International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February 2026

Cyber security challenges in online education platform

Rupali Prakash Thakare, pthakre645@gmail.com
Shrutika Vikas Patil, shrutikapatil372004@gmail.com
Jagruti Bhagwan Bhoi, jbhoi6771@gmail.com
Affiliation: Maulikayanshu Foundation,Thalner

Abstract –

Online education is widely used today, but it faces many cybersecurity problems. Online learning platforms store personal and academic information, which makes them targets for cyberattacks like phishing, malware, and data theft. This study looks at the cybersecurity problems in online education platforms and how aware users are about online safety.

The study uses survey data to understand user behaviour and security practices. The results show that many users do not follow safe cybersecurity practices, and institutions provide very little security training. Even though users think they use strong passwords, their security habits are not always good.

The study concludes that better security systems, more user awareness, and new technologies like AI and block chain are needed to make online education platforms safe and trustworthy.

Introduction –

Online education is growing quickly and is now used by schools, colleges, and training centers around the world. It allows learning to continue anytime and anywhere, but it also creates new cybersecurity problems. E-learning platforms store personal details, academic records, and financial information, which makes them a common target for cyberattacks. Some of the most common threats include phishing emails, malware, ransomware, data breaches, and unauthorized access to systems. During the COVID-19 pandemic, the sudden increase in online learning led to a rise in cyber-attacks, including DDoS attacks and security weaknesses in popular online classroom tools.

Studies show that many of these problems happen because of weak passwords, poor authentication methods, insecure data storage, and lack of user awareness. Hackers often trick users into clicking harmful links or sharing login details. To reduce these risks, researchers recommend stronger security measures such as multifactor authentication, encryption, AI-based threat detection, and regular security updates. Educating teachers and students about safe online behavior is also important. Improving cybersecurity in online education is necessary to protect user data, ensure smooth learning, and build trust in digital learning systems.

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February 2026

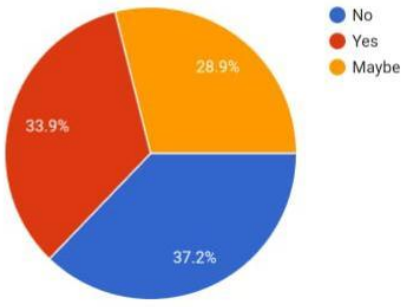
In the future, online education platforms can be made safer by increasing cybersecurity awareness among students and teachers through regular training programs. Using strong passwords, two-factor authentication, and keeping software updated can help reduce cyber risks. Institutions should protect personal and academic data using secure storage and encryption methods, while advanced technologies like AI and block chain can be used to detect and prevent cyberattacks. Clear security policies, safe online habits such as avoiding suspicious links, and quick reporting of security issues will help create a safe, reliable, and trustworthy online learning environment.

Objective –

1. To study the awareness level of cybersecurity practices among students and education using online education platform.
2. To evaluate existing security measures and policies implemented by online education platform.
3. To compare traditional education security risks with online education cybersecurity challenges.
4. To study and analyze the major cybersecurity challenges faced by online education platform and their impact on students, teachers and institutions.
5. To explain why cybersecurity is important.
6. To analyze real-world case studies of cyber attack on online education platform.

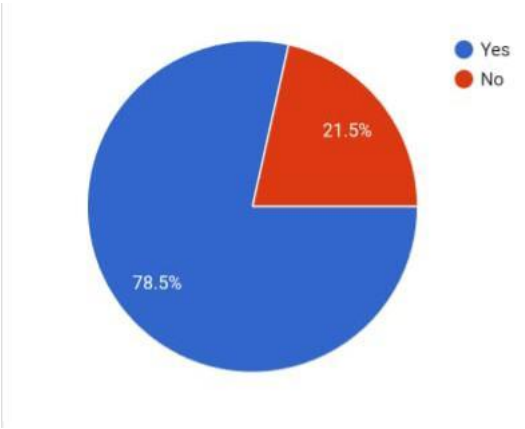
Data Analysis –

1.Are online exam vulnerable to cyber attacks ?

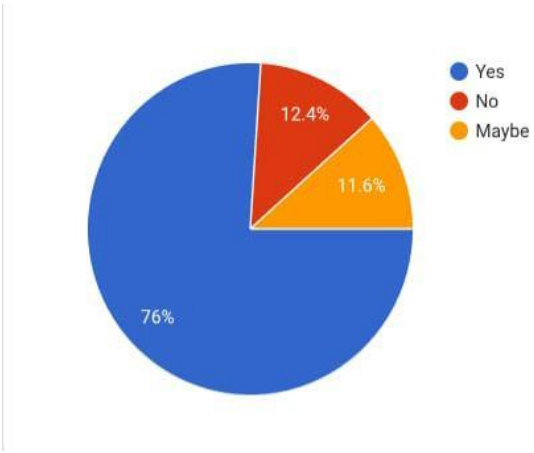


2. Has your institution provided cybersecurity awareness training?

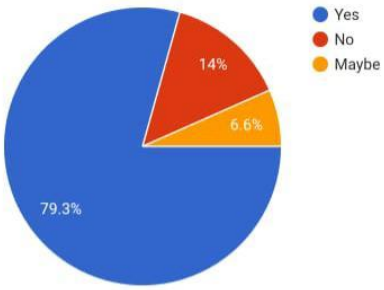
International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February 2026



3.Would you recommend online education platform as secure?

