Sachetas
सा विद्या या विमुक्तये
Sachetas
An International, Peer Reviewed, Open Access & Multidisciplinary Journal
E-ISSN: 2583-312X

CYBERCRIME AWARENESS AND ITS IMPLICATIONS FOR DIGITAL TRANSACTIONS: A STUDY AMONG SCHOOL EDUCATORS IN AHMEDABAD CITY

Dr. Bhavesh H. Bharad

Assistant Professor
University School of Law, Gujarat University Ahmedabad-380009
Email: dr.bharad@gmail.com
ORCID ID: https://orcid.org/0000-0002-8042-8626

Dr. Komal B. Sharma

Assistant Professor
Centre of Excellence, University School of Law, Gujarat University, Ahmedabad-380009
Email: sharma.komal0096@gmail.com
ORCID ID: https://orcid.org/0000-0001-9121-5362

Abstract

In 2025, India's digital transformation has significantly heightened its vulnerability to cyber threats, affecting individuals, organizations, and governmental institutions alike. This study focuses on assessing the awareness of cybercrime among school educators in Ahmedabad City, an essential demographic for enhancing cybersecurity education. Through a quantitative research design and structured questionnaire, data was collected from 120 educators using stratified random sampling. Key findings reveal a high level of awareness among educators regarding cybercrimes like phishing, financial crime and malware, yet significant gaps exist in preparedness and response strategies. Financial cybercrime emerges prominently among the surveyed respondents. Gender was found to influence satisfaction with available cybersecurity solutions, while the type of cybercrime experienced varied across demographic groups. Educators predominantly seek self-education and IT support post-incident, underscoring the need for improved resources and training. The study underscores the importance of tailored cybersecurity strategies and comprehensive educational initiatives to mitigate cyber risks effectively.

Keywords: *Cybercrime awareness, School educators, Ahmedabad City, Cybersecurity education, Educational initiatives, Cybersecurity training*

Editorial Record

First submission received:
August 19, 2025

Accepted for publication:
September 01, 2025

Cite this article

Bharad, B., & Sharma, K. (2025). Cybercrime Awareness And Its Implications For Digital Transactions: A Study Among School Educators In Ahmedabad City. Sachetas, 4(3), 58-68. https://doi.org/10.55955/430006

INTRODUCTION

In 2025, cybercrime has grown to be a major worry for people, companies, and government organisations all over India as the country continues its fast digital transformation. In India's rapidly digitalizing world, cybercrime has emerged as a substantial danger to individuals, organisations, and government institutions nationwide.

The present study endeavours to evaluate the existing state of cybercrime awareness across several Indian demographic groups and pinpoint crucial aspects that require enhancement in cybersecurity practices and education.

The maturity of Digital India programmes and the growing usage of digital technology have increased India's susceptibility to cyber threats. Comprehending the level of knowledge among the Indian populace regarding these hazards is vital in devising efficacious tactics to counter cybercrime and safeguard confidential data in the most populous nation globally.

Sachetas
An International, Peer Reviewed, Open Access & Multidisciplinary Journal
E-ISSN: 2583-312X

BACKGROUND OF THE STUDY

India's cybercrime trend has consistently demonstrated an increase. The number of cybercrime cases in India has risen dramatically over the last three years, from 50,035 in 2020 to an expected 85,000 in 2023, according to the most recent data from the National Crime Records Bureau (NCRB) (https://ncrb.gov.in/).

