International Journal of Cybersecurity Intelligence & Cybercrime

Volume 4 | Issue 1 Article 4

4-5-2021

# Cyber-victimization Trends in Trinidad & Tobago: The Results of An Empirical Research

Cybertechnology has brought benefits to the Caribbean in the form of new regional economic and social growth. In the last years, Caribbean countries have also become attractive targets for cybercrime due to increased economic success and online presence with a low level of cyber resilience. This study examines the online-related activities that affect cybercrime victimization by using the Routine Activity Theory (RAT). The present study seeks to identify activities that contribute to different forms of cybercrime victimization and develop risk models for these crimes, particularly the understudied cyber-dependent crimes of Hacking and Malware. It also aims to explore if there are similarities or differences in factors leading to victimization, which correlate to the classification of crimes as either cyber-dependent or cyber-enabled. The data analysis suggests that there is significant applicability for RAT in explaining Online Harassment victimization, while the usability of the RAT for predicting Malware victimization proved to be minimal, with only two significant variables being identified, with both being associated with Capable Guardianship.

cyber-victimization, routine activity theory, Trinidad & Tobago, cyberbullying, unauthorized access



Recommended Citation
Smith, T., & Stamatakis, N. (2021). Cyber-victimization Trends in Trinidad & Tobago: The Results of An Empirical Research, International Journal of Cybersecurity Intelligence & Cybercrime, 4(1), 46-63. https://doi.org/10.52306/04010421JINE3509

Smith, T., & Stamatakis, N. (2021). *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(1), 46-63.

# Cyber-victimization Trends in Trinidad & Tobago: The Results of An Empirical Research

Troy Smith*, University of Trinidad and Tobago, Trinidad and Tobago
Nikolaos Stamatakis, United Arab Emirates University, United Arab Emirates

*Keywords; cyber-victimization, routine activity theory, Trinidad & Tobago, cyberbullying, unauthorized access*

**Abstract:**
Cybertechnology has brought benefits to the Caribbean in the form of new regional economic and social growth. In the last years, Caribbean countries have also become attractive targets for cybercrime due to increased economic success and online presence with a low level of cyber resilience. This study examines the online-related activities that affect cybercrime victimization by using the Routine Activity Theory (RAT). The present study seeks to identify activities that contribute to different forms of cybercrime victimization and develop risk models for these crimes, particularly the understudied cyber-dependent crimes of Hacking and Malware. It also aims to explore if there are similarities or differences in factors leading to victimization, which correlate to the classification of crimes as either cyber-dependent or cyber-enabled. The data analysis suggests that there is significant applicability for RAT in explaining Online Harassment victimization, while the usability of the RAT for predicting Malware victimization proved to be minimal, with only two significant variables being identified, with both being associated with Capable Guardianship.

## Introduction

Cybercrime is a relatively new phenomenon and the intricacies of this form of criminality are yet to be fully understood. Research into cybercrime victimization is still scarce although cybercrime is increasing rapidly within the Caribbean and Latin America regions (Caribbean Cyber Security Centre, 2019; Kshetri, 2013). Therefore, this research aims to contribute to the existing literature and the understanding of cybercrime in two ways: 1) by identifying the activities that contribute to two forms of cybercrime victimization and developing risk models for these crimes, and 2) by exploring the similarities and differences in factors that lead to victimization in Trinidad and Tobago in relation to past studies in North America and Europe. This will contribute to understanding the state of cybercrime in Trinidad and Tobago. Further, it will fill the data void that past research has left, which can aid in identifying if geographic location may affect cybercrime victimization patterns either through theoretical analysis or meta-analysis. Further, this research adds to the growing application of machine learning in research studies (Schmidt, Marques, Botti & Marques, 2019).

The Routine Activity Theory (RAT) was chosen for this study because it has been successfully applied in the examination of cybercrime victimization (e.g., Bossler & Holt, 2009; Bossler, May, & Holt, 2012; Choi, 2008; Kranenbarg, Ruiter, & van Gelder, 2019; Leukfeldt & Yar, 2016; Nasi, Oksanen, Keipi, & Rasanen, 2015; Reyns, Fisher, Bossler, & Holt, 2018). In addition, comparison to previous research will be more intuitive given the same theoretical base for the identification of independent variables was used. In addition,

*Corresponding author
Troy Smith, Institute of Criminology and Public Safety, University of Trinidad and Tobago, Trinidad and Tobago
Email: troy.smith078@we.edu.utt.tt

RAT has proven to be a highly generalizable theory that examines both individual and situational factors. However, the literature reveals that while researchers have examined aspects of RAT with some consistency in the theory's applicability, majority of the studies considered have had the following shortcomings that are addressed in this study: 1) Only one form of cybercrime is studied in isolation with a focus on people-centric victimization whereas this study includes two forms of cybercrime, namely unauthorized access (techno-centric) and cyberbullying (people-centric) (Holt & Bossler, 2014; Marcum, Ricketts, & Higgins, 2010; Moore, Guntupalli, & Lee, 2010; Navarro & Jasinski, 2012; Reyns, 2015). These specific crimes were chosen as they are known to be prevalent in Trinidad and Tobago based on reports by local Law Enforcement and the Organization of American States (OAS). 2) All three constructs (i.e., motivated offender, target suitability, and capable guardianship) have not been given equal attention in past research projects. The theory's basis lies in the convergence of its three constructs in time and space. In June 2016, the Cyber Crime Bill and amendments to the Data Protection Act became a priority on the Government's legislative agenda and a new round of consultations was initiated. However, to date (2019), there is no dedicated law that governs cybercrime in Trinidad and Tobago (Dhoray, 2020). The successful prosecution of cybercrime is still hampered by the absence of a formal mechanism to report cyber incidents as well as a lack of digital capacity to investigate charges against this type of crime.

## Conceptual Framework

The Routine Activity Theory focuses on the pivotal role opportunity plays in crime or disorder (Clarke, 2018). The approach of RAT is based on two basic premises: first, crime occurs when motivated offenders are in proximity to targets with insufficient guardianship; and second, on the probability of convergence leading to the criminal act being affected by an individual's 'routine activities' (Cohen & Felson, 2003; DeGarmo, 2011). Routine activities can be defined as generalized temporal and spatial patterns of recurrent and prevalent social activities, irrespective of the biological and cultural origins of the population or any generalized patterns of social activities in society (Cohen & Felson, 1979; Wikström, 2018). This suggests that previous criminal intent, experience or mind-set are not necessary for a crime to occur; rather crime may be opportunistic and only require an individual to determine that at that moment the potential benefits outweigh the risk (Clarke, 1999). Therefore, the theory avoids speculation about the source of the offenders' motivation, which immediately distinguishes it from most other criminological theories.

