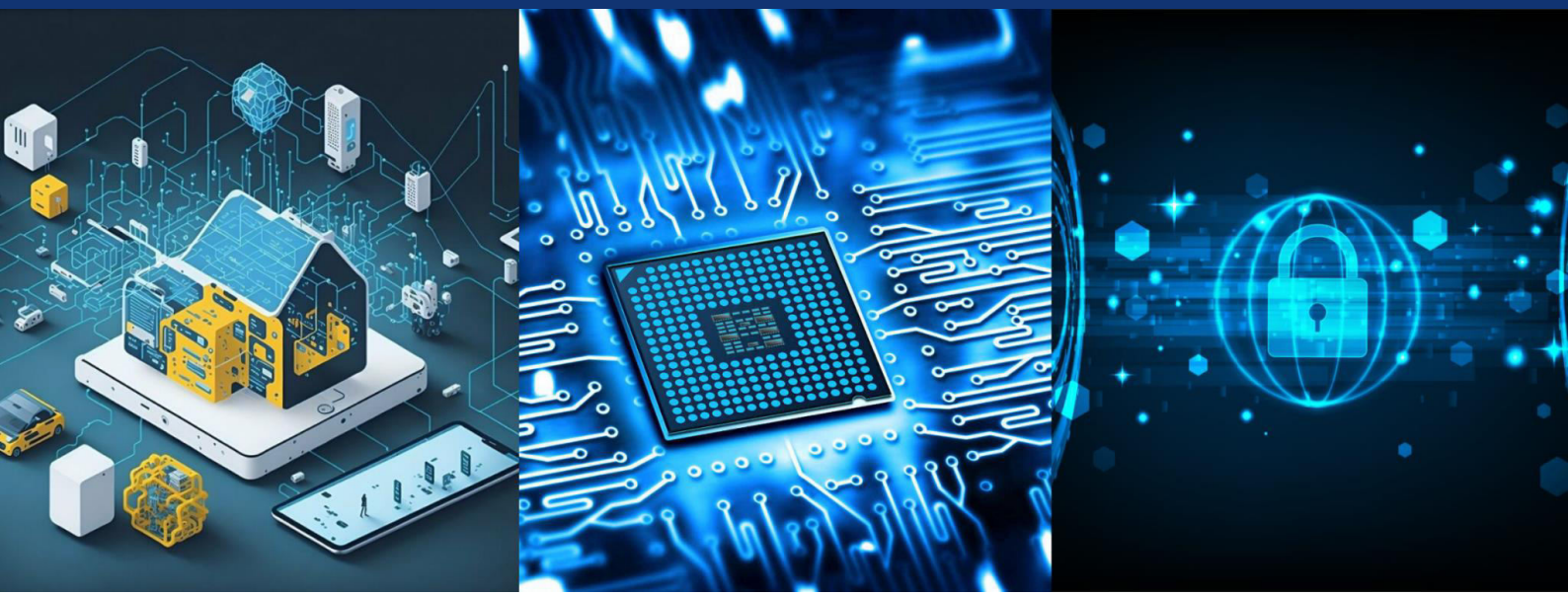
IJIRCCE

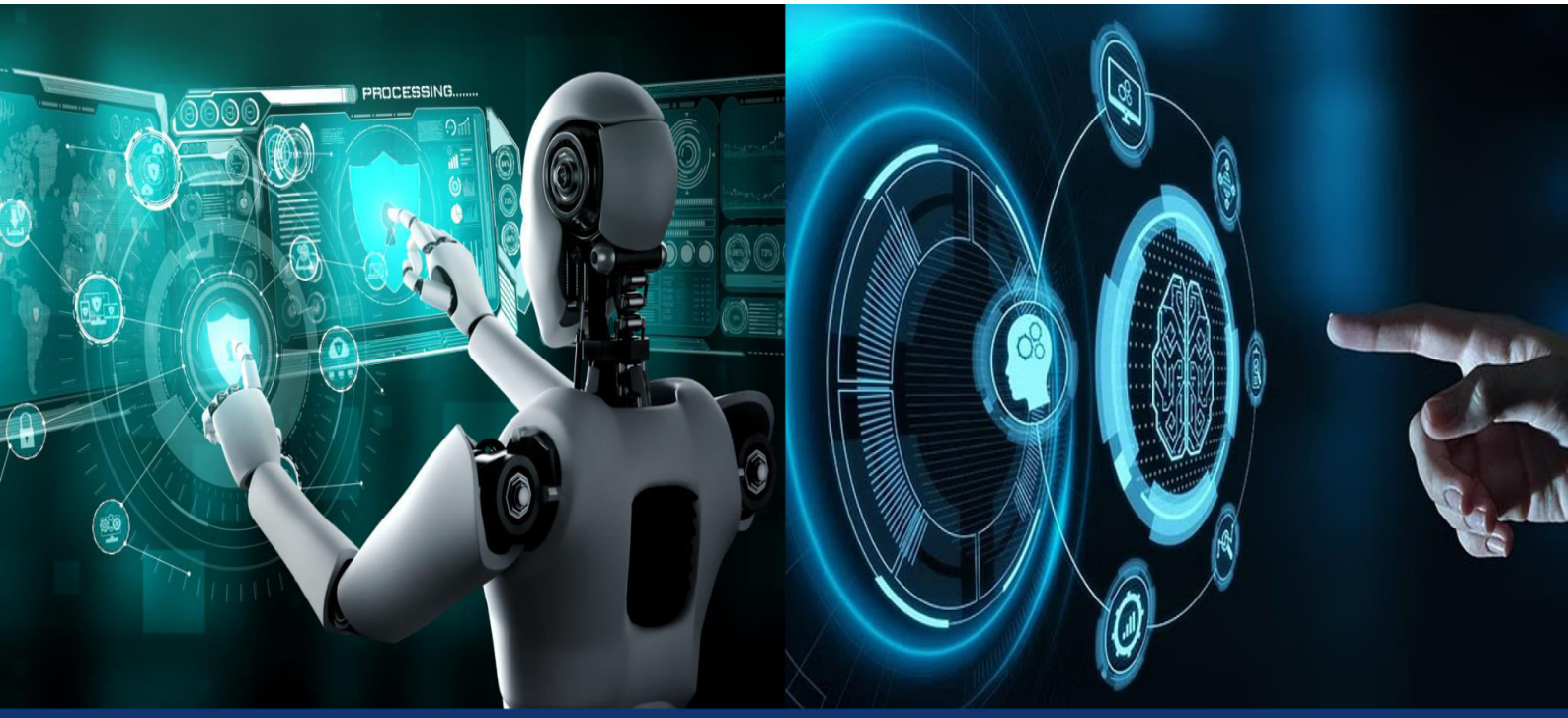
ISSN(O): 2320-9801

ISSN(P): 2320-9798



# International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)




**Impact Factor: 8.771**

**Volume 13, Issue 5, May 2025**

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305168

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

# Identity Guardian: Cyber Security Awareness

**Dr. Gobi N[1], Ajay Maharajan[2], Akshara Chindam[3], Mohammed ibrahim[4], Mihir Kapuriya[5]**

Professor, School of CS and IT, JAIN (Deemed to be) University, Bengaluru, India [1]

Student, School of CS and IT, Department of MCA, JAIN (Deemed to be) University, Bengaluru, India[2-5]

**ABSTRACT:** Cybersecurity risks are growing more concerning in today's digital environment, particularly in sectors where data breaches and cyberattacks can have dire repercussions. The increasing number of sophisticated cyberthreats that both individuals and companies must deal with highlights the significance of proactive cybersecurity awareness and education. With a focus on simulation-based learning and the development of an interactive awareness game, this research article examines the importance of cybersecurity awareness in lowering threats. By reviewing previous cyber-attacks and applying a gamified learning strategy, this study tries to improve user understanding and readiness. According to the results, combining interactive gaming with realistic simulations significantly boosts user engagement and comprehension of cybersecurity procedures. The study also highlights how crucial it is to have adaptable and dynamic teaching resources in order to successfully handle the ever-evolving threat scenario. Establishing a culture of continuous learning and awareness can significantly reduce an organization's vulnerability to cyberattacks. The several modules and functionalities that make up Identity Guardian's core are carefully examined in this paper. The website provides a variety of instructional materials, such as cybersecurity best practices and an interactive test that mimics actual assault situations. Additionally, Identity Guardian has a dedicated module that incorporates web apps like OWASP Juice Shop, bWAPP, and DVWA that are purposefully vulnerable.Users can conduct real-world cyberattacks like as SQL Injection, Cross-Site Scripting (XSS), Cross-Site Scripting (CSRF), and failed authentication in these secure and authorized environments. Users are better equipped to identify and counteract these risks as a result of this hands-on exposure, which also helps them comprehend the attacker's perspective. Additionally, by enabling users to actively participate in conversations, share their stories, and collectively fortify their defenses against identity theft, Identity Guardian fosters community resilience. This paper serves as a thorough guide as we examine Identity Guardian's intricacies, offering a thorough description of the platform's inception, development, and expected impact. Identity Guardian is proof of the constant innovation in the quest for a safer, more secure digital future, which is necessary given the dynamic nature of the digital world.

