International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-4 || Oct – Dec 2026 || PP. 1 – 7
https://ijcscer.org

Cybersecurity Threats in Online Education Platforms

S. Venkatasubramanian

Associate Professor

Computer Science And Business Systems

Saranathan College Of Engineering

Trichy, Tamilnadu, India

Orcid Id: https://orcid.org/0000-0001-7560-0164

http://www.ijcscer.org/ || Vol. 3 No. 4 (2026): October Issue

Date of Submission: 03-09-2026 **Date of Acceptance:** 16-09-2026 **Date of Publication:** 04-10-2026

Abstract— Online education platforms now hold identity records, assessment data, and payment information for very large learner populations, which makes them attractive targets for attackers. This study examines the prevalence, distribution, and drivers of cybersecurity threats across 18 online education platforms using a convergent multi-source design. Twelve months of confirmed incident records (1,486 incidents), a vulnerability assessment aligned with the OWASP Top 10, and a survey of 312 students, instructors, and IT staff were analyzed. Phishing and credential-based attacks accounted for half of all incidents (50.0%). Platforms enforcing multi-factor authentication (MFA) recorded a mean of 8.0 account takeover incidents, compared with 25.0 for platforms without it ($p < .001$). Incident experience differed by user role, $\chi^2(2) = 10.99$, $p = .004$. Password reuse was associated with higher odds of reporting an incident (OR = 2.14), whereas recent security training was associated with lower odds (OR = 0.58). Incidents peaked at the start of term and during assessment periods. The findings indicate that identity and human factors, rather than novel technical exploits, drive most exposure, and that enforced MFA, centralized logging, and tested response plans offer the clearest measurable benefit.

Keywords: online education platforms, cybersecurity threats, phishing, account takeover, multi-factor authentication, learning management systems, vulnerability assessment

Introduction

Online education has moved from a supplementary delivery channel to core infrastructure for schools, universities, and professional training providers. Learning management systems (LMS), massive open online course (MOOC) providers, video conferencing tools, and remote assessment services now process identity records, academic results, payment details, and behavioral data for large user populations. The rapid expansion of these services during and after the COVID-19 pandemic widened the attack surface faster than many institutions could adapt their security governance (Lallie et al., 2021; Pranggono & Arabo, 2021).

Education is attractive to attackers for reasons that differ from those in finance or healthcare. Platforms must remain open and easy to use for diverse and often inexperienced users, rely on decentralized administration, and hold valuable personal and research data while operating with limited security budgets (Ulven & Wangen, 2021). Industry evidence reflects the consequences: a 2024 survey of 600 education-sector IT and cybersecurity leaders found that 66% of higher education

@2026. This is an open access article distributed under the terms of the Creative Commons License [CC BY NC 4.0] and is available on www.ijcscer.org

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-4 || Oct – Dec 2026 || PP. 1 – 7
https://ijcscer.org

organizations had been hit by ransomware in the preceding year (Sophos, 2024).

Despite this exposure, empirical research that combines objective incident data with user-level evidence remains scarce. Ulven and Wangen (2021) concluded that empirical studies of cybersecurity risk in higher education are limited, and much of the available evidence relies on single-institution surveys or vendor reports. Few studies connect measured incident patterns with platform-level control choices and with the behaviors of the people who use these platforms.

This study addresses that gap by examining 18 online education platforms through three complementary lenses: twelve months of confirmed incident records, a structured vulnerability assessment, and a survey of 312 learners, instructors, and IT staff. It makes three contributions. It quantifies the distribution and timing of threats, it estimates the association between specific controls and incident outcomes, and it identifies user-level factors linked to incident experience. The remainder of the paper reviews related work, states the research questions and hypotheses, describes the methodology, reports results, and discusses implications and limitations.

