International Journal of Human-Computer Interaction

ISSN: 1044-7318 (Print) 1532-7590 (Online) Journal homepage: https://www.tandfonline.com/loi/hihc20

The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity

Leah Zhang-Kennedy, Sonia Chiasson & Robert Biddle

To cite this article: Leah Zhang-Kennedy, Sonia Chiasson & Robert Biddle (2016) The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity, International Journal of Human-Computer Interaction, 32:3, 215-257, DOI: 10.1080/10447318.2016.1136177

To link to this article: https://doi.org/10.1080/10447318.2016.1136177

Intl. Journal of Human–Computer Interaction, 32: 215–257, 2016

ISSN: 1044-7318 print / 1532-7590 online
DOI: 10.1080/10447318.2016.1136177

Taylor & Francis
Taylor & Francis Group

The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity

Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle
School of Computer Science, Carleton University, Ottawa, Ontario, Canada

Although computer security technologies are the first line of defense to secure users, their success is dependent on individuals' behavior. It is therefore necessary to persuade users to practice good computer security. This interview analysis of users' conceptualization of security password guessing attacks, antivirus protection, and mobile online privacy shows that poor understanding of security threats influences users' motivation and ability to practice safe behaviors. An online interactive comic series called *Secure Comics* was designed and developed based on instructional design principles to address this problem. An eye-tracking experiment suggests that the graphical and interactive components of the comics direct users' attention and facilitate comprehension of the information. In the evaluations of *Secure Comics*, results from several user studies show that the comics improve understanding and motivate positive changes in security management behavior. The implication of the findings to better understand the role of instructional design and persuasion in education technology are discussed.

1. INTRODUCTION

Home computer systems are largely administered by end-users with little security knowledge. These systems include password mechanisms, password managers, malware and spyware detection software, intrusion recovery software, personal firewalls, and privacy tools. Even though many of these systems are automated and act as the first line of defense against security threats, certain security decisions and system management tasks still require user attention. Some expert argue that users should be kept out of the security decision loop (Nielsen, 2004), but due to the complexity and rapid evolution of security threats, it is most likely that secure solutions in the near future will continue to include intervention. An integrated approach of training and improving the security and usability of secure technologies is more likely to produce a holistic solution to securing end-user computer systems.

Address correspondence to Leah Zhang-Kennedy, School of Computer Science, Carleton University, Ontario, Canada. E-mail: leah.zhang@carleton.ca

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/hihc.

Increasing security awareness enables users to make informed decisions and encourages compliance with security policies and advice provided by experts. Studies in Usable Security (e.g., Kumaraguru et al., 2007; Sheng et al., 2007) show that training can successfully communicate threats to users. The problem is that users are typically uninterested in learning about security (Whitten & Tygar, 1999). We propose that persuasion, implemented through instructional design elements, can be applied to security training to increase appeal, comprehension, and memorability of security information.

Unlike many corporate workers, home users are not subject to mandatory training and are unable to delegate the maintenance of security software to expert technical staff (C. L. Anderson & Agarwal, 2010). Having nonexpert users manage essential security tasks represent a significant point of weakness in securing computer security systems. As a result, there was an upsurge of research in security education in the past few years, which we summarize in our background section.

We study two research questions. First, what are end-users' initial conceptualizations of password guessing attacks, malware protection, and mobile online privacy? Second, do integrated visual—textual–interactive education material form a memorable and persuasive approach for computer security understanding by altering user perception and improving user behavior?

To address the first research question, we build on prior work in Usable Security (Asgharpour, Liu, & Camp, 2007; Camp, 2009; Wash, 2010; Raja, Hawkey, Hus, Wang, & Beznosov, 2011) that identifies users' mental models of security threats. We provide a qualitative analysis of semistructured interviews that capture users' conceptualizations, attitudes, and perceptions toward three security areas: password-guessing attacks, antimalware protection, and mobile online privacy. The results of our analysis show that users' poor understanding of security threats and defense strategies impede their motivation and ability to carry out basic security tasks.

To address the second research question, we created a humorous, interactive three-part comic series drawn and implemented by us to help to motivate learners' interest in the aforementioned computer security topics essential in everyday computing. Our work focuses on building security knowledge

about passwords, malware protection, and mobile online privacy without burdening users with technical details (which most users find uninteresting). Rather, we aim to build situational awareness of the risks and sensible protection strategies that empower users to make their own decisions leading to positive security outcomes. *Secure Comics* are fully available online (http://www.versipass.com/edusec). During development, our designs were refined through an eye-tracking experiment, in which we made possible connections between visual attention and comprehension of the information. After completion of the design, we followed up with empirical testing from multisession user studies with 52 users, which showed increased knowledge and positive behavioral changes.

The organization of this article is as follows. In Section 2, we provide background on Usable Security and identify its key challenges, and we outline the security areas addressed in the article. In Section 3, we review the literature on the instructional design principles that we applied and their media approach. We give a summary of our preliminary infographic studies on security metaphors in Section 4, before moving on to the design of *Secure Comics* in Section 5, where we give a detailed rationale for using comics to educate and describe ways in which instructional design principles are applied. In Section 5.4, we report the results of an eye-tracking experiment that we conducted to improve the comic design. In Section 6 we describe the methodology for our main user studies, then present the results of our experiments in Sections 7 to 9. Although the focus of this article is computer security, our findings and design approach may be generalizable to many different areas. We conclude the article by summarizing the key findings and discussing their implications for designing persuasive education systems.

2. UNDERSTANDING USABLE SECURITY

2.1. Usable Security Challenges

Users are sometimes regarded as the "weakest link" in computer security because attackers exploit the human link in the security chain (A. Adams & Sasse, 1999). Usable Security recognizes that the design of technical security mechanisms to protect users should consider human factors in their design because even the most secure system could fail if it has poor usability. For example, in password security, there is evidence that many users do not comply with password rules (A. Adams & Sasse, 1999) due to usability challenges, such as the difficulty of remembering stronger passwords. In addition, a strong password could be obtained by attackers using social engineering techniques.

Nevertheless, home users are required to make security decisions on a daily basis but lack the experience, knowledge, and training to effectively manage computer security systems and to protect themselves against threats. It is necessary to improve their understanding of computer security. Some experts argue that users should be kept out of the security decision loop (Nielsen, 2004) and that education has negligible effects on user behavior (Görling, 2006), but due to the complexity and rapid evolution of security threats, it is most likely that secure solutions in the near future will continue to include human interaction. An integrated approach of training and improving the security and usability of secure technologies is most likely to produce a holistic solution to securing end-user computer systems. Several other works (Kumaraguru et al., 2007; Sheng et al., 2007) have demonstrated that exposure to user education has positive outcomes in building awareness, enhancing security understanding, and even changing user behavior. We argue that educational efforts supplementary to technical, legal, and regulatory approaches are more likely to produce a holistic solution to securing computer systems than any individual approach. The challenge is that home users are typically uninterested in computer security (Whitten & Tygar, 1999). They remain vulnerable despite an abundance of security information and advice provided by experts. This problem persists because of several challenges unique to Usable Security.

Users Are Typically Uninterested in Security

Users are uninterested in security because it is a secondary task (Whitten & Tygar, 1999) in their everyday computer interactions. For example, authentication is necessary to prevent unauthorized access to user accounts, but people's primary task is to use their accounts, not to manage security. Understandably, when security tasks become difficult, time-consuming, or burdensome, users try to avoid security and develop coping strategies that allow them to bypass security mechanisms.

Security Systems Are Complex And Abstract

End-users have difficulty interacting with computer security systems in a meaningful way because they are complex and abstract. An early study (Dourish, Grinter, De La Flor, & Joseph, 2004) on how users experience and handle security issues in corporate settings found that security systems often match poorly with users' needs. Another study by Grinter, Edwards, Newman, and Ducheneaut (2005) found that users require considerable effort to set up, maintain, and coordinate home networks. Gross and Rosson (2007) argued that computer security systems must be designed to help bridge the gaps of users' mental models and should mask system complexities where possible. However, usability studies of modern security software such as password managers (Chiasson, van Oorschot, & Biddle, 2006) found that these software programs have very poor usability and that many users have difficulties using them effectively.

Users Have Poor Mental Models of Security

Because security systems are complex and security threats are constantly evolving, users have a poor understanding of how security works and what to do in defense of the threats. They rely on a variety of "mental models" to make security decisions (Wash, 2010). A "mental model" is a simplified internal thought process about how something works in the real world

(Craik & James, 1967). Mental models are applied to reasoning, learning new concepts, and problem solving. The term was first coined in the 1940s by Craik and James (1967) to provide a basis for understanding the process of human thought. Young (1983) later suggested that users' reasoning about using technological devices is made based on mental models. Furthermore, Johnson-Laird, Girotto, and Legrenzi (1998) suggested that minimum functionality may be required to understand a subject through mental models, because people fills in gaps of knowledge based on their mental models.

In Usable Security research, mental models of home users are often referred to as "folk models" (Wash, 2010). They are users' decision models based on how they think about security. In a study with home computer users, Wash (2010) found that people's security decisions about the effects of their actions correlate to their conceptualizations of risks. For example, users who believe hackers are teenagers who cause mischief are more likely to protect their computers by installing software to keep them out. Others who thought hackers target only the wealthy believe they do not need to secure their computers because they are not rich or important. Wash demonstrated that "folk models" do not necessarily have be "correct" or "complete" to induce positive behaviors that lead to increased security.

2.2. Security Topics Addressed

The security areas addressed in our work are password-guessing attacks, antivirus protection, and mobile online privacy. We give a brief background of these areas and the challenges users face to provide context for our design in later sections.

Password-Guessing Attacks

Long, complex, and therefore more secure passwords tend to be difficult to remember and are frequently forgotten (Florêncio & Herley, 2010; Warkentin, Davis, & Bekkering, 2004; Weirich & Sasse, 2001). Some users cope by making short, easy-to-remember passwords such as common dictionary words, but conversely, the passwords are easier to crack. To cope with a large number of online accounts, they may also reuse or create variations of the same password (Gaw & Felten, 2006). These behaviors put users at risk of online password guessing attacks, where attackers try to break into user accounts through brute force, dictionary, or targeted attacks. An *exhaustive brute-force attack* guesses every possible password in a theoretical password space.[1] Strong passwords are less likely to be cracked by brute force due to the size of the search space. *Dictionary attacks* use a precompiled library of common words to guess passwords or use a list of high-probability candidate passwords that are popular among users. *Targeted attacks* exploit specific users' personal information shared online or offline and obtained through social engineering. Mainstream password advice typically stresses the need to create long passwords with alphanumeric and special characters but offers little insight on why this strategy is effective.

Antivirus Protection

Antivirus software prevents, detects, and removes malware from computer systems. Detection methods are based on signatures or heuristics. During the scanning process, signature-based antivirus software compares contents of the scanned file with the software's database of known virus fingerprints or virus signatures (Sanok, 2005). This detection method is most effective against known malware. The heuristic-based detection method uncovers malware based on previously seen virus behaviors (Sanok, 2005). It is effective against variants of known viruses and may also detect some zero-day viruses.[2] In either case, it is essential to keep antivirus software up to date with the latest malware information. Many antivirus providers also require users to renew their software subscription at the end of each subscription period. Even though most software checks for updates automatically, users may choose to ignore or bypass update prompts and subscription renewals. Many users do not recognize that when antivirus software becomes outdated, it is less effective at detecting malware.

Mobile Online Privacy

Global positioning systems (GPS) on smartphones are capable of tracking and transmitting users' locations. This information could be collected by third parties, exploited for behavioral advertising, or maliciously used for identity theft or stalking (Friedland, Maier, Sommer, & Weaver, 2011; Goga et al., 2013). Even though most apps ask for user permission to enable location services during installation, many users are unaware that this setting can be changed. Unknowingly, users reveal more personal information than they intend (Friedland & Sommer, 2010), putting themselves at risk of online tracking. For example, when a user takes a photo on their smartphone to share on social media, they may be unaware that location data are automatically attached as metadata to the image file (unless this function is explicitly disabled), a process called geo-tagging (Friedland & Sommer, 2010). Metadata could reveal personal information such as the exact location, date, and time of when the photograph was taken.

3. INSTRUCTIONAL DESIGN PRINCIPLES AND PERSUASION IN SECURITY EDUCATION

Fogg (2003) described the education domain as an area where persuasive technology could grow. We argue that education has unique contextual differences than traditional application areas of persuasive technology. In education, persuasion could function on two levels: (a) activation of interest and

[1] The set of all possible password combinations for a given system configuration.

[2] A previously unknown computer virus or other malware for which specific antivirus software signatures are not yet available.

engagement, and (b) behavior change. In education, behavior or attitude change can occur if and only if the learning material is accessed and absorbed.

Activation of engagement is necessary if the learner has poor attention or low motivation to learn. Motivation to learn means to seek with interest to acquire the knowledge and skill that an educational activity is designed to develop (Brophy, 1983).

Learners must first be persuaded to direct their attention toward the educational material and maintain the learning state in order to acquire new knowledge. Only then can behavior change be possible. Persuasive technology used for this purpose, said Fogg (2003), "can motivate people to initiate a learning process to stay on task, and then to review material as needed" (p. 246). Therefore, we argue that in the domain of education, it is useful to distinguished these two types of persuasion. Our work focuses on the use of persuasion to activate interest and engagement that results in positive learning outcomes, although our users studies do also suggest positive changes in behavior.

Although the security industry provides users with ample security advice to help them stay informed about the latest threats and the best security practices, many users remain vulnerable because of noncompliance with security policies and the recommended security advice. Many of the security communication focus on the action level, such as giving direct advice like "do not reuse passwords" or "keep your antivirus software up to date." Although this is good advice, it does not help users build an understanding of why this is necessary. Prior work in Usable Security suggests that good advice could be rationally rejected if users have poor conceptualizations of security (Herley, 2009). Improving security understanding makes it possible for users to make informed decisions and motivates positive behaviors.

Education researchers developed instructional design (ID) principles by examining how people learn and acquire new skills. The principles help to guide the design of effective and appealing instructional materials (Gagne Wager, Golas, Keller, & Russell, 2005). Many works in Usable Security focus on improving users' security understanding through education, but they lack a unified theoretical background to enable meaningful synthesis and comparison. They include computer games, e-mail systems, card games, mobile applications, visualizations, and comics. We provide clarity and structure to this body of literature by summarizing and synthesizing the design approaches under a well-defined set of instructional design principles.

With each system, we carefully reviewed their characteristics to identify which ID principles were exemplified. A work is shown to employ the principle if it explicitly incorporates its use into the lesson (e.g., images are used as a learning tool instead of decoration). The results of our analysis is summarized in Table 1, and individual principles are discussed in more detail in the following subsections.

3.1. Multimedia

Multimedia refers to the use of multiple media types in the educational material, such as images, text, or sound. The combination of different modes can be helpful in learning. For example, Paivio's (1991) dual coding theory suggests graphics, text, and audio are coded into memory differently. People process text and audio in their phonetic working memory, whereas images are encoded in visual working memory. The theory implies that the combination of related text and images helps to enhance comprehension and increases long-term memory. Graphics could involve a range of visual media such as illustrations, photographs, animation, or video. Research suggests that a multimedia-supported learning environment helps students engage in learning and results in a superior learning outcome than text alone approaches (Mayer & Anderson, 1992).

Recently, there is a growing trend toward "Edutainment," which is educational media designed to both entertain and educate, with the goal to increase the audience's knowledge about an educational issue, create favorable attitudes, and change overt behavior (Singhal & Rogers, 2012). Wade (2001) identified that one important source of motivation for learning is interest in the activity, such as to embedded training in a fun recreational activity like gameplay. However, researchers caution that using an excess of multimedia in educational material could actually decrease learning (Dixon, 1990). Similarity, Harp and Mayer (1998) found that the overuse of multimedia details could distract learners from key instructional points, disrupt their ability to mentally organize information, and activate irrelevant prior knowledge that increases the cognitive load.

Communicating through a combination of visual and textual means is a frequently applied approach in Usable Security. Several studies (Mekhail, Zhang-Kennedy, & Chiasson, 2014; Raja et al., 2011; Zhang-Kennedy & Chiasson, 2014; Zhang-Kennedy, Chiasson, & Biddle, 2013, 2014) demonstrated that users learn more effectively from graphics and text than text alone. For example, studies by Zhang-Kennedy, Chiasson, et al. (2013, 2014), Zhang-Kennedy and Chiasson (2014), and Mekhail et al. (2014) showed that infographics are more effective at improving the comprehensibility and retention of security advice compared to text-only information in various security areas. Another work, "Privacy Leaks" (Balebako, Jung, Lu, Cranor, & Nguyen, 2013), also found that it is useful to provide users with visualized information within the user interface of a mobile privacy application. The app visualized data as it left the device and summarized usage over time to improve users' understanding of privacy data leaks. It also provided users with just-in-time notifications with sound effects the moment data are shared to improve users' awareness of their privacy disclosures. Work that uses the Edutainment approach includes computer game, card game, and comic approaches (the see Media Type section in Table 1).

TABLE 1
Summary of Usable Security Work That Shows the Application of ID Principles.

