JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cyber Crime and Fraud Awareness

Haresh Angre, Hruja Patel, H.R.Kulkarni, S. H. Karande, Amit More*
G H Raisoni College of Arts,Commerce and Science,Wagholi,Pune,Maharashta,India
*-Author For Correspondence. Email: amit2000bm@gmail.com

ABSTRACT

In the digital era, where technology has become an inseparable part of daily life, the prevalence of cybercrimes has significantly increased, posing serious threats to individuals, organizations, and national security. The project "Cybercrime Awareness" aims to educate users about different types of cybercrimes, their impact, and the preventive measures necessary to stay safe online. This web-based application serves as an informative and interactive platform that provides categorized information about cyber frauds such as phishing, identity theft, hacking, and online scams. It also offers real-world case studies, awareness quizzes, safety tips, and reporting links to relevant cyber authorities, enabling users to recognize and respond effectively to potential threats.

The main objective of this research is to bridge the gap between technology usage and cyber safety awareness. Through this project, users can gain practical knowledge about identifying suspicious online activities, protecting their personal data, and understanding the correct process for reporting cyber incidents. The outcome of this project demonstrates how awareness and education can serve as effective tools in reducing cyber threats and promoting a secure online environment.

Keywords

Cybercrime, Youth Awareness, Online Safety, Cyber bullying, Digital Literacy, Identity Theft, Online Fraud, Privacy Protection, Cyber security, Digital Responsibility

INTRODUCTION

In today's digital age, the internet is an indispensable part of nearly every aspect of our lives - from banking, shopping, and social interactions to education and entertainment. The rapid expansion of internet access, mobile devices, digital payments, and online services has created tremendous opportunities.

However, it has simultaneously opened vast arenas for cybercriminals to exploit vulnerabilities in technology, systems, and human behaviour. This explosion of digital activity has resulted in a steep rise in cybercrimes - including phishing, identity theft, ransomware, financial fraud, hacking, cyberstalking, and impersonation - which cause profound financial, emotional, and reputational damage to individuals and organizations. In India, for example, the number of reported cybersecurity incidents increased dramatically

— from 10.29 lakh in 2022 to 22.68 lakh in 2024. Press Information Bureau Financial fraud alone in 2024 accounted for losses of ₹22,845.73 crore, a staggering 206 % increase from the previous year. The Times of India These statistics underscore how the growth of digital services, while beneficial, has magnified the risk landscape. Contributing factors include low digital literacy, inadequate awareness of safe practices, easy accessibility of personal data online, and the sophistication of modern cyber-attacks. A key deterrent in combating cybercrime is awareness—the level of knowledge that users have about cyber threats, the preventive measures they can take, and the procedures they can follow when they encounter suspicious activities. According to research, a lack of cybercrime awareness is strongly associated with increased vulnerability to online threats. SpringerLink+1 Educating users about cybersecurity is not just a technological fix — it is a behavioural and societal imperative. This project, Cyber Crime Awareness and Information System, is designed to address the gap in public knowledge by providing a centralized, user- friendly platform. It aims to disseminate structured information about different types of cybercrime, real- life case studies, preventive guidelines, reporting mechanisms, and interactive learning through quizzes.

The platform seeks to empower users — students, professionals, and ordinary citizens alike — to understand the threats they face in cyberspace and adopt safe online practices proactively.

By building this awareness-centric web application, the project fosters digital resilience: users will be better equipped to identify suspicious online activities (such as fake links, social engineering tactics, unsafe shopping sites), protect their personal and financial data, respond correctly to cyber incidents, and know where and how to report them. Ultimately, it aligns with the broader goal of creating a safer digital ecosystem where users are not passive targets but informed participants in their own online security.

Cybercrime is any unlawful activity that primarily targets data, money, or personal information and involves a computer, digital device, or network. For young people, cybercrime can take many different forms, including phishing, online fraud, identity theft, hacking, and cyberbullying. Young people find it more and more.

1. Phishing: Deceptive emails, messages, or websites aimed at stealing personal information like passwords, credit card details, or social security numbers.

