Karan Sharma

Gamification based cybersecurity training in higher institutions: an analysis of Delhi University

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

5 May 2025

Abstract

Author:	Karan Sharma
Title:	Gamification based cybersecurity training in higher institutions: an analysis of Delhi University
Number of Pages:	64 + 16 appendices
Date:	5 May 2025
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Networking and Services
Supervisors:	Chau Truong Minh, Lecturer

Cybersecurity challenges are particularly relevant for higher education institutions, which maintain large quantities of sensitive information. Although organizations deploy numerous security controls, the human error aspect leaves them open to attacks such as phishing, using weak passwords and failing to comply with the organization's security policy. Most cybersecurity training programs today take a passive, very technical approach that fails to create long-lasting changes in behavior. Traditional means, such as lectures or videos, do not excite students and faculty, leading to low retention of cybersecurity best practices.

This concludes with the Design of an Interactive Cybersecurity Training Guidelines, which combines gamification, real-world simulation-led learning, and behavior reinforcement to improve engagement and compliance. This research will use a mixed-methods research approach, including surveys to compare traditional interactive cybersecurity education. The research will also evaluate obstacles to the adoption of corporate policies and initiatives, as well as discuss how to integrate cyber hygiene into academic coursework.

The resulting outcome will be a scalable, curriculum-integrated guideline that increases cybersecurity content retention, empowers institutional policy adherence, and reduces human-error-based cyber risks. To the best of the knowledge, this is the first research showing an increase in security training and security culture in higher education that empowers students and faculty to combat poor security practices.

Keywords: Cybersecurity training, higher education, gamification, interactive learning, phishing awareness, cyber hygiene,

security policy compliance, behavior reinforcement, simulation-based learning, human error, cybersecurity education, institutional security policies, mixed-method research, security culture, curriculum integration.

The originality of this thesis has been checked using Turnitin Originality Check service.

Table of Contents

List of Abbreviations

Abbreviation	Full Form
AI	Artificial Intelligence
CTF	Capture The Flag
DU	Delhi University
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
ICT	Information and Communication Technology
IoT	Internet of Things
MFA	Multi-Factor Authentication
ML	Machine Learning
NIST	National Institute of Standards and Technology

PhD	Doctor of Philosophy
PII	Personally Identifiable Information
SME	Subject Matter Expert
SQL	Structured Query Language
TFA	Two-Factor Authentication
VPN	Virtual Private Network
VR	Virtual Reality
UX	User Experience
UI	User Interface

1 Introduction

1.1 Background and context:

Emerging cyber threats and attacks targeting higher education institutions are on the rise due to the open-access environment, large amounts of data across universities, and the varied levels of cybersecurity training among the people they host (students, faculty, and staff). Despite substantial investment in technological defenses, human factors continue to be a weakness. According to studies, security breaches, phishing attacks, and data leaks related to academia are often attributed to poor cybersecurity habits, low training levels, and lack of engagement in annual training[8]. Standard cybersecurity training is primarily technical, focused on tasks like detecting malware or managing passwords, disregarding behavior and motivation[6]. As traditional approaches, such as lectures, policy documents, and passive online training modules, are not interactive, these methods fail to engage the audience, leading to low retention and compliance[3].

Since there are growing threats in cyberspace, and significant weaknesses in digital defense, cybersecurity training at Indian universities, including for students of Delhi University, is the need of the hour. Most current standard training programs do not have engagement and retention strategies. Delhi University: A premier institution offering programs such as computer science, information security, and digital forensics, is also engaged in teaching cybersecurity. Undergraduate and postgraduate courses at the university include network security, ethical hacking, cryptography, and risk management. Yet, current cybersecurity training is largely based on old, passive methodologies such as lectures and written policy documents, rather than an interactive, engagement-driven experience.

"This research investigates the current level of cybersecurity awareness and explores the use of gamification and simulation-based training as an alternative to traditional training methodologies to strengthen cybersecurity awareness, policy compliance, and hands-on skill development.

1.2 Problem statement:

Despite existing cybersecurity training programs, faculty and students continue to engage in risky practices, leading to non-compliance with security policies and increased vulnerability to data breaches. A key issue is the lack of data management skills and engaging, experiential learning methods that reinforce security training effectively. This research aims to address these challenges by developing a curriculum-integrated guidelines that balances technical knowledge with behavioral conditioning to improve cybersecurity awareness and compliance.

1.3 Research aim and scope:

The research presents a conceptual design of a gamified, simulation-based interactive cybersecurity training Guidelines for higher educational institutions, integrating stimulation- and behavior reinforcements. The research will compare the effectiveness of traditional training methods against interactive learning strategies, assess adoption rates of cybersecurity policies, and suggest methods for embedding training in academic curricula.

1.4 Research objectives:

- Assess cybersecurity training levels among students and faculty.
- Understand how to motivate and increase the participation of students and staff.
- Investigate the impact of gamification and interactive learning on engagement and retention.
- Understand how the cybersecurity policy is applied/aligned in training programs.
- Develop a curriculum-integrated cybersecurity training Guidelines for higher education institutions.

1.5 Research questions:

- How effective is current cybersecurity training at Delhi University?

- Can gamification-based approaches improve student engagement and policy compliance?
- What curriculum improvements can enhance cybersecurity education?

2 Literature review

2.1 Human factors in cybersecurity

According to Miranda et al, 2018, the protection of information security within academic institutions functions as a top priority because these organizations manage many different sensitive data types. Higher education institutions maintain student and faculty personal data, together with monetary information and scholarly research, which makes them highly attractive to cybercriminals. Institutions spend significant funds on cybersecurity technology, but human factors continue to represent the main security weakness. This part investigates why human mistakes and insufficient cybersecurity understanding, and inadequate training methods, together with institutional enforcement barriers, lead to cybersecurity policy compliance difficulties.

2.1.1 The role of human error in cybersecurity breaches:

2.1.2 Common human errors leading to cybersecurity breaches:

As per the opinion of Zhang et al, 2021, A major percentage of cybersecurity incidents that target higher education institutions stem from human-related mistakes. A recent research study has established that human error behind successful cyberattacks exceeds 90% because people need better security awareness and behavior practices to protect themselves.

2.1.3 Common errors contributing to these breaches include:

According to Alruwaili et al, 2019, Users who create passwords which are simple to guess through the use of "123456" or "password" expose themselves to

unauthorized access attempts from attackers. Multiple account access becomes more vulnerable when users select the same password for all their accounts.

Failure to recognize phishing attacks: Cybercriminals utilize phishing attacks as their most successful social engineering strategy because many users fail to detect them. The impersonation of university emails sent through phishing causes students and faculty members to lose their credentials or fall prey to malware infections.

Unsecured devices and networks: The practice of students and faculty connecting to unsecured public Wi-Fi networks exposes them to man-in-the-middle attacks because they do not use VPNs or similar security measures. Data breaches become more likely when people operate their devices with security software that is out of date.

Neglecting software updates and security patches: Outdated software without proper update maintenance serves as an entry point for unauthorized cybercriminals through known system vulnerabilities. Security problems occur because numerous university staff members and students avoid installing critical security updates, which results in systems becoming accessible to attackers who launch ransomware attacks.

One of the examples is the case of University of California phishing attack:

In 2020 the University of California San Francisco (UCSF) became a victim of ransomware which required them to pay $1.14 million to the attackers. The attack was initiated through a phishing email that tricked an employee into clicking a malicious link, granting hackers access to critical systems. This case highlights the direct impact of human error on cybersecurity and the importance of robust awareness programs.

2.2 Low awareness and training effectiveness:

2.2.1 Cybersecurity awareness gaps in higher education:

According to Chen, 2023, despite the increasing number of cyber threats, many university students and staff remain unaware of basic cybersecurity best practices. Studies have shown that a significant percentage of students (over

60%) reuse passwords, while 30% admit to clicking on suspicious links in emails without verifying their legitimacy. This lack of awareness directly contributes to the frequency of successful cyberattacks on educational institutions.

Several factors contribute to low cybersecurity awareness among students and faculty, including:

Lack of formal cybersecurity education: Most educational institutions fail to instruct students about cybersecurity basics through their standard curriculum, which results in students understanding very few cyber risks.

Overconfidence in institutional security measures: Some members of the university community incorrectly believe that the IT department should handle all security responsibilities which causes them to neglect their personal responsibility for safe online conduct.

Rapid technological changes: The quick development of cyber security threats creates difficulties for universities when they attempt to maintain updated training programs.

Ineffectiveness of traditional cybersecurity training: The cybersecurity training initiatives at numerous universities prove insufficient in achieving their intended results. The traditional training methods primarily use static educational content such as video lectures and PowerPoint slides and written guides, without effectively retaining student attention.

2.2.2 Key limitations of these training methods include:

According to Thomas et al, 2013, Security policies that require passive reading do not create effective cybersecurity behaviors because of low engagement.

One-Time training approach: Universities deliver their cybersecurity training only at the beginning of student and employee admissions, before discontinuing further sessions. The lack of follow-up training leads to gradual forgetting of essential security practices by users.

No real-world application: Real-world learning scenarios are absent from most training programs because they lack practical simulations which hinders individuals from implementing classroom concepts outside the classroom.

An example how to overcome these limitations is MIT’s Cybersecurity Awareness Initiative:

To combat low cybersecurity awareness, Massachusetts Institute of Technology (MIT) launched an interactive cybersecurity awareness program incorporating gamification, phishing simulations, and real-time feedback mechanisms. The program resulted in a 40% reduction in phishing attack success rates among students and staff, demonstrating the effectiveness of interactive learning techniques.

2.3 Institutional challenges in enforcing cybersecurity policies:

2.3.1 Difficulties in policy implementation:

According to Liu et al, 2021, Many students, together with faculty members, show resistance to following cybersecurity policies because they see these rules as protective measures rather than protective ones thus, they deliberately break them.

- **Resistance to compliance**: The security guidelines that universities distribute tend to remain unclear because their policy documents become too lengthy and complex.
- **Lack of clarity in cybersecurity guidelines:** Some educational institutions face resource limitations because they do not have enough budget or staff to establish strong security programs.
- **Resource constraints:** Some educational institutions face problems with limited resources that prevent them from implementing strong security programs.
- The implementation of inadequate cybersecurity culture enforcement leads to various negative consequences.
- Universities that do not enforce cybersecurity policies effectively expose themselves to growing threats from cyberattacks. Poor enforcement leads to:
- **Increased data breaches:** Students and faculty members can perform dangerous online activities because weak security policy enforcement leads to higher data breaches.

- **Financial losses:** University cyberattacks produce major financial losses because institutions pay ransomware ransoms and must spend money to recover data and face legal penalties.
- **Damage to institutional reputation:** An educational institution that experiences frequent cyber incidents faces severe damage to its institutional reputation because it loses trust from students along with faculty members, and all other stakeholders.

2.3.2 To address enforcement challenges, universities can adopt several strategies:

According to Karpiuk, 2018, integrate cybersecurity awareness into academic programs: Embedding cybersecurity courses into general education curricula ensures all students develop essential security skills.

- Implement a zero-trust security model: A zero-trust security model should be implemented because it limits data access through secure identity controls that track user activities across specific locations.
- Introduce role-based security training: The university should deliver security education specifically designed for each university role, starting from faculty members and IT staff, and students, to improve policy compliance.

Regular security audits and penetration testing: Conducting frequent security assessments can help institutions identify and address vulnerabilities proactively.

Example: University of Cambridge's Security Policy Revamp

According to Azıonya and Nhedzı, 2022, the University of Cambridge revamped its cybersecurity policies by introducing role-specific security training and enforcing multi-factor authentication (MFA) across all university accounts. These measures led to a 75% reduction in unauthorized account access within a year, showcasing the effectiveness of structured policy implementation.

2.4 Current training approaches and their limitations:

2.4.1 Traditional cybersecurity training methods

According to Czuryk, 2022, higher education institutions have implemented various cybersecurity training methods to equip students and faculty with essential knowledge to mitigate cyber threats. Most universities rely on conventional training methods such as lectures, informational videos, and written policy documents to educate users about cybersecurity risks and best practices. These training programs typically introduce fundamental cybersecurity concepts, such as password management, phishing awareness, and software updates, to foster a security-conscious culture within the institution.

The security training starting points set by these methods are insufficient because they fail in meaningful engagement or training application. Instructional materials alongside lectures deliver general security information without acknowledging distinct security issues that students and faculty members need to handle. Institutions that conduct cybersecurity training as a single event instead of a sustained education experience reduce effectiveness because of this approach.

The implementation of traditional training methods remains a challenge for universities that aim to fulfil their cybersecurity education guidelines. The poor knowledge retention and ineffective security practice implementation stems from the low level of engagement among faculty members and students with these programs. Traditional training models frequently deprive students and professors of necessary content updates because cyber threats continue to change at a rapid pace.

2.4.2 Challenges of passive learning

As per the review of Gwenhure and Rahayu, 2024, Traditional cybersecurity training faces its main challenge because it depends on passive learning methods as its primary approach. The learning approach of passive methods delivers information to students who remain inactive throughout the educational process. Security policies for reading and pre-recorded training videos,s together with

large-scale lectures that lack student interaction, exemplify traditional training methods.

Multiple studies have proven that passive learning approaches deliver much lower results than active learning techniques when it comes to sustaining permanent behavior modifications. The majority of people lose important cybersecurity information within a short time following their training thus creating a recurring pattern of security failures. Students together with faculty find it difficult to identify actual cyber threats while also failing to implement protective measures for university data through training programs that focus on passive learning methods.

The main disadvantage of passive learning occurs through its inability to provide customized interaction with learners. Security policies along with training resources adopt generic standards that overlook the distinct skill levels and technological competencies of the university community members. Less security-knowledgeable faculty members need interactive educational content that helps them learn basic cybersecurity principles, while technologically adept students find traditional training methods uninteresting. Training content that fails to match the user experience minimizes the performance of passive learning methods.