## I. INTRODUCTION

The "identity guardian" idea emphasizes the preventative measures that people and institutions need to take to safeguard digital identities from online attacks. Cyberattacks are growing more complex and common as more and more personal and business interactions take place on digital platforms. The significance of cybersecurity awareness and its function in protecting private information are examined in this research. The report highlights how cyber hazards are becoming more prevalent across a range of businesses and how important informed user behavior is to reducing these risks. Cybersecurity risks have become a major concern for people, companies, and governments in the current digital era. As technology continues to advance, fraudsters get better at taking advantage of system flaws. Phishing attacks, ransomware, malware, social engineering, and insider threats are just a few of the many challenges that require heightened cybersecurity awareness. More than 85% of security breaches are caused by human error, according to research (Verizon Data Breach Investigations Report, 2024). This report underscores the need of instructional programs that provide users with the information and skills to recognize and manage possible dangers in a proactive manner. Gamification—the use of game-based features to engage consumers in learning activities—is one of the best ways to raise awareness of cybersecurity. Gamification's capacity to boost motivation, engagement, and information retention has made it a successful training tool in a variety of fields, including business training, healthcare, and education. Gamification in the context of cybersecurity uses interactive learning challenges, simulations, and experiences to help users comprehend real-world cyberthreats. This study uses interactive simulations, digital media (blogs), and gamification to examine the importance of cybersecurity knowledge. It evaluates how well they work to improve security procedures and lessen cyberthreats. The rising sophistication and frequency of cyber-attacks have positioned cybersecurity as a critical concern in our linked society.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305168

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

## II. LITERATURE REVIEW

Research on cybersecurity threats already conducted shows a notable rise in assaults targeting several industries, including ransomware, malware, and phishing. According to research, cybersecurity blogs are essential for disseminating current knowledge on new dangers, practical solutions, and safeguards. Additionally, research on simulation-based learning and gamification shows that interactive methods are effective in educating users about cybersecurity. A theoretical framework for the investigation is developed in this section by integrating data from various sources. Since cybersecurity is a universal problem that impacts everyone, it has become a major worry for all Malaysian people, professionals, lawmakers, and decision-makers. It has grown to be a significant issue for civilizations that need to protect themselves from cyberattacks, requiring both proactive and reactive measures that need close observation. Finding a balance between defending individual freedoms and avoiding extensive surveillance is essential. Computer security, sometimes known as information security or cyber security, is synonymous with cybersecurity. It protects computer systems against damage to their data, software, or hardware as well as from interruptions or loss of service (Roca et al., 2019). The cybercrime statistics for 2018 and 2019 are shown in Fig. 1. 1. After reviewing the data from the Royal Malaysia Police, the writers of the cyber security strategy discovered that they had dealt with 10742 instances of cybercrime in 2018. An estimated 400 million RM was lost as a result of these accidents. The number of cybercrime incidents increased to 11875 in just one year, from 2019 to 2020, with an anticipated loss of around RM500 million (n. A. Malaysia cyber security policy, 2019).

### 1. CYBERSECURITY OVERVIEW FOR 2025

The top themes influencing the cybersecurity environment of 2024, according to Gartner, are identity-first security methods, continuous attacks, third-party provider risk, unprotected employee behaviour, and Generator AI (Genai). Approximately half of managers think they will be governed by Genai. sophisticated, contentious abilities such deep counterfeiting, malware, and phishing. Businesses may still use Genai's expertise to enhance operational security even if they accept additional risks. This is 12.6% even though they worked in cybersecurity globally in 2023. There is a 4 million cybersecurity professional deficit in 2024, and if cutting-edge technologies and creative solutions are not handled, the number might rise to 8 million by 2030. The number of firms sustaining minimal sustainable cyber resilience has increased by 30% in 2024, widening the gap between those battling and those that are resilient. For 52% of these firms, the largest obstacle to designing cyber resistance is a lack of resources and expertise, despite the fact that process changes and legacy technology are also significant obstacles.

