American Journal of Engineering Research (AJER) **2026**
American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN: 2320-0936
Volume-15, Issue-8, pp-61-67
www.ajer.org
Research Paper Open Access

User Awareness Training Platform on Windows Bitlocker Security

Mubarak Olayiwola Ahmed[1] and Hammed Olajide Jimoh[2]
[1]*Cisco Nigeria Limited, Lagos,*
[2]*Department of Cybersecurity and Data Protection, Federal Polytechnic, Offa,*

ABSTRACT
Windows BitLocker uses a Trusted Platform Module (TPM) chip, embedded on every system motherboard, to improve security by sealing encryption keys until the system boots securely. Despite Windows BitLocker's strong AES-256 encryption, its effectiveness is often undermined by low user awareness, as seen in disabled encryption, insecure recovery key storage, and overreliance on TPM-only mode. This paper is a web-based interactive awareness and assessment platform to address these issues. Developed using Python (Flask), React.js, and PostgreSQL, the system integrates cybersecurity tools: OpenVAS and Nmap to scan for potential BitLocker-related vulnerabilities, such as misconfigurations and weak endpoint security. It delivers scenario-based modules on BitLocker setup, secure configuration (e.g., PIN + TPM), and recovery key management without collecting sensitive data. The platform effectively improved BitLocker awareness and adoption by combining technical vulnerability assessment with user-centred education. Findings confirm that integrating automated security scanning with behavioural training enhances overall BitLocker resilience, particularly in resource-constrained environments such as Nigerian institutions.

Keywords*: BitLocker, full-disk encryption, user awareness, cybersecurity tools, PIN, TPM, cybersecurity education.*

Date of Submission: 17-08-2026 Date of acceptance: 31-08-2026

I. Introduction

The exponential growth of digital information in recent decades has transformed data into one of the most valuable organizational assets. As enterprises and individuals increasingly rely on mobile computing devices such as laptops and tablets, the risks associated with data breaches and unauthorized access have intensified. A stolen or lost device can expose sensitive personal or corporate information, resulting in financial losses, reputational damage, and regulatory penalties. To mitigate these risks, full-disk encryption has emerged as a critical safeguard, ensuring that data remains protected even if physical devices fall into the wrong hands. Microsoft's BitLocker was first introduced in Windows Vista and has been significantly improved in subsequent versions of Windows. It is one of the most widely deployed full-disk encryption solutions [1]. BitLocker integrates tightly with the Windows operating system to provide drive encryption using the Advanced Encryption Standard (AES), protecting data against offline attacks. When combined with Trusted Platform Module (TPM) chips, BitLocker can enforce pre-boot integrity checks, ensuring that devices have not been tampered with before unlocking encrypted volumes [2]. Much research has shown that properly configured BitLocker implementations significantly reduce the risk of data exposure following theft or loss of a device [3]. However, encryption technologies alone cannot fully eliminate security risks; their effectiveness depends on proper and strict configuration, consistent usage, and user compliance.

User awareness is often cited as the weakest link in information security [4]. While technical measures such as BitLocker provide strong cryptographic guarantees, human factors, including ignorance of the technology, failure to enable encryption, or improper key management, can undermine security. Several projects on BitLocker indicate that many organizations deploy them but fail to enforce robust key storage policies, leaving recovery keys unprotected and thus weakening the intended protection [5]. This demonstrates the need for not only technical

enforcement but also comprehensive awareness training to ensure that end users understand the role of encryption, recognize their responsibilities, and comply with best practices. Training interventions in cybersecurity have proven effective in improving user behaviour. For example, security awareness programs targeting phishing susceptibility have reduced successful attacks by over 30% in corporate environments [6]. Similarly, encryption-focused awareness training has been shown to increase compliance with data protection policies, particularly when combined with interactive learning and assessments [7]. By contextualizing security controls such as BitLocker within broader organizational and individual security responsibilities, training fosters a culture of accountability and reduces the probability of misconfiguration or neglect. In response to this need, online awareness platforms have gained popularity as scalable methods for delivering security training. Such platforms often include instructional modules, practical demonstrations, assessments, and certification of completion. Certifications not only reinforce knowledge retention but also provide organizations with evidence of compliance in audits and regulatory reviews [8]. An awareness training system specifically dedicated to Windows BitLocker thus provides a timely and necessary intervention in the fight against data breaches, aligning technical safeguards with user responsibility.

