Cognitive ability and usable security and privacy.

Joakim Kävrestad[1] & Marcus Nohlberg[1]

[1]University of Skövde, Skövde Sweden *firstname.lastname*@his.se

Abstract

Privacy, Information Security, and Cybersecurity (PICS) are related properties that concern anyone (OECD 2019). We rely on digital services and data for our personal life and work-life, and while the benefits are undeniable, digital risks are introduced. PICS is socio-technical and requires that social and technical factors are considered(Al Sabbagh and Kowalski 2012; Paja et al. 2013). Recent reports suggest that human behavior plays a part in most security incidents(EC-Council 2019; Soare 2020). As such, human behavior is an integral part of PICS and requires that users make use of guidelines (such as guidelines for the creation of strong passwords) and tools (such as encryption software) designed to enhance PICS. However, such guidelines and tools do not appear to be adopted by a large enough potion of the users. One explanation given in the literature is a (perhaps perceived) lack of usability (Benenson et al. 2015; Florencio and Herley 2007).

While the need for continued efforts into the usability of PICS tools and guidelines seems apparent, we argue that the domain should be problematized further. We do that by including cognitive ability into the mix of factors that affect usability. The reasons for that are threefold:

1. The cognitive ability determines the amount of effort a user can spend on PICS tools and guidelines.
2. By not including the perspective of cognitive ability, there is a risk of excluding users who, because of a cognitive disability, have a limited cognitive ability which is an inclusion problem.
3. Since persons with cognitive disabilities are working in organizations, just like anyone else, excluding those from the design of PICS tools and guidelines becomes an organizational cybersecurity problem.

We seek to address the problem area described above in a new-started research project where we seek to research the usability of PICS guidelines and tools from the perspective of users with cognitive disabilities. The project aims to identify how PICS tools and guidelines' perceived usability is impacted by cognitive ability. The project will be executed as a design science project to develop a browser plugin that will educate the user on password management, fake news, online fraud, and phishing. In addition to the plugin itself, the project will provide valuable insight into how PICS tools and guidelines can be developed to work for neurotypical users and users with cognitive disabilities and thereby contribute to solving the problems raised above.

Our initial results indicate that the major impact of cognitive disabilities is not that they impact what usability factors are perceived as hindering. Instead, a general usability problem is often much worse for a user with a limited cognitive capacity. This is because a limited cognitive capacity requires the user to spend significantly more energy to complete a cognitively demanding task. Thus, when a neurotypical user may find a poor interface a nuisance, someone with a cognitive disability may not be able to use it at all. In this regard, our initial results suggest that including the perspective of users with cognitive disabilities when designing PICS tools and guidelines will make the tools more usable for everyone. Initial results further show that some PICS functions, such as captchas, are simply impossible to use for some

user groups leading to the tentative conclusion that some design elements must be reconsidered to archive inclusive PICS.

List of references

Al Sabbagh, B., and Kowalski, S. 2012. "St (Cs) 2-Featuring Socio-Technical Cyber Security Warning Systems," *Proceedings title: 2012 international conference on cyber security, cyber warfare and digital forensic (cybersec)*: IEEE, pp. 312-316.

Benenson, Z., Lenzini, G., Oliveira, D., Parkin, S., and Uebelacker, S. 2015. "Maybe Poor Johnny Really Cannot Encrypt: The Case for a Complexity Theory for Usable Security," in: *Proceedings of the 2015 New Security Paradigms Workshop*. pp. 85-99.

EC-Council. 2019. "The Top Types of Cybersecurity Attacks of 2019, Till Date." Retrieved 20201006, 2020, from https://blog.eccouncil.org/the-top-types-of-cybersecurity-attacks-of-2019-till-date/

Florencio, D., and Herley, C. 2007. "A Large-Scale Study of Web Password Habits," *Proceedings of the 16th international conference on World Wide Web*: ACM, pp. 657-666.

OECD. 2019. "Hows Life in the Digital Age?."

Paja, E., Dalpiaz, F., and Giorgini, P. 2013. "Managing Security Requirements Conflicts in Socio-Technical Systems," *International Conference on Conceptual Modeling*: Springer, pp. 270-283.

Soare, B. 2020. "Vectors of Attack." Retrieved 20201006, 2020, from https://heimdalsecurity.com/blog/vectors-of-attack/