IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN OVERVIEW OF CYBER-CRIME AND CYBER-SECURITY IN JALGAON'S DISTRICTS EDUCATIONAL SECTOR

[1]Nitin Namdeo Patil, [2]Dr. Bechoo Lal, [3]Name of 3rd Author Dr. Chandrakant R. Satpute

[1]Research Scholar, [2]Associate Professor, [3]Information Scientist
[1]Department of Computer Science,
[1]Shri JJT University, Jhunjhunu Rajasthan, India

Abstract: The introduction of technology in Jalgaon's education sector has brought many benefits, but also brought along a variety of cyber threats. The objective of this abstract is to give an overview of the cybercrime and cyber security situation within educational institutions in Jalgaon. Significant challenges exist in cybercrime, including the occurrence of phishing and social engineering attacks, ransomware attacks, data breaches, compromised exam integrity, and intellectual property theft. Student records, sensitive research data, and institutional information are the targets of these threats, which could lead to identity theft, financial loss, and reputational damage. Institutions to combat these challenges have initiated various cyber security measures. These encompass heightened awareness campaigns, comprehensive staff and student training programs, implementation of robust security protocols including encryption and firewalls, incident response planning, and collaboration with cyber security experts to assess vulnerabilities and fortify defenses. The purpose of this abstract is to provide a primer for stakeholders in Jalgaon's education sector, highlighting the significance of being vigilant, taking proactive steps, and maintaining a consistent commitment to cyber security. The safety and integrity of educational systems and data must be ensured**.**

Index Terms **- Cybercrime, Cyber Threats, Prevention of Cyber-crime, Cyber security.**

I. Introduction

Technology has revolutionized education, providing unprecedented opportunities for learning and collaboration. Although this digital evolution has brought about transformative benefits, it has exposed educational institutions in Jalgaon to a multitude of cyber threats. Cybercrime has introduced by the growing reliance on digital infrastructure for administrative processes, academic activities, and information storage. The goal of this introduction is to offer an insightful examination of the landscape of cybercrime and cyber security in Jalgaon's educational sector. It examines the challenges of cyber threats, their implications for educational institutions, the measures taken to mitigate risks, and the proactive strategies necessary to reinforce cyber security. Innovation, research, and knowledge dissemination are all part of the education sector in Jalgaon. Despite this, cyber threats have become a growing concern for this sector. From phishing attacks aimed at faculty members to ransomware infiltrations disrupting academic operations and data breaches compromising student records, these threats pose a substantial risk to the confidentiality, integrity, and availability of sensitive information. Proactive measures to strengthen their cyber security posture have adopted by educational institutions in response to these challenges. These policies cover a broad range of topics, such as cyber-security awareness programs, rigorous data protection protocols, the deployment of cutting-edge security technologies, and the creation of comprehensive incident response strategies. Additionally, the Jalgaon government has acknowledged that cyber security is crucial for the education sector. Initiatives have been launched to foster collaboration between educational institutions and cyber security experts, establish dedicated cells to address cyber threats, and promote awareness campaigns to empower stakeholders with the necessary knowledge to combat cybercrime effectively. The cyber threats landscape is constantly changing. Continuous adaptation and enhancement of cyber security measures becomes imperative as cybercriminals use increasingly sophisticated tactics. Collaboration, sharing insights, and being vigilant against emerging threats is crucial for educational institutions, policymakers, and cyber security experts. Through this exploration, I will be able to effectively combat cybercrime with the necessary knowledge. The intention is to emphasize the importance of giving priority to cyber security in Jalgaon's educational sector. The challenges, understanding the implications, and fostering a culture of proactive cyber security measures, educational institutions can safeguard their infrastructure, preserve the integrity of information, and ensure uninterrupted learning environments for the benefit of students, faculty, and the broader academic community.

