Password Advice Shouldn't Be Boring: Visualizing Password Guessing Attacks

Leah Zhang-Kennedy
Human-Computer Interaction
Carleton University
Email: leah.zhang@carleton.ca

Sonia Chiasson
School of Computer Science
Carleton University
Email: chiasson@scs.carleton.ca

Robert Biddle
School of Computer Science
Carleton University
Email: robert_biddle@carleton.ca

***Abstract*—Users are susceptible to password guessing attacks when they create weak passwords. Despite an abundance of text-based password advice, it appears insufficient to help home users create strong memorable passwords. We propose that users would be empowered to make better password choices if they understood *how* password guessing attacks work through visual communication. We created three infographic posters and an online educational comic to help users to learn about the threats. We conducted two studies to assess their effectiveness. All four methods led to superior learning outcomes than the text-alone approach. Our pre-test questionnaires also highlighted that users' understanding of password guessing attacks is limited to a "target" mental model. One week after viewing our materials, the majority of users created strong sample passwords, and correctly described all three attacks: targeted, dictionary, and brute-force.**

I. Introduction

Knowledge-based authentication requires users to remember data created for authentication purposes. Text passwords and personal identification numbers (PINs) remain popular, despite the growing number of alternative graphical and textual schemes [1], [2]. Among many problems, text-based passwords are difficult to remember and are frequently forgotten [2], [3]. Some users cope by creating short, easy to remember passwords. Such weak passwords are vulnerable to dictionary, brute-force, and targeted guessing attacks [1], [2].

Although most users understand the importance of passwords, they continue to use poor password practices. There is a lack of resources available that explain the reasons behind the advice given and why these rules are important [4]. Herley [5] argues that users often reject security advice because it offers poor cost-benefit tradeoffs. Without an understanding of the threat, users cannot make robust decisions, and so intentionally choose to ignore good password advice if they believe that the benefits are moot.

Security education in general has a few well known challenges. Some experts argue that educational material does not have positive effects on user behaviour [6], and that security experts should not put the burden on users [7]. Security is a secondary task for most users and therefore, motivation to learn is low. Ideally, automated systems would protect users so they would not to need to worry about security. Realistically however, users will need some involvement in the foreseeable future, especially with choosing passwords. Despite an abundance of security advice for strengthening passwords, there is a lack of explanations of *why* users should follow the advice. We argue that when users are unaware or have incomplete conceptions of how password guessing attacks work, it can hinder their motivation and ability to create strong passwords. We feel a viable strategy is to raise awareness about the risks by teaching them how the attacks work. Since our target audience is novice home users, we chose a visual approach to deliver the teaching material. Research in education provides strong evidence that integrating visual and verbal strategies facilitate better learning than text-alone [8], [9], [10], especially when prior knowledge is low [10].

Keeping the challenges of security education in mind, we designed the teaching material to be light and enjoyable to learn. Our first three prototype designs are information graphics, often called *infographics*. These are visual representations of information, data, or knowledge, sometimes using metaphor to demonstrate an idea [11]. Well-designed infographics are easy and fast for people to read and understand, and help to visually break down complex concepts to aid comprehension. In the usable security field, researchers have explored information design in *A Nutrition Label for Privacy*, to improve the visual presentation and comprehensibility of privacy policies [12]. Our work differs in that it uses both text and images to convey information. Other works, like *Anti-Phishing Phil*, also use integrated graphical representations to convey security information to teach users about the risks [13].

Each of our three infographic prototypes uses a different metaphor for risk communication:*"users as targets," "passwords as locks,"* and *"passwords have lifespans"*. A fourth text-alone condition is used as a baseline to compare the effectiveness of our infographic prototypes. We tested the four conditions using a between-subject study with 55 participants.

Drawing from the concepts and results of the first study, we designed an interactive prototype in an online comic format, and conducted a second study. We suggest that presenting a serious security topic like password guessing attacks as a comic could help users to overcome the "intimidation factor." One security education effort exploring this approach is *Security Cartoon*, which uses short comic strips to explain various security risks [14]. Our prototype uses a similar approach, but incorporates interactivity, and delivers the information in a 14-page online comic book that offers a comprehensive overview of password guessing attacks, including coping strategies for how to create good passwords. We conducted a second user study with an additional 21 participants to assess the effectiveness. For interested readers, we have made the three infographics and the interactive comic available online [15].

