

Measuring Awareness Of Common People About Cyber Crime Methods

Nazmuddin

Research Scholar

Janardan Rai Nagar Rajasthan Vidyapeeth (Deemed) University

Pratap Nagar, Udaipur, Rajasthan-India

E-mail: kvraghwan@gmail.com

ABSTRACT

You might think that the only form of cybercrime you have to worry about is hackers stealing your financial information. But it may not be so simple. There are far more concerns than just basic financial ones. Cybercrime continues to evolve, with new threats surfacing every year. When you hear and read about the range of cybercrimes out there, you might be tempted to stop using the internet entirely. That's probably too drastic. This research would try to analyze understanding of common people about cyber law and crimes related with cyber. Further to measure the effects concluded society with the future trends of cybercrimes among various categories. The paper revealed that majority of respondents are not aware of large number of cybercrimes.

Keywords: *cybercrime, cyber law, preventive measure, perception*

Introduction

Instead, it's a good idea to know how to recognize cybercrime, which can be the first step to helping protect yourself and your data. Taking some basic precautions and knowing who to contact when you see others engaged in criminal activities online are also important steps. Cybercrime is any crime that takes place online or primarily online. Cybercriminals often commit crimes by targeting computer networks or devices. Cybercrime can range from security breaches to identity theft. Other cybercrimes include things like "revenge porn," cyber-stalking, harassment, bullying, and child sexual exploitation.

Cybercrimes in India almost doubled in 2017, according to statistics released by the National Crime Record Bureau (NCRB) in the month of later October, 2019. Cybercrime accounted for less than a percentage (0.43%) or 21,796 cases of a total of 50 lakh cognizable crimes in India. Karnataka had the highest rate of cybercrime, followed by Assam, Telangana, Maharashtra, and Uttar Pradesh. India recorded over 9,500, 11,500 and 12,000 cases of cybercrime in 2014, 2015 and 2016 respectively. The data for 2017 comes after a two-year delay, with the Centre blaming states in providing statistics for compilation. As per the report, "During 2017, 56% of cyber-crime cases registered were for the motive of fraud (12,213 out of 21,796 cases) followed by sexual exploitation with 6.7% (1,460 cases) and causing disrepute with 4.6% (1,002 cases). Thus it is important that common people must have common understanding and awareness about cybercrimes and its types.

Reviews of literature

Nobles, M.R. (2019) offered “an explanatory opinion on the assets and inadequacies in the sub-field of ecological crime, counting discussion of the emerald criminology movement to maximize the potential for impact”. Mistry & Dahiya (2019) commented that “artifacts identification done using keywords and default hex values. In this research various challenging scenario is discussed and using regular expressions evidence signatures are identified. Besides these scenarios recent Ransom ware attacks can also be solved using volatile memory forensic analysis”.

Marcum& Higgins (2019) “made their declarations about the efficiency of scholastic work and its effect on what we are doing to battle these forms of cyber victimization”.

Norris, Brookes& Dowell (2019) provided “some insight into how criminals target and exploit people in the online environment; based literature to establish the key theories and empirical research that promise to impact on anti-fraud policies and campaigns”. Bossler, Holt, Cross, et al. (2019) examined “constables’ and sergeants’ apparent training to respond to connected fraud finished a quantitative analyses of survey data collected from over 1300 officers from 35 local police activities crossways England and Wales and exposed that first responder training and resource development to respond to cybercrimes are considered”. Okutan, Werner, Yang (2018) “builds on multi-faceted machine learning solutions and develops an integrated system to transform large volumes of public data to aggregate signals with imputation that are relevant and predictive of cyber incidents. A comprehensive analysis of the individual parts and the integrated whole demonstrates the effectiveness and trade-offs of the proposed approach”. Al-khateeb & Agarwal (2019) introduced “the concept of social cyber forensics and its usability. Constantine al. (2019) explored the applicability of Artificial Intelligence (AI) along with computational logic tools – and in particular the Answer Set Programming (A SP) approach to the automation of evidence analysis”. Efthymiopoulos (2019) integrated and proposes “reflects cyber-defence as crucial instrument for present and upcoming working and system centric processes”. Andrews, S., Brewster, B. & Day, T. (2018) “defines an method for sensing the attendance or appearance of organised corruption (OC) signals on communal media. It demonstrations how arguments and expressions, charity by memberships of the community in communal television columns, can be preserved as feeble signs of OC, allowing material to be secret rendering to a catalogue”. Hazra& Cui(2018) considered “Johansen co integration test confirms the presence of co integration relationship between the variables”. Paoli et.al.,(2018) “understand the impact as the overall damage of cybercrime, that is, the “sum” of the evils to physical sustenance, or prices, and the evils to other attention sizes i.e., useful (or active) honesty, reputation and privacy”. Stubbs-Richardson et.al., (2018) investigated “the association between Internet searches and property crime levels in the United States. States with the highest levels of property crime tended to have the highest levels of Google crime prevention queries for target hardening, surveillance, and formal and informal social control”.

METHODOLOGY

Approach: The present research use deductive research approach. In the deductive research approach the researchers generate hypothesis from theory.

Primary Data: questionnaire has been prepared, this was filled by the respondents who are using the online transaction in selected geographical area of study i.e. Rajasthan.

Secondary Data: from the files, newspapers, reports, records, policies, government publications, magazines, company publications, journals, books, articles, websites, etc.

