowed our scope of cyber hygiene to four target behaviors: 1) preventing web browsers from auto-saving passwords, 2) deleting or reporting suspicious emails, 3) answering security questions with unique information, and 4) complying with dangerous website warnings. These target behaviors were selected due to their prevalent risk factors in cybersecurity. Many users store authentication credentials within web browsers, which poses the threat of unauthorized logins and malware downloads [11]. Additionally, phishing emails are often not recognized by users. As a result, millions of users have their personal information stolen each year [9]. Users also make poor decisions when creating answers to account security questions. These answers can often be found in public records; for example, a mother's maiden name [7]. Finally, users place themselves at greater risk of phishing and malware attacks when they ignore warnings about potentially dangerous websites [10].

We conducted a hierarchical task analysis (HTA) for each target behavior to break down the series of goals required at each cyber hygiene decision point (see Figure 1 below, for example).

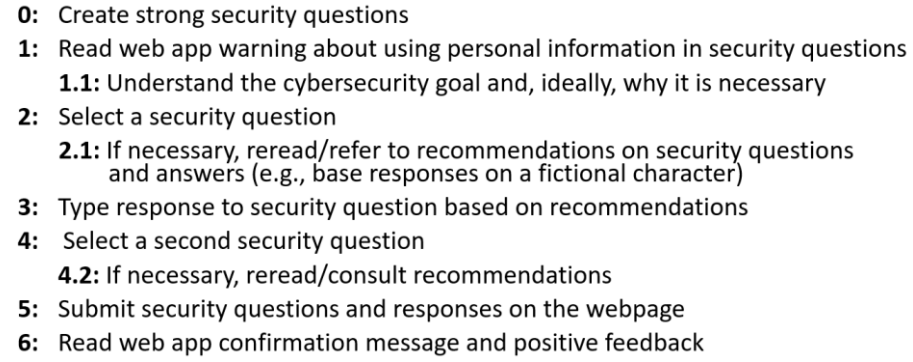


Fig. 1. HTA for creating strong security questions.

We next conducted a competitive analysis to better understand key stakeholders and the user requirements of related solutions. Our spreadsheet came to include categories such as the solution's company/developer, program or feature name, domain (i.e., Department of Defense or online banking), method of delivery (i.e., mobile app), and the actions available to managers and/or end-users. As we had previously seen, current solutions in the cybersecurity marketplace tended not to be targeted to end-users, but to corporations and government agencies. Not only was pricing unrealistic for individual users, but descriptions assumed more technical language (e.g., cascaded learning framework, PCAP file, and CVE matching). Clearly, such solutions are not intended to further the end-users' mental model or significantly boost CSA.

Our competitive analysis allowed us to identify a wide range of potential stakeholders, including end-users, IT and cybersecurity professionals, cybersecurity educators, and private sector stakeholders. We recognized end-users as the primary stake-

holder, but we also identified the role of IT and cybersecurity professionals to maintain the web app and further assist users with questions, support tickets, etc. Cybersecurity educators comprised another class of stakeholders, as our web app could further education of sporadic training modules and inspire training certificates based on real-world user behavior. Internet service providers are one example, as they are responsible for providing a line of defense against cyberattacks [6].

During this early stage, we also summarized user requirements for the application's interface. We had previously identified the need for users to receive transparent information and timely feedback. Thus, we summarized the need for our interface to clearly communicate the nature of the cyber threat, the actions available to the user, how to carry them out, and why they are necessary. We also established the need for users to receive information that is specific to the task at hand and to access additional information and feedback as desired.