II. Background

A. Overview of Online Password Guessing Attacks

In knowledge-based authentication, users are vulnerable to *online password guessing attacks* when they set up "weak" passwords that can be easily predicted by attackers. While *offline* guessing attacks are also possible (e.g., when attackers gain access to databases), our prototypes focus on the threat of online attacks. Online guessing attacks rely on interaction with the live system to determine if a guess is correct. After a series of unsuccessful password entry attempts, some sites will increase system response delay times or disable future attempts. Although these security mechanisms help to reduce password guessing, they also run the risk of locking out legitimate users who forget their passwords, and could enable a denial-of-service attack to purposely lock user accounts.

Users cope with the challenge of remembering passwords by making them short and easy to remember. They also reuse or create variations of the same password [16]. This puts users at risk of three types of online guessing attacks: exhaustive brute-force, dictionary, and targeted attacks. Tools are readily available online to help launch automated attacks. Sophisticated large-scale attacks may require expertise, but many attacks could easily be replicated by "script kiddies" with basic computer hacking skills.

Exhaustive Brute-force Attack: Brute-force attacks consist of guessing every possible password in a theoretical password space. All passwords can eventually be cracked by brute-force, but the size of the search space, time, and processing power can make it infeasible to crack strong passwords. Users' best defence against brute-force attacks is to create long, random-looking passwords containing alphanumeric and special characters to maximize the search space, thus minimizing attackers' chance to crack passwords using brute-force.

Dictionary Attack: Dictionary attacks use pre-compiled or computerized lists of high probability candidate passwords to guess the target password. Attackers exploit the fact that people like to use whole words or a string of words to create their passwords. Attackers also search for predictable patterns in user behavior supported by empirical data, such as commonly used character substitutions (e.g. @ for a), popular passwords (e.g. qwerty123), or predictable character distribution and composition (e.g., P@ssword1). Such pre-compiled lists are easily computed, available online, and shared amongst attackers [17].

Targeted Attack: In a targeted attack, the attackers try to obtain information about a specific user. It exploits the fact that people use personal information as their passwords to cope with memorability challenges [16]. For example, names, birth dates, hobbies, pets, or phone numbers are frequently used as passwords, and could be traced back to the user. This information is often readily available online, such as on social media sites, making it easy for attackers to gather user information even if they do not personally know their victims.

B. Mental Models, Passwords, and Metaphors

A *mental model* is a simplified internal concept of how something works in reality [18], [19], [4], [20]. People rely on the reasoning of their mental models to make predictions about the outcome of their actions in real life, including when they make security decisions. In password guessing attacks, users imagine hackers manually inputting guesses, and try to make passwords difficult for a human to guess [16]. For example, users rationalize "p1a1s1s1w1o1r1d" is strong because it consists of 15 alphanumeric characters, not knowing that it is highly susceptible to dictionary attacks. Many users also mistakenly believe that attackers only target "big fish" [4], and feel it is unlikely that they will be victims.

Several theories exist to explain how graphics help to build mental models. One is Paivio's dual coding theory [21] that suggests graphics and text are coded into memory differently. People process text in their phonetic working memory, while 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.

Theories in education literature show that the use of visual-verbal strategies in learning is more effective than text alone [8], [9], [22]. Scientific text books, for example, incorporate illustrations of theories and diagrams to support text explanations. Graphic design is applied to the page layout to make reading and finding information more intuitive and accessible. Information design is utilized to visually represent information or data in figures or diagrams so that it is readily understandable.

Research suggest that visuals depict the content of the text they accompany may facilitate the construction of a mental model [22]. In one study, researchers compared the effects of text-alone, text accompanied by visuals that only represented 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-alone. Secondly, visuals that show relationships between elements being described in the text are the most beneficial [22]. This suggests that visual information would be more effective if it offers additional insights by highlighting relationships between the objects being described in the text.