### 2. FORECASTS FOR CYBERSECURITY IN 2024

Among Genai's numerous cybersecurity applications, two standout prospects tackle the issues of insufficient expertise and unsafe human conduct. Companies may bridge the qualification gap and do away with 50% of entry-level positions requiring specialized expertise by 2028 by implementing Genai. event involving cybersecurity. Genai may assist companies in creating highly customized training materials by considering the responsibilities and individual characteristics of each employee. By 2026, the organization will assist in a 40% staff reduction.

Over the last two years, 45% of firms have used third-party suppliers, whose commitment represents the largest security concerns. More and more companies are growing in importance and strengthening their resistance as we seek an identity-based strategy to cybersecurity, identity and access management (IAM).

### AI's Role in Addressing Cybersecurity Challenges

By tackling two significant issues—the skills gap and human error in security procedures—generative artificial intelligence (GenAI) is transforming cybersecurity. Nearly 50% of entry-level cybersecurity positions are expected to require no specialist expertise by 2028 thanks to AI, opening up the industry to newcomers. Additionally, by 2026, AI can assist companies in creating highly customized training programs based on the jobs of their employees, lowering human error linked to security by 40%. Through automation and predictive analytics, these AI-powered systems seek to improve efficacy while streamlining cybersecurity processes.

### The Rising Threat of AI-Driven Attacks

AI has benefits for security, but it also brings with it new dangers. Threat actors are using AI to carry out complex assaults, including narrative attacks, deepfakes, and phishing campaigns driven by AI. Deepfakes have been used to produce incredibly realistic fake voice and video recordings, tricking staff members into sending money or divulging private information. One such instance included a Hong Kong finance clerk who fell victim to a deepfake scam and was defrauded of $25 million. Another AI-driven concern is narrative assaults, which use AI-generated material to

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305168

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

undermine organizations or propagate false information. Threat intelligence and early detection systems will be essential for organizations in 2024 as these attacks have the potential to seriously harm a company's brand and influence public opinion.

**Cybersecurity Budgets and Strategic Investments**

Spending on cybersecurity in 2024 is anticipated to be strategic and laser-focused, notwithstanding economic uncertainty. Businesses are giving priority to investments in sectors that yield the highest business value, like: Several crucial areas require concentrated attention in order to successfully handle today's cybersecurity challenges: Strong threat detection and response tools are necessary for real-time system monitoring and prompt incident mitigation; Zero Trust security frameworks are essential for preventing unauthorized lateral movement within networks, which lessens the impact of breaches; API security is critical for preventing data leaks and unauthorized access to sensitive information; and complete cloud security solutions are becoming more and more important as companies keep moving to cloud-based services and infrastructures. However, budget constraints are forcing companies to optimize their cybersecurity spending, making it critical to balance risk mitigation with cost-effective security solutions.

## III. AWARENESS SIMULATOR GAME CONCEPT

By creating an interactive awareness simulator game, the Identity Guardian project presents a fresh and captivating method of cybersecurity teaching. This game's primary goals are diverse and include offering a thorough and useful educational experience. First and foremost, the game will simulate real-world cyberattacks, giving players a secure and regulated environment in which to encounter a variety of cybersecurity dangers. To comprehend the real-world effects of these risks, experiential learning is essential. Second, educating on best practices is a major goal. To this end, the game will offer concise, practical advice on how to recognize various cyberthreats and the best ways to counteract their effects. Thirdly, in order to optimize the educational process, Through the clever use of gamification components, such as challenges that call on players to apply their knowledge and incentives that encourage learning and advancement, the game integrates engaging and interactive learning, increasing user motivation and engagement. Finally, recognizing the diverse needs of different organizations, the game will offer Customizable Scenarios, enabling organizations to tailor the simulated threats and learning modules to accurately reflect the specific cybersecurity risks prevalent within their particular industry or operational context. The Identity Guardian game seeks to close the current knowledge gap in cybersecurity awareness by skilfully incorporating these essential components and equipping players with the knowledge and abilities needed to proactively implement strong cybersecurity measures in their everyday digital interactions.