2. Objectives of the study

- To purpose is to evaluate and record the most frequently encountered cyber menaces that affect educational institutions in Jalgaon, such as phishing, ransomware, data breaches, and other cybercrimes.
- To assess how cyber threats affect educational institutions, taking note of the financial implications, disruptions to academic operations, manipulation of student or institution data damage to their reputation.
- To recognize and comprehend specific vulnerabilities that exist in the education sector in Jalgaon, which could be due to weak points in cyber security infrastructure, a lack of awareness among staff or students, or out-dated security protocols.
- To evaluate the present cyber security protocols, strategies, and initiatives implemented by educational institutions in Jalgaon, and evaluate their effectiveness in combating cyber threats.
- To examine the initiatives, policies, and support frameworks provided by the government of Jalgaon in addressing cyber security challenges within the education sector.
- To anticipate and forecast future cyber threats and trends likely to impact educational institutions in Jalgaon, and propose strategies for future preparedness and resilience.

3. Cybercrime

Cybercrime refers to criminal activities that are carried out using computers, networks, or digital devices, often-targeting individuals, organizations, or entire systems. These criminal activities leverage technology and the internet to perpetrate unlawful actions, often with the intent to steal data, disrupt operations, or cause harm. Cybercrime evolves continuously as technology advances, posing challenges to cyber security. Efforts to combat cybercrime involve implementing robust security measures, educating individuals about online safety, enhancing cyber security laws and regulations, and collaborating across sectors to prevent and respond to these criminal activities.

4. Cyber threats

Cyber threats encompass a wide range of malicious activities conducted through digital means, targeting computer systems, networks, devices, or data. These threats exploit vulnerabilities to compromise the confidentiality, integrity, or availability of information, causing harm or disruption. Here are some common cyber threats:

- **Malware**: Malware, a term encompassing viruses, worms, trojans, and ransomware, is software designed to damage, disrupt, or gain unauthorized access to systems or data. It can infect devices, steal information, or encrypt data for ransom.
- **Phishing:** Phishing involves fraudulent attempts to obtain sensitive information (like passwords, financial details) by masquerading as a trustworthy entity through emails, messages, or websites. It aims to trick individuals into revealing their confidential information.
- **Ransomware**: Ransomware is a type of malware that encrypts files or systems, rendering them inaccessible until a ransom is paid. It can severely disrupt operations and compromise sensitive data.
- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:** These attacks flood networks or systems with excessive traffic, overwhelming them and causing services to become unavailable. It disrupts normal functioning or online services.
- **Social Engineering:** It involves manipulating individuals into divulging confidential information or performing actions that may compromise security. It often exploits human psychology rather than technical vulnerabilities.
- **Data Breaches:** Unauthorized access or exposure of sensitive or confidential information, such as personal records, financial data, or intellectual property. Breaches can occur due to various vulnerabilities or through targeted attacks.
- **Insider Threats**: These involve malicious activities or unintentional breaches caused by individuals within an organization who have access to sensitive information. This could be due to negligence, disgruntlement, or intentional malicious actions.
- **Zero-Day Exploits**: These are vulnerabilities in software or hardware that are unknown to the vendor or without a patch available. Cybercriminals exploit these vulnerabilities before developers can create a fix, making them particularly potent.
- **IoT (Internet of Things) Vulnerabilities**: With the rise of interconnected devices, inadequate security in IoT devices can lead to vulnerabilities that hackers can exploit to gain access to networks or conduct attacks.
- **Supply Chain Attacks**: These attacks target vulnerabilities in third-party software or services used by an organization. By compromising a supplier or partner, cybercriminals gain access to the targeted organization's systems.

Understanding these threats is crucial for developing effective cyber security measures to protect against them. A comprehensive approach that includes awareness, robust security protocols, regular updates, and proactive measures is essential to mitigate the risks posed by cyber threats and also it is cybercrime.