Another study offers further evidence that visual aids like diagrams can help to build mental models in the learning process. Cuevas et al. [23] compared learning of aviation lessons between text-alone, and text with diagrams. The study found that participants who learned through text and diagrams scored higher on tests than participants who viewed the text-alone tutorial. The authors concluded that diagrams presented with text in tutorials could improve learning efficiency, and consequently, lend further evidence of the benefits of visuals to help build mental models.

Mental models are often constructed from metaphors. From a cognitive linguistic point of view, a *metaphor* is defined as understanding a target domain in terms of other source domains [24]. Analogies and metaphors are often used to help users understand computer security risks such as explaining the concept of firewalls in terms of physical barriers [25]. A breadth of past research on the benefits of using metaphors exist in the HCI community, but Marcus [26] cautions that relying solely on metaphors could be limiting, and may not give users a complete mental model of the concepts. For example, when a physical security metaphor is used, the

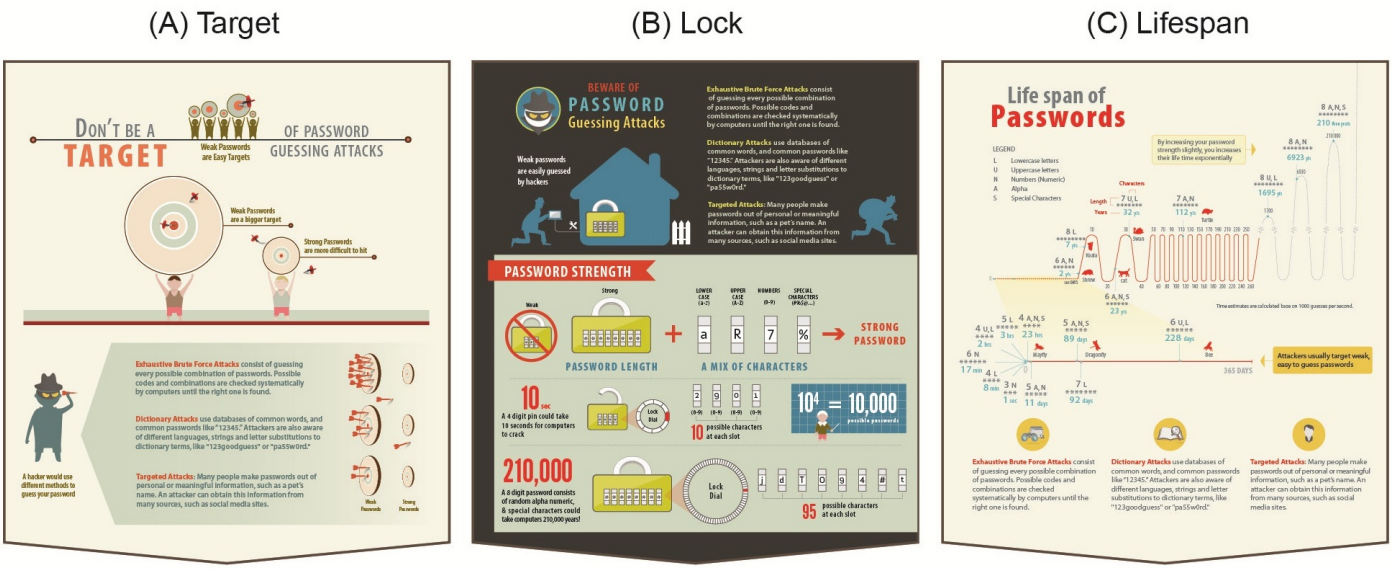

Fig. 1. The portion of our three infographics explaining how password guessing attacks work

concept could be limited by physical barriers, such as a wall, whereas Internet security is not [25]. When a metaphor is unfit to represent the target domain, it can cause users to make errors or to have a false sense of security. Metaphorical references can also vary over time across technological and cultural shifts [26]. However, the many benefits of using metaphors to communicate to users are highly attractive, and they have been widely used across disciplines. Computer security is no exception. Metaphors can increase the pace of learning, memorization, ease of use, and engagement because they leverage concepts that are familiar to users [26]. Marcus [26] argues that even though some metaphors cannot support a complete mental model, they can help to fill in the details from users' experience. Metaphorical references used in computer security software and user interface design include the concept of keys, locks, and walls.

