An Instructional Module for Protecting Privacy on Social Networking Sites

Rachael L.M. Inake
Department of Educational Technology
University of Hawai'i at Mānoa
Honolulu, Hawaii, U.S.A.
rinake@hawaii.edu

Abstract: Many college students are misled into making uninformed choices about what to disclose online and avoid taking the necessary precautions to protect their privacy on social networking sites. This study was aimed at developing and evaluating a multimedia, Web-based, instructional module to educate college students about protecting privacy on social networking sites. The module covered privacy, threats to one's privacy, and ways to protect oneself on social networking sites. It was hoped that students would also gain awareness for protecting their privacy in all online activities. A formative evaluation was conducted with a small group of 19 college students. Improvements in participants' pre- and post-test scores indicated that the instructional module was successful in educating the students about protecting privacy on social networking sites. Additionally, survey results showed that the participants felt that they increased their knowledge about protecting privacy on social networking sites and took a positive liking to the module. While the module proved to be successful in educating college students about protecting privacy, the researcher concluded that a different instructional approach may be even more effective in teaching how to protect privacy.

Introduction

"Cyberspace is privacy invasive" (Regan, 2002, p. 401). Yet people choose to disclose personal information in exchange for the benefits and conveniences they get from using the Internet. Web sites such as social networking sites where "people create a self-descriptive profile and then make links to other people they know on the site" (Donath & Boyd, 2004, p. 72) purposely share personal information with others online, but users enjoy and benefit from participating in them.

College students particularly benefit from participating in social networking sites because it allows them to keep in touch with high school and college friends (Ellison, Steinfield, & Lampe, 2007). However, without knowing about privacy, threats to one's privacy and ways to protect privacy on social networking sites, college students may be uninformed when choosing what to disclose and how to protect their privacy online. Without awareness and education, college students may risk their privacy leading to many avoidable consequences such as harassment and identity theft. This instructional design project was conducted to develop and evaluate the effectiveness of a Web-based,

multimedia, instructional module to educate college students about protecting privacy on social networking sites.

Background

The Internet is a public space where anyone can access anyone's information and use it maliciously. However, "most internet users do not seem to think much about the size and scope of their digital footprint. Fully 60% say they are not worried about how much information is available about them online" (Madden, Fox, Smith, & Vitak, 2007, p. 30). Even among "internet users who worry about their personal information, … [only] (54%) say they take steps to limit the amount of personal information that is available about them" (Madden, et al., 2007, p. 30). There are many reasons why people do not limit how much or what they disclose in online activities such as social networking.

In some cases, public and private boundaries are often blurred (Barnes, 2006) giving users a false sense of security and privacy. There is a certain level of trust that users have in participating in social networking sites that may make them feel they can openly share information about themselves (Acquisti & Gross, 2006). Many teens and young adults intentionally want to be seen online (Lange, 2007; Tufekci, 2008). According to Russell Research (September 2006), 72% of people 18 to 34 years old were aware that "anyone can see my site" (p. 19). Also, 57% "allow[ed] anyone to read my profile" (p. 12).

College students are heavy social networking site users. For some, although they may have general privacy concerns, their privacy concerns in regards to social networking sites are not significant because they feel that they have control in what they disclose and who will see it (Acquisti & Gross, 2006; Tufekci, 2008). However, there are some who unknowingly disclose information that could threaten their privacy. For example, disclosing their address or schedule of classes on their profile pages could provide a stranger with information about where they live and their daily routine.

On the other hand, a "significant minority" do not even know they may have a way to control who sees their profile (Acquisti & Gross, 2006, p. 17). In Acquisti and Gross' (2006) study, "30% claim not to know whether [Facebook] grants any way to manage who can search for and find their profile, or think that they are given no such control" (p. 16). This may be due in part by being unaware of privacy policies and settings because it "requires more time, attention and effort" (Regan, 2002, p. 388) making it less likely for the user to take necessary measures in protecting his privacy.

The reality is social networking sites are just like anything else on the Internet – it is online and public for anyone in the world to access, steal, or manipulate information from anyone. Online social networking users risk having their identities stolen, reputations slandered, sensitive information such as usernames and passwords stolen through phishing, and being stalked or bullied online and in real life (European Network and Information Security Agency, October 2007).