3.2 Ideate

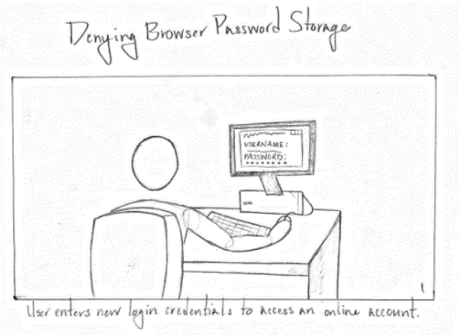
The ideation stage primarily involved brainstorming and storyboarding to find an appropriate name, platform, and representation for our interface. In early brainstorming sessions, we tested combinations of words to find an acronym that suited our interface's overarching goals. This resulted in the name CHIP, an acronym for Cyber Hygiene Intelligence and Performance.

While brainstorming, we also considered the previously identified user requirements to establish a method of delivery. We found that the ideal platform to encourage our target behaviors was a web application, which could gather and communicate information directly within the user's browser. The development of web apps has also enabled richer and more interactive content compared to desktop applications (e.g., firewalls and anti-virus software), which are considered more "cumbersome and monolithic" [16].

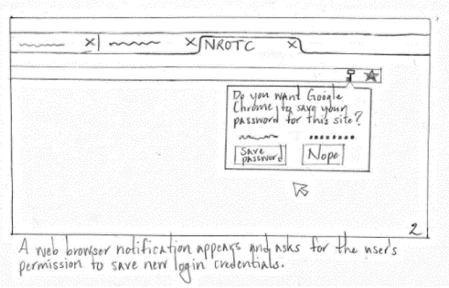
Next, we considered the identity of our web application. We found that the best representation to meet user needs was a helpful bot or virtual assistant, commonly portrayed as avatars using conversational language [17]. On the other hand, previous literature also informed the need to avoid qualities that are *too* human-like. Schneiderman [18] contends that designing intelligent agents to mimic humans outright is inappropriate and ineffective. Our web app's more ambiguous and informal nature was also an intentional shift away from "informant" programs whose central goal is to escalate non-compliance.

Through paper storyboarding, we visualized how CHIP might interact with end-users. The premise of each storyboard entailed a user reaching a cyber hygiene decision point, which triggered a CHIP notification. For each target cyber hygiene behavior, we sketched a series of 3-5 panels. Each panel contained a concise description of the user's actions and/or CHIP's responses in the form of a push notification from the web app. The notifications began with brief, actionable information (e.g., "Just say nope" to password-saving, or "Be original" to create account security questions), followed by additional information on the nature of the threat, such as the hacker's motivations.

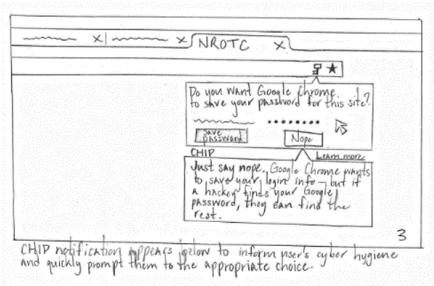
See Figures 2-3 for sample storyboards.



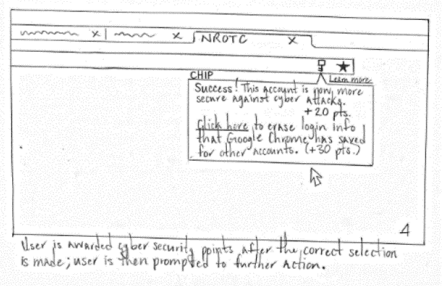
User enters new login credentials to access an online account.



A web browser notification appears and asks for the user's permission to save new login

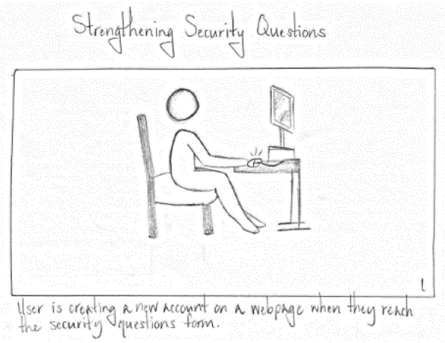


CHIP notification appears below to inform user's cyber hygiene decision and quickly prompt them to the appropriate choice.

