

# Advancing Cybersecurity through Civic Skills

**Marianne LINDROTH, Elisa NORVANTO, Sari LATVANEN, Kaisa CULLEN, Mirva SALMINEN, Teemu MATILAINEN, Niko CANDELIN, Yki KORTESNIEMI**

Department of Information and Communications Engineering,  
School of Electrical Engineering, Aalto University, Finland  
marianne.lindroth@aalto.fi

## Abstract

*The rise of sophisticated cybercrime, often perpetrated through linking the devices of unwitting individuals to criminal botnets, has drawn attention to the critical role the cybersecurity skills of individuals play in achieving effective cybersecurity. This paper identifies the key cybersecurity civic skills, explores how these skills have been taught in Europe, and identifies more effective approaches to training. The results highlight the importance of personalised and continuously updated training materials, and the potential of innovative training methods, such as gamification and learning portals.*

**Index terms:** cybersecurity, civic skills, learning framework

## References

- Anderson, R. B. (2019). *Measuring the changing cost of cybercrime*. Boston, US: Presented at: The 2019 Workshop on the Economics of Information Security.
- European Commission. (2021). *2030 Digital Compass: the European way for the Digital Decade*. Brussels: European Commission.
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346.
- Kovalchuk, O. S. (2021). *Econometric Models for Estimating the Financial Effect of Cybercrimes*. Deggendorf, Germany: 021 11th International Conference on Advanced Computer Information Technologies (ACIT). doi: 10.1109/ACIT52158.2021.9548490
- Limnell, J., Alasuutari, M., Candelin, N., Cullen, K., Halonen, O., Helenius, M., ... Virkkunen, P. (2023). *Cyber citizen skills and their development in the European Union*. Espoo: Aalto University.
- Ogu, E. O. (2019). A Botnets Circumspection: The Current Threat Landscape, and What We Know So Far. *Information*, 10(11), 337. doi: <https://doi.org/10.3390/info10110337>
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), 597-611. doi: <https://doi.org/10.1016/j.cose.2011.12.010>

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the Human: The Prevalence Paradox in Cybersecurity. *Human factors*, 60(5), 597-609.

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, 2(3), 573-586. doi: <https://doi.org/10.3390/jcp2030029>

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*. Luxembourg: Publications Office of the European Union. doi: <https://dx.doi.org/10.2760/115376>