ID Principles	*Secure Comics*	Anti-Phishing Phil	PhishGuru	APWG Phishing Program	Auction Hero	Ctrl-Alt-Hack	Nutrition Label for Privacy	Privacy Leaks	Brick Wall/ Door/ Bandit	Security Infographics	Security Cartoons
Multimedia	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
Personalization	✓	✓	✓	✓	✓	✓					✓
Segmenting	✓	✓			✓	✓					✓
Signaling	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Contiguity	✓	✓	✓	✓					✓	✓	✓
Conceptual & procedural	✓	✓	✓	✓	✓					✓	✓
Reflection	✓	✓	✓	✓	✓	✓		✓	✓		
Immediate feedback	✓	✓	✓	✓	✓			✓	✓		
Media type											
Computer game		×			×						
Comic	×		×								×
Visualization	×			×			×	×	×	×	
E-mail system			×								
Mobile app								×			
Card game						×					

Note. ID = instructional design; ✓ = work that uses the ID principle, × = work designed based on the media type.

3.2. Personalization

We note that the instructional design principle of "personalization" addresses the concept of "attributing social characteristics to the user interface" rather than "customizing on a per user basis" as is commonly used in persuasive technology.

Work on Media Equation by Reeves and Nass (1996) states that people respond to computers in a similar way to how they respond to other people through social conventions. Based on this theory, Clark and Mayer (2011) established that learners engage better with educational content when the message is delivered in conversational style rather than formal language.

It is also evident that the use of an "agent," a pedagogical character who offers instructional advice, can improve learning (Mayer, 2002). People pay more attention to someone who is speaking directly to them by evoking a conversation (Clark & Mayer, 2011). Agents can be human or nonhuman characters, realistically depicted or cartoon style, and represented visually or verbally. They could effectively narrate the lesson and put it in context of a story, demonstrate the concepts, and direct visual attention to key features on screen (Atkinson, 2002; Mayer, Dow, & Mayer, 2003; Moreno, Reislein, Ozogul, 2010).

Several works use agents with a conversational tone (see Table 1). In educational computer security games, agents provide users with immediate positive feedback and encourage users to continue playing. For example, in the game Anti-phishing Phil (Sheng et al., 2007), users play as the fish character Phil, who tries to identify legitimate and fraudulent links. The characters speaks to users in a friendly, first-person style throughout interventions in the game, such as using the words "I" and "you."

Social cues from computers could function as persuasive social actors (Fogg, 2003). Several security works leverage social influence to motivate and persuade users to behave securely. Social presence can be conveyed through physical presence. Anthropomorphized characters increase humanistic and emotional appeal. For example, as a pun for fishing, Anti-phishing Phil (Sheng et al., 2007) is centered around fish characters. In Security Cartoon (Srikwan & Jakobsson, 2008), anthropomorphism is used to personify various computer devices and malware. Social presence could also be psychological. For example, it is suggested that characters designed with a sense of humor are perceived to be well rounded, interesting, and more believable (Nijholt, 2002). Serious games use humor to ease the social, emotional, and cognitive challenges of serious topics and to enrich the overall user experience (Dormann & Biddle, 2009). The use of humor in education increases persuasion, comprehension, and retention (Garner, 2006).

3.3. Segmenting

Research suggests that giving learners opportunities to pause and process the information before continuing to the next step helps them learn more deeply. This could be achieved by segmenting a multimedia message into learner-paced chunks rather than presenting the information as a continuous unit (Mayer, 2002). For example, Mayer and Chandler (2001) found that students' performance increased if a narrated animation is broken into segments where they could press a Continue button to progress to the next section.

Auction Hero (Chiasson, Manas, Biddle, 2013) is a game that embeds security training in the game activity of buying and selling robot parts online while evading various security attacks. Users earn money and reputation points while staying vigilant against security risks to become an Auction Hero. Learning is segmented into five missions where learners encounter progressively more challenging game tasks and complex security concepts.

3.4. Signaling

The signaling principle states that deeper learning can be achieved when cues are added to highlight the organization of the essential content and to call to attention the important material in the lesson (Mayer, 2002). Signaling could be applied to text (e.g., bold, highlight, underline) and visual content (e.g., colors, arrows, spotlight). For example, Mautone and Mayer (2001) found that students' performance increased if the lesson included headings, outline, and voice emphasis on key words during a narrated animation of how an airplane achieves lift. Mayer (2005) suggested that the signaling principle may be applied most strongly when it is used sparingly rather than excessively.

Signaling is used to emphasize important information. For example, Kelley, Bresee, Cranor, and Reeder (2009) explored how good information design can improve comprehensibility of online privacy policies in "A Nutrition Label for Privacy." The authors designed a privacy label using design elements and principles from nutrition, warnings, energy labeling, and banking privacy notifications to make information easier to find and understand. Colors are used to highlight important information on the label. Based on this design, users discovered information more quickly and accurately on the proposed privacy label compared to existing natural language privacy policies.

3.5. Contiguity

Mayer and Anderson (1992) proposed that when text is integrated on the screen close to related visuals, learning is more effective than when they are placed in isolation. In an experiment comparing learning about science topics, they found that isolation of text and visuals require the learner to expend extra cognitive load to integrate them. When they are placed contiguously, learning is more effective because the integration is done for the learner. Another study suggests that visuals depicting the content of accompanying text may facilitate the construction of a mental model (Gyselinck & Tardieu, 1999). The researchers compared the effects of text-only, text accompanied by visuals that represented only elements described in the text, and text accompanied by visuals that represented the

relationships of elements described in the text. In all cases, visuals returned higher accuracy and response times in recognition and problem solving than text only. Second, visuals that show relationships between elements being described in the text are the most beneficial.

In the design of firewall warnings, Raja et al. (2011) found that a personal firewall illustration based on the concept of physical security placed on the text warning to facilitate better comprehension and risk communication increased the likelihood of safe behavior compared to warning messages from existing firewall software. Text and images in comics are inherently contiguous. "Security Cartoon" (Srikwan & Jakobsson, 2008) delivers security messages through entertaining comic strips.

3.6. Conceptual and Procedural Knowledge

Instruction that focuses on building a mental representation of an idea builds conceptual knowledge, whereas instruction that focus on the correct steps to solve a problem or complete a task builds procedural knowledge (Clark, 2011). Research suggests that there is a causal relationship between conceptual and procedural knowledge. For example, a study (Rittle-Johnson & Alibali, 1999) that examines the relations between children's conceptual understanding and procedures for solving mathematical equivalence problems found that conceptual knowledge led to increased understanding and transfer of a correct procedure, whereas procedural knowledge led to increased conceptual understanding. The two types of instructions are therefore mutually supportive in learning.

For example, Anti-Phishing Working Group and CMU-Cylab's phishing education landing page program (Anti-Phishing Working Group, 2013) uses both conceptual and procedural instruction to teach users about phishing. The program repurposes inactive phishing URLs to redirect users to the education page when they have just clicked on a phishing link as part of their regular online activities. On the landing page, it teaches users about the concept of phishing, as well as providing step-by-step advice on how to protect yourself.

3.7. Reflection

Reflection is a form of mental processing used to fulfill a purpose or to achieve some anticipated outcome to further the processing of knowledge and understanding (Moon, 2013). Research shows that learning increases if the learner is given opportunities to reflect on what they have learned (Pellegrino, Bransford, Donovan, 1999).

Designing instructional material for reflection often involves self-monitoring tools. For example, PhishGuru (Kumaraguru et al., 2007) is an education system that directs users to instructional content when they have just fallen for a phishing communication. It uses an embedded training system that delivers simulated attacks to teach users about phishing during regular use of e-mail. Training takes place when users "fall" for a simulated phishing email. Users are directed to an intervention message in comic strip format that explains the risks and provides tips on how to stay safe. Educating learners immediately after they have made a mistake causes a moment of reflection. Although this approach is effective at getting users to pay attention to security information, it would need to be carefully regulated by organizations so that it does not infringe on users' privacy. Another example that leverages reflection to create security awareness is Ctrl-Alt-Hack (Denning, Kohno, & Shostack, 2013), a security-themed tabletop game. Users play the card game with a group of friends in a physical environment. Role-playing as fellow hackers causes players to reflect on a variety of security breach scenarios in the game.

3.8. Immediate Feedback

Immediate feedback is a comment made right after the fact, which includes praise, advice, and evaluation that could help the learner assess how they are doing. A number of researchers (e.g., Schmidt & Bjork, 1992; J. R. Anderson, Corbett, Koedinger, Pelletier, 1995)) showed that immediate feedback provides efficient guidance in learning. Positive feedback such as giving praise and reward is a form of conditioning that reinforces a target behavior (Fogg, 2003). However, Hattie and Timperley (2007) stressed the importance of avoiding ambiguous feedback like "Great job" or "Not quite there yet," because they do not provide any insight into what was done right or wrong and how it could be corrected. Feedback should supply learners with concrete information to help them improve.

Immediate feedback is used in several works, including Anti-phishing Phil (Sheng et al., 2007). Phil's father provides immediate feedback of whether a link Phil identified is legitimate or fraudulent. Another work that best exemplifies the use of immediate feedback is the Privacy Leaks mobile app (Balebako et al., 2013). The app enables users to self-monitor the frequency and destination of users' shared data. Feedback is given as just-in-time notifications to alert users at the moment data were being sent. Such tools help to correct misconceptions between what users think is happening on their devices and the actual events.

4. PRELIMINARY INFOGRAPHIC STUDIES ON SECURITY METAPHORS

Our earlier work (Mekhail et al., 2014; Zhang-Kennedy et al., 2013; Zhang-Kennedy, Chiasson, et al., 2014) suggests that simplification of security information through metaphors and graphical explanations may facilitate users' understanding of new security concepts. The security topics addressed were password-guessing attacks (Zhang-Kennedy et al., 2013), antivirus protection (Zhang-Kennedy, Chiasson, et al., 2014), and mobile online privacy (Mekhail et al., 2014). We selected several conventional metaphors from the computer security literature and mainstream public communication media and incorporated each metaphor into an infographic. For example, in

the antivirus study (Zhang-Kennedy, Chiasson, et al., 2014), we selected a "surveillance" metaphor inspired by physical security (Camp, 2009; Raja et al., 2011) and a "medical" metaphor inspired by biological models used to predict computer virus outbreaks (Kephart et al., 1995; Pastor-Satorras & Vespignani, 2001). We tested the effectiveness of the infographics against text-only advice with no metaphors and graphics. We provide a summary of the main results to support our design decisions and the selected metaphors in *Secure Comics*.

4.1. General Methodology

We conducted three separate, ethics-approved users studies using the same methodology. A between-subject design was used to evaluate two to three infographic designs against one text-only condition for each security topic during two sessions set one week part. We recruited 55 participants for the password infographic study, 40 participants for the antivirus infographic study, and 36 participants for the privacy infographic study. In the pretest session, participants completed a pretest questionnaire, viewed the prototype, then completed a prototype evaluation questionnaire. One week later, participants completed a posttest questionnaire. For the password and antivirus infographic studies, we used nonparametric Kruskal-Wallis and Mann–Whitney U significance tests to compare participants' evaluations of the different prototypes. McNemar significance tests were used to assess whether knowledge about the security topic significantly changed in the pretest and posttest.[3] Results of the privacy infographic study include descriptive statistics and thematic analysis of questionnaire data.

4.2. Summary of the Results

Password—Lock

The metaphors used in each of the three password infographics were *target, lock, and lifespan.*[4] A text condition is used as a baseline. From the pretest and posttest questionnaires, we found that participants showed statistically significant increase in knowledge about brute force and dictionary attacks in all three infographics but no significant increase for text (Zhang-Kennedy et al., 2013). The prototype evaluation questionnaire showed that the infographics were perceived to be more effective ($p < .001$) than the text condition (Zhang-Kennedy et al., 2013). Based on participants' feedback, the lock metaphor resonated most positively with participants due to the familiarity with the concept of physical security.

Antivirus—Medical

The metaphors used in each of the two antivirus infographic prototypes were *surveillance & Medical,*[5] plus a text condition. Results from the prototype evaluation questionnaire showed that both surveillance ($p = .001$) and medical ($p < .001$) were perceived to be more effective than text (Zhang-Kennedy, Chiasson, et al., 2014). However, based on the results from the pretest and posttest questionnaires, we found a significant increase in knowledge for the medical condition ($p = .031$) but not for surveillance or text (Zhang-Kennedy, Chiasson, et al., 2014), suggesting that a medical metaphor is the most effective for portraying the concept of malware protection. Participants' feedback suggests that the concept of a computer virus is well understood because it is rooted from the biological term. This supports prior findings that users tend to rely on medical terminology to describe malware (Wash, 2010) and use expressions such as having their computer "infected" with a virus.

Privacy—Trail

The metaphors used in the two privacy infographic prototypes were puzzle and trail,[6] plus a third text condition. The pretest suggests that our participants initially had little knowledge of the concepts relating to online privacy. In the posttest, we saw a larger increase in knowledge about online tracking and geo-tagging in puzzle and trail than text. Although participants from both the infographic conditions and the text-only condition self-reported behavior changes in the posttest, such as disabling geo-location tracking on their smartphones, half of the participants who viewed the text prototype said they would not have bothered learning the information on their own. Participants' prototype evaluations also suggest that they perceived the infographics to be more useful than the text-only condition. They responded most positively to the "trail" metaphor because it alludes to tracking, where attackers could obtain the digital trail left online by users through geo-tagging and shared location information.

5. DESIGN OF *SECURE COMICS*

5.1. Why Comics?

Comics are a form of "sequential art" (Eisner, 1985) that use a series of images to deploy graphic storytelling and to convey information. Over the past 100 years, comics have evolved into a variety of distinct genres, styles, formats, and cultural-political connotations, from epic American superhero classics and Japanese Manga, to short comic strips and political cartoons. Comic styles have matured from cartoon style to literary graphic novels that are now recognized as a serious genre of literature (McCloud, 2000). Stories told in comics have expanded their audience beyond young people to cater toward adults who are interested to learn about an array of important issues.

Comics have unique advantages over other media types. They are quicker to produce and have lower production costs than other popular media like computer games, film, and animation. They are a flexible communication medium that enables

[3] In all cases, $p < .05$ is considered significant.

[4] See Zhang-Kennedy et al. (2013) for detailed descriptions of the infographic designs.

[5] See Zhang-Kennedy, Chiasson, et al. (2014) for detailed descriptions of the infographic designs.

[6] See Mekhail et al. (2014) for detailed descriptions of the infographic designs.

users to consume the content at their own pace; the pages can be easily browsed through and read at leisure. The media provide a wide range of communication tools. Designers have enormous breadth of control to create customized content through many visual symbols and word–image pairing techniques (McCloud, 2000). New digital interactive comics further extend the communication power of the media through gamelike interactions.

Comic is a powerful evolutionary communication medium that has found a niche in a variety of domains. In education, the comic medium has attracted the attention of educators because of its potential to foster students' interest in science and help with retention of knowledge (Negrete & Lartigue, 2004). In healthcare research, there is a growing trend of using comics to help enhance doctor-to-patient and public health communications (Green & Myers, 2010). For example, "pathographies," a subgenre of illness graphic stories, help patients to learn about their illness and provide doctors a way to gain insights into the patients' personal experiences. Compelling pathographies like *Cancer Vixen* (Marchetto, 2014) and *Mom's Cancer* (Fies, 2011) capture real patients' physical and emotional experiences of living with cancer in a manner that people can understand. In computer security education, the short comic strip format is explored in *Security Cartoons* (Srikwan & Jakobsson, 2008) and adapted as a part of a intervention message in *Phish Guru* (Kumaraguru et al., 2007). Mainstream comic strips that sometimes include security advice are Dilbert (S. Adams, 2012) and *XKCD* (Munroe, 2012).