Several studies concluded that there is a need to raise awareness and to educate individuals about online privacy and what one can do to protect privacy online (Barnes, 2006; European Network and Information Security Agency, October 2007; Tufekci, 2008). Existing Web sites are targeted primarily towards teens and parents and presented in an informational, "freely browsing learning mode" (Chen, 2007, p. 800). However, a multimedia, Web-based module with a systematic, guided approach geared towards college students could provide awareness and understanding that educate this audience about privacy, threats to one's privacy, and things that one can do or precautions to take to protect oneself on social networking sites. On a larger scale this may also help college students to become aware of protecting privacy in all online activities.

Methodology

Design Methodology

The instructional module was designed for college students with the purpose to educate them about protecting privacy on social networking sites. It was Web-based to reach the wide target audience and to also allow the module to play online videos. The module incorporated videos from YouTube and other online websites to engage the learner in the module and to facilitate learning. The module's instruction was presented in five sequential units (see Figure 1), taking the learners through a methodical process to acquire the necessary subskills to achieve the module's terminal objective which was to correctly identify appropriate actions and behaviors to protect privacy on social networking sites. The effectiveness of the module's instructional content, as outlined by 15 performance objectives, was assessed by pre-, embedded, and post-tests.

Figure 1. Example page from the instructional module including a video.

Sample

The target audience for this instructional module was college students. The sample audience for testing was chosen from a 400-level, educational technology class at the University of Hawaii at Manoa. The sample test audience consisted of 19 volunteered students. In total, only 18 pre- and post-tests and 15 exit surveys were successfully submitted online and thus, usable for this study. The 15 exit survey results showed that the group was comprised of eight males and seven females. Of the 15 students, eight were undergraduate students, seven graduate students, and one "other". Their ages ranged from 21 years old to 39 years old. All but two students claimed that they participate in at least one social networking site.

Evaluation Procedures

The evaluation started with an initial review from two college students in individual one-on-one test sessions followed by revision and then a formal review from a small group test of 19 college students.

The researcher initially conducted two individual one-on-one test sessions with an undergraduate student and a graduate student to get feedback on the module's content, format, and effectiveness. Each student spent about an hour to participate in the module and take the pre-, embedded, and post-tests and about 10 minutes to complete the exit survey.

Pre-, embedded, and post-tests were conducted online through the University of Hawaii at Manoa's, College of Education (COE) Portal Survey Tool. The test questions were multiple choice questions relating to each of the 15 performance objectives in the instructional analysis. Some objectives were assessed using several questions, totaling 25 questions. All questions in the pre-, embedded, and post-tests were designed to be parallel and based from the performance objectives to measure how effective the module's instruction was by comparing the quantitative results from the pre-test with the post-test.

The exit survey was also given via the COE Portal Survey Tool which included a mix of 15 Likert-scale and open-ended question types. The exit survey collected both quantitative and qualitative data about participants' demographics and attitudes. Attitudinal information collected regarded participants' knowledge, understanding, behaviors, and attitudes about online privacy and how they felt about the module's content, format, and design.

After completing the module, each student in the one-on-one sessions engaged in a 15-minute informal interview with the researcher regarding content, format, design, what worked, what did not work, what they liked, and what they did not like. The one-on-one session was audio recorded for documentation and review for the researcher when making revisions to the instructional module using the results and feedback from the one-on-one students.