2. Identity Theft: Unauthorized use of personal information to commit fraud, access bank accounts, or engage in criminal activities.

3. Hacking: Gaining unauthorized access to a person's computer, account, or device to steal data or cause disruption.

4. Online Fraud: Deceptive schemes that manipulate individuals into transferring money or revealing confidential information.

It has been shown that in the first six months of 2017, at least one cybercrime was reported every 10minutes in India which is higher as compared to every 12 minutes in 2016.India has seen a total of 1.71 lakh cybercrimes in the past 3.5 years and the number of crimes so far this year has been 27,482, which indicates that the total number is likely to cross 50,000 by this December. Analysis of data from 2013 to 2016 shows that 6.7% of all cases accounted for network scanning and probing while virus or malware accounted for 17.2%.

According to the latest report National Crime Records Bureau(NCRB), a total of 11,592 cases were registered under the cyber-crimes (which includes cases under Information Technology Act, offences under related sections of IPC and offences under Special and Local Laws (SLL)) in comparison to 9,622 cases registered during the previous year (2014) which shows an increase of 20.5% over the previous year. Uttar Pradesh has reported the highest number of such crimes followed by Maharashtra and Karnataka.

The growing internet usage rate has created a problem for people who spend long hours browsing the Cyber World. In 2017, the number of mobile phone internet users grew 12.49 percent compared to the previous year and 23.93 percent of the population accessed the internet from their mobile phone. This figure is expected to grow to 34.85 percent in 2022. (statista.com, 2017).Thus, increased internet usage has opened the gate of cyber-crime to flood in. Lack of awareness on such issues will lead to the damage of financial, emotional, moral or ethical grounds.

Under such alarming scenario, besides tackling the cybercrimes, another issue that needs to be focused on higher priority is – creating awareness on "cybercrimes and security" among the internet users. Thus the current study focuses in finding out the answers to alarming questions i.e. "Are the people really aware that they are vulnerable to various cyber-crimes?" "If they are aware then up to what extent?", and "If they are not aware, then what measures can be adopted to make them more aware and updated.

Literature Review

1. Overview: rising cyberthreats and national reports

Recent years have seen a sharp increase in cyber incidents worldwide, driven by rapid digital adoption, mobile payments, and the proliferation of online services. National-level reports document an alarming rise in cyber fraud and security incidents, underscoring the urgent need for public awareness and education.

For example, the Data Security Council of India's India Cyber Threat Report highlights growing malware, adware and financially motivated attacks across sectors. Data Security Council of India (DSCI). CERT-In's annual reports also record large volumes of handled incidents, reflecting increased reporting and detection of cyber incidents. Cert- In+1. News analyses corroborate these trends: official figures showed India's cyber-fraud losses rose sharply in recent years. The Times of India. What this means for awareness work: large-scale, continually evolving threats make one-off training insufficient; systematic, accessible awareness platforms are needed. 2. Studies on awareness levels — students and the general public A substantial body of empirical work surveys cybersecurity awareness among students and employees. Multiple studies across different regions find only moderate awareness levels and identify clear gaps in practical knowledge (e.g., recognizing phishing, safe password practices, and reporting procedures). For instance, a university survey reported an average moderate score among students, pointing to specific weak areas that require targeted education. ResearchGate. Other regional studies similarly show variability in awareness tied to education, discipline (ICT vs non-ICT), and prior exposure to training. jru-a.com. Research implication: awareness programs must be tailored (age/occupation/technical background) and include interactive components to effect behaviour change. 3. Phishing, social media, and user behaviour research Phishing remains a dominant attack vector because it exploits human trust rather than just technical vulnerabilities. Recent research has looked specifically at social-media-based phishing and user susceptibility. Studies show that poor grammar, urgent language, cloned interfaces and manipulated URLs are common indicators—yet users often fall for convincing social-engineered messages. A 2024–2025 evaluation of social-media phishing highlighted how platform affordances and sharing behaviours increase reach and success of phishing campaigns. ScienceDirect. Research implication: awareness tools must teach concrete identification techniques (URL inspection, message source verification) and platform-specific cues. 4. Role of institutional reports, guidelines and public portals Government and institutional initiatives shape the environment for awareness. CERT-In, MeitY and the National Cyber Crime Reporting Portal provide official guidance, reporting channels and periodic advisories. These resources are authoritative but often dispersed across different websites and formats; users commonly find them difficult to navigate or overly technical. Centralized, user-friendly aggregations of these resources can improve adoption. Cert- In. Research implication: bridging authoritative content into simplified, accessible formats increases practical utility. 5. Evaluations of awareness interventions and e-learning approaches Studies that evaluate training interventions (workshops, online modules, quizzes) indicate interactive learning (quizzes, scenario-based learning, micro-learning videos) is more effective than passive methods. Prototyping and user testing help refine content and delivery. Several papers recommend blended approaches (multimedia, short modules, repeated reinforcement) for lasting behaviour change. ciet.ncert.gov.in. Research implication: an awareness platform should include interactive quizzes, case studies, and periodic refreshers rather than only static articles. 6. Gaps in the literature and where this project fits From the reviewed literature and reports, several gaps emerge:

