Cyber-Victimization Trends in Trinidad & Tobago: The Results of an Empirical Research

Nikolaos STAMATAKIS, Troy SMITH
United Arab Emirates University
n.stamatakis@uaeu.ac.ae

Abstract
In the last years, Caribbean countries have become attractive targets for cybercrime due to increased economic success and online presence with a low level of cyber resilience. The available data on cybersecurity and critical infrastructure shows that cyber-attacks and -incidents, particularly those carried out with criminal intent, have been increasing in frequency and sophistication. This study examines the variables or more specifically the online-related activities in Trinidad and Tobago that affect cybercrime victimization by using the Routine Activity Theory. Using Bayesian classifiers and Facebook as a data collection instrument, the analysis of the quantitative data demonstrates that the use of only the accuracy measures to judge model performance or compare models could be misleading. It also shows that awareness and education related to cybercrime is necessary to persons of all ages, suggesting that in order to move forward as a digital economy, the region must secure the trust of users by providing an open, stable, and secure environment.

Index terms: Cybercrime, Victimization, Routine Activity Theory, Trinidad & Tobago

References:


