Evaluating Online Security Training for Journalists Through the Lens of Learning Science

Mahdi Nasrullah Al-Ameen
Clemson University
malamee@clemson.edu

Elizabeth Anne Watkins
Columbia University
eaw2198@columbia.edu

Byron Lowens
Clemson University
blowens@g.clemson.edu

Franziska Roesner
University of Washington
franzi@cs.washington.edu

Susan Mcgregor
Columbia Journalism School
sem2196@columbia.edu

Kelly Caine
Clemson University
caine@clemson.edu

ABSTRACT

Journalists are targets of computer security attacks because of the type, value, and temporally sensitive nature of information that they communicate with sources, colleagues, and eventually the public. One way journalists can help to prevent targeted attacks is by being well-aware of risks and taking appropriate security measures. Despite the existence of several security training modules specifically designed for journalists, many are still unaware of computer security concepts and procedures. In this paper, we identify existing online security training modules designed for journalists and evaluate them through the lens of learning science. We find that none of the security training modules we evaluated conformed to accepted learning science principles. We conclude by offering recommendations for the design of online security training targeted at journalists, where we emphasize on interdisciplinary research collaboration in developing such training.

Keywords

Journalists; Security training; Learning science principles

1. INTRODUCTION

As digital communication technologies improve, they help journalists perform an array of activities more quickly and effectively, including accessing information, doing research, communicating with sources, and filing stories. This technology, however, also puts them at the risk of attacks: 21 of the world's top-25 news organizations have been the target of hacking attacks [35]; in recent years, several prominent US news organizations including The New York Times, The Wall Street Journal, Bloomberg, and The Washington Post revealed that they have been targets of state-sponsored digital attacks designed to identify journalists' sources [28, 29]. As another example, Ethiopian Satellite Television Service (ESAT) employees were attacked with sophisticated computer spyware designed to steal secret credentials, and intercept Skype calls and instant messages [18].

Computer security training aims to make journalists aware of potential security threats and guide them to adopt appropriate security tools and behaviors [15]. While many online security training modules exist to train journalists on security concepts and behaviors [15], recent research [21, 22] indicates that individual journalists are not actively thinking about or protecting themselves from common attacks like phishing and malware. While a range of factors affect an individual's computer security behaviors—including organizational culture, task-specific requirements, and personal preferences [3, 4]—education about the security implications of one's behaviors is an important component.

In this work, we evaluate the educational efficacy of available online security training materials targeted at journalists. We focus on online training because it is among the most common training delivery format for journalists [23]. We ground our evaluation in learning principles established and validated by the learning sciences. Specifically, we evaluate the extent to which each module meets accepted principles of learning science and provide recommendations for improvement in cases where the training modules fall short.

We are not aware of prior work evaluating these materials. Although prior research [17] has offered an analysis of online anti-phishing training materials, these were materials targeted at general web users and focused on presentation details (e.g., number of words, pages, images, etc.) rather than the principles of learning science. Our focus is specifically on security training for journalists, because, as prior work found [21, 22], these users may be unaware of the specific security vulnerabilities and the corresponding countermeasures necessary for working with sensitive information in the public interest, especially while facing increasing surveillance and digital attacks.

In summary, in this paper, we analyze existing online security training modules through the lens of learning science. We find that none of the training modules we evaluate meets accepted principles from learning science, and we draw recommendations for improved training modules from our findings. This work is formative research to inform our eventual goal: to design an online security training module ensuring

Table 1: Online Security Training Modules: Through the Lens of Learning Science Principles [●: Leverages a learning principle, ○: Does not leverage a learning principle, ◑: Partially leverages a learning principle, env.: environment, T: Text, SI: Still Image, AV: Animated Video].

Training Modules	*Presentation*	*Learning Science Principles*						
		Learning-by-doing	*Immediate feedback*	*Conceptual procedural*	*Contiguity*	*Persona-lization*	*Story-based agent env.*	*Reflection*
APC [14]	T	○	○	●	○	●	○	○
FPF [25]	T+SI	○	○	●	◑	●	○	○
CIJ [12]	T+SI	○	○	●	◑	●	○	○
CPJ [33]	T	○	○	●	○	●	○	○
SKeyes [13]	T+AV	○	○	●	●	●	◑	○
WeFC [36]	T+SI	○	○	●	◑	●	○	○
FLD [9]	T	○	○	●	○	●	○	○
StoryMaker [32]	T+SI	○	◑	●	◑	●	○	●
Internews [16]	T	○	○	●	○	●	○	○
EFF [11]	T+SI+AV	○	○	●	◑	●	○	○

appropriate knowledge acquisition and retention for journalists, through a collaboration among information security, journalism, and HCI research community.