5. Cyber terrorism.

The use of digital technology, especially the internet and computer systems, as a means of committing acts of terrorism is known as cyber terrorism. The aim of this type of terrorism is to cause widespread fear, disruption, or harm to individuals, groups, organizations, or governments by launching political motivated attacks against information systems, networks, or digital infrastructure. Targeting critical infrastructure, financial systems, or essential services is the goal of cyber terrorists in creating fear, panic, and chaos. Widespread societal and economic impacts can be caused by disrupting these systems. It is possible to use threats or significant damage to coerce governments, organizations, or societies with the aim of achieving political, ideological, or social goals. To combat cyber terrorism, it is necessary to have a multi-faceted approach that encompasses strong cyber security measures. Developing response protocols, sharing information, gathering threat intelligence, and cooperating internationally among law enforcement and intelligence agencies. To reduce the potential risks and minimize the impact of cyber-attacks caused by terrorist motives.

6. Cyber security

Cyber security refers to the practice of protecting computer systems, networks, programs, and data from digital attacks, unauthorized access, and damage or theft of information. It encompasses a range of technologies, processes, and practices designed to safeguard digital assets and mitigate the risks posed by cyber threats. Cyber security is crucial across various sectors, including businesses, government agencies, healthcare, finance, and education, among others. With the ever- evolving nature of cyber threats, continuous adaptation, investment in cyber security measures, and collaboration between organizations, governments, and cyber security experts are essential to stay ahead of emerging threats and protect digital assets.

Importance of Cyber Security:

- Robust cyber security measures are vital to safeguard student records, research data, and institutional information from unauthorized access or breaches.
- By demonstrating a commitment to cyber security, educational institutions can uphold their reputation, fostering trust among students, faculty, and stakeholders.
- Securing intellectual property and research data fosters a environment for innovation and encourages research endeavours.
- Compliance with data protection laws and regulations becomes crucial in avoiding legal consequences due to data breaches or mishandling of sensitive information.

II. RESEARCH METHODOLOGY

In this our research we use the quantitative research methods. To comprehend patterns, relationships, or trends in a population, quantitative research involves collecting and analyzing numerical data. Structured methodologies are utilized to collect information and draw conclusions by utilizing statistical, computational, or mathematical techniques. Surveys, experiments, questionnaires, or observations are commonly use in this type of research to quantify behaviors, attitudes, preferences, or characteristics. By providing statistical reliability and generalization of findings to larger populations, it allows for objective analysis and comparison of data, which is its strength. 2806 individuals between 18 and 30 years old participated in this survey by filling out questionnaires on 'Cyber Security and Safety Awareness'. Interview, governments issue reports from various departments for cybercrime.

At various conferences, seminars, and colleges, 2806 people ranging from 18 to 30 and over 30 were given questionnaires for 'Cyber Safety Awareness'. A total number of 2806 respondents answered the questionnaire. Data was collected in hard copy format. To compile and analyse data in required formats such as Excel format, graphs, and others, it became easier to do so by converting this data to Google's online utility, Google Form.

Primary data:

Various methods, such as questionnaires, observing, interviews, and emailing, used to collect primary data by the researcher from their original sources. The data collected by the researcher is precisely aligned with the research requirements.

Secondary data:

Online and offline sources were utilized to collect secondary data. The study consisted of examining reports from both the government's official websites and information security companies' websites. The review of articles on cyber-crimes and information security involved reviewing journals, e-Journals, magazines, newspapers.

III. RESULTS AND DISCUSSION

TRAI (Telecom Regulatory Authority of India) is a non-governmental organization that provides yearly data on internet and phone subscribers in India. TRAI produced state-specific data for rural and urban areas, including numbers and Internet subscribers for each population. TRAI reports that 28.67 percent of rural subscribers are able to access the Internet. Out of every 100 people in urban areas, there are 105.21 urban subscribers, while in the country; there are 57.08 total internet subscribers.