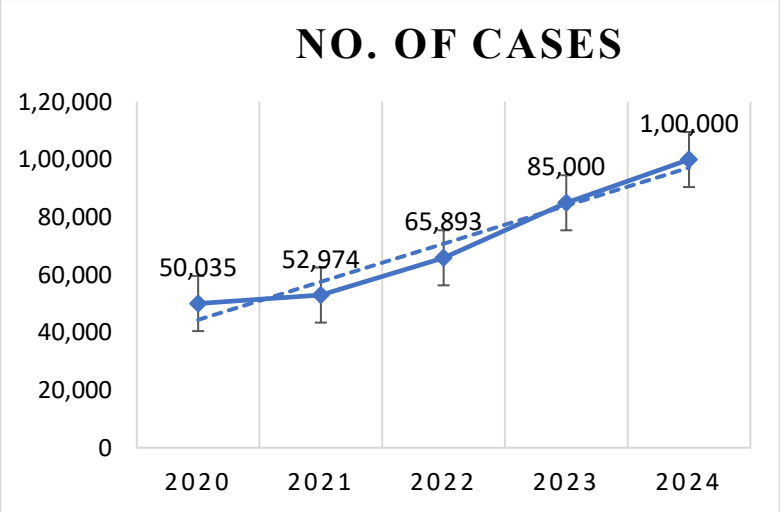
Important data that demonstrate the significance of this research in the Indian context by 2024 are as follows:

- ✓ With an estimated 60 million Indians impacted by cybercrime in 2023, India currently holds the second-place position in the world.
- ✓ In 2023, approximately 2 million cybersecurity events were reported by the Indian Computer Emergency Response Team (CERT-In), a 42% increase over 2021.
- ✓ With ransomware attacks making up 35% of all recorded cases in 2023, they are now the type of cybercrime in India that is expanding the quickest.
- ✓ In India, the average cost of a data breach increased by 42% from 2022 to ₹25 crore in 2023.
- ✓ As of early 2024, just 52% of Indian organisations had adopted a thorough cybersecurity strategy, despite advancements.

Cybercrime Landscape in India (2020-2024)

The trajectory of cybercrime in India has shown a consistent upward trend:

YEAR	NO. OF CASES
2020	50,035
2021	52,974
2022	65,893
2023	85,000
2024	Projected to exceed 100,000 cases



Types of Cybercrimes:

1. **Phishing**: Deceptive practice where criminals impersonate legitimate entities to trick individuals into revealing sensitive information. In India, phishing often targets bank customers and e-commerce users via fake SMS or emails. It accounts for 28% of cyber-attacks as of 2023.
2. **Identity Theft:** Criminals steal personal information to impersonate victims for financial gain or other malicious purposes. In India, this often involves misuse of Aadhaar numbers or PAN cards. Over 50,000 cases were reported in 2023, a 30% increase from 2022.
3. **Unauthorized Transactions:** Financial transactions made without the account holder's consent, often through compromised mobile banking apps or stolen card details. In 2023, unauthorized electronic transactions in India amounted to ₹1,500 crore.
4. **Malware Attacks:** Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. In India, malware often targets Android devices. CERT-In reported over 10 million affected devices in 2023.
5. **Financial Crimes:** Various cybercrimes with financial motives, including investment frauds and cryptocurrency scams. Often promoted through social media in India. Cost Indian victims over ₹15,000 crore in 2023.
6. **Unauthorized Access to Personal Information:** Illegal access to individuals' private data, often through hacking or exploiting system vulnerabilities. Several high-profile data breaches in India have affected millions of users. The Personal Data Protection Bill, passed in 2023, aims to address such issues.

An extensive examination of cybercrime awareness across different factors in Ahmedabad City will be provided by this study. Our goal is to provide policymakers, educators, and cybersecurity experts with essential information to improve public awareness and resilience against cyber threats in the Indian context by detecting knowledge gaps and understanding levels.

RESEARCH QUESTION

To achieve the objectives of present study, the following research questions are as mentioned below:

1. What is the current level of awareness regarding different types of cybercrime among school educators in Ahmedabad City?
2. How prepared are educators to recognize and respond to various cyber threats, including phishing, malware attacks, identity theft, and financial Crime?
3. What are actions taken by educators after experiencing cybercrime and the support received from IT departments and external experts.?
4. What are the preferred resources and methods for improving cybercrime awareness and preparedness among educators?

OBJECTIVES OF THE STUDY

1. To assess general awareness of cybercrime among school educators in Ahmedabad city.
2. To determine the prevalence and types of cybercrime incidents experienced by educators and necessary actions post-incident
3. To investigate the actions taken by educators after experiencing cybercrime and the support received from IT departments and external experts.
4. To identify preferred resources and methods for improving cybercrime awareness and preparedness among educators.

