Maintaining Quality in Online Learning Environments– Issues and Challenges

Melissa Aldredge, Sarah DuBois, Diane Mobley, Elizabeth Prejean, Margaret Vienne
Northwestern State University, USA

Abstract

The online classroom continues to play an ever-increasing role in higher education. There are proven, research-based pedagogical techniques available to instructors who want to create online courses that are both dynamic and engaging. With careful planning, online learning can provide students with a positive learning experience without sacrificing the academic quality of learning. Addressing security issues and challenges is vital to maintaining the desired academic rigor and quality. This paper discusses these important security issues and offers a variety of solutions for facilitating a secure learning environment.

***Key words**: Distance Learning, Online Security, E-cheating, Academic Dishonesty, Security Issues*

Introduction

Over the last 20 years, the online learning phenomenon has exploded in higher education and shows no signs of slowing down. Although the demand for online courses is higher than ever, the debate about the quality of online instruction continues. As indicated by Furnell and Karweni (2001), trust in the status and credibility of online service providers is “vital for both online students and prospective employers, as it obviously reflects upon the value of the associated awards” (pg. 29). Online education will always produce a tempting environment for students because of the relative anonymity afforded the distance learning student, the difficulty instructors have in policing online exams, and the growing availability of e-cheating tools. Added security measures are necessary to facilitate the trust needed in such an educational environment and to protect the reputation and quality of an online program. According to Case, King, and Case (2019), current research trends point to a need for increased vigilance among educators in searching for cheating. Pedagogies should be modified with respect to e-cheating and online ethics in the areas of student education, security, and enforcement. This paper discusses the security challenges inherent with online course platforms and offers a variety of solutions for facilitating a secure learning environment.

Challenges

In today's world, college students are virtually connected with others throughout a typical day. The evolution of social media has provided students with the ability to stay connected to friends, family, and instructors in real time with the touch of a button. Online Learning Management Systems such as Blackboard, Moodle, Canvas, Brightspace, Sakai or Schoology are required in most Internet classes and can be accessed through electronic devices of all types including cell phones, iPads, and laptops. Social media sites such as Facebook, Instagram, and Twitter or interactive video software such as Skype and Facetime are all used for online education (Kimmons, Veletsianos, & Woodward, 2017). These technological advancements have created mounting challenges for higher education institutions in the area of online instructional design. Maintaining quality instruction, academic integrity, and security in online learning platforms are areas that must be addressed. These areas are vital for successful E-learning environments to function. This is so important to academic institutions of higher learning that in 2001 a resource center was established, The International Center for Academic Integrity (ICAI). The center offers resources to combat security threats such as cheating, plagiarism, and academic dishonesty in higher education (Cultivating Integrity Worldwide, n.d.).

An endless challenge for academia, especially in the technology age, is the occurrence of cheating. Students are often more aware than educators of the different ways cheating can be accomplished with computers and/or smart devices. According to Rowe (2004), the ignorance of administrators and educators can increase the chances of cheating in online classes. When a university chooses to provide online classes to its student population, the security of the delivery of the assessment should be clear and proven. If this does not occur, then the reputation of the university will be damaged. In online classes, nontraditional students are sometimes under tremendous pressure from their jobs to just "get the degree". This pressure can increase the chances of cheating.

One recent study suggests that e-cheating is on the rise and continues to be a "fluid and ongoing challenge for educators" (Case et al., 2019, p. 102). Cheating in a digital environment can be accomplished by copying other student's assignments, plagiarizing from Internet sources, purchasing ready-made essays, or using mobile devices during class to cheat (Case et al., 2019). The availability of electronic sites such as Quizlet, Chegg, Course Hero, or other similar online resource "study" sites, creates a problematic environment that exacerbates unethical student behavior.

