Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 8, 1527-1532

Research On Solutions To Ensure Information Security For Online Classes In Our Smart Society

Nguyen Tan Danh

Faculty of IT, FPT University, Vietnam.
Corresponding author: DanhNT16@fe.edu.vn

Abstract

Online teaching is the optimal solution during the epidemic season, but even in the process of implementation, this form also raises many unavoidable problems. The lack of consistency and synchronization when implementing online teaching and learning has caused many difficulties for schools, teachers and students. In addition to the quality of transmission lines and technology equipment, many teachers expressed concern about the security of online teaching software. The article focuses on the disadvantages besides the inherent benefits of applying technology. The method used in this article is a qualitative method and the research object is information security. The results show that paying attention to information security is extremely important that we need to consider and have the most appropriate solution.

Keywords: Online teaching, information security, learning, disadvantages.

1. Introduction

In addition to outstanding positive benefits such as no direct contact to avoid disease transmission, elimination of space distances, learning anytime, anywhere, opening learning opportunities for everyone, online learning methods (Mohd Alwi & Fan, 2010). There are also limited risks, especially risks of network information insecurity if appropriate solutions are not applied (Miguel et al., 2013).

In Vietnam, the online teaching method has only really been implemented in the last few years, most strongly when the epidemic is complicated when students can't go to school, both teachers and learners are new to it. almost have not been fully trained in information security knowledge and skills in general, so the issue of information security in online teaching needs to be paid attention to and solved methodically. This will minimize the risks and fully promote the advantages of this advanced learning method, an irreversible learning trend in the future (Hentea et al, 2006).

2. Potential risks regarding using technology during online class

According to a report by Microsoft Security Intelligence in May 2020 only, the percentage of cyberattacks in the education sector was the highest compared to other sectors, accounting for about 61% of the total 7.7 million attacks. According to Kaspersky, in the first 6 months of 2020, the number of DDoS attacks targeting educational resources increased by at least 350% compared to the same period last year (Miguel et al., 2013).

Specifically, in the first quarter of 2020 there were only 131 users in the affected area, in the second quarter of 2020, this number increased to 1,483, equivalent to an increase of 1032%. The number of users who were almost infected with malware in the third quarter was 1,166. Affected apps and tools include Zoom, Google Meet, Google Classroom, etc.

Globally, the total number of DDoS attacks increased by 80% in Q1 2020 compared to Q1 2019. Furthermore, attacks on educational resources accounted for a large share of this

increase. From January to June 2020, the number of DDoS attacks targeting educational resources increased by at least 350% over the same period in 2019. In denial of service (DDoS) attacks, cybercriminals actually overloads the network server with service requests causing the server to crash and stop serving user access requests (Mohd Alwi & Fan, 2010).