Table 3.1 Indian internet service providers

S.N.	ISP	Share (%)
1	Relince Jio	51.76
2	Bharati Airtel	21.58
3	Vodafone Idea	20.52
4	BSNL	04.91
5	Atria Cov. Tech.	0.32
6	Hathway	0.26
7	Others	0.33

Source: TRAI, 2020

The Western Region of India

Rural regions experienced a variety of internet usage, with Maharashtra (23.61 million), Rajasthan (16.91 million), Gujarat (13.52 million), and Mumbai (1.48 million) being the most popular. Maharashtra had the largest number of internet users (35.444 million) in urban areas, followed by Gujarat (29.65 million), Mumbai (28.45 million), and Rajasthan (21.98 million). Maharashtra is home to 57.59 million internet users, while Gujarat and Rajasthan have respectively 42.61 million and 37.21 million. However, in terms of subscribers in a rural setup, out of hundred people, Maharashtra (37.73) is leading followed by Gujarat (32.792), and Rajasthan (28.981) while in urban geographies Rajasthan (97.15) is leading followed by Gujarat (98.44), and Maharashtra (99.38). The Western regions have an average of 68.01 internet users, with Maharashtra leading the pack at 78.11 followed by Gujarat (65.34) and Rajasthan (52.36). Maharashtra is the most popular internet destination in the region.

We collect the total 2806 number of responses from various ways like questionaries' (offline mode) after that we put the data in excel and analyses it.

Table 3.2 Responses (Age Group Wise)

Age Group	Response	Percentage	Cumulative Frequency	Cumulative Percentage
Below 18 years	1	0.04%	1	0.04%
18-30 Years	2248	83.69%	2249	80.15%
30-45 Yeas	465	12.84%	2714	96.72%
45-60Years	45	1.68%	2759	98.33%
60 years Above	47	1.75%	2806	100.00%
Total	2806	100%		

Table 3.3 the questionnaire revealed the existence of vulnerability gateways

S. N.	Existence of vulnerability gateways (How it may happen)	Y (%)	N (%)	May Be cyber threats are detects
1	Do you have Email	98.00	2.00	-
2	Are you confident in the security of your password?	37.10	62.90	It is possible for anyone to guess the password. Data theft is something that could happen.
3	Can you combine letters, symbols, and numbers in your password?	65.40	34.60	It is simple for passwords to be hacked, and data or important information can also be hacked.
4	Do you make sure to change your password on a regular basis?	45.21	54.79	Their accounts may be threatened by hackers because of this. Hacking is carried out by using the zero day testing method
5	Is 2 step verification something you are knowledgeable about?	26.73	73.27	Hackers are unable to crack passwords easily if the 2-step verification is implemented.
6	Are you known for using distinct passwords for your email and social media accounts?	75.30	24.70	Having multiple passwords is advantageous, but it's possible for people to forget them. It is possible for it to be hacked if it is stored on a mobile or database. Social networking accounts are being harmed by 24.70% of people using the same passwords.
7	Are you familiar with smartphones?	98.00	2.00	-
8	Are you a user of social media?	89.00	11.00	-
9	Are you open to receiving friend requests from individuals you don't know on social media?	29.60	70.40	Take risks in both personal and professional life.
10	Is there antivirus software installed on the computer?	78.80	21.20	Despite this, antivirus is not being used by 21.2% of people. Data loss could happen because of virus intrusion.
11	Do you have a license to use licensed antivirus software?	54.00	46.00	Pirated software is being used by almost 46% of users, which is incorrect. Security updates and patches provided by legitimate vendors are often absent from pirated software
12	Are you currently using antivirus and firewall on your computer?	33.00	67.00	The objective is to educate 67% of the population about the use of firewalls.
13	Is your internet wi-fi password secure?	78.00	22.00	There is a possibility of losing information or data.
14	Have you ensured that your sensitive information is protected?	72.30	27.70	There is a possibility of losing information or data.
15	Having knowledge of your mobile phone's IMEI number.	45.00	55.00	Provides assistance in preventing mobile theft. Having the IMEI is a risk factor for hacking personal information or financial loss.
16	Are you utilizing either a debit or credit card?	65.60	34.40	The risk of using cards incorrectly is amplified by their use.
17	Do you make online purchases from trusted websites?	59.60	40.40	If online shopping is not used properly, there are more threats that can arise.
18	After using ATMs, receipts are discarded as they contain contact information.	73.80	26.20	Hackers may use transaction details to their advantage.
19	Log out of your email-Account and Internet Banking service after using them.	88.00	12.00	Hackers/cyber criminals can enter the account by logging off without leaving.
20	Are you using your mobile device to store your PIN or password?	25.30	74.70	Cyber criminals use details when it comes to mobile theft.
21	Does your Bluetooth device or cell phone have Bluetooth on?	17.50	82.50	Bluetooth increases the likelihood of transferring data and files.
22	Are you being offered large sums of money or discounts through emails, SMSs, or phone calls?	55.40	44.60	Cybercrimes response gateways.
23	Do you respond to these calls, SMS, or emails?	15.60	84.40	By accepting such calls, cyber criminals are invited.
24	Are you sharing your personal information, including a photo, mobile number, and other details, on social media platforms?	50.10	49.90	It is possible to experience personal, financial, and social loss
25	How to respond to calls via SMS, email, call, or entertainment.	26.00	74.00	The danger of cybercrimes is increasing.