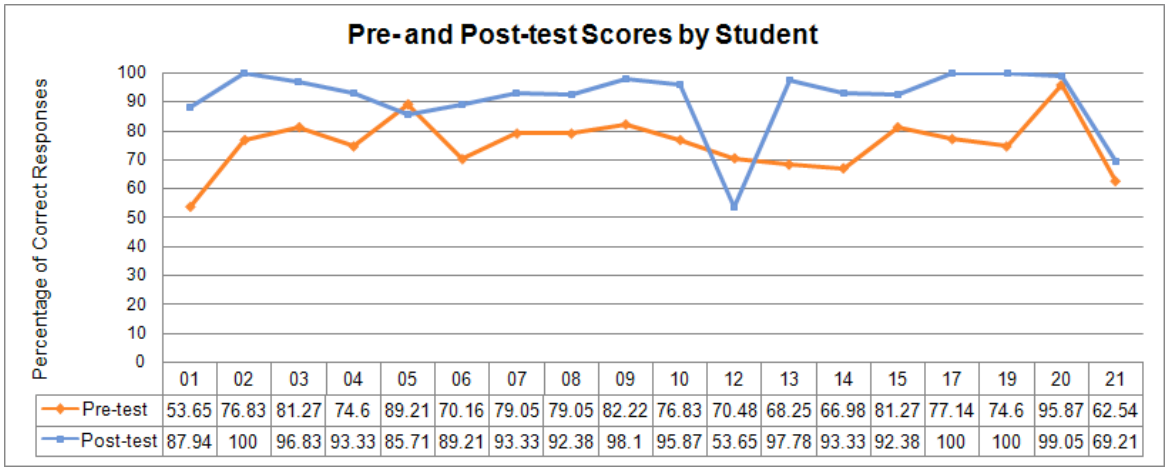
After revisions were made to the module, the researcher conducted a small group test with 19 students following a similar procedure where the students engaged in the module and took the pre-, embedded, and post-tests and exit survey. Results from the tests and exit survey were collected and analyzed to assess the instructional module's effectiveness. The students in the small group did not engage in an interview following the test session. All identities were kept anonymous by using usernames when they took the tests and exit survey.

Results and Findings

Both quantitative and qualitative data were collected from the small group test session. The module's effectiveness was determined from analyzing the data results from the pre- and post-tests (which evaluated the instructional content) and attitudinal data from the exit survey.

Instructional Content

The effectiveness of the module's instructional content was evaluated by comparing students' pre- and post-test scores. The pre-test measured what students knew prior to instruction and the post-test measured what students learned after instruction. As illustrated in Figure 2, results showed that 16 out of 18 students (about 89% of the group) improved on the post-test.



	01	02	03	04	05	06	07	08	09	10	12	13	14	15	17	19	20	21
Pre-test	53.65	76.83	81.27	74.6	89.21	70.16	79.05	79.05	82.22	76.83	70.48	68.25	66.98	81.27	77.14	74.6	95.87	62.54
Post-test	87.94	100	96.83	93.33	85.71	89.21	93.33	92.38	98.1	95.87	53.65	97.78	93.33	92.38	100	100	99.05	69.21

Figure 2. Pre- and post-test scores by student.

By learning objective, 80% of the post-test scores (representing 12 out of 15 objectives) stayed the same or showed improvement from the pre-test scores (as shown in Figure 3). There were three questions which scored less correct responses on the post-test than on the pre-test. These questions regarded objectives 3.4, 3.6, and 3.8 which asked students to correctly select the example that identifies a threat (i.e. identity theft, spear phishing, and cyberstalking).

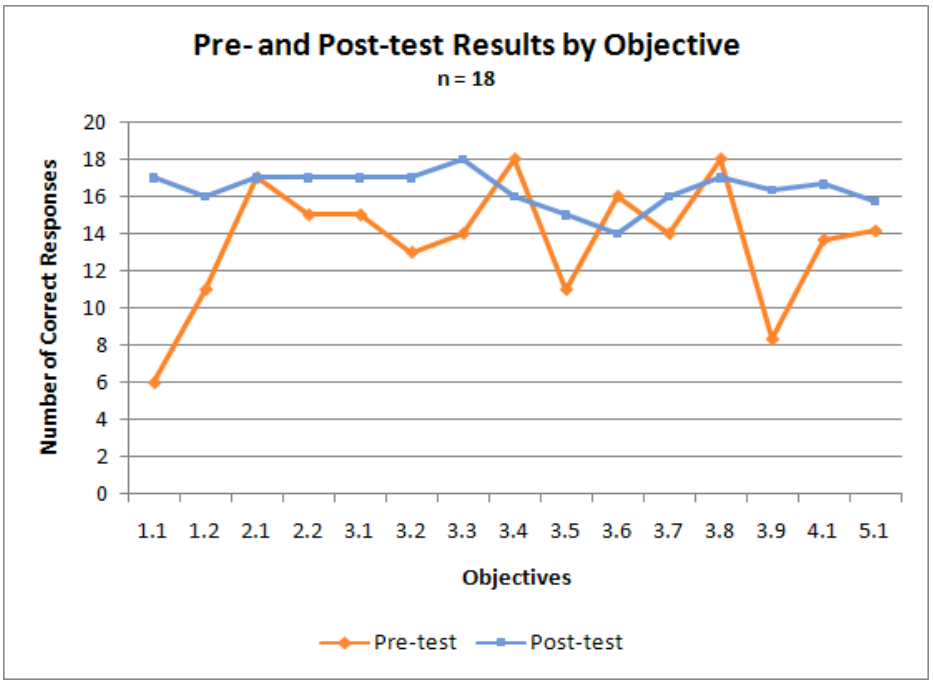


Figure 3. Pre- and post-test results by objective.