Literature Review

Threat landscape in education

Large-scale incident reports consistently show that the human element and stolen credentials are central to breaches. The 2024 Verizon Data Breach Investigations Report found that 68% of breaches involved a non-malicious human element, such as a person falling for a social engineering attack or making an error (Verizon, 2024). In education specifically, the Cybersecurity and Infrastructure Security Agency and its partners warned that the Vice Society ransomware group had disproportionately targeted the education sector (CISA et al., 2022). Sophos (2024) reported that 66% of surveyed higher education organizations had experienced ransomware in the previous year, which suggests the threat is persistent rather than episodic.

Online learning and pandemic-era exposure

After the pandemic-driven shift to remote delivery, cloud services, learning platforms, and video conferencing became primary assets for higher education. Alexei and Alexei (2021) identified the classes of attack with the greatest effect on these assets and recommended patch management, access policies, and cryptographic protocols. A questionnaire study of Moldovan institutions found that malware, phishing, and denial-of-service attacks were the dominant threats and resembled those reported internationally (Alexei et al., 2021). Wider analyses of pandemic-era cybercrime documented sharp growth in phishing, malicious domains, and ransomware as organizations moved activity online (Lallie et al., 2021; Pranggono & Arabo, 2021).

Systematic evidence and assessment integrity

Ulven and Wangen (2021) synthesized the higher education cybersecurity literature, proposed a generic threat model, and derived nine strategic cyber risks, while noting that empirical research was scarce despite a high level of agreement among sources about the main issues. Their conclusion motivates studies that measure, rather than only catalogue, risk. Remote examinations add threats beyond confidentiality. Hussein et al. (2020) evaluated online proctoring tools and highlighted the difficulty of maintaining academic integrity without a live proctor, along with the technical and cost requirements of the tools themselves. Such tools add further components that platform operators must secure.

Human factors and technical controls

Aldawood and Skinner (2019) argued that organizations with strong technical preparations remain vulnerable when staff knowledge of social engineering is low, and they identified recurring pitfalls in training programs. Bada et al. (2019) examined why awareness campaigns often fail to change behaviour, pointing to the gap between knowing about a risk and acting on it. These findings suggest that training alone is an incomplete defense. On the technical side, the OWASP Top 10:2021 ranks broken access control as the leading web application risk category and also lists identification and authentication failures and security logging and monitoring failures (OWASP Foundation, 2021). NIST digital identity guidance defines authentication assurance levels and requires multi-factor authentication at higher levels (Grassi et al., 2017).

Taken together, the literature establishes the main threat classes and the importance of human factors, yet it offers little quantitative evidence linking platform-level controls to measured incident counts across multiple education platforms. The present study responds to this gap.

Research Questions and Hypotheses

Three research questions guided the study. RQ1: What is the distribution and timing of confirmed cybersecurity incidents across online education platforms? RQ2: Which technical vulnerabilities and control gaps are most prevalent? RQ3:

@2026. This is an open access article distributed under the terms of the Creative Commons License [CC BY NC 4.0] and is available on www.ijcscer.org

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-4 || Oct – Dec 2026 || PP. 1 – 7
https://ijcscer.org

Which platform-level and user-level factors are associated with incident outcomes? Four hypotheses followed from the literature.

H1: Phishing and credential-based attacks together account for at least half of confirmed incidents. H2: Platforms that enforce MFA record fewer account takeover incidents than platforms that do not. H3: Incident experience differs by user role. H4: Password reuse is associated with higher odds, and security awareness training with lower odds, of reporting an incident.

Methodology

Research design

A convergent multi-source design was used. Three quantitative data sources (security incident records, a vulnerability assessment, and a user survey) were collected over the same period and analyzed separately before being integrated during interpretation. Figure 1 presents the conceptual framework that guided variable selection: threat actors use attack vectors against platform assets, and vulnerabilities, human factors, and defensive controls shape the resulting outcomes.