As information is moving online, there is a shift of the comic medium from print to digital form. Unlike their print cousins, webcomics are born, distributed, and read entirely online. We argue that webcomics open up the potential for a greater degree of dialogue through interactivity that is not possible in print format. In many ways, webcomics are read much like print comics, through words and images, but enable the ability for added layers of information over the traditional narrative. For example, simple mouseover images or text could

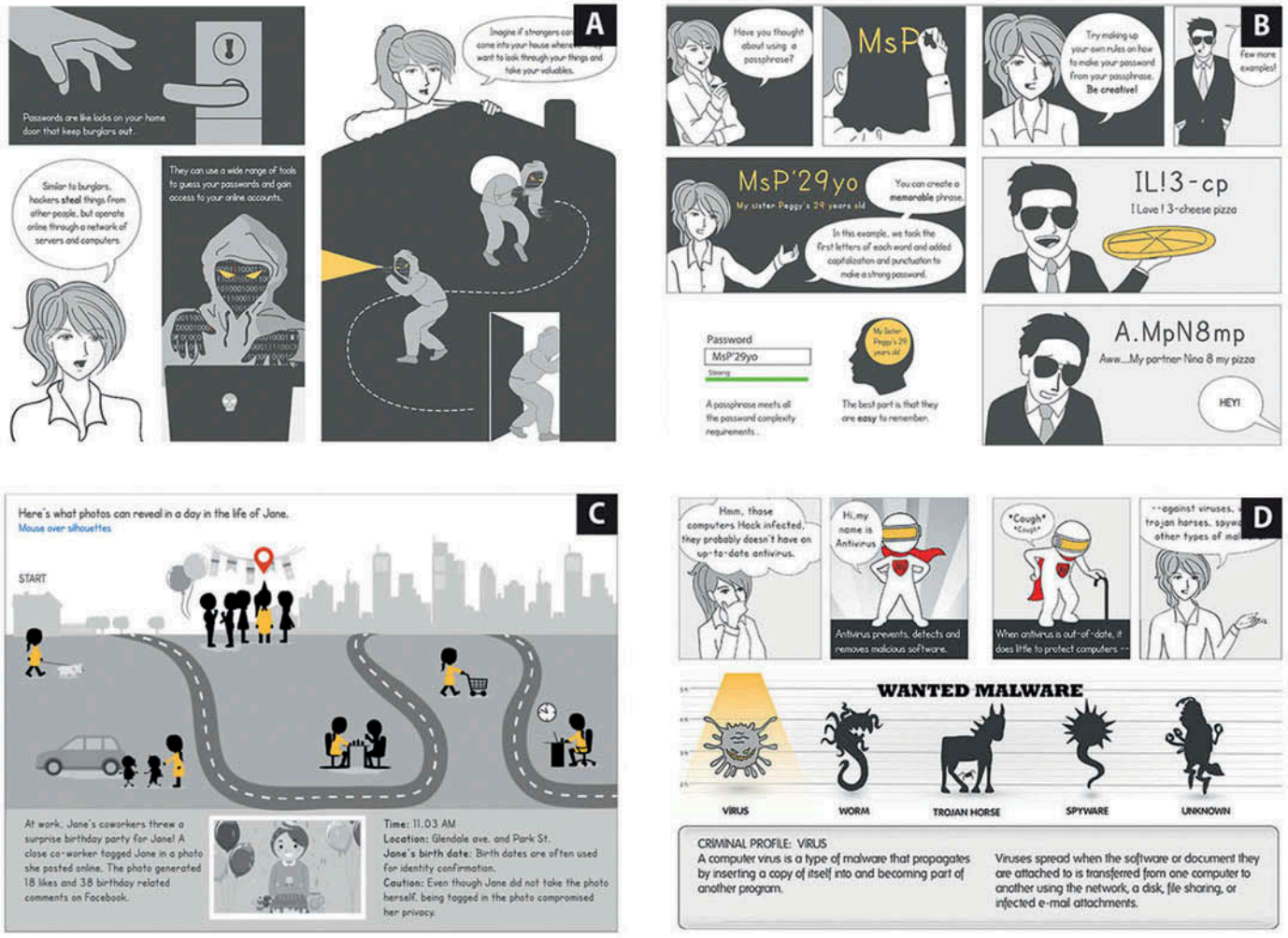

FIG. 1. Individual panels from *Secure Comics*. (A) and (B) page 4 and page 11 of the password comic. (C) page 5 of the privacy comic. (D) page 3 of the antivirus comic (Zhang-Kennedy, Dorey, Mekhail, & Chiasson, 2014).

supply the reader with additional commentaries, portray cause-and-effect relationships, or include a punch line to make a point. Examples of user interaction can be found in Figures 1C and 1D.

Although this type of interface offers modest interactivity, it opens new avenues for experimenting with the narrative and how the reader makes sense of the material. Not only does this feature in webcomics offers readers with additional content, it also could condition them for the anticipation of discovery, as mouseover images or text is always a possibility.

We designed a webcomic series called *Secure Comics* to educate the public about three important computer security topics. The comic inherited some of the most successful elements from our preliminary infographic studies, such as focusing on graphic design and metaphors to visually break down complex security concepts to increase security understanding. For example, we illustrated the lock concept visually through burglary in the password comic, shown in Figure 1A. Our work also explores modern media trends like using online webcomics and games to further engage users and enhance learning. For each security area, *Secure Comics* teach users about the threats, how they work, and what users can do to protect themselves. The maximum length of each comic is 14 pages for quick and easy reading. Each comic begins with a brief introduction to the characters and concludes with minigames that reinforce the main take-away messages. We drew the comics and produced using Adobe Creative Suite graphics software.

5.2. Instructional Design Principles Applied in *Secure Comics*

In this section, we explain the principles of instruction that describe our design approach for *Secure Comics*. We assembled the ID principles into the appropriate category that best addresses the main challenges in computer security education identified in Section 2. We give a summary of the principles and how they are applied in our work in Table 2.

Principles of *multimedia* and *personalization* address the problem that many users are not interested in learning about computer security (Activation and Engagement section). Therefore, methods of capturing the users' interest and helping them to stay on task are necessary. Principles of *segmenting* and *signaling* help to make security lessons easier for users to absorb. They address the issue that security is complex and abstract (Demonstration section). Last, principles of *contiguity, conceptual and procedural knowledge, refelction,* and *immediate feedback* help users to build good mental models of security (Understanding section) so they can make security-conscious decisions.

Activation and Engagement

Multimedia. We chose the comic media because it is an efficient tool that uses juxtaposition of text and images to communicate. Comics convey graphic stories, are fun to read, and have large readerships of all ages. Our comic design leverages the media's power to express ideas through text and images but also explores modern media techniques like graphic design and interactivity to engage users. For example, we used a combination of visual and typographic treatments, as well as text explanations, to teach users how to create a passphrase in the password comic (see Figure 1B). Interactive tools are implemented on certain pages of the comic, such as the two examples shown in Figures 1C and 1D. We avoided using gratuitous multimedia so it does not distract users from learning.

Personalization. The comic is built around the characters Jack and Nina, who are partners in solving computer security crimes. They protect users against Hack, the supervillain who exploits people's poor understanding of security and executes various attacks and schemes against users. We created both male and female characters to appeal to a wide range of learners. Jack and Nina guide users through the lesson content and motivate them along the way. They use a positive conversational language when speaking to users about various security concepts. We designed the "good guys" with a sense of humor to make them seem well rounded and interesting. Users encounter various humoros moments throughout the comic, such as when Jack and Nina make jokes or use funny gestures and expressions (e.g., Figure 1B).

Characters such as Hack and Antivirus Man are symbolically designed to appeal to readers' emotions. Hack, who is portrayed in Figure 1A, is the supervillain that embodies all computer security crimes. His physical appearance is dark, mysterious, and inhuman. Antivirus man (shown in Figure 1D) is personified as a superhero. He is portrayed as bright and valiant. Elements of malware, password strength, and Exchangeable Image File (EXIF) editors are also personified. This gives these abstract concepts a physical presence and emotional appeal. In the antivirus comic, the different types of malware resemble unpleasant creatures such as bugs, serpents, mutants, and evil robots (Figure 1D). In the password comic, strong and weak passwords are portrayed as lock characters. One appears to be strong and confident; the other appears scrawny and scared. In the privacy comic, we portrayed the EXIF editor as a friendly robot mechanic who fixes picture files by removing metadata.

Demonstration

Segmenting. The comic series cover one security topic per issue as Agents Jack and Nina tackle a new security crime committed by Hack. Each comic is segmented into sections and pages to enable users to progress at their own pace. Users press a forward button or a section button to move ahead, or go back to a previously read page.

Signaling. We designed the comic to be monochromatic so that we can use bright colors to highlight visual elements of importance or objects of interest. For example, a yellow spotlight shines on each type of malware as users mouseover them to see their descriptions (see Figure 1D). Various text

TABLE 2
Summary of Instructional Design (ID) Principles Applied in *Secure Comics*

Problem	ID Principle	Description	Application in Secure Comics
Security is uninteresting.	Multimedia	Adding graphics to words improves learning.	Comics rely on the juxtaposition of text and images. Only topic-relevant multimedia content is included.
	Personalization	The use of conversational language and pedagogical agents increase learning.	A male and a female main character are included to appeal to audiences of both genders. Agents Jack and Nina guide users through the lesson content and motivate users along the way. They use a positive and humorous conversational language to speak to users.
Security is complex.	Segmenting	Deeper learning occurs when content is broken into small chunks.	The comics are segmented into sections and pages to enable users to progress at their own pace. Users press a forward button or a section button to move ahead or go back to a previously read page.
	Signalling	Visual cues draw attention to critical elements of the lesson.	Colors are used sparingly to highlight visual elements of importance. Various text treatments (e.g., bold, color-highlighting) are applied to textual information to direct the learners' attention.
Users have poor mental models.	Contiguity	Placing text near graphics improves learning.	Words and images in comics are inherently contiguous.
	Conceptual Procedural	Conceptual and procedural instructions are mutually supportive in building new knowledge.	The comics help users develop conceptual knowledge by building mental models through metaphors and telling analogies, then provide procedural examples to help reinforce the concepts. For example, after explaining the concept of online tracking in the privacy comic, the interactive page "A day in the life of Jane" demonstrates how and where online tracking could take place.
	Reflection	Learning increases if the learner is given opportunities to reflect on what they have learned.	Interactive components in the comic cues reflection of the lesson content by concealing answers under graphics that are activated on mouseover.
	Immediate Feedback	Immediate feedback provides efficient learning guidance.	The mini-games at the end of each comic incorporate the principle of immediate feedback by explaining why a response is correct or incorrect each time the user answers a question.

treatments (e.g., bold, color-highlighting) are applied to textual information to direct the learners' attention.

Understanding

Contiguity. Words and images in comics are inherently contiguous. We applied graphic design principles, good typography, and simple writing to the design of each panel to strategically break down complex security topics into manageable learning steps. The graphics are designed to complement the text explanations to facilitate comprehension by illustrating connections between concepts or providing visual examples. For instance, when explaining the rules for creating a strong and memorable password, both Jack and Nina demonstrate strong passwords (see Figure 1B).

Conceptual and procedural knowledge. The comics help users develop conceptual knowledge by building mental models through metaphors and telling analogies, then provide procedural examples to help reinforce the concepts. For example, after comparing the concept of online tracking to physical tracking in the privacy comic, we included an interactive page: "A day in the life of Jane" (shown in Figure 1C) to illustrate the step-by-step process of how online tracking could take place. As users interact with Jane's various daily activities, they procedurally witness how this ordinary person's seemingly harmless interactions could reveal sensitive information. Jane's story aims to reinforce their conceptual knowledge about online tracking.

Reflection. Interactive components in the comic cue the reflection of the lesson content by concealing answers under graphics that are activated on mouseover. For example, in the Types of Attacks section of the password comic, users can rollover silhouettes of people to see examples of strong and weak passwords. People with weak passwords are highlighted with a target icon, indicating that they are vulnerable to password-guessing attacks. At the end of each comic, users have the option to play a "test your knowledge" minigame. The purpose of the minigame is to review and reflect on important concepts that were taught in the comic. These interactive tools extend the main content by showing users examples, portraying cause-and-effect relationships, and testing the acquired knowledge.

Immediate feedback. The minigames at the end of each comic incorporate the principle of immediate feedback. For example, when users correctly answer a question, an agent gives praise such as "Good work," "Thanks for your help!," or "that's right!," followed by an explanation of what they answered right. When they answer incorrectly, we provide cautionary feedback such as "Are your sure?" or "Uh-oh," followed by a constructive explanation of the correct response.

5.3. Design Process

We used a process-driven design approach adapted from the ADDIE instructional design model. ADDIE is a five-phase iterative model that stands for Analyze, Design, Develop, Implement, and Evaluate. It was first introduced as an instructional systems development program for military service training (Branson, Rayner, Cox, Furman, & King, 1975) and has evolved into a general iterative process applicable to many areas of instructional design.

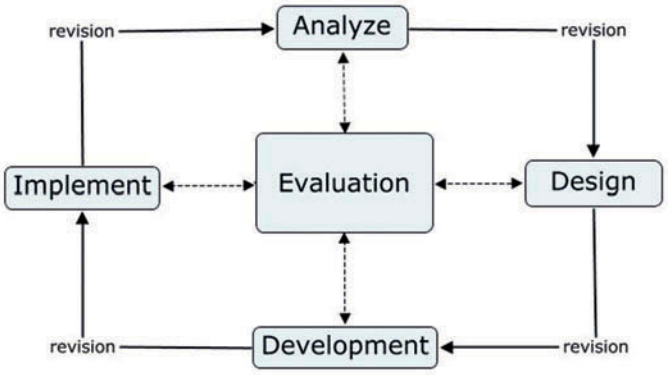

FIG. 2. The ADDIE instructional design process. Diagram adapted from Wikimedia Commons (2013).

Figure 2 illustrates the ADDIE process most commonly used today. The designer first gathers information about the target audience, project objectives, constraints, and desired learning outcomes during the *analyze* phase. Then, lesson content is planned to meet the desired behavioral outcomes in the *design* phase. These may include low-fidelity prototypes and concepts so that they can be iterated quickly at low cost. During *development,* content is assembled in storyboards, and sample graphics are created to get feedback and iterate the designs. The content is then *implemented* and error checked before it is evaluated to monitor periodic learning outcomes. ADDIE is a dynamic iterative process. Therefore, formal (e.g., pilot studies) and informal (e.g., constructive feedback) *evaluations* may be involved at any stage of the process.

In the *analyze* phase, we surveyed the problem space, including our previous work on metaphors for risk communication using infographic posters (Zhang-Kennedy & Chiasson, 2014; Zhang-Kennedy et al., 2013; Zhang-Kennedy, Chiasson, et al., 2014). To understand users' existing mental models and misconceptions, we reviewed relevant literature in Usable Security, as well as online resources available to end-users. In the *design* process, we conceptualized the characters through concept art drawings and drafted a written script of the narrative. From there, we created complete storyboards of the comics in the *development* phase. The storyboards were shown to members of our lab for constructive feedback and iterated several times before they were implemented. During the *implementation* phase, we drew and colored the artwork in Adobe Illustrator using a Wacom Intuos graphics tablet and imported them into Adobe Flash to implement the interactive components. Finally, we tested and evaluated the comics in user studies during the final *evaluation* phase.

5.4. Eye-Tracking Experiment of the Password Comic

To validate our design decisions, we ran an ethics approved eye-tracking experiment after the initial design of the password comic to evaluate users' interactions with our prototype. We observed users' attention, average reading times, and ways users processed the comic.

Experiment Methodology

The study was approved by the Research Ethics Board at Carleton University. Thirteen students and staff from our university were recruited through flyers and mailing lists. Each study session lasted no more than 1 hr. Participants were given a $20 honorarium. The eye-tracking data are stored on a password-protected computer in our research lab. Only researchers associated with study have access to the data. Participants signed a informed consent form at the start of the study and were given a debriefing form and signed a receipt of remuneration form at the end of the study.

A Tobii 1750 eye-tracking system and Tobii Studio software were used to collect real-time data. The Tobii eye-tracking system uses an infrared camera embedded at the bottom of the computer screen to track eye movements and fixations. The participant sat in front of the eye-tracking computer screen in a normal sitting position that enabled mouse navigation of the comic. Each session began with a short gaze calibration process. Next, participants read the comic on the eye-tracking computer. They were asked to proceed at their normal reading pace and interact with the on-screen elements in any way they like. Eye movements were recorded in real time and later outputted as AVI videos with time stamps.

To analyze the path and pattern of fixations, we watched the eye-tracking videos and observed sequential and recurring patterns of visual attention. We documented the reading direction and general characteristics of fixation sequences by identifying the corresponding eye positions on the comic panels. We also noted whether users skipped pages, reread panels, or backtracked to previously viewed screens. To document time spent looking at display elements, we tracked and calculated the average of participants' reading times on each page and the time spent on interactive elements.

Eye-Tracking Results

We observed several behaviours from our analysis of the eye-tracking data.

Back-and-forth eye fixations between text and images. The path of fixation usually starts with headings, text blocks, and then graphics. After a text block is read, users' eyes move to the closest surrounding graphic. Images typically get eye fixation for 1 s or less between frames. In some cases, the eye-tracking video show users' gaze switching back and forth between text and accompanying images. At times, users' gaze moved to nearby text after seeing the related images. Our participants did not exhibit any major differences in reading patterns between noncomic readers and those who read comics for leisure.

TABLE 3
Mean Time in Seconds Spent on Each Page of the Password Comic, Excluding the Mini-Game

Page No.	1	2	3	4	5[a]	6[a]	7	8	9[a]	10	11	12	13
Time (s)	37	53	58	45	104	101	91	76	89	69	87	52	34

[a] Contains interactive elements.

Prolonged eye fixations on interactive elements. Table 3 summarizes the mean viewing time for each page, where pages 5, 6, and 9 contain interactive elements. Participants spent as much as 60% longer viewing these pages compared to the static pages. They showed prolonged eye fixations on the interactive elements. For example, Figure 3 demonstrates a common reading pattern we observed for page 6 of the password comic.[7] Users can rollover boxes that contain sample passwords, shown on the lower right of Figure 3. It shows that the participant spent much longer looking at the password rollovers on the page. Most participants moused over all password examples at least once.

Back-tracking. We observed back-tracking behavior for 31% (4/13) of participants. These participants reviewed previously read content after looking at an image or an interactive example.

After the password comic study, we made some improvements to our designs. We shortened the next two comics to under 10 pages to reduce reading time, but still deliver a comprehensive lesson plan. We modified the reading flow on some panel designs to make them more intuitive, and included visual cues for the interactive elements so they can be easily discovered.