2. METHOD

We evaluated how well existing online security training modules for journalists conform to seven accepted learning science principles [2, 5, 7, 17, 19, 20, 31]. To identify available English-language security training modules designed for journalists, we manually searched the web using appropriate keywords in popular search engines (e.g., Google) and accessed training modules listed by Henrichsen et al. in their report prepared for UNESCO [15]. Because of our focus on online training modules, we excluded offerings that promoted specific security tools or advertised in-person training courses. Our final list includes all of the online security training modules that we found designed specifically for journalists. We note that though there may exist additional training modules that our search did not uncover, our set of ten modules covers many well-known organizations and provides an important first look at security training for journalists.

Computer Security Training Modules for Journalists. Through the above selection process, we identified the computer security training modules, all designed specifically for journalists by the following organizations: the Centre for Investigative Journalism (CIJ) [12], Freedom of the Press Foundation (FPF) [25], Electronic Frontier Foundation (EFF) [11], Committee to Protect Journalists (CPJ) [33], SKeyes Center for Media and Cultural Freedom [13], Association for Progressive Communications (APC) [14], Internews [16], Front Line Defenders (FLD) [9], StoryMaker [32], and We Fight Censorship (WeFC) [36] (See Table 1).

Learning Science Principles. Learning science principles refer to instructional design principles, developed by education researchers to guide the development of effective education and training materials. In this work, we use seven learning science principles as our evaluation criteria: learning-by-doing, immediate feedback, conceptual procedural, contiguity, personalization, story-based agent environment, and reflection. Our selection is in line with that of previous work [17], which used a set of learning principles for the evaluation of their anti-phishing education tool designed for general web users.

3. RESULTS

We report results on how well existing online security training modules for journalists implement each of the seven learning science principles (see Table 1 for a summary).

3.1 Learning-by-doing

Adaptive Control of Thought-Rational (ACT-R) is one way to model human cognition and learning, which aims to define the basic and irreducible cognitive and perceptual operations that enable the human mind [2]. One of its primary contributions to learning science is the conclusion that knowledge and skills are acquired and strengthened through practice [2]. For example, students whose learning is followed by practice perform better than the students who do not practice [1].

None of the security training modules we evaluated leverages learning-by-doing, and thus the trainees did not get hands-on experience of using a security tool as a part of the training.

3.2 Immediate Feedback

As shown in prior study [8], it is important to provide immediate feedback during the knowledge-acquisition phase to ensure efficient learning and proper guidance towards correct behavior, where providing immediate feedback, rather than delayed feedback, results in significantly better performance from the students.

The security training module developed by StoryMaker partially leverages this principle. In this module [32], users are presented with multiple choice questions at the conclusion of each section. The system immediately informs the user whether the given answer is correct. However, completing these questions is not required by the training [32], and the system does not respond to open questions from users [32].

3.3 Conceptual Procedural

Concept is a mental representation or prototype of objects or ideas (e.g., malware) [6]. *Procedure* refers to clearly defined steps for the successful completion of a task (e.g., logging into an account) [6]. According to the *conceptual-procedural principle*, conceptual and procedural knowledge are built together in an iterative process, influencing one another in mutually supportive ways. The findings from prior research [31] support this learning principle: presenting students with concepts and procedures in an interwoven pattern had a better impact on learning, as compared to giving students all of the concepts followed by all of the procedures.

This learning principle is leveraged by all of the security training modules in our research. For instance, in the section on "Anonymous Communication", the operation of how to use an anonymous communication tool (e.g., Tor) is presented just after the concept of anonymity. However, the modules differ on exactly how concepts and procedures are presented to users, with four of ten modules using only textual information [9, 14, 16, 33], and others exploit graphical interpretation of security concepts with still images or animated videos [11–13, 25, 32, 36]. The Electronic Frontier Foundation (EFF) is an exception in this case, using both still images and animated videos for security training [11].

3.4 Contiguity

According to the contiguity principle [20], presenting words and pictures contiguously (rather than isolated from one another) in time and space increases the effectiveness of computer-aided instructions, which is supported by the findings in later research [24]. Using comic strips in security education is an example of leveraging the contiguity principle [17], where users are presented with graphical characters and their contiguous conversations in text form. Using comic strips is more effective in knowledge acquisition than plain text [17]. However, none of the security training modules we evaluated uses comic strips.