II. Review of Related Work

Current Research on Cybersecurity Awareness Training Efficacy

Contemporary research suggests a consensus that traditional, compliance-oriented training, typically consisting of static presentations or annual modules, produces negligible behavioural change. More effective models employ interactive, scenario-based, and context-aware learning techniques that simulate real-world cyber threats [9]. Organizations utilizing such dynamic training approaches report measurable reductions in policy violations and incident recurrence over time. For instance, longitudinal assessments indicate a 42% decrease in risky behaviours within twelve months of adopting interactive awareness interventions. This improvement is attributed to experiential learning mechanisms that strengthen threat recognition and procedural memory. Further research demonstrates that "just-in-time" microlearning delivered at the moment of potential error, such as when a user handles an encryption key, significantly improves retention and operational application [10]. These findings challenge the notion of one-off annual training, suggesting instead that awareness should be woven into daily workflows through adaptive learning technologies.

User Behaviour in Managing BitLocker Recovery Keys

The intersection of usability and security remains one of the most persistent paradoxes in cybersecurity design. Decades of research demonstrate that even knowledgeable users struggle with cryptographic tools due to poor interface design, abstract terminology, and cognitive overload [11]. In the case of BitLocker, users frequently conflate recovery keys with standard credentials, storing them in plaintext or easily accessible locations such as email drafts or shared notes [12]. Empirical investigations into user behaviour reveal that mismanagement of recovery keys is a systemic vulnerability. Many users perceive recovery keys as *administrative inconveniences* rather than critical cryptographic elements, leading to high-risk behaviours such as storing them on local drives or in unsecured cloud services [14]. This negligence effectively creates alternative, unencrypted access channels that compromise BitLocker's protections. The issue is compounded by inadequate system feedback; users receive no meaningful warnings or contextual guidance regarding insecure key storage. Awareness programs must therefore go beyond procedural instruction to reshape mental models, framing the recovery key as a master cryptographic credential rather than a secondary password. Incorporating behavioural insights and interactive design elements into BitLocker's interface could drastically reduce mismanagement rates, reinforcing security through cognitive alignment rather than external enforcement [15].

Review of Methodologies for Measuring Security Training Effectiveness

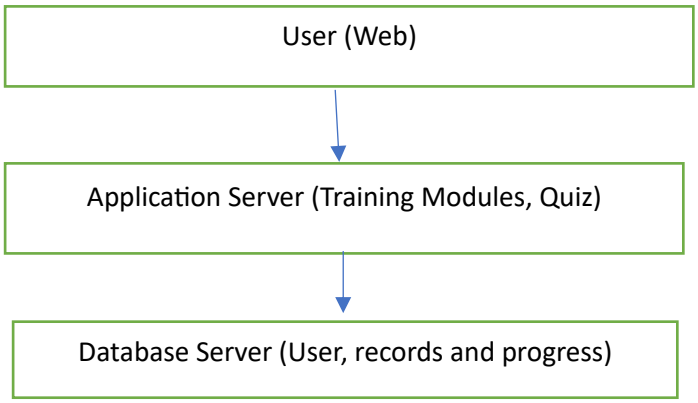
Evaluating security awareness effectiveness demands metrics that move beyond training completion rates. A comprehensive measurement model integrates knowledge retention assessments with behavioural telemetry, such as BitLocker enablement rates, recovery key escrow compliance, and response to simulated threats [16]. This dual-metric framework aligns with established evaluation hierarchies; however, it introduces cybersecurity-specific dimensions linking human knowledge to observable technical outcomes. Temporal analysis also reveals that behavioural adherence diminishes over time without reinforcement. Continuous engagement, periodic refreshers, and just-in-time reminders are therefore critical to sustaining long-term compliance [9]. These insights highlight that effective security awareness must operate as an iterative process, evolving alongside user experience and emerging threat landscapes.