6. MAIN METHODOLOGY

We developed the remaining comics and evaluated all three in users studies. In this section, we outline the methodology used for the evaluations.

6.1. Participants, Data Collection, and Storage

Our user studies were approved by the Research Ethics Board. We recruited 52 participants from our school. Table 4 shows a summary of our participant demographics for the three studies. Participants were recruited through flyers, a faculty- and staff-subscribed e-mail newsletter, and an e-mail list of volunteers. Participants were given a $20 honorarium. The duration of each study session lasted at most 1 hr. Participants signed a informed consent form when they met with researcher, and they were given a debriefing form and signed a receipt of remuneration form at the end of the study.

[7]Image was obtained from the original screen recording and outputted as a JPEG.

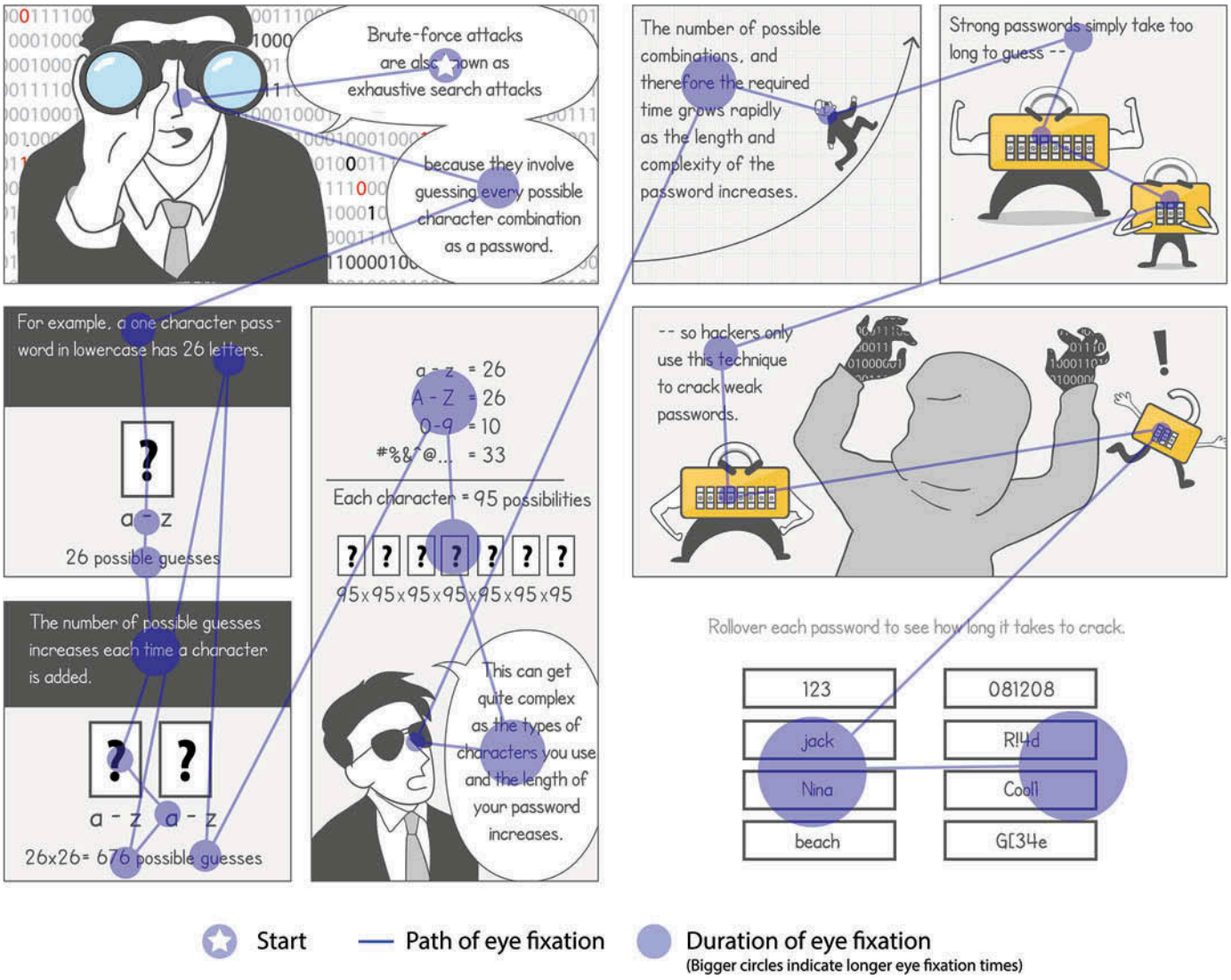

FIG. 3. Eye-tracking for one page of the password comic. Lines represent the reading path, and the size of circles represent the time spent on each fixation point (larger circles means longer fixation times).

TABLE 4
Participant Demographic and Distribution

User Studies	Sample Size	Mean Age	Gender M/F
Password comic	$n = 21$	29 years	M = 8, F = 13
Antivirus comic	$n = 16$	22 years	M = 5, F = 11
Privacy comic	$n = 15$	22 years	M = 7, F = 8

Our questionnaires are hosted on our own research servers, physically located in our research labs, using Limesurvey software. The system is password protected and only researchers associated with the study have access to the data. Audio files were stored on a password-protected computer in our research labs and kept up to 1 year. Transcribed interview data are stored in on a secure server in the United States for up to 2 years and are subject to the Patriot Act (for more information, http://www.dedoose.com/Public/Terms.aspx). The only personally identifiable information will be the signed paper consent forms and signed Receipt of Remuneration forms. These will be kept in a locked filing cabinet and not associated with the electronic data.

6.2. Study Procedure and Material

We conducted separate user studies evaluating each of the three comics using the same methodology. Each study consists of a pretest and a posttest session conducted 1-week apart. During the pretest session, participants answered a demographic questionnaire collecting basic demographic information like age, gender, and educational backgrounds. Then

TABLE 5
Summary of Study Procedure and Materials

Sessions	Material	Description
	Demographic questionnaire	The demographic questionnaire collected background information about the participants.
I	Pretest questionnaire	The questionnaire assessed users' prior knowledge about the security topic and current practice.
	Pretest interview	The semistructured interview inquired about users' prior understanding of security risks.
	Prototype viewing	Participants took as much time as they required to view the prototype.
	Prototype evaluation questionnaire	The postviewing questionnaire evaluated the prototype through Likert-scale questions.
		One-Week Interval
II	Posttest questionnaire	The posttest questionnaire assessed information retention after 1 week, repeating portions of the pretest questionnaire.
	Posttest interview	The semistructured posttest interview inquired about understanding of security risks and behavioral changes after 1 week, repeating portions of the pretest interview.

TABLE 6
Sample Interview Excerpts and Corresponding Codes Used to Identify the "Pest" Concept

The Pest Concept Interview Data Extract	Codes
"Like a bug, or a worm. Just some type of pest that's invasive that might get inside your house or something. So if I were to visualize it, it's something that got inside my computer that's eating things up."	Viruses are invasive (like pests) Viruses damage my computer
"It's annoying. A bug? I would connect it with bedbugs. Like even if you want to kill it you can't destroy it. Like it's tough."	Viruses are annoying Viruses are difficult to get rid of (like bedbugs)
"I don't know it kind of just takes on a life of its own, that's kind of how I always thought. Its like a little worm."	Viruses have a life of its own Viruses are alive (like a worm)
"I think about a worm moving around."	Viruses are alive (like a worm)
"Something like a worm I think? Something that pops out. Your screen turns red or black. I don't know something not what you expect I perceive it as a virus."	Viruses are alive (like a worm) Viruses damage my computer
"Little bugs that's gotten in there."	Viruses are invasive (like pests)

they completed a pretest questionnaire assessing prior experience and knowledge about the security area. We conducted semistructured pretest interviews to understand users' initial security practices and perceptions. Afterward, we asked participants to take as much time as they required to view the prototype on a laptop computer. Participants completed a prototype evaluation questionnaire where they rated various statements about the prototype on a Likert scale. We reversed the direction of some questions to avoid bias.

Participants returned to our lab to complete the posttest session of the study 1 week later. They first filled out a posttest questionnaire to assess information retention of the prototype, then participated in a posttest interview about updated understanding, security practices, and behavior changes as a result of viewing the prototype 1 week earlier. We are able to assess learning gains and information retention from participants' answers in the pretest data and compare them to the posttest data.[8]

6.3. Assessing Learning and Behavioral Outcomes

We compared the pretest data with the posttest data to assess participants' learning outcomes. In the pretest, we asked users to

[8]For the password comic, interviews were conducted with only 13 participants; therefore, the comparison between the pretest and posttest results were based on these 13 responses.

give general descriptions of how security works with regards to each security topic. Example questions include "Please describe ways a hacker would try to guess other people's passwords." (password comic study), or "Can you describe how antivirus software works to protect you from malware?" (antivirus comic study), or "Can you describe what geo-tagging is?" (privacy comic study). The purpose was not to test participants' ability to describe the technical aspects of security but to identify general concepts relating to how users think about security. We repeated many questions verbatim in the posttest session to evaluate whether the comics had improved users' understanding of security. The analysis was conducted by comparing codes and themes identified for each interview question in the pretest and the posttest using the qualitative analysis methodology described in Section 6.3. For example, we noted changes in participants' response in their conceptualization of how the security mechanism works in the pretest and the posttest interview data. To assess the effect on user behavior, we asked participants to report any behavioral changes or new actions taken after reading the comic.

Interview Analysis

The pretest and posttest interviews were audio-recorded and transcribed verbatim by the experimenter. Data were coded using the online data analysis application Dedoose (2013). To conduct qualitative analysis of the interview data, we used the grounded theory methodology (Corbin & Strauss, 1990). The process consists of three stages. First, we used open coding to analyze the transcribed responses point by point to generate descriptive codes. A code identifies a feature of the data that refer to the "most basic segment, or element of the raw data or information that can be assessed in a meaningful way" (Boyatzis, 1998). Table 6 shows a sample of codes applied to data extracts in the antivirus comic study. Second, axial coding was used to identify structure in the data by compiling and merging the open codes into themed categories. A theme captures something important about the data and represents a pattern of response or meaning within the data set (Braun & Clarke, 2006). For example, from the segment of codes in Table 6, we identified the "viruses are like pests" conceptualization (see Section 7.2.2). Third, selective coding was used to integrate the result of the open and axial coding around a "core" category to represent the central phenomenon of our data. We identified that certain conceptualizations related to specific behaviors. For example, participants who possess the "viruses are like pests" conceptualization of viruses perceive that viruses behave like a bug infestation that is difficult to remove (e.g., bedbugs). Several of these participants believed that reformatting the hard drive is the only way to completely wipe out a computer virus.

6.4. Evaluations and User Opinions of the Comics

Participants evaluated the comic and their learning experience in a questionnaire immediately after viewing the prototype. The questionnaire consisted of Likert-scale and open-ended questions. In this article, we focus on two areas of user perceptions: effectiveness and usefulness. For example, a question for measuring effectiveness is "visually teaching about smartphone geo-tagging and how to protect my privacy is an effective method to communicate this topic" (privacy comic study). Participants were asked to rate the validity of the statement on a 5-point Likert scale from 1 (*not at all effective*) to 5 (*very effective*). We also report participants' opinions of the prototypes based on open-ended feedback in the questionnaires and interviews.

6.5. Organization of the Results

We report on three areas from our comic user studies. First, we discuss users' pre- and postconceptualizations of password-guessing attacks in Section 7.1, malware and malware detection in Section 7.2, and mobile privacy concerning geo-tagging in Section 7.3 based on qualitative analysis of interviews with participants. Second, we discuss participants' self-reported behavioral changes during the posttest with respect to their password practices in Section 8.1, malware protection in Section 8.2, and mobile privacy practices in Section 8.3. Third, in Section 9, we summarize participants' prototype evaluations of the comics along with their opinions and feedback.

7. INTERVIEW RESULTS

7.1. Pre- and Postunderstanding of Guessing Attacks and Passwords

In our preinterview with participants about password-guessing attacks and password management, we uncovered the presence of a general target belief that may impact users' password-creation strategies, account prioritization, and understanding of "good passwords." Users believe that attackers target specific people. This belief may undermine users' perceived vulnerability based on the rationale that ordinary people with ordinary assets are unlikely targets. In the posttest, users had improved conceptualizations that more closely reflect a realistic threat model and understanding of the defenses. A summary of our analysis is provided in Table 7.

Guessing Attacks and Passwords Preconceptualizations

Password-guessing attacks are targeted. Seventy-seven percent of the participants believed that all password-guessing attacks are targeted attacks. The participants from this group correctly identified how targeted attacks work, but a few incorrectly described dictionary or brute-force attacks as variants of targeted attacks. For example, a participant described dictionary attacks as using dictionary words to guess the password but then went on to say that these words are based on your personal information: "I know you can run a program that can combine your significant things like name of our pets, names of your parents, names of your sisters, your name, your birthday, and it kind of just ran them with possible letter combinations" (PC10).

TABLE 7
Pre- and Posttest Conceptualizations of Guessing Attacks and Passwords

Password Preconceptualizations	% Subjects	Password Postconceptualizations	% Subjects
Password guessing attacks are targeted attacks	77	Password guessing attacks could be brute-force, dictionary, and targeted attacks	100
High-value accounts are bigger targets	69	Stronger passwords should be prioritized for high-value accounts that contain personal information	46
I'm an unlikely target because I'm small fish	46	A strong password does not contain personal info, dictionary words, or letter substitutions	100
"Secret" personal information is safe to use as passwords	38		

Another participant described a targeted variants of brute-force attacks: "Use a computer program to analyze everything and then try out different passwords a bunch of different times and combinations of information that's out there about me on the Internet" (PC9).

We found that a lack of understanding about dictionary and brute-force attacks may lead users to misjudge poor password combinations, like "P—a—s—s—w—0—r—d". This password may seem strong because it meets standard password rules (it is longer than eight characters and contains alphanumeric and special characters). Such a password may seem very secure because it would be very difficult for humans to guess in a targeted attempt, but it is highly susceptible to computerized dictionary attacks.

High-value accounts are bigger targets. Based on participants' "target" model, 69% of the participant believed that high-value accounts are bigger targets for attackers and therefore are more likely to be hacked. Online banking and primary e-mail accounts used for formal communication are identified are high value. Some who considered social media like Facebook to be a form of e-mail communication believed that it was also high value. Those who saw Facebook as a social tool deemed it unimportant. This group of participants said that they are more likely to create stronger passwords for the high-value accounts.

Participants classified "unimportant" accounts as sites that do not request personal information and accounts that are accessed only occasionally, like some entertainment sites, gaming sites, and forums. Participants perceive these accounts to contain very few assets and therefore are less likely to be hacked. Of interest, in some cases, important accounts like online banking are devalued when they contain few assets. PC5 explained, "I feel like who would want to get my money, who wants to get my banking information, there's nothing in there [no money] anyway!" The participant expressed low motivation to use a strong password for her online banking account because it is perceived as low value.

I'm an unlikely target because I'm small fish. Forty-six percent of participants believe that they are not vulnerable because attackers only target the wealthy and the famous. This finding coincides with Wash's (2010) "big fish" model. For example, PC10 stated, "I don't think there's anything in particular that makes me special, I don't have access to large amounts of money. I don't have an important job. I think I'm just equally at risk as any other university student." Many also believe that their ordinary life is simply not interesting to others:

> I don't really have any assets and I don't have any power or status. If you hack into a celebrity's Twitter, all of a sudden everyone is reading your message, but if you hack into my Twitter, literally no one would read the message. (PC13)

"Secret" personal information is safe to use as passwords. Participants thought that passwords associated with personal information are "bad," but 38% thought that only "public" personal information like birthdays, place of birth, current phone numbers or addresses, and names of close family should not be used as passwords. For example, participants would make statements like "I might use some things like my dog's name, but I would not use my birth date" (PC10). Other types of personal information are considered "secrets." One participant responded, "I use personal information, like the name of somebody I know or the name of a place that means something to me, but I think even if you knew me, you'd have a hard chance of guessing. . . . . " (PC10). Several participants also believe that outdated information like past addresses and phone numbers are safe to use. PC13 described,

> I often use words or names that are important to me that are not obvious. Like I'll use the names of all of my former bosses in a row, so that makes a really long word, and I can remember all of my former bosses' names. Again you would have to know all of my work history and worked in those places to figure that out.

Another said," I made [the password] something that no one would ever be able to guess. It's because it's my phone number when I grew up. Well no one is going to know that!" (PC2) These participants sincerely believed that outdated pieces of information are personal secrets and therefore are safe to use as passwords.

Guessing Attacks and Passwords Postconceptualizations

Password-guessing attacks could be brute-force, dictionary, and targeted attacks. When asked about how an attacker could guess someone's password in the pretest, many participants identified targeted attacks but were unaware of dictionary and brute-force attacks. In the posttest, all of our participants were able to identify that there are various attack methods, including brute-force, dictionary, and targeted attacks. They were able to describe how each attack works based on the information provided in the comic. For example, a participant described brute-force attacks as "using a computer algorithm to generate all the combinations of letters, numbers, and symbols" (PC13). They also demonstrated understanding of the rationale behind each attack, such as it is inefficient to use a brute-force attack to guess long and complex passwords, but it can be used to crack the simple passwords (PC1).