**Challenges in Cybersecurity Education:**

The efficacy of cybersecurity education is now hampered by a number of important issues, especially in academic institutions. One major issue is that smaller institutions sometimes lack the funds and resources necessary to invest in state-of-the-art cybersecurity training materials. Second, standard teaching techniques (textbooks, lectures) are less successful in involving students in what is frequently seen as a difficult and abstract topic, which results in decreased levels of interest and retention. Thirdly, students frequently lack real experience in recognizing and addressing cyber dangers, which is crucial for converting theoretical knowledge into readiness and practical abilities. This is a significant gap in existing teaching techniques.

**Gamification as a Solution:**

The application of Using game-based learning approaches (quizzes) offers a compelling answer to these educational issues by demonstrating enhancing information retention and overall student engagement. Additionally, the use of real-world cybersecurity attack simulations gives students priceless real-world experience that aids in their ability to identify different threat vectors and formulate suitable response plans in a risk-free setting. Important problem-solving and critical thinking skills that are directly applicable to real-world cybersecurity scenarios are also developed in this interactive learning environment, which is promoted through gamified simulations and challenge.

**Implementation and Results:**

A study was carried out to see how beneficial a Students participated in the study to test a gamified cybersecurity learning platform. The results demonstrated a considerable improvement in participants' cybersecurity knowledge as well as higher student involvement when compared to traditional techniques. Notably, after using the gamified learning

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305168

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

platform, students expressed increased confidence in their ability to identify malware risks and phishing schemes, demonstrating a successful conversion of information into useful identification abilities.

## IV. PROBLEM STATEMENT

**Common Cybersecurity Challenges in Everyday Life**

Inadequate understanding of security best practices is a major cause of cybersecurity risks. This frequently shows up as common errors like using weak or repetitive passwords for several online accounts, which makes it much easier for hackers to obtain user credentials. Additionally, a lot of people are duped by sophisticated phishing schemes that are spread by text messages, emails, or phony websites that are intended to steal private information, including financial information. Social engineering attacks, in which cybercriminals expertly use psychological tricks to trick people into disclosing private information under false pretenses, further increase their effectiveness.

**How Identity Guardian Addresses This Issue:**

By providing interactive cybersecurity tests and extensive learning materials created especially to help users recognize increasingly complex phishing attempts, greatly improve their password security practices by educating them on complexity and uniqueness, and successfully identify the manipulative techniques used in social engineering attacks, the Identity Guardian project directly addresses these issues. Additionally, users may practice safe online behaviors and decision-making in a controlled environment without the dangers associated with real-world cyber events thanks to the platform's immersive real-world threat simulations.

**Ineffective and Outdated Training Programs**

A persistent issue in the realm of cybersecurity education is the continued reliance by many organizations on traditional training methodologies. These often involve passive lectures and lengthy, often monotonous presentations that struggle to effectively engage learners and, consequently, result in knowledge that is quickly forgotten and rarely translated into practical behavioral changes.

**How Identity Guardian Enhances Learning:**

Identity Guardian carefully employs gamification strategies to get around these restrictions, making cybersecurity education more participatory, interesting, and ultimately pleasurable for users. Through the use of scenario-based learning, the platform immerses users in simulated cyber-attack situations, forcing them to make decisions in real time and watch the results of those actions firsthand in a secure virtual setting. Identity Guardian uses game-like components to further encourage and maintain participation, including leaderboards that promote healthy competition, material rewards for effective knowledge acquisition and application, and extensive progress tracking tools that support ongoing education and strengthen the gradual adoption of important security procedures.

**Increasing Complexity of Cyber Attacks**

The rising use of sophisticated AI-driven tactics by hackers to carry out highly targeted and deceitful cyberattacks greatly increases the evolving sophistication of cyberthreats. These include deepfake scams, in which victims are tricked into doing harmful things by using realistic voice recordings or AI-generated videos that convincingly mimic well-known people. Furthermore, both individuals and organizations are at serious risk from targeted ransomware attacks, which entail denying users access to their important data and requesting large ransom payments to restore it. Additionally, a common strategy that allows unwanted access to private user accounts and data is credential harvesting, which is accomplished by building complex phony login websites.

