https://doi.org/10.48009/4_iis_2019_1-7

LEARNER SECURITY & PRIVACY RISKS: HOW USAGE OF ONLINE SOCIAL MEDIA OUTSIDE A LEARNING MANAGEMENT SYSTEM AFFECTS LEARNERS' DIGITAL IDENTITY

Loreen M. Powell, Bloomsburg University of PA, lpowell@bloomu.edu
Hayden Wimmer, Georgia Southern University, hwimmer@georgiasouthern.edu
Carl Rebman, University of San Diego, carlr@sandiego.edu
Chaza Abdul al, Harrisburg University, cabdul@harrisburgu.edu

ABSTRACT

Millennial learners are the first group of learners to grow up using social media on a daily basis. Consequently, educators often seek to incorporate social media applications and tools in their efforts to engage the learner in the learning process. Unfortunately, one challenge is that most social applications are constantly connected to the Internet and thus are susceptible to security attacks and abuse of data. There seems to be a limited amount of research on the security and data privacy risks of using open or free social media application and tools outside of a secure learning management system (LMS). This paper examined seven common online social media applications, typically used by educators outside of a LMS, for existing data privacy security settings. Specifically this research investigated if secured and un-secured content posted appeared in a simple google search. The results revealed that content posted was easily found when the data privacy options were turned off. These results imply that a learner's digital identity may be affected for potential employers, significant others, friends, or educators when they are googling information to learn more about them. This research provides an important foundation for future research on how required usage of online social media applications outside a LMS affects the learners' digital identity.

Keywords: Social media, digital identity/profile, learning management system, data privacy, online security settings

INTRODUCTION

The rapid development of internet, applications, and mobile connectivity have revolutionized the way one communicates, collaborates and educates (Rainie, 2012 Stantchev, Prieto-González, & Tamm, 2015). Thiele, Mai, and Post (2017) state that today education goes beyond "the presentation of information in a way to actively engage a student in a room" (p. 80). They argue that education environment has shifted to interactive learning as students and educators are tech-savvy. As a result, educators often seek out new technologies to integrate into their classrooms for student engagement (Powell & Wimmer, 2015).

Extensive research has been conducted on the advantages and disadvantages of integrating social media tools and applications in the online and face-to-face classroom environments (Menkhoff, Chay, Bengtsson, Woodard, & Gan, 2014; Thoms & Eryilmaz, 2014; Wheeler, 2010; Thiele & Mai, 2014; Chawinga, 2017). Almost every discipline has explored the use of technology and social media integration into their courses.

LMS have the capability of learning content and resources, tracking and reporting of training or content accessed, as well as, maintaining student submissions, grades, and interactions online within a controlled location that is accessible 24/7 (Lonn and Teasley, 2009; Little-Wiles & Naimi, 2018; Wikipedia, 2019). Thus, the use of LMS has vastly grown over the last two decades (Little-Wiles & Naimi, 2018). Today, many LMS integrate social media tools and applications within their system.

However, one problem is that any LMS connected to the internet is susceptible to security attacks and abuse of data (Furnell, Onions, Knahl, Sanders, Bleimann, Gojny and Roder, 1998; Furnell & Karweni, 2001; Warren and Hutchinson, 2003; Raitman, Ngo, Augar, and Zhou, 2005; Mohd Alwi & Fan, 2010a, 2010b, 2010c; Schultz, 2012). Exploitations and vulnerabilities of secure LMS have occurred within some of the most widely known platforms. Specifically, several zero-day security vulnerabilities were discovered in Blackboard (Pauli, 2011; Schultz, 2012).

There are also a few reported cases of admin or user logins compromised within Blackboard (Tillman, 2009; Daily, 2008).

Additionally, open source LMSs have similar, if not more, exploits and vulnerabilities (Schultz, 2012). Moodle is a free, open-source LMS (Thiele, Mai, and Post, 2014). Moodle continuously releases several comprehensive updates to address security vulnerabilities (Hawkins, n.d.; Constantin, 2017; Nagel, 2011; Shcultz, 2012).