## Methodology

The cybercrime victimization/experiences examined in this study are unauthorized access and cyberbullying. The effects of online exposure, location, and digital and personal guardianship that relate to the tenets of RATs factors of target suitability (exposure/visibility and accessibility) and capable guardianship were examined as the primary independent variables using the supervised machine learning algorithm, random forest on data collected from a sample of Facebook users in Trinidad and Tobago.

### *Objectives*

1) To identify cybercrime patterns among Facebook users in Trinidad and Tobago
2) To investigate the predictors of two types of cybercrime victimization experiences separated using a binary classification for cybercrimes; i.e.

- Techno-centric/computer – These cybercrimes were made possible through the development of ICTs and cannot exist without such a framework.
- People-centric – These cybercrimes encompass all crimes that existed before the advent of ICTs and they can now be digitalized.

### *The Sample*

The target population for this study was Facebook users over 18 years of age and located in Trinidad and Tobago. There were 715 500 Facebook users in Trinidad and Tobago in June 2019, which accounted for 51.9% of the country's population (Central Statistical Office, 2019; Hootsuite and We Are Social, 2019). Facebook could potentially address the issue of overreliance on samples based on secondary data, or student populations in past research (Kosinski, Matz, Gosling, Popov, & Stillwell, 2016; Samuels & Zucco, 2013; Zucco, Luna, & Baykal, 2017)). Further, this project was self-funded hence access to a large sample must be balanced with the cost of data collection. Facebook allows access to large and diverse samples of persons in their natural environment while being parsimonious (Kosinski et al., 2016).

### *Data Collection*

Possibly, the least expensive and most efficient way to utilize Facebook as a recruitment pool is by snowball sampling (Dusek, Yurova, & Ruppel, 2015). The initial seed consisted of Facebook friends of the researcher, and it was made up of 450 people of varying ages, ethnicities, and geographic locations within Trinidad and Tobago. The participants were either male or female residents of Trinidad and Tobago who were over18 years and users of Facebook. From April 1, 2019 to September 1, 2019, a self-report survey designed to measure the main constructs of the RAT was distributed and allowed to propagate among Facebook users. The collection of data ceased when a two-week period passed without any new submissions. At the end of the collection period, 105 surveys had been submitted and out of those, only 94 were useable because the others were either blank or the participants did not agree to participate.

### *Dependent Variables*

The Dependent variables in this study were "Unauthorized Access" and "Cyberbullying". These variables were coded as dichotomous (No = 0, Yes = 1).

***Unauthorized access***. It is the subversion of a computer, system or network for malicious purposes to access content or control the device without the owner's permission. Example, hacking of a computer or email to access information or to send messages to associates of the legitimate owner to fraudulently obtain funds, steal information, or prevent normal operation.

***Cyberbullying.*** This is any activity that occurs online with the intention of humiliating and terrorizing the victim. This includes instant or text messaging harassment, password and digital pictures stealing, and creation of fake social media accounts.

### *Independent Variables*

The independent variables observed in this study are capable guardianship, and target suitability (target exposure and target accessibility). These variables are based on the theoretical constructs of the RAT

and cannot be directly observed. These variables are based on the theoretical constructs of the RAT and cannot be directly observed. The operationalization of the observed variables used as proxies to these constructs and their respective operational definitions are as follows:

***Target accessibility.*** The accessibility of targets by motivated offenders was measured using five survey items reflecting activities that may create opportunities for online victimization through accessibility or online visibility. The variables measuring Internet browsing hours, online shopping hours, social media hours, watching adult content, and downloading music or videos represent the time spent per day by the respondent engaging in these online activities. Response choices included: less than 1 hour a day; at 1-2 hours; 2-3 hours; 3-4 hours, 4-5 hours; 5-6 hours and More than 6 hours. Responses were coded with a value of 1 indicating less than 1-hour daily participation in the online routine, and 5 representing more than 6 hours a day.

***Target exposure.*** Target exposure was measured using three survey items reflecting activities that make an individual appear more attractive to an offender. It was measured by the degree of self-disclosure of personal information in various online settings, which includes nonverbal communication such as pictures posted of self, posting of personal information, and/or direct sharing of this information with persons online. The variables measured the number of times a user posts their picture, personal information, and location online per week. Response choices included: less than 2 times; 3-4 times; 5-6 times; 3-4 hours, 4-5 times and more than 5 times. Responses were coded with a value of 1 indicating less than 2 times per week engaging in the online routine, and 5 representing more than 6 times a day.

***Capable guardianship.*** 1) Physical guardianship denotes software applications, such as antivirus, firewall, and anti-spyware, which are developed to guard/protect computer systems and networks from offenders. The concept of physical guardianship, sometimes called technical guardianship, is examined in several works but only with a question on the use of anti-virus software (Bossler & Holt, 2009; Choi, 2008; Ngo & Paternoster, 2011; Reyns, Henson, & Fisher, 2011). However, this research found it necessary to expand this to include areas related to email and web browsing, which tend to be areas assessed for providing increased accessibility to a motivated offender (Bossler & Holt, 2009; Choi, 2008; Marcum, 2010).
2) Personal guardianship was measured using three items that assessed the potential target's skill level and knowledge with computers, technology, and awareness of victimization risk. The responses were coded on a 5-point scale where at the lower end 1 represents that the respondent Strongly Disagrees and at the upper end 5 represents that the respondent Strongly Agrees.

***Control Variables / Demographics.*** Findings from various studies on victimization in the terrestrial world reveal that the demographic characteristics of people are closely connected to victimization (Holtfreter, Reisig, & Blomberg, 2006; Reyns, 2013; Yucedal, 2010). Therefore, to identify the relationship between the dependent and independent variables, these potentially contributing factors must be controlled. To control the demographic characteristics of the respondents' data, it was necessary to collect data on their sex and age.