This can be seen in the table above, Social networking sites, financial transactions through debit and credit cards, and online shopping are just a few of the various technologies that people are using for communication and other tasks. Using online or social networking sites requires individuals to be aware of safety rules, as indicated by the significance of these percentages. Nearly 98 percent of the population utilizes the Internet and emails, while 89 percent utilize social networking sites like Facebook , Instagram, WhatsApp, , and Twitter. This increases their chances of becoming victims of cyber-crimes. Virus protection software is used by 78.80 percent of people. It's beneficial to be aware of how to use antivirus software. The fear of information security or data security may be triggered by 21.20 percent of educated groups not using antivirus. Online shopping is a popular choice for almost 59.60 percent of people. There is a possibility that this percentage will increase in the future. Thus, the danger of engaging in digital crimes (such as sharing personal information and divulging financial details) is also elevated. 65.60 percent of individuals in this age group, mostly students, use debit or credit cards. Cybercrimes are possible due to the risk associated with losing cards, careless ATM usage, or online transactions.

The conclusion of the data analysis based on the above survey.

- The observations made in the Technology Awareness and Cyber security Risk Analysis Report suggest that a proactive awareness campaign on cyber safety is needed.
- Financial transactions are being made using new technologies like the Internet, emails, social networking sites, antivirus, online shopping, and debit/credit cards by individuals. The lack of knowledge about the appropriate use of these technologies poses a serious risk of increasing cyber-crimes.

IV Conclusion

The intersection of cybercrime and cyber security within Jalgaon’s education sector presents a complex landscape fraught with challenges and opportunities for growth. The evolving technological landscape has brought forth tremendous advancements in education but has concurrently exposed educational institutions to various cyber threats. Cybercrime, encompassing phishing attacks, ransomware incidents, data breaches, and intellectual property theft, poses significant risks to the confidentiality, integrity, and availability of sensitive information within educational systems. These threats can disrupt academic activities, compromise student records, erode trust, and potentially lead to financial losses or reputational damage. However, the importance of robust cyber security measures cannot be overstated. Effective cyber security practices serve as a shield against these threats, ensuring the protection of sensitive data, maintaining academic continuity, preserving institutional reputation, and fostering an environment conducive to innovation and research. The government's initiatives, collaborative efforts with cyber security experts, and institutional commitments to proactive measures are crucial steps toward fortifying cyber security defenses within educational institutions. Education, awareness, regular risk assessments, implementation of cutting-edge technologies, and comprehensive incident response strategies are key elements in mitigating the risks posed by cyber threats. Moving forward, a holistic approach that emphasizes continuous adaptation, collaboration, and investment in cyber security infrastructure is essential. By prioritizing cyber security measures, educational institutions in Jalgaon can create resilient defenses, mitigate risks, and ensure a safe and secure digital environment conducive to learning, research, and innovation in the digital age. The education sector faces a spectrum of cyber threats due to its increasing reliance on technology for administrative, teaching, and learning purposes. Addressing these threats requires a multifaceted approach:

- Training students, faculty, and staff on cyber security best practices and how to identify and respond to potential threats.
- Implementing strong encryption, firewalls, multi-factor authentication, and regular software updates to protect systems and data.
- Creating strategies to respond quickly to cyber security incidents, minimizing damage, and ensuring a swift recovery.
- Engaging with cyber security experts and leveraging partnerships to assess vulnerabilities and fortify defenses against evolving cyber threats.