Nmap & OpenVAS for BitLocker Vulnerability Scanning

Nmap (Network Mapper) is an open-source network discovery and security-auditing tool widely used for host discovery, port enumeration, service/version detection, and TCP/IP stack fingerprinting. Its core strength is fast, flexible network enumeration using multiple scanning techniques and the Nmap Scripting Engine (NSE), which enables custom probes and basic vulnerability checks or automation tasks. Nmap outputs (open ports, service versions, OS fingerprints) commonly serve as the foundational reconnaissance stage for deeper vulnerability assessment and penetration testing. [8]. Moreso, OpenVAS (Open Vulnerability Assessment System) is part of the Greenbone Vulnerability Management ecosystem, a dedicated and full-featured automated vulnerability scanning framework that performs authenticated and unauthenticated checks against hosts and services using a regularly updated feed of vulnerability tests. It automates CVE checks, configuration audits, and produces detailed reports and remediation guidance. OpenVAS is designed for comprehensive vulnerability detection across a network and is optimized for systematic scanning and large-scale assessments; it is therefore used where in-depth vulnerability enumeration and prioritized remediation data are required [17]. In practice, Nmap and OpenVAS are often used together: Nmap provides fast discovery and service/version details, which can be fed into OpenVAS to refine scanning targets or to reduce scan scope and false positives. Several comparative studies and applied research recommend a layered approach, where Nmap is used for discovery and surface mapping, typically called manual scanning. Then, the application of an automatic vulnerability scanner like OpenVAS or Nessus for vulnerability detection and verification. This combined workflow improves efficiency and coverage in security assessments. Nmap's advantages are speed, flexibility, deep protocol-level probing, and extensibility via NSE; its limitations are that it does not maintain an authoritative vulnerability database and can miss configuration-level or authenticated issues that a full vulnerability scanner would catch. OpenVAS excels at systematic CVE detection, authenticated scanning, and reporting, but it can be heavier on resources, dependent on frequent feed updates, and may require more configuration and tuning to avoid false positives or performance bottlenecks in large environments [12]. Together, they form a practical, cost-effective open-source toolchain for reconnaissance and vulnerability assessment.

III. METHODOLOGY

The application is an interactive, user-friendly, web-based training and assessment platform, designed to enhance user awareness and promote practical knowledge of Windows BitLocker security. In addition to educational modules, the platform is preloaded with the Kali Linux operating system, on which Nmap and OpenVAS will be used to perform manual and automated vulnerability scans to help users identify potential security weaknesses related to BitLocker deployment and device configuration. The system provides interactive tutorials, simulations, and self-assessment quizzes that educate users on the importance of data encryption, secure BitLocker setup, and safe recovery key management. Nmap is integrated to perform host discovery and network reconnaissance, identifying connected systems and open ports that may expose encryption-related risks. OpenVAS complements this by conducting in-depth vulnerability assessments, scanning for misconfigurations, outdated security policies, and potential attack vectors affecting BitLocker-protected systems.



The figure above shows the system architecture of the interaction between users, the application server, and the database. Users access the platform through a web browser, while the application server processes user requests and communicates with the database to retrieve or store information.