Stronger passwords should be prioritized for high-value accounts that contain personal information. Forty-six percent of our participants remained more concerned about accounts that they classify as high value than other types of accounts. The results from the pretest suggest that these consist mainly of banking, primary e-mail, and sometimes social media accounts. However, the comic influenced how they classified high-value accounts. For example PC2 said, "I reprioritized [my e-mail] as more important because all of my new changed passwords will go to that account, and so I changed it first."

A strong password does not contain personal info, dictionary words, or letter substitutions. All of the participants demonstrated a good understanding of how to create a strong password in the post-test. We believe that gaining knowledge about attack methods helped the participants understand why they should not use dictionary words, letter substitutions, or any personal information in their passwords. Participants gave examples such as "like how they have 'password' but the 'a' was the '@' symbol. When people try to use those easy passwords they try to make it harder somehow like using '0' for the 'o' but it's still really easy to guess" (PC12), or "They can do a random Google search of you, look at social networking sites, and basically put together information like your favourite pet, your hometown, birthdays and other stuff" (PC5).

7.2. Pre- and Postunderstanding of Malware and Malware Detection

Most participants were initially unable to distinguish between various types of malware. For example, computer worms were perceived the same as viruses. AC15 said, "I don't know if I'm familiar with that as a specific thing. So to me if I hear someone say computer worm, I would just think oh, do you mean a virus." Participants initially had an easier time describing how trojans spread, mainly because of their familiarity with Greek mythology. To most participants, trojans are a type of virus in disguise. For example AC10 said, "I've heard of this one mainly because of mythology. It basically masks itself as one thing but there is something deadly inside." "Adware" and "spyware" were perceived as types of malware, mainly because the terms sounded alike. They believed "malware" is something that causes annoyance rather than real harm to computer systems, like spam, pop-up ads, or behavioral advertising. In the posttest, most participants could distinguish different types of malware and demonstrate understanding of how antivirus software works.

Malware Pretest Conceptualizations

A "virus" is more harmful than "malware.". Table 8 summarizes participants' perception of the harm caused by "virus" and "malware." A computer virus is a class of malware; however, half of our participants perceived "virus" and "malware" to be distinct threats. They thought that "malware" was less harmful than a "virus." AC9 said, "To me the word virus just sounds like it could be worse. Malware kind of sounds like it's just a pain, like something that is added-on." AC2 associated malware to spam: "From what I heard, a virus can basically . . . sometimes it can prevent you from opening your files. Compared to malware . . . I usually call that spam." In general, "malware" caused irritation and annoyance, such as interruptions by pop-up ads, spam, or personal information used for advertising. A "virus," on the other hand, caused serious damage that could be devastating for users. This may include corrupting data and compromising or entirely disabling systems and networks. Many participants believed that malware does not cause harm directly to computers but instead just disturb users. For instance, AC1 said, "Virus is more dangerous. It damages your whole computer. Malware just distracts you."

Thirty-one percent of participants perceived "virus" and "malware" to be nearly equivalent but were unable to exactly define malware. These participants generally felt that both were "bad" and should be avoided. For example AC15 said,

To me they aren't really different. To me it's a lament basically. They are all things that I don't want to have. They are all things that I would worry about somehow wrecking my experience with the computer. So whether they are officially classified as viruses or not, I treat them the same way.

Thirteen percent of participants had no idea how to define the terms.

We asked our participants to define the term "virus." Their responses are summarized in Table 8.

Viruses are like pests. Thirty-eight percent of participants associate viruses with pests, such as a bug or a worm. They imagine them to have "somehow got through the cracks" of a

TABLE 8
Pre- and Posttest Conceptualizations of Antivirus and Malware

Antivirus preconceptualizations	% of Subjects	Antivirus postconceptualizations	% of Subjects
Inclusion	31	Inclusion	88
Exclusion	38	Exclusion	1
Risk assessment	12	Risk Assessment	1
Don't know	19	Don't know	0
Malware preconceptualizations		**Malware postconceptualizations**	
"Virus" more harmful than "malware"	50	A virus is a specific type of malware; malware causes varying degrees of harm	69
"Malware" more harmful than "virus"	6	Signature	31
Both are equally harmful	31	DNA	25
Don't know	13		
Pest	38		
Biology	25		
Mechanical	25		
Code	12		

TABLE 9
Pre- and Postconceptualizations of Mobile Online Privacy

Privacy preconceptualizations	% of Subjects	Privacy postconceptualizations	% of Subjects
Geo-tagging is geographically tagging people	67	I need to switch off geo-tagging and GPS to protect my mobile online privacy	50
I base by sharing decisions on social relationships and context	72	I need to check location information before I post photos on social media	33
I control my privacy	33	I should not upload photos from my phone	11
I have nothing to hide	27		
1 I have nothing to lose	20		

Note. GPS = global positioning

computer, much like how pests slip through the cracks of a home to get inside. AC15 described it as "a bug or a worm or some type of pest that's invasive that might get inside your house." Viruses that got inside of the computer could be "eating things up" and could "take on a life of its own . . . like a little worm." Those who associate viruses with pests perceived them to be difficult to remove. For example, AC13 said, "I would connect it with bedbugs. Like even if you want to kill it you can't destroy it." Several participants believe that the only way to completely get rid of a computer virus is to reformat the hard drive.

Viruses are like infectious micro-organisms. Twenty-five percent of participants believed that computer viruses are like infectious viruses in living organisms. To visualize what viruses might look like, participants associate them with images of actual viruses under a microscope, such as AC12's description of "a sphere with the little bumps on it." Viruses can grow and take over the host. AC3 said, "I have no idea how it works on computers. Viruses seem like, from TV shows, cancer cells that just convert everything." Participants in this category believe that computer viruses spread from computers to computers, just like how a real virus could spread from one host to another.

Viruses cause computers to mechanically break down. Twenty-five percent of participants gave much more general descriptions. They literally visualized computers breaking down and not working properly. Participants such as AC2 described that viruses can "basically damage my work and my computer" but were unable to specify how that can be achieved.

Viruses are pieces of code. Thirteen percent of participants described viruses as pieces of codes or computer programs. Visually, the participants pictured viruses as binary numbers. As AC14 described it, a virus is "some code, some program, 0101010, numbers."

Malware Post test Conceptualizations

A virus is a specific type of malware; malware causes varying degrees of harm. During the posttest, 69% of our participants were able to distinguish various types of malware. They understood that "malware" is an umbrella term for malicious software like viruses, trojans, worms, spyware, and adware that have different purposes and causes varying levels of harm.

Malware has a "signature.". Thirty-one percent of participants identified that malware have unique signatures and that antivirus software identifies malware by their signatures. They have a general conceptualization that a signature "has to do with the code" and that antivirus software "detects series of code and raises a red flag (if there's a match)" (AC15). If the signature is "in its memory it's able to catch it. Otherwise it's not able to catch it. The more you update it [antivirus software] . . . it's able to capture [malware]" (AC13). These kinds of descriptions suggest that participants has a basic understanding that antivirus detects malware by its signatures and therefore it needs to be updated frequently.

Malware has a "DNA.". A variation in participants' description of malware signature is "DNA." We believe this is due to the existing biology conceptualization from the pretest, as well as being influenced by the medical metaphor we used throughout the antivirus comic. Specifically, we used a DNA graphic to portray malware signatures on page 11 of the comic. Twenty-five percent of participants used the term "DNA" to directly describe malware signatures. An example description is "antivirus detects the DNA of the virus" (AC16).

Malware Detection Pretest Conceptualizations

We identified three basic beliefs about how antivirus software "catches" viruses, summarized in Table 8.

Inclusion detection. The inclusion detection belief is closely related to how antivirus software actually works. Thirty-one percent of participants believed that the antivirus has a blacklist database of previously known viruses. When a file matches a known virus, the antivirus alerts the user. AC12 described antivirus software as having "a database of files categorized that are virus files, and checks to see if you got any on your computer, and if there's a match they will try to delete it or isolate it somehow." Another said, "It has a database on its own since it keeps updating itself. Each time it increases, it scans the computer and sees if there is any files that are the same, then it detects it as a virus" (AC5). These participants had a basic understanding that antivirus works with a library or database that needs to be updated to recognize new viruses.

Exclusion detection. Thirty-eight percent of participants believed that the antivirus has a whitelist of legitimate programs. When a file does not match the antivirus's list of "good" programs, it flags it as a virus. Some participants imagined the antivirus to work like a filter, where it segregates legitimate files from malicious ones. As AC15 described it, if I were to visualize it might be some kind of net and only certain shapes fit through, and the viruses are not shaped properly and that it catches them. Perhaps that shape has something to do with the data or code or something like that.

Risk assessment. Thirteen percent of participants believed that downloaded files are somehow linked to the original source, and the antivirus software tracks the origin of both legitimate and malicious files. One participant believed that the software scans and checks for potential risks associated with the site from which he is downloading. Another participant believes that there is an active link between files and their source, especially from peer-to-peer sharing sites. AC9 said

It's still connected to a IP address. If you just download a file, the file is on your computer and that link is cut from where it came from, but if it was a peer-to-peer sharing site with a virus, it is still be connected to different computers. It's looking for atypical files.

This user believes that antivirus software assesses the origin of the file and evaluates the risks, but once the user accepts and downloads the file, the active link is cut.

Malware Detection Posttest Conceptualizations

In the posttest, the majority (88%) of our participants correctly held the inclusion conceptualization based on the information obtained from the comic. Participants recognized that antivirus software maintains a blacklist of malware, and therefore the database needs to be updated regularity to detect new malware.

7.3. Pre- and Postunderstanding of Mobile Online Privacy and Geo-tagging

When we initially asked about how people could be tracked online, only 2% of participants mentioned geo-tagging. They primarily described other types of online tracking methods like GPS, status updates or images on social media, location check-in, IP addresses, and browser cookies. In the posttest, participants understood the dangers of geo-tagging and knew strategies to protect against it.

Privacy Preconceptualizations

"Geo-tagging" is geographically tagging people. Most participants were able to identify that "geo-tagging" is somehow related to geographic locations due to the word "geo" but mistakenly thought "tagging" referred to manually tagging a photo or a person to a location (i.e., checking in friends on social media). For example, MC10 described

> I think it's pretty much tagging your friend or someone in a photo, video, or status, or any topic. You just indicate where that thing was, or where this thing took place to give a better description of what you are talking about, or what you are trying to share on that social network.

Many participants used vocabulary like "if you tag someone" or "when you tag a photo." This demonstrates a sense of control over what location information is shared. They believed that only explicitly shared location information could

be tracked by others. Alarmingly, only one participant specifically mentioned metadata containing geographical coordinates automatically attached to image files.

I base my sharing decisions on social relationships and context. Participants unanimously agreed that they have a social obligation to protect the privacy and personal information of others, particularly close family members. Of interest, when probed deeper about social obligation and current practices used to protect others, few actually seek consent. Instead, we found that sharing decisions are based on assumptions of *who* the friend is and the *social context.* For instance, a participant may choose to share "normal" pictures of their friends but not drunken photos from a party. MC14 explained, "It is a courtesy to not to share anything that (people) won't appreciate being shared." Some said they would share photos of their friends unless they receive requests to stop:

> Some friends actually asked me not to tag them in some photos, and I respect that because they don't want people to see them in it . . . other than that I don't think my friends would be offended if I post something. (MC10)

A few participants also received requests from friends to take down posted photos: "Sometimes they did ask me to remove the picture and stuff, because I hold the camera most of the time when I go to parties so I upload" (MC18). A few participants thought group photos were OK to share because they would not be considered personal photos. Participants were even less inclined to ask for permission from individuals when sharing group photos online.

Many participants expressed mild concern over their online privacy. Within this group, we identified three conceptualizations of online privacy:

I control my privacy. Thirty-three percent of participants were not very concerned about their online privacy, because they believed that they had control over what they shared and with whom. MC5 said, privacy tools "make you feel safer in a way that I can choose who I share things with." Several participants expressed that they do not overshare and believed that as long as they are careful about what they put online, they are not vulnerable.

I have nothing to hide. Twenty-seven percent of participants were not concerned about their online privacy, because they believed that they had nothing to hide or to be "ashamed of." As MC3 explained,

> Personally I feel like I don't really have anything to hide . . . . If I were someone who did have some sort of information that could be damaging, then I would be deeply concerned about it. As it stands right now, I just don't really have anything to hide.

This group of participants felt that they only upload things that they *want* people to see, so there is no need to protect them.

I have nothing to lose. Another 20% of participants were unconcerned about their online privacy because they felt they had nothing to lose. This attitude coincides with the "big fish" model (Wash, 2010), where people believe that only the rich and famous are vulnerable.

Privacy Postconceptualizations

I need to switch off geo-tagging and GPS to protect my mobile online privacy. In the posttest interview, half of the participants were very concerned about mobile online privacy after learning about geo-tagging. Many said that they were not aware that this setting existed prior to the study. This group of participants recalled from the comic that geo-tagging is often enabled by default. To protect their online privacy, they believe that they should disable geo-tagging and GPS on their mobile device and enable them only needed. This advice was recommended in the privacy comic, and given their lack of awareness beforehand, we assume that these strategies came from the comic.

I need to check location information before I post photos on social media. This group of participants (33%) believe that when posting pictures on social media, they should check whether the photo contains location-based information, such as location check-in and locations revealed in photo content.

I should not upload photos from my phone. A small number of participants (11%) now believe that uploading photos from the phone is unsafe and therefore they would not upload any photos from their mobile device.

8. POSTTEST RESULTS: PERSUASIVE EFFECT

8.1. Persuasive Effect on Password Behavior and Understanding

When our participants returned 1 week later for the posttest interview, we asked them whether they had changed their passwords. Their responses are grouped based on their self-evaluated password strength prior to the intervention, shown in Table 10. Understandably, some respondents felt that they already have strong passwords. The eight participants with self-assessment of prior strong or moderately strong passwords did not change them. However, most important, 80% of respondents with prior weak passwords changed them at home after reading the comic. Respondents changed passwords primarily for high-value accounts with sensitive information like online banking, e-mail, and Facebook. PC2 responded, "In the past, I've been told 'you shouldn't do this' and I was like yeah-yeah-yeah, but none of us did." The comic persuaded her to move from "I *should* do that" to "I did that." Encouragingly, 85% of our study participants said they would use the tips learned in the comic to create new passwords in the future. Respondents who changed their passwords used the recommended passphrase strategy.

In the pretest interview, we found that most participants had a poor understanding of brute-force and dictionary attacks, and believed all password guessing attacks were variants of targeted attacks. Figure 4 shows that 57% of respondents demonstrated understanding of brute-force attacks and 62% for dictionary attacks, compared to just 19% and 29% prior to

TABLE 10
Password Comic: Behavioral Change

Behavior Change	% of Subjects	
	Weak Passwords	Moderate to Strong Passwords
Changed passwords	80	0
Used passphrase	80	0

TABLE 11
Antivirus Comic: Behavioral Change

Behavior Change	% of Subjects
Updated antivirus within 1 week	31
More conscious of security warnings	19
More cautious when browsing and downloading	38
Shared knowledge	69
No effect	13

learning 1 week after learning. Most respondents were able to describe targeted attacks on both occasions. Participants defined dictionary attacks as "using pre-existing words from different languages," "slangs," "misspellings," or "names." Brute-force attacks involved trying to guess "every possible combination" and using "computer algorithm to generate all the combinations of letters, numbers, and symbols."

Several respondents said that learning about the attacks made them rethink the strength of their current passwords and ask questions like, "Are my passwords actually good? Am I vulnerable?" PC9 said, "The different methods they can use to figure out what your password is . . . so my passwords might not have been as good as I thought."

8.2. Persuasive Effect on Antivirus Behaviour and Understanding

To assess the persuasiveness of the antivirus comic on user behavior, we asked participants to self-report any changes in habits. Table 11 provides a summary of participants' self-reported behavior. Thirty-one percent of respondents said they performed updates after viewing the comic.

AC15 said,

> I did go update Avira after our first meeting. I thought I might as well just go and do it, it's not going to be that hard, and I suppose it probably made me more cautious of things that could infect my computer.

AC10 said,

> It made me realize that I need to be more aware and actually, I went back to my computer and looked at my antivirus software that I had (at work) and I went home and looked at my antivirus and made sure that it was up to date. I made sure everything was working on it.

Thirty-eight percent of respondents reported more caution when surfing the Internet and/or downloading files. Nineteen percent said they paid more attention to security warnings. It is interesting that, 69% of respondents voluntarily shared the advice from the comic with friends and family without prompting. We view this sharing behavior as extremely positive.