By prioritizing cyber security measures and staying vigilant against emerging threats, educational institutions can better protect their sensitive data, uphold academic integrity, and ensure a safe learning environment for students and staff.

REFERENCES

[1]. P DUTTA, S SARKAR – “Trend and Differentials of a Socio-Demographic Scenario and Extent of Adolescent Fertility in Jalgaon, India.”, Journal of Settlements & Spatial Planning, 2014

[2]. P Chintal, RJ Gaikwad, RR Deshmukh –“ Cyber-crime analysis of Jalgaon state using gradient descent approach with linear regression” Int. J. Pure Appl. Math, 2018

[3]. AK Mokha – “A Study on Awareness of Cyber Crime and Security”, Research Journal of Humanities and Social Sciences, March 2018

[4]. Shekh Moinuddin, “Contours of Internet Access in Rural-Urban Landscapes in India”, DOI reference: 10.1080/13673882.2021.00001100

[5]. Ali, M. M. (June 2016). Determinants of preventing cybercrime: A survey research [Abstract]. International Journal of Management Science and Business Administration, 2(7), 16-24. doi:10.18775/ijmsba.1849-5664-5419.2014.27.1002

[6]. Sukhai, Nataliya B. (8 October 2004). "Hacking and cybercrime". Proceedings of the 1st annual conference on Information security curriculum development. New York, NY, USA: ACM. doi:10.1145/1059524.1059553.

[7]. Ramdinmawii, Esther; Ghisingh, Seema; Sharma, Usha Mary (15 June 2015). "A Study on the Cyber-Crime and Cyber Criminals: A Global Problem". International Journal of Web Technology. 004 (001): 7–11. doi:10.20894/ijwt.104.004.001.003. ISSN 2278-2389.

[8]. Swati S. , Asha N, “Analysis of cyber safety awareness amongst internet user in pune”, International journal of applied business and economic research, Vol 15,Part II, 2017

[9]. https://en.wikipedia.org/wiki/Cybercrime

[10]. https://www.mass.gov/info-details/know-the-types-of-cyber-threats

[11]. Annual Report 2020-21, Telecom Regulatory Authority of India
[12]. Annual Report 2019-20, Telecom Regulatory Authority of India
[13]. Annual Report 2018-19, Telecom Regulatory Authority of India
[14]. Cyber Crimes. Retrieved July 20, 2021, from http://cybercellmumbai.gov.in
[15]. Cyber Threats. (2020, November 21). Times of India, p. 4.
[16]. Crime Statistics 2020. Retrieved October 2, 2023, from http://www.ncrb.org
[17]. http://cybercellmumbai.gov.in/html/cyber-crimes/index.htm
[18]. https://www.nasscom.in/knowledge-center/publications/dsci-kpmg-secure-india-2023- gcc-empowered-global-cybersecurity-and-digital-risk-management
[19]. http://www.internetlivestats.com/internet-users/india/.
[20]. https://factly.in/cyber-crimes-in-india-which-state-tops-thechart/
[21]. All net Available: http://www.all.net/CID/Threat/Threat22.html
[22]. http://www.businessinsider.com/worlds-10-cybercrime-hotspots-in-2016-ranked-symantec-2017-5?IR=T#10-vietnam-216-1
[23]. https://cyware.com/news/top-10-countries-withmost-hackers-in-the-world-42e1c94e
[24]. https://factly.in/cyber-crimes-in-india-which-statetops-the-chart/