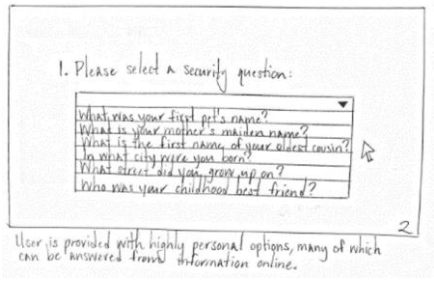


User is awarded cyber security points after the correct selection is made; user is then prompted to further action.

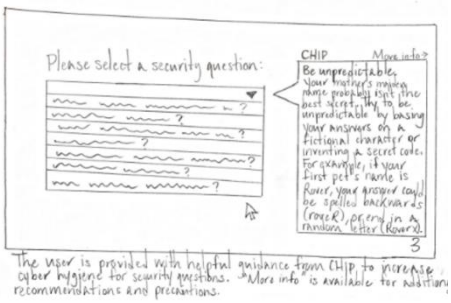
Fig. 2. "Denying browser password storage" storyboard.



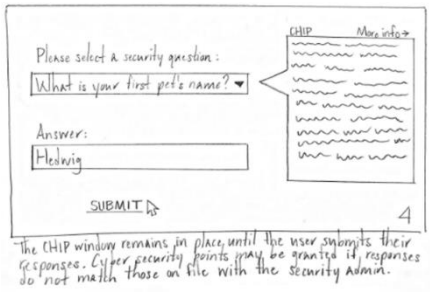
User is creating a new account on a webpage when they reach the security questions form.



User is provided with highly personal options, many of which can be answered from information online.



The user is provided with helpful guidance from CHIP to increase cyber hygiene for security questions. "More info" is available for additional recommendations and



The CHIP window remains in place until the user submits their responses. Cybersecurity points may be granted if responses do not match those on file with the security admin.

Fig. 3. "Strengthening security questions" storyboard.

3.3 Prototype

Using paper sketches and storyboards from the ideation process, we developed a mid-fidelity prototype through Adobe XD. We focused on developing web app notifications. From previous literature, we had learned that users tend to relate to bots despite knowing that they rely on artificial intelligence [19]. According to Friedman [20], "users tend to be more receptive to conversational messages that feel more casual and less like system notifications." We therefore designed CHIP notifications to leverage conversational and straightforward language, omitting unnecessary technical jargon (see Figure 4). Notifications appeared as speech bubbles emerging from the user's primary task.

In later iterations, however, we further developed the bot representation by adding a logo-like avatar (see Figures 5 and 6). At this point, we needed to be wary of developing a relatable bot without mimicking a human entity (for further discussion, see Schneiderman, 2020). Therefore, we designed the CHIP avatar to be abstract (i.e., genderless and faceless) and removed the chat bubble response option from the user, which we ultimately found unnecessary. Instead, we included a collapsible drop-down menu that would allow users to pursue additional information and actions on their own terms.

