Choose Your Own Hacking Adventure: Contextualized Storytelling to Enhance Security Education and Training

Ersin Dincelli
University of Colorado Denver
Denver, CO 80202, USA
ersin.dincelli@ucdenver.edu

InduShobha Chengalur-Smith
University at Albany, SUNY
Albany, NY 12222, USA
shobha@albany.edu

Abstract
Most cybersecurity incidents and data breaches have been caused by human error and negligence. Therefore, there has been a keen interest in developing security education and training programs to mitigate users' security lapses. This study proposes a contextualized and participatory storytelling approach in which learners alter the course of the storyline by making their own decisions, determine the main character's actions, and the outcome of the storyline. The proposed "choose your own adventure" style storyline allows learners to determine security threats that they are most susceptible to and provides personalized feedback based on the threat outcomes they encounter. Such interactive and participatory approaches that provide personalized feedback and mnemonics can be an effective tool for educating users about complex cybersecurity threats.

Author Keywords
Storytelling; contextualized learning; security education and training; SETA; usable security; human factors.

ACM Classification Keywords
H.1.2 Information Systems: User/Machine Systems – Human Factors.

"There's nothing in the world more powerful than a good story."

- Tyrion Lannister

"In simple terms, people learn from stories. They want a sense of what's the journey they're on that gives them their bearings"

- Barack Obama

"Storytelling reveals meaning without committing the error of defining it."

- Hannah Arendt

Introduction

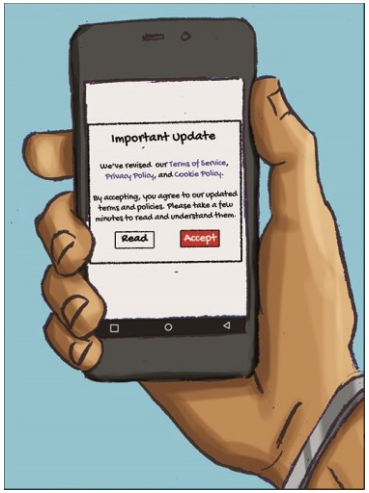
Security education, training, and awareness (SETA) programs aim to inform users about potential security threats and increase their awareness to reduce the likelihood of security incidents. However, SETA programs have not yet demonstrated their effectiveness as human error and exploitation of human weaknesses by hackers were considered the main causes of the majority of the security incidents [14]. This may be partly due to the fact that traditional SETA programs are narrowly focused on technical issues, not contextualized, and designed as one-size-fits all [3]. Additionally, such generic security interventions require a great deal of cognitive effort from users [9], which may potentially lead to security fatigue [17], promoting habits and emotions that compromise users' security behaviors [13]. A pedagogy that focuses on contextualization of abstract security topics in a feedback-rich and engaging environment has been suggested as a more effective teaching method [15].

Considering the fact that security involves complex and abstract concepts, contextualized learning approaches that engage learners can boost learning outcomes [15]. To this end, we propose the use of contextualized storytelling to educate learners about security threats by establishing relevance and personalized feedback through storytelling. In particular, we designed a visual, "choose your own adventure" style, storyline in which learners make their own decisions, determine the main character's actions, and the outcome of the storyline. Our intervention allows learners to alter the course of the storyline, determines the security threat that they are most susceptible to, and provides personalized feedback based on the threat outcome(s) they encounter.

Background and Related Work

Storytelling is one of the oldest forms of teaching. For centuries, people have learned from myths, legends, folk tales, and stories. Storytelling involves a narrative that illustrates complex interconnections between diverse events, agents, and abstract concepts [7]. Framing knowledge as a sequence of actions and their subsequent effects, connected together to establish a plot, more closely resembles how people learn from others' experiences [19]. The plot transforms singular situated experiences into a framework of successive events with causal linkages, which enables individuals to make sense of the events by reconstructing the experiences and embedding it in an information-rich context.

Stories make learning fun and more enjoyable, which results in a more *engaging* learning process. Engaging participants in the learning process creates interest and increases their attention, resulting in a *deeper* and *longer-lasting learning*. Stories allow examination of various outcomes through human actions. For example, in the context of cybersecurity, stories not only can convey how to avoid various security threats, they can also show potential consequences of the threat by making relations among various decisions, events, and outcomes. Stories bring information to life and *stimulate learners' imagination*, encouraging them to think of a wide range of potential outcomes that could result from different circumstances [1]. Therefore, learners go beyond simply receiving information and engage in *active learning*. Exposing people to ideas about security through games or stories improves their understanding of the diversity of potential threats and makes it more likely that they will engage in security and privacy behaviors that require time and effort [5].