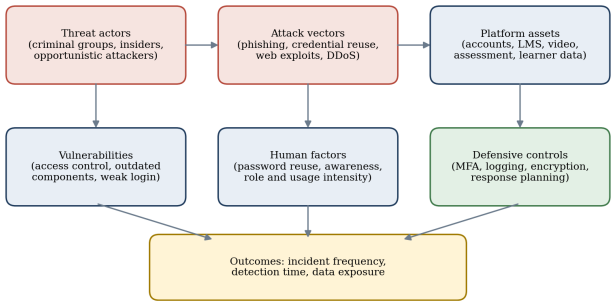


Figure 1. Conceptual framework of threats, vulnerabilities, human factors, and controls in online education platforms.

Platforms and incident data

Eighteen platforms were selected through purposive sampling to cover different delivery models: eight institutional LMS deployments, six MOOC or course-marketplace platforms, and four assessment and tutoring platforms. Operators provided incident records for January to December 2025. An incident was counted only when a platform security team confirmed it as a security event with a documented impact or containment action; unverified alerts were excluded. Incidents were classified into eight categories using a common taxonomy agreed with the security teams, and detection time was measured in hours from the earliest log evidence to confirmed detection.

Vulnerability assessment

Each platform underwent a non-intrusive assessment covering seven OWASP Top 10:2021 categories that can be evaluated from externally observable configuration and application behavior, supplemented by a structured checklist of defensive controls. A platform was recorded as having a category finding if at least one confirmed issue was present. The absence of enforced MFA, centralized logging, or encryption at rest was recorded as a finding in the authentication, logging, and cryptographic categories, respectively.

Survey instrument and sample

A structured questionnaire was distributed between January and March 2026 to 400 invited users drawn from the participating platforms, yielding 312 complete responses (78.0% response rate). Respondents were 186 students, 84 instructors, and 42 IT or security staff (Table 1). The instrument captured self-reported security incidents in the previous 12 months, clicking on suspicious links, password reuse, security awareness training, weekly platform use, and perceived severity of seven threat types on five-point scales (1 = not severe, 5 = extremely severe). The severity scale showed good internal consistency (Cronbach's α = .87), and the instrument was piloted with 20 respondents before distribution.

Table 1. Survey sample characteristics and reported incident experience (N = 312)

Role	n	% of sample	Weekly platform use (h), M (SD)	Reported incident, n (%)
Students	186	59.6	16.9 (6.8)	77 (41.4)
Instructors	84	26.9	12.9 (5.4)	31 (36.9)
IT / security staff	42	13.5	9.1 (4.7)	28 (66.7)
Total	**312**	**100.0**	**14.8 (6.8)**	**136 (43.6)**

Ethical considerations and data handling

Participation was voluntary, informed consent was obtained, and survey responses were anonymized. Platform operators supplied incident records under confidentiality agreements, and platform identities were coded to prevent identification.

@2026. This is an open access article distributed under the terms of the Creative Commons License [CC BY NC 4.0] and is available on www.ijcscer.org

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-4 || Oct – Dec 2026 || PP. 1 – 7
https://ijcscer.org

Data analysis

Descriptive statistics summarized incident counts, vulnerability prevalence, and control adoption. Chi-square tests compared proportions across user roles. Because platform-level samples were small, MFA groups were compared with Welch's t-test, and Cohen's d was reported as an effect size. Detection times, which were right-skewed, were compared using the Mann–Whitney U test. A binary logistic regression modeled the odds of reporting an incident, with role, password reuse, security training, and weekly platform use as predictors. The significance level was set at α = .05, and all analyses were run in Python using SciPy and statsmodels.

Results

Incident profile

The 18 platforms recorded 1,486 confirmed incidents in 2025, a mean of 82.6 per platform. Phishing and social engineering accounted for 412 incidents (27.7%) and credential stuffing and account takeover for 331 (22.3%). Together these identity-centered categories represented 743 incidents (50.0%), which supports H1. Malware and ransomware (12.6%) and distributed denial-of-service (DDoS) attacks (11.8%) followed (Table 2; Figure 2). The median detection time across all incidents was 11.3 hours, but it varied widely: DDoS attacks were detected in 0.4 hours, whereas data exfiltration required 96.5 hours.