Among security experts, there is discrepancy on the "correct" model that non-expert users should use to think about computer security [4]. Camp [19] proposed five possible models as a framework, which included physical security, medical risks, crime, warfare, and markets. The concepts were explored by Asghapour et al. [18] in a card sorting experiment, who found that there are significant differences in the metaphors based on users' expertise level. Wash [4] goes beyond prior research on assumptions of the usefulness of mental models, and investigated home users' actual mental models through interviews. Among other insights, he found that people with low-security knowledge do not understand how the process of "hacking" works or how hackers choose their victims.

III. Design of the Infographics

We selected three metaphors for our infographic prototypes, *Target*, *Lock*, and *Lifespan* (see Figure 1 A, B, and C, and available at [15]). They were selected because they represent a sample of metaphors commonly used in public communications media (ie., [27], [28], [29]), or in computer security literature (ie., [19], [25], [4]). The goal was to test the potential use of infographics in computer security compared to text-alone advice. To ensure that our findings are not specific to one design, we tested three different visualizations and assessed their effectiveness with a text-alone condition. The foundation of our approach is based on prior findings in education that supports the use of visual strategies to facilitate better learning compared to text-alone strategies [8], [9], [10]. We provided the same basic textual information on all three prototypes, first teaching about *how* guessing attacks work, by describing Brute-Force, Dictionary, and Targeted attacks. Secondly, we gave advice on creating and managing secure, memorable passwords. We used a metaphorical explanation unique to each infographic accompanied by graphic devices that most powerfully represented each metaphor. The amount of information included on each infographic varies from the least complex (*Target*), to moderately complex (*Lock*), to the most complex (*Lifespan*).

A. Selected Metaphors

Target Metaphor: "Don't be a Target" is a common tactic used in public safety and security communications media. For example, financial institutions like Royal Bank of Canada have used this approach to raise awareness about theft prevention in public settings [27]. Similarity, our *Target* concept promotes risk reduction. It communicates the message that weak passwords are easier to crack than strong passwords, therefore users with weak passwords are bigger targets for attackers. We illustrated the idea showing a hacker taking aim at dartboards of various sizes. Weak passwords are represented by large dartboards, and strong passwords by smaller ones, suggesting that weak password are more vulnerable to password guessing attacks because they are easy targets.

Lock Metaphor: The lock is a widely used security metaphor, due users' familiar understanding of the use of padlocks and keys in the physical world. Most security programs like anti-virus software, encryption software, and SSL certificates use the lock as a verbal and visual metaphor. In "A

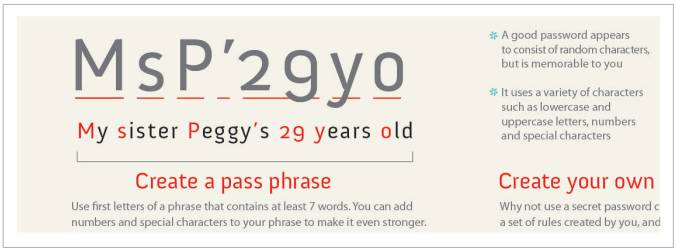

Fig. 2. A Portion of the password creation advice common to the Infographics

Brick Wall, a Locked Door, and a Bandit" [25], the concept of a locked door was tested as one of the physical security metaphor for firewall warnings. In our prototype, we illustrated the concept through burglary, which is one of non-expert users' mental models of hackers [4]. We use combination locks to visually depict password strength. Length is portrayed by the number of dials on the lock, while strength is portrayed by the size of each dial and how many characters it contains.