The presentation of cybersecurity concepts through static training formats becomes challenging because these concepts tend to be complex. The principles of information security need continuous support because they contain complex technical language alongside multiple security threats that evolve yearly. The limitations of passive teaching approaches make it impossible to properly address all complexities, thus leading to basic comprehension rather than functional skills learning.

2.4.3 Lack of hands-on experience

According to Chowdhury, 2022, Multiple university cybersecurity training curriculums suffer from an essential deficiency because they lack practical application elements. Theoretical knowledge training approaches neglect to

expose students or faculty members to practical experiences with contemporary cyber security threats that prevent them from converting basic cybersecurity principles into concrete security behavior.

Cybersecurity training requires hands-on experience because it gives participants the opportunity to handle simulated threats within a controlled simulation environment. Through interactive cybersecurity training models which include cybersecurity labs and both virtual simulations and gamified learning modules users can develop real-time response abilities toward cyber threats. Many universities lack proper inclusion of experiential learning approaches in their training programs which results in students and faculty members being unready to confront cyber risks during actual practice.

The lack of hands-on training stems from the expensive nature which characterizes interactive cybersecurity education. The establishment and operation of cybersecurity laboratories and simulated phishing tests and practical security evaluation systems demand substantial technological infrastructure together with skilled personnel. Higher education institutions generally do not possess enough financial support and technical abilities to establish interactive training elements thus they maintain outdated passive learning methods.

The importance of contextual learning receives insufficient recognition from many universities when it comes to cybersecurity education. The way cyber threats display depends on which digital setting users interact with. Security threats experienced by university faculty who access research data through university servers differ from the risks students encounter while using public Wi-Fi networks. When hands-on training does not target specific user contexts these different contexts maintain their separation from practical cybersecurity implementation.

2.4.4 Ineffectiveness of one-time training models

According to Alnajim et al, 2023, The current cybersecurity training systems in universities face limitations because educators view cybersecurity education as a singular event instead of continuous learning. Universities and colleges

mandate that new students and employees to perform one cybersecurity training session when they start, but they do not supply additional training during their educational or professional period.

Multiple issues arise because of this method. Individuals must follow current cybersecurity threats because they develop at a fast pace, in addition to requiring knowledge of the latest protection methods and attack techniques. A single training session provides fundamental cybersecurity education, although it fails to develop user abilities to address new security threats. When reinforcement stops, individuals tend to return to their risky cyber behaviors in the future.

The development of secure behaviors through cybersecurity requires regular repetition and ongoing reinforcement for users to transform them into automatic actions. The research indicates periodic training and routine reminders increase human adoption rates of secure practices. Repetitive phishing simulation exercises help users learn to identify fake emails so they can appropriately report them which decreases the success rate of phishing attempts. College institutions using a training approach limited to a single event prevent themselves from developing an environment of continuous cybersecurity education and practical experience.

University members with different cybersecurity expertise levels are not adequately supported by training approaches that only provide one-time sessions. Students who are new to the university, along with faculty members, might not have basic cybersecurity training experience, yet some staff already possess this knowledge. Universities lack flexibility in cybersecurity training since one session cannot adapt to different professional levels, which results in inconsistent security preparedness among staff members.

2.4.5 Overlooking behavioural and psychological factors

According to Mittal, 2021, the effectiveness of cybersecurity training requires attention to both technical skills and behavioral attributes that control digital environment choices of users. Universities currently implement training methods that neglect essential human behavior aspects, resulting in minimal success in modifying user conduct.

The decision-making process in cybersecurity heavily relies on how cognitive biases influence the choices of users. Most people display optimism bias through their belief that cybercriminals would not target them personally. People who hold this assumption often become careless about following security best practices and they stop taking necessary precautions. Traditional training programs that focus solely on technical knowledge fail to address these behavioral tendencies, making it difficult to achieve lasting behavioral change.

The current cybersecurity training programs fail to consider the social and cultural elements which affect security practices in higher education institutions. The approach to cybersecurity from students and faculty members gets affected by peer influence and institutional norms and the availability of time. The absence of underlying factor consideration in cybersecurity training makes programs non-substantial for genuine, real-world security decision processes.

2.4.6 Lack of institutional support and reinforcement

As per the opinion of Rizvi and Nabi, 2021, Cybersecurity training by itself proves insufficient to create effective security practices because institutions need to combine training with formal policies and leadership backing, as well as an organizational focus on security education. University institutions face difficulties in establishing proper institutional support for cybersecurity training programs.

University leaders should communicate effectively with their constituents about cybersecurity yet most institutions fail to do so properly. Students and faculty members tend to dismiss security measures when they view cybersecurity training as a bureaucratic obligation rather than an essential institutional commitment. Higher education institutions that neglect cybersecurity in their complete risk management framework develop spaces where cybersecurity training becomes voluntary instead of mandatory.

Many educational institutions lack adequate systems that both motivate their personnel and hold them responsible for following recommended cybersecurity standards. Both faculty members and students tend to focus their activities on research and teaching rather than cybersecurity education, while they consider

security protocols cumbersome to their work routines. Secure behaviour engagement stays low because students receive neither penalties nor benefits for their actions during cybersecurity training sessions.

Universities must establish a complete cybersecurity training method which combines interactive educational approaches with continuous learning and behavioral analysis and institutional backing. Educational institutions will reduce their security vulnerabilities effectively when they commit to implementing dynamic hands-on cybersecurity training beyond passive one-time training sessions and systems.

2.5 Gamification and interactive approaches in cybersecurity training:

2.5.1 Introduction to gamification in cybersecurity training

According to Saeed and Masters, 2021, the educational field of cybersecurity makes use of gamification to create an innovative retention and engagement solution for students and faculty members. The standard training procedures depend on passive learning approaches, which include policy document reading and video viewing, and classroom attendance. These educational methods establish essential learning but deliver limited retention among students because they fail both in keeping students engaged and in changing long-term behavior patterns. Security education through gamification incorporates gameplay aspects of scores and badges alongside competitive leaderboards and interactive training simulations, which gradually converts training into an absorbed and interesting educational journey.

The core idea behind gamification uses gaming motivational elements to stimulate participant engagement. Studies prove that learners accept and keep information better when they study in opposing learning situations or earn prizes. The training system for cybersecurity education includes challenging material that demands thorough knowledge about security dangers and weak points plus defense approaches. Through gamification technologies information becomes easier to understand because learners can interact with security principles through real-world simulations.

The implementation of gamification systems helps students develop active security practices in addition to their motivational effects. Users receive security threat education through traditional training only after incidents have taken place. Gamification systems enable learners to develop skills which allow them to prevent cyber threats from occurring. Electronic training systems which present students and faculty to virtual cyberattack simulations develop security-oriented approaches through interactive training programs that emphasize constant protection measures.

2.5.2 Enhancing cybersecurity training through interactive methods

According to Raffiotta, 2022, interactive learning through physical collaboration paired with real-time assessment supports gamification as it helps learners keep information and develop their abilities. The training method uses interactive approaches because it requires learners to actively work with cybersecurity tools and attack simulations, and problem-solving tasks. The method proves highly successful for cybersecurity education because theoretical information by itself fails to teach students sufficient skills to confront actual security challenges.

Through interactive learning, students and faculty members can build their critical thinking and decision-making abilities through the handling of simulated cyber incidents. The cybersecurity domain demands immediate response along with flexibility since its threats undergo continuous changes. Students can use cybersecurity labs together with CTF competitions and simulation-based exercises as interactive training tools that help them practice secure principles in actively managed environments. The hands-on training generates better comprehension and develops users' capabilities to detect and protect against actual cyber threats.

The primary benefit of interactive learning consists of instant feedback delivery. Current security educational training systems fail to deliver real-time evaluation tools that would help students evaluate their learning progress related to security principles. The instant feedback capabilities of interactive systems help users inspect their security choices, making it possible for them to derive learning benefits from their errors. Security education programs at universities reach

higher effectiveness levels when interactive training features are implemented, which creates opportunities for students to learn continuously.

2.5.3 Real-world applications of gamification in cybersecurity training

According to Ulven, 2023, Different educational institutions and organizations have implemented gamified training models with interactive learning methods for cybersecurity education. Educational institutions, together with cybersecurity companies, have produced gamified training systems to improve the security knowledge and abilities of their users.

A prime illustration is the SCORPION Cyber Range, which functions as a gamified cybersecurity platform that provides players with interactive exercises while allowing real-time challenge and progress tracking capabilities. The platform allows students and professionals to conduct authentic cyberattack simulations, which helps them master practical cybersecurity skills. The SCORPION Cyber Range delivers a programmed educational pathway that permits users to move from simple to advanced levels while receiving acknowledgments for their accomplishments. Through its replication of real cybersecurity threats, the platform prepares students for professional security incidents.

The application of serious games which duplicate cyberattack scenarios represents a successful gamification approach in cybersecurity training programs. These educational games provide users with interactive simulations which challenge them to solve security problems in real time. The simulation-based game presents participants with the task of detecting phishing emails inside a secure training domain. Experiential learning through these scenarios helps users build natural understanding about cybersecurity risks which improves their identification of threatening situations.

Universities across the nation have started integrating CTF competitions into their cybersecurity curriculum as standalone educational platforms. CTF competitions present participants with the task of resolving cybersecurity puzzles while they

must discover system vulnerabilities and protect virtual environments from security attacks. Educational competitions offer students a dynamic environment to evaluate their cybersecurity competencies through high-pressure situations. CTF competitions play an essential role in helping cybersecurity professionals reach their field expertise according to many professionals in the field.

IBM and Google alongside other entities have developed gaming-based cybersecurity training platforms to boost employee security mindfulness. The IBM Cybersecurity Escape Room provides participants with an interactive scenario where they join forces to recognize security vulnerabilities along with implementing defensive countermeasures in a simulated cyberattack situation. Organizations benefit from team-based training because it develops essential skills of collaboration and critical thinking for cybersecurity defence.

2.5.4 Advantages of gamified and simulation-based training

According to Jamil et al, 2021, gamification and simulation-based cybersecurity training offer numerous advantages over traditional learning methods. The main advantage of this approach consists of higher motivation and stronger student involvement. Conventional cybersecurity education is typically viewed as dull by students, which produces minimal class participation alongside poor memory retention of taught information. The learning process becomes more exciting through gamification because it includes competitive elements as well as rewards and advancement features. Security concepts become more accessible to learners as they maintain active engagement during the learning process.

The main benefit of gamified training includes behavior reinforcement through continuous exposure and practice of cybersecurity principles. Theoretical education of cybersecurity principles alone does not lead to substantial behavioral change in students. Through gamification, users can perform security-related tasks multiple times which including phishing email identification and secure password configuration and simulated cyber incident responses. By providing ongoing practice, the system strengthens secure behaviours while making human-error-based security breaches less likely to occur.

Software simulation systems help users acquire better decision-making abilities through authentic security situations. Cyberattacks frequently develop without warning so people must use critical thinking abilities to respond swiftly in urgent situations. Students and faculty members who take part in virtual cyberattacks gain essential problem-solving abilities needed to handle security threats more effectively. Through simulation training, participants can test various security techniques in a protected virtual setting, thus gaining insight into how their actions affect results, but without actual consequences.

Gamified cybersecurity training proves valuable because it adjusts its presentation based on multiple learning approaches. The standard training approaches tend to implement identical methods for all students although these methods do not work well with diverse learners. People have different learning preferences between hands-on work and visual and competitive training approaches. The learning Guidelines of gamification adapt to multiple learning preferences which enables participants to select educational methods that best fit their individual needs.

Beyond individual learning benefits, gamification also fosters a culture of cybersecurity awareness at an institutional level. When cybersecurity training is engaging and interactive, it encourages a broader adoption of security best practices across the university community. Faculty members and students who actively participate in gamified training programs are more likely to share their knowledge with peers, creating a ripple effect that strengthens the institution's overall cybersecurity posture.

2.6 Gaps in existing research:

2.6.1 Limited empirical evidence on long-term effectiveness

According to Shillair et al, 2023, despite the increasing adoption of gamified cybersecurity training and interactive learning approaches, there remains a significant gap in empirical research assessing their long-term effectiveness. Many studies demonstrate the short-term benefits of gamification, such as

increased engagement, motivation, and knowledge retention. However, research evaluating whether these improvements persist over time remains limited.

The duration of behavioral changes in security practices among students and faculty members following gamified cybersecurity training remains uncertain because data shows these behaviors might not persist beyond the short-term. The discipline of cybersecurity changes over time because new security threats persistently appear. The lack of enduring behavioral changes from training programs will maintain existing vulnerabilities derived from human mistakes throughout institutions.

Moreover, the lack of longitudinal studies assessing the impact of gamification and interactive learning limits the ability to measure the real-world effectiveness of such approaches. Most available research focuses on immediate post-training assessments rather than tracking participants over extended periods. Without robust, long-term studies, educational institutions cannot determine whether gamified learning translates into sustainable improvements in cybersecurity behaviors.

Another concern is whether gamification creates a genuine understanding of cybersecurity principles or merely encourages participants to focus on achieving high scores or completing challenges. Some critics argue that gamification, if not carefully designed, can lead to superficial engagement, where learners prioritize winning over internalizing fundamental cybersecurity concepts. Therefore, additional research is required to determine how gamification can be structured to ensure both engagement and deep learning, leading to a sustained cybersecurity culture.

2.6.2 Focus on technical students rather than broader university populations

As per the opinion of El-Bably et al, 2023, most existing cybersecurity training programs target IT and computer science students, assuming they are the primary stakeholders responsible for managing and mitigating cyber threats. While it is true that IT professionals play a crucial role in securing institutional systems, cybersecurity is not solely the responsibility of technical experts. Non-

technical students, faculty members, administrative staff, and researchers also interact with institutional networks and handle sensitive data, making them potential entry points for cyberattacks.

Despite this, non-technical students and faculty often receive minimal cybersecurity training. Many universities offer specialized cybersecurity courses for IT students while neglecting to provide similar education for other disciplines. This approach creates a dangerous gap in cybersecurity preparedness. For instance, a humanities professor or a business student may inadvertently fall victim to phishing scams, ransomware attacks, or social engineering tactics simply due to a lack of awareness.