Table 2. Confirmed incidents by category and median detection time (N = 1,486)

Incident category	n	%	Median detection time (h)
Phishing / social engineering	412	27.7	6.5
Credential stuffing / account takeover	331	22.3	18.4
Malware / ransomware	187	12.6	3.2
DDoS	176	11.8	0.4
Web application exploits	154	10.4	52.0
Data exfiltration	118	7.9	96.5
Exam integrity attacks	71	4.8	30.0
Session hijacking	37	2.5	1.5
Total	**1,486**	**100.0**	**11.3**

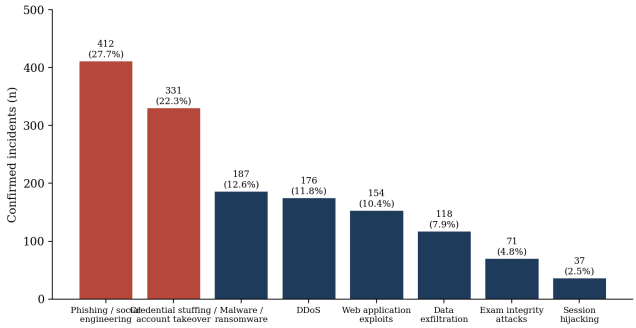


Figure 2. Distribution of confirmed incidents by category across 18 platforms, January to December 2025.

Temporal pattern

Monthly incident counts ranged from 85 in December to 162 in September (M = 123.8, SD = 22.9). The three highest months, September (162), May (152), and November (142), contained 456 incidents (30.7%) and coincide with the start of term and assessment periods (Figure 3).

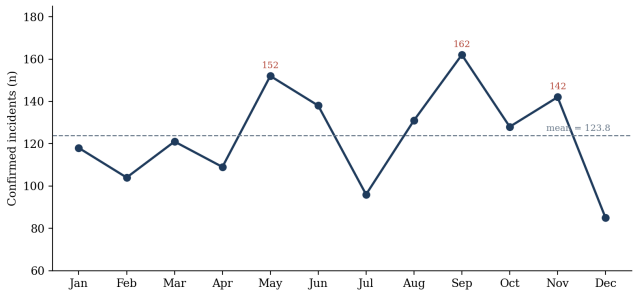


Figure 3. Monthly confirmed incidents across all platforms, 2025.

Vulnerabilities and control adoption

Broken access control was the most common finding (14 platforms, 77.8%), followed by vulnerable and outdated components (13 platforms, 72.2%) and security misconfiguration (12 platforms, 66.7%) (Table 3). Control adoption was uneven (Table 4). TLS 1.2 or higher was universal, but only 7 platforms (38.9%) enforced MFA for all users and only 6 (33.3%) had tested their incident response plan in the previous 12 months. The 11 platforms with authentication findings were those without enforced MFA, the 10 with logging findings lacked centralized logging, and the 6 with cryptographic findings lacked encryption at rest.

Table 3. Vulnerability findings by OWASP Top 10:2021 category (18 platforms)

Category	Platforms, n	%
Broken access control	14	77.8

@2026. This is an open access article distributed under the terms of the Creative Commons License [CC BY NC 4.0] and is available on www.ijcscer.org

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-4 || Oct – Dec 2026 || PP. 1 – 7
https://ijcscer.org

Vulnerable and outdated components	13	72.2
Security misconfiguration	12	66.7
Identification and authentication failures	11	61.1
Security logging and monitoring failures	10	55.6
Injection	9	50.0
Cryptographic failures	6	33.3

Table 4. Adoption of defensive controls (18 platforms)

Control	Platforms, n	%
TLS 1.2 or higher for all traffic	18	100.0
Encryption at rest	12	66.7
Security awareness training for staff	12	66.7
Web application firewall	10	55.6
Penetration testing at least annually	9	50.0
Centralized logging / SIEM	8	44.4
MFA enforced for all users	7	38.9
Incident response plan tested in past 12 months	6	33.3

Effect of multi-factor authentication

Platforms enforcing MFA (n = 7) recorded a mean of 8.0 account takeover incidents (SD = 2.9), compared with 25.0 (SD = 8.4) for platforms without MFA (n = 11), Welch's $t(13.3) = 6.16$, $p < .001$, $d = 2.47$ (Figure 4). H2 was supported. Platforms with centralized logging (n = 8) also detected incidents faster, with a median of 7.9 hours versus 19.6 hours for platforms without it (Mann–Whitney U, $p < .001$).