### *Procedure*

The independent variables derived from the RAT were assessed in the first instance using the random forest algorithm to develop predictive models. The random forest algorithm is an ensemble learning method

used for classification i.e. it strategically generates multiple decision trees, which are combined to produce the final model (McDaniel, 2018; Zhu, Qiu, Ergu, Ying, & Liu, 2019). Use of random test in this study is beneficial as it allows effective visualization of interrelationships and the cumulative effect of predictors on the responses; i.e., the strength of the relationship of the covariates with the response variable is measurable. In addition, random forest can deal with "small n large p"-problems, high-order interactions, correlated predictor variables, unbalanced data sets, and is generally unsurpassed among current algorithms (Zhu et al., 2019).

However, random forest does not indicate the size or direction of the effect on the outcome variable. To fill the gap Logistic Regression was used to determine the direction/sign of the effect and how they individually changed the outcome i.e. the odds of becoming a victim. Assessment of the size of the effect and its direction was given by the odds ratios and correlation coefficients provided for the variables in question.

To determine the predictive ability of the RAT in conjunction with the learning algorithm performance metrics were used. It was expected that the datasets may be imbalanced so accuracy was not used as the only metrics for model performance. Other metrics which are more robust in relation to imbalance were chosen. Descriptions of the performance metrics used are given below:

Accuracy is the ratio of correctly predicted cases

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

F-Measure or more specifically the F1-Score is the harmonic mean of precision and recall

$$F_1 \text{ - Score} = \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}}$$

MCC, is a measure of the correlation between the observed and anticipated classes using the data contained in the confusion matrix (Song, Guo, & Shepperd, 2018; Chicco & Jurman, 2020). Unlike Accuracy and even F1-Score the MCC considers both the model's success of predicting the positive and negative classes (Delgado & Xavier-Andoni, 2019).

$$MCC = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$$

The ROC AUC is the area under a two-dimensional plot of the true positive rate (TPR) against the false positive rate (FPR) that illustrates the performance of the classifier over a range of threshold values given the data in the testing set. The performance of the classifier is considered better as the values tends to 1. The benefit of the ROC AUC is that allows a user to potentially optimize the classifier by changing the threshold value in cases of real-world application. The data was split using 20% as testing data and validation was performed using a leave-one-out method to maximize the limited available data.

## Results

The presentation of the findings of the questionnaire survey starts by assessing the demographic information and comparing the control variables to the Trinidad and Tobago population. This is followed by an analysis of the remaining variables using random forest and logistic regression.

Before performing any statistical analysis, all the collected data were tested. Initially, the Little's Missing Completely at Random (MCAR) test was performed on the collected survey data to ascertain whether the data had missing values. The Little's MCAR test was performed on the data and returned a p-value of 0.8. The null hypothesis for this test is that data is missing completely at random and does not follow a particular pattern that is dependent on the data values (Garson, 2015; Little, Jorgensen, Lang, & Moore, 2014). Since the p-value is greater than 0.05 the null hypothesis is rejected i.e. the data is missing completely at random (Beaujean, 2014).

The characteristics of the data collected can be assessed by conducting a reliability test on the scales used to capture the information of interest. In this case, Cronbach's alpha is preferable because it indicates the reliability of the data set and as a result, its suitability for statistical analysis. It also measures the internal consistency or reliability of a data set, which is one of the considerations used to ascertain the suitability of a data set for statistical analysis (e.g., factor analysis) (Parsian & Dunning, 2009; Sijtsma, 2009). In this study, the overall results of the questionnaire are satisfactory as the Cronbach alpha coefficients are all ≥0.50 (see Table 1) (Taber, 2018; van Griethuijsen et al., 2015).

Table 1. *Cronbach's Alpha Coefficient for Reliability Analysis*

| Scale | Cronbach's Alpha | Cronbach's Alpha based on standardized items | Number of items |
|---|---|---|---|
| Target Suitability | 0.624 | 0.645 | 3 |
| Target Exposure/ Accessibility | 0.572 | 0.578 | 5 |
| Physical Guardianship | 0.751 | 0.752 | 3 |
| Personal Guardianship | 0.520 | 0.525 | 3 |

### *Demographics*

Two demographic variables were assessed in the questionnaire, namely age and gender. In line with the Facebook demographics for Trinidad and Tobago, the survey shows a greater representation of females than males, with 54.3% of the respondents being female and 45.7% being male. This gives a sex ratio of 1.19, which is close to the 1.12 sex ratio of Facebook but represents an over overrepresentation of females when compared to the national sex ratio of 0.99 (Central Statistical Office, 2019) (see Table 2).

Table 2. *Distribution of Participants by Gender*

| Gender | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|
| Male | 43 | 45.7 | 45.7 | 45.7 |
| Female | 51 | 54.3 | 54.3 | 100.0 |
| Missing | 0 | 0.0 | | |
| Total | 94 | 100.0 | | |

All age groups were represented in the sample, with the highest number of participants coming from the '35-44" age group (32 participants) and the lowest was the "55 and over" age group (7 participants). This information is summarized in Table 3. The mean age of the participants was found to be 34.8, and this was compared to the population mean of 34.3 using a Bayesian one-sample t-test. The results of the t-test are given in Table 4 and a graph showing the sequential analysis of the t-test with a robustness check (sensitivity prior to selection) is also presented in Figure 1. The Bayes Factor (BF01) of 7.998 shows that the sample data is statistically similar to the population and the sequential analysis shows that the sample size was more than sufficient to accurately select the null hypothesis of Ho: μ1 = μ2.

Table 3. *Frequency of Ages*

| Age | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|
| 15-24 | 22 | 23.4 | 23.4 | 23.4 |
| 25-34 | 22 | 23.4 | 23.4 | 46.8 |
| 35-44 | 32 | 34.0 | 34.0 | 80.9 |
| 45-54 | 11 | 11.7 | 11.7 | 92.6 |
| 55 and over | 7 | 7.4 | 7.4 | 100.0 |
| Missing | 0 | 0.0 | | |
| Total | 4 | 100.0 | | |

| | | | | | 95% Credible Interval | |
|---|---|---|---|---|---|---|
| | N | Mean | SD | SE | Lower | Upper |
| Age | 94 | 34.80 | 11.22 | 1.157 | 32.51 | 37.10 |

Table 4. *Bayesian One-Sample T-Test (Age)*

| | $BF_{01}$ | Error% |
|---|---|---|
| Age | 7.998 | 1.186e-4 |

Note. 1)Respondents were all over 18, however, for comparability to national statistics grouping the age group was written as 15-24. 2) For the test, the alternative hypothesis specifies that the population mean is different from 34.3.