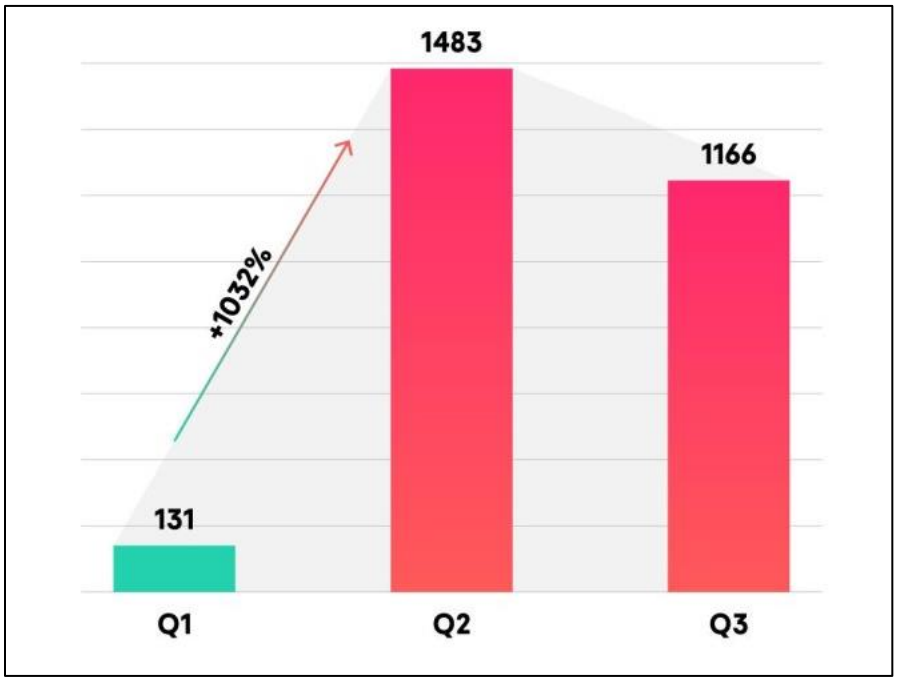

Figure 1. Number of people affected by online learning-related security threats in 2020

The organization of online teaching is mainly based on the capacity and experience of the school's leaders and the fact that there are inefficient online schools due to the limited IT qualifications of principals and vice principals. Due to the lack of training as well as the lack of a curriculum framework and lesson plans, the teachers have to tinker with and create their own teaching methods. Some older teachers cannot keep up with modern software (Kim, 2014).

Previously, the application of IT mainly stopped at presentations in online classrooms, so when entering the online teaching environment, teachers would be surprised. Therefore, the training of skills in using online teaching software is very important. When teachers have the skills to run an online classroom, teachers will confidently and proactively respond to situations (Mohd Alwi & Fan, 2010).

Faced with concerns about the safety of online classes, the Ministry of Education and Training has sent an official letter to requesting units and schools to organize propaganda and training to disseminate knowledge and skills to use the Internet and social networks to ensure safety. network safety and security when participating in teaching and learning activities via the Internet (Hentea et al, 2006); skills to prevent and avoid possible risks, situations and harms to teachers, students and parents in teaching via the Internet. At the same time, introducing and disseminating to teachers reliable and reputable solutions and management software, organizing teaching via the Internet; encourage the use of copyrighted software, those introduced by the Ministry of Education and Training and the Ministry of Information and Communications for free use during the epidemic season; develop and implement regulations on management and organization of teaching via the Internet, clearly guiding the process of managing and organizing an online class; online classroom management skills for teachers, learners' responsibilities when participating in online classes, especially behaviors not to be done for learners (Kim, 2014).

In addition, units and schools need to strengthen coordination between schools and families in

managing and organizing online teaching activities; suggested that parents increase their responsibilities, spend time supporting students to connect, use the online classroom safely and take measures to manage the time their children learn online.

In the face of students revealing their classroom IDs and passwords, the Ministry of Education and Training requires that if negative situations occur, teachers, students, and parents need to provide timely information to school leaders and agencies. education management agencies, police agencies to investigate and handle according to the provisions of law.

For learners, it is mandatory to use real names, absolutely do not comment or have other behaviors that affect the class. Learners are responsible for protecting personal accounts; absolutely do not share your class account and password with others (Tabor, 2007).

In addition, security experts advise users to be careful when using e-learning applications, and apply safety measures such as always updating software to the latest version; use passwords for meetings; use the Waiting room feature to control participants; turn off member screen sharing, etc.

3. Methodology

The study selects data collection techniques that allow the best data to be obtained, reliable data based on current and previous studies, compared and analyzed to find out the most effective solutions.

4. Common form of attack regarding online teaching

Online teaching is a teaching activity conducted on an online teaching system. The online teaching software system includes online teaching organization software, online learning management software (LMS/LCMS) or a combination of these two software. At Vitenam, the most popular is teaching online directly on some software such as Google Classroom, Microsoft Teams or online meeting applications such as Zoom, Google Meet.