Lifespan Metaphor: In password policies, the "lifespan" of a password usually refers to the period of time before the password of a user account expires [29]. In our *Lifespan* prototype, we used a similar metaphor to refer to password cracking, where weak passwords that are easily guessed by attackers are represented by short lifespans, and strong passwords represented by exponentially longer lifespans. Based on our experience in authentication research, users often overestimate the length of time it takes hackers to crack passwords, because they assume most passwords would be difficult for humans to guess [16]. According to research conducted by Deloitte Canada, more than 90% of user-generated passwords would be vulnerable to hacking in 2013 [30]. The "life expectancy" of passwords can demonstrate how long it would take to crack [28]. We illustrated this concept on a line graph with passwords plotted over the time it takes to crack them. We overlaid animal icons on the graph to give users a reference to animal lifespans. Our calculations are based on the estimated theoretical password space of attacks with the computational power of delivering 1000 guesses per second.

B. Password Advice

There is a body of evidence indicating that typical computer users suffer from "password overload" [31]. In order to cope with remembering multiple passwords, users turn to unsafe practices such as password reuse. Standard password advice recommends that users create passwords that are unique to each account, at least 8 characters long, and consists of alphanumeric and special characters. Although this is ideal practice, cognitive challenges of remembering complex passwords mean users often ignore the advice and continue to use unsafe alternatives. We believe that in addition to giving users security advice, users should be given practical coping strategies for remembering their passwords. With this in mind, our password advice is based on the following considerations:

- Use a strategy like a passphrase
- Prioritize strong passwords for high-value accounts
- Use passwords that are long enough to be secure
- Choose passwords that are hard to guess

The infographics recommend that users create a personal strategy to help them remember passwords. An example of our recommendation is to use a passphrase such as *"My sister Peggy's 29 years old"* to make the password *"MsP'29yo"* (see Figure 2). Passwords created from a personalized passphrase can help to ease the memorability challenges of strong passwords [32], but they should be personalized rather than using popular slogans, song lyrics, or other sources that are easily accessible by attackers building attack dictionaries. We further recommended to users that they should prioritize strong passwords, and always create unique, strong passwords for high-value accounts like banking and email.

C. Infographics Approach

We used infographics to communicate to users about the risks of password guessing attacks. The purpose of the visualizations is to put technical language into a more easily understood form of communication. Infographics are capable of transforming abstract, complex, or otherwise difficult to understand concepts into intuitive, instant knowledge [33]. Compared to text documents, juxtapositions of text and image helps to increase ease of learning, comprehension, and engagement [34]. Our prototypes aim to deliver knowledge and ideas visually, so users can understand them quickly.

IV. Infographics User Study

A. Study Design

We performed a user study to test the effectiveness of our three infographics with corresponding metaphors to communicate to users about password guessing attacks, as well as a text-alone condition with no metaphor. As shown in Figure 1, the *Target* infographic focuses on the message that people who have weak passwords are bigger targets for hackers. The *Lock* infographic illustrates the threat through a physical security concept, burglary, where the malicious intention of hackers is explicitly shown. The *Lifespan* infographic makes the case that passwords have a life expectancy, based on how long it takes for hackers to crack them. The three concepts were presented to participants on posters measuring 36×42 inches each. The text-based condition was directly from Wikipedia's description of how "password cracking" works, and included a section giving advice on how to create passwords that are "easy to remember" but "hard to guess" [35]. We chose this source because the content is comparable to our infographics, written in plain language that is easy to understand. The source is a good example of publicly available information on the subject of password guessing attacks. We presented the information on letter size printouts, in 12pt font across 2 pages. We used a between-subject design to assess which condition best facilitates learning about the subject. Testing was conducted through one-on-one sessions with the experimenter. The components of the study are described below. In the following descriptions, "prototype" refers to the user-assigned infographic poster or text printout.

Pretest questionnaire: Before prototype viewing, we gave participants a pretest questionnaire to have a base understanding of their current knowledge of password guessing attacks, as well as their present password behaviours. This data enabled us to make meaningful comparisons with the follow-up questionnaire completed a week later.

Demographic questionnaire: The demographic questionnaire collected standard demographic information about the participants, such as age, gender, education, and background. Participants also provided information about whether they had prior training on password guessing attacks.