The training modules [9,14,16,33] that use only text cannot exploit the contiguity principle. By contrast, we found that the training modules using a combination of text and images partially satisfy the contiguity principle [12, 25, 32, 36], where images and text are placed contiguously in some sections and separately in others. The security training module developed by SKeyes Center for Media and Cultural Freedom adheres to the contiguity principle, where animated videos are presented with integrated text [13]. Four sections of the training module designed by Electronic Frontier Foundation (EFF) satisfy this learning principle by splicing text in animated videos.

3.5 Personalization

According to Clark and Mayer [7], conversational style is a better approach to deliver knowledge than formal. The prior research [19] suggests that using "I", "we", "me", "my", "you", and "your" in instructional materials contributes to enhanced learning. People become more engaged and learn better if the material makes them feel that they are part of a conversation rather than passively receiving information.

All security training modules we analyzed leverage the personalization principle, as they follow a conversational style in security training by using the terms "we", "you", and "your".

3.6 Story-based Agent Environment

Studies show that learning is enhanced if instructional materials are presented within the context of a story [19], where people are more motivated to learn when guided by an agent [17]. Here, agents are cartoonish or real-life characters presented either visually or verbally.

The security training module developed by SKeyes Center for Media and Cultural Freedom partially leverages this learning principle [13] by, instead of visual or verbal agent, using a background voice to explain security concepts and procedures in the context of a story. For example, an animated video about protecting a source's identity presents a scenario where a journalist meets his source, and then shows a step-by-step process that the journalist can adopt to ensure security and privacy while communicating with sources. While four out of 43 sections in the training module of the Electronic Frontier Foundation [11], use animated videos, none offers security training in the context of a story, or uses any visual or verbal agent to guide users.

The study of Kumaraguru et al. [17] used the image of an agent, in the form of still picture, to train users on identifying phishing emails, and found this method to be more effective in security education than plain text.

3.7 Reflection

Reflection is the process by which learners get an opportunity to pause and think about what they are learning, and its implications [5]. The research [5] suggests that educational systems should offer opportunities for learners to reflect on their newly acquired knowledge.

Out of ten security training modules analyzed in this research, the one from StoryMaker helps users to reflect on their learning by including a set of multiple choice questions at the end of each training section, where questions are related to the content of that section [32]. For example, the question: "What is the best way to avoid being tracked by my mobile phone?" is featured at the end of a section titled, "How does my mobile phone put me at risk?".

Because the questions in this module are optional to answer [32], they cannot be relied upon to measure the progress of trainees. It is possible to force users to answer the questions before they can move on to the next section. However, this may increase the overall training time and/or cause frustration for users, impacting usability. An opportunity for future work is investigating the appropriate balance between knowledge acquisition and usability of a training module.

4. RECOMMENDATIONS

In this section, we provide recommendations for the design of computer-security training for journalists, and furnish examples of how to implement such recommendations. Based on our findings above, we recommend deploying the following strategies in an online security training module for journalists: i) User Interaction, ii) Graphical Presentation, iii) Evaluation of Learning, and iv) Leveraging Professional Motivation.

4.1 User Interaction

It is imperative that a security training module not only explains the security concepts and procedures, but also lets the trainees have hands-on learning experience (i.e., learning-by-doing) and immediate feedback from the system.

None of the training modules we evaluated leverages learning-by-doing. We recommend that a security training module leverage learning-by-doing in the form of practice. For example, after presenting information about how to use an encrypted email service, a trainee could be asked to actually install an encrypted email service and send a dummy encrypted email to the training server before proceeding to the next phase of training.

One of the training modules that we evaluated partially leverages immediate feedback. To fully leverage this learning principle, a training module should let the trainees ask open questions through its user interface, and provide users with immediate feedback. In this case, the training module could present users with a "question-box" (e.g., a text-field on the webpage) to let them ask questions any time. We note that designing an automated or otherwise efficient process for providing a user with the most appropriate answer to her question is an independent research problem.

4.2 Graphical Presentation

Graphical presentation in a training module is important to leverage conceptual procedural and contiguity principles. However, 40% of the security training modules analyzed in this research use only text to deliver knowledge.