RESEARCH METHODOLOGY

⇒ RESEARCH DESIGN

This study employs a **Quantitative Research Design** to assess cybercrime awareness among school educators in Ahmedabad City, providing a clear and systematic approach to understanding the current state of cybercrime awareness and actions among educators.

⇒ SAMPLING METHOD

The target population for this study comprises school educators in Ahmedabad City. There are approximately 50 Schools, and around 650 school educators working in Ahmedabad City. A total of 120 school educators were selected using a **Stratified Random Sampling Technique** to ensure representation from various sectors and educational professionals within the city. This method allows for a more accurate reflection of the diverse experiences and awareness levels of educators across Ahmedabad City.

Sample Size Determination

An ideal sample size can be found using the Cochran formula, which takes into account the expected proportion of the attribute in the population, the precision and confidence level that are supplied.

The Cochran formula:

$$no = \frac{Z2pq}{e\ 2}$$

Where,

- n is sample size
- e is the desired level of precision (i.e. the margin of error),
- z is Z- score corresponding to the desired confidence level
- p is the (estimated) proportion of the population which has the attribute in question,
- q is 1 – p

95% level of confidence is used, so z = 1.96. Next, the p = q = 50% situation is customarily assumed as it is the worst possible case of variability. Let's take a ± 8% sample error.

$$no = \frac{Z2pq}{e\ 2}$$

$$= \frac{(1.96)2 * 0.5\ (0.5)}{0.008}$$

$$= 120$$

Total sample size determination: 120

⇒ DATA COLLECTION INSTRUMENT

Data was collected using a **Structured Questionnaire** designed to gather detailed information on educators' awareness, experiences, and responses to cybercrime incidents. The questionnaire was developed based on a thorough review of existing literature and consultations with cybersecurity experts to ensure its relevance and comprehensiveness. It comprised the following sections:

- ✓ **Demographic Information:** Collected basic demographic data, including name, email ID, contact number, and gender.
- ✓ **General Awareness:** Assessed educators' general awareness and understanding of cybercrime.
- ✓ **Experience with Cybercrime:** Explored the prevalence and types of cybercrime incidents experienced by the educators.
- ✓ **Post-Incident Actions:** Focused on the actions taken by educators following a cybercrime incident and the support they received from IT departments and external experts.
- ✓ **Solution & Preferred Resources:** Identified educators' solutions and preferred resources and methods for improving their cybercrime awareness and preparedness.

⇒ RESEARCH TOOLS AND TECHNIQUES FOR DATA ANALYSIS

The responses collected from the questionnaires underwent a detailed examination, and a coding system was established for each question to quantify the qualitative elements. This data was then entered into a master table, which served as the foundation for various tables incorporated in the study as needed. The study utilized the following tools to collect and analyze the data:

- Microsoft Office Excel 2021
- IBM SPSS Statistics 20
- Google Form

The techniques used for analyzing the collected data are as follows:

- Frequency Distribution
- Chi- Square Test
- Factor Analysis
- One- way ANOVA

⇒ ETHICAL CONSIDERATIONS

Throughout the study, ethical considerations were rigorously upheld. Participants were fully informed about the research's purpose, and their informed consent was obtained prior to data collection. To ensure confidentiality and anonymity, responses were anonymized, and data was securely stored with access restricted to the research team. Participants were assured that their information would be used exclusively for research purposes.

⇒ LIMITATIONS OF THE STUDY

While this study offers important insights into cybercrime awareness among school educators in Ahmedabad City, it is important to recognize certain limitations. The purposive sampling technique, while ensuring a diverse representation of educational settings, may lead to selection bias. Moreover, the self-reported nature of the questionnaire responses might be influenced by social desirability bias. Future research could improve robustness by using a larger, randomized sample and incorporating additional data collection methods, such as interviews or focus groups.