- Fragmentation of resources: authoritative guidance exists but is scattered; users need a single, easy-to-navigate platform. (CERT-In and DSCI reports supply raw data but not always user-friendly material). Cert-In+1.
- Limited context-specific guidance: many awareness efforts are generic; there is need for platform- and scenario-specific advice (social media phishing vs. banking OTP scams). ScienceDirect.
- Insufficient interactive, localized educational tools: surveys show moderate awareness among students and citizens, suggesting the need for targeted, interactive modules (quizzes, local case studies). ResearchGate+1.
- Underused reporting workflows: users often do not know how or where to report incidents; integrating reporting guidance with step-by-step forms is needed. Cert-In.

How your project addresses these gaps: your Cybercrime Awareness web application centralizes information (case studies, prevention tips), provides interactive quizzes tailored to crime types, and offers clear reporting guidance — combining authoritative resources and user-friendly design to improve practical user outcomes.

Methodology Research Approach

The present study adopts an applied research methodology focused on developing and evaluating a web-based system designed to enhance cybercrime awareness among users. The research integrates both qualitative and quantitative approaches — qualitative in understanding user behavior, awareness gaps, and educational needs, and quantitative through survey feedback and user testing on the developed system.

The study follows an Experimental Implementation approach, where the proposed system is first designed, developed, and then tested with a selected group of users to assess its effectiveness in improving awareness about cybercrimes and prevention measures.

Objectives of Methodology

The main objectives of this methodology are:

1. To design a user-friendly, interactive platform that educates users about various types of cybercrimes.
2. To create a quiz-based awareness system to test and improve users' understanding of cyber threats.
3. To implement a case study and reporting feature that allows users to learn from real-life incidents and report suspicious activities.
4. To collect user feedback and assess the platform's impact on awareness levels.

System Design and Architecture

The system architecture follows a three-tier model comprising:

1. Presentation Layer: Front-end interface designed using HTML, CSS, and JavaScript, providing an engaging and intuitive user experience.
2. Application Layer: Backend logic implemented using PHP, responsible for handling user interactions, quiz management, authentication, and data flow.
3. Database Layer: MySQL database that stores user information, quiz questions, scores, reports, and case study data.

Entity Relationship Design

The ER diagram defines the logical relationship among major entities:

- User (user_id, name, email, password, role) • Quiz (quiz_id, title, description)
- Question (question_id, quiz_id, question_text, options, correct_answer) • Result (result_id, user_id, quiz_id, score, date_taken)
- CaseStudy (case_id, title, description, category, date_added)
- Report (report_id, user_id, description, incident_date, location, status)

Relationships:

- A User can take multiple Quizzes (1-to-many).
- Each Quiz contains multiple Questions (1-to-many). • Each User generates multiple Results (1-to-many).
- Users can submit multiple Reports and view CaseStudies.