System Design

The system design phase outlines some fundamental key components of the platform. The phases convert the conceptual analysis into a more practical model for implementation. The phases include: architectural framework, data flow, and functional components. Furthermore, the system was designed to explain how to understand the functionality, feasibility, and contribution to improving encryption awareness. Critical analysis of the system identifies its objectives, components, and the expected impact on user behaviour towards BitLocker usage. The primary objective is to simplify BitLocker education for non-technical users. By providing interactive demonstrations, users can learn step-by-step processes without relying on complex documentation. The analysis revealed that users often neglect encryption due to perceived complexity. Hence, a hands-on platform offering practical engagement increases adoption and retention rates. A key aspect of the design was evaluating system security and usability. The platform ensures that no classified data, such as recovery keys or passwords, is collected. Instead, it focuses solely on educational interactions. However, usability testing revealed that an intuitive interface with simplified navigation enhances participation, particularly for beginners unfamiliar with cybersecurity tools. From a feasibility perspective, the proposed system is achievable using readily available web technologies, including HTML, CSS, JavaScript, Python, and Django; a full-stack framework. However, the administrator side utilizes Nmap and OpenVAS to scan for BitLocker vulnerabilities. The hosting environment would be a secure cloud-based server with SSL encryption for data protection.

Architectural Framework: The system architecture follows a three-tier model that comprises the presentation, application logic, and database layer. The presentation layer contains the user interface where learners interact with the system. The application layer processes inputs, controls module flow, and handles logic for quizzes and progress tracking. The database layer stores user information, learning records, and results.

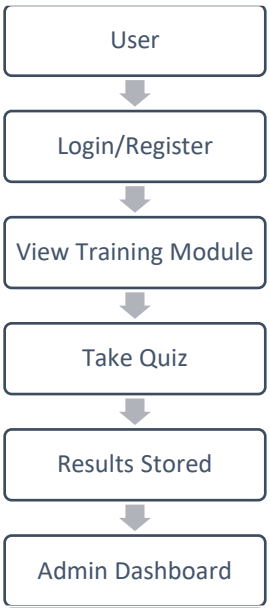


Figure 2: Data Flow Diagram

The figure above illustrates the flow of data through the system, from user authentication to result storage and administrative reporting.

Database Design: The database was designed to ensure data consistency, security and ease of retrieval. It consists of entities such as Users, Modules, Quizzes, and results. Each of the attributes in the Entity Relationship table is related through primary and foreign keys to maintain relational integrity. The database was implemented using PostgreSQL.

Backend Development

The backend was implemented using Python's Flask framework to handle server-side operations, API connections, and database interactions. Functions were written to manage user authentication, module progress, and quiz submission. SQL Alchemy ORM was used to connect the system to the PostgreSQL database

Frontend Development

The frontend interface was developed using HTML, CSS, and Bootstrap to ensure responsiveness and aesthetic presentation. React.js was used to enhance interactivity, allowing users to navigate between modules and quizzes seamlessly.

Scanning

The module for vulnerability scanning was implemented using Nmap for host discovery and OpenVAS for subsequent vulnerability scanning of the target host or IP address

System Operation

When users access the platform, they first register (if they are new) or log in (existing applicants) using secure credentials. Upon login, they can navigate through modules that include videos and interactive lessons. After completing each module, a short quiz assesses comprehension. Results are automatically recorded in the database and displayed on the user's dashboard. Administrators can generate reports to assess training participation and progress.

IV. RESULTS

After implementing each module, the system components were integrated. The backend was linked to the frontend through RESTful APIs, ensuring real-time synchronization between the interface and stored data. The user is displayed with a log in interface as shown below