DATA ANALYSIS AND DISCUSSION

❖ DEMOGRAPHIC & GENERAL AWARENESS ANALYSIS

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	101	84.2	84.2	84.2
	Female	19	15.8	15.8	100.0
	Total	120	100.0	100.0	

Do you Know What is Cybercrime?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	99	82.5	82.5	82.5
	No	21	17.5	17.5	100.0
	Total	120	100.0	100.0	

Have You/ Family been victim of Cybercrime?

	Frequency	Percent	Valid Percent	Cumulative Percent

	Yes	64	53.3	53.3	53.3
Valid	No	56	46.7	46.7	100.0
	Total	120	100.0	100.0	

Interpretation: The sample consists predominantly of male respondents (84.2%), with females making up 15.8% of the participants. This indicates a gender disparity in the sample, which may need to be considered when interpreting results and drawing conclusions.
A significant majority of the respondents (82.5%) are aware of what cybercrime is, while 17.5% are not. This high level of awareness is promising but indicates that there is still a need for further education among a portion of the respondents.
More than half of the respondents (53.3%) reported that they or their family members have been victims of cybercrime, while 46.7% have not had such experiences. This indicates a substantial impact of cybercrime among the respondents, highlighting the importance of awareness and preventive measures.

❖ **CHI- SQUARE TEST**

Statements	Chi-Square Value (x^2)	P-value (α)	Decision for Null Hypothesis
Gender vs. How satisfied are you with the available solutions for addressing cybercrimes? **H0: There is no significant relationship between satisfaction levels with available solutions for addressing cybercrimes and the demographic variables.** **H1: There is a significant relationship between satisfaction levels with available solutions for addressing cybercrimes and the demographic variables.**	62.125	.000	**Rejected** - Gender affects satisfaction with cybercrime solutions
Gender vs. Have You/ Family been a victim of Cybercrime? **H0: There is no significant relationship between being a victim of cybercrime and the demographic variables.** **H1: There is a significant relationship between being a victim of cybercrime and the demographic variables.**	0.533	.465	**Accepted** - Gender does not affect victimization by cybercrime
Gender vs. What type of Cybercrime did you Experience? **H0: There is no significant relationship between the type of cybercrime experienced and the demographic variables.** **H1: There is a significant relationship between the type of cybercrime experienced and the demographic variables.**	29.594	.000	**Rejected** - Gender affects the type of cybercrime experienced
Gender vs. Do you know what cybercrime is? **H0: There is no significant relationship between knowing what cybercrime is and the demographic variables.** **H1: There is a significant relationship between knowing what cybercrime is and the demographic variables.**	50.700	.000	**Rejected** - Gender affects knowledge of cybercrime
Gender **H0: There is no significant relationship between gender and other variables.** **H1: There is a significant relationship between gender and other variables.**	56.033	.000	**Rejected** - Gender is significantly related to the other variables

Interpretation: The Chi-Square test results indicate that gender significantly influences satisfaction with cybercrime solutions, the type of cybercrime experienced, and knowledge of cybercrime, with p-values of .000 for these variables. However, gender does not significantly affect whether individuals or their families have been victims of cybercrime (p-value of .465). These findings highlight that demographic factors like gender play a crucial role in shaping educators' interactions with and perceptions of cybercrime.

❖ **FACTOR ANALYSIS**

Major Actions did participants take after experiencing a cybercrime incident
Hypothesis of the study are as under:

Ho: There is no significant relationship between the actions taken after experiencing a cybercrime incident and the demographic variables of the participants.

H1: There is significant relationship between the actions taken after experiencing a cybercrime incident and the demographic variables of the participants.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.019	25.234	25.234	2.019	25.234	25.234
2	1.331	16.643	41.877	1.331	16.643	41.877
3	1.040	13.005	54.882	1.040	13.005	54.882
4	.950	11.872	66.754			
5	.791	9.888	76.641			
6	.717	8.967	85.608			
7	.611	7.633	93.241			
8	.541	6.759	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component		
	1	2	3
Changed passwords	.420	.643	-.171
Contacted IT support	.483	.275	.314
Ran antivirus/malware software	.231	.747	-.129
Ignored the incident	.471	-.346	-.609
Notified law enforcement	.379	-.153	.700
Informed colleagues or peers	.714	-.154	-.127
Sought help from a cybersecurity expert	.633	-.338	-.014
Educated myself on cybersecurity practices	.529	-.058	.135

Extraction Method: Principal Component Analysis.
a. 3 components extracted.

