Journal of Cybersecurity Education, Research and Practice

Volume 2020 | Number 2 Article 1

2020

Editorial

Michael E. Whitman
Kennesaw State University, mwhitman@kennesaw.edu

Herbert J. Mattord
Kennesaw State University, hmattord@kennesaw.edu

Hossain Shahriar
Kennesaw State University, hshahria@kennesaw.edu

Follow this and additional works at: https://digitalcommons.kennesaw.edu/jcerp

 Part of the Information Security Commons, Management Information Systems Commons, and the Technology and Innovation Commons

Recommended Citation

Whitman, Michael E.; Mattord, Herbert J.; and Shahriar, Hossain (2020) "Editorial," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2020 : No. 2 , Article 1.
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss2/1

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Editorial

Keywords
editorial

This article is available in Journal of Cybersecurity Education, Research and Practice:
https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss2/1

FROM THE EDITORS:

Greetings and welcome to the ninth issue of the Journal of Cybersecurity Education, Research and Practice (JCERP). Despite the global effects of the COVID-19 pandemic during 2020, the cybersecurity education and research effort has not stopped. In fact, we have noticed new kinds of cyber threats have emerged as more Internet and online services are being used for remote work and daily activities. This pandemic also brought new challenges and opportunities to effectively deliver cybersecurity curriculum across institutes.

We thank to all authors who have submitted their articles in this journal. As our journal strives to publish high quality articles, we are also pleased to share that the Journal of Cybersecurity Education Research and Practice is now indexed in the DOAJ, where anyone looking for a reputable, open access journal can find it. Here's the link to the listing.

In This Issue

In Volume 2020, Issue 2, we are pleased to share the following articles:

In the article, “GDOM: Granulometry For The Detection of Obfuscated Malware”, John Aruta and Paul Schembari demonstrated that mathematical morphology method of granulometry is a tool for the detection of malware, including obfuscated malware. They observed that files exhibit identifiable texture patterns when converted to images, and that these patterns can be detected by a granulometry filter. The work further aligns with the learning goals of a thesis requirement

As the Internet is essential for work and activities among young generations, it also brings the challenge to remain safe again online threats such as cyberbullying. In the article, "An Assessment of Internet Use and Cyber-risk Prevalence among Students in Selected Nigerian Secondary Schools", Adeola Opesade and Abiodun Adetona, performed an empirical analysis among secondary school students and reported while majority teenagers use the Internet for limited time during the week, there is a considerable exposure to different cyber-risk behaviors. Some common risks experienced by students include cyberbullying and provocative contents. They provided some suggestions to minimize the risk of using Internet for the teenagers.

In the article, "Applying High Impact Practices in an Interdisciplinary Cybersecurity Program", Brian Payne and colleagues integrated five high impact practices into the interdisciplinary cybersecurity undergraduate program. They described efforts on developing learning communities, fostering undergraduate research projects, teaching select courses using service-learning activities, expanding internship opportunities, and connecting interdisciplinary courses through ePortfolios. The authors shared their experiences in integrating high impact practices into the curricula of Old Dominion University.

Social engineering is one of the biggest security issues facing both individuals and corporations today. Many academic institutions now teach concepts related to security and penetration testing. In the article, "Gophish: Implementing a Real-World Phishing Exercise to Teach Social Engineering", Andy Lust and Jim Burkman, provided a model for a single course project that gave students an experiential learning experience on social engineering. In cooperation with a participating corporation, a phishing exercise was utilized to instruct students in both the technical

and behavioral aspects of social engineering. Students developed a statement of purpose document, designed the system, setup the environment, and conducted a phishing exercise on actual employees. Students then took the results and presented the information to the corporation for usage in security awareness training.

We hope you find this issue useful and interesting and that you will consider submitting one of your own works to JCERP for consideration.

Dr. Mike Whitman
Dr. Herb Mattord
Dr. Hossain Shahriar