Moreover, some faculty members perceive cybersecurity training as irrelevant to their roles, further reducing engagement levels. Without comprehensive awareness programs tailored to various academic disciplines, universities risk leaving significant portions of their communities vulnerable to cyber threats. Expanding cybersecurity education beyond IT and computer science departments is essential to cultivating a strong cybersecurity culture across the entire institution.

2.6.3 The digital divide and accessibility challenges

The digital divide presents a crucial problem because it determines students' and faculty members' capability to access cybersecurity training materials. Most gamified training systems and interactive educational platforms need access to the internet and high-performance computing equipment and modern software applications. Students along with faculty members do not share equivalent access to these resources. The lack of dependable internet access and suitable personal computers becomes a barrier for students from disadvantaged backgrounds who want to participate in gamified training sessions.

Some faculty members who lack experience with digital tools encounter difficulties when using interactive learning platforms because of their unfamiliarity with these tools. Individuals with different abilities in digital literacy face higher chances of being excluded from obtaining essential cybersecurity information

through inadequate training programs. The practice of excluding users from cybersecurity preparedness leaves fields unprotected against potential security breaches resulting from their lack of knowledge.

Universities need to make gamified cybersecurity training programs available to every student and faculty member without considering their technical skills or financial situation. Universities can reduce digital disparities by offering training modules in both online and offline formats and providing text-based content as well as designing easy-to-use platforms.

2.6.4 Need for curriculum integration

The current cybersecurity training systems lack effectiveness because they do not bridge cybersecurity education into standard educational programs at educational institutions. Education institutions today deliver cybersecurity training separately from their core academic requirements even though they handle it as a standalone requirement.

For example, cybersecurity training in most institutions consists of one-time workshops, online courses, or informational sessions that students and faculty complete independently. While these programs may provide valuable insights, they are often treated as optional or non-essential. Without continuous reinforcement, students and faculty members quickly forget what they have learned, reducing the overall effectiveness of cybersecurity training.

By embedding cybersecurity education within academic curricula, universities can ensure that students encounter cybersecurity concepts regularly throughout their studies. For instance, business students can learn about cybersecurity risks in financial transactions, medical students can explore the importance of data privacy in healthcare, and engineering students can study secure software development practices. Integrating cybersecurity topics into existing coursework makes the learning experience more relevant, increasing the likelihood of long-term retention and application.

Furthermore, universities should consider making cybersecurity literacy a graduation requirement. Just as students must fulfil certain general education

requirements, they should also be required to complete cybersecurity training as part of their degree programs. This approach would ensure that all students, regardless of their field of study, develop a foundational understanding of cybersecurity principles before entering the workforce.

2.6.5 Insufficient customization and personalization of training programs

According to Catal et al, 2023, another major gap in existing research is the lack of personalized cybersecurity training programs. Many current training approaches adopt a one-size-fits-all model, assuming that all learners have the same level of cybersecurity knowledge and face identical threats. However, cybersecurity risks vary depending on an individual's role, responsibilities, and digital habits.

For example, a university professor handling confidential research data faces different cybersecurity threats than a first-year student primarily using institutional networks for coursework and social interactions. Similarly, administrative staff members who manage financial transactions must be trained on fraud prevention and secure payment processing techniques, whereas IT staff may require in-depth training on network security and system vulnerabilities.

Despite these differences, many universities provide uniform cybersecurity training to all users, failing to address their specific needs. This approach results in disengagement, as learners do not see the relevance of the training to their daily activities. Research is needed to develop adaptive learning models that tailor cybersecurity training to individual needs based on role, experience level, and risk exposure. Personalized training programs that adjust content based on user responses and learning progress can significantly improve engagement and retention.

2.6.6 Challenges in measuring the effectiveness of cybersecurity training

According to Chenet, 2021, a crucial gap in current research is the lack of standardized metrics to evaluate the effectiveness of cybersecurity training programs. Many universities implement cybersecurity training without clear

mechanisms to assess whether the training translates into improved security behaviors. While knowledge-based assessments such as quizzes and exams can measure theoretical understanding, they do not provide insights into whether learners apply cybersecurity best practices in real-world scenarios.

For instance, a student may perform well on a cybersecurity quiz but still engage in risky online behavior, such as clicking on phishing links or using weak passwords. Without behavioral assessments, universities cannot accurately determine whether training programs result in meaningful security improvements.

Research is needed to develop effective evaluation Guideliness that measure both knowledge acquisition and behavioral change. Potential assessment methods include simulated phishing attacks, real-world security exercises, and monitoring compliance with institutional cybersecurity policies. By incorporating behavioral assessments into cybersecurity training, universities can identify areas where additional intervention is needed and refine their training programs accordingly.

2.7 Summary of literature review

The current body of research on cybersecurity training highlights significant gaps that must be addressed to enhance the effectiveness of educational programs. While gamification and interactive learning show promise in improving engagement and retention, there is limited empirical evidence on their long-term impact. Additionally, cybersecurity training programs often prioritize technical students while neglecting broader university populations, leaving non-technical faculty and students vulnerable to cyber threats.

The digital divide presents another challenge, as not all students and faculty members have equal access to cybersecurity training resources. Furthermore, most universities fail to integrate cybersecurity education into their curricula, treating it as a separate, non-essential requirement rather than an integral part of academic learning.

Insufficient customization of training programs and the lack of standardized metrics to evaluate effectiveness further hinder the success of current

cybersecurity education initiatives. To address these gaps, universities must adopt a more inclusive, integrated, and personalized approach to cybersecurity training. Future research should focus on developing adaptive learning models, creating long-term evaluation guidelines and ensuring that cybersecurity education reaches all members of the academic community.

By addressing these research gaps, universities can build a stronger cybersecurity culture, reduce human-error-based security breaches, and better protect institutional data and digital assets

3 Current state analysis / Project specifications

3.1 Evaluation of existing cybersecurity training programs:

Most universities have cybersecurity training programs, but these are primarily passive—delivered through lectures, policy documents, and informational videos. These methods result in limited engagement, leading to low retention and minimal real-world application of security principles.

At Delhi University, cybersecurity-related courses are integrated into undergraduate and postgraduate programs in disciplines such as Computer Science, Information Security, and Digital Forensics. Courses include Network Security, Ethical Hacking, Cryptography, Risk Management, and Data Protection Regulations. However, despite covering technical aspects of cybersecurity, these courses primarily rely on traditional teaching methods such as theoretical lectures and written assignments, lacking interactive or experiential learning components. As a result, students often struggle to apply cybersecurity principles in practical scenarios.
Additionally, cybersecurity training at Delhi University is largely focused on technical students, while faculty members, administrative staff, and students from non-technical backgrounds receive minimal or no formal training. This creates a security gap, as cyber threats can target anyone with access to institutional networks and data (Draper et al, 2021).

3.2 Common challenges identified:

Countless cybersecurity training programs also fall flat, often due to low participation rates, lack of institutional support, and minimal real-world application. Cyber threats are underestimated by a large number of students and faculty, causing little interest. The adoption of interactive cybersecurity education models is also hampered by time constraints, a lack of resources, and poor enforcement of policy during a period of adaptation.

- Engagement Gap: One of the major disadvantages of traditional training is that it's boring.
- Confusing policy: Security policies are often as technical as they are opaque
- Users forget security protocols without periodic reinforcement.

3.3 Effect of the constitutional cybersecurity:

This helps to increase the cyber risk faced by higher education. A report[7] shows that these core vulnerabilities persist, with phishing and weak passwords and unpatched systems remaining leading causes. Cybersecurity training programs for institutions need to be engaging, interactive, and behavior-based to raise training and enhance compliance (Taherdoost, 2021). Universities with poor cybersecurity doubtlessly suffer from enhanced data breaches, terrorist attacks, burglaries, financial loss, and damage to their reputation. Undetailed training breeds bad password practices, inadvertent insider threats, and non-compliance initiatives. Implemented correctly, a robust cyber security system reduces risks due to human-error behavior, optimizes response time and strengthens institutional cyber resilience.

3.4 Selection of traditional and gamified cybersecurity training programs

3.4.1 Traditional cybersecurity course (Existing program at Delhi University)

Delhi University offers cybersecurity-related courses under Computer Science, Information Security, and Digital Forensics programs. Some of the core subjects include:

- Network Security – Covers firewall configurations, VPNs, and encryption techniques.
- Ethical Hacking – Focuses on penetration testing and vulnerability assessment strategies.
- Cryptography – Explores encryption methods and data protection principles.
- Risk Management – Discusses risk mitigation techniques and compliance policies.

However, these courses primarily rely on lecture-based delivery, policy documents, and theoretical assessments, offering limited hands-on engagement. The focus remains on technical knowledge rather than behavioural adaptation or real-world cybersecurity challenges.

3.4.2 Gamified cybersecurity course (Reference-based program)

Since Delhi University does not currently offer a fully gamified cybersecurity training program, this research draws upon the structure and delivery style of “TryHackMe”, a globally recognized interactive cybersecurity training platform. This course has been selected because it closely mirrors the core objectives of this study.

“TryHackMe” delivers cybersecurity concepts through gamified learning environments, enabling participants to earn points, badges, and unlock new training levels as they complete hands-on labs. It incorporates real-world scenarios, step-by-step guided exercises, and role-specific learning paths for students and professionals.

This course was chosen as a comparison model because:

- It emphasizes active learning through simulations, aligned to reinforce behavioral change.
- It maintains high engagement levels by incorporating competition and rewards.
- It allows flexible, modular learning, which is ideal for academic integration.

The platform serves as a benchmark for evaluating the effectiveness of gamified training approaches in enhancing cybersecurity awareness, practical skills, and compliance. By comparing participant responses from a traditional training program with those exposed to a TryHackMe-like experience, this study seeks to assess the benefits of gamification in cybersecurity training within higher education institutions.

3.4.3 Justification for the comparison

By comparing the traditional cybersecurity training approach with a gamified model, this research aims to assess:

- Engagement Levels – Does gamification increase student participation?
- Knowledge Retention – Are gamified concepts easier to recall than traditional training?
- Behavioral Change – Does interactive training encourage better cybersecurity habits?
- Policy Compliance – Are students more likely to follow institutional security policies after gamified training?

4 Methodology

This chapter outlines the research design, data collection methods, sampling strategy, data analysis techniques, and ethical considerations. The study aims to evaluate the effectiveness of cybersecurity training approaches in higher education institutions by comparing traditional training methods with a gamified cybersecurity training model (Quraishi et al, 2024). A mixed-methods approach is employed to analyze the impact of these training methods on student and faculty engagement, knowledge retention, and behavioral changes in cybersecurity practices.

4.1 Research design

The research compares conventional cybersecurity training—such as lecture-based learning, policy documents, and theoretical coursework—with interactive learning techniques, including gamification and simulation-based cybersecurity exercises.

A control group will undergo traditional cybersecurity training, while an experimental group will participate in a gamified cybersecurity training model. This design allows for a structured comparison by measuring changes in knowledge retention, engagement levels, and real-world application of

cybersecurity principles over a defined period. Two distinct participant groups will be used to facilitate this comparison:

- **Group 1 – Traditional training group:**

The conventional cybersecurity education which Delhi University delivers to students will be provided to participants in this group. Participants in this group receive lectures and static policy documents together with reading assignments and slide-based learning which lacks interactive elements and practical activities.

- **Group 2 – Gamified training group:**

The online gamified cybersecurity training through "TryHackMe" simulations will serve as the educational method for this participant group. The platform was chosen for this research because it aligns with all crucial goals by delivering practical hands-on scenarios that enhance motivation and knowledge retention while promoting policy compliance.

Justification for using the online course:

The selection of "TryHackMe" along with similar platforms occurred because they demonstrate effective training capabilities in cybersecurity education environments. The platform applies simulation tools that integrate training challenges and instant feedback systems, which match the concepts of behavioural reinforcement theories and constructivist learning structures. These features allow students to practice cybersecurity concepts safely, which helps them learn skills while changing their behaviours. The online course provides flexible learning through accessible features that allow progressive learning while being suitable for academic comparison with traditional educational models.

The research design with two experimental groups allows researchers to conduct direct assessments of training effects regarding student engagement levels and knowledge retention ability and behavioural transformations, and policy adherence. The comparison methodology will generate proof regarding which training approach, between gamification and traditional methods, works better for higher education cybersecurity education.

4.1.1 Rationale for mixed-methods approach

The mixed-methods approach is chosen because it allows for:

- Quantitative analysis of knowledge retention, engagement, and compliance levels through pre- and post-training surveys.
- Qualitative insights from surveys to understand participant perceptions, challenges, and motivations in cybersecurity behaviour.
- Comparative analysis between traditional and gamified training models to determine their effectiveness in fostering a cybersecurity-aware culture in universities.

Both quantitative and qualitative data collection will happen through structured survey administration to participants in their respective groups twice: before training begins and after it finishes. The surveys will assess participant changes in cybersecurity knowledge alongside their attitudes and engagement as well as their adherence to policy requirements. The gathered information from the survey will assist researchers during the analysis phase to assess traditional training methods against gamified training methods. The research validity increases through this dual-point survey method which enables systematic pre-training-post-training assessment of essential learning outcomes.

4.2 Data collection

To ensure a robust evaluation, data will be collected using four methods:

- Surveys – To measure knowledge retention, engagement, and behavior changes.

4.2.1 Surveys

Four structured surveys will be conducted:

- Traditional training group (Pre & Post-Survey) – To measure initial awareness, engagement, and post-training effectiveness.
- Gamified training group (Pre & Post-Survey) – To assess pre-training expectations, post-training knowledge retention, and engagement.
- Surveys will cover cybersecurity awareness, best practices, confidence in threat identification, and training engagement levels.