Interpretation: The Factor Analysis revealed three main components that encapsulate the actions taken by participants:

- **Component 1** proactive security measures (e.g., changing passwords, running antivirus software)
- **Component 2** seeking external support and reporting (e.g., contacting IT support, notifying law enforcement),
- **Component 3** self-education and awareness enhancement (e.g., educating oneself on cybersecurity practices).

These components suggest that participants exhibit varied responses to cybercrime incidents, indicating a multifaceted approach to addressing cybersecurity challenges. The findings support the hypothesis that actions taken after a cybercrime incident are not significantly influenced by demographic variables, highlighting a universal need for cybersecurity awareness and preparedness across different groups.

❖ FACTOR ANALYSIS

Solutions did participants receive after facing a cybercrime incident.

Hypothesis of the study are as under:

H0: There is no significant difference in the solutions received after facing a cybercrime incident among the educators.

H1: There is a significant difference in the solutions received after facing a cybercrime incident among the educators.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.772	22.153	22.153	1.772	22.153	22.153
2	1.447	18.084	40.237	1.447	18.084	40.237
3	1.207	15.081	55.319	1.207	15.081	55.319

4	1.148	14.349	69.668	1.148	14.349	69.668
5	.828	10.350	80.018			
6	.681	8.509	88.527			
7	.528	6.598	95.125			
8	.390	4.875	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component			
	1	2	3	4
IT Department Assistance	.150	-.035	.793	-.002
External Cybersecurity Expert Help	.342	.398	.260	-.586
Updated Security Software/Tools	.225	.528	-.179	.700
Updated Security Software/Tools	.452	.552	-.371	-.301
Guidance on preventive measures	.489	-.342	-.484	-.275
No support provided	.682	-.476	.173	.012
Support in monitoring my accounts for suspicious activities	.598	-.417	-.056	.335
Financial compensation or credit monitoring services	.562	.430	.271	.189

Extraction Method: Principal Component Analysis.
a. 4 components extracted.

Interpretation: The factor analysis results reveal four distinct components that account for 69.668% of the total variance in the solutions received after facing a cybercrime incident. This indicates that the educators' experiences with solutions after a cybercrime incident can be grouped into four main factors.

- **Component 1** suggests a group of solutions focused on the lack of support and monitoring services.
- **Component 2** represents solutions involving software updates and financial compensation.
- **Component 3** highlights the assistance from IT departments.
- **Component 4** emphasizes the role of updated security tools and monitoring activities.

The significant loadings on these components indicate diverse responses and experiences among educators, suggesting variability in the support and solutions received. Given the extraction of four distinct components, the null hypothesis (H0) can be rejected, and it can be concluded that there are significant differences in the solutions received after facing a cybercrime incident among the educators.

❖ FACTOR ANALYSIS

Hypothesis of the study are as under:

H0: There is no significant difference in the various resources for improving cybercrime awareness among participants.

H1: There is a significant difference in the various resources for improving cybercrime awareness among participants.

Resources would participants find most helpful in improving cybercrime awareness.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.696	33.913	33.913	1.696	33.913	33.913
2	1.149	22.971	56.884	1.149	22.971	56.884
3	.884	17.689	74.572			
4	.837	16.745	91.318			
5	.434	8.682	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component	
	1	2
Regular training sessions	.358	.502

Online courses	.193	-.735
Informational newsletters	.391	.552
Dedicated cybersecurity staff at nearest place	.817	-.096
Easily accessible online resources	.843	-.207

Extraction Method: Principal Component Analysis.
a. 2 components extracted.

Interpretation: The factor analysis results reveal two distinct components that account for 56.884% of the total variance in the resources participants find most helpful for improving cybercrime awareness. This indicates that participants' preferences for resources can be grouped into two main factors.

