The Challenges Of Identifying Dangers Online And Predictors Of Victimization

By: **Catherine D. Marcum**

Abstract

This short paper will provide an overview of the impressive pieces included in this issue of the International Journal of Cybersecurity Intelligence and Cybercrime. This issue includes articles on the following pertinent topic, utilizing a range of approaches and methodologies: 1) online credibility; 2) cyberbullying; and 3) unauthorized access of information. An emphasis on the importance of policy development and better protection of potential victims is a common thread throughout the issue.

Marcum, C. D. (2021). The Challenges of Identifying Dangers Online and Predictors of Victimization, International Journal of Cybersecurity Intelligence & Cybercrime, 4(1), 1-2. https://www.doi.org/10.52306/04010121QNFW5915. Publisher version of record available at: https://vc.bridgew.edu/ijcic/vol4/iss1/1/

International Journal of Cybersecurity Intelligence & Cybercrime

Volume 4 | Issue 1 Article 1

4-2021

The Challenges of Identifying Dangers Online and Predictors of Victimization

cyberbullying, cybervicimization, Internet, access

Recommended Citation

Marcum, C. D. (2021). The Challenges of Identifying Dangers Online and Predictors of Victimization, International Journal of Cybersecurity Intelligence & Cybercrime, 4(1), 1-2. https://www.doi.org/10.52306/04010121QNFW5915

Marcum, C. D. (2021). *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(1), 1-2.

The Challenges of Identifying Dangers Online and Predictors of Victimization

Catherine D. Marcum*, Appalachian State University, U.S.A.

Keywords; cyberbullying, cybervicimization, Internet, access

Abstract:
This short paper will provide an overview of the impressive pieces included in this issue of the *International Journal of Cybersecurity Intelligence and Cybercrime*. This issue includes articles on the following pertinent topic, utilizing a range of approaches and methodologies: 1) online credibility; 2) cyberbullying; and 3) unauthorized access of information. An emphasis on the importance of policy development and better protection of potential victims is a common thread throughout the issue.

Introduction

In a world where technology is a mainstay in daily life and access to the Internet is a constant necessity to obtain information, communicate, or entertain, the dangers lurking behind each electronic corner is often disregarded. The current issue of the *International Journal of Cybersecurity Intelligence and Cybercrime* provides an in-depth examination of the very real dangers present online, specifically noting behaviors of cyber-offenders that online users should be aware. This issue includes articles on the following pertinent topics: 1) online credibility; 2) cyberbullying; and 3) unauthorized access of information. As can be seen in this impressive set of contemporary literature, there is a range of approaches and methodologies utilized in these studies. Provided below is a brief overview of the research featured in this issue.

Jenny Wells, Dana LaFon and Margaret Gratian (2021, this issue) delve into the challenge of determining if individuals providing information online can be considered credible in their article, "Assessing the credibility of cyber adversaries." In the age where any private citizen to large corporation can create websites, data banks and other houses of intellectual property, it can be extremely difficult to discern who and what to trust. Wells and colleagues provide an extensive examination on current literature involving online credibility, trust, deception, and fraud detection in an effort to consolidate this information to understand adversary online credibility. The latter part of the piece provides a suggested model that includes examining information, as well as user and interaction characteristics, to best inform an online user's assessment of online credibility (Wells et al., 2021).

*Corresponding author
Catherine D. Marcum, Ph.D., Department of Government and Justice Studies, Appalachian State University, PO Box 32107, Boone, NC, 28608, U.S.A.

Email: marcumcm@appstate.edu

In the article, "Cyberbullying: Its Social and Psychological Harms Among Schoolers," Hyeyoung Lim and Hannarae Lee (2021, this issue) provide a unique and much needed contribution to cyberbullying literature through their investigation of the effectiveness of treatments for peer victims to reduce and recover from their social and psychological suffering of cyberbullying. While much of the literature examines predictors of cyberbullying victimization or offending, there is very little that provides insight into treatment for those who suffer. This study used data from the National Crime Victimization Survey-School Crime Supplement data in 2011 and 2013 to examine the impact of two emotional support groups (i.e., adult and peer groups) on cyberbullying victims' social and psychological harm. Results indicated success from both age groups in regard to reduced social and psychological harm inflicted by cyberbullying victimization, allowing Lim and Lee (2021) to provide suggestions for future program planners to better help victims of this form of cybercrime.

The last article in this issue, "Cyber-Victimization Trends in Trinidad and Tobago: An Empirical Research," applies a theoretical basis to attempt to explain two forms of cybervictimzation: cyberbullying and unauthorized access. Smith and Stamatakis (2021, this issue) utilized Routine Activity Theory (RAT) to examine online-related activities that potentially increase the likelihood of cybercrime victimization in the Caribbean country of Trinidad and Tobago. The findings of the study indicated online activities that increase target exposure and accessibility increased victimization risk, while physical methods of guardianship were weakly protective. Smith and Stamatkis (2021) asserted they were better able to explain cyberbullying compared to victimization via unauthorized access with the RAT application.

Concluding Remarks

Part of our responsibility as criminologists and cyber-experts is to not only perform empirical research, but use it to help stakeholders create policies, programs and laws to benefit the billions of people who use technology and the Internet on the regular basis. The studies featured in this issue of the *International Journal of Cybersecurity Intelligence and Cybercrime* provide recommendations and findings that can be applied to real-life educational and training programs to better protect Internet users, especially those vulnerable to victimization. These scholars should be commended for their contributions from their efforts and we look forward to seeing how the fields of cybersecurity and cybercrime will grow because of them.

References

Lim, H. & Lee, H. (2021). Cyberbullying: Its social and psychological harms among schoolers. *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(1), 25-45.

Smith, T. & Stamatakis, N. (2021). Cyber-victimization trends in Trinidad and Tobago: An empirical research. *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(1)*,* 46-63.

Wells, J., LaFon, D., & Gratian, M. (2021). Assessing the credibility of cyber adversaries. *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(1)*,* 3-24.