In the pretest interview, most respondents were unaware that antivirus software needs regular updates. After interacting with the antivirus comic, the majority of the respondents showed improvements in their conceptualization of antivirus protection. Figure 4 shows that 88% of participants correctly described how the software works to detect viruses, compared to just 13% in the pretest interview. Eighty-one percent of respondents articulated why they should perform regular updates. They made statements like, "I didn't know that by updating it's actually able to catch more things" (AC13) and "It now actually allows me to understand how it's worked and why is it so important to keep it up to date" (AC10). Six respondents specifically used the comic's analogies, narrative, and characters to describe various concepts. For example, respondents used the DNA analogy made on page 12 of the comic. It explained that each virus has a unique signature like a DNA sequence. This information is stored in the antivirus database that must be frequently updated to be effective at detecting new viruses. In the posttest, participants made statements like, "It detects the DNA of the

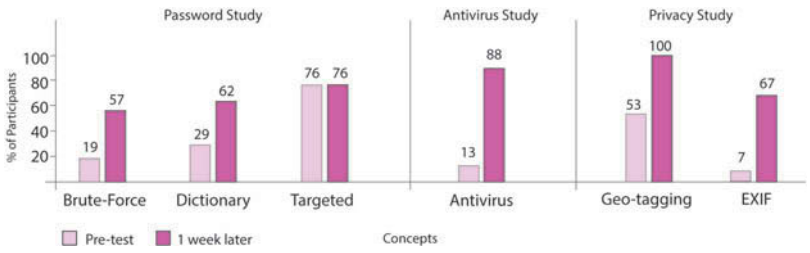

FIG. 4. Participants' ability to describe various security concepts before and after viewing the comic.

TABLE 12
Privacy Comic: Behavioral Change

Behavior Change	% of Subjects
Changed location-based settings	53
Cautious photo sharing behavior	27
No effect	20

virus" (AC16) and "It analyses the sequence, so I guess the code sequence just like an DNA in a human" (AC11). AC7 described scenes from pages 8 and 12 of the comic involving the character Hack: "Because the villain is constantly coming up with new ones, spreading them out to get information, to send more spam. So to update it is to recognize the ones that are being put out on an ongoing basis."

8.3. Persuasive Effect on Privacy Behavior and Understanding

One week after viewing the privacy comic, 53% of participants self-reported to have changed location-based settings on their smartphones. These include disabling GPS on their devices and removing location metadata from photos. Participants were also more aware of photo content that could reveal personal information. For example MC8 said, "Since viewing the material, I definitely took actions online (and on my smartphone) to protect my privacy online. I changed my settings on my phone . . . and I am also careful when uploading pictures in case there is anything in the background of the photo that could be used like my drivers licence or a credit card." Another 27% of participants said that the comic has raised their awareness about online privacy and therefore motivated them to behave more cautiously online. Interestingly, some respondents also took the initiative to share their experience with others. For example MC7 said, "I told my sister about it and if I ever do upload pictures more frequently I will take precautions to ensure important information cannot be extracted from the picture." Participants' behavior changes are summarized in Table 12.

Participants showed excellent retention of knowledge 1 week after viewing the comic. We assessed retention based on our participants' ability to describe two major concepts conveyed in the comic–geo-tagging and Exchangeable Image File (EXIF). Figure 4 shows that all respondents were able to identify what geo-tagging means in the posttest compared to 53% in the pretest. Similarly, 67% of respondents correctly described the EXIF concept compared to just 7% in the pretest.

Our participants demonstrated a reasonable understanding of the concepts in their responses. An example of a response for geo-tagging was "assigning geographical co-ordinates information to the metadata of a photograph, indicating where the picture was taken" (MC14). An example response for EXIF was "a format in which your location and information is present for viewing and extraction when sharing images online" (MC5). Most participants also recalled the prevention measures such as disabling the GPS when not in use, refraining from sharing photos with sensitive personally identifiable content, and removing metadata with EXIF editors.

9. POSTTEST RESULTS: PERCEIVED EFFECTIVENESS AND USEFULNESS

As shown in Figure 5, participant evaluations for the *effectiveness* and *usefulness* of the three comics as an educational tool were highly positive.[9] There was consensus among participants that presenting the information visually as an comic was easy to read and understand, and they reported a pleasurable learning experience. The comics took little time and effort to read but gave useful information about the threats and practical protection strategies. Some commented that even though they are familiar with some of the advice, they have never heard it in a cohesive fashion like in *Secure Comics*. Participants believed that presenting the information as a comic has positive effects on how well they could recall the advice later. AC11 said, "I might read the information but I wouldn't remember it normally, but I think I would remember what I read in the comic."

Our participants expressed interest in the narrative and the characters of *Secure Comics* and believed that the medium would be suitable for a wide range of age groups, including children. The characters helped users relate to the topics and created interest. We observed several participants chuckle while reading the comic, which is a reassuring response that the use of humor in *Secure Comics* was appreciated. PC10 responded, "I think it's great and some parts are really funny; I never thought that you could present security information like this before."

After reading the comic, most participants believed they gained useful knowledge about the topic. They thought it was most useful for clarifying common misunderstandings and learning about coping strategies. Some participants admitted that even though they are aware of the risks, they were often not sure what to do about them. The comics taught them practical advice, such as how to create a passphrase so that strong passwords are memorable.

10. DISCUSSION

We now provide a summary of the key findings and discuss their potential applications, frame our work within the Elaboration Likelihood Model (ELM) of persuasion, and discuss how our work crosses the boundaries between instructional design and persuasive technology.

10.1. Applications for Educational Online Interactive Comics

Interactive comics open new avenues for experimenting with the narrative. During the eye-tracking experiment, we made

[9]Although our studies used different point scales for these two questions, the results were all clearly highly positive.

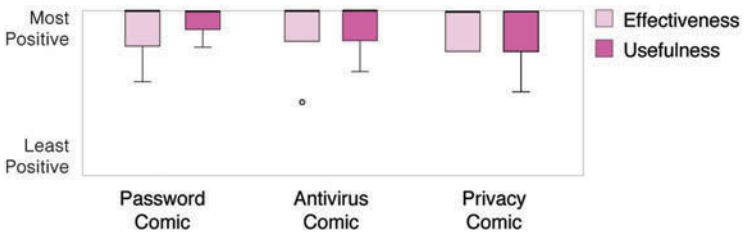

FIG. 5. Summary of participants' Likert-scale responses assessing the comics' effectiveness at conveying information and usefulness of the presented information.

possible connections between visual attention and comprehension of the information. We noted that participants spent a much longer time looking at the interactive content and engaged with them at least once. For some participants, we also observed back-tracking behavior after looking at an image or an interactive example. It is often the case that educators want users not only to look at the educational content but also specifically to focus their attention on important points, such as parts that deliver a key take-away message. Interactive techniques demonstrated in *Secure Comics*, such as interactive examples, mouseovers that demonstrate cause-and-effect relationships, and minigames, could be used to emphasize or clarify the message to be communicated.

Our qualitative and quantitative results show that the majority of participants demonstrated improved knowledge and awareness, which led to positive self-reported behavioral changes 1 week after viewing the comics. These behaviors include updating/changing security system settings, being more cautious while web surfing or downloading files, and voluntarily sharing security information with family and friends without prompting. Participants' evaluations show that they found the comics to be effective and useful as learning tools.

We believe that our findings and design approach of educational online interactive comics may be generalizable to many different areas. For example, in healthcare research, there is already a growing trend of using graphic stories to help enhance doctor-to-patient and public health communications (Green & Myers, 2010). We believe that the use of interactive online comics provides doctors with the opportunity to give important health information. *Secure Comics* demonstrated the potential for added layers of information over the graphic narrative. Even modest interactions like mouseovers could supply the reader with additional insights and related information. For example, making "pathographies" interactive to help patients to learn about their illness could provide them with important treatment information and other resources embedded within the story.

10.2. Using Comics to Direct Users Toward the Central Route

Modern theories of persuasion have evolved to consider the multiple processes of persuasion that could affect attitude and behavior, such as the ELM (Petty & Cacioppo, 1986). The model describes two routes to persuasion-based decision making. We consider our work through the lens of ELM to understand how the comic can persuade users to learn and take positive actions.

When people are motivated to pay attention, they take the *central route* to decision making based on careful, logical, and conscious thinking about the communication, which could lead to permanent change in attitude or behavior. The ELM suggests that effective persuasion is more likely to occur when the communication is personally relevant, which results in a higher elaboration likelihood and causes people to take the central route. In our interactive comic, we carefully crafted our narrative to make the characters relatable, keep the language conversational, and use examples relevant to most users. We encouraged users to reflect on the content by providing contiguous graphics and text and embedding small interactive components highlighting the main lessons. Our empirical results suggest that our comics were successful to the extent that we tested. Users appeared engaged, demonstrated increased knowledge, provided positive feedback, and self-reported behavior changes 1 week later.

When people take the *peripheral route,* they are influenced by superficial characteristics such the attractiveness of the communication, causing a temporary change in attitude or behavior. At first glance, this seems undesirable, but we suggest that the peripheral route could be useful if the receiver has little or no interest in the communication, as is frequently the case with security education. The surface attractiveness of the message might be sufficient to direct people into a temporary state where they are more susceptible to further change or suggestion. If the initial attractiveness and novelty of our comic caught users' attention when they would have otherwise ignored the information, this gives us a clear opportunity to convince users that the information is personally relevant and thus convert them to the *central route.* We have evidence of this happening from user comments suggesting that they would never have paid attention to the same information presented in standard text format.

10.3. Parallels Between Instructional Design and Persuasive Principles

According to Mintz and Aagaard (2012), discussion about persuasion is certainly not absent from the field of instructional design, but little attention has given to drawing possible connections between instructional design and persuasive technology principles. From our experience designing, implementing, and

evaluating *Secure Comics*, we discuss how principles of instructional design relate to principles of persuasive technology and how one can support the implementation of the other.

1. ID principles that reduce the cognitive load (multimedia and contiguity) and support the easy reading and navigation of the instructional material (signalling and segmenting) may help to reinforce the persuasive principle of reduction.

The persuasive principle of reduction states that by making learning easy to do, users are more likely to complete the task (Fogg, 2003). The ID principles of multimedia and contiguity reduce the cognitive load, enhance comprehension, and increase long-term memory (Mayer & Anderson, 1992; Paivio, 1991). For example, one of our participants explained, "Graphics would get more attention and draw more people in. It is also easier to commit to memory when there are graphical parallels you can draw upon." In the ELM, we argued that the surface attractiveness of a comic may draw users' attention to the education material. Because higher interest and greater learning are correlated (Wade, 2001), this potential to increase the elaboration likelihood could reduce the need for high motivation to learn about security and privacy content, which is a central problem to overcome in security education. Past work also suggests that the comic media may help users overcome the "intimidation factor" associated with technical topics (Srikwan & Jakobsson, 2008). Therefore, we argue that ID principles that simplify learning could assist in the design of persuasive technology tools that persuade through the reduction principle.

Our eye-tracking data show that participants alternated their attention between related image and textual content. In addition, they showed prolonged eye-fixations when graphics and text were integrated with interactivity.

Special graphical treatments in the comic such as circular graphics highlighted with color and adding faces to objects drew users' attention to certain areas of the page. Segmenting the material into chucks encouraged users to progress at their own pace. For example, some of our participants read a certain panels more than once, or backtracked to a previously viewed page before moving forward.

2. The ID principle of reflection provides "checkpoints" for users to self-monitor their learning progress and adjust their pace as necessary.

The ID principle of refelction could be useful in self-monitoring tools, which are designed to make it easier for users to monitor their own behavior (Fogg, 2003). In *Secure Comics*, moments of reflection are prompted with interactivity, which caused users to pause and think about what they were reading. We believe these reflection tools could be placed throughout the learning material to act as "checkpoints" to help learners identify if they thoroughly understood the concepts. For example, our eye-tracking data suggest that after viewing an interactive tool, some users back-tracked and reviewed a previously read page. This behavior suggests that the tools helped them to refocus their attention on a previously learned concept to gain a deeper understanding.

3. The use of conversational language and pedagogical agents from the ID principle of personalization increases user immersion in the lesson. It reinforces the persuasive principle of social interaction.

Our results support prior research that the use of pedagogical agents motivate users to learn (Mayer, 2002) and increase attention (Clark & Mayer, 2011). If people are interested in what they are learning, they take more care while processing the information (Wade, 2001). In *Secure Comics*, we successfully demonstrated that "agents" can achieve user immersion in the lesson. Participants' feedback indicate that the inclusion of characters and a story made the topics more relevant and interesting. For example, one of our participant responded, "Any time you have characters and a story, everything becomes more relatable." Our eye-tracking data showed that participants focused their attention on characters' facial features and showed back-and-forth viewing patterns between interacting characters. User feedback and in-lab observations show that the characters' use of informal language and social cues like humor generated positive attitudes toward them. We observed several of the participants chuckling during learning. The comics were described by our participants as "funny," "relatable," "enjoyable," and "fun" to read.

4. Recalling prior knowledge through metaphors helps users build conceptual and procedural mental models.

The comics help users to develop conceptual knowledge by building mental models through metaphors and analogies, then provide procedural examples to help reinforce the concepts. Our pretest interview analyses showed that users have poor conceptualizations of risks in computer security. To help users improve them, we used metaphorical explanations in *Secure Comics*. The metaphors were described by participants as "familiar" and "relatable." For instance, the medical metaphor from the antivirus study provides meaningful comparisons between computer viruses and biological viruses. A participant explained, "If you just portray computers, people may not understand what it means because it's technical. Everybody understands how germs and viruses can affect the human body, so they can make meaningful comparisons with how computer viruses work." This result shows that a well-understood concept, such as how biological viruses can spread in epidemic proportions, can help users understand new topics such as computer viruses. In our posttest studies, some participants directly applied metaphors used in the comics to their descriptions of security concepts 1 week later, suggesting that the use of metaphor could assist in the recall of learned information. For example, several participants used scenes from the comic to describe how antivirus software works and describing virus signatures as "DNA" sequences. Therefore, the principle of conceptual and procedural knowledge could be leveraged in persuasive technology tools

to increase the rhetorical appeal of the lesson and increase the recall of information.

10.4. Limitations and Future Work

One limitation of evaluating educational material in a lab environment is that users cannot experience the learning materials in the context in which they will be displayed and used. Environmental factors such as placement, location, format, size, and time, and the technological platform, may influence how the material is absorbed by end-users.

The reading format of comics is different across cultures. For example, the standard reading direction of panels in Japanese Manga is from right to left. Text direction is also read differently in some non-English languages. Our comics are adapted for a North American audience, but cultural differences will need to be considered if the comics were to be translated into different languages to reach a wider audience.

In the eye-tracking study, we did not find users skimming or skipping content, but users may exhibit different reading behavior outside of lab settings, particularly when they are not prompted to read.

Our participants are limited to students from our university. University students tend to be fairly young and may have more experience with computers than the general population. The next step of this research is to evaluate the educational material with a wider range of end-users in their own environment.

Research into end-users' password management strategies has found that there is a discrepancy between what users know and what they actually do (Riley, 2006). Although difficult in practice, measuring actual behavioral change would be more desirable than relying on self-reports.

Our study does not measure knowledge retention and transfer beyond 1 week. Although many of our participants reported positive learning outcomes and changes in behavior, it is unknown whether they will retain the knowledge and continue with these practices in the long term. Future longitudinal studies are needed to determine whether users will continue with these practices over a longer period.

We suggested several ways that instructional design principles can be applied to persuasive tools. Giving immediate feedback in education has similar goals as the persuasive principle of conditioning, which is to provide positive reinforcement for targeted behaviors (Fogg, 2003). In *Secure Comics*, although this principle is applied to the minigames at the end of each series, its effectiveness will need to be formally evaluated.

In future work, we propose that the comic could be tailored to individual users by substituting users' information in the lesson content. For example, agents could address users by their first name or use the user's real pet's name in a password demonstration. During deployment, the comic could be suggested to users by our industry supporters, such as when they have just entered a weak password or during security software installation.

11. CONCLUSION

We designed and implemented three entertaining interactive comics addressing security topics based on persuasive principles to help users refine their understanding of threats and defense strategies and to persuade users to embrace positive security behavior. Our user studies confirmed the effectiveness of our designs. We show that simplifying security content through graphical communication and metaphors reduced cognitive load and increased comprehension. The interactive components of the comics increased persuasion by providing insights into why users should follow the recommended advice. The interactive user experience created entertainment and engaged users in the lesson content. In addition, the inclusion of humorous characters and a compelling story generated interest and motivated users to learn. Our comic prototypes are available as a public learning resource, at http://www.versipass.com/edusec.

Our interview analysis shows that users had poor initial understanding of security threats, which may influence their motivation and ability to practice safe behavior. The comics successfully induced positive self-reported behavior changes in users, including updating security software settings, cautious web surfing or downloading behavior, and sharing of information with family and friends without prompting. Participants showed good retention of information after 1 week and demonstrated improvements in awareness of the threats and why they should follow the recommended security advice. Their feedback indicated that the comics were enjoyable and useful learning tools, which persuaded them to adopt improved security practices.

The empirical evidence from our user studies suggests that communicating the benefits of the advice is necessary to persuade users to change their behavior. We showed that embedding security training in an entertaining interactive comic series helped users overcome the difficulties associated with learning. The highly visual nature of comics supported comprehension and increased retention. Metaphors used to illustrate abstract concepts further improved users' security understanding. Interactive storytelling was used to immerse users and increase engagement. From our experience, we provided a discussion of how instructional design principles can be used to help implement and reinforce principles of persuasive technology. Although the focus of our research was computer security, we believe that our approach is generalizable for end-user communication in various domains sharing similar characteristics.