The study of Bada and Sasse [3] depicts that a persuasive message should have four characteristics: i) it needs to attract attention; ii) it must be understood; iii) it must relate to a matter worthy of processing; and iv) its contents will need to be stored and recalled easily from memory. The prior study [17] shows the effectiveness of graphical contents in knowledge acquisition and retention through the process of gaining users' attention, illustrating the importance of secure behavior, and offering clear understanding of security concepts. Also, graphical information is easier to remember than plain text because of the picture-superiority effect [26]. Especially because computer security topics often involve concepts that are invisible and abstract, such as the Internet or encryption, the use of graphical representations may be particularly powerful for security training modules.

Thus, either in the form of still image or animated video, we recommend that a training module exploit graphical presentation, and provide an agent to guide users through security concepts and procedures. Animated video, for example, leverages "vicarious experience", which refers to vivid stories that allow the listener to become a participant by identifying with a character [27]. The study of Patterson et al. [27] shows that changing the emotion associated with an activity is a powerful way to motivate the change in behavior (e.g., security behavior), while "vicarious experience" is an effective technique to influence emotions. Future work should investigate which graphical presentation (e.g., image, animated video, comic strip) performs best for knowledge acquisition and retention of particular aspects of information security-related content.

4.3 Evaluation of Learning

In the Results section, we explain how the reflection principle is leveraged through the evaluation of users' learning. As we found, only one of the security training modules reviewed evaluates the learning of trainees, which asks multiple choice questions at the end of each training section. We recommend that a training module should also let a user reflect on her learning by presenting her with a scenario that is common in her profession, and then ask how she would use her learning to handle that situation in a secure and privacy-preserving way. For example, to reflect upon the knowledge on "anonymous communication" and "verifying source material", a journalist could be asked how she would balance the needs to protect a source's identity and ensure the credibility of information received from that source.

4.4 Leveraging Professional Motivation

The study of Uskul et al. [34] showed that messages are more persuasive when there is a match between the recipient's motivational characteristics and the content of the message. So, it is important to identify the motivation and prior knowledge of target users before designing a security training module.

Protecting sources is one of the prime security concerns of journalists [21, 22], and thus, should be an important motivation for them to adopt better security practices. Several of the training modules presented in this paper (e.g., [13,32]) devote space to explaining how to protect a source's identity. We recommend that modules leverage this motivation to nudge journalists towards adopting additional security practices. For example, consider phishing attacks, a type of threat on the rise against journalism organizations [30], but of which individual journalists may not be sufficiently cognizant [22]. To motivate journalists to take precautions against such attacks, they should be informed about the possible consequences: failing to identify phishing emails could lead to accidentally revealing information about a protected source (e.g., clicking on a malicious link in an email could lead to a spyware infection, remotely sending source information to the attacker, or an account compromise).

Presenting the security issues in the context of target profession (e.g., journalism) motivates the trainees to better focus on learning, whereas people possess a tendency to care less about "distant" harms [10]. Also, any security training that "feels" generalized so as to apply to many different professions fails to motivate the targeted professionals to change their behavior [37].

5. CONCLUSION

By subjecting the designs of security training modules for journalists to a learning-science-based analysis, we identify a gap between current designs and those that would satisfy learning science principles. We fill in the gap with a set of recommendations, and identify the potentials for future research through a collaboration among information security, journalism, and HCI community. Our work is a primary but important step towards designing a security training module satisfying appropriate knowledge acquisition and retention for journalists. Our recommendations for effective security training modules for journalists, especially around finding the unique professional motivation to leverage, may be applicable to other professions as well.

6. REFERENCES

[1] V. A. Aleven and K. R. Koedinger. An effective metacognitive strategy: Learning by doing and explaining with a computer-based cognitive tutor. *Cognitive science*, 26(2):147–179, 2002.

[2] J. Anderson. Rules of the mind lawrence erlbaum associates. *Hillsdale, NJ*, 1993.

[3] M. Bada and A. Sasse. Cyber security awareness campaigns: Why do they fail to change behaviour? 2014.

[4] J. M. Blythe, L. Coventry, and L. Little. Unpacking security policy compliance: The motivators and barriers of employeesâĂŹ security behaviors. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 103–122, 2015.

[5] J. Bransford, A. Brown, and R. Cocking. Committee on developments in the science of learning. national research council. *How people learn: Brain, mind, experience, and school*, 2000.

[6] R. Clark. Developing technical training: A structured approach, 1989.

[7] R. C. Clark and R. E. Mayer. *E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning.* John Wiley & Sons, 2016.

[8] A. T. Corbett and J. R. Anderson. Locus of feedback control in computer-based tutoring: Impact on learning rate, achievement and attitudes. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 245–252. ACM, 2001.