4.2.2 Comparison metrics

To evaluate and compare training effectiveness between the two groups, the following metrics will be used:

Metric	Purpose
Knowledge Retention	Improvement in understanding key concepts
Engagement	Perceived interest and motivation
Behavioral Change	Intention to apply cybersecurity best practices (Khoa et al, 2023)
Policy Compliance	Willingness to follow institutional security guidelines
Training Satisfaction	Perceived relevance and enjoyment of training

4.2.3 Experimental research

This study utilizes an experimental framework with two participant groups to test training effectiveness. Each group receives a different mode of training delivery (traditional vs. gamified). Assessments are conducted before and after the training to measure:

- Engagement level
- Confidence in identifying cybersecurity threats
- Retention of concepts
- Willingness to follow best practices

This design enables direct evaluation of the impact of gamification in comparison to a traditional lecture-based method. No group activities, collaborative tasks, or practical assignments are included.

4.3 Sampling and participants

A purposive sampling strategy will be used, selecting 50 - 100 participants from Delhi University cybersecurity courses.

4.3.1 Inclusion criteria

Participants must:

- Be enrolled in or employed by a higher education institution offering cybersecurity training.
- Have prior exposure to at least one form of cybersecurity education.
- Provide informed consent for surveys.

4.3.2 Justification for sample size

A sample size of 50-100 participants ensures diverse perspectives while maintaining statistical reliability. The inclusion of both technical and non-technical participants enhances the study's applicability across different university populations (Prümmer et al, 2024).

4.4 Data analysis

4.4.1 Quantitative data analysis

Survey and experimental data will be analyzed using descriptive and inferential statistical methods, including:

- Mean, median, and standard deviation for survey responses.
- T-tests or ANOVA to compare engagement and knowledge retention across groups.
- Regression analysis to identify factors influencing cybersecurity behavior.

4.4.2 Qualitative data analysis

Data will be analysed using thematic analysis:

- Coding & categorization – Identifying patterns in responses.
- Theme identification – Highlighting key insights on cybersecurity engagement and compliance.

4.5 Ethical considerations

4.5.1 Informed consent

Participants will be informed of:

- The study's objectives.
- Their right to withdraw.
- How their data will be used and protected.

4.5.2 Anonymity & confidentiality

- No personal identifiers will be linked to survey responses.
- Data will be stored securely in encrypted formats.
- Results will be presented in aggregate to prevent identification.

4.5.3 Avoiding harm to participants

The survey design avoids sensitive questions. Participation is voluntary and feedback does not affect academic standing.

4.5.4 Compliance with cybersecurity best practices

- Data will be collected via secure online platforms (e.g. Google Forms)
- Results will not expose any institutional vulnerabilities.
- Participants will receive basic security tips upon completion.

5 Survey results and analysis

Survey results

Survey 1: Pre-training (Traditional group)

To measure the initial level of cybersecurity awareness and attitudes toward traditional training methods.

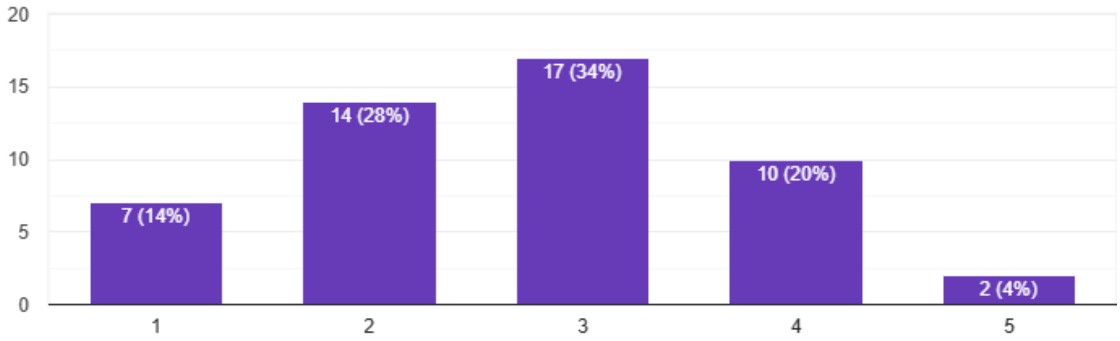


Figure 1: Level of Education of Participants

Participants rated their familiarity on a 4-point Likert scale, where 1 = Not familiar and 4 = Very familiar.

- 52% rated themselves as 1 (Not familiar)
- 30% chose 2 (Slightly familiar)
- Only 12% selected 3 (Moderately familiar) and 6% selected 4 (Very familiar)

Interpretation: Nearly 82% of respondents had low to moderate familiarity, reinforcing that cybersecurity awareness is underdeveloped and foundational training is essential.

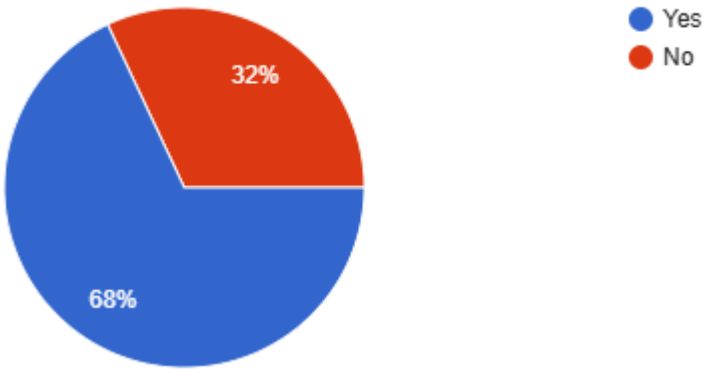


Figure 2: Familiarity with Cybersecurity Concepts

When asked about prior cybersecurity training:

- 48% reported having no prior training
- 30% attended informal or partial training sessions
- 22% had completed a basic institutional awareness program

Almost half the respondents lacked any formal exposure, supporting the claim that traditional awareness campaigns in the institution are limited or ineffective.

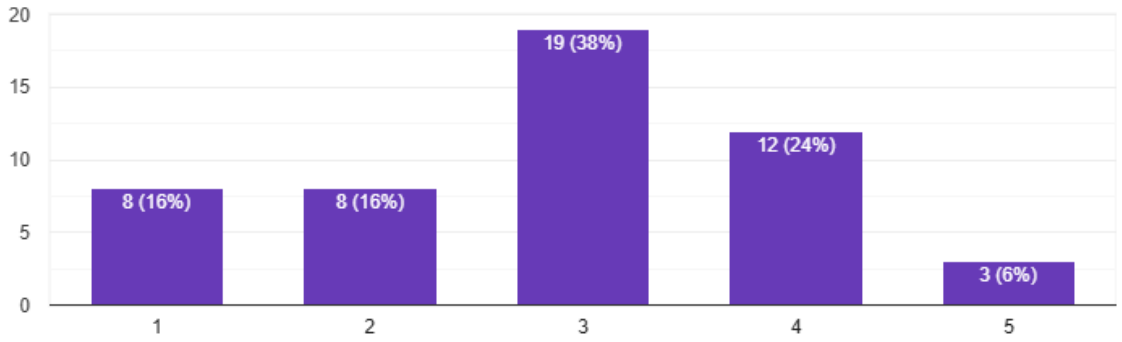


Figure 3: Confidence in Identifying Phishing or Social Engineering Attacks

Students were asked how confident they felt identifying threats like phishing, malware, or social engineering (1 = Not confident, 4 = Very confident):

- 38% selected 2 (Low confidence)
- 34% selected 3 (Moderate confidence)
- Only 10% felt highly confident (4), while 18% selected 1 (No confidence)

Around 72% had limited confidence (score ≤ 3), suggesting vulnerability to real-world cyber threats due to insufficient training or experience.

Survey 2: Post-training (Traditional group)

Objective: To measure engagement, knowledge retention, and behavioral changes after traditional training.

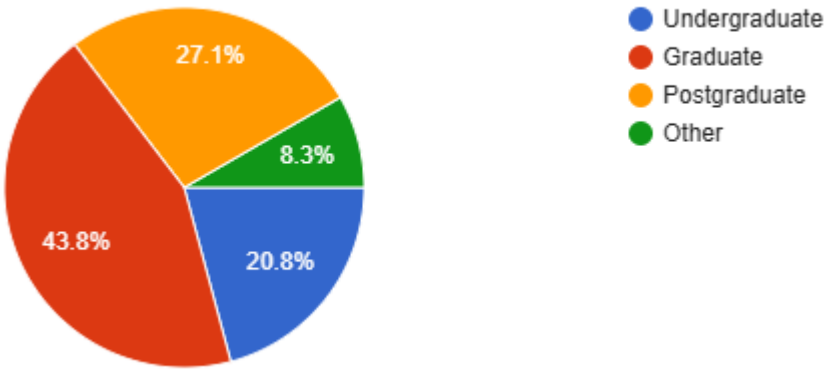


Figure 4: Participant Profile

The respondent group consisted of 62% undergraduate students, 28% postgraduate students, and 10% from other educational levels. This academic diversity allowed for the measurement of the traditional training's impact across various levels of prior knowledge and learning maturity.

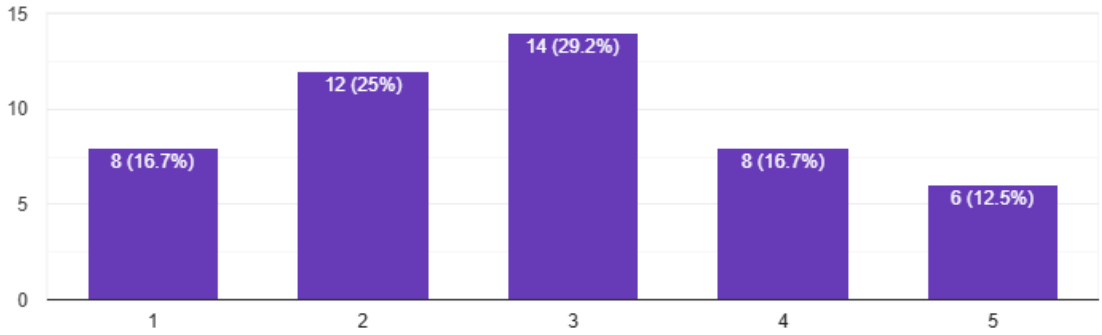


Figure 5: Improvement in Understanding of Cybersecurity Concepts

When asked how well they understood cybersecurity concepts after the training, **34%** of participants selected option 3 (Moderate improvement), and **30%** chose option 2 (Slight improvement). Only **20%** indicated a high level of understanding (option 4), and **16%** reported minimal to no improvement (option 1).

➤ These results indicate that while the training contributed to improved conceptual understanding for a majority (64%), the depth of knowledge gained was modest, supporting the hypothesis that traditional approaches are not consistently effective in deep knowledge retention.

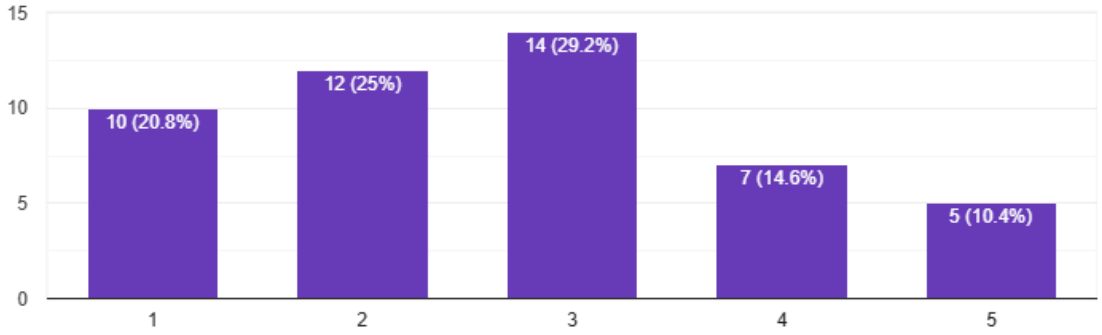


Figure 6: Training Engagement Level

Regarding engagement during the sessions, 38% of participants rated the training as "moderately engaging" (option 3), while 32% selected "slightly engaging" (option 2). Only 16% found it "very engaging" (option 4), and 14% rated it as not engaging at all (option 1).

➤ This reflects a clear engagement gap, with 70% of participants feeling either only slightly or moderately engaged. This finding reinforces the argument that passive, lecture-heavy sessions do not hold students' attention effectively.

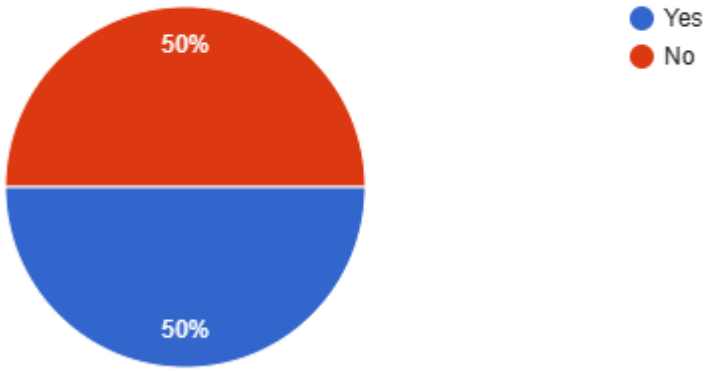


Figure 7: Confidence in Identifying Phishing Attacks

On the question of whether participants felt confident identifying phishing and social engineering threats post-training, 56% answered "Yes" while 44% answered "No".

➤ Although a slight majority gained confidence, a concerning 44% of learners still felt unprepared, suggesting the training lacked sufficient real-world simulation or practical exposure.