Sampling Technique: convenience sampling (using a cross-sectional design)

Sample Size: 200 online users

DATA ANALYSIS

Table 1: Sample Demographics, N=200

Age	15-24	20%	Gender	Male	64%
	25-34	35%		Female	36%
	35-above	45%	Education	Graduate or lower	56%
Monthly income	0-20,000 INR	19%		Post Graduate	44%
	20,000-40,000 INR	32%	Occupation	Student	13%
	Above 40,000 INR	49%		Employed	45%
				Business	42%

Table-2: measuring categories

One-Sample 't' test result

Variable	One-Sample Statistics				
	SPSS codes	N	μ	σ	σ/μ
Cyber-Stalking	Cat_CC_1	200	1.7450	.43695	.03090
Hardware Attacks	Cat_CC_2	200	1.5050	.50123	.03544
Trojan attacks	Cat_CC_3	200	1.6350	.48264	.03413
Data diddling	Cat_CC_4	200	1.7500	.43410	.03070
Cyber Grooming	Cat_CC_5	200	1.5150	.50103	.03543
Online Gaming	Cat_CC_6	200	1.8350	.37211	.02631
Salami slicing attack	Cat_CC_7	200	1.9950	.07071	.00500
Piracy/cloning	Cat_CC_8	200	1.7050	.45719	.03233
Cyber Defamation	Cat_CC_9	200	1.4700	.50035	.03538
Hacking	Cat_CC_10	200	1.5900	.49307	.03487
Theft of FTP Passwords	Cat_CC_11	200	1.4500	.49874	.03527
Cross-site scripting	Cat_CC_12	200	1.5850	.49396	.03493
Virus dissemination	Cat_CC_13	200	1.8250	.38092	.02694
Denial-of-Service attack	Cat_CC_14	200	1.7650	.42506	.03006
Cracking	Cat_CC_15	200	1.6300	.48402	.03423
E-Mail Spoofing	Cat_CC_16	200	1.8300	.37658	.02663
Carding / Card cloning	Cat_CC_17	200	1.7550	.43117	.03049
Identity Theft	Cat_CC_18	200	1.6800	.46765	.03307
Cyber Bullying	Cat_CC_19	200	1.8050	.39719	.02809
Cyber Squatting	Cat_CC_20	200	1.6000	.49113	.03473

Spamming/ Email bombing	Cat_CC_21	200	1.8400	.36753	.02599
Web jacking	Cat_CC_22	200	1.6550	.47656	.03370
Cyber terrorism	Cat_CC_23	200	1.5850	.49396	.03493
Cyber Vandalism	Cat_CC_24	200	1.8300	.37658	.02663
Online Gambling	Cat_CC_25	200	1.8300	.37658	.02663
Cyber extortion	Cat_CC_26	200	1.4150	.49396	.03493
Phishing	Cat_CC_27	200	1.6650	.47317	.03346

One-Sample Test						
	Test Value = 1.5					
	t	d.f.	Sig. (2-tailed)	μ Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Cat_CC_1	7.929	199	.000	.24500	.1841	.3059
Cat_CC_2	.141	199	.888	.00500	-.0649	.0749
Cat_CC_3	3.956	199	.000	.13500	.0677	.2023
Cat_CC_4	8.145	199	.000	.25000	.1895	.3105
Cat_CC_5	.423	199	.672	.01500	-.0549	.0849
Cat_CC_6	12.732	199	.000	.33500	.2831	.3869
Cat_CC_7	99.000	199	.000	.49500	.4851	.5049
Cat_CC_8	6.341	199	.000	.20500	.1413	.2687
Cat_CC_9	-.848	199	.397	-.03000	-.0998	.0398
Cat_CC_10	2.581	199	.011	.09000	.0212	.1588
Cat_CC_11	-1.418	199	.158	-.05000	-.1195	.0195
Cat_CC_12	2.434	199	.016	.08500	.0161	.1539
Cat_CC_13	12.066	199	.000	.32500	.2719	.3781
Cat_CC_14	8.817	199	.000	.26500	.2057	.3243
Cat_CC_15	3.798	199	.000	.13000	.0625	.1975
Cat_CC_16	12.393	199	.000	.33000	.2775	.3825
Cat_CC_17	8.364	199	.000	.25500	.1949	.3151
Cat_CC_18	5.443	199	.000	.18000	.1148	.2452
Cat_CC_19	10.860	199	.000	.30500	.2496	.3604
Cat_CC_20	2.880	199	.004	.10000	.0315	.1685
Cat_CC_21	13.083	199	.000	.34000	.2888	.3912
Cat_CC_22	4.600	199	.000	.15500	.0885	.2215
Cat_CC_23	2.434	199	.016	.08500	.0161	.1539
Cat_CC_24	12.393	199	.000	.33000	.2775	.3825
Cat_CC_25	12.393	199	.000	.33000	.2775	.3825
Cat_CC_26	-2.434	199	.016	-.08500	-.1539	-.0161
Cat_CC_27	4.931	199	.000	.16500	.0990	.2310

Table presented with the observed *t*-value, the degrees of freedom ("d.f."), and the statistical significance of the one-sample t-test. The *p* value for all dimension are $< .05$, therefore, it can be concluded that the population μ s and sample μ s are significantly different. Result from 't' test and μ value analysis, it can be concluded that majority of respondents are not aware of large

number of cybercrimes like Cyber-Stalking, Hardware Attacks, Trojan attacks, Data diddling, Cyber Grooming, Online Gaming Salami slicing attack, Piracy/cloning, Cyber Defamation , Hacking , Theft of FTP Passwords, Cross-site scripting, Virus dissemination, Denial-of-Service attack, Cracking , E-Mail Spoofing , Carding / Card cloning, Identity Theft, Cyber Bullying , Cyber Squatting , Spamming/ Email bombing, Web jacking, Cyber terrorism, Cyber Vandalism , Online Gambling, Cyber extortion , Phishing.