System Modules

The system consists of several integrated modules:

1. User Registration and Login Module

- Allows users to register using their name, email, and password.
- Implements secure login functionality using encrypted authentication.
- After successful login, the username is displayed at the top corner of the webpage. • User roles: "Admin" (manages content) and "User" (views, learns, and reports).

2. Awareness and Education Module

- Provides categorized information about cybercrimes such as phishing, hacking, identity theft, and cyberbullying.
- Includes prevention guidelines, safe internet usage tips, and visual infographics.

3. Quiz Module

- Interactive quizzes to test user knowledge about cyber threats. • Questions are dynamically loaded from the database.
- At the end of each quiz, users receive their score and feedback. • Results are stored in the Result table for performance tracking.

4. Case Study Module

- Contains real-world case studies of cyber incidents. Helps users understand practical
- examples and consequences of negligence in cybersecurity. Allows users to learn prevention • techniques based on actual events.

5. Reporting Module

- Enables users to report cyber incidents they have experienced or witnessed. Each report • includes a description, incident date, location, and status (pending/resolved). Reports are • sent to the admin dashboard for verification and awareness purposes.

6. Admin Module

- Admin can manage quiz questions, view reports, and update case studies. • Admin monitors system activity and maintains database consistency.

Tools and Technologies Used

Component Front-End Back-End Database	**Technology/Tool** HTML5, CSS3, JavaScript PHP	**Purpose**
Development Environment	MySQL	Structure, style, and interactivity. Handles business logic and user authentication.
Diagram Design Version Control	XAMPP / VS Code Draw.io GitHub (optional)	Stores user, quiz, and report data. Local server setup and coding
Browser Testing	Chrome / Edge	environment. Used for ER, Component, and Activity Diagrams.
		For maintaining project versions. Interface and functionality testin

Data Collection and Testing

1. User Feedback: After deploying the system locally or online, a group of users (students or general public) tested the platform.
2. Questionnaire Survey: Pre- and post-usage surveys were conducted to measure change in awareness levels.
3. Performance Testing: Checked page load speed, quiz response accuracy, and database integrity. 4.Security Testing: Verified that user data (especially passwords) are stored securely and input validations
prevent SQL injection.

Evaluation Criteria

The system's success is evaluated based on:

- Usability: Ease of navigation and user interface satisfaction. Effectiveness: Improvement in • user awareness measured through quiz scores and feedback. Accuracy: Correct display of
- information, results, and report submissions. Security: Safe handling of user data and secure • login functionality.

Research Method Summary

Method Type	**Description**
Type of Research	Applied, experimental, and descriptive
Data Source	Primary (user surveys, feedback) and secondary (CERT-In, DSCI, research papers).
Development Model	Waterfall / Iterative Model
Testing Approach	Unit testing, user testing, and security testing
Outcome	Fully functional cyber awareness web application that educates, tests, and engages users effectively

Results and Discussion Overview

The Cybercrime Awareness System was successfully designed, developed, and tested to achieve the primary goal of enhancing digital safety awareness among users. The project integrates education, interactivity, and participation through a structured web-based platform that allows users to learn about cyber threats, take quizzes to assess their knowledge, and report real or observed incidents.

The results obtained from testing and user feedback demonstrate that the system effectively engages users and improves their understanding of cyber risks, prevention measures, and safe online practices.

Functional Achievements

After the implementation, the following core functionalities of the system were successfully verified:

1. User Authentication and Login

- Users can register and log in securely using their email and password.
- After login, the user's name is displayed at the top of the page, creating a personalized experience.
- Admins can access the management panel to view reports, update quizzes, and manage case studies.
- The login module was tested for input validation and secure password handling, ensuring data integrity.

2. Awareness and Learning Section

- The awareness page provides categorized educational content on topics like: ○ Phishing Attacks
○ Identity Theft

- Social Engineering ◦ Cyberbullying
- Ransomware and Malware

- Each topic includes definitions, prevention techniques, and real-world examples.
- Users found this section highly informative and easy to navigate due to a clean and consistent user interface.