Do you think Taylor should read the updated privacy policy?

- *Read the privacy policy.*
- *Accept the privacy policy without reading it.*

Figure 1. A decision point in the storyline

Note: The storyline includes various decision points. Participants can alter the course of events in the storyline based on the decisions they make. Certain decisions are affiliated with a particular outcome, allowing them to determine the threat they are most susceptible to.

The human brain learns and remembers by *making associations*. Stories help illustrate how abstract concepts relate to real world examples, more effectively *teaching abstract* and *complex subjects*. The process of actively using knowledge through imagination extracts *more meaning* from the learning material, facilitating storage of the information in long-term memory, which increases the likelihood of *retaining* and *recalling* the information. Therefore, stories increase retention and make the learning outcomes *more memorable* [10].

Storytelling can take various forms, including aural, textual, visual or combination of aural and visual (e.g., cartoons), and textual and visual (e.g., comics). Visual content can lead to better comprehension and retention of the information compared to aural and textual storytelling. Textual content is stored in our short-term memory where we can only retain up to 9 bits of information [11]. Visual content, on the other hand, go into our long-term memory where information is stored over an extended period of time [2]. The human brain processes visual information more effectively. The brain processes an image in 150 milliseconds, 60,000 times faster than text [8], and attaches a meaning to it in approximately 100 milliseconds [18].

Storytelling could also be participatory by providing learners a role to play in the story. Training that is contextual and interactive, and provides opportunities for reflection, is more likely to be effective. In role-play stories, learners take the role of a character, interact with other characters, and make decisions that would help them actualize the consequences of different decisions. Role-play can enhance the immersiveness of storytelling by not just describing the actions but also allowing participants to perform them, thus allowing participants to contribute to the construction of the reality being depicted [16]. Dale [4] compared the effectiveness of aural, textual, visual, and participatory presentation styles. He found that learning recall for aural and textual presentations were the least effective for both short-term and long-term recall. Visual and participatory presentations were the most effective for both short-term and long-term recall.

Method

We propose a participatory storyline in which learners make decisions throughout a visual narrative involving various security threats. The proposed "choose your own adventure" style interactive storyline has three main functions: (1) enable learners to make decisions and alter the course of the storyline, (2) determine the threat that they are most susceptible to, and (3) debrief them about the threat. Decisions made throughout the storyline determine how the story ends, i.e. the threat the learner is most susceptible to, as each decision is tied to a specific threat. The identification of the most relevant threat triggers a debriefing explaining the threat, the decisions that led to the threat, and countermeasures to prevent it. Figure 1 presents a decision point in the storyline.

The storyline was designed to reflect the security threats affiliated with social media use. To ensure that the storyline was contextualized, we followed a belief elicitation process to collect information from a college student sample (n = 47) who actively used social media. Participants were asked to identify five different types of security threats and explain how those threats could affect the users. These short cases were used to outline the narrative. After outlining the narrative, a script and accompanying scenes were drafted by the researchers

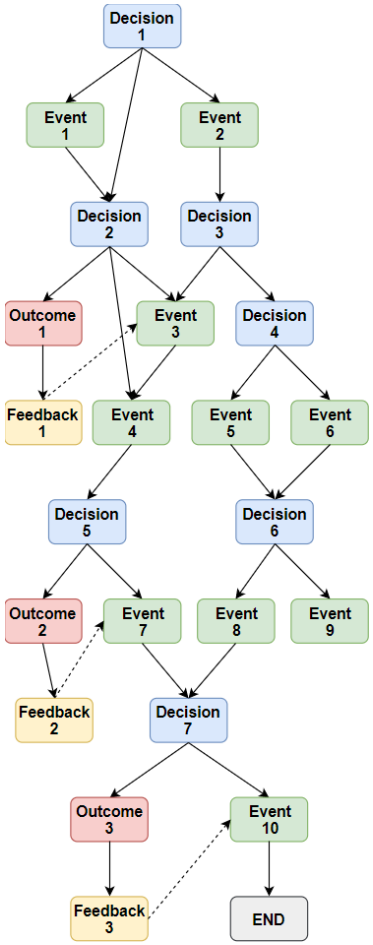


Figure 2. A part of the narrative structure involving seven decision points leading to three outcomes.