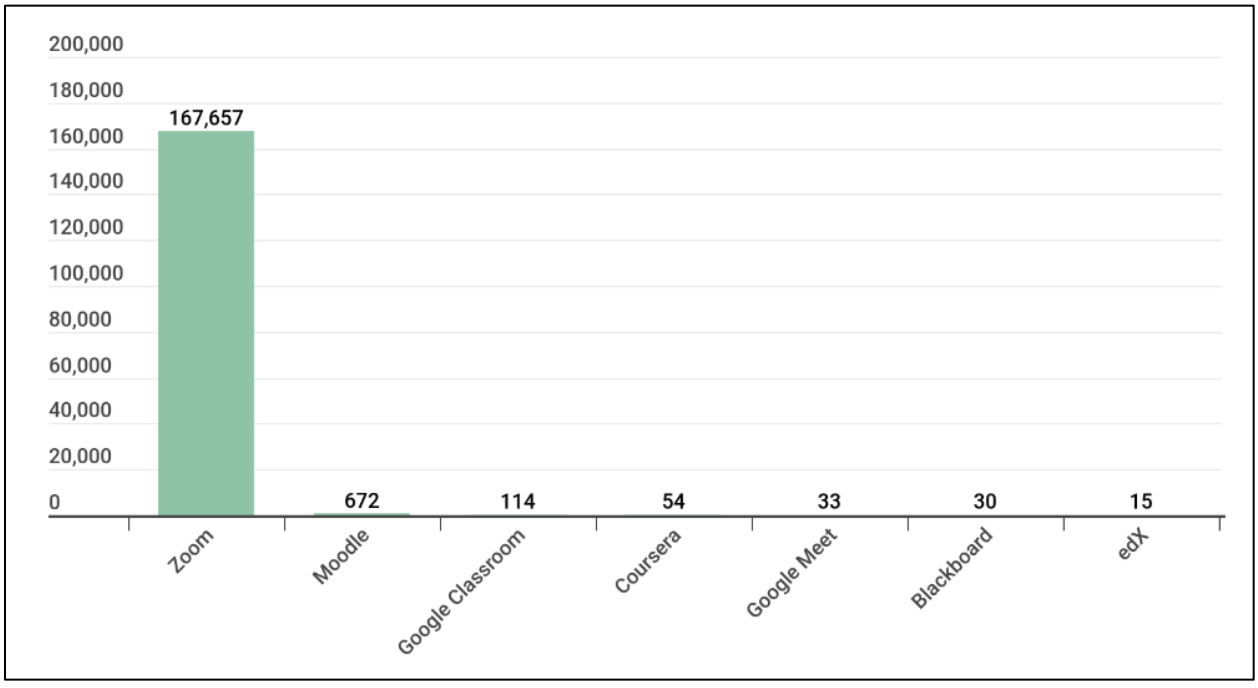

Figure 2. The number of users that encountered various threats disguised as popular online learning/video conferencing platforms in the first 6 months of 2020

Recently, many information insecurity situations have occurred in the process of online teaching on the network environment, leaving many immediate and long-term consequences. The risk of insecurity and its consequences in online

teaching can be divided into several main groups as follows (Miguel et al., 2013).

The first risk is that the online teaching system does not guarantee information security, which can be broken into the classroom by strangers, and by hackers installing applications to eavesdrop, peek, and steal data. Then the class will not be possible, personal information is stolen, information about diplomas, certificates, scores, tests can be modified for illegal purposes, buying and selling. , valuable learning materials may be illegally copied. More dangerously, when the system is sabotaged (or even crashed), it will take a lot of time and effort to restore, disrupting learning, and in some cases not being able to recover completely. lost data (Kim, 2014).

Next is taking advantage of online learning, taking advantage of the need to learn about online learning solutions, the desire to improve the knowledge and skills of teachers and students, hackers can also be lured into accessing them. access advertising links about courses, free learning applications, discounts on the Internet from which to install malicious code, steal data. Teachers and students access fake online teaching links (with the same interface as a real online learning page), which can be tricked, have their personal information and data stolen to be used in other activities. activities such as impersonation, threats (threat to beat, threaten to boycott, threaten to disclose sensitive personal information or images), bully, harassment, mental terror, cause panic, thereby taking advantage of , intimidation and coercion to perform illegal actions, blackmail.