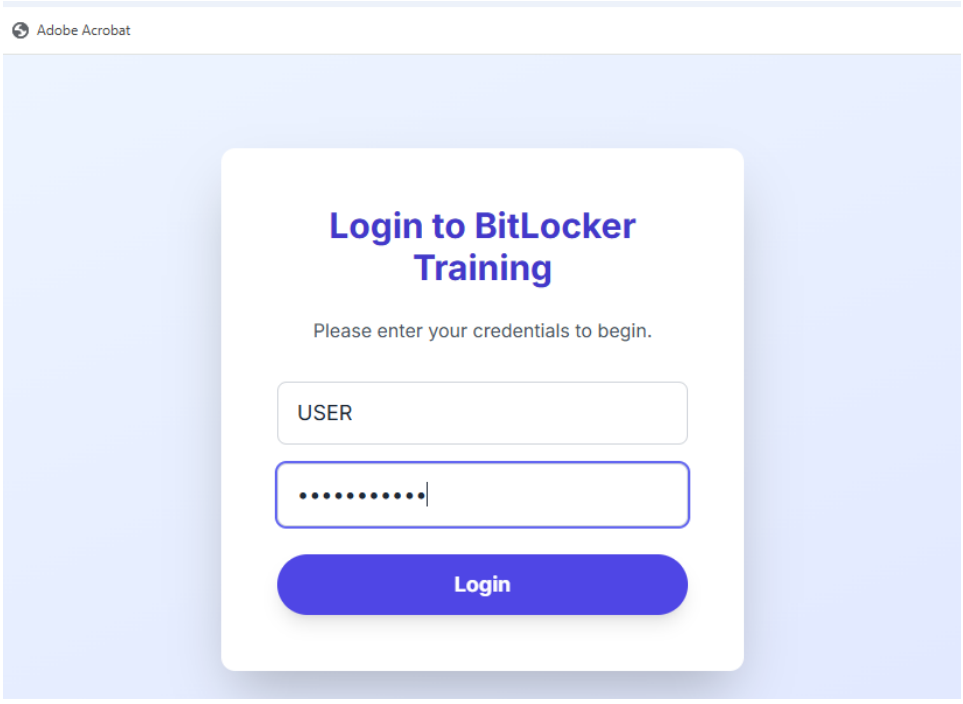


Figure 3: Log in Page

From the figure above, the users will have to log in with their required credentials, after which they are welcomed with a dashboard as shown in Figure 4, which presents available training modules on BitLocker concepts. The system allows users to view educational videos, read security instructions, and attempt quizzes to test their understanding. Upon completion, certificates of participation are automatically generated.

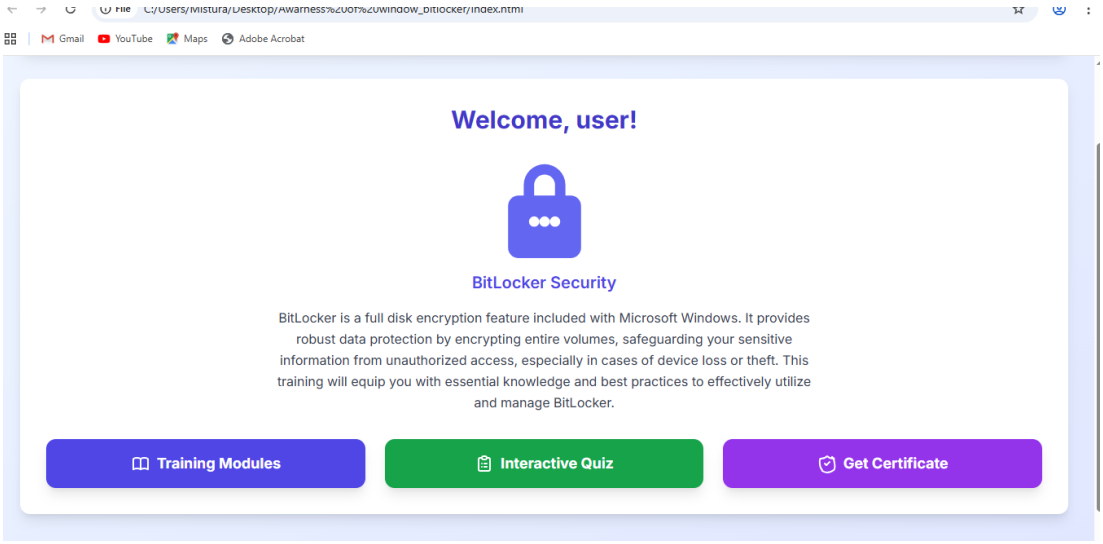


Figure 5: User Dashboard Showing Training Modules

From the above, the user can choose to commence the training by clicking on the training modules or have a glance on the quiz. After completion of the training modules and Quiz, a certificate will be presented and can be downloaded using the "Get Certificate" tab.