Security Measures

In order to maintain the integrity and quality of online programs, rigorous standards must be in place. One crucial area to address in the design of a quality online course should be in the area of delivery. Because learning is done at a "distance", controls should be in place to protect the information that is being delivered and received. Testing security is always an issue, even with a face-to-face class. In an online class, the security and stability of testing can be more complex. User authentication is crucial, but other critical issues involve verifying that users don't collaborate with others or utilize unauthorized resources during assessments (Hylton, Levy, & Dringus, 2016).

Browser Security

Controlling the students' testing environment is a very important aspect of maintaining course integrity. One assessment tool for online instruction is the use of a lockdown browser (LDB). The LDB is a separate software program installed on the test-takers' computer that works with both Windows and Mac computer operating systems as well as most current Learning Management Systems (LMS).

Respondus LockDown Browser software is a popular, customized browser that locks down the testing environment within the LMS. The software is currently being utilized by over 1,500 higher education institutions to create, deliver, and analyze online exams (Respondus, n.d.). Subscribers to the service are able to administer locked exams so that students are unable to print, copy, go to another URL, or access other applications; thereby increasing the security and stability of the testing environment. Further, while the lockdown software is running, students can't access other online applications like email, instant messaging, screen capture, or search engines. Students are locked into an assessment until it is submitted for grading. Respondus doesn't interfere with any security or anti-virus software already running on a computer. The software can continue to run in the background and keep the computer protected (Respondus, n.d.).

One area of concern with the Respondus system is that the program has to be installed on every computer where testing takes place. Once downloaded, the student logs into the Respondus site to complete an assessment. Students using public computers may run into problems because of this. For example, most military bases and school boards will not allow the LDB system to be downloaded on their computers. In order to avoid this issue, the student should be informed of the LockDown requirement at the beginning of the course.

Proctoring

Requiring proctored exams is another option instructors have to strengthen assessment security and deter misconduct. According to Hollister and Berenson (as cited in Hylton et al., 2016), the increase of technological advancements in the digital age have intensified dishonesty in online exams, particularly in unmonitored settings. Proctored exams can accomplish several purposes. Proctors can be asked to check photo identification, input passwords for exam access, and verify that students only have the allowed materials for an exam. It is very important for a proctor to be verified and approved by the instructor near the start of the semester. This can be accomplished through the use of a proctor approval form. Students should complete and submit the completed form at the beginning of every course so that the instructor can investigate the proctor. In order for the proctor to be approved, the student should adhere to several policies concerning the proctor selection such as 1) relatives, friends, employers, or tutors cannot be proctors, 2) exams cannot be mailed to or accessed at a residential address, and 3) a proctor's email address and other contact information must be from a verifiable place of business. Even with these requirements, students can "cheat" the system if the proctor is not properly vetted.

It is also crucial for instructors to create a personal relationship with the proposed proctor. By creating and fostering that relationship, instructors can increase the proctors' willingness to adhere to the stated responsibilities and duties. An in person or telephone conversation is the best method of establishing a relationship. It is also important for the proctor's exam instructions to be clearly laid out. For security purposes, exam instructions should contain some of the following information, as appropriate 1) check student's photo identification upon arrival to verify their identity, 2) student will need a computer with Internet access and a lock down browser to take the exam, 3) proctor will control and enter the required password for the exam, 4) no books, notes or study aids are allowed, and 5) no printing is allowed.

In addition, when considering proctoring requirements for a course, a strong proctoring option might be to prohibit any proctor except one at an approved site such as a national testing center (i.e. Sylvan or Prometric) or an official university proctoring center. Further, a stricter proctoring policy could only allow proctoring through an online, webcam-based proctoring service. Monitoring of online exams via webcam offered by providers such as ProctorU or Kryterion has become increasingly popular along with the explosion of online degree programs. These services employ a combination of different approaches to monitoring exams, including monitoring live feeds, recording exams, sharing monitors and computer control, and installing software that restrict the use of web browsers and chat programs while taking an exam. These service providers report "incidents" to instructors who must then determine the severity and consequences of violations of exam protocols (Kolowich, 2013). Many of these providers are also employing new technologies such as artificial intelligence (AI) to assist in identifying suspicious behaviors. In 2018, ProctorU updated their platform to utilize AI in addition to the human proctor to add a "second set of eyes" to the monitoring process (ProctorU Raises the Bar, 2018). A 2015 study conducted to investigate the effect of webcam-based proctoring in deterring misconduct found that web-based surveillance techniques did limit the student's opportunity to collaborate with others or use unauthorized resources (Hylton et al., 2016). The perception of the exam-taker that there was less opportunity to cheat was also an important factor in the actual deterrence of the negative behaviors.