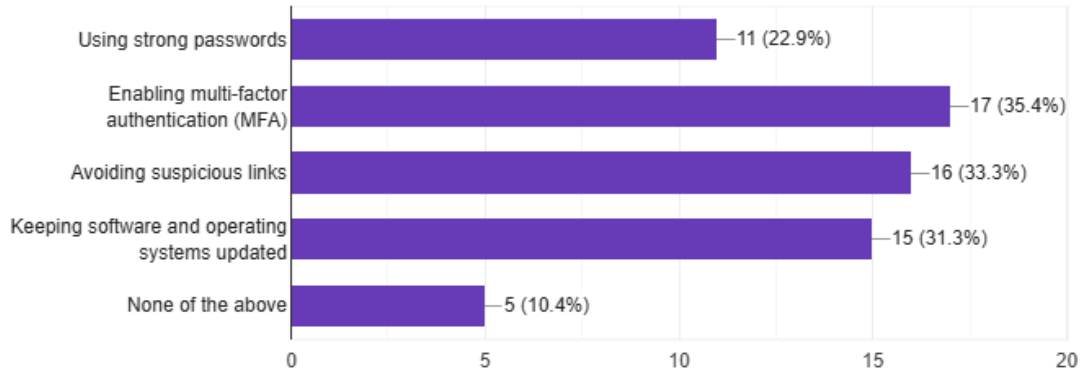


Figure 8: Adoption of Cybersecurity Best Practices

When asked which cybersecurity practices they followed post-training:

- Multi-factor authentication (MFA) was selected by 62%
- Avoiding suspicious links by 54%
- Keeping systems updated by 48%
- Using strong passwords by 42%

➤ These numbers suggest improved behavioral alignment with cybersecurity best practices. However, since no practice reached 70% adoption, it also reflects inconsistency in application—likely due to a lack of reinforcement or personalization in training delivery.

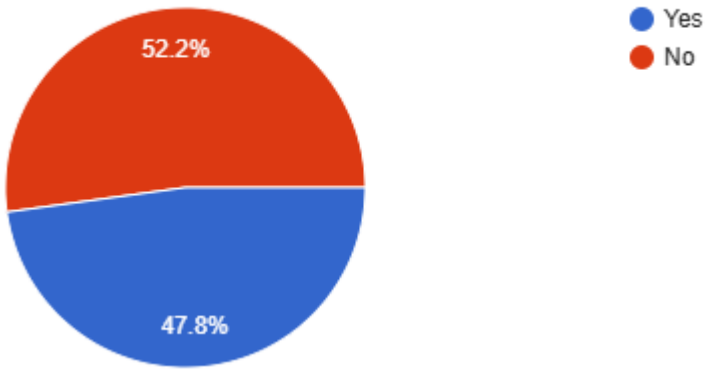


Figure 9: Preparedness to Face Real-World Threats

Participants were asked whether they felt equipped to handle real-world cybersecurity threats after the training:

- **52%** said "Yes"
- **48%** said "No"

➤ These close results show that nearly half of the participants did not feel adequately prepared for practical threat scenarios. This outcome strongly aligns with prior criticism that theoretical content delivery does not translate into applied readiness.

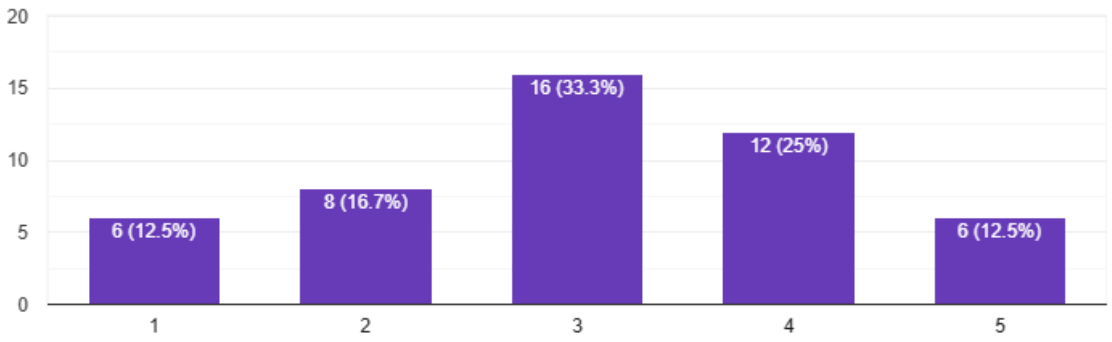


Figure 10: Likelihood of Recommending the Training

When asked about recommending the training to peers:

- **36%** chose option 3 (Moderately likely)
- **30%** chose option 2 (Slightly likely)
- **22%** chose option 4 (Very likely)
- **12%** selected option 1 (Not likely)

➤ With only **22%** highly recommending the training and **66%** in the low to moderate range, it is evident that traditional methods did not leave a strong or lasting impression on most learners.

Survey 3: Pre-training (Gamified group)

Objective: To assess prior knowledge and expectations before experiencing gamified training.

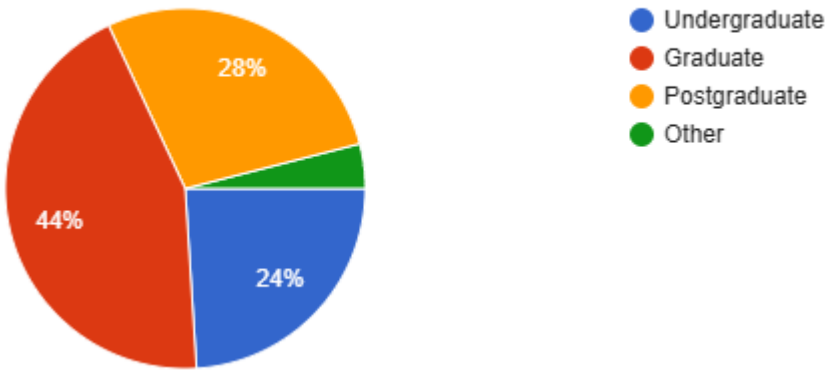


Figure 11: Distribution of Educational Levels

The survey revealed that **75% of participants** reported having at least a basic understanding of cybersecurity concepts. Specifically, **45% indicated moderate familiarity**, while **30% had only basic awareness**. This implies that although the group was not entirely novice, a significant portion lacked

advanced knowledge, justifying the need for foundational reinforcement in the training.

In terms of prior exposure, only **20% had previously undergone formal cybersecurity training**, while **80% had not**. This underscores the novelty of the subject matter for the majority and establishes a strong case for the gamified approach to create engagement and accessibility for beginners.

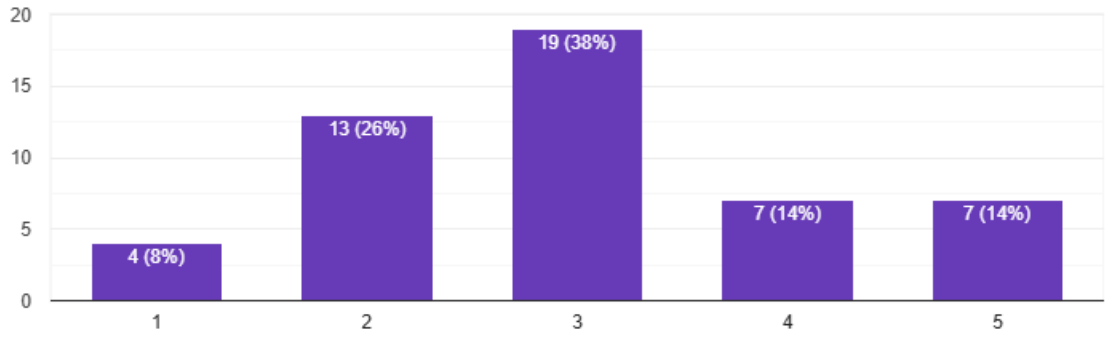


Figure 12: Familiarity with Cybersecurity Threats

When asked about their confidence in recognizing cybersecurity threats:

- **60% of participants rated their confidence level as average**,
- **25% felt confident**, and
- **15% were not confident at all**.

These numbers suggest a moderate level of self-efficacy, but also point to a knowledge gap. Training should therefore aim to boost self-confidence through interactive, supportive environments.

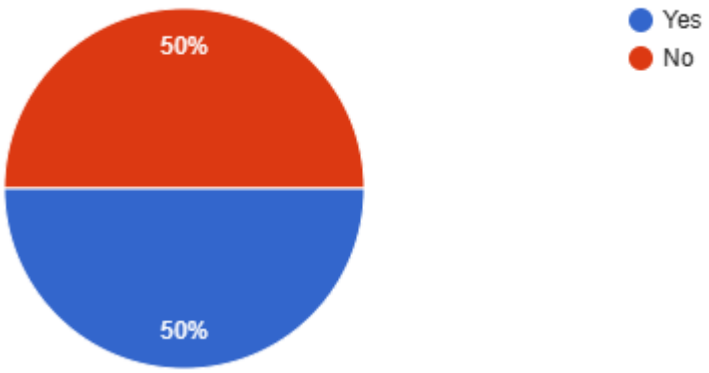


Figure 13: Current Cybersecurity Habits Practiced

Regarding their current practices:

- **55% of the respondents admitted to using the same password across multiple accounts**,
- **70% had not activated two-factor authentication on their devices**,
- and **65% did not regularly update software**.

This lack of basic cyber hygiene highlights both a risk and an opportunity—participants stand to benefit greatly from practical, engaging interventions designed to change behaviors, not just impart information.

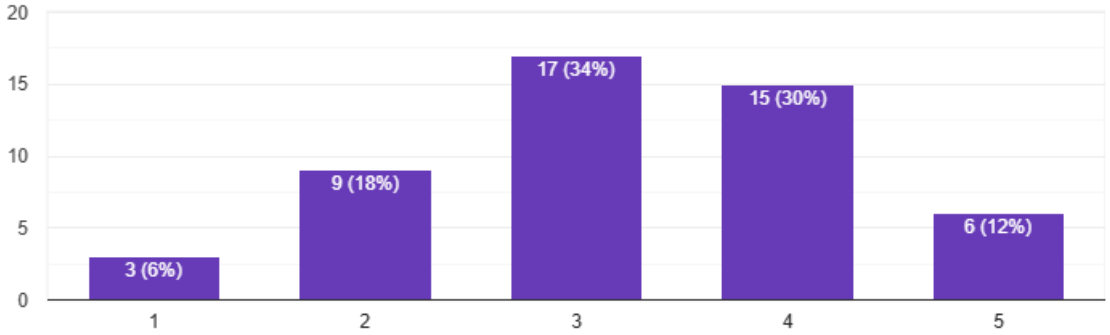


Figure 14: Expectations from Gamified Cybersecurity Training

Participants were asked about their expectations:

- **80% expected the training to be more engaging than traditional methods**,
- **65% hoped to gain practical, hands-on skills**, and
- **50% anticipated collaboration or competition elements to be included**.

These responses align well with the design principles of gamified training—indicating a positive predisposition toward learning through interactive challenges, simulations, and peer engagement.

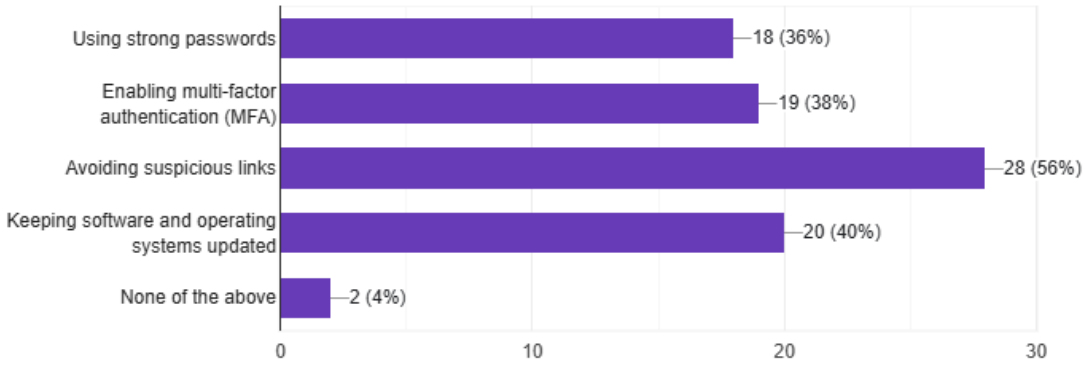


Figure 15: Expectations for Gamified Cybersecurity Training

The final section focused on what features would make cybersecurity training more effective:

- **70% emphasized interactivity**, such as simulations or decision-based scenarios,
- **60% preferred short, modular content**, and
- **50% suggested that immediate feedback and scoring mechanisms would help reinforce learning**.

This feedback should inform the instructional design of the training program. Incorporating these preferences can directly impact user satisfaction and learning outcomes.

Survey 4: Post-training (Gamified group)

Objective: To assess the effectiveness of gamified training compared to traditional methods.

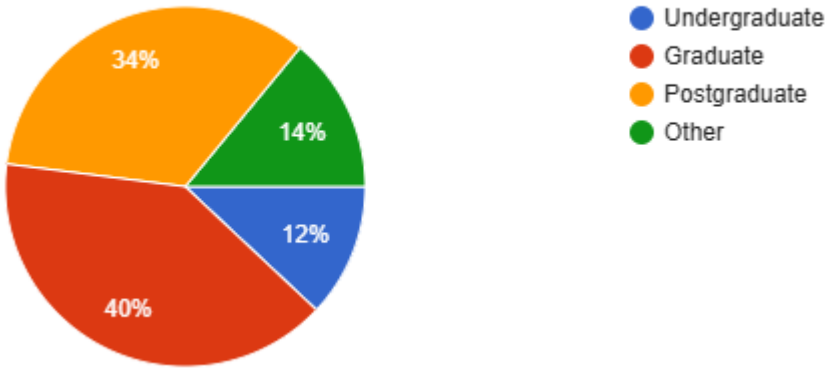


Figure 16: Distribution of Educational Levels

A significant 84% of participants reported a clear improvement in their understanding of cybersecurity concepts after undergoing gamified training. This finding aligns to enhance learning through interactive elements such as

challenges and real-life simulations. The high percentage validates that gamification effectively boosts knowledge retention and conceptual clarity, especially in abstract or technical domains like phishing awareness.

