1. Record Nr. UNISA996547960803316

Titolo	Cybersecurity Teaching in Higher Education [[electronic resource] /] / edited by Leslie F. Sikos, Paul Haskell-Dowland
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	9783031242168 9783031242151
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (144 pages)
Disciplina	005.8071
Soggetti	Education—Data processing Computer security Computer networks—Security measures Data protection Computers and Education Principles and Models of Security Mobile and Network Security Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Chapter. 1. Challenges and Opportunities of Teaching Cybersecurity in UK University Computing Programmes -- Chapter. 2. Using the Delphi Method to Elicit Requirements for an International Master’s Program in Information Security Management -- Chapter. 3. Designing and Developing a Scenario-Based Curriculum for Cyber Education in HE -- Chapter. 4. Enabling teamwork in Cybersecurity courses -- Chapter. 5. Towards a Light-Weight Certification Scheme for Cybersecurity MOOCs -- Chapter. 6. Learning Environments for Digital Forensics Teaching in Higher Education.
Sommario/riassunto	This book collects state-of-the-art curriculum development considerations, training methods, techniques, and best practices, as well as cybersecurity lab requirements and aspects to take into account when setting up new labs, all based on hands-on experience in teaching cybersecurity in higher education. In parallel with the

increasing number and impact of cyberattacks, there is a growing demand for cybersecurity courses in higher education. More and more educational institutions offer cybersecurity courses, which come with unique and constantly evolving challenges not known in other disciplines. For example, step-by-step guides may not work for some of the students if the configuration of a computing environment is not identical or similar enough to the one the workshop material is based on, which can be a huge problem for blended and online delivery modes. Using nested virtualization in a cloud infrastructure might not be authentic for all kinds of exercises, because some of its characteristics can be vastly different from an enterprise network environment that would be the most important to demonstrate to students. The availability of cybersecurity datasets for training and educational purposes can be limited, and the publicly available datasets might not suit a large share of training materials, because they are often excessively documented, but not only by authoritative websites, which render these inappropriate for assignments and can be misleading for online students following training workshops and looking for online resources about datasets such as the Boss of the SOC (BOTS) datasets. The constant changes of Kali Linux make it necessary to regularly update training materials, because commands might not run the same way they did a couple of months ago. The many challenges of cybersecurity education are further complicated by the continuous evolution of networking and cloud computing, hardware and software, which shapes student expectations: what is acceptable and respected today might be obsolete or even laughable tomorrow.