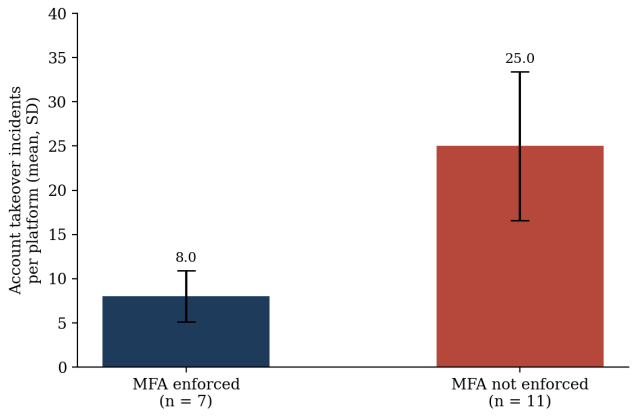


Figure 4. Mean account takeover incidents per platform by MFA enforcement (error bars show SD).

Survey findings

Overall, 136 of 312 respondents (43.6%) reported at least one security incident in the previous 12 months, and the rate differed by role: 41.4% of students, 36.9% of instructors, and 66.7% of IT staff, $\chi^2(2) = 10.99$, $p = .004$, supporting H3. Clicking a suspicious link was reported by 29.0% of students, 21.4% of instructors, and 7.1% of IT staff (overall 24.0%; $\chi^2(2) = 9.42$, $p = .009$). Password reuse across services was reported by 50.6% of respondents (58.1% of students), and 48.1% had received security training in the previous year. Perceived severity was highest for phishing ($M = 4.21$, $SD = 0.82$), data breaches ($M = 4.15$, $SD = 0.85$), and ransomware ($M = 4.08$, $SD = 0.91$), and lowest for session hijacking ($M = 3.11$, $SD = 1.10$) and exam integrity attacks ($M = 3.34$, $SD = 1.07$).

In the logistic regression (Table 5), password reuse (OR = 2.14, $p = .002$) and weekly platform hours (OR = 1.04 per hour, $p = .008$) predicted higher odds of reporting an incident, whereas security training predicted lower odds (OR = 0.58, $p = .034$). IT staff had higher odds than students (OR = 2.87, $p = .004$), while instructors did not differ from students. These results support H4. Model fit was adequate (Hosmer–Lemeshow $p = .54$; Nagelkerke $R^2 = .19$).

Table 5. Logistic regression predicting self-reported incident experience (N = 312)

Predictor	OR	95% CI	p
Role: instructors (vs. students)	0.88	0.50–1.55	0.66
Role: IT / security staff (vs. students)	2.87	1.41–5.84	0.004
Password reuse (yes)	2.14	1.31–3.50	0.002
Security training in past year (yes)	0.58	0.35–0.96	0.034
Weekly platform use (per hour)	1.04	1.01–1.07	0.008

Discussion

The results show that identity-centered attacks dominate the threat profile of online education platforms. Half of all incidents involved phishing or credential-based account takeover, which is consistent with industry evidence on the role of the human element in breaches (Verizon, 2024) and with the prominence of phishing and malware in earlier education-sector studies (Alexei et al., 2021). The temporal pattern suggests that attackers exploit periods when many new or returning users log in and when platforms are under

@2026. This is an open access article distributed under the terms of the Creative Commons License [CC BY NC 4.0] and is available on www.ijcscer.org

operational pressure, so security monitoring may need to be intensified at these points in the academic calendar.