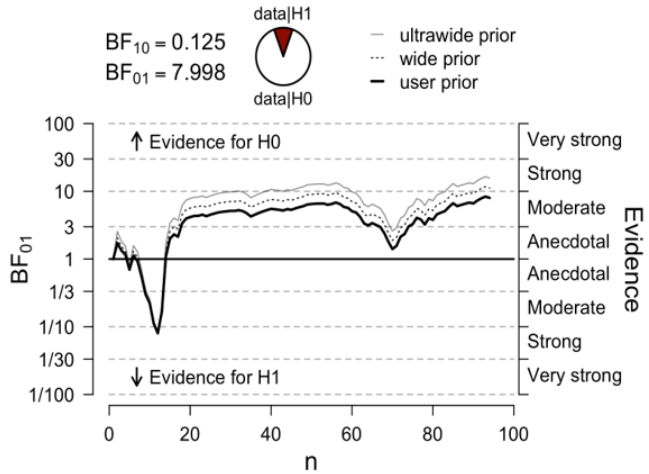


*Figure 1.* Sequential Analysis at 95% Confidence Interval with Robustness Check

Overall, 40% of the respondents were victims of at least one of the two forms of cybercrime. When comparing the prevalence of the different forms of cybercrime victimization, unauthorize access was twice as prevalent as cyberbullying i.e. 18.1% of respondents were cyberbullied while 34.1% respondent were victims of Unauthorized Access.

Table 5 provides the distribution of cybercrime victims split by the classes of respective demographic variables of sex and age for each type of cybercrime observed. The table provides the interclass percentage – this is the percentage of cybercrime victims among/between all classes for that variable – and the intra-class percentage, which is the percentage of cybercrime within the class for that variable. The intra-class percentage is provided as a means of normalizing the data to compare risk in each class because the classes were not equally represented.

Table 5. *Distribution of Cybercrime Victims Split by Demographic Classes*

| Unauthorized Access | | | | | |
|---|---|---|---|---|---|
| Sex | Interclass (%) | Intraclass (%) | Age | Interclass(%) | Intraclass (%) |
| Male | 37.5 | 27.9 | 15-24 | 15.6 | 22.7 |
| Female | 62.5 | 39.2 | 25-34 | 18.8 | 27.3 |
| | | | 35-44 | 34.4 | 34.4 |
| | | | 45-54 | 28.1 | 81.8 |
| | | | 55 + | 3.1 | 14.3 |
| Cyberbullying | | | | | |
| Sex | Interclass (%) | Intraclass (%) | Age | Interclass(%) | Intraclass (%) |
| Male | 29.4 | 11.6 | 15-24 | 52.9 | 40.9 |
| Female | 70.5 | 23.5 | 25-34 | 29.4 | 22.7 |
| | | | 35-44 | 11.8 | 6.3 |
| | | | 45-54 | 5.9 | 9.1 |
| | | | 55 + | 0.0 | 0.0 |

For both unauthorized access and cyberbullying female participants were twice as likely to report victimization than their male counterparts. The intraclass analysis shows that this observation holds particularly true for cyberbully as the prevalence among females is twice the prevalence among males. Cases of cyberbullying were particularly high among persons in the "15-24" age group. The lowest instances of cyberbullying were witnessed in the "55 and over" age group. In relation to unauthorized access the occurrences were spread among the age groups observed. However, notably the age group of "45-54" showed the highest relative prevalence with 82% of the persons within that age bracket reporting victimization. Overall, from the initial analysis it appears that cyberbullying is most prevalent among young females. Unauthorized access is also most prevalent among females, however, age does not appear to be necessarily a key factor.

### *Models Inferential Statistics – Classifiers*

This section presents the results of model development using random forest and logistic regression. The variables tested are given in Table 6 with the abbreviations used to reference them in the text.

Table 6. *Abbreviations Used to Represent the Variables Under Review in this Research*

| Variables | Abbreviation |
|---|---|
| Target Exposure (Frequency of the activity) | |
| Posting pictures online | (E1) |
| Posting personal information online | (E2) |
| Posting location online | (E3) |
| Target Accessibility (Time spent engaging in the activity) | |
| Internet browsing hours | (A1) |
| Online shopping hours | (A2) |
| Social media hours | (A3) |
| Watching adult content (e.g., pornography) | (A4) |
| Downloading videos and music (piracy) | (A5) |
| Capable Guardianship | |
| Use of antivirus software | (PhG1) |
| Use of spam filters | (PhG2) |
| Use of pop-up blockers | (PhG3) |
| Setting social networking/media accounts to "private" | (PG4) |
| Skill level and knowledge with computers and technology | (PG5) |
| Knowledge of victimization risk/awareness of cybercrime | (PG3) |

Unauthorized access victimization. We investigated the RAT based predictions in detail because these are fundamental attributes that the existing studies mentioned above also tried to predict. Looking at the accuracy, the classifier predicted victimization with about 71.4% accuracy during the validation phase, however, the accuracy score in the test data (hold-out data) was only 58.8% (see Table 7). This means that the model will classify 58.8% of a dataset, which was not used to train the mode i.e. real-world usage. This suggests that the model is a relatively poor predictor of unauthorized access victimization. Table 8. shows the evaluation metrics scores for individual classes and overall predictions. The Precision and recall scores reflect the effect of unbalanced datasets on these scalar measures and why they may be misleading. The model can predict all of the negative class but only approximately 50% of all the data instance predicted will belong to the negative class. Similarly, the model will accurately classify all instances of the positive class but will only detect 12.5% of the instances with a positive outcome in the given dataset. Therefore, the overall model based on the RAT performs poorly as is shown by the low F1-Score, MCC and AUC. Specifically, the AUC score of 0.5 suggests that the model and hence the RAT as operationalized in this study has no discriminating capacity to distinguish between the classes.