While, there are many security and data privacy issues researched and addressed with LMS, there is little to no research on the security and data privacy risks of using open or free applications or tools outside the LMS. Many educators utilize some of the most common social media tools and applications provided outside of their LMS. Such tools may include Twitter, Blogs, Facebook, Youtube (Awadhiya, Miglani, and Gowthaman, 2014), Screencast-o-matic, LinkedIn, Voicethread, Prezi, and more.

Social Media Applications/Tools Outside of the Learning Management System

Educators often utilize open or free applications or social media tools housed outside of their universities LMS. Research has shown numerous of examples of open or free programs housed outside of their universities LMS. Table 1 highlights various research studies conducted on the common online social media applications.

Table 1. Highlights of Research Studies Where Educators Utilized Common Social Media Applications/Tools in the Classroom

Social Media Application/Tool	Research Study
Facebook (www.Facebook.com)	Sánchez, Cortijo, and Javed (2014) found that a primary use of Facebook by students, when used in an academic context, was to facilitate and support peer-relations.
Twitter (www.twitter.com)	Powell, O'Connor and Gehris (2013) utilized Twitter in an undergraduate business application development to help students prepare for assessments. They found that Twitter did help enhance student performance.
Screencasts (www.screencast-o-matic.com)	Powell and Wimmer (2015) utilized screencasts in an undergraduate hands-on computer programming course as a means to help student learn. They found that screencasts did help enhance student learning.
Youtube (www.youtube.com)	Campbell and Cox (2018) required graduate student to utilize Youtube for personalized learning assignment. They found that creating a video on YouTube was appositive learning experience that encouraged peer collaboration.
Prezi (www.prezi.com)	Samer (2017) examined the effect of using Prezi on Al Zaytoonah students' performance in French Language reading skill using two groups of students in Amman’s public schools. They found Prezi to be beneficial.
VoiceThread (https://voicethread.com)	Fox (2017) utilized VoiceThread in an undergraduate clinical nursing course. She reported on positive the experiences of 17 students who used VoiceThread.
LinkedIn (www.linkedin.com)	The National Association for colleges and Employers (NACE) (2017) reported that many members incorporate Linked-in-in into the college curriculum. Specifically, one member reported that their “freshman experience course has a LinkedIn component”.

Additionally, Thom’s and Eryilmaz (2014) studied online social networking (OSN) software and how it differentiates itself from LMS software. They presented a theoretical model for OSNs in education that focuses primarily on the individual learner. Their model indicates that the learner’s constructivism is heavily influenced by their interactions with OSN applications and tools outside of the LMS which impacts their overall social presence.

Digital Profile/Identity
Szymielewicz (2019) defines a person's digital identity via three layers: 1.) What you share, do and feed into social media and applications, 2.) Your behavioral observations online in social media and applications as well as the metadata, 3.) Interpretations of the first and second layers. Her research indicates that people realistically only have the ability to control the first layer.

Today, almost everyone's digital profile is looked at by employers, banks, family, friends and future significant others, educators, and hackers. Unfortunately, the countless decisions that affect one's life professionally, personally, and educationally may possibly be dictated by the interpretation of their online digital profile.. Recently, Salm (2017) reported information from the CareerBuilder Survey that stated "70% of employers use social media to screen candidates before hiring". Likewise, in the online dating world, Broster (2018) reports viewing a potential date's online digital profile prior to the date. Furthermore, she revealed that results of a survey which revealed that 40 percent of the respondents changed their decision to go on a date after viewing the person's digital profile. Finally, Thoms and Eryilmaz (2014) found that that social media applications and tools provided a larger number of interactions and learning experiences than a LMS. Thus, there is a strong attractiveness for educators to use social media applications outside the LMS for course assignments.

The discloser and traceable amounts of personal information found online is vast and growing daily. Today, privacy invasive profiling applications and tools may collect identifiable data disclosed on the internet as well as an aggregate analysis of metadata from one's communication patterns (AlMusallam. & AlMuhatdi, 2014). By the time the average learner reaches college, their digital identity is already established and Google, Apple, Amazon, Facebook, Instagram, Microsoft, and Twitter already know all about you via the applications and tools you use online, the websites your visit, the post and interactions you make, and the devices you use (Newman, 2014; Zaidi, 2018).Hence, using social applications/tools in education may further transform and alter a learner's digital identity and additional research needs to be conducted in this area (Kirkup, 2010).