Prototype viewing: Participants were told that they could take as much time as they want to view the prototype. The infographics took on average 2 minutes to read, and the text condition took on average 6 minutes to read. The experimenter noted immediate reactions from the participant. Afterwards, we had a brief interview with each person to openly discuss their opinions of the prototype. Participants were encouraged to be honest and point out if there is anything difficult to understand or confusing about the concepts. The experimenter took notes of the comments made by the participant, and any misunderstandings of the metaphors, layouts, and other graphical elements on the infographics, and comments about the information presented in the text condition.

Post-viewing questionnaire: After prototype viewing, participants were asked to complete a questionnaire about the prototype. It had 14 Likert scale questions, on a scale of 1 (strongly disagree) to 10 (strongly agree). Participants were asked to give a rating to each statement about the prototype. We reversed the direction of a few questions to avoid bias.

One-week follow-up questionnaire: Participants were emailed a link to an online follow-up questionnaire one week after their scheduled lab session. The purpose of the questionnaire was to assess information retention. We intended to compare the results to the pretest questionnaire to evaluate if there are improvements in users' understanding of guessing attacks. We included one question verbatim from the pretest questionnaire, which asked users to describe in their own words how password guessing attacks work. This enabled us to compare answers from the two occasions. To assess if participants learned useful password strategies, we asked them to create two strong passwords and explain how they created them. Additionally, we created a knowledge quiz with 7 true and false questions and a multiple-choice question.

B. Participants

We recruited 55 participants from our university and randomly assigned 15 users to each infographic prototype, and 10 users to the text-alone condition. Participants were recruited through flyers posted on bulletin boards across campus, and through a faculty and staff subscribed email newsletter. Participants were given a $10 honorarium.

To obtain a small random sample of average home computer users, we did not specify a knowledge level of computer security to qualify for the study. According to our pretest questionnaire, our randomly selected participants' behaviour for creating and maintaining passwords are in line with past research on the challenges of text-based authentication schemes [16], [36]. 50 out of 55 (91%) of our participants said they have difficulty remembering passwords. Other strategies used by our participants also correspond to past findings [16], [36], including password reuse (32 participants, 58%), use of personal information in passwords (24 participants, 44%), and writing down passwords (11 participants, 20%). Ten participants said they use a password manager (18%), 4 (7%) use variations of the same password, and 2 (4%) make passwords based on account information.

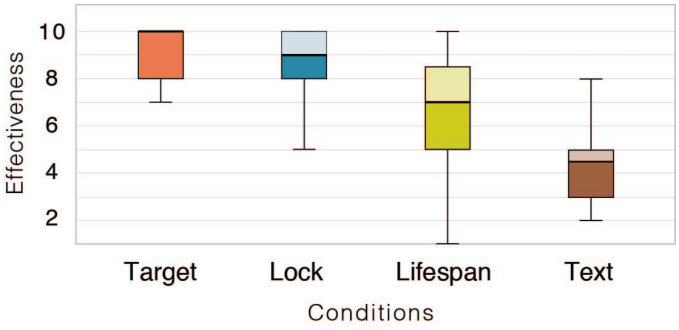

Fig. 3. Likert scale responses assessing the *effectiveness* of each prototype at conveying information (10 = most effective, 1 = least effective)

For current passwords, 47 (85%) participants reported using at least 6-8 alphanumeric characters or longer, and the remainder reported using insecure passwords that are less than five characters. Lastly, participants self-rated their knowledge about how password guessing attacks work. More than half (32 participants, 58%) self-declared to have very little or no idea about how the attacks work. Only three participants considered themselves to be very knowledgeable, and 20 (36%) participants said they have some ideas about how password guessing attacks work.

V. Infographics Study Results

A. Post-viewing questionnaire results and feedback

Participants evaluated their learning experience in a questionnaire immediately after viewing the material. In this paper, we focus on four particular comments from the questionnaire and user feedback: effectiveness of the visualization, usefulness of the information, persuasiveness to update current passwords, and memorability of the information. In what follows, all Likert scale data is presented positively for readability, with 10 = most positive and 1 = least positive. To analyze the Likert scale responses, we used the non-parametric Kruskal-Wallis and Mann-Whitney significance tests to evaluate whether any differences were apparent between the four conditions. In all cases, $p < 0.05$ is considered significant.