Table 7. *Overview of Random Forest Classification Model for Unauthorized Acces*

| Trees | Predictors per split | n(Train) | n(Validation) | n(Test) | Validation Accuracy | Test Accuracy |
|---|---|---|---|---|---|---|
| 46 | 4 | 54 | 14 | 17 | 0.714 | 0.588 |

Table 8. *Evaluation Metrics Scores for Random Forest Classification Model for Unauthorized Access*

| Class | Precision | Recall | $F_1$-Score | MCC | AUC |
|---|---|---|---|---|---|
| 0 | 0.563 | 1.000 | 0.720 | NA | 0.417 |
| 1 | 1.000 | 0.125 | 0.222 | NA | 0.583 |
| Average / Total | 0.768 | 0.588 | 0.486 | 0.265 | 0.500 |

Note. Area Under Curve (AUC) is calculated for every class against all other classes.

While the effectiveness of the model is not simply a cumulative sum of different parts, it is possible to identify the predictors that are functional and most important. This is done by observing how the overall predictive power of the model drops if a specific variable is removed from the model i.e. mean decrease in accuracy. The "importance" ranking of the variables is given graphically in Figure 2. The shaded bars in Figure 2 represent the predictors, with those right of 0 being more important and causing a decrease in model performance. Therefore, a parsimonious model may contain those predictors given to the left of the 0 mark as removal of the other variables will not negatively affect model performance.

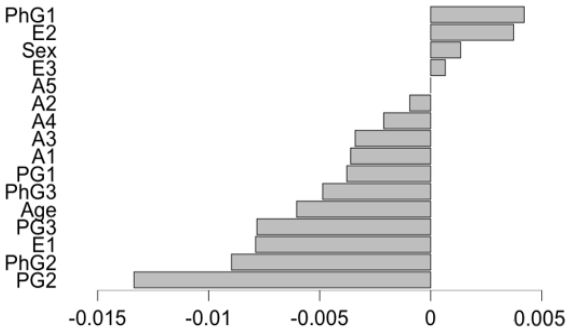


*Figure 2.* Evaluation Metrics Scores for Random Forest Classification Model for Unauthorized Access

To see how strongly and in which direction the predictors are associated with victimization, we further investigated the coefficients and odds ratios given by logistic regression. We used the logistic regression classifier because, unlike tree-based methods it not only shows the strength of the predictors, but also the sign/direction of their effect. Table 9 gives the summary of the hypothesis test for the Logistic Regression, which suggests that at the 95% confidence interval that the RAT is not associated with unauthorized access. This aligns with the output of the random forest analysis.

From Figure 2 we see the most 'important' factors are; using antivirus software, posting location online, posting personal information online and sex. The results of the logistic regression suggest that all the predictors that are 'important' to the model with the exception of using antivirus software increase the possibility of victimization. This means that only using antivirus software was found to be an effective protective

measure among the variables representing the RAT's tenet of Capable Guardianship. Further, the odds ratio suggests that sex had the largest effect (increased risk approx. 8-fold), followed by posting personal information online, then posting location online and finally using antivirus software. Therefore, although using antivirus software is a significant factor its protective effect is small.

Table 9. *Overview of Logistic Regression Analysis for Victimization by Unauthorized Access*

| Model | Deviance | AIC | df | $X^2$ | p | Nagelkerke $R^2$ |
|---|---|---|---|---|---|---|
| $H_0$ | 79.220 | 81.220 | 84 | | | |
| $H_1$ | 46.809 | 94.809 | 61 | 32.411 | 0.092 | 0.523 |

***Cyberbullying victimization.*** The estimated classification accuracy of the best model found during the validation phase was 85.7%. However, the accuracy of the model on the test data was 94.1% (see Table 10). Table 11. shows the evaluation metrics scores for individual classes and overall predictions in relation to cyberbullying. The model shows high recall and precision in relation to both classes. It should be noted that while the model will identify all instances of the positive class, the overall class predictive accuracy will be 66.7% i.e. 66.7% of person predicted to become a cyberbullying victim will have succumb to this form of criminality. Given the high overall accuracy of the model, the mid-range accuracy level suggests that the model is better at predicting true negatives than true positives i.e. it is 'easier to predict who will not be a victim rather than who will be one. This means avoiding set behaviours can decrease risk, however, engaging in risky online behavior does not guarantee a victimization i.e. there is a degree of randomness. However, controlled behaviours can decrease risk. The F1-Score, MCC and AUC scores are all high showing that the model for cyberbullying based on the RAT has strong predictive power. Specifically, the AUC score of 0.815 suggests that the model performs well over a wide range of threshold values. Further, the MCC score of 0.789 shows that the model is good at accurately predicting both classes.

Table 10. *Overview of Random Forest Classification Model for Cyberbullying*

| Trees | Predictors per split | n(Train) | n(Validation) | n(Test) | Validation Accuracy | Test Accuracy |
|---|---|---|---|---|---|---|
| 24 | 4 | 54 | 14 | 17 | 0.857 | 0.914 |

Table 11. *Evaluation Metrics Scores for Random Forest Classification Model for Cyberbullying*

| Class | Precision | Recall | $F_1$-Score | MCC | AUC |
|---|---|---|---|---|---|
| 0 | 0.933 | 1.000 | 0.966 | NA | 0.881 |
| 1 | 1.000 | 0.667 | 0.800 | NA | 0.750 |
| Average / Total | 0.945 | 0.941 | 0.936 | 0.789 | 0.815 |

Note. Area Under Curve (AUC) is calculated for every class against all other classes.

The "importance" ranking of the variables in the random forest model for cyberbullying is illustrated in Figure 3. The graphic indicates that the cyberbullying class variable is best predicted by the following variables: posting personal information online, online shopping hours, social media hours, use of spam filters, use of pop-up blockers, knowledge of victimization risk/awareness of cybercrime, age, and sex. Notably these variables represent all three aspects of the RAT tested in this study i.e. target exposure, target accessibility and capable guardianship.