Tablante (2013) argued that learner's data privacy needs to be protected "as they begin exploring new personal identities in college because, sometimes, this exploration is not something you want to stick with you forever". There is a challenge in that the learner's digital identity could possibly be altered as a result of their required course assignment. Learners may post content for the grade rather than their true opinion or a reflection of their identity. In this scenario, the digital profile is altered from the learner's identity and could have an impact upon the learner's professionally, personally, and educationally.

RESEARCH METHODOLOGY

The aim of this exploratory study is to examine seven common social media applications, typically utilized outside of a LMS, for data privacy and security settings. Additionally, this research investigated if secured and un-secured content posted appeared in a simple google search. Our research centered upon the following research questions:

1. Do the applications/tools contain default security and privacy settings?

2. Do the default settings of the applications/tools contain data privacy settings?

3. Do any of the secure of unsecured posted content appear in a simple google search?

Each application/tool was examined by the authors for available privacy and security options for learners required to utilize the application/tool. Next, the authors created a fake user name and signed-up for all of the commonly used social media applications and tools. Once registered, using all the commonly used applications and tools listed above, the authors posted content out onto the internet under the fake username. The authors targeted specific course content within the Information Technology (IT) discipline in all the usage of the commonly used applications and tools. Next, the authors completed a google search on the fake username, similar to what a potential employer, date, or educator might do. By doing so, the authors recorded if the potential for data privacy and security risks exists within each application/tool.

RESULTS

The results on this research revealed most of the social media applications have data privacy options and settings available for the users. However, these security options and data privacy setting are not automatic or the default settings. These security options and data privacy setting must be manually turned on by the user. Additionally, this study revealed that content posted from five (5) out of the seven (7) online social media application tools, used outside of a LMS, were easily found in a simple google search when the data privacy options were turned off. Additionally, the content posted by the learner was for an assignment and may not necessary be a true representation of themselves. These results imply that a learner's digital identity may be affected for potential employers, significant other, friend, or educator when they are googling information to learn more about them. Table 2 contains the detailed results for each social media application or tool.

Table 2. Highlights Various Research Studies Where Educators Use Common Social Media Applications/Tools In The Classroom

Social Media Application/Tool	Data Privacy Options/Settings Available Within the Application/ Tools	Default Settings of Application/Tool Contain Data Privacy	Content was Easily Found by a Google Search	Implied Security Risk & Opportunity to Alter Students Digital Profile if Required to Use for Class Purposes
Facebook (www.Facebook.com)	Yes	No	Yes, if data privacy options are turned off.	Yes
Twitter (www.twitter.com)	Yes	No	Yes, if data privacy options are turned off	Yes
Screencasts (www.screencast-o-matic.com)	Yes - Multiple	No	No	Limited
Youtube (www.youtube.com)	Yes	No	Yes, if data privacy options are turned off	Yes
Prezi (www.prezi.com)	No	No	Yes	Yes
Voice Thread (Voicethread.com)	Yes	No	No	Yes
LinkedIn (www.linked-in.com)	Limited	No	Yes	Yes

DISCUSSION

Salazar and Woodward (2017) studied Millennials learners' perceptions on data privacy. They noted that this generation is typically the first group to begin using technology and social media on a daily basis. Since social media is so prevalent in their lives they indicate that this increases the opportunities for abuses proliferate. Yet, they report that, "in general, the millennial generation is not highly concerned about privacy". Their lack of concern regarding their data privacy is of great interest as the results of this study indicate that a learners' digital profile can be affected if they don't purposefully utilize the social media application's/tool's security and privacy settings.

The results of this study support the research conducted by Salazar & Woodward (2017) and correspond with the Tablante (2013) argument that learner's data privacy needs to be protected "as they begin exploring new personal identities in college because, sometimes, this exploration is not something you want to stick with you forever". As illustrated in Table 1, the content posted from 5 out of the 7 online social media applications outside of a LMS were easily found in a simple google search when the data privacy options were turned off. The findings of this exploratory study reinforce the research by Salm (2017). The results suggest that academic educators and administrators should develop a policy that will require educators, that utilize social media applications and tools outside of a university's LMS, to encourage learners protect their work by deploying the data privacy and security options within the application/tool.