**How Identity Guardian Helps Combat These Threats:**

By exposing users to real-time cybersecurity threat simulations that faithfully replicate changing attack tactics, Identity Guardian directly addresses these more sophisticated threats and proactively prepares users for the possibility of running into such situations in the real world. Users may stay updated about the most recent attack patterns and upcoming dangers by using the platform's insightful blog material and frequent, up-to-date cybersecurity news updates. Importantly, Identity Guardian provides interactive incident response training modules that promote practical experience, giving users the tools they need to identify, lessen the effects of, and react to cyberattacks when they happen.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305168

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

**Reactive Rather Than Proactive Security Approaches**

The propensity to adopt security measures only after a security breach occurs, as opposed to proactively putting preventative protection measures in place, is a key risk seen in many people and enterprises. Common mistakes that lead to this reactive posture include not enabling multi-factor authentication (MFA) on online accounts, which makes them much more vulnerable to unauthorized access attempts, and postponing important software updates, which exposes systems needlessly to known and exploitable vulnerabilities. Additionally, when cyber threats do arise, inadequate incident response training frequently results in inefficient and delayed treatment, which increases the potential damage.

**How Identity Guardian Encourages Proactive Security:**

By immersing users in authentic real-world situations and posing useful challenges that reinforce safe behaviors, Identity Guardian actively promotes the development of proactive security habits. The platform offers concise and practical step-by-step security instructions aimed at enhancing online safety. These instructions cover crucial procedures like correctly configuring and using multi-factor authentication, identifying suspicious online activity, and putting strong secure data management plans into place. Moreover, Identity Guardian contains practice-based cybersecurity challenges that allow users to actively implement learnt security procedures in simulated situations, so cultivating a proactive and preventative security attitude rather than a reactive one.

## V. HOW IDENTITY GUARDIAN HELPS USER

The Identity Guardian initiative is designed to empower users with the knowledge and skills required to combat cybersecurity threats. Key benefits of the project include:

**Enhanced Awareness:** The simulator game educates users about various cyber threats and prevention strategies.

**Improved Decision-Making:** Users learn to recognize and respond to cyber threats effectively.

**Practical Training:** The interactive nature of the game allows users to practice cybersecurity measures in a safe environment.

**Increased Organizational Security:** Businesses can leverage the game to train employees and strengthen overall security posture.

By fostering a culture of cybersecurity awareness, Identity Guardian contributes to a more secure digital ecosystem.

## VI. PREVENTIVE MEASURES AGAINST CYBER ATTACK

The recommended actions are intended to greatly increase college students' understanding of cybersecurity and successfully reduce the danger of cyberattacks, taking into account their increased susceptibility in the digital world. This may be done through many main measures: Enabling multifactor authentication on all available accounts to provide a crucial additional security layer that significantly strengthens account protection even in the event that a password is compromised; installing and diligently maintaining protective software with routine scans and regular virus definition updates; and making sure that all operating systems, software applications, and passwords are consistently changed to strong, complex passwords that incorporate a mix of character types and memorable techniques and antivirus software is often updated to fix known flaws; putting strict physical security measures in place for devices, such as making sure they are never left unattended or logged on in unprotected public areas, constantly logging out of accounts, and closely monitoring system access; using the internet and email in a safe manner by avoiding unsolicited emails, being extremely cautious when clicking on attachments, links, and forms from dubious or untrusted sources, staying away from dubious downloads, and always considering the situation carefully before clicking, as most cyberattacks start with phishing emails; employing secure remote connectivity and file transfer options when off-campus, turning off unused services, changing default passwords, and properly configuring security settings, as well as giving security top priority when setting up systems and applications; implementing regular backup processes to secure vital work and private documents in a safe place, avoiding the loss of important information in the case of an assault; putting network segmentation into practice to prevent unwanted access and lessen the possible harm from a hack; making use of the desktop firewalls that come with both Macintosh and Windows computers, making sure that they are set up properly to stop illegal file scanning.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305168

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

**The Role of Digital Media (Blogs) in Cybersecurity Awareness**

Digital media, especially cybersecurity blogs and larger awareness campaigns, play a crucial and complementary role in the widespread dissemination of critical cybersecurity knowledge, even though gamification greatly improves interactive learning experiences in cybersecurity education. As real-time information centers, cybersecurity blogs offer immediate updates on the constantly changing world of cyberthreats, new attack patterns, and practical mitigation techniques that both people and companies may implement. However, Paper 6 wisely points out a number of significant drawbacks to using blogs alone as the main tool for raising awareness of cybersecurity. One of these issues is the possibility of information overload, which can arise from the sheer number of cybersecurity blogs and news articles on the internet. This can make it challenging for consumers to identify trustworthy and dependable sources. Furthermore, blogs usually provide passive learning experiences, which may result in poorer information retention rates among readers than the active involvement promoted by gamification.