As for correct responses, each learning objective was met in the post-test with at least 15 or more students (about 83% of the total sample) correctly responding (as shown in Figure 3). Notably, the lowest number of correct responses for a post-test question was 14 (about 77% of the total sample) and it was also lower than the corresponding pre-test question result of 16 correct responses. This question regarded objective 3.6 which asked the students to correctly select the example that identifies how social networking sites can allow for spear phishing attacks.

Attitudes Towards the Module

Overall, the students had positive feedback regarding the module's content and format/design. Of the 15 exit surveys collected, all students either "agreed" or "strongly agreed" that the module: increased their knowledge and understanding about why it is important to protect privacy on social networking sites, thought that the layout of the module was logical and easy to follow, and thought that the multimedia aspects were appropriate and added value to their learning. Additionally, students commented that the module was very informative, made them more aware of privacy issues, and some even wanted to share the module with others (such as with their classes of students). On the other hand, some commented that they felt the module was too long.

The students felt that the module was very informative and they learned a couple of new things even if they did consider themselves at least somewhat knowledgeable about protecting privacy. One student commented, "The digital dossier and spear phishing were new to me, so I found those intriguing. I also didn't realize that you could never truly 'delete' digital data footprints that you leave in cyberspace."

Students reported that the videos were beneficial to their learning. One student commented, "The videos really helped to illustrate everything. I'm glad the module didn't require loads of reading." Another student commented, "The videos helped make the material relevant and entertaining without compromising the overall message." Students also found the recap/summary at the end of each section to be helpful "because it emphasized the important information" and "helped [to] reinforce the information".

Suggestions for Future Changes

Although successful in testing, the researcher felt that more could be done to improve the instructional module. First, the instructional content for objectives 3.4, 3.6, and 3.8 should be improved in a future revision due to the slight drop in correct responses on the corresponding post-test questions compared to the pre-test questions. All three objectives dealt with identifying which example puts one at risk to a privacy threat. Perhaps these objectives could be broken down further to explain different concepts associated with the threats and compromising scenarios.

Second, the researcher felt that Unit 5's instruction could be improved. How one chooses to protect privacy is a rather subjective topic. It is often situational and based on one's own preferences. For instance, privacy options that a college student who is promoting his music would probably configure his settings to be more public or may choose to share personal contact information compared to a college student who just wants to keep in touch with friends he already knows from school. The researcher considered several future changes to help students achieve the module's terminal objective in Unit 5 more effectively than what this current study has done. These changes included: using a different instructional approach, revising the existing Unit 5, and revising the assessment questions.

Different Instructional Approach

Since the nature and purpose of the instructional module was to deliver succinct informational content, the content could not always be elaborated in the many ways that it might have needed to be explained in Unit 5. Instead, some of the content had to be generalized or would present the most restrictive ways to protect privacy (such as configuring settings to be all private for the features in a profile). The researcher felt that it did not fully support what Unit 5 was supposed to which was really to be able to know what the appropriate actions would be to protect privacy, not to know how to have the most private settings. Perhaps it may be more effective to use a different instructional approach to teach Unit 5 such as in small group discussions with scenario-based activities to encourage the learners to think critically and apply concepts they learned to different situations.

Revising Unit 5

Another option could be to revise Unit 5 to elaborate on the scenarios before explaining what appropriate actions should be done to protect privacy. However, that may be text-heavy for the module. A better approach may be to change the content to instead, be a checklist of "questions to ask yourself when you are on social networking sites" and then having yes or no responses with the appropriate actions. This will then cover more options and with reasoning/tips of what to one can do rather than having one right or wrong answer. Figure 4 shows a possible example of the revised content for Unit 5.