CONCLUSION, LIMITATIONS, AND FUTURE RESEARCH

Online social media application offer a lot of potential to engage students and foster an enhanced learning environment. There are many different types of online social media applications and that are used within a LMS as well as, outside a LMS. This research focused on the commonly used online social media applications/tools that educators use outside of their LMS and examined its privacy and security options/settings. Additionally, this research investigated the content posted, secured and un-secured, to appear in a simple google search. The results revealed that content posted from 5 out of the 7 online social media applications/tools, outside of a LMS, were easily found in a simple google search when the data privacy options were turned off. The results also imply that a learner's digital identity may be altered for potential employers, significant other, friend, or educator as the content posted was for an assignment grade and not necessary a representation of themselves.

This research is important because as it provides information for learners, educators, and academic administrators should consider when discussion how faculty engage student via social media applications/tools outside their LMS. Additionally, it will help academic administrators' recommendation for LMS, which incorporate the commonly used social media applications and tools, so that the learners' data will not be searchable on the internet, since it is located within a private LMS.

It is important to note that this research is not without limitations. First, the research is limited in size as only three fake user names were created for this research. Secondly, the research only accounted for commonly used social media applications/tools used outside a LMS. Future research should address these limitations. Additionally, future research should focus on examining actual learner profiles pre and post the use of social media applications outside of the LMS for required course work. Despite these limitations, this research provides an important foundation for additional research on how required usage of social media application/tools, outside a LMS, affects the learner's digital identity.

REFERENCES

Al-Hammouri, S. (2019). The Effect of Using Prezi on Al Zaytoonah University Students' Performance in French Language Reading Skills. *International Education Studies*, *12*(1), 128–135.

AlMusallam, M. & AlMuhatdi, J. (2014). De-correlating User Profiles: Exploring Anonymity Tools. *Proceedings of MEDES 2014 - 6th International Conference on Management of Emergent Digital EcoSystems*, 220-222.

Awadhiya, A. K., Miglani, A., & Gowthaman, K. (2014). ICT Usage by distance learners in India. *Turkish Online Journal of Distance Education*, *15*(3), 242–253.

Broster, A. (2018). How Many People Google Their Date? A Study Has Revealed More Of Us Are At It Than You Might Think. Available: from https://www.bustle.com/p/how-many-people-google-their-date-a-study-has-revealed-more-of-us-are-at-it-than-you-might-think-15552941

Campbell, L. O. & Cox, T. D. (2018). Digital Video as a Personalized Learning Assignment: A Qualitative Study of Student Authored Video Using the ICSDR Model. *Journal of the Scholarship of Teaching & Learning*, *18*(1), 11–24.

Chawinga, W. D. (2017). Taking social media to a university classroom: Teaching and learning using Twitter and blogs. International *Journal of Educational Technology in Higher Education*, *14*(3), 1-19. DOI 10.1186/s41239-017-0041-6

Constantin, L. (2017). Flaws in Moodle CMS put thousands of e-learning websites at risk. Available: https://www.csoonline.com/article/3183533/flaws-in-moodle-cms-put-thousands-of-e-learning-websites-at-risk.html

Daily, S. (2008, January 28). BIN breached over break, Its still recovering. Available: http://www.baylor.edu/lariat/news.php?action=story&story=48754

Furnell, S.M., Onions, P.D., Knahl, M., Sanders, P.W., Bleimann, U., Gojny, U., & Roder, H.F. (1998). A security framework for online distance learning and training. *Internet Research*, *8*(3), 236.

Furnell, S.M., & Karweni, T. (2001). Security issues in online distance learning. *VINE: The Journal of Information and Knowledge Management Systems*, 31(2), 28-35.

Hawkins, M. (n.d.) Security announcements. Available: https://moodle.org/security/

Fox, O. H. (2017). Using Voice Thread to Promote Collaborative Learning in On-Line Clinical Nurse Leader Courses. *Journal of Professional Nursing*, *33*(1), 20–26.