Exam Design

As one can imagine, there is no security method that is 100% fool proof. In today's age of cell phones, smartwatches, and other hand held devices, a camera alone can breach exam security. There is virtually no protection, other than personal monitoring, to defend against a camera phone. Anything displayed on a screen should be considered compromised. We can however, make it difficult for the student to cheat. For example, instead of displaying all exam questions at once, display each question separately on the screen. Another option is to not allow the student to backtrack to a previous question once they begin an exam. The questions must be answered in the order they are presented. In addition, choose random questions for each examination. Another line of defense might be to use large test banks to pull questions from if worried about exams "getting out".

Many times with homework assignments, students are encouraged to work together in groups to enhance the learning experience. However, student collaboration is typically not allowed when administering exams, and can be mitigated by choosing algorithmic problems when designing the exam. With algorithmic problems, each student sees the same question, but with different numbers. When students are taking online tests at different times or on different days, this feature eliminates a student being given the answers by another student. The student may tell another student what type of problem is on the test, but each student will see a different set of numbers. Therefore, no two exams are alike.

With respect to exam security, verifying a student's authenticity should be of utmost importance. Instances of using another person to take exams and complete assignments in an online class has recently been in the news (Horka, 2019; James, 2019). The focus has been on high profile instances involving college athletes and their tutors; however, this is an issue that affects all distance learners. Preventing this type of breach must be a priority to preserve academic integrity for online programs. Using a web-based proctoring service who verifies the student's identity with photo identification is a best practice.

Further Research

A plethora of prior research has focused on comparing the quality of instruction in different course formats based on learning outcomes. The results of these studies have produced exciting yet contradictory results; with some indicating higher effectiveness in traditional courses while others indicating lower achievement in traditional course formats (Ary & Brune, 2011; Cavanaugh & Jacquemin, 2015; Harwood, McDonald, Butler, Drago, & Schlumpf, 2018; McKeever, 2019; Weldy, 2018). Regardless of the results of the research, the critical focus of institutions of higher learning should be to deliver quality instruction irrespective of the delivery method used. Instructors must constantly adjust curriculum relevant to different course formats, develop direct and indirect measures of learning outcomes, and evaluate the effectiveness of various pedagogical tools for online learning delivery methods (Weldy, 2018). While an image of successful distance education is taking shape (McKeever, 2019), more research is needed to continue to understand this educational practice. Future research should address trends in online security and examine the most effective techniques for minimizing e-cheating; especially with the dramatic increase institutions of higher learning are seeing in Web-based course enrollments.

Conclusion

The workforce expects students to be educated, have leadership skills, and to be ready to start work upon graduation. In that effort, teachers are expected to get students quickly through classes and use different methods of testing for the development of future graduates and ensure a new and innovative workforce. Due in large part to technological advancements and lower costs, online courses and exams have become a practical option for many higher education institutions and students. Technology continues to evolve making more online class options available for students. Security issues in online learning have become increasingly important as the demand for these types of classes has increased. As students become more technology savvy, their ability to devise new ways of cheating increases. Educators attempt to prevent cheating and dishonesty in their classes but are frequently frustrated with the effectiveness of the results. In online classes, students sometimes see the anonymity as an excuse to cheat. Instructors should see this issue as an opportunity to reduce the students' perception of being invisible by increasing opportunities to engage the students. Browser security, the use of proctors, and exam design are important areas that can give the educator the necessary tools to increase the security of the online learning experience. The end result of the use of these tools is to improve the learning experience for the student and reassure the educator of the integrity of the course.