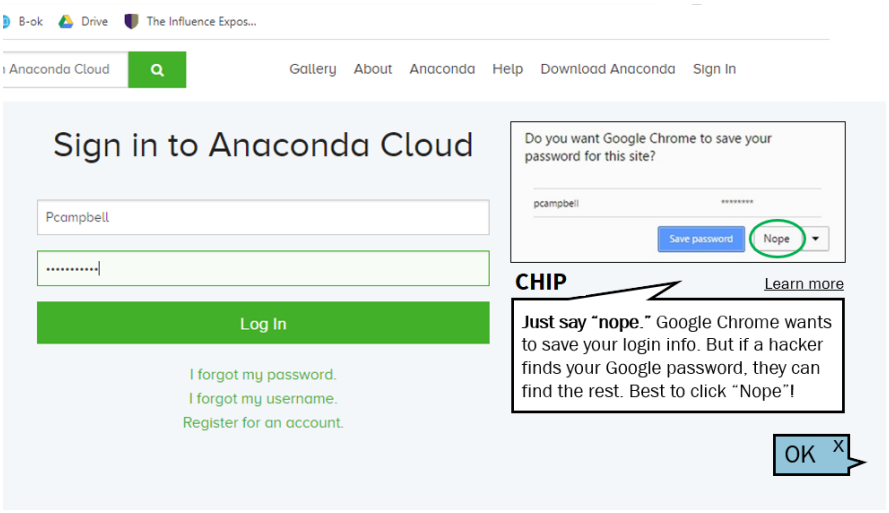


Fig. 4. An early Adobe XD prototype. Our prototype would later incorporate an avatar and collapsible menu.

Fig. 5. CHIP avatars. As users demonstrate better cyber hygiene, they may progress to higher tiers (e.g., bronze to silver, silver to gold).

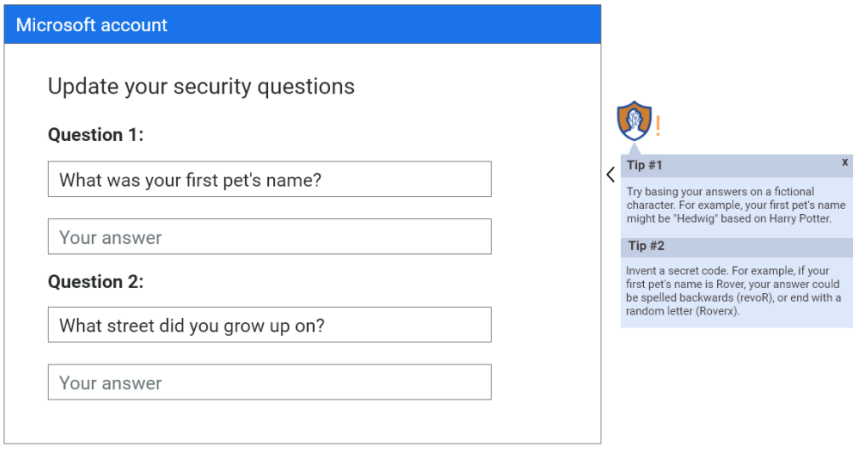


Fig. 6. Late iteration of the CHIP prototype. While creating account security questions, the user receives a push notification to access tips to create secure responses, for example, basing responses on a fictional character instead of using personally identifiable information (PII) that may be accessed online.

Other design decisions during the prototyping stage were based on heuristic standards. For example, Fitts's Law states that the time required for a user to reach a "target" (i.e., a command button) is a function of the size and distance to the target. Our solution for CHIP as a web app allows notifications to float beside the task at hand, allowing users to quickly access information in the periphery. This solution also prevents a pop-up window from obstructing the user's primary task, which might lead users to close the notification window without reading it [21]. Once users' attention is directed toward the task, the amount of time required for them to make a decision depends on the sum and complexity of their choices. This heuristic, known as Hick's Law [22], resulted in simplifying choices to "more info" and "actions" with a handful of action choices nested within the drop-down menu, such as "contact help desk" or "report phishing email." Another heuristic known as the goal-gradient effect states that "the tendency to approach a goal increases with proximity to the goal" [23], and informed our decision to utilize progress indicators for cyber hygiene goals (see Figure 7). In this case, the progress bars illustrate users' task completion and motivate them to reach the goal (e.g., creating a stronger password).