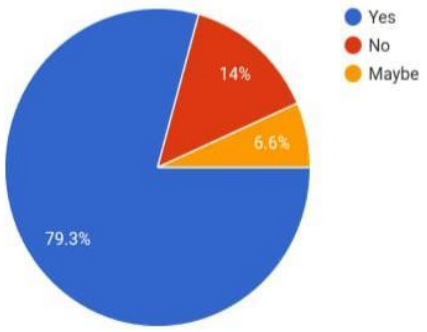


4.Do you enjoy learning online.

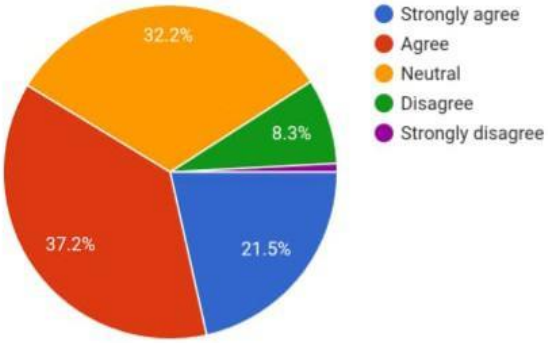


5.Have you ever experienced a cybersecurity?

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February 2026



6.Do you think your personal data is safe on online education platform?



Hypothesis -

H1: Do you use strong password for online learning platform?

This, applying The Formula $x^2=\Sigma(Oi-Ei)^2/Ei$

Here, **Oi**=Observed Frequency (Response collected from survey),

Ei=Expected Frequency(Expected Response)

Method: Chi-square Test

	Oi	Ei	Oi-Ei	$(Oi-Ei)^2$	$(Oi-Ei)^2/Ei$

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February 2026

Always	93	40	53	2809	70.225
Never	13	40	-27	729	18.225
Sometimes	14	40	-26	676	16.900
Total	120	-	-	-	105.35

$\Sigma(Oi-Ei)^2/E=105.35$
Degree of freedom (df)=2
Calculated $x^2=105.35$
Tabulated $x^2= 5.991$
Since 105.35> 5.991

The response is strongly positive. The data shows that a vast majority of the participants (77.5\%) reported that they "Always" use strong passwords for online learning platforms.The result indicates a high level of security awareness and positive behavior among the respondents.

H2: Should cybersecurity be improved in online education platform?
This, applying The Formula $x^2=\Sigma(Oi-Ei)^2/Ei$
Here, **Oi**=Observed Frequency (Response collected from survey),
Ei=Expected Frequency(Expected Response

Method: Chi-square Test

	Oi	Ei	Oi-Ei	$(Oi-Ei)^2$	$(Oi-Ei)^2/Ei$
Strongly agree	45	30.25	14.75	217.56	7.19
Agree	61	30.25	30.75	945.56	31.26
Neutral	15	30.25	-15.25	232.56	7.69
Disagree	0	30.25	-30.25	915.06	30.25
Total	121	-	-	-	76.39

$\Sigma(Oi-Ei)^2/E=76.39$
Degree of freedom (df)=3
Calculated $x^2=76.39$

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
Email: maulikavyanshuijctfs@gmail.com | ISSN No: 3108-1312
Research Today, Future Tomorrow Volume 02 Issue-01 January-February 2026

Tabulated $x^2=7.815$

Since 76.39> 7.815

The response is overwhelmingly positive. Since approximately 87.6% of the respondents fall into the "Strongly Agree" or "Agree" categories, there is a very strong consensus that cybersecurity should be improved on online education platforms

Conclusion:

As per my research we conclude that online education platforms face many security problems like phishing, malware, and data theft. Many users do not know enough about safe online practices, and institutions give very little security training. Even though users think they use strong passwords, their security habits are not always good.

Reference

1. Cybersecurity and Online Education – Risks and Solutions (Z. Sadiqzade, 2025): Examines threats like data breaches, malware, and phishing in e-learning, proposing MFA, AI detection, and blockchain solutions.
2. Cybersecurity Challenges in Educational Information Systems**:** Identifies phishing, malware, and unauthorized access as top risks in digital learning platforms, recommending multifactor authentication and encryption.journal.pandawan
3. Enhancing Cyber Security in E-Learning Portals (2023): Details vulnerabilities in authentication, XSS attacks, data breaches, and phishing, with case studies on recent exploits.
4. Digital Education: The Cybersecurity Challenges in the Online Classroom **(**2019-2020 analysis, pub. 2026): Highlights DDoS surges (up 550% in 2020), malware, and platform-specific issues like Zoom vulnerabilities during COVID.
5. Cybersecurity in Online Learning: Innovations for Teacher Education: Covers malware, ransomware, phishing, DoS, and privacy risks across schools and universities, suggesting innovative mitigations.
6. Overview of Cyber Security in e-Learning Education**:** Discusses authentication failures, availability threats, insecure storage, and internal attacks in distributed e-learning systems.