Bad people can use account information to access the system of teachers and students to create spam, phishing, to access other systems or simply collect personal information to use for attacks. network later.

Next is the failure to ensure information security, teachers not only cannot ensure the progress and quality of the lectures, cannot convey all the content of the lecture to the majority of students, but also may be hijacked, taking advantage of the classroom space to transmit malicious and provocative information to students, and to deceive students and families (such as through school money transfer notices, school time change notices). Classes can be disrupted, lectures can be edited, teachers can't control the classroom, teachers' images can be smeared, discredited before students, with lasting consequences.

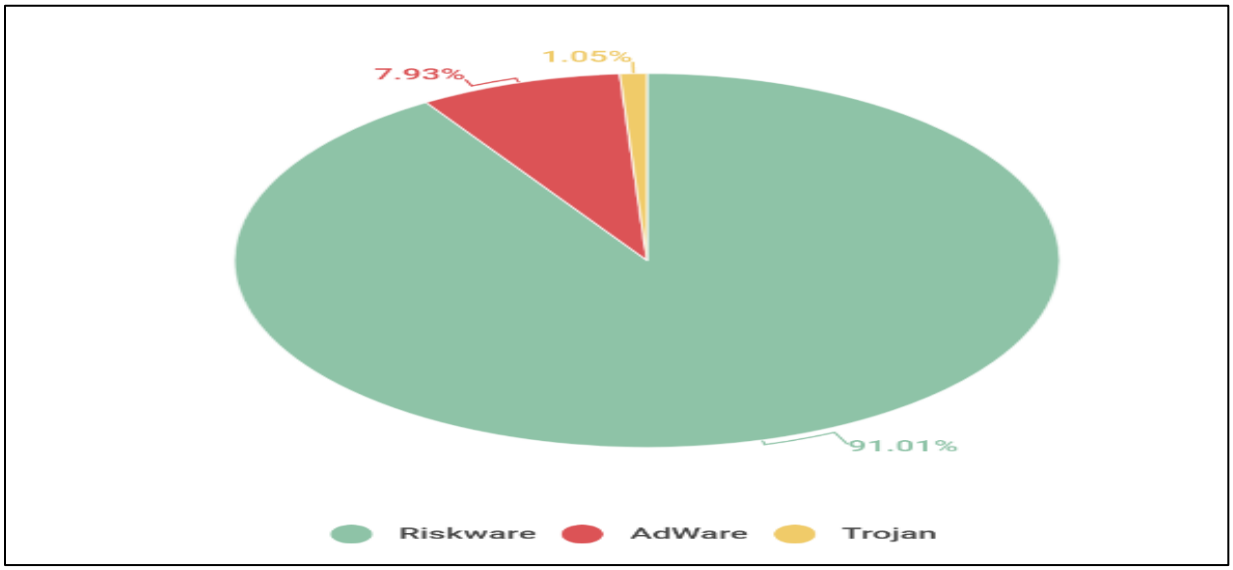

Figure 3. Type of threads found during online learning

When the lecture is always interrupted by unwanted sounds and images that distract students; The content of the lecture was edited, leading to misconceptions and confusion about knowledge for students. More dangerously, students may also encounter videos, sounds, images, obscene, violent, erotic messages, stimulating curiosity, causing distorted thinking, imitating actions, and reactions. scientific and

unethical, aggressive or socially awkward. In addition, loss of information security can make school hours longer, affecting students' physical and mental health (leading to eye diseases, spine problems, psychological fatigue, and loss of concentration).

The most common is a form of denial of service attack, in which cybercriminals overload a network server with service requests, causing the server to crash and stop serving user access requests (Tabor, 2007). DDoS attacks are extremely dangerous because they can last from days to weeks or longer, disrupting an organization's operations. In the case of educational institutions, the consequence is that learners and teachers cannot access important resources; The online teaching system is paralyzed, operating in moderation or unable to work, teaching - learning is interrupted or stopped altogether.