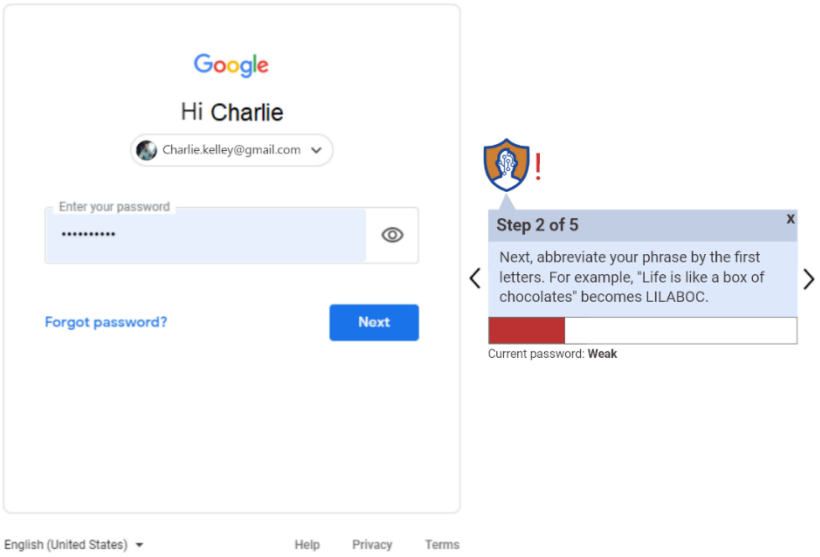


Fig. 7. Progress indicators are shown as users incrementally strengthen a weak password.

3.4 Analyze

Using screenshots of our prototypical notifications, we conducted a survey experiment to determine whether CHIP participants would demonstrate significantly better cyber hygiene and CSA than a control group. Forty-three undergraduate participants completed our online Qualtrics study, which periodically required cyber hygiene decisions to complete fictional web-browsing tasks. Of these, 20 participants belonged to an experimental group whose cyber hygiene decisions were accompanied by CHIP notifications, and 23 participants belonged to a control group that completed all tasks without notifications.

One goal was to assess whether participants who received CHIP notifications would demonstrate better cyber hygiene than participants who completed the control survey. That is, we assessed whether users would make safer decisions when presented with CHIP notifications compared to traditional situations (no notifications). To make a decision, participants indicated their choices through clickable regions on static screenshot images. They completed one scenario for each of the four cyber hygiene behaviors, with responses coded as either good cyber hygiene (e.g., navigating away from a dangerous website) or bad cyber hygiene (e.g., proceeding to the dangerous website). Preventing password auto-saves, deleting or reporting a phishing email, changing their answer to the account security question, and complying with an unsafe website warning (e.g., not continuing to the site) were all considered safe decisions. Saving the password, replying to or forwarding the phishing email, maintaining the same security answer, and continuing to the potentially dangerous website were considered unsafe decisions. For CHIP participants, the page margins of cyber hygiene decision points were supplemented by a notification window containing additional information about the cyber threat.

Following each cyber hygiene decision, all users completed a modified version of the 10-D SART, a valid and reliable measure of situation awareness [24] originally developed by Selcon and Taylor [25] to evaluate aircrew system design. Advantages to the 10-D SART include high ecological validity, ease of use, and the ability to be administered after various tasks due to the general nature of its questions [24,25].

Independent-samples *t*-tests revealed that CHIP participants made significantly safer decisions during the password-saving (p<.001), phishing email (p<.001), and account security question scenarios (p<.001). CHIP users also demonstrated significantly greater CSA compared to a control group for the phishing email scenario (p= .048) and risky website scenario (p=.032), and when averaged across all four scenarios (p=.048) (see Figure 8).

These findings show promise for CHIP as an interface that promotes cyber hygiene and CSA for specific behaviors. Given that user interactions with CHIP were limited to selections on simple static screenshot images, these results are especially encouraging.