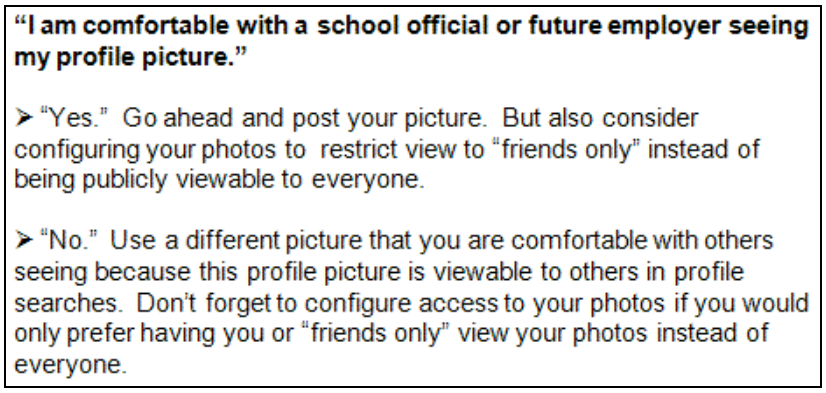


Figure 4. Possible example (excerpt) to be used in a revision for Unit 5.

Revising Unit 5's Assessment Questions

The assessment questions to test the content presented in Unit 5 could use revision. Originally, questions presented a screenshot/scenario and asked the student what he or she should do to protect privacy with 'yes' or 'no' answer choices. The problem with that was there had to be a definite right or wrong answer. However, without sufficient explanation, the scenarios might have been too general or may not have provided enough context making the "right" answer debatable. For example, one of the questions presented a profile picture of a woman in a bikini swimsuit, carrying a surfboard. The learner was asked if the woman should change her profile picture, 'yes' or 'no'. The right answer was 'yes', the woman should change her profile picture. Conversely, a student thought otherwise and commented, "I found the surfer picture to be tasteful and there wasn't anything wrong. I think an employer would see that she has an interest in surfing and nothing more." Thus, perhaps it would be clearer and more specific to revise the questions so that the learner would assist a decision presented in the scenario. Figure 5 shows a possible example question.

1. Molly is not comfortable with letting others see her current profile picture. What should she do?
    a) Leave her picture, but configure the settings so that "friends only" can see it
    b) Use a different picture
    c) Leave her picture because it has already been posted
    d) Post a picture of her friend as her profile picture instead

Figure 5. Possible example assessment question for Unit 5.

Conclusions

As several studies recommended (Barnes, 2006; European Network and Information Security Agency, October 2007; Tufekci, 2008), there is a need to educate young people about protecting privacy online especially since more and more of our daily activities are being done online. Overall improvements in post-test scores and positive feedback given from the exit surveys suggested that the instructional module was indeed effective in achieving its purpose to raise awareness and educate college students about protecting privacy on social networking sites.

Particularly, the students felt that the module's mix of textual and video content aided their learning and helped to reinforce concepts. Although, what could be improved is to have the videos embedded directly in the module instead of linked to the external (hosts') websites. But due to time and resource limitations, the researcher was unable to fulfill this.

The researcher found that the instructional module was effective in presenting informational content to the learners. But for learning objectives that required critical thinking and decision-making skills, such as making informed choices on what to do to protect privacy, a different format or instructional means may be more appropriate or effective. Further studies would be necessary to explore other options.

References

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook.* Paper presented at the Privacy Enhancing Technologies 2006.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).

Chen, C.-M. (2007). Intelligent web-based learning system with personalized learning path guidance. *Computers & Education, 51*, 787-814.

Donath, J., & Boyd, D. (2004). Public displays of connection. *BT Technology Journal, 22*(4), 71-82.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites [Electronic version]. *Journal of Computer-Mediated Communication, 12*(4), article 1.

European Network and Information Security Agency (October 2007). *ENISA position paper no.1 - Security issues and recommendations for online social networks.*

Lange, P. G. (2007). Publicly private and privately public: Social networking on YouTube. *Journal of Computer-Mediated Communication, 13*(1), article 18. Retrieved from http://jcmc.indiana.edu/vol13/issue1/lange.html

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). *Digital footprints: Online identity management and search in the age of transparency.* Washington, D.C.: Pew Internet & American Life Project.

Regan, P. M. (2002). Privacy as a common good in the digital world. *Information, Communication& Society, 5*(3), 382-405.

Russell Research (September 2006). CA/NCSA Social networking study report. 1-44.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36.