Some types of traditional attacks, which have been around for a long time, but still many people still suffer from it, are phishing, users accessing fake e-learning websites (with the same form as the real ones) will being lured into clicking a malware download link; or being tricked into entering personal account information (such as username, password) without knowing. Hackers then do not even need to use this account to access the e-learning system, but use it for many other purposes.

In addition to the fake pages, hackers actually send phishing emails to students of the online teaching system with content such as class postponement notice, password change request, account activation. Learning. When students receive the notice, do not check carefully, click on the attached links, they have also downloaded the malicious code.

5. Some solutions to ensure information security in online teaching

First, we need to learn about the tools we are using, know their capabilities and features well by reading the user manual, learning the interface and searching the configuration guide online. Internet, ensuring that we fully comply with the regulations of the organization.

Next is to limit the user's own tools. The information technology tools we choose to conduct lessons need to be convenient for both instructors and students. Having more tools doesn't always mean a better experience. Before starting the lessons, make sure we have the tools to do the job and that everyone involved in the training can use them easily (Mohd Alwi & Fan, 2010).

We also need to set a separate password for each service. For each account, we need to use a separate password. All passwords should be strong, long enough, and not too easy to guess.

It is quite important to protect your education and training accounts. We need to pay special attention to those accounts used for educational and training activities. The account is easily accessible at any time without anyone else being able to log in (Kim, 2014).

We also need to understand how to distinguish phishing emails, that is, how to distinguish phishing emails from legitimate emails sent from legitimate services. Phishing sites often have flaws, messy layouts, and inactive links, but sometimes hackers also try to build phishing sites that are very similar to legitimate sites and are difficult to distinguish (Tabor, 2007).

We need reliable protection on every device used to access educational resources. For example, if a student's school computer is infected with ransomware, it will take a long time to restore the computer and data files. And if a lecturer's computer is hijacked, the consequences can be much more serious. Some malicious code may continue to infect students' devices. That's why we need reliable protection on every computer, smartphone and tablet.

6. Conclusion

While the issue of information security for online teaching is becoming a pain, teachers still have to face the fact that students have not really adapted, enjoyed and cooperated with teachers. This is a consequence of the lack of interaction in online classes, and teachers do not well manage teaching resources to supplement the classroom. Integrating a solution that not only ensures the effectiveness of online teaching, but also meets the security requirements and stimulates the

interest of students is more important than ever. This not only helps reduce the workload for teachers, but also minimizes parents' worries about their children's online learning. In learning, there will be no content that is too secret, so private that teachers can still use it with good governance requirements. When it is not possible to manage to let strangers in, it is due to the way in which teachers use and operate. Any software will also have a part to manage learners, give information ... so teachers only need to learn how to use and administer it. If the teacher is not a professional, then someone with knowledge, guidance or help with classroom management is needed.

References

[1] Tabor, S. W. (2007). Narrowing the distance: Implementing a hybrid learning model for information security education. Quarterly Review of Distance Education, 8(1), 47.

[2] Mohd Alwi, N. H., & Fan, I. S. (2010). Information security threats analysis for e-learning. In International Conference on Technology Enhanced Learning (pp. 285-291). Springer, Berlin, Heidelberg.

[3] Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Management & Computer Security.

[4] Miguel, J., Caballé, S., & Prieto, J. (2013). Providing Information Security to MOOC: Towards effective student authentication. In 2013 5th International Conference on Intelligent Networking and Collaborative Systems (pp. 289-292). IEEE.

[5] Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards changes in information security education. Journal of Information Technology Education: Research, 5(1), 221-233.

[6] Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. Academy of Information and Management Sciences Journal, 14(2), 91-116.

[7] Yan, Q., Lai, W., & Wang, Z. (2021, August). Online Experiments Based on the CTF Model for Information Security MOOC Courses. In 2021 16th International Conference on Computer Science & Education (ICCSE) (pp. 783-788). IEEE.

[8] Khlifi, Y., & Allehaibi, M. M. (2014, June). Information Security Services and Requirements for E-learning Infrastructure Success. In 2014 World Congress on E-Learning, Education and Computer Science (WCEECS'2014), Hammamet.

[9] Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia manufacturing, 13, 1253-1260.