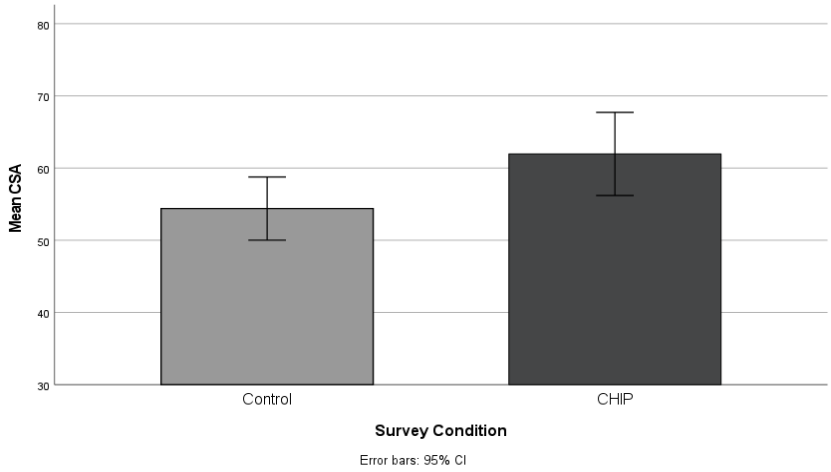


Fig. 8. Mean CSA for each survey condition across all four scenarios.

4 Conclusion

Our goal in describing CHIP's design process is not to produce a formal set of guidelines or principles for developing human-centered cybersecurity systems, but to begin a conversation in this emerging area. Too many current cybersecurity solutions are driven by the needs of large organizations rather than end users themselves. Our solution is primarily targeted toward end users, with implications for the ecosystems *within* users' work environments.

As human-centered solutions like CHIP evolve, it is essential to consider whether these systems could potentially replace traditional cybersecurity training, or simply function as a "red flag" virtual assistant. We must also consider how to respond when

systems like CHIP make mistakes and how these mistakes will be tolerated. Users may prefer real-time animation that only occurs when CHIP has high confidence in a critical issue. Therefore, it may be beneficial to employ a survey to understand users' cybersecurity needs, preferences, and values. This information might positively impact end-users' experience with CHIP.

We faced many challenges in fully testing and implementing CHIP. A specific challenge included how to collect data (e.g., how to scrape this information from a variety of websites) and how to store/encrypt this information (e.g., who should maintain control/own the data). A technical question remains as to how we might collect personal information like login credentials, given a wide variety of authentication processes. It also remains to be seen how we might deliver personal feedback in a consistent manner across a variety of platforms. These challenges will need to be overcome for CHIP to be successful. Simply considering strong authentication, CHIP must access all of the user's passwords and know their preference or employer requirements for authentication. Knowing passwords can combat reuse and make end-users aware of recent breaches (i.e., requiring a password change). Online services have a wide variety of authentication security standards. However, if their employer requires very strong authentication, CHIP can help end-users maintain consistency across their online accounts.

Our initial data demonstrates increased CSA and better cyber hygiene among CHIP users compared to non-users, even when using a static prototype not situated within a real-world scenario. Additional work is needed to make our cybersecurity environment more visible. We as end-users are often in the dark, which reduces motivation to comply with best practices. We are left wondering whether the time and effort required to improve our cyber hygiene keeps us safer or how many threats we actually face. In home security, we are able to see whether a door is locked or a gate is closed. By taking action, we establish a sense of ownership and control over our home security situation, and we feel safer as a result. As designers, we must develop a similar awareness in cyberspace. Users should know their cyber situation (e.g., understand what is happening, know what can be done, how to access help). Increasing CSA ought to encourage users to appreciate the threat, understand their behavior in relationship to the threat, and feel a sense of control over future consequences.

Acknowledgments. 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 cyberinitiative.org. We thank everyone at MI Technical Solutions for their involvement in identifying cyber hygiene concerns and technical constraints.

References

1. Ng, B. Y., & Xu, Y.: Studying users' computer security behavior using the Health Belief Model. In: Pacific Asia Conference on Information Systems (PACIS) 2007 Proceedings, 45, pp. 423-437 (2007).