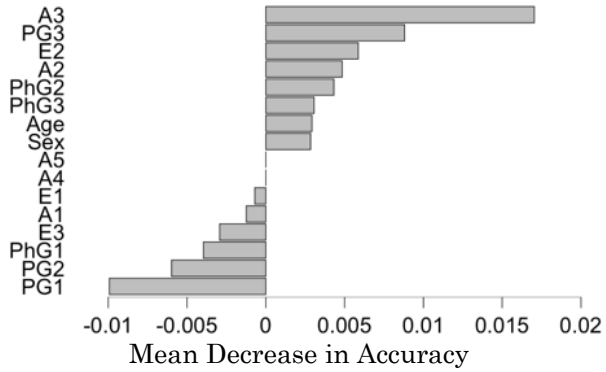


*Figure 3*. The Estimated Effect that Each Variable has on the Predictive Accuracy of the Cyberbullying Model

Table 12 gives the summary of the hypothesis test for the logistic regression for cyberbullying which suggests that at the 95% confidence interval that the tenets of the RAT are associated with cyberbullying. In other words, routine activities are predictive of cyberbullying, and that by extension the RAT is capable of explaining cyberbullying victimization. Further, analysis of the regression coefficients show that posting personal information online, social media hours and of cybercrime victimization risk/awareness increase risk of victimization. The fact that cybercrime victimization risk/awareness increases risk is counter-intuitive and may be related to the fact that the study is cross-sectional i.e. victims seeks knowledge about cybercrime after victimization. As expected from a theoretical understanding of the role of guardianship spam filters and pop-up blockers were found to be protective in relation to cyberbullying. Strangely, online shopping, which was expected to be a risk factor was found to have a protective effect. Examination of the odds ratio suggests that posting personal information online has the greatest effect on cyberbullying risk, increasing its probability approximately 6-fold. Further, being female increased risk by a factor of 4 and being in the age group of 25-34 increased risk by a factor of 5.

Table12. *Overview of Logistic Regression Analysis for Victimization by Cyberbullying*

| Model | Deviance | AIC | df | $X^2$ | p | Nagelkerke $R^2$ |
|---|---|---|---|---|---|---|
| $H_0$ | 79.220 | 81.220 | 84 | | | |
| $H_1$ | 46.809 | 94.809 | 61 | 32.411 | 0.092 | 0.523 |

**Discussion**

The usability of the RAT in predicting unauthorized access proved to be minimal with both classification algorithms showing little discriminatory power. However, cyberbullying was well explained by the RAT as demonstrated by the high values of the performance metric scores. The taxonomies presented by Gordon and Ford (2006) place unauthorized access in the category of techno-centric cybercrimes and cyberbullying in the category of people-centric. The vast difference in the performance of the RAT between the two forms of cybercrime support the proposed taxonomy. Further, it suggests that the RAT may have different explanatory capability depending on the category of cybercrime. However, further study with a larger number of crimes would be needed to confirm this inference and to determine the underlying cause of difference.

Target exposure, measured by the divulgence of information online, was expected to increase with the increasing frequency of posting or sharing personal information, photographs, and locations online, which matches the outcome of previous studies (Reyns, 2015). In the study, the risk of victimization of both form of cybercrime was increased by posting personal information online. However, for cyberbullying this online activity increased the risk by twice as much. Suggesting that obtaining information on the human target is more important in cyberbullying, which is logical given that it is an interpersonal crime. The observed increased risk associated with "posting information online" is in line with previous research (e.g., Goldschmidt, 2018; Reyns, 2015). Posting location online also increased risk of unauthorized access, which suggest that users with high levels of exposure may be more attractive targets for this form of cybercrime.

Target accessibility was measured by the amount of time spent engaged in various online activities, including Internet browsing, online shopping, social media, watching pornography, and downloading videos and music. Interestingly, activities associated with deviant behavior were not found to be significant as in the literature, which is inconsistent with work by previous scholars such as Reyns et al. (2018). Time spent on social media was found to increase risk of cyberbullying. The increased risk associated with social media is consistent with previous victimization studies (e.g., Leukfeldt & Yar, 2016; Reyns, 2015; Reyns et al., 2018). However, other activities that increase time spent online were not found to be risk factors. This suggests that the nature of the activity the user engages in may be more important than simply how many hours spent online. Surprisingly, online shopping appeared to be protective i.e. it decreased risk of victimization in cyberbullying. There is the possibly that this is associated with persons utilizing such services having a greater awareness of technology and cybercrime. Further, they may exercise greater caution online given increasing media on credit card fraud and other risks associated with online shopping.

Capable guardianship was operationalized as physical and personal guardianship. For both cybercrimes physical guardianship was found to be protective while personal guardianship was not. Actually, "knowledge of victimization risk/awareness of cybercrime" slightly increased the risk of cyberbullying. The observed effect of computer literacy has generally been inconsistent in the literature (Grzybowski, 2012; van Wilsem, 2013). However, given that this study is cross-sectional, the reason may be attributable to persons seeking greater knowledge about cybercrime subsequent to victimization. Another consideration is that persons with greater computer literacy and cybercrime awareness are more likely to detect intrusions (Wall, 2007; Yucedal, 2010). The use of antivirus software was found to be a significant protective factor for victimization by unauthorized access, which is consistent with past research (e.g., Bossler & Holt, 2013; Reyns, 2015). Similarly, use of spam filters and pop-up blockers decreased risk of cyberbullying. Other research does not appear to test these specific variables. It is possible that other studies subsume pop-up blockers and spam filters under the use of antivirus (e.g., Reyns, 2015) or choice of browser (e.g., Leukfeldt & Yar, 2016). However, given the different importance of anti-virus, spam filters and pop-up blockers between the two cybercrimes, it appears their application differs and hence should be examined independently. Further, the results suggest that forms of physical guardianship may not be equally effective for all cybercrimes and as such as spectrum of such solutions may be necessary for holistic protection. Overall, physical guardianship was found to be weakly protective and as such is unlikely to be sufficient to prevent cybercrime in isolation.

The study also examined the effect of demographic factors, which was found to be inconsistent between the cybercrimes studied. Age proved to be a significant demographic factor in cyberbullying. This is in alignment with previous research that showed that younger age groups had a higher probability of being harassed (Bossler et al., 2012; Nasi, 2015; Reyns et al., 2018; Wilsem, 2013).

Young people may engage in riskier behaviors and may be more active on social networking sites, which was found to be in itself a risk factor. However, age was insignificant in unauthorized access. This is in agreement with previous research that proposed that this form of cybercrime is a random event that cannot be explained by an opportunity framework (e.g. Bossler & Holt, 2013; Ngo & Paternoster, 2011; Reyns, 2015). Sex was found to be associated with both forms of cybercrimes, with females being at higher risk in both instances. The is possibly attributable to the effect of offline situational factors, such as interactions in school or work and interpersonal relationships (Fisher et al., 2002; Pelfrey & Weber, 2013). However, odds of a female being a victim of unauthorized access was twice as high as them being a victim of cyberbullying. The overall importance of demographic factors may be linked to them having a constraining effect on online and offline activities, similar to their effect on conventional crime (Cohen & Felson, 1979; Stein, 2011). Additional research testing sex and age for moderation effects could aide in confirming their role in victimization.