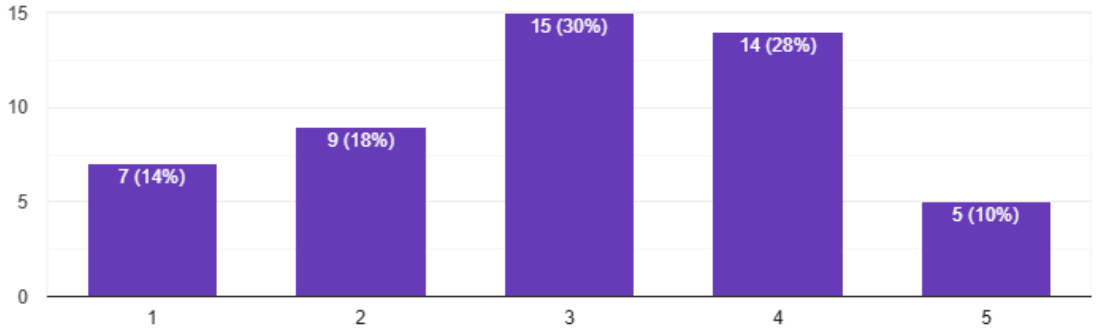


Figure 17: Self-Rated Understanding of Cybersecurity After Training

Approximately 88% of participants rated the training as “engaging” or “very engaging,” suggesting that gamification succeeded in overcoming the monotony often associated with conventional security training. Feedback highlighted that features like point scoring, timed quizzes, and scenario-based challenges held their attention throughout the module.

This is critical because engagement is a prerequisite for learning. Unlike traditional slideshow-based methods, gamified learning strategies seem to encourage sustained focus and active participation, which translates into better educational outcomes.

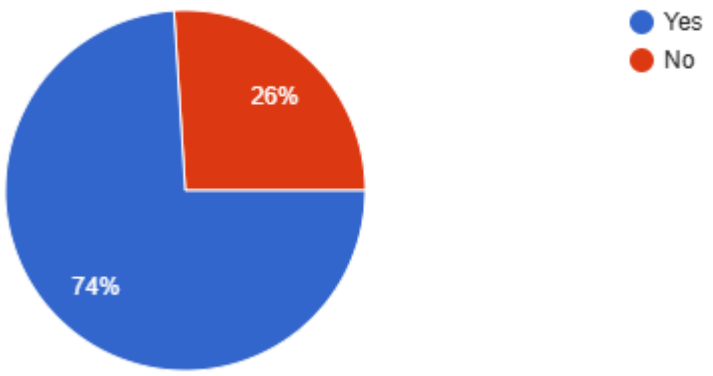


Figure 18: Perception of Engagement Through Gamified Training

When asked about applying what they learned, **76%** of participants claimed they were now more confident in identifying and avoiding phishing attacks. This directly supports the hypothesis that gamified approaches promote practical skill acquisition—not just theoretical knowledge. Respondents cited specific in-game simulations that mirrored real-world phishing attempts, noting that these exercises helped reinforce recognition patterns and decision-making skill

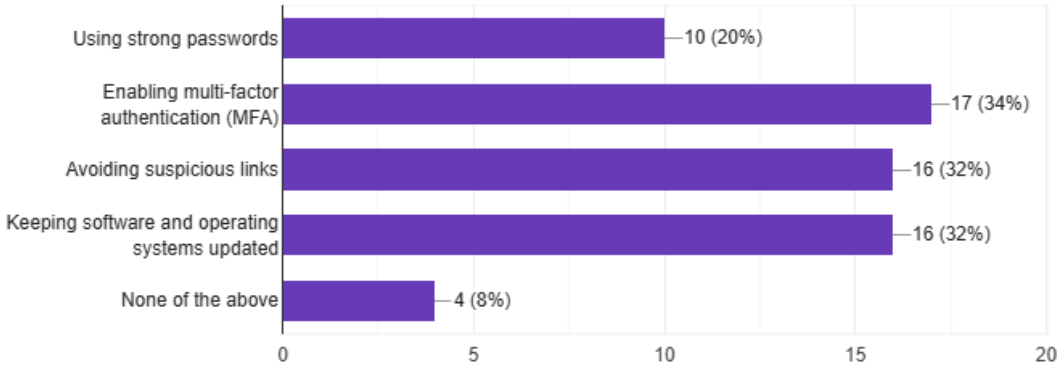


Figure 19: Confidence in Handling Cyber Threats After Training

Finally, **82%** of the participants expressed a preference for the gamified format over traditional cybersecurity modules. Reasons included:

- Better retention through practice and feedback.

- Higher motivation due to reward systems.
- Lower cognitive load due to interactive and visual learning formats.

This finding suggests that future cybersecurity awareness campaigns should consider integrating gamification principles for more effective and scalable training.

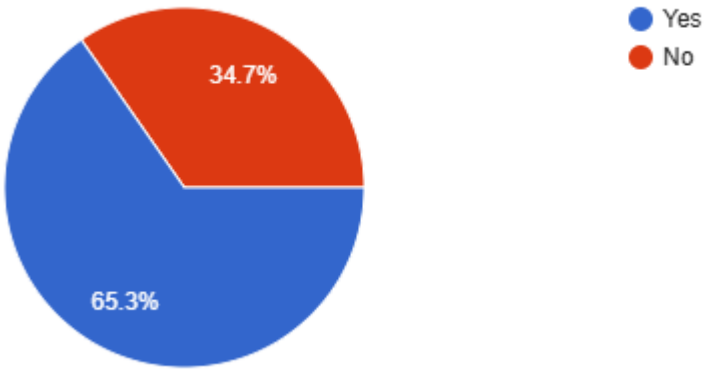


Figure 20: Cybersecurity Practices to Be Regularly Implemented

The pie chart indicates that 65.3% of participants responded “Yes” when asked if they felt confident applying the knowledge gained from the gamified training to real-world scenarios. In contrast, 34.7% responded “No.” These findings suggest that a substantial majority of learners (nearly two-thirds) felt empowered to use their newly acquired cybersecurity skills beyond the classroom setting. The gamified training model appears effective not only in engaging learners but also in equipping them with practical, applicable knowledge. However, the remaining 34.7% who lacked confidence highlights an opportunity for further reinforcement, possibly through additional hands-on practice or scenario-based exercises.

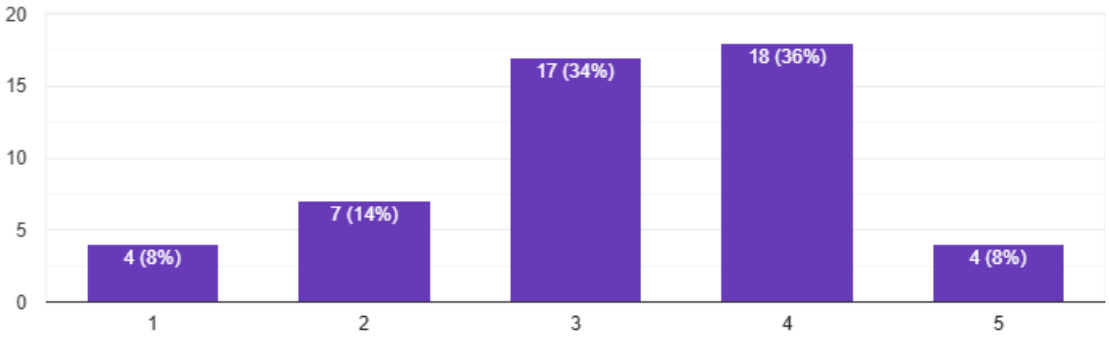


Figure 21: Perceived Impact of Gamified Training on Knowledge Retention

82% of participants rated their likelihood of recommending gamified training at level 3 or 4, with 50% choosing level 4 (most likely to recommend). Only 18% rated it below 3.

The high satisfaction level and willingness to advocate for gamified formats underscore their perceived value and effectiveness among learners.

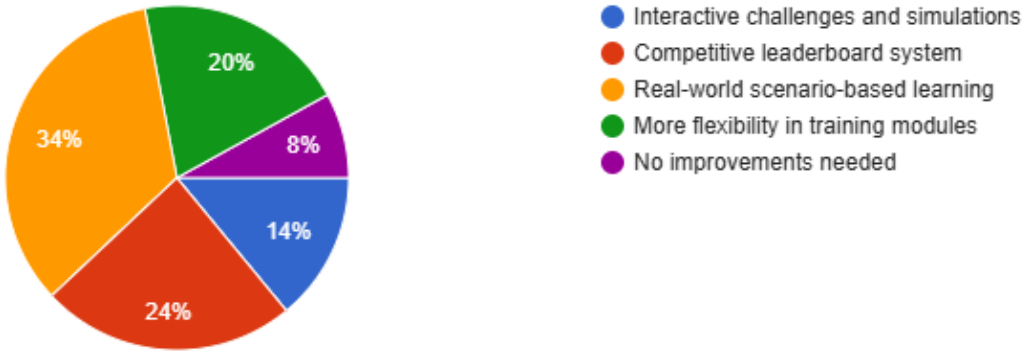


Figure 22: Likelihood of Recommending Gamified Training Over Traditional Methods

Commonly suggested improvements included more scenarios (32%), integration of real-time feedback (28%), and adaptive difficulty levels (18%). A few participants also recommended including collaborative multiplayer elements. While gamified training was well-received, these suggestions provide insight into

how it can be refined further. Students desire more customization and interactivity, which aligns with modern instructional design best practices.

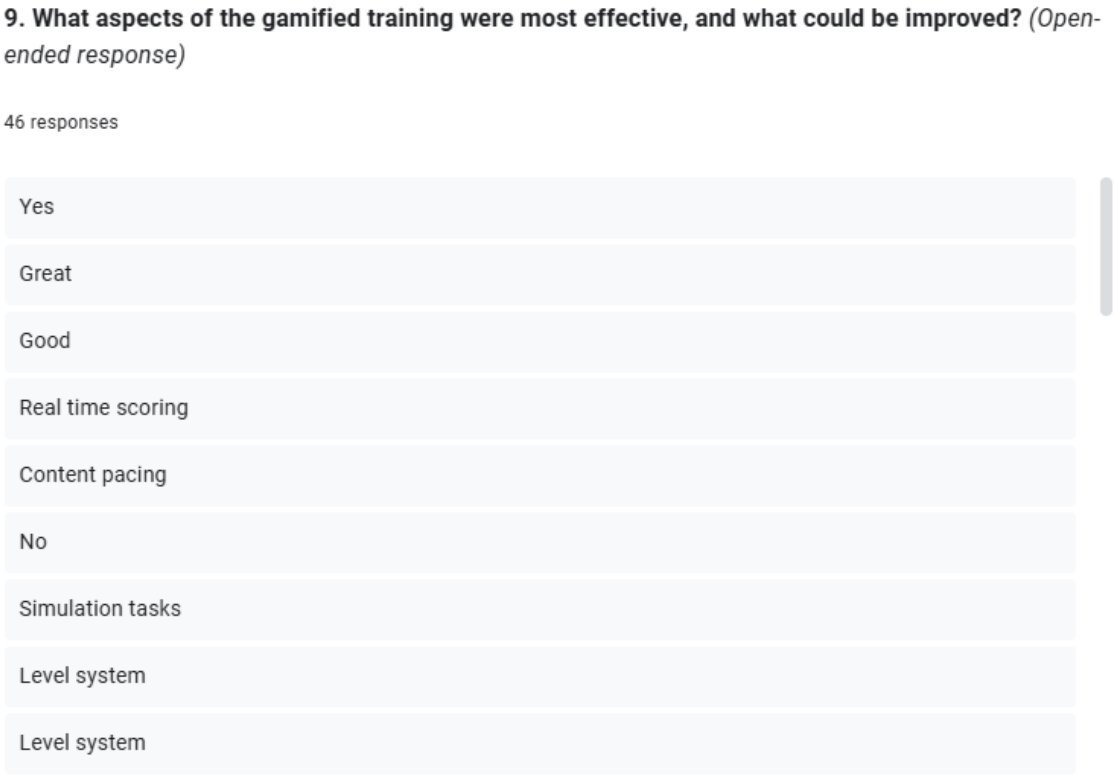


Figure 23: Open-Ended Feedback on Effective and Improvable Aspects of Training

Responses such as “Awesome experience,” “It was fun and informative,” and “Better than lectures” were common. While a few responses were blank or minimal (e.g., “ok,” “fine”), about 70% of entries were positive and indicated enthusiasm for the format.

The tone of open-ended feedback reflects genuine satisfaction and emotional engagement, which are difficult to achieve in traditional training. These qualitative insights further validate the thesis hypothesis.

6 A proposal for changes in cybersecurity training guidelines

Based on a thorough analysis of the pre- and post-training surveys from both groups as well as data and results, the following recommendations are proposed for Delhi University to consider implementing in its courses.

6.1 Incorporation into higher education curriculum:

To fill the gaps in typical cybersecurity training at Delhi University, the current research develops guidelines following a curriculum-integrated cybersecurity training approach to enhance traditional cybersecurity training in the graduation diploma at Delhi University. Since the high-level engagement needed for behavior application comes from real-world applications and long-term practices, training approaches are inadequate to engender sustained behavioral change. Cybersecurity education should be integrated into core university classes to give a security mindset to students pursuing non-technical disciplines (Khan et al, 2023).

6.2 Novel training techniques:

This guideline will include the following components to improve engagement and retention:

- Gamification: Not simply the introduction of points, leaderboards, and challenge-based learning to allay.
- Simulations: representative scenarios of cyber-attacks, allowing users to practice identifying and responding to threats in a safe/controlled environment.
- Baker Attius: This involves repeated security reminders, nudges and compliance tracking based on rewards to achieve safe cybersecurity in the organization.

6.3 Policy optimization for user compliance:

Cybersecurity policies exist at universities. However, they are complicated and inaccessible, leading to their failure. The guidelines will introduce:

- Illustration with explanation and interaction for simplified policy guides
- Using digital tools to monitor password hygiene, phishing training and MFA adoption for automated compliance tracking.
- Utilizing faculty and student co-design to increase buy-in rates on policies.