- **Component 1** suggests a preference for having dedicated cybersecurity staff and easily accessible online resources.
- **Component 2** represents a preference for online courses and informational newsletters.

The significant loadings on these components indicate that participants have diverse preferences for resources that would help them improve their cybercrime awareness. Given the extraction of two distinct components, the null hypothesis (H0) can be rejected, and it can be concluded that there are significant differences in the helpfulness of various resources for improving cybercrime awareness among participants.

❖ **ONE- WAY ANOVA**

Solutions received after facing a cybercrime incident

Hypothesis of the study are as under:

H0: There is no significant difference in the solutions received after facing a cybercrime incident among different groups of participants.

H1: There is a significant difference in the solutions received after facing a cybercrime incident among different groups of participants.

ANOVA

		Sum of Squares	Df	Mean Square	F	Sig.
Regular training sessions	Between Groups	.070	3	.023	.379	.768
	Within Groups	3.680	60	.061		
	Total	3.750	63			
Online courses	Between Groups	.514	3	.171	1.422	.245
	Within Groups	7.221	60	.120		
	Total	7.734	63			
Informational newsletters	Between Groups	.279	3	.093	.831	.482
	Within Groups	6.721	60	.112		
	Total	7.000	63			
Dedicated cybersecurity staff at nearest place	Between Groups	.110	3	.037	.319	.812
	Within Groups	6.890	60	.115		
	Total	7.000	63			
Easily accessible online resources	Between Groups	.204	3	.068	.309	.818
	Within Groups	13.156	60	.219		
	Total	13.359	63			
IT Department Assistance	Between Groups	.403	3	.134	2.409	.076
	Within Groups	3.347	60	.056		
	Total	3.750	63			
External Cybersecurity Expert Help	Between Groups	.498	3	.166	.955	.420
	Within Groups	10.439	60	.174		
	Total	10.938	63			
Updated Security Software/Tools	Between Groups	.379	3	.126	1.499	.224
	Within Groups	5.058	60	.084		
	Total	5.437	63			
	Between Groups	.379	3	.126	1.499	.224

Updated Security Software/Tools	Within Groups	5.058	60	.084		
	Total	5.437	63			
Guidance on preventive measures	Between Groups	.709	3	.236	1.032	.385
	Within Groups	13.729	60	.229		
	Total	14.438	63			
No support provided	Between Groups	1.616	3	.539	2.587	.061
	Within Groups	12.493	60	.208		
	Total	14.109	63			
Support in monitoring my accounts for suspicious activities	Between Groups	.678	3	.226	.886	.454
	Within Groups	15.306	60	.255		
	Total	15.984	63			
Financial compensation or credit monitoring services	Between Groups	3.439	3	1.146	5.949	.001
	Within Groups	11.561	60	.193		
	Total	15.000	63			

Interpretation: The results of the ANOVA indicate varied impacts of different interventions on respondents' perceptions of cybersecurity effectiveness. Notably, financial compensation or credit monitoring services show a significant effect ($F(3, 60) = 5.949$, $p = .001$), suggesting these measures are perceived as more effective compared to other interventions. Conversely, the IT Department Assistance intervention shows a trend towards significance ($F(3, 60) = 2.409$, $p = .076$), implying potential effectiveness. In contrast, interventions such as regular training sessions, online courses, informational newsletters, dedicated cybersecurity staff, easily accessible online resources, external cybersecurity expert help, updated security software/tools, guidance on preventive measures, support in monitoring accounts, and no support provided did not yield statistically significant effects ($p > .05$). These findings highlight the nuanced effectiveness of different cybersecurity strategies, with financial compensatory measures standing out as particularly impactful in enhancing perceived cybersecurity protection among respondents.

❖ **One- Way ANOVA**

Resources most helpful in improving cybercrime awareness

Hypothesis of the study are as under:

H0: There is no significant difference in the perceived different helpful resources for improving cybercrime awareness among educators in Ahmedabad City.

