

Human-Computer Interaction Considerations When Developing Cyber Ranges

Lynsay A. SHEPHERD¹, Stefano DE PAOLI², Jim CONACHER¹

¹ School of Design and Informatics, Abertay University,
Dundee, United Kingdom

lynsay.shepherd@abertay.ac.uk, j.conacher@abertay.ac.uk

² School of Business, Law and Social Sciences, Abertay University,
Dundee, United Kingdom
s.depaoli@abertay.ac.uk

Abstract

Cyber-attacks are continuing to rise globally. It is therefore vital for organisations to develop the necessary skills to secure their assets and to protect critical national infrastructure. In this short paper, we outline human-computer interaction elements which should be considered when developing a cybersecurity training platform, in an effort to maintain levels of user engagement. We provide an overview of existing training platforms before covering specialist cyber ranges. Aspects of human-computer interaction are explored with regards to their relevance in the context of cyber ranges. We conclude with design suggestions when developing a cyber range platform.

Index terms: cybersecurity, security awareness, cyber range, human-computer interaction, cybersecurity education

References:

- [1]. AIT: Cyber range & training (2020), <https://www.ait.ac.at/en/research-topics/cyber-security/cyber-range-training/> (Accessed 1 July 2020).
- [2]. Amorim, J.A., Hendrix, M., Andler, S.F., Gustavsson, P.M.: Gamified training for cyber defence: Methods and automated tools for situation and threat assessment. In: NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111), (2013).
- [3]. Carroll, J.M.: Human computer interaction (hci). In: The Encyclopedia of Human-Computer Interaction, 2nd Edition, chap. 2, pp. 21–62. The Interaction Design Foundation (2013).
- [4]. Čeleda, P., Čegan, J., Vykopal, J., Továrník, D.: Kypo: A platform for cyber defence exercises. M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization (2015).

- [5]. Cook, A., Smith, R., Maglaras, L., Janicke, H.: Using gamification to raise awareness of cyber threats to critical national infrastructure. In: 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR). BCS (2016).
- [6]. CyberEDU: CTF Cyber Security Challenges Online Platform (2019), <https://cyberedu.ro/> (Accessed 12 July 2020).
- [7]. Duolingo: Duolingo (2020), <https://www.duolingo.com/> (Accessed 1 July 2020).
- [8]. ENISA: Cyber Europe 2020 (2020), <https://www.cyber-europe.eu> (Accessed 12 July 2020).
- [9]. FORESIGHT: Foresight -advanced cyber-security simulation platform for preparedness training in aviation, naval and power-grid environments (2019), <https://foresight-h2020.eu/> (Accessed 30 June 2020).
- [10]. Guralnick, D.A.: User interface design for effective, engaging e-learning. In: Proceedings of the International Conference on E-learning. pp. 22–23. Citeseer (2006).
- [11]. IBM: X-force command cyber tactical operations center (2020), <https://www.ibm.com/security/services/managed-security-services/xforce-command-cyber-tactical-operations-center> (Accessed 1 July 2020).
- [12]. Immersive Labs: The human cyber readiness platform (2020), <https://www.immersivelabs.com/product/benefits/equip-cyber-workforce> (Accessed 1 July 2020).
- [13]. Kaspersky: Cyber Threat Real-Time Map (2020), <https://cybermap.kaspersky.com/> (Accessed 1 July 2020).
- [14]. Klerkx, J., Verbert, K., Duval, E.: Enhancing learning with visualization techniques. In: Handbook of research on educational communications and technology, pp. 791–807. Springer (2014).
- [15]. Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X.: Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv preprint arXiv:2006.11929 (2020).
- [16]. Lewis, C.: Irresistible Apps: Motivational design patterns for apps, games, and web-based communities. Springer (2014).
- [17]. Liferay: Liferay DXP for Portals (no date), <https://www.liferay.com/download-features/l/portal> (Accessed 1 July 2020).
- [18]. Marines-The official website of the United States Marine Corps: DoD Cyber Security Range (2020), <https://www.hqmc.marines.mil/doccsr/> (Accessed 1 July 2020).
- [19]. McKenna, S., Staheli, D., Meyer, M.: Unlocking user-centered design methods for building cyber security visualizations. In: 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). pp. 1–8. IEEE (2015).
- [20]. National Institute of Standards and Technology (NIST): Cyber ranges (2018), <https://www.nist.gov/system/files/documents/2018/02/13/cyberranges.pdf> (Accessed 30 June 2020).
- [21]. OutThink: Cyber Security by CISOs, for CISOs (2020), <https://outthink.io/> (Accessed 12 July 2020).
- [22]. Scholefield, S., Shepherd, L.A.: Gamification techniques for raising cyber security awareness. In: Moallem, A. (ed.) HCI for Cybersecurity, Privacy and

- Trust. HCII 2019., Lecture Notes in Computer Science, vol. 11594, pp. 191–203. Springer, Cham (2019).
- [23]. SecDevOps@Cuse: The Open-Source AWS Cyber Range (2019), <https://github.com/secdevops-cuse/CyberRange> (Accessed 12 July 2020).
- [24]. Secure Code Warrior: Secure your Code, From the Start (2020), <https://securecodewarrior.com/> (Accessed 12 July 2020).
- [25]. Talos: Cyber Attack Map (2020), <https://talosintelligence.com/fullpagemaps/pulse> (Accessed 1 July 2020).
- [26]. Tondello, G.F.: An introduction to gamification in human-computer interaction. XRDS: Crossroads, The ACM Magazine for Students 23(1), 15–17 (2016).