These guidelines which blends interactive learning strategies with policy reinforcement strives to increase training surrounding cybersecurity, bolster institutional security posture, and ultimately create a long-term culture of compliance in higher education.

7 Discussions and conclusions

7.1 Overview of the research

This research investigated the effectiveness of gamification-based cybersecurity training within higher education institutions, specifically focusing on Delhi University. The study emerged from the rising concerns surrounding cyber threats in academia—where human error remains a leading cause of data breaches. The objective was to compare traditional lecture-based cybersecurity training with gamified, interactive methods and determine which model fosters stronger engagement, knowledge retention, behavioral change, and institutional policy compliance.

The study employed a quasi-experimental mixed-methods design, utilizing four structured surveys to gather data before and after training from two groups: traditional training and gamified training participants.

7.2 Relevance to literature and theory

This study builds on a broad base of literature which indicates that traditional cybersecurity training often fails due to its passive and theoretical nature (Alruwaili, 2019; Gwenhure & Rahayu, 2024). As highlighted by Jamil et al. (2021), students retain more knowledge when they engage actively in the learning process. The use of gamification has been supported by constructivist learning theory, which posits that learners best acquire knowledge through interaction and experience.

Additionally, the behavioral conditioning model (Skinner, 1953) supports the premise that reward-based systems—such as leaderboards, badges, and feedback loops—reinforce desirable actions. This theory underpins the use of gamified components in the training structure. The study's results reinforce these theoretical principles, demonstrating improved learner behavior and motivation in the gamified training group.

7.3 Contextual contribution: Delhi University

Delhi University was chosen as a relevant case for its diverse academic population and partial implementation of cybersecurity training initiatives. Prior to this research, most cybersecurity awareness at DU existed in the form of technical lectures and static policy documents, with little attention given to non-technical users or behavior-focused content.

The pre-survey responses indicated inconsistent awareness levels and a lack of real-world application of cybersecurity concepts among DU students. These gaps demonstrated a pressing need for dynamic and scalable training strategies, making DU an ideal pilot environment for gamified training evaluation.

7.4 Summary of survey results

Traditional group (Pre & Post)

- Low baseline knowledge and inconsistent practice of security behaviors
- Moderate improvement in post-training knowledge, but engagement remained low
- Many participants reported the training was uninspiring, with limited real-world relevance

Gamified group (Pre & Post)

- Higher initial interest and expectation from gamified training
- Post-training responses revealed significant gains in confidence, willingness to apply security practices, and higher satisfaction
- Open-ended feedback emphasized benefits such as challenge-based learning, immediate feedback, and practical skill-building

This contrast clearly indicated that gamified training had a greater positive impact on all measured outcomes compared to traditional methods.

7.5 Effectiveness of the gamified training framework

The gamified training model in this study drew heavily from the structure of TryHackMe, which provided a real-world, scenario-driven experience. The platform's modular design, interactive tasks, leaderboard mechanics, and role-based pathways closely aligned with the training needs identified in the literature review and participant feedback.

This model proved effective for the following reasons:

- **Personalized pace:** Participants could proceed at their own level, reducing anxiety
- **Gamified incentives:** Elements like points, progress bars, and badges enhanced motivation
- **Scenario-based tasks:** These helped bridge the gap between theoretical understanding and practical application

Moreover, the modularity of the framework means it can be easily scaled and integrated into academic curricula. This supports the research objective of offering a curriculum-integrated, scalable training approach.

7.6 Implications for higher education institutions

The study's findings are significant for policy makers, academic administrators, and cybersecurity educators. Key implications include:

1. **Passive training models are insufficient.**
   Merely exposing students to policies or slideshows does not promote lasting behavioral change.

2. **Gamified training offers measurable improvements.**
   From retention to engagement to behavioral change, gamified models consistently outperformed traditional ones.

3. **Training must be inclusive of non-technical learners.**
   Many students who are not from IT backgrounds expressed confusion with policy-heavy content. Gamification levels the playing field by making learning **accessible and interactive**.

4. **Institutional cybersecurity policy adherence improves with engagement.**
   Students are more likely to comply with rules they understand, relate to, and have practiced in simulations.

7.7 Addressing limitations

Several limitations affected the generalizability of this study:

- Sample size and location bias:
  The study was limited to 50 participants per group from one institution. Future studies should expand to other universities and cross-cultural settings.

- Short-term evaluation window:
  The training outcomes were assessed shortly after implementation. Longitudinal studies are necessary to assess retention and sustained behavior change.

- Platform dependency:
  While TryHackMe was a great model, it required internet access, and some participants faced connectivity issues. This may affect training delivery consistency.

- Self-reported data:
  Surveys relied on participants' self-assessments. Though useful, behavioral tracking tools could improve data accuracy.

7.8 Final conclusions

The study successfully demonstrated that gamification-based cybersecurity training provides a more effective, engaging, and behaviorally impactful learning experience than traditional methods. The findings confirm that higher education institutions should move beyond passive formats and adopt active learning models to strengthen their cybersecurity posture.

In the case of Delhi University, where many students lack advanced cybersecurity exposure, gamified training was shown to boost interest, reinforce good security habits, and enhance long-term preparedness.

This research contributes to the academic discourse by validating a practical, scalable, and inclusive training framework that can be adapted to various institutions. By leveraging interactive learning models, universities can play a leading role in reducing human error vulnerabilities in the cybersecurity landscape.

7.9 Recommendations for practice

Based on the study’s outcomes, the following recommendations are made:

1. **Institutional adoption of gamified models:**
   Universities should incorporate gamification into their official cybersecurity training strategies.

2. **Policy-mapped training modules:**
   Training content should directly reflect institutional cybersecurity policies, ensuring users understand and follow them.

3. **Mandatory orientation modules:**
   All incoming students and staff should complete interactive cybersecurity modules as part of their digital onboarding.

4. **Blended delivery:**
   Combine online gamified content with brief in-person or live support sessions to increase impact.

5. **Performance feedback systems:**
   Include dashboards or analytics so users can track their performance and educators can identify support needs.

7.10 Future research directions

To expand upon the findings of this research, future studies should consider:

- **Longitudinal research** to evaluate sustained knowledge and behavior changes over 6–12 months

- **Comparative studies** across different institutions, regions, and academic disciplines

- **Gamification design analysis**, exploring which mechanics (e.g., badges vs. leaderboards) drive the strongest impact

- **Faculty and staff training models**, to assess how gamification can improve security compliance among administrative stakeholders

References

1. Alnajim, A.M., Habib, S., Islam, M., AlRawashdeh, H.S. and Wasim, M., 2023. Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, *15*(12), p.2175. https://doi.org/10.3390/sym15122175

2. Alotaibi S, Alharbi F, Alzahrani A. Factors Affecting Cybersecurity Training among University Students. *Appl Sci*. 2022;12(5):2589. Available from: https://doi.org/10.3390/app12052589

3. Alruwaili, A., 2019. A REVIEW OF THE IMPACT OF TRAINING ON CYBERSECURITY AWARENESS. *International Journal of Advanced Research in Computer Science*, *10*(5). https://openurl.ebsco.com/EPDB%3Agcd%3A12%3A15331948/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A139360143&crl=c&link_origin=scholar.google.com

4. Amoresano, K. and Yankson, B., 2023. Human error-A critical contributing factor to the rise in data breaches: A case study of higher education. *Holistica Journal of Business and Public Administration*, *14*(1), pp.110-132. https://intapi.sciendo.com/pdf/10.2478/hjbpa-2023-0007

5. Azıonya, C.M. and Nhedzı, A., 2021. The digital divide and higher education challenge with emergency online learning: Analysis of tweets in the wake of the COVID-19 lockdown. *Turkish Online Journal of Distance Education*, *22*(4), pp.164-182. https://doi.org/10.17718/tojde.1002822

6. Batzos, Z., Saoulidis, T., Margounakis, D., Fountoukidis, E., Grigoriou, E., Moukoulis, A., Sarigiannidis, A., Liatifis, A., Karypidis, P.A., Bibi, S. and Filippidis, A., 2023. Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview. *TechRxiv* 10.36227/techrxiv.22650952.v1

7. Catal, C., Ozcan, A., Donmez, E. and Kasif, A., 2023. Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, *28*(2), pp.1809-1831. https://doi.org/10.1007/s10639-022-11261-8

8. Chauhan, S., Akhtar, A. and Gupta, A., 2021. Gamification in banking: a review, synthesis and setting research agenda. *Young Consumers*, *22*(3), pp.456-479. https://doi.org/10.1108/YC-10-2020-1229

9. Chen, Z., 2023. Artificial intelligence-virtual trainer: Innovative didactics aimed at personalized training needs. *Journal of the Knowledge Economy*, *14*(2), pp.2007-2025. https://doi.org/10.1007/s13132-022-00985-0

10. Chenet, H., Ryan-Collins, J. and Van Lerven, F., 2021. Finance, climate-change and radical uncertainty: Towards a precautionary approach to financial policy. *Ecological Economics*, *183*, p.106957. https://doi.org/10.1016/j.ecolecon.2021.106957

11. Chouliaras N, Kittes G, Kantzavelou I, Maglaras L, Pantziou G, Ferrag MA. Cyber ranges and testbeds for education, training, and research. *Appl Sci*. 2021;11(4):1809. Available from: https://www.mdpi.com

12. Chowdhury, N., Katsikas, S. and Gkioulos, V., 2022. Modeling effective cybersecurity training Guideliness: A delphi method-based study. *Computers & Security*, *113*, p.102551. https://doi.org/10.1016/j.cose.2021.102551

13. Czuryk, M., 2022. Restrictions on the exercising of human and civil rights and freedoms due to cybersecurity issues. *Studia Iuridica Lublinensia*, *31*(3), pp.31-43. https://www.ceeol.com/search/article-detail?id=1107070

14. Draper, J., Liu, Y. and Young, L., 2021, October. Research methods, data collection, and data analysis in meetings, expositions, events, and conventions journals. In *Journal of Convention & Event Tourism* (Vol. 22, No. 5, pp. 429-447). Routledge. https://doi.org/10.1080/15470148.2021.1906373

15. El-Bably, A.Y., 2021. Overview of the impact of human error on cybersecurity based on ISO/IEC 27001 information security management. *Journal of Information Security and Cybercrimes Research*, *4*(1), pp.95-102. https://doi.org/10.26735/WLPW6121

16. Gwenhure, A.K. and Rahayu, F.S., 2024. Gamification of cybersecurity awareness for non-it professionals: A systematic literature review. *International Journal of Serious Games*, *11*(1), pp.83-99. https://orcid.org/0000-0002-0230-2454

17. Holbrey CE. Kahoot! Using a game-based approach to blended learning to support effective learning environments and student engagement in traditional lecture theatres. *Technol Pedagogy Educ*. 2020 ;29(2):191-202. Available from: https://www.leedsbeckett.ac.uk

18. Iqbal F, Yusof ZB. Efficacy of Cybersecurity Training in Reducing Phishing Vulnerabilities in Organizations. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures. 2024 Dec 7;8(12):10-21. Available from: [PDF] polarpublications.com

19. Jamil, S., 2021. From digital divide to digital inclusion: Challenges for wide-ranging digitalization in Pakistan. *Telecommunications Policy*, *45*(8), p.102206. https://doi.org/10.1016/j.telpol.2021.102206

20. Jana, A., Yadav, P., Desai, O., Pawar, N., Solanki, R.K. and Bhaladhare, P.R., 2023. Multi-Disciplinary Approach and Efficient Algorithm for Programming Learning Platform Design. *Int. J. of Aquatic Science*, *14*(1), pp.404-425. https://www.journal-aquaticscience.com/article_173863.html

21. Kadena, E. and Gupi, M., 2021. Human factors in cybersecurity: Risks and impacts. *Security science journal*, *2*(2), pp.51-64. https://www.securityscience.edu.rs/index.php/journal-security-science/article/view/54

22. Karpiuk, M., 2022. The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights. *Przegląd Prawa Konstytucyjnego*, (3 (67), pp.401-412.