## VII. CONCLUSION

In an era marked by fast digital transformation, the constant and growing nature of cybersecurity threats targeting individuals, businesses, and whole sectors needs a paradigm shift in how we approach security education. The "Identity Guardian" project presents a thorough cybersecurity awareness framework in recognition of the shortcomings of conventional, frequently passive security training techniques like workshops and static awareness campaigns in providing users with the necessary tools to identify, address, and lessen cyberthreats. This unique strategy deliberately blends the engaging power of gamification, the practical experience of real-world simulations, and the rapid information transmission of digital media. Cybersecurity awareness initiatives must go beyond passive learning by putting users in realistic situations, posing interesting problems, and encouraging decision-based learning settings if they are to genuinely empower users.

because studies constantly show that using such interactive techniques results in noticeably better rates of engagement and retention. A key component of this change is gamification, which provides users with simulated cyberattack experiences that provide them firsthand knowledge about the strategies used by cybercriminals.

## VIII. FUTURE DIRECTIONS

The Need for Ongoing Innovation Static training approaches will become outdated due to the ongoing evolution of cyber threats. Adaptive learning systems that tailor training according to user behavior, risk exposure, and changing threat landscapes are essential for raising cybersecurity awareness in the future. Intelligent cybersecurity assistants, real-time risk assessment tools, and AI-driven awareness platforms may all improve user readiness. The "Identity Guardian" initiative establishes the groundwork for a cybersecurity awareness framework that is more dynamic, captivating, and successful. Businesses and people may greatly improve their cyber resilience, lower human vulnerabilities, and keep one step ahead of cybercriminals by adopting gamification, digital media, and real-world simulations.

## IX. FINAL THOUGHT

Nowadays, cybersecurity is a shared responsibility rather than just an IT issue. Securing the digital world requires funding creative, interactive, and adaptable awareness campaigns. We can build a security-conscious society that is prepared to face the always evolving cyber threat landscape by fusing the power of gamification, digital learning, and continuous education. In summary, this study highlights a basic reality: cybersecurity in the connected world of today goes beyond the confines of a strictly technical field and firmly establishes itself as a shared responsibility that necessitates proactive participation from all digital citizens and group efforts. The results clearly support a large and deliberate investment in the creation and deployment of dynamic, interactive, and flexible cybersecurity education initiatives as a vital component for successfully safeguarding our increasingly digital world. By strategically harnessing the engaging power of gamification to immerse users in realistic threat scenarios, leveraging the broad reach and timely information delivery of digital learning platforms to disseminate crucial knowledge, and fostering a culture of continuous education that emphasizes lifelong learning and adaptation to the evolving threat landscape, we can collectively strive to cultivate a security-aware society. Such a society will be significantly more robust and able to proactively handle the constantly expanding and increasingly complex cyber threat landscape that pervades our personal and professional life if it is endowed with the requisite information, abilities, and mentality. This all-

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

encompassing and proactive approach to cybersecurity awareness goes beyond simple prevention; it is a foundational investment in building a more secure, resilient, and trustworthy digital future for all stakeholders.

## REFERENCES

1. Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 65-88.
2. Alexei, L. A. (2021). Network security threats to higher education institutions. In Central and Eastern European eDem and eGov Days (pp. 323-333).
3. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189.
4. Fadi A. Aloul, "The Need for Effective Information Security Awareness," Journal of Advances in Information Technology, Vol. 3, No. 3, pp. 176-183, August, 2012.doi:10.4304/jait.3.3.176-183 institutions. Information, 13(4), 192.
5. Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In 2015 IEEE 2nd international conference on cyber security and cloud computing (pp. 307-311). IEEE.
6. Chivukula, R., Lakshmi, T. J., Kandula, L. R. R., & Alla, K. (2021, November). A Study of Cyber Security Issues and Challenges. In 2021 IEEE Bombay Section Signature Conference (IBSSC) (pp. 1-5). IEEE.
7. Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), 192.Bulgurcu, B., Cavusoglu, H., &Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details