FUNDING

This project has been partially funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC. Sonia Chiasson acknowledges funding from NSERC for her Canada Research Chair in Human Oriented Computer Security. This work was also partially funded by the

NSERC ISSNet Strategic Network and the GRAND Networks of Centres of Excellence.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46.

Adams, S. (2012). Dilbert. Available from http://search.dilbert.com/comic/Security

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*, 613–643.

Anderson, J. R., Corbett, A. T., Koedinger, K. R., & Pelletier, R. (1995). Cognitive tutors: Lessons learned. *Journal of Learning Sciences*, *4*, 167–207.

Anti-Phishing Working Group (2013). APWG CMU-Cylab phishing education landing page program. Availabel from http://phish-education.apwg.org.

Asgharpour, F., Liu, D., & Camp, L. (2007). Mental models of security risks. In *Financial cryptography & data security, LNCS* (pp. 367–377). New York, NY: Springer.

Atkinson, R. K. (2002). Optimizing learning from examples using animated pedagogical agents. *Journal of Educational Psychology*, *94*, 416–427.

Balebako, R., Jung, J., Lu, W., Cranor, L., & Nguyen, C. (2013, July). *Little brothers watching you: Raising awareness of data leaks on smartphones*. Paper presented at the *symposium on Usable Privacy and Security*, Newcastle, UK.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Thousand Oaks, CA: Sage.

Branson, R. K., Rayner, G. T., Cox, J., Furman, J. P., & King, F. J. (1975, August 1). *Interservice procedures for instructional systems development: Executive summary and model*. (Tech. Rep.). DTIC Document.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101.

Brophy, J. (1983). Conceptualizing student motivation. *Educational Psychologist*, *18*, 200–215.

Camp, L. J. (2009). Mental models of privacy and security. *IEEE, Technology & Society Magazine*, *28*, 37–46.

Chiasson, S., Manas, M., & Biddle, R. (2013). *Auction hero: The design of a game to learn and teach about computer security*. Retrieved from http://hotsoft.carleton.ca/~sonia/content/Chiasson_Auctionhero_ELearn2011.pdf.

Chiasson, S., van Oorschot, P. C., & Biddle, R. (2006). A usability study and critique of two password managers. *Proceedings of the 15th USENIX Security Symposium*, Article 1.

Clark, R. C. (2011). *Developing technical training: A structured approach for developing classroom and computer-based instructional materials*. New York, NY: Wiley & Sons.

Clark, R. C., & Mayer, R. E. (2011). *E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning*. New York, NY: Wiley & Sons.

Commons, W. (2013). Addie model of design. Retrieved from http://upload.wikimedia.org/wikipedia/commons/d/d3/ADDIE_Model_of_Design.jpg.

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *13*, 3–21.

Craik, K., & James, W. (1967). *The nature of explanation*. New York, NY: Cambridge University Press.

Dedoose (2013). Dedoose research application. http://www.dedoose.com.

Denning, T., Kohno, T., & Shostack, A. (2013). Control-alt-hack: A card game for computer security outreach and education. *Technical Symposium on Computer Science Education*, 729–729.

Dixon, N. M. (1990). *Evaluation: A tool for improving HRD quality*. San Diego, CA: University Associates.

Dormann, C., & Biddle, R. (2009). A review of humor for computer games: Play, laugh and more. *Simulation & Gaming*, *40*, 802–824.

Dourish, P., Grinter, R. E., De La Flor, J. D., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal & Ubiquitous Computing*, *8*, 391–401.

Eisner, W. (1985). *Comics & sequential art*. Tamarac, FL: Poorhouse Press.

Fies, B. (2011). *Mom's cancer*. New York, NY: Abrams.

Florencio, D., & Herley, C. (2010). Where do security policies come from? *Proceeding of the 6th Symposium on Usable Privacy and Security*.

Fogg, B. J. (2003). *Persuasive technology: Using computers to change what we think and do*. San Francisco, CA: Morgan Kaufmann.

Friedland, G., Maier, G., Sommer, R., & Weaver, N. (2011). Sherlock holmes' evil twin: On the impact of global inference for online privacy. *Proceedings of the 2011 New Security Paradigms Workshop*, 105–114.

Friedland, G., & Sommer, R. (2010). Cybercasing the joint: On the privacy implications of geo-tagging. *Proceedings of the 5th USENIX Workshop on Hot Topics in Security*.

Gagne, R. M., Wager, W. W., Golas, K. C., Keller, J. M., & Russell, J. D. (2005). *Principles of instructional design*. Wiley Online Library.

Garner, R. L. (2006). Humor in pedagogy: How ha-ha can lead to aha! *College Teaching*, *54*, 177–180.

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. *Proceedings of the Symposium on Usable Privacy and Security*, 44–55.

Goga, O., Lei, H., Parthasarathi, S. H. K., Friedland, G., Sommer, R., & Teixeira, R. (2013). Exploiting innocuous activity for correlating users across sites. *Proceedings of the International Conference on the World Wide Web*.

Görling, S. (2006). The myth of user education. *Virus Bulletin Conference*, *11*, 13.

Green, M. J., & Myers, K. R. (2010). Graphic medicine: Use of comics in medical education and patient care. *BMJ*, *340*, C863.

Grinter, R. E., Edwards, W. K., Newman, M. W., & Ducheneaut, N. (2005). The work to make a home network work. *European Conference on Computer-Supported Cooperative Work*, 469–488.

Gross, J. B., & Rosson, M. B. (2007). Looking for trouble: Understanding end-user security management. *Symposium on Computer–Human Interaction for the Management of Information Technology*, 10.

Gyselinck, V., & Tardieu, H. (1999). *The role of illustrations in text comprehension: What, when, for whom, and why?* Mahwah, NJ: Erlbaum.

Harp, S. F., & Mayer, R. E. (1998). How seductive details do their damage: A theory of cognitive interest in science learning. *Journal of Educational Psychology*, *90*, 414.

Hattie, J., & Timperley, H. (2007). The power of feedback. *Review of Educational Research*, *77*, 81–112.

Herley, C. (2009). So long, and no thanks for the externalities. *Proceedings of the 2009 New Security Paradigms Workshop*, 133–144.

Johnson-Laird, P. N., Girotto, V., & Legrenzi, P. (1998). Mental models: A gentle guide for outsiders. *Sistemi Intelligenti*, *9*, 33.

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A nutrition label for privacy. *Symposium on Usable Privacy and Security*, Article it.

Kephart, J. O., Sorkin, G. B., Arnold, W. C., Chess, D. M., Tesauro, G. J., White, S. R., & Watson, T. J. (1995). Biologically inspired defences against computer viruses. *International Joint Conference on Artificial Intelligence*, 985–996.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *APWG eCrime Summit*, 70–81.

Marchetto, M. A. (2014). *Cancer vixen: A true story*. New York, NY: Pantheon.

Mautone, P. D., & Mayer, R. E. (2001). Signaling as a cognitive guide in multimedia learning. *Journal of Educational Psychology*, *93*, 377–389.

Mayer, R. E. (2002). Multimedia learning. *Psychology of Learning & Motivation*, *41*, 85–139.

Mayer, R. E. (2005). Principles for reducing extraneous processing in multimedia learning: Coherence, signaling, redundancy, spatial contiguity, and temporal contiguity principles. In *The Cambridge handbook of multimedia learning* (pp. 183–200.) New York, NY: Cambridge University Press.

Mayer, R. E., & Anderson, R. B. (1992). The instructive animation: Helping students build connections between words and pictures in multimedia learning. *Journal of Educational Psychology*, *84*, 444–452.

Mayer, R. E., & Chandler, P. (2001). When learning is just a click away: Does simple user interaction foster deeper understanding of multimedia messages? *Journal of Educational Psychology*, *93*, 390–397.

Mayer, R. E., Dow, G. T., & Mayer, S. (2003). Multimedia learning in an interactive self-explaining environment: What works in the design of agent-based microworlds? *Journal of Educational Psychology*, *95*, 806–812.

McCloud, S. (2000). *Reinventing comics: How imagination and technology are revolutionizing an art form*. New York, NY: William Morrow.

Mekhail, C., Zhang-Kennedy, L., & Chiasson, S. (2014). Visualizations to teach about mobile online privacy. *Persuasive Technology, Adjunct Proceedings of the* 9th *International Conference on*. 43–45.

Mintz, J., & Aagaard, M. (2012). The application of persuasive technology to educational settings. *Educational Technology Research & Development*, *60*, 483–499.

Moon, J. A. (2013). *Reflection in learning and professional development: Theory and practice*. New York, NY: Routledge.

Moreno, R., Reislein, M., & Ozogul, G. (2010). Using virtual peers to guide visual attention during learning. *Journal of Media Psychology: Theories, Methods, and Applications*, *22*, 52–60.

Munroe, R. (2012). XKCD: A webcomic of romance, sarcasm, math, and language. Retrieved from http://xkcd.com/936/

Negrete, A., & Lartigue, C. (2004). Learning from education to communicate science as a good story. *Endeavour*, *28*, 120–124.

Nielsen, J. (2004, October). User education is not the answer to security problems. *Alertbox*.

Nijholt, A. (2002). Embodied agents: A new impetus to humor research. In *The April Fools' Day Workshop on Computational Humour* (Vol. 20). University of Twente, Twenty the Netherlands.

Paivio, A. (1991). Dual coding theory: Retrospect and current status. *Canadian Journal of Psychology*, *45*, 255–287.

Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic spreading in scale-free networks. *Physical Review Letters*, *86*, 3200–3203.

Pellegrino, J. W., Bransford, J. D., & Donovan, M. S. (1999). *How people learn: Bridging research and practice*. Washington, DC: National Academies Press.

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology*, *19*, 123–205.

Raja, F., Hawkey, K., Hsu, S., Wang, K., & Beznosov, K. (2011). A brick wall, a locked door, and a bandit: A physical security metaphor for firewall warnings. *Symposium on Usable Privacy and Security*.

Reeves, B., & Nass, C. (1996). *How people treat computers, television, and new media like real people and places*. CSLI Publications & Cambridge University Press.

Riley, S. (2006). Password security: What users know and what they actually do. *Usability News*, 8(1).

Rittle-Johnson, B., & Alibali, M. W. (1999). Conceptual and procedural knowledge of mathematics: Does one lead to the other? *Journal of Educational Psychology*, *91*, 175.

Sanok, D. J., Jr. (2005). An analysis of how antivirus methodologies are utilized in protecting computers from malicious code. In *Information security curriculum development* (pp. 142–144). New York, NY: ACM.

Schmidt, R. A., & Bjork, R. A. (1992). New conceptualizations of practice: Common principles in three paradigms suggest new concepts for training. *Psychological Science*, *3*, 207–217.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the 7th Symposium on Usable Privacy and Security*, 88–99.

Singhal, A., & Rogers, E. M. (2012). *Entertainment-education: A communication strategy for social change*. New York, NY: Routledge.

Srikwan, S., and Jakobsson, M. (2008). Using cartoons to teach Internet security. *Cryptologia*, *32*, 137–154.

Wade, S. E. (2001). Research on importance and interest: Implications for curriculum development and future research. *Educational Psychology Review*, *13*, 243–261.

Warkentin, M., Davis, K., & Bekkering, E. (2004). Introducing the check-off password system (COPS): An advancement in user authentication methods and information security. *Journal of Organizational & End-User Computing*, *16*, 41–58.

Wash, R. (2010). Folk models of home computer security. *Proceedings of the 6th Symposium on Usable Privacy and Security*, Article 11.

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: A first step towards effective password security in the real world. In *New Security Paradigms Workshop*, 137–143.

Whitten, A., Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*, 169–184.

Young, R. M. (1983). Surrogates and mappings: Two kinds of conceptual models for interactive devices. *Mental Models*, 35–52.

Zhang-Kennedy, L., & Chiasson, S. (2014). *Using comics to teach users about mobile online privacy* (Tech. Rep. TR-14-02). School of Computer Science, Carleton University, Ottawa, Canada.

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2013). Password advice shouldn't be boring: Visualizing password guessing attacks. *APWG eCrime Summit*, 1–10.

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2014). Stop clicking on "update later": Persuading users they need up-to-date antivirus protection. In *Persuasive technology, LNCS* (pp. 302–322). New York NY: Springer.

Zhang-Kennedy, L., Dorey, S., Mekhail, C., & Chiasson, S. (2014). *Secure comics*. Retrieved from http://www.versipass.com/edusec

ABOUT THE AUTHORS

Leah Zhang-Kennedy is a PhD candidate at Carleton University in the School of Computer Science, and a member of the CHORUS lab. She has a MASc in human–computer interaction from Carleton University. Her primary research interests are in the interdisciplinary areas of usable security, persuasive technology, and information visualization.

Sonia Chiasson is the Canada Research Chair in Human Oriented Computer Security and a faculty member in the School of Computer Science at Carleton University in Ottawa, Canada. Her main research interests are in usable security and privacy: the intersection between human–computer interaction and computer security and privacy.

Robert Biddle is a professor at Carleton University in Ottawa, appointed both to the School of Computer Science and the Institute of Cognitive Science. His research is primarily in human factors in cyber-security and software design, especially creating and evaluating innovative designs for computer security software and collaborative software development.

APPENDIX: USER STUDY MATERIALS

Interviews

Password Pre-test Interview

Past Experiences

1. Have you had previous experience with educational material regarding passwords or password guessing attacks? Can you describe the contents of the material?
    - Did you follow any of this advice? If yes, which parts? Otherwise, why not?
    - How does this advice help protect your account?
    -

2. Have your online account(s) been hacked in the past?

    If answered yes,
    - Can you describe the experience?
    - How did it make you feel?
    - Did you strengthen your passwords for that account afterwards?
    - Did you strengthen password for other accounts as a result of the experience?

    If answered no,
    - Do you think your current passwords are secure?
    - How likely do you think an attacker would break into one of your accounts? Why or why not.

Password Practice and Management

1. Do you have trouble remembering passwords? How do you manage your passwords for multiple accounts?

2. What is the typical strength of your passwords? Without revealing any of your passwords…
    - What are your criteria for creating passwords that you use frequently?
    - What are your criteria for creating very secure passwords?
    - When do you choose to create weak passwords? What influences your decision?

3. Do you currently use a strategy to help you create and remember your passwords? Can you describe this strategy without giving away your real passwords?

4. In a hypothetical scenario when your email account is hacked, what measures would you take to increase the security of your online account(s)?

Current Knowledge about Password Guessing Attacks

1. Would you say you have low, intermediate, or expert knowledge about password guessing attacks?

2. In the best of your knowledge, can you describe in detail methods hackers would use to guess your passwords?
    - What types of tools/resources would they need and use?
    - What are the various types of attacks they would deploy? How do the attacks work?
    - What types of weak passwords do you think are susceptible to password guessing attacks?

Password Post-test Interview

1. Did you update any of your passwords after last week's session?

    If answered yes,
    - For which type of accounts?
    - Did you use the passphrase strategy to create the new password?
    - If not, what strategy did you use?

    If answered no,
    - Can you give me a reason why, such as if you feel your current passwords are already secure?

2. Do you recall the methods hackers would use to guess people's passwords?

3. Can you describe in detail how each of the attacks you mentioned work?

Antivirus Pre-test Interview

Current practice

1. What computer operating system do you use?

2. Do you currently have an antivirus installed on your computer?

If answered yes,

- What type of antivirus do you have?
- Do you have more than one antivirus programs installed? (If yes, why do you have multiple antivirus programs?)
- How often do you update your antivirus?

If answered no,

- Can you give me reasons why not?

Current understanding of viruses

1. How would you define the term "virus"?

2. What is your understanding of viruses and malware? How are they similar or different?

3. Where do you think computer viruses' come from? What is their purpose?

4. Based on your understanding, can you describe how computer viruses could harm your computer?

5. Have you had previous experience with educational material regarding antivirus software? (It may include instructional manuals that came with your antivirus software)

- Can you describe the contents of the material?
- Did it help with your understanding of how your antivirus works?

Experience of getting infected

1. Have your computer ever been infected with viruses or other types of malware?

If answered yes,

- Can you describe the experience?
- How did it make you feel?
- Did you have an antivirus installed when this happened?

If answered yes,

- What did you think happened?

If answered no,

- Do you think if you had an antivirus, this could've been prevented?
- Did you install an antivirus software afterwards?

If answered no,

- How likely do you think your computer will be infected in the future? Why?

Current knowledge of how antivirus works

1. Are you confident in your knowledge of properly configuring and using antivirus software?

If answered no,

- If you are not confident, can you describe what aspect of the software you don't understand?

2. Can you describe how antivirus software detects viruses or other types of malware?

3. What is the difference between "clean", "quarantine", and "delete"? Which option do you use most often? Why?

4. Can you describe in detail the possible ways you could get infected with a virus?

5. In a hypothetical scenario that your computer is infected, what would you do?

Antivirus Post-test Interview

Ability to describe viruses and antivirus

1. Based on your understanding, can you describe what are viruses and malware?

2. Can you describe in detail the possible ways you could get infected with a virus?

3. Can you describe how antivirus works? Such as the ways an antivirus can detect viruses?

4. Did the lesson alter the way you currently manage the security on your computer? This includes actions such as installing an antivirus, updating your antivirus, or improved internet surfing behaviours?