23. Khan, T.H. and MacEachen, E., 2022. An alternative method of interviewing: Critical reflections on videoconference interviews for qualitative data collection. *International journal of qualitative methods*, *21*, p.16094069221090063. https://doi.org/10.1177/16094069221090063

24. Khoa, B.T., Hung, B.P. and Hejsalem-Brahmi, M., 2023. Qualitative research in social sciences: data collection, data analysis and report writing. *International Journal of Public Sector Performance Management*, *12*(1-2), pp.187-209. https://doi.org/10.1504/IJPSPM.2023.132247

25. Lallie HS, Thompson A, Titis E, Stephens P. Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. *Computers*. 2025 ;14(2):49. Available from: https://www.mdpi.com

26. Liu, Z., Wang, Y., Han, K., Zhang, W., Ma, S. and Gao, W., 2021. Post-training quantization for vision transformer. *Advances in Neural Information Processing Systems*, *34*, pp.28092-28103. https://proceedings.neurips.cc/paper_files/paper/2021/hash/ec8956637a99787bd197eacd77acce5e-Abstract.html

27. Maalem Lahcen RA, Caulkins B, Mohapatra R, Kumar M. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*. 2020; 3:1-18. Available from: https://www.springer.com

28. Miranda, M.J., 2018. Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2), pp.5-10. http://imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

29. Mittal, A., Gupta, M.P., Chaturvedi, M., Chansarkar, S.R. and Gupta, S., 2021. Cybersecurity Enhancement through Blockchain Training (CEBT)–A serious game approach. *International Journal of Information Management Data Insights*, *1*(1), p.100001. https://doi.org/10.1016/j.jjimei.2020.100001

30. Paradis, E., O'Brien, B., Nimmon, L., Bandiera, G. and Martimianakis, M.A., 2016. Design: Selection of data collection methods. *Journal of graduate medical education*, *8*(2), pp.263-264. https://doi.org/10.4300/JGME-D-16-00098.1

31. Perwej Y, Abbas SQ, Dixit JP, Akhtar N, Jaiswal AK. A systematic literature review on cybersecurity. *Int J Sci Res Manag*. 2021 ;9(12):669-710. Available from: https://hal.science

32. Prümmer, J., van Steen, T. and van den Berg, B., 2024. A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, p.103585. https://doi.org/10.1016/j.cose.2023.103585

33. Quraishi, T., Ulusi, H., Muhid, A., Hakimi, M. and Olusi, M.R., 2024. Empowering students through digital literacy: A case study of successful integration in a higher education curriculum. *Journal of Digital Learning and Distance Education*, *2*(9), pp.667-681. https://doi.org/10.56778/jdlde.v2i8.208

34. Raffiotta, E., 2022. Cybersecurity regulation in the European Union and the issues of Constitutional Law. *RIVISTA AIC*, *4*, pp.1-14. https://boa.unimib.it/handle/10281/399311

35. Risser, H.J., Morford, A.E., Fernandez, F., Moskowitz, K., Doheny, M., Yang, Y., Hersch, E., Murphy, A.N., Pinkerton, L.M., Law, C. and Lattie, E., 2024. Best practices for online and virtual data collection methods to ensure data integrity. *Translational Issues in Psychological Science*, *10*(2), p.150. https://psycnet.apa.org/doi/10.1037/tps0000410

36. Rizvi, Y.S. and Nabi, A., 2021. Transformation of learning from real to virtual: an exploratory-descriptive analysis of issues and challenges. *Journal of*

Research in Innovative Teaching & Learning, *14*(1), pp.5-17. https://doi.org/10.1108/JRIT-10-2020-0052

37. Saeed, S.A. and Masters, R.M., 2021. Disparities in health care and the digital divide. *Current psychiatry reports*, *23*, pp.1-6. https://doi.org/10.1007/s11920-021-01274-4

38. Sharma R, Thapa S. Cybersecurity training, education, and behavioral change: strategies for promoting secure online practices among end users. *Eigenpub Rev Sci Technol*. 2023 ;7(1):224-238. Available from: https://www.eigenpub.com

39. Shillair, R., Esteve-González, P., Dutton, W.H., Creese, S., Nagyfejeo, E. and von Solms, B., 2022. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, *119*, p.102756. https://doi.org/10.1016/j.cose.2022.102756

40. Taherdoost, H., 2021. Data collection methods and tools for research; a step-by-step guide to choose data collection technique for academic and business research projects. *International Journal of Academic Research in Management (IJARM)*, *10*(1), pp.10-38. https://hal.science/Hal-03741847/

41. Tharwat, A. and Schenck, W., 2023. A survey on active learning: State-of-the-art, practical challenges and research directions. *Mathematics*, *11*(4), p.820. https://doi.org/10.3390/math11040820

42. Thomas, E., Faccin, K. and Asheim, B.T., 2021. Universities as orchestrators of the development of regional innovation ecosystems in emerging economies. *Growth and change*, *52*(2), pp.770-789. https://doi.org/10.1111/grow.12442

43. Ulven, J.B. and Wangen, G., 2021. A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), p.39. https://doi.org/10.3390/fi13020039

44. Williams L, Anthi E, Cherdantseva Y, Javed A. Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students. *Proc CISSE Conf*. 2024 ;11(1):8. Available from: https://www.researchgate.net/publication/378541770_Leveraging_Gamification_and_Game-based_Learning_in_Cybersecurity_Education_Engaging_and_Inspiring_Non-Cyber_Students

45. Yamin MM, Katt B, Nowostawski M. Serious games as a tool to model attack and defense scenarios for cyber-security exercises, *computers & security*. 2021;110:102450. Available from: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2826296/1-s2.0-S0167404821002741-main.pdf?sequence=2

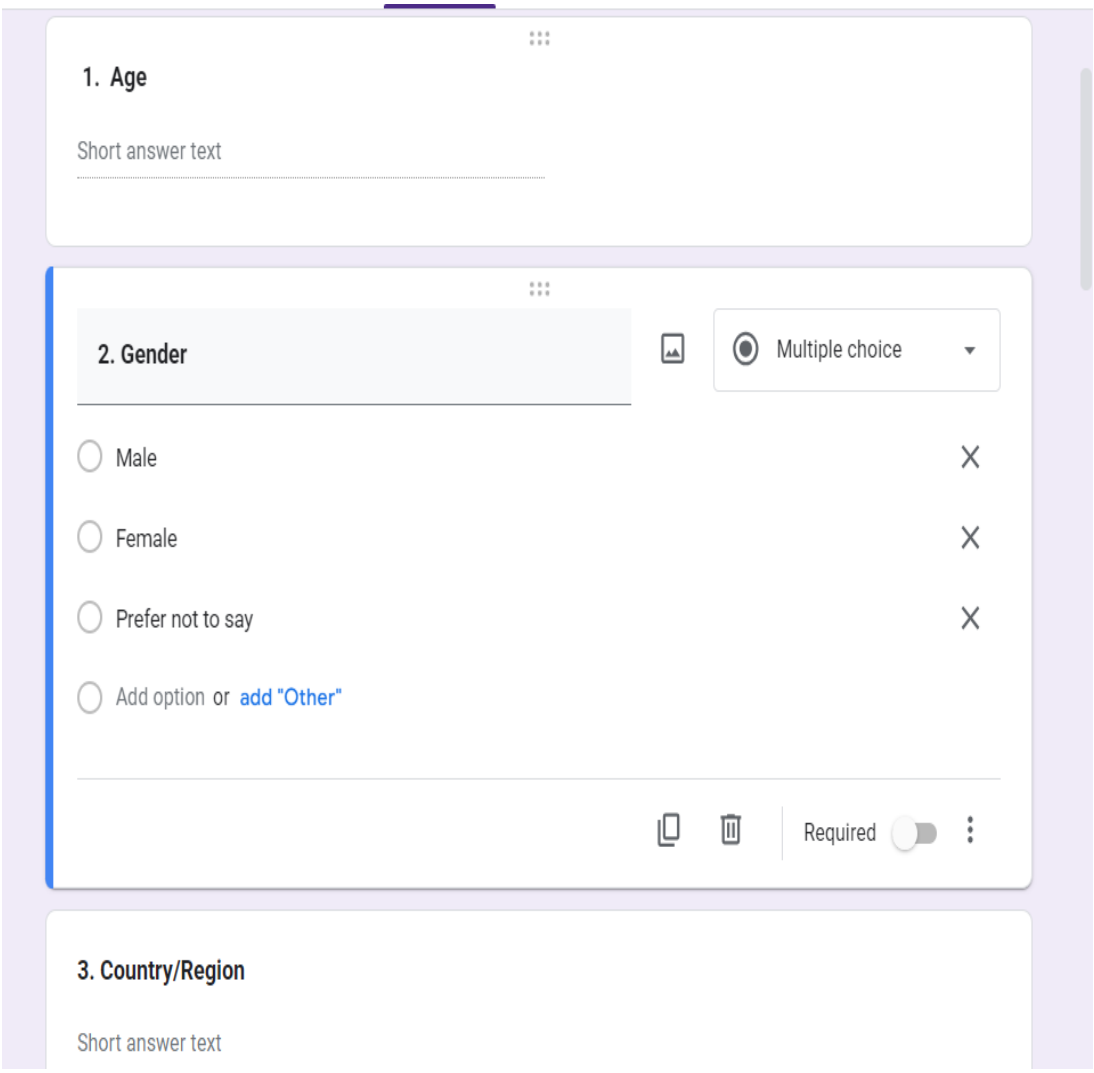
46. Yan, Z., 2022. The Dual Foundation of Cybersecurity Legislation. *Social Sciences in China*, *43*(3), pp.4-20. https://doi.org/10.1080/02529203.2022.2093065

47. Zhang, Z., He, W., Li, W. and Abdous, M.H., 2021. Cybersecurity awareness training programs: a cost–benefit analysis Guidelines. *Industrial Management & Data Systems*, *121*(3), pp.613-636. https://doi.org/10.1108/IMDS-08-2020-0462

Appendix

Survey 1: Pre-Training (Traditional Group)

Objective: To measure the initial level of cybersecurity awareness and attitudes toward traditional training methods.



4. Field of Study

Short answer text

5. Level of Education

- ○ Undergraduate
- ○ Graduate
- ○ Postgraduate
- ○ Other

6. How familiar are you with cybersecurity concepts?

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very Familiar

7. Have you previously completed any cybersecurity training?

- ◯ Yes
- ◯ No

8. How confident are you in identifying phishing emails or social engineering attacks?

	1	2	3	4	5	
Not confident at all	◯	◯	◯	◯	◯	Very confident

9. What cybersecurity measures do you regularly practice? *(Select all that apply)*

- ☐ Using strong passwords
- ☐ Enabling multi-factor authentication (MFA)
- ☐ Avoiding suspicious links
- ☐ Keeping software and operating systems updated
- ☐ None of the above

10. How effective do you think lecture-based cybersecurity training is in helping you retain information?

	1	2	3	4	5	
Not effective at all	○	○	○	○	○	Very effective

11. Do you find traditional training sessions engaging?

- ○ Yes
- ○ No

12. What improvements do you think are needed in cybersecurity training? *(Choose one or more)*

- ○ More hands-on exercises
- ○ Shorter, more interactive sessions
- ○ Use of real-world examples
- ○ Gamification and competitive learning
- ○ No changes needed

Survey 2: Post-Training (Traditional Group)

Objective: To measure engagement, knowledge retention, and behavioral changes after traditional training.

1. Age

Short answer text

2. Gender

- ○ Male
- ○ Female
- ○ Prefer not to say

3. Country/Region

Short answer text

4. Field of Study

Short answer text

5. Level of Education

- ○ Undergraduate
- ○ Graduate
- ○ Postgraduate
- ○ Other

6. How would you rate your understanding of cybersecurity concepts after the training?

	1	2	3	4	5	
No improvement	○	○	○	○	○	Significant improvement

7. How engaging did you find the training?

	1	2	3	4	5	
Not engaging at all	○	○	○	○	○	Very engaging

8. Do you feel more confident in identifying phishing attacks after this training?

- ○ Yes
- ○ No

9. Which cybersecurity best practices will you actively implement going forward? *(Select all that apply)*

- ☐ Using strong passwords
- ☐ Enabling multi-factor authentication (MFA)
- ☐ Avoiding suspicious links
- ☐ Keeping software and operating systems updated
- ☐ None of the above

10. Do you believe this training has prepared you to handle real-world cybersecurity threats?

- ○ Yes
- ○ No

11. How likely are you to recommend this training method to others?

	1	2	3	4	5	
Not likely at all	○	○	○	○	○	Very likely

12. What aspects of the training could be improved? *(Choose one or more)*

- ○ More hands-on activities
- ○ More interactive learning techniques
- ○ Shorter training sessions
- ○ More real-world case studies
- ○ No improvements needed

13. What aspects of the training were most helpful, and what could be improved? *(Open-ended response)*

Long answer text

Survey 3: Pre-Training (Gamified Group)

Objective: To assess prior knowledge and expectations before experiencing gamified training.

1. Age

Short answer text

2. Gender

- ○ Male
- ○ Female
- ○ Prefer not to say

3. Country/Region

Short answer text

4. Field of Study

Short answer text

5. Level of Education

- ○ Undergraduate
- ○ Graduate
- ○ Postgraduate
- ○ Other

6. How familiar are you with cybersecurity threats?

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very familiar

7. Have you ever participated in an interactive cybersecurity exercise (e.g., simulations, gamified challenges)?

- ○ Yes
- ○ No

8. How confident are you in recognizing and responding to cybersecurity threats?

	1	2	3	4	5	
Not confident at all	○	○	○	○	○	Very confident

9. What cybersecurity habits do you currently practice? *(Select all that apply)*

- [ ] Using strong passwords
- [ ] Enabling multi-factor authentication (MFA)
- [ ] Avoiding suspicious links
- [ ] Keeping software and operating systems updated
- [ ] None of the above

10. Do you think interactive and gamified training methods improve engagement?

- ○ Yes
- ○ No

11. What are your expectations for a gamified cybersecurity training program? *(Choose one or more)*

- ○ More engagement compared to traditional training
- ○ Better knowledge retention
- ○ Fun and competitive learning environment
- ○ More hands-on experience

12. What are your expectations for an ideal gamified cybersecurity training experience? *(Open-ended response)*

Long answer text

Survey 4: Post-Training (Gamified Group)

Objective: To assess the effectiveness of gamified training compared to traditional methods.

1. Age

Short answer text

2. Gender

- ○ Male
- ○ Female
- ○ Prefer not to say

3. Country/Region

Short answer text

4. Field of Study

Short answer text

5. Level of Education

- ○ Undergraduate
- ○ Graduate
- ○ Postgraduate
- ○ Other

6. How would you rate your understanding of cybersecurity after the training?

	1	2	3	4	5	
No improvement	○	○	○	○	○	Significant improvement

7. Did the gamified approach make the training more engaging?

- ○ Yes
- ○ No

8. How confident are you in recognizing and responding to cyber threats after this training?

	1	2	3	4	5	
Not confident at all	○	○	○	○	○	Very confident

9. Which cybersecurity practices will you now implement regularly? *(Select all that apply)*

- [ ] Using strong passwords
- [ ] Enabling multi-factor authentication (MFA)
- [ ] Avoiding suspicious links
- [ ] Keeping software and operating systems updated
- [ ] None of the above

10. Do you think gamified training improved your ability to retain cybersecurity concepts?

- ○ Yes
- ○ No

11. How likely are you to recommend gamified training over traditional training?

	1	2	3	4	5	
Not likely at all	○	○	○	○	○	Very likely

12. What aspects of the gamified training were most effective, and what could be improved? *(Choose one or more)*

- ○ Interactive challenges and simulations
- ○ Competitive leaderboard system
- ○ Real-world scenario-based learning
- ○ More flexibility in training modules
- ○ No improvements needed

13. What aspects of the gamified training were most effective, and what could be improved? *(Open-ended response)*

Long answer text