H1: There is a significant difference in the perceived different helpful resources for improving cybercrime awareness among educators in Ahmedabad City.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Regular training sessions	Between Groups	.070	3	.023	.379	.768
	Within Groups	3.680	60	.061		
	Total	3.750	63			
Online courses	Between Groups	.514	3	.171	1.422	.245
	Within Groups	7.221	60	.120		
	Total	7.734	63			
Informational newsletters	Between Groups	.279	3	.093	.831	.482
	Within Groups	6.721	60	.112		
	Total	7.000	63			
Dedicated cybersecurity staff at nearest place	Between Groups	.110	3	.037	.319	.812
	Within Groups	6.890	60	.115		
	Total	7.000	63			
Easily accessible online resources	Between Groups	.204	3	.068	.309	.818
	Within Groups	13.156	60	.219		
	Total	13.359	63			

Interpretation: The One-Way ANOVA results indicate that there were no statistically significant differences in perceived helpfulness among various resources for improving cybercrime awareness. Across categories such as regular training sessions, online courses, informational newsletters, dedicated cybersecurity staff availability, and easily accessible online resources, the F-values were all below critical

thresholds, and p-values were above the significance level of 0.05. This suggests that participants' perceptions of these resources did not vary significantly. Therefore, the null hypothesis, which posited no significant differences in perceived helpfulness among these resources, is accepted. These findings imply that while various resources are available, their perceived effectiveness in enhancing cybercrime awareness may not differ significantly among the surveyed educators in Ahmedabad City.

CONCLUSION

The findings of this study provide a comprehensive insight into the current state of cybercrime awareness among school educators in Ahmedabad City, India. Through a structured questionnaire administered to 120 educators, the study explored their awareness levels, experiences with cybercrimes, actions taken post-incidents, and preferences for enhancing cybercrime awareness.

Key Findings:

1. **Awareness Levels**: A majority of educators demonstrated a high awareness of cybercrimes, with 82.5% indicating familiarity with different types of cyber threats. This is encouraging, suggesting that foundational knowledge among educators is robust but still requires continuous reinforcement.
2. **Incident Prevalence**: More than half of the respondents (53.3%) reported personal or family experiences with cybercrimes. This underscores the pervasive nature of cyber threats in Ahmedabad City.
3. **Actions Post-Incident**: Educators exhibited a varied response to cybercrimes, ranging from proactive measures such as changing passwords and running antivirus software to seeking assistance from IT departments and cybersecurity experts.
4. **Support Mechanisms**: The study identified significant disparities in the support received post-cybercrime incident, with financial compensation or credit monitoring services proving particularly impactful in mitigating the aftermath of cybercrimes.
5. **Preventive Measures**: Preferred resources for enhancing cybercrime awareness included regular training sessions, accessible online resources, and expert guidance, highlighting the need for ongoing educational initiatives tailored to educators' needs.

Implications and Recommendations:

- **Educational Interventions**: Continuous training sessions and workshops tailored to different aspects of cybercrime can enhance educators' preparedness and response capabilities.
- **Policy Advocacy**: Advocating for robust cybersecurity policies at institutional levels can ensure systematic support and response frameworks for cyber incidents in educational institutions.
- **Collaborative Efforts**: Strengthening collaborations between educational institutions, cybersecurity agencies, and policy-makers is essential to foster a secure digital environment for educators and students alike.

REFERENCES

Abubakari, Y., & Amponsah, A. A. (2024). Economic cybercrime in the diaspora: case of Ghanaian nationals in the USA. Journal of Money Laundering Control.

Adewopo, V., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. (2024). A comprehensive analytical review on cybercrime in West Africa. arXiv preprint arXiv:2402.01649.

Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205-217.

Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., & Mazurenko, O. (2024). Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. Multidisciplinary Science Journal, 6.

Bekkers, L. M., Moneva, A., & Leukfeldt, E. R. (2024). Understanding cybercrime involvement: A quasi-experiment on engagement with money mule recruitment ads on Instagram. Journal of Experimental Criminology, 20(2), 375-394.