The strongest platform-level finding was the association between enforced MFA and fewer account takeovers. This aligns with guidance that places multi-factor authentication at higher assurance levels (Grassi et al., 2017) and with the OWASP emphasis on authentication failures (OWASP Foundation, 2021). Detection time showed a similar pattern: slow detection of data exfiltration and web application exploits, and faster detection where centralized logging existed, indicate that visibility is a limiting factor even where preventive controls are in place.

User-level results reinforce the importance of behavior. Password reuse was common and strongly associated with incident experience, while training showed a protective but modest association, in line with arguments that awareness programs alone rarely change behaviour reliably (Aldawood & Skinner, 2019; Bada et al., 2019). The higher incident rate among IT staff should be read cautiously, because these respondents have greater visibility into incidents and are more likely to recognize and report them. Exam integrity attacks formed a small share of incidents (4.8%) and received the lowest severity ratings among data-related threats, although this does not diminish the academic concerns raised by remote proctoring research (Hussein et al., 2020).

Practical Implications

Three actions follow from the evidence. First, platforms should enforce MFA for all accounts, since this control was associated with the largest measured reduction in incidents. Second, operators should deploy centralized logging and rehearse incident response, because both address detection and recovery speed. Third, institutions should replace generic training with short, interactive exercises focused on phishing and password hygiene, and should schedule additional monitoring around the start of term and examination periods. Regular reviews of access control and timely patching address the two most common technical findings.

Limitations

Several limitations apply. The platform sample was small (n = 18) and purposive, so platform-level comparisons are exposed to confounding, because platforms that enforce MFA may also invest more in other controls. Confirmed incidents undercount attacks that were never detected. Survey measures were self-reported and cross-sectional, which limits causal interpretation and may introduce recall bias. Findings may not generalize to regions or platform types outside the sample.

Future Research Directions

Future work should use longitudinal designs across a larger and more diverse set of platforms, evaluate controlled interventions such as phishing-resistant authentication and interactive training, and examine emerging threats, including AI-assisted social engineering and attacks on remote proctoring and assessment systems.

Conclusion

This study examined cybersecurity threats across 18 online education platforms using incident records, a vulnerability assessment, and a user survey. Identity-centered attacks accounted for half of all confirmed incidents, incidents peaked around the start of term and assessments, and the most common technical weaknesses were broken access control and outdated components. Enforced MFA was associated with substantially fewer account takeovers, centralized logging with faster detection, and password reuse with higher odds of incident experience. Strengthening authentication, visibility, and user behavior together offers the most practical route to reducing risk in online education.

References

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), 73. https://doi.org/10.3390/fi11030073

Alexei, A., & Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. International Journal of Scientific & Technology Research, 10(3), 128–133.

Alexei, A., Nistiriuc, P., & Alexei, A. (2021). Empirical study of cyber security threats in Moldovan higher education institutions. Proceedings of the 11th International Conference on Electronics, Communications and Computing. https://doi.org/10.52326/ic-ecco.2021/NWC.05

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://arxiv.org/abs/1901.02672

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, & Multi-State Information Sharing and Analysis Center. (2022). #StopRansomware: Vice Society (Joint Cybersecurity Advisory AA22-249A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-249a

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines (NIST Special Publication 800-63-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

@2026. This is an open access article distributed under the terms of the Creative Commons License [CC BY NC 4.0] and is available on www.ijcscer.org

Hussein, M. J., Yusuf, J., Deb, A. S., Fong, L., & Naidu, S. (2020). An evaluation of online proctoring tools. Open Praxis, 12(4), 509–525. https://doi.org/10.5944/openpraxis.12.4.1113

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

OWASP Foundation. (2021). OWASP Top 10:2021. https://owasp.org/Top10/

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2), e247. https://doi.org/10.1002/itl2.247

Sophos. (2024). The state of ransomware in education 2024. https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-education-2024

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

Verizon. (2024). 2024 data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/

IJCSCER.ORG
ISSN: 3143-9748 (US)

@2026. This is an open access article distributed under the terms of the Creative Commons License [CC BY NC 4.0] and is available on www.ijcscer.org