Note: Event scenes are included to improve the flow of the storyline and add context. Feedback scenes provide debriefing about the threat outcomes.

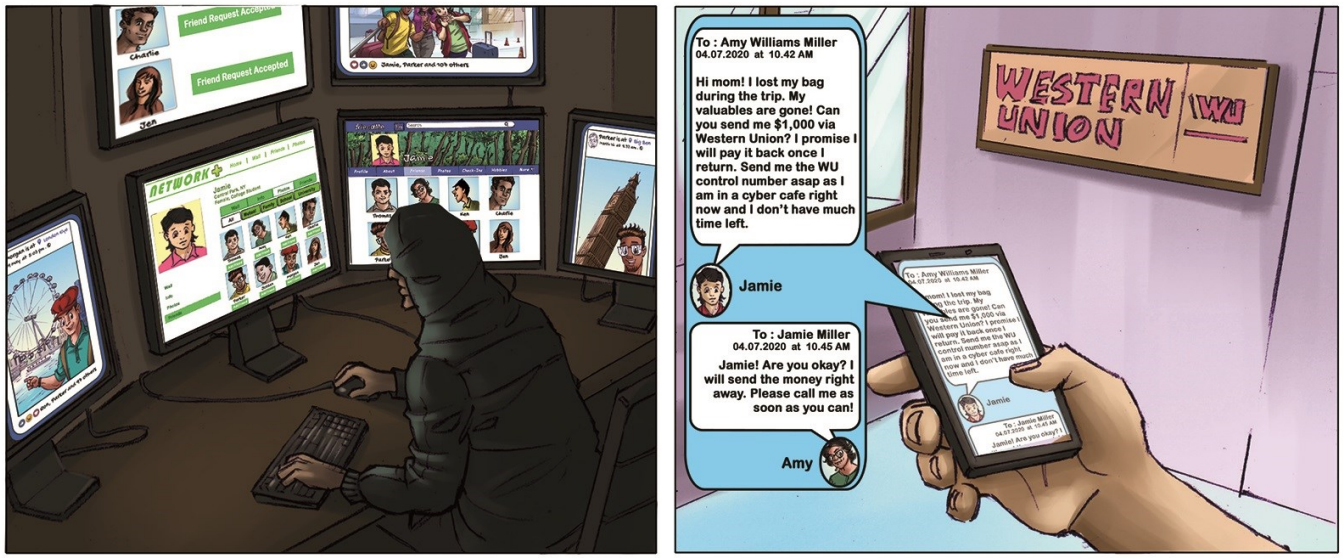


Figure 3. An example of an outcome scene. The participant's decisions led her to identity theft by cross-site profile cloning.

for the visual narrative. A professional artist was hired to draw the scenes. Due to the size of the visual narrative, we cannot present it in its entirety. Figure 2 shows a part of the branching storyline logic. Figure 3 presents an outcome scene from the visual narrative.

Preliminary Results

We conducted a randomized-control, longitudinal experiment comparing the *storyline group* with an *email group* that received security warnings via emails and a *control group* that received no interventions. The preliminary results indicated that the storyline was significantly more effective than both the security warning emails and the control group in terms of increasing participants' awareness and reducing their intention to disclose personal information. Figure 4 presents the results of the independent sample *t*-test.