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. Plos one, 19(4), e0297312.

Buil-Gil, D., Trajtenberg, N., & Aebi, M. F. (2024). Measuring cybercrime and cyber evidence in Surveys.

Europol. (2023). **Cybercrime.** Retrieved from https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

Federal Bureau of Investigation. (2023). **Internet crime complaint center (IC3).** Retrieved from https://www.ic3.gov

Gajjar, V. R., & Taherdoost, H. (2024, January). Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies. In 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI) (pp. 668-676). IEEE.

Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. Progress in Human Geography, 03091325241246015.

Hughes, J., Pastrana, S., Hutchings, A., Afroz, S., Samtani, S., Li, W., & Santana Marin, E. (2024). The art of cybercrime community research. ACM Computing Surveys, 56(6), 1-26.

Kaspersky. (2021). **What is cybercrime?** Retrieved from https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Kaur, G., Bonde, U., Pise, K. L., Yewale, S., Agrawal, P., Shobhane, P., ... & Gangarde, R. (2024). Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. Engineering Proceedings, 62(1), 6.

Mamadalieva, S., Abdurakhimov, O., & Tojidinov, A. (2024). CYBERCRIME AND TECHNOLOGICAL GADGETS. Research and implementation, 2(2), 16-22.

National Crime Agency. (2022, September 5). Cybercrime statistics 2022. National Crime Agency. https://www.nationalcrimeagency.gov.uk/cybercrime-statistics-2022

National Cyber Security Centre. (2023). **Cyber crime and online fraud.** Retrieved from https://www.ncsc.gov.uk/cyber-crime-and-online-fraud

NortonLifeLock. (2022). **What is cybercrime?** Retrieved from https://us.norton.com/internetsecurity-emerging-threats-what-is-cybercrime.html

Okoru, A. O., & Oluku, O. (2024). Cybercrime, Crime Security and National Development in Nigeria. FUOYE JOURNAL OF CRIMINOLOGY AND SECURITY STUDIES, 3(2).

Rafie, P. A., Merta, M. M., & Junaidi, J. (2024). THE ENFORCEMENT OF CYBERCRIME LAW WITHIN THE LEGAL SYSTEM OF INDONESIA. JOURNAL OF HUMANITIES, SOCIAL SCIENCES AND BUSINESS, 3(3), 594-600.

Rasyid, M. F. F., SJ, M. A., Mamu, K. Z., Paminto, S. R., Hidaya, W. A., & Hamadi, A. (2024). CYBERCRIME THREATS AND RESPONSIBILITIES: THE UTILIZATION OF ARTIFICIAL INTELLIGENCE IN ONLINE CRIME. Jurnal Ilmiah Mizani: Wacana Hukum, Ekonomi Dan Keagamaan, 11(1, April), 49-63.

Rughiniș, R., Bran, E., Stăiculescu, A. R., & Radovici, A. (2024). From cybercrime to digital balance: How human development shapes digital risk cultures. Information, 15(1), 50.

Sankhwar, S., Ahuja, R., Choubey, T., Jain, P., Jain, T., & Verma, M. (2024). Cybercrime in India: An analysis of crime against women in ever expanding digital space. Security and Privacy, 7(1), e340.

Shafik, W. (2024). Predicting future cybercrime trends in the metaverse era. In Forecasting cyber-crime in the age of the metaverse (pp. 78-113). IGI Global.

Taherdoost, H. (2024). Insights into Cybercrime Detection and Response: A Review of Time Factor. Information, 15(5), 273.

University of Cybersecurity. (2023, February 8). Resources for educators on preventing cybercrime. University of Cybersecurity. https://www.universityofcybersecurity.edu/resources/preventing-cybercrime

Wall, D. S. (2024). Cybercrime: The transformation of crime in the information age. John Wiley & Sons.

Whelan, C., Dupont, B., Harkin, D., Martin, J., Miccelli, M., & Villeneuve-Dubuc, M. P. (2024). Expertise integration in cybercrime policing: Exploring civilian career lifecycles. Deviant Behavior, 1-18.