## Limitations

Every effort was made to ensure the rigor of the methods and analyses employed in this study; however, there are still some limitations that should be examined. These limitations affect the inferences that can be drawn from the results. First, it is somewhat difficult to ascertain if a person has been a victim of a cybercrime. Persons may have been victims of cybercrimes without their knowledge and attributed associated difficulties to faulty hardware or software in their electronic devices or blamed their Internet Service Providers (ISPs). In some instances, depending on the extent of damage, people may not even recall the victimization.

Second, the observations in this study are limited to the way the RAT has been operationalized. This is an intrinsic limitation in all studies because the range of online activities that can have an impact on victimization is extensive (Bossler et al., 2012; Marcum et al., 2010). Further, it may also be fruitful to include off-line activities and protective factors that may also affect cybercrime risks. Arguably, adding additional variables can strengthen the inferences. On the other hand, it can also adversely affect the participation or completion rate of surveys.

## Conclusions

The study made several key observations, which add to the extant literature. First, the study concludes that the explanatory power of the RAT and the predictors of cybercrime are not constant for all forms of cybercrime. The difference is possibly correlated to the dichotomous categorization of cybercrime i.e. people-centric crimes (strong social engineering context) vs. techno-centric (technology focused/crimes made possible through the development of ICTs) (Barn & Barn, 2016). Specifically, the RAT is better suited to explain cyberbullying than unauthorized access. Second, activities that increase target exposure and accessibility increase risk of victimization. While physical guardianship acts as a weak protective factor. Given the small protective effect of physical guardianship measures it is important to not only focus on physical protection. Hence, reduction in cybercrime would require some focus on the online activities that increase risk. In a society where there is increasing social and practical reasons it would be difficult to persuade persons to decrease time spent online. However, this study shows it is the type of online activity that is important.

Therefore, education on online activities and behavior may be more prudent in cybercrime prevention. Fourth, demographics have varying importance in victimization, however, the fact that sex and age are factors suggest some level of linkage between cybercrime and structural factors. Lastly, there is significant alignment between the characteristics of victimization in Trinidad and Tobago and the results obtained from research performed in North America and Europe with the exception of deviant behavior not being a risk factor. However, victimization rates in Trinidad and Tobago are lower suggesting that structural factors may not affect the activities that lead to victimization but rather the tendency to engage in those behaviors.

**Declaration of Interest Statement**

The authors declare that they have no conflicts of interest.

**References**

Barn, R., & Barn, B. (2016). *An ontological representation of a taxonomy for cybercrime.* /z-wcorg/. Retrieved from /z-wcorg/.

Beaujean, A. (2014). *Latent Variable Modeling Using R: A Step-by-Step Guide.* New York: Routledge.

Bossler, A., Holt, T., & May, D. (2012). Predicting Online Harassment Victimization Among a Juvenile Population. *Youth and Society, 44*(4), 500–523.

Bossler, A., & Holt, T. (2009). Examining The Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior, 30*(1), 1–25. http://dx.doi.org.ezproxy.uky.edu/10.1080/01639620701876577

Bossler, A., & Holt, T. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice, 29*(4). http://dx.doi.org/10.1177/1043986213507401

Bryan, C. (2015). Cybercrime—An Emergenct Global Phenomenon with Implications for the Caribbean. *The Jamaica Observer*. Retrieved from http://www.jamaicaobserver.com/columns/Cybercrime---An-emergent-global-phenomenon-with-%20implications-for-the-Caribbean_18719905

Bynoe, J. (2015, August 22). Caribbean is Losing Millions to Cyber Criminals! *St. Kitts and Nevis Observer.* Retrieved from http://stkittsandnevisobserver.com/2015/08/22/caribbean-businesses-governments-and-people-losing-%20millions-to-cyber-criminals/

Caribbean Cyber Security Center. (2019). *Caribbean Cyber Security.*

CARICOM. (2016). *Cybersecurity and the CARICOM Environment.*

Central Statistical Office. (2019). Mid Year Estimates Of Population. Retrieved April 22, 2017, from http://cso.gov.tt/data/?productID=32-Mid-Year-Estimates-of-Population-by-Age-Group

Chicco, D., & Jurman, G. (2020). The Advantages of the Matthews Correlation Coefficient (MCC) Over F1 score and Accuracy in Binary Classification Evaluation. *BMC Genomics, 21*(1), 1–13.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology, 2*(1), 308–333.

Clarke, R. (1999). *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods.* Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

Clarke, R. (2018). *The Theory and Practice of Situational Crime Prevention.* Oxford University Press.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*(4), 588–608.

Cohen, L., & Felson, M. (2003). Routine Activity Theory. In *Criminological Theory: Past to Present*. L.A.: Roxbury.

Delgado, R., & Xavier-Andoni, T. (2019). Why Cohen's Kappa should be avoided as performance measure in classification. *PLoS ONE, 14*(9).

Dhoray, D. (2020). Sexting 101. Retrieved March 10, 2020, from CyberSafeTT website: https://cybersafett.com/sexting101/

Dusek, G., Yurova, Y., & Ruppel, C. (2015). Using Social Media and Targeted Snowball Sampling to Survey a Hard-to-Reach Population: A Case Study. *International Journal of Doctoral Studies, 10*, 279–299. https://doi.org/10.28945/2296

Fisher, B., Cullen, F., & Turner, M. (2002). Being Pursued: Stalking Victimization in A National Study of College Women. *Criminology, & Public Policy, 1*(2), 257–308.

Garson, G. (2015). Missing Values Analysis and Data Imputation. *Statistical Associates Publishers, 1*–26.

Goldschmidt, M. (2018). *Social Engineering is the New Norm in Hacking*.

Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology*. https://doi.org/10.1007/s11416-006-0015-z

Grzybowski, M. (2012). *An Examination of Cybercrime and Cybercrime Research: Self-Control and Routine Activity Theory*. Arizona: Arizona State University

Holt, T., & Bossler, A. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior, 35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Holtfreter, K., Reisig, M., & Blomberg, T. (2006). Consumer Fraud victimization in Florida: An Empirical Study. *St. Thomas Law Review, 18*, 761-879.