2. Assante, M. J., & Tobey, D. H.: Enhancing the cybersecurity workforce. IT Professional, 13(1), 12-15 (2011).
3. Aloul, F. A.: The need for effective information security awareness. Journal of Advances in Information Technology, 3(3), 176-183 (2012).
4. Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L.: Exploring game design for cybersecurity training. In: 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 256-262 (2012).
5. Cain, A. A., Edwards, M. E., & Still, J. D.: An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, 36-45 (2018).
6. Carter, A.: The Department of Defense cyber strategy. The US Department of Defense, Washington, DC (2015). https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf, last accessed 2021/6/10.
7. Griffith, V., & Jakobsson, M.: Messin' with Texas: Deriving mothers' maiden names using public records. In: International Conference on Applied Cryptography and Network Security, pp. 91-103, Springer, Berlin, Heidelberg (2005).
8. Rabkin, A.: Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. In: Proceedings of the 4th Symposium on Usable Privacy and Security, pp. 13-23 (2008).
9. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J.: Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 373-382 (2010).
10. Malkin, N., Mathur, A., Harbach, M., & Egelman, S.: Personalized security messaging: Nudges for compliance with browser warnings. In: 2nd European Workshop on Usable Security. Internet Society (2017).
11. Harris, M. A., Patten, K., & Regan, E.: The need for BYOD mobile device security awareness and training. In: Proceedings of the Nineteenth Americas Conference on Information Systems (2013).
12. Caldwell, T.: Training–the weakest link. Computer Fraud & Security, vol. 9, pp. 8-14 (2012).
13. Franke, U., & Brynielsson, J.: Cyber situational awareness – a systematic review of the literature. Computers & Security, 46, 18-31 (2014).
14. Hutchins, E. M., Cloppert, M. J., & Amin, R. M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 113-125 (2011).
15. Denis, C., & Karsenty, L.: Inter-usability of multi-device systems: A conceptual framework. Multiple user interfaces: Cross-platform applications and context-aware interfaces, 373-384 (2004).
16. Google Chrome Developers: Extensions and apps in the chrome web store, https://developer.chrome.com/docs/webstore/apps_vs_extensions/, last accessed 2021/6/9.
17. Rafailidis, D., & Manolopoulos, Y.: Can Virtual Assistants Produce Recommendations?. In: Proceedings of the 9th International Conference on Web Intelligence, Mining and Semantics, pp. 1-6 (2019).
18. Shneiderman, B.: Human-centered artificial intelligence: Three fresh ideas. AIS Transactions on Human-Computer Interaction, 12(3), 109-124 (2020).
19. Geiger, R. S.: Are computers merely "supporting" cooperative work?: Towards an ethnography of bot development. In: Proceedings of the 2013 conference on Computer Supported Cooperative Work Companion, pp. 51-56 (2013).

20. Friedman, V.: Privacy UX: Better notifications and permission requests. Retrieved from https://www.smashingmagazine.com/2019/04/privacy-better-notifications-ux-permission-requests/, last accessed 2021/6/9.
21. MacKenzie, I. S.: Fitts' law as a research and design tool in human-computer interaction. Human-Computer Interaction, 7(1), 91-139 (1992).
22. Proctor, R. W., & Schneider, D. W.: Hick's law for choice reaction time: A review. Quarterly Journal of Experimental Psychology, 71(6), 1281-1299 (2018).
23. Kivetz, R., Urminsky, O., & Zheng, Y.: The goal-gradient hypothesis resurrected: Purchase acceleration, illusionary goal progress, and customer retention. Journal of Marketing Research, 43(1), 39-58 (2006).
24. Endsley, M. R., & Garland, D. J. (Eds.): Situation awareness analysis and measurement. CRC Press (2000).
25. Selcon, S. J. & Taylor, R. M.: Evaluation of the situation awareness rating technique (SART) as a tool for aircrew systems design. Paper presented at the AGARD AMP symposium 'Situational Awareness in Aerospace Operations', pp. 23-52, Neuilly Sur Seine, France (1990).