Little-Wiles, J., & Naimi, L. L. (2018). Faculty Perceptions of and Experiences in using the Blackboard Learning Management System. *Feature Edition*, 2018(4), 13–25.

Lonn, S., & Teasley, S. (2009). Saving time or innovating practice: Investigating perceptions and uses of Learning Management Systems. *Computers and Education, 53*(3), 686–694.

Mohd Alwi, N.H., & Fan, I.S. (2010a). E-learning and information security management. *International Journal for Digital Society*, *1*(2), 148-156.

Mohd Alwi, N.H., & Fan, I.S. (2010b). Information security in e-learning: A discussion of empirical data on information security and e-learning. *Proceedings of the 5th International Conference on e-Learning*, 282-290.

Mohd Alwi, N.H. and Fan, I.S. (2010c). Threats analysis for e-learning. *International Journal of Technology Enhanced Learning, 2*(4), 358–371.

NACE (2017). Should First-Year Students Be on LinkedIn?. Available: https://www.naceweb.org/career-development/special-populations/should-first-year-students-be-on-linkedin/

Nagel, D. (2011). 3 Moodle updates address 15 security vulnerabilities. *THE Journal.* Available: http://thejournal.com/articles/2011/10/19/3-moodle-updates-address-15-security-vulnerabilities.asp

Pauli, D. (2011). Millions of student exams, tests and data exposed. *SC Magazine*. Available: http://www.scmagazine.com.au/News/272215,millions-of-student-exams-tests-and-data-exposed.asp

Powell, L. M., Wimmer, H. (2015). Evaluating the Effectiveness of Self-Created Student Screencasts as a Tool to Increase Student Learning Outcomes in a Hands-On Computer Programming Course. *Information Systems Education Journal, 13*(5),106-111.

Powell, L., O'Connor, M., & Gehris, D. (2013). Using Twitter to Enhance Student Performance of Content Knowledge in a Business Education Course: An Exploratory Study. *Business Teacher Education Journal, 39*(1), 39-42.

Rainie, L. (2012). The new normal in the digital age. *Pew Research Center, Internet & Technology*. Available: https://www.pewinternet.org/2012/02/26/the-new-normal-in-the-digital-age/

Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). Security in the online e-learning environment. *Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05)*, 702-706.

Salazar, M. & Woodward, B. (2017). With Great Data, Comes Great Responsibility: University Students' Perceptions on Data Privacy. *Issues in Information Systems,* 18 (1). 191-201.

Salm, L. (2017) 70% of employers are snooping candidates' social media profiles. Available: https://www.careerbuilder.com/advice/social-media-survey-2017

Schultz, C. (2012). Information Security Trends and Issues in the Moodle E-Learning Platform: An Ethnographic Content Analysis. *Journal of Information Systems Education*, *23*(4), 359–371.

Szymielewicz, K. (2019). Your digital identity has three layers, and you can only protect one of them. Available: https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/

Thiele, A. K., Mai, J. A. and Post, S. (2014). Student-Centered Classroom of the 21st Century: Integrating Web 2.0 Applications and Other Technology to Actively Engage Students. *Journal of Physical Therapy Education*. 28(1), 80-93.

Thoms, B., & Eryilmaz, E. (2014). How media choice affects learner interactions in distance learning classes. *Computers & Education*, 75, 112–126.

Tillman, L. (2009, August 1). 'Gross academic fraud' at UTB-TSC rocked Office of Distance Education. Available: http://www.brownsvilleherald.com/news/online-100590-utb-employees.htm

Warren, M., & Hutchinson, W. (2003). Information security: An e-learning problem. In W. Zhou et al. (Eds.), Advances in Web-Based Learning - ICWL, *Lecture Notes in Computer Science* (2783)2003, 21-26.

Wikipedia (2019) Learning management systems. Available: http://en.wikipedia.org/wiki/Learning_ management_system.

Zaidi, Z. (2018). What Apple, Amazon, Google, Facebook, Microsoft and Twitter Know About You. Available: https://www.digitalinformationworld.com/2018/12/here-is-what-the-big-tech-companies-know-about-you.html

.