Inter-American Development Bank & Organization of American States. (2016). *Cybersecurity: Are we Ready in Latin America and the Caribbean?: 2016 Cybersecurity Report*. Washington, D.C.: Inter-American Development Bank.

Inter-Ministerial Committee for Cyber Security. (2012). *National Cyber Security Strategy*. Port of Spain: Government of the Republic of Trinidad & Tobago.

Jessop, D. (2016). Action Needed to Address Caribbean Cybersecurity. Retrieved April 11, 2017, from Trinidad Express Newspaper website: http://www.caribbean-council.org/action-needed-address-caribbean-cyber-security/

Kosinski, M., Matz, S., Gosling, S., Popov, V., & Stillwell, D. (2016). *Facebook as a Research Tool: A Look at How to Recruit Participants Using Facebook and the Ethical Concerns That Come With Social Media Research.*

Kranenbarg, M., Ruiter, S., & van Gelder, J. (2019). Do Cyber-Birds Flock Together? Comparing Deviance Among Social Network Members of Cyber-Dependent Offenders and Traditional Offenders. *European Journal of Criminology.*

Kshetri, N. (2013). *Cybercrime and Cybersecurity in Latin American and Caribbean Economies BT - Cybercrime and Cybersecurity in the Global South* (N. Kshetri, Ed.). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137021946_7

Leukfeldt, E., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Little, T., Jorgensen, T., Lang, K., & Moore, E. (2014). On the Joys of Missing Data. *Journal of Pediatric Psychology, 39*(2), 151–162. https://doi.org/10.1093/jpepsy/jst048

Marcum, C., Ricketts, M., & Higgins, G. (2010). Assessing Sex Experiences of Online Victimization: An Examination of Adolescent Online Behaviors Using Routine Activity Theory. *Criminal Justice Review, 35*(4), 412–437.

McDaniel, T. (2018). Using Random Forests to Describe Equity in Higher Education: A Critical Quantitative Analysis of Utahs Postsecondary Pipelines. *Butler Journal of Undergraduate Research, 4*(1). /z-wcorg/. Retrieved from /z-wcorg/.

Moore, R., Guntupalli, N., & Lee, T. (2010). Parental Regulation and Online Activities: Examining Factors that Influence a Youth's Potential to Become a Victim of Online Harassment. *International Journal of Cyber Criminology, 4*, 685–698.

Nasi, M., Oksanen, A., Keipi, T., & Rasanen, P. (2015). Cybercrime Victimization Among Young People: A Multi-Nation Study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*. https://doi.org/10.1080/14043858.2015.1046640

Navarro, J., & Jasinski, J. (2012). Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences. *Sociological Spectrum, 32*(1), 81–94.

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology, 5*(1), 773–793.

Parsian, N., & Dunning, T. (2009). D*eveloping and Validating a Questionnaire to Measure Spirituality: A Psychometric Process.* Canadian Center of Science and Education. Retrieved from http://hdl.handle.net/10536/DRO/DU:30019516

Pelfrey, W., & Weber, N. (2013). Keyboard Gangsters: Analysis of Incidence and Correlates of Cyberbullying in a Large Urban Student Population. *Deviant Behavior, 34*(1), 68–84.

Reyns, B. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory Beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216–238.

Reyns, B. (2015). A Routine Activity Perspective on Online Victimisation. *Journal of Financial Crime, 22*(4), 396–411. https://doi.org/10.1108/JFC-06-2014-0030

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2018). *Opportunity and Self-Control: Do they Predict Multiple Forms of Online Victimization?* https://doi.org/10.1007/s12103-018-9447-5

Reyns, B., Henson, B., & Fisher, B. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior, 38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Samuels, D., & Zucco, C. (2013). Using Facebook as a Subject Recruitment Tool for Survey-Experimental Research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2101458

Scandlbauer, A. (2016). *Latin America and the Caribbean: Climbing the Cybersecurity Ladder*. Global Forum on Cyber Expertise. Retrieved from https://www.thegfce.com/news/news/2016/06/20/climbing-the-cybersecurity-ladder

Schmidt, J., Marques, M. R. G., Botti, S., & Marques, M. A. L. (2019). Recent advances and applications of machine learning in solid-state materials science. *Npj Comput Mater Npj Computational Materials, 5*(1), 1–36. Retrieved from /z-wcorg/.

Sijtsma, K. (2009). On the Use, the Misuse and the Very Limited Usefulness of Cronbach's Alpha. *Psychometrika, 74*(1), 107–120.

Song, Q., Guo, Y., & Sheppard, M. (2018). A Comprehensive Investigation of the Role of Imbalanced Learning for Software Defect Prediction. *IEEE Transactions on Software Engineering, 45*(12), 1253–1269.

Stein, R. (2011). *The Contextual Variation of Routine Activities: A Comparative Analysis of Assault Victimization. 1*(10), 11–24.

Symantec. (2014). *Internet Security Threat Report*. California: Symantec Corporation.

Taber, K. (2018). The Use of Cronbachs Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education, 48*(6), 1273–1296.

Taitt, R. (2018, April). CitizensLose $14M to Cybercrime. *Trinidad Express.*

van Griethuijsen, R., van Eijck, M., Haste, H., den Brok, P., Skinner, N., Mansour, N., … BouJaoude, S. (2015). Global Patterns in Students' Views of Science and Interest in Science. *Research in Science Education, 45*(4), 581–603.

van Wilsem, J. (2013). Hacking and Harassment-Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437–453. https://doi.org/10.1177/1043986213507402

Wall, D. (2007). Hunting, Shooting and Phishing: New Cybercrime Challenges for Cybercanadians in the 21st Century. *The Second Eccles Centre for American Studies Plenary Lecture given at the British Association Annual Conference.*

Yucedal, B. (2010). *Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories* (Kent State University). Kent State University, Kent, Ohio. Retrieved from http://rave.ohiolink.edu/etdc/view?acc_num=kent1279290984.

Zhu, L., Qiu, D., Ergu, D., Ying, C., & Liu, K. (2019). A study on predicting local default based on the random forest algorithm. *Procedia Computer Science, 162.*

Zucco, C., Luna, J., & Baykal, G. (2017). *Are Conditional Government Transfers a Politically Acceptable form of Redistribution?*