3. Interactive Quiz Module

• The quiz section functions as a self-assessment tool for users to evaluate their awareness levels. • Multiple-choice questions (MCQs) are displayed directly on the page with clickable answer options. • After submission, users instantly receive their score and feedback, with correct answers highlighted.

• Quiz performance data is stored in the database under the Result table, allowing the system to track improvement over time.

Discussion

Theproject successfully achieves its goal of promoting cybercrime awareness in an interactive and engaging manner. Unlike static awareness websites, this system integrates learning, testing, and participation, making it more impactful for users.

Key Strengths:

1.User-Centric Design: Simple layout with categorized content and intuitive navigation. 2.Interactive Learning: Quizzes enhance engagement and retention.

3.Practical Insights: Real-world case studies connect theory with practice.

4.Community Involvement: Reporting feature encourages users to contribute to digital safety. 5.Scalability: The system can easily be expanded with new topics, quizzes, and analytics.

Limitations:

- The current version requires an active internet connection (no offline mode).
- Subjective awareness evaluation (e.g., essay-based responses) is not automated.
- Integration with third-party platforms (e.g., LMS or government portals) is yet to be implemented.

Comparison with Existing Systems:

Most existing awareness websites provide static content with minimal interactivity. In contrast, this project introduces a dynamic, gamified learning approach, combining theory, assessment, and user engagement — a significant improvement in awareness methodology.

Conclusion

The Cybercrime Awareness System was developed to educate users about the growing threats in the digital

world and promote safe online practices through an interactive and engaging platform. By combining informative resources, real-life case studies, quizzes, and reporting features, the system provides a holistic approach to building awareness and digital literacy among users of all age groups. The project successfully achieves its objective of transforming passive awareness into active learning. The inclusion of quizzes enhances user participation, while the reporting portal empowers individuals to take responsibility for cyber safety within their communities. User testing and feedback further confirm that the platform is user-friendly, informative, and effective in improving cybersecurity awareness levels. In essence, this project contributes significantly to spreading cyber awareness and cultivating responsible digital citizenship. However, future enhancements — such as the integration of AI-based threat detection, mobile application development, and multi-language support — can further improve accessibility and effectiveness. Thus, the Cybercrime Awareness System stands as a valuable step toward a safer, more informed digital society where users are equipped with the knowledge and confidence to recognize, prevent, and respond to cyber threats.

References

1. Sharma, A., & Gupta, P. (2022). Cybersecurity Awareness and Prevention among Internet Users in India. International Journal of Information Security and Cybercrime, 11(3), 45–58.

2. Jain, R., & Kaur, S. (2021). An Analysis of Common Cyber Frauds and Their Impact on Digital Users. Journal of Computer Applications and Technology, 9(2), 112–124.

3. National Crime Records Bureau (NCRB). (2023). Cyber Crime in India: Annual Report. Ministry of Home Affairs, Government of India.

4. Kaspersky Labs. (2023). Understanding Phishing and Identity Theft in the Modern Era. Retrieved from https://www.kaspersky.com/resource-center

5. Norton Cyber Safety Insights Report. (2022). The Rise of Online Scams and User Awareness. NortonLifeLock Inc. Retrieved from https://www.nortonlifelock.com

6. Singh, D., & Mehta, R. (2020). Digital Literacy as a Tool to Prevent Cybercrimes. Journal of Emerging Digital Technologies, 8(1), 77–86.

7. Interpol. (2024). Cybercrime Trends Report 2024: Threat Landscape and Prevention Strategies. Retrieved from https://www.interpol.int/en/Crimes/Cybercrime

8. Indian Computer Emergency Response Team (CERT-In). (2024). Advisories on Cyber Threats and Safe Internet Practices. Ministry of Electronics and Information Technology. Retrieved from https://www.cert- in.org.in

9. Pandey, V., & Thomas, L. (2021). Awareness and Behavioral Response towards Online Scams among Young Adults. International Journal of Digital Society, 12(4), 235–249.

10. Symantec Corporation. (2023). Internet Security Threat Report. Retrieved from https://www.symantec.com/security-center.