[9] F. L. Defenders. Security in-a-box. `https://securityinabox.org/en`, Accessed: August 2016.

[10] P. Dolan, M. Hallsworth, D. Halpern, D. King, and I. Vlaev. Mindspace: influencing behaviour through public policy [internet]. london: Institute for government; c2010, Accessed: March 31, 2012.

[11] E. F. F. (EFF). Surveillance self-defense. `https://ssd.eff.org/en`, Accessed: August 2016.

[12] T. C. for Investigative Journalism (CIJ). Information security for journalists. `http://tcij.org/resources/handbooks/infosec`, Accessed: August 2016.

[13] S. C. for Media and C. Freedom. The journalist survival guide. `http://video.skeyesmedia.org`, Accessed: August 2016.

[14] A. for Progressive Communications (APC). Digital security first-aid for human rights defenders. `https://www.apc.org/en/irhr/digital-security-first-aid-kit`, Accessed: August 2016.

[15] J. R. Henrichsen, M. Betz, and J. M. Lisosky. *BUILDING DIGITAL SAFETY FOR JOURNALISM.* United Nations Educational, Scientific and Cultural Organization, 2015.

[16] Internews. Speak safe toolkit. `https://www.internews.org/sites/default/files/resources/Internews_SpeakSafeToolkit.pdf`, Accessed: August 2016.

[17] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):7, 2010.

[18] B. Marczak, J. Scott-Railton, and S. McKune. Hacking team reloaded? us-based ethiopian journalists again targeted with spyware. *The Citizen Lab*, March 2015.

[19] R. E. Mayer. Multimedia learning. *Psychology of learning and motivation*, 41:85–139, 2002.

[20] R. E. Mayer and R. B. Anderson. The instructive animation: Helping students build connections between words and pictures in multimedia learning. *Journal of educational Psychology*, 84(4):444, 1992.

[21] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner. Investigating the computer security practices and needs of journalists. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 399–414, 2015.

[22] S. E. McGregor, F. Roesner, and K. Caine. Individual versus organizational computer security and privacy concerns in journalism. *Proceedings on Privacy Enhancing Technologies*, 4:1–18, 2016.

[23] D. Monahan. Security awareness training: It's not just for compliance. Technical report, Enterprise Management Associates (EMA) Research Report, April 2014.

[24] R. Moreno and R. E. Mayer. Cognitive principles of multimedia learning: The role of modality and contiguity. *Journal of educational psychology*, 91(2):358, 1999.

[25] F. of the Press Foundation. Encryption works: How to protect your privacy in the age of nsa surveillance. `https://freedom.press/encryption-works`, Accessed: August 2016.

[26] A. Paivio. *Mind and Its Evolution: A Dual Coding Theoretical Approach.* Lawrence Erlbaum: Mahwah, N.J., 2006.

[27] K. Patterson, J. Grenny, et al. *Influencer: The power to change anything.* Tata McGraw-Hill Education, 2007.

[28] N. Perlroth. Hackers in china attacked the times for last 4 months. *NY Times, Jan*, 30, 2013.

[29] N. Perlroth. Washington post joins list of news media hacked by the chinese. *The New York Times*, 1, 2013.

[30] A. Press. Hackers compromise ap twitter account. `http://bigstory.ap.org/article/hackers-compromise-ap-twitter-account`, April 2013.

[31] B. Rittle-Johnson and K. R. Koedinger. Comparing instructional strategies for integrating conceptual and procedural knowledge. 2002.

[32] StoryMaker. Security lessons. `https://storymaker.cc/lessons/?Nav=/2&Lang=en`, Accessed: August 2016.

[33] C. to Protect Journalists (CPJ). Journalist security guide. `https://cpj.org/reports/2012/04/journalist-security-guide.php`, Accessed: August 2016.

[34] A. K. Uskul, D. K. Sherman, and J. Fitzgibbon. The cultural congruency effect: Culture, regulatory focus, and the effectiveness of gain-vs. loss-framed health messages. *Journal of Experimental Social Psychology*, 45(3):535–541, 2009.

[35] J. Wagstaff. Journalists, media under attack from hackers: Google researchers, March 2014.

[36] W. F. C. (WeFC). Online survival kit. `http://www.wefightcensorship.org/online-survival-kithtml.html`, Accessed: August 2016.

[37] M. Wilson and J. Hash. Building an information technology security awareness and training program. *NIST Special publication*, 800:50, 2003.