References

Ary, E. & Brune, C. (2011). A comparison of student learning outcome in traditional and online personal finance courses. *MERLOT Journal of Online Learning. 7*(4). 465-474. Retrieved from https://jolt.merlot.org/vol7no4/brune_1211.pdf

Cavanaugh, J. & Jacquemin, S. (2015). A large sample comparison of grade based student learning outcomes in online vs. face-to-face courses. *Online Learning*. 19(2) 25- 32. Retrieved from http://search.ebscohost.com.nsula.idm.oclc.org/login.aspx?direct=true&db=eric&AN=EJ 1062940&site=ehost-live&scope=site

Cultivating Integrity Worldwide. (n.d.). Retrieved from https://academicintegrity.org/about/

Furnell, S. & Karweni, T. (2001). Security issues in online distance learning. *VINE Journal of Information and Knowledge Management Systems*. 31. 28-35. doi:10.1108/03055720010803998.

Harwood, K., McDonald, P., Butler, J., Drago, D., & Schlumpf, K. (2018). Comparing student outcomes in traditional vs intensive, online graduate programs in health professional education. *BMC Medical Education* 18: 240. doi:10.1186/s12909-018-1343-7

Horka, T. (2019, August 23). Mississippi State hit with NCAA sanctions: Tutor took exams for football, basketball players. *Clarion Ledger*. Retrieved from https://www.clarionledger.com/story/sports/2019/08/23/mississippi-state-university-athletics-academic-violations-ncaa-penalties-john-cohen-mark-keenum- msu/2041804001/

Hylton, K., Levy Y.,& Dringus, L. (2016). Utilizing webcam-based proctoring to deter misconduct in online exams. *Computers & Education*. 92 (1). 53-56. Retrieved from http://search.ebscohost.com.nsula.idm.oclc.org/login.aspx?direct=true&db=eoah&AN=3 6961537&site=ehost-live&scope=site

James, E. (2019, January 1). Former Missouri tutor completed coursework for 12 student- athletes. Retrieved from http://www.ncaa.org/about/resources/media-center/news/former- missouri-tutor-completed-coursework-12-student-athletes

Kimmons, R., Veletsianos, G. & Woodward (2017). Institutional uses of twitter in US higher education. *Innovative Higher Education*, 42, 97-111. doi:10.1007/s10755-016-9375-6

Kolowich, S. (2013). Behind the webcam's watchful eye, online proctoring takes hold. *Chronicle of Higher Education.* 4/19/2013, Vol. 59 Issue 32, A12-A12. Retrieved from https://www.chronicle.com/article/Behind-the-Webcams-Watchful/138505

McKeever, B. W. (2019). Different formats, equal outcomes? Comparing in-person and online education in public relations. *Journal of Public Relations Education*, 5(2). Retrieved from https://aejmc.us/jpre/2019/08/17/different-formats-equal-outcomes-comparing-in-person-and-online-education-in-public-relations/

ProctorU Raises the Bar for Academic Integrity in Online Proctoring. (2018, September 5). Retrieved from https://www.proctoru.com/industry-news-and-notes/proctoru-raises-bar-academic-integrity-online-proctoring

Respondus (n.d.). Retrieved from https://web.respondus.com/about/

Rowe, N. C. (2004). Cheating in online student assessment: Beyond plagiarism. *Online Journal of Distance Learning Administration*, *7*(2),1-10. Retrieved from https://www.westga.edu/~distance/ojdla/summer72/rowe72.html

Weldy, T. (2018). Traditional, blended, or online: Business student preferences and experience with different course formats. *e-Journal of Business Education and Scholarship of Teaching*, 12(2).55-62.Retrievedfrom https://eric.ed.gov/?q=Traditional%2c+Blended%2c+or+Online%3a+Business+Student+Preferences+and+Experience+with+Different+Course+Formats&id=EJ1193431