5. Did the lesson improve your awareness of the need for antivirus?

Questions about the prototype

1. Did you gain new knowledge after viewing the prototype? If so which part?

2. Which part of the information did you find the most useful?

3. Is there any anything you would like to change/add?

Privacy Pre-test Interview

1. In your own words, can you describe some of the ways people can be tracked online?

2. Are you concerned about your online privacy? Can you explain why or why not?

If answered yes,

- what are some of the current strategies you use on your mobile device to protect your online privacy?

If answered no,

- to what extent are you willing to share information about you or others online through your mobile device?

3. What types of information do you share about your family or friends online through social networks or other means on your mobile device? These may include photos, videos, news feeds, or other types of information.

4. Do you feel you have an obligation to protect the privacy of others, such as family members or friends? Why or why not?

5. Can you describe what geotagging is? Even if you never heard of the term before, what do you think the term might mean?

Privacy Post-test Interview

1. Can you describe some of the ways people can be tracked online?

2. Are you concerned with your online privacy after learning about the topic? Can you explain why or why not?

3. Were you already practicing some of the actions to protect your online privacy as suggested in the comic before you viewed the material? If so, what are they?

4. Since viewing the educational material, did you take any new actions to protect your online privacy? If so, what were they?

5. Can you describe what you learned about how to protect yourself from being tracked online on your smartphone?

Questionnaires

(Note: To conserve space, open-ended questions are denoted with a short line after the questions.)

PASSWORD COMIC USER STUDY

Pretest Questionnaire

What is a typical length of your passwords?

☐ 8 characters or more
☐ 6-8 characters
☐ less than 5 characters
☐ depends on the minimum allowed by the site

What best describes the type of password you use most often?

☐ lower case letters
☐ lower and upper case letters
☐ lower, upper case letters, and numbers
☐ numbers only
☐ A combination of lower, upper case letters, numbers and special characters

How do you currently cope with remembering passwords for different accounts? Select all that apply.

☐ I reuse the same passwords
☐ I write them down
☐ I use a password manager
☐ I use easy to remember words
☐ I use information that is meaningful to me (dates, numbers, names, places, hobbies etc)
☐ I never have trouble remembering passwords
☐ Other, please describe _____

Have any one of your online accounts been comprised in the past?

☐ Yes ☐ No

How often do you visit password protected websites?

☐ Daily
☐ Several times a week
☐ Once a week
☐ Less than once a week

Do you consider yourself a visual learner?

☐ Yes ☐ No

In your own words, please describe ways a hacker would try to guess other people's passwords (password guessing attacks).

_____

Please rate your level of knowledge about how password guessing attacks work.

I know very little 1 2 3 4 5 6 7 8 9 10 I know a lot

Prototype Evaluation Questionnaire

Please answer the following questions for the visualization you have examined:

Based on your experience, the visualization is an effective method for teaching people about password guessing attacks.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

The visualization has helped me to gain useful knowledge about online password guessing attacks.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

The information was difficult to understand
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

The information was presented in an pleasant and appealing way.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

I prefer to learn from a plain text document about password guessing attacks than a graphical visualization.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

Visualizing the concept and process of how password guessing attacks happen is a good way for me to learn about the issue.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

The visualization was confusing.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

The visualization has taught me what I wanted to know.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

I will most likely remember what I have learned weeks later.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

The visualization has convinced me to use best practices for the passwords I create in the future.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

The visualization has taught me useful coping strategies of having strong and memorable passwords.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

Based on this information, I believe that my passwords are already secure.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

I will update some of my passwords as a result of this session.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

I would recommend this visualization to other people.
Strongly Disagree 1 2 3 4 5 6 7 8 9 10 Strongly Agree

Post-test Questionnaire

Using the advice from the lessons in the study, please create 2 new password samples that you think would be resistant to attacks but still would be able to remember. These should not be a password that you have used in the past, or are currently using. Please describe how you have created the passwords in detail.

Password 1: _____
Description: _____

Password 2: _____
Description: _____

Which of the following password(s) are weak? Select all that apply.

☐ 123456789 ☐ BB#s3034 ☐ MdEi@gd
☐ abc123 ☐ BlackCaT
☐ 1m1a1s1t1e1r

True or False:

It is safe to tell my password to a close friend.
T
F

Slang, dialect and jargons terms are safe to use because they are not dictionary words.
T
F

It is not safe to use word or number patterns (eg. “aaabbb”, “qwerty”, “zyxwvuts” etc).
T
F

I should not use personal information such as names (relatives, pets, etc.), or dates such as birthdays or anniversaries to create passwords.
T
F

Strong passwords contain a minimum length of (7) characters.
T
F

If I use non-English words, my passwords are safe from Dictionary Attacks
T
F

Good passwords appear to be random characters
T
F

Attackers target weak, easy to remember passwords
T
F

Antivirus Pre-test Interview

Current practice

1. What computer operating system do you use?

2. Do you currently have an antivirus installed on your computer?

If answered yes,

- What type of antivirus do you have?
- Do you have more than one antivirus programs installed? (If yes, why do you have multiple antivirus programs?)
- How often do you update your antivirus?

If answered no,

- Can you give me reasons why not?

Current understanding of viruses

1. How would you define the term "virus"?

2. What is your understanding of viruses and malware? How are they similar or different?

3. Where do you think computer viruses' come from? What is their purpose?

4. Based on your understanding, can you describe how computer viruses could harm your computer?

5. Have you had previous experience with educational material regarding antivirus software? (It may include instructional manuals that came with your antivirus software)

- Can you describe the contents of the material?
- Did it help with your understanding of how your antivirus works?

Experience of getting infected

1. Have your computer ever been infected with viruses or other types of malware?

If answered yes,

- Can you describe the experience?
- How did it make you feel?
- Did you have an antivirus installed when this happened?

If answered yes,

- What did you think happened?

If answered no,

- Do you think if you had an antivirus, this could've been prevented?
- Did you install an antivirus software afterwards?

If answered no,

- How likely do you think your computer will be infected in the future? Why?

Current knowledge of how antivirus works

1. Are you confident in your knowledge of properly configuring and using antivirus software?

If answered no,

- If you are not confident, can you describe what aspect of the software you don't understand?

2. Can you describe how antivirus software detects viruses or other types of malware?

3. What is the difference between "clean", "quarantine", and "delete"? Which option do you use most often? Why?

4. Can you describe in detail the possible ways you could get infected with a virus?

5. In a hypothetical scenario that your computer is infected, what would you do?

How concerned are you with regards to the security of your computer?
☐ Not at all concerned
☐ Not very concerned
☐ Somewhat concerned
☐ Very concerned

I feel antivirus software is too complicated to use
☐ Not at all complicated
☐ Not very complicated
☐ Somewhat complicated
☐ Very complicated

Please rank each operating system based on how secure you think they are. Place "1" beside the OS that you think is the most secure, 2 for the less secure, and 3 for the least secure.
__Macs
__Windows
__Linux

True or false:

Viruses can damage your computer's hardware.
T
F

Running multiple Anti-virus programs on the same computer is beneficial.
T
F

Having an Anti-virus is enough to be secure.
T
F

I can't get a virus if I'm not connected to the Internet.
T
F

I can't get a virus if I don't download anything.
T
F

I can't get a virus if I don't visit "shady" sites, such as porn, gambling, or file sharing websites.
T
F

Macs are far more secure than Windows.
T
F

Do you consider yourself a visual learner?
☐ Yes ☐ No

In your own words, describe what the following terms mean. Even if you are unsure, write down your best guesses.

What is a computer "virus"? _____

What is a "trojan"? _____

What is a computer “worm”? _____

What is “spyware”? _____

What is “adware”? _____

Please list and describe the ways people can get viruses?

_____

Can you describe how antivirus works to protect your computer? Such as the ways an antivirus can detect viruses?

_____

Prototype Evaluation Questionnaire

Please answer the following questions for the visualization you have examined:

Based on your experience, teaching about antivirus and virus prevention visually is an effective method to communicate about this topic.
Teaching visually is **not effective** 1 2 3 4 5 6 Teaching visually is **very effective**

Presenting the topic in a graphical way has made the information more pleasurable to read.
Not pleasant 1 2 3 4 5 6 Very pleasant

I have gained useful knowledge about antivirus software.
Gained no useful knowledge 1 2 3 4 5 6 Gained a lot of useful knowledge

I have gained useful knowledge about virus prevention.
Gained no useful knowledge 1 2 3 4 5 6 Gained a lot of useful knowledge

The visualization has improved my understanding of how antivirus works.
Did not improve my understanding 1 2 3 4 5 6 Strongly improved my understanding

The information was difficult to understand.
Not at all difficult 1 2 3 4 5 6 Very difficult

The graphics used to portray the topic was confusing.
Not at all confusing 1 2 3 4 5 6 Very confusing

I prefer to learn information from a plain text document instead.
Strongly dislike learning from plain text 1 2 3 4 5 6 Strongly prefer learning from plain text

I will most likely remember what I have learned weeks later.
I won’t remember 1 2 3 4 5 6 I will most likely remember

The visualization has convinced me to maintain an up-to-date antivirus.
Not at all convincing 1 2 3 4 5 6 Very convincing

The visualization has taught me useful tips on how to stay safe.
Not at all useful 1 2 3 4 5 6 Very useful

After learning about the topic, I believe I’m already doing all that I can with regards to computer security.

I'm not doing enough 1 2 3 4 5 6 I'm doing everything I can

I would spend time reading this visualization if I came across it elsewhere.
I wouldn't read it at all 1 2 3 4 5 6 I would read all of the visualization

I would recommend this visualization to other people.
Would not recommend 1 2 3 4 5 6 Strongly recommend

I would share the information I learned with other people.
Would not share it 1 2 3 4 5 6 Definitely share it

Did the metaphor help you to understand how computer viruses and antivirus work?
Not at all helpful 1 2 3 4 5 6 Very helpful

Please provide your feedback regarding the information provided (i.e. Was the information useful? Is there other additional information you would like to see?)

_____

Please provide your feedback regarding the graphics provided (i.e., Is it appealing? Is it appropriate for the topic? Did it help to enhance your understanding of the topic?)

_____

How would you interact with this information in a public setting, such as on a wall in a hallway, or perhaps at a bus or train station? (i.e., Would you read it? How long would you spend reading it?)

_____

Post-test Questionnaire

The following questions give you hypothetical scenarios. Describe what you would do in response to each situation. Please be as specific as possible:

Scenario A: You received an email from your bank in your primary email inbox. The subject line states "Your requested document". You opened the email and everything looks legitimate. The email contains your banks' logo and looks professional. The email explained that they are sending you a confidential document that you have requested online. You have recently logged in to your online bank account. The document is attached to the email reads "Customer_102554009.DOC.exe". How would you proceed?

_____

Scenario B: You found a USB key left on a desk in a conference room. You feel you should return it to the owner, but you are unsure whom the USB key belonged to. You decided to take a look at the contents to see if it can give you hint of who the owner is. How would you proceed?

_____

Scenario C: You received an email from a good friend of yours. The subject line says, "A cool video I found". You opened the mail and it reads, "Hey, I found this thought you might like it. ☺" Below the message there is a link to the video. How would you proceed?

_____

Can you describe how antivirus works to protect your computer? Such as the ways an antivirus can detect viruses?

_____

True or false: (Repeated questions from the pre-test questionnaire)

Viruses can damage your computer's hardware.
T
F

Running multiple Anti-virus programs on the same computer is beneficial.
T
F

Having an Anti-virus is enough to be secure.
T
F

I can't get a virus if I'm not connected to the Internet.
T
F

I can't get a virus if I don't download anything.
T
F

I can't get a virus if I don't visit "shady" sites, such as porn, gambling, or file sharing websites.
T
F

Macs are far more secure than Windows.
T
F

PRIVACY COMIC USER STUDY

Pretest Questionnaire

What is your smartphone operating system?
☐ Android
☐ IOS (iPhone operation system)
☐ Blackberry
☐ Windows Phone

How would you rate your smartphone experience level?
Novice 1 2 3 4 5 Expert

How would you rate your knowledge of the "smartphone geotagging"?
Not at all 1 2 3 4 5 Very well

Do you have any of these social media apps?
☐ Facebook
☐ Twitter
☐ Pinterest
☐ Instagram
☐ flickr
☐ ebay
☐ kijiji
☐ craigslist

Do you upload photos from your smartphone?
☐ Yes ☐ No

If answered "Yes" to the previous question then how often do you upload photos online from your smartphone?
☐ Daily
☐ Weekly
☐ Two to Three times a month
☐ Monthly
☐ Every six months
☐ Once a year

Do you upload photos from your smartphone to any of the following sites?
☐ Facebook
☐ Twitter
☐ Pinterest
☐ Instagram
☐ flickr
☐ ebay
☐ kijiji
☐ craigslist

How concerned are you with regards to your online privacy?
☐ Not at all concerned
☐ Not very concerned
☐ Somewhat concerned
☐ Very concerned

How concerned are you with regards to sharing your photo location data uploaded from your smartphone phone?
☐ Not at all concerned
☐ Not very concerned

☐ Somewhat concerned
☐ Very concerned

Do you consider yourself a visual learner?
☐ Yes ☐ No

In your own words, describe what the following terms mean. Even if you are unsure, write down your best guesses.

What is "Geolocation"? _____

What is a "Geotagging"? _____

What is a "EXIF" (Exchangeable Image FIle) data? _____

Please list and describe the ways people can be tracked online?
_____

True or false:
Using my phone to upload photos is safe.
T
F

Someone can track my location using the photos uploaded from my smartphone.
T
F

My location is used only for the GPS app on my smartphone.
T
F

Location information can be extracted from images uploaded online by default.
T
F

Prototype Evaluation Questionnaire

Please answer the following questions for the visualization you have examined:

After viewing the visual information how concerned are you with regards to your online privacy?
☐ Not at all concerned
☐ Not very concerned
☐ Somewhat concerned
☐ Very concerned

Based on your experience, teaching visually about smartphones geotagging and how to protect my privacy is an effective method to communicate about this topic.
Teaching visually is **not effective** 1 2 3 4 5 Teaching visually is **very effective**

Presenting the topic in a graphical way has made the information more pleasurable to read.
Not pleasant 1 2 3 4 5 Very pleasant

I have gained useful knowledge about smartphone geotagging.
Gained no useful knowledge 1 2 3 4 5 Gained a lot of useful knowledge

The visualization has improved my understanding of the smartphone geotagging.
Did not improve my understanding 1 2 3 4 5 Strongly improved my understanding

The information was difficult to understand
Not at all difficult 1 2 3 4 5 Very difficult

The graphics used to portray the topic was confusing.
Not at all confusing 1 2 3 4 5 Very confusing

I prefer to learn information from a plain text document instead.
Strongly dislike learning from plain text 1 2 3 4 5 Strongly prefer learning from plain text

I will most likely remember what I have learned weeks later.
I won't remember 1 2 3 4 5 I will most likely remember

The visualization has convinced me to change my picture settings on my smartphone.
Not at all convincing 1 2 3 4 5 Very convincing

The visualization has taught me useful tips on how to stay safe while uploading photos online from my phone.
Not at all useful 1 2 3 4 5 Very useful

After learning about the topic, I believe I'm already doing all that I can with regards to protecting my online privacy and safety.
I'm not doing enough 1 2 3 4 5 I'm doing everything I can

I would spend time reading this visualization if I came across it elsewhere.
I wouldn't read it at all 1 2 3 4 5 I would read all of the visualization

I would recommend this visualization to other people.
Would not recommend 1 2 3 4 5 Strongly recommend

I would share the information I learned with other people.
Would not share it 1 2 3 4 5 Definitely share it

Did the concepts used in the visualization help you understand how the smartphones geotagging work and how to protect yourself from being tracked online?
Not at all helpful 1 2 3 4 5 Very helpful

Please provide your feedback regarding the information provided (i.e., Was the information useful? Is there other additional information you would like to see?)
_____

Please provide your feedback regarding the graphics provided (i.e., Is it appealing? Is it appropriate for the topic? Did it help to enhance your understanding of the topic?)
_____

How would you interact with this information in a public setting, such as on a wall in a hallway, or perhaps at a bus or train station? (i.e., Would you read it? How long would you spend reading it?)
_____

Post-test Questionnaire

Question A:
Can you describe how to protect yourself from being tracked online on your smartphone?
_____

Question B:
Have you seen someone taking a photo of their family or friends recently using their smartphone? What did that make you feel regarding their online privacy?
_____

Question C:
Since viewing the educational material, did you take any actions to protect your online privacy?
If so, what were they?
_____

(Repeated questions from the pre-test questionnaire)
In your own words, describe what the following terms mean. Even if you are unsure, write down your best guesses.

What is "Geolocation"? _____
What is "Geotagging"? _____
What is "EXIF" (Exchangeable Image File) data? _____

Please list and describe the ways people can be tracked online?
_____

True or false:
(Repeated from the pre-test questionnaire)

Using my phone to upload photos is safe.
T
F

Someone can track my location using the photos uploaded from my smartphone.
T
F

My location is used only for the GPS app on my smartphone.
T
F

Location information can be extracted from images uploaded online by default.
T
F