V. CONCLUSION

This paper conclusively demonstrates that cryptographic strength alone is insufficient for data security; human behaviour is the decisive factor. BitLocker's vulnerabilities are not in its algorithm, but in its *usage*: TPM-only mode, unscrewed recovery keys, and a lack of user enablement persist due to poor models and inadequate security requirements. The developed platform proves that interactive, just-in-time training grounded in behavioural theory and usability principles can bridge this gap. By reframing security as a learnable skill rather than a compliance checkbox, the system fosters self-efficacy and sustained behaviour change. Crucially, the architecture ensures privacy and scalability, making it viable for institutions with limited IT support especially in Nigerian higher institutions or SMEs. Thus, effective encryption governance must integrate technical controls, process design, and user capability development in equal measure.

REFERENCE

[1] D. Grebennikov, "Windows BitLocker drive encryption: A new security feature in Windows Vista," Digital Investigation, vol. 3, no. 2, pp. 128–136, Jun. 2006.
[2] J. Chen and C. A. Shue, "BitLocker: A comparative analysis of Windows full disk encryption," Proc. Int. Conf. Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Oxford, UK, Jun. 2019, pp. 1–8.
[3] A. Pettersen and K. Sanderud, "Evaluating security of full disk encryption solutions on Windows platforms," Journal of Information Security and Applications, vol. 53, pp. 1–10, Feb. 2020.
[4] M. Chiew, K. C. Tan, and C. S. Wong, "A survey of phishing attacks: Their types, vectors and technical approaches," Expert Systems with Applications, vol. 106, pp. 1–20, Sep. 2018.
[5] P. Heaslip, A. Behm, and J. S. Ferguson, "Practical risks in enterprise deployment of BitLocker full disk encryption," Computers & Security, vol. 85, pp. 110–120, Jul. 2019.
[6] A. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," Computers & Security, vol. 98, pp. 1–16, Dec. 2020.
[7] J. Furnell and N. Clarke, "Organizational security culture: Embedding security awareness, education, and training," Information Management & Computer Security, vol. 20, no. 4, pp. 239–254, 2012.
[8] S. Parsons, A. Calic, and M. Pattinson, "The effectiveness of security awareness training in reducing risky behavior: Evidence from experiments," Computers & Security, vol. 106, pp. 1–15, Sep. 2021.
[9] A. Vishwanath, B. Harrison, and Y. J. Ng, "The impact of training modality on phishing susceptibility: A field experiment," Comput. Secur., vol. 102, p. 102157, Mar. 2021.
[10] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," Telematics Inform., vol. 34, no. 1, pp. 119–127, Feb. 2017.
[11] Whitten, A., & Tygar, J. D. (1999, August). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In USENIX security symposium (Vol. 348, pp. 169-184).
[12] S. Ruoti, J. Andersen, T. Dickinson, M. O'Neill, and K. Seamons, "'I don't understand what I'm supposed to do': User challenges with BitLocker," in Proc. ACM CHI Conf. Hum. Factors Comput. Syst., 2019, pp. 1–13.
[13] Furnell, S. (2016). The usability of security–revisited. Computer Fraud & Security, 2020(9), 5-11.

[14] K. Krol, Y. Moroz, and M. A. Sasse, "'It's just a number': User perceptions of BitLocker recovery keys," in Proc. Symp. Usable Privacy Secur. (SOUPS), 2020, pp. 231–248.
[15] He, P., Zhou, Y., & Qin, X. (2024). A survey on energy-aware security mechanisms for the internet of things. Future Internet, 16(4), 128.
[16] D. D. Caputo, S. L. Pfleeger, and J. D. Freeman, "Beyond click rates: Measuring the effectiveness of security awareness training using behavioral analytics," IEEE Secur. Privacy, vol. 20, no. 3, pp. 45–53, May 2022.
[17] 12] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Upper Saddle River, NJ, USA: Pearson, 2021.