Cyber threats to businesses and organizations have increased since the global pandemic. However, during these circumstances, there is a shortage of experts to defend against these cyber-attacks. Thus, cybersecurity education is becoming important, and there is a need to equip students to be highly skilled cybersecurity experts. Research has demonstrated that experiential learning is a more effective pedagogical approach than traditional lecture-based instruction in teaching educational concepts to students. The present review investigates and synthesizes empirical evidence of hands-on instructional tools using Interactive, Constructive, Active and Passive learning processes. The review synthesized instructional practices such as comics, games, lab activities, simulations, and live competitions from 41 individual studies used to teach K-12 and college students. The study found that engaging in hands-on activities such as games to teach cybersecurity concepts improves learning performance and motivation. This study highlights areas for further research and outlines the advantages for school administrators, educators, and other stakeholders involved in designing and implementing cybersecurity curricula. In addition, the practical implications and limitations of the study are discussed below.

Keywords: cybersecurity, education, cyber-threats, phishing, engagement