Conclusion

The power of storytelling lies in its ability to boil down complex and abstract concepts into meaningful life experiences. When used in a training context, participatory storytelling approaches facilitate the development of strong connections to the training material. This kind of self-directed learning in an interactive environment adds context and relevance to the tasks in the training program and provides participants more meaningful learning experiences. Our proposed approach enables contextualization of the training material based on the characteristics of specific audience. For example, certain populations are more likely to be targeted by certain threats than others. Young adults are more susceptible to cyber stalking that can take place on social media, whereas, elderly people are more susceptible to financial fraud that can

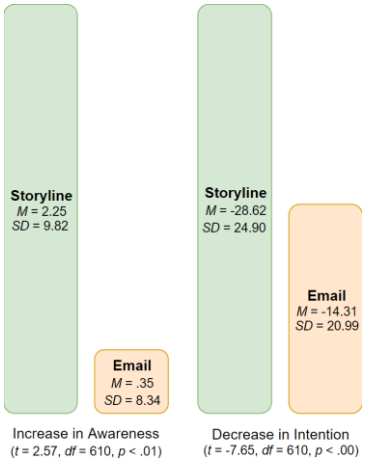


Figure 4. Preliminary results of the independent sample *t*-test comparing contextualized storyline and email groups in increasing awareness and reducing intention to disclose personal information.

Note: Panel data was collected from Amazon Mechanical Turk workers (n = 612). The survey instruments for *awareness of disclosing personal information* and *intention to disclose personal information* were adapted from previously validated scales. Study constructs were measured using seven-point semantic scale. Reliability, construct validity, and discriminant validity of the scales were satisfactory.

be carried out by vishing attacks [12]. Similarly, working professionals are more likely to be targeted by spear phishing attacks [6]. By adapting the characters, events, and outcomes based on the characteristics of the target audience, the training material can be further contextualized to improve its effectiveness.

References

1. Jerome S. Bruner. 1996. *The Culture of Education*. Harvard University Press, Cambridge, UK.
2. Lynell Burmark. 2002. *Visual Literacy: Learn To See, See To Learn*. Association for Supervision and Curriculum Development, Alexandria, VA.
3. John D'Arcy and Anat Hovav. 2009. Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, 89(1): 59-71.
4. Edgar Dale. 1969. *Audiovisiual Methods in Teaching* (3rd. ed.). Holt, Reinhart & Winston, New York, NY.
5. Tamara Denning, Tadayoshi Kohno, and Adam Shostack. 2013. Control-Alt-Hack™: A card game for computer security outreach and education. In *Proceedings of the 44th ACM Technical Symposium on Computer Science Education* (SIGCSE '13).
6. Sanjay Goel, Kevin Williams, and Ersin Dincelli. 2017. Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1): 22-44.
7. David Hutchens. 2015. *Circle of the 9 Muses: A Storytelling Field Guide for Innovators and Meaning Makers*. John Wiley & Sons, Hoboken, NJ.
8. David Hyerle. 2000. *A Field Guide to Using Visual Tools*. Association for Supervision and Curriculum Development, Alexandria, VA.
9. Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Proceedings of the 11th Symposium on Usable Privacy and Security* (SOUPS '15), 327-346.
10. Jean M. Mandler and Nancy S. Johnson. 1977. Remembrance of things parsed: Story structures and recall. *Cognitive Psychology*, 9(1): 111-151.
11. George A. Miller. 1956. The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63(2).
12. Rachel E. Morgan and Britney J. Mason. 2014. *Crimes Against the Elderly, 2003-2013*. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, Washington, DC.
13. Simon Parkin, Kat Krol, Ingolf Becker, and M. Angela Sasse. 2016. Applying cognitive control modes to identify security fatigue hotspots. In *Proceedings of the 12th Symposium on Usable Privacy and Security* (SOUPS '16), 1-6.
14. Ponemon Institute Research Report. 2017. *State of Cybersecurity in Small & Medium-Sized Businesses*.
15. Jungwoo Ryoo, Angsana Techatassanasoontorn, Dongwon Lee, and Jeremy Lothian. 2011. Game-based InfoSec education using OpenSim. In *Proceedings of the 15th Colloquium for Information Systems Security Education*, 101-106.
16. Ulrike Schultze and Wanda J. Orlikowski. 2010. Virtual worlds: A performative perspective on globally distributed, immersive work. *Information Systems Research*, 21(4): 810-821.
17. Brian Stanton, Mary F. Theofanos, Sandra Spickard Prettyman, and Susanne Furman. 2016. Security fatigue. *IEEE IT Professional*, 18(5): 26-32.
18. Simon Thorpe, Denis Fize, and Catherine Marlot. 1996. Speed of processing in the human visual system. *Nature*, 381(6582): 520-522.
19. Rick Wash and Molly M. Cooper. 2018. Who provides phishing training?: Facts, stories, and people like me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18).