1) Effectiveness for learning: Most of our study participants (84%) said they are visual learners. Less experienced users perceived visualizing the process of password guessing attacks to be the most helpful. Although knowledgeable users felt that they did not learn new information, they agreed that visualization was a good way to teach novice users. Participants commented that they liked the graphics in *Target* and *Lock* infographics and thought the metaphors were effective. The *Lifespan* infographic was generally perceived to be the least effective because participants did not easily comprehend how the metaphor is associated with passwords.

Figure 3 shows the Likert scale responses for users' perceived effectiveness of each of the infographics compared to the text-alone condition at communicating about password guessing attacks. From the figure, it appears that the *Target* (median 10/10) and *Lock* (median 9/10) infographics are more effective than the *Lifespan* infographic (median 7/10), but

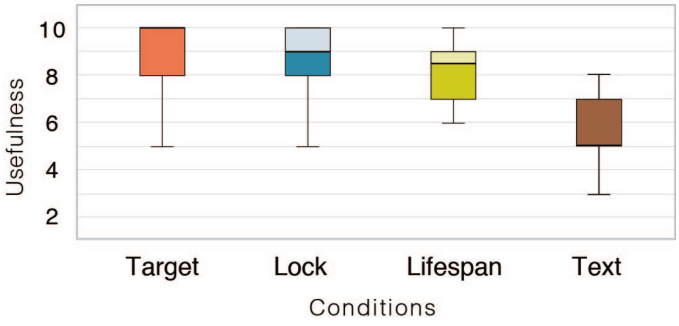

Fig. 4. Likert scale responses assessing the *usefulness* of the presented information (10 = most useful, 1 = least useful)

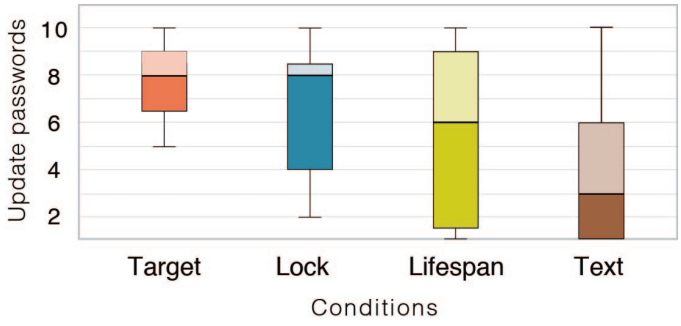

Fig. 5. Likert scale responses assessing the *likelihood to update current passwords* (10 = most likely, 1 = least likely)

all three infographics were considerably more effective than the text-alone condition (median 4.5/10). To confirm this result, a Kruskal-Wallis test showed a statistically significant difference between perceived effectiveness of the four conditions ($H(3) = 22.5$ with $p < 0.001$). To determine where the differences lay, Mann-Whitney tests with a Bonferroni-corrected p-value of ($p < 0.05/4 = 0.013$) were used. All three infographics are perceived to be more effective than the text-alone condition: *Target* ($U = 4.5, p < 0.001, r = -0.804$), *Lock* infographic ($U = 17, p = 0.001, r = -0.651$), and *Lifespan* ($U = 38, p = .038, r = -0.416$). Results suggest that infographics are perceived to be significantly more effective by users than text-alone information.

Based on verbal feedback, participants responded most positively to the *Target* infographic and found the *Lifespan* infographic most confusing. They found the concept of *Lifespan* to be too abstract for depicting password security. The information also takes a long time to read. Participants did not find password cracking times relatable to animal lifespans, since most people admit to have only vague ideas of how long animals live. Conversely, participants said that the *Target* poster took very little effort to read and understand. They felt that the concept is concise, "simple but informative." It is "easy to understand" and the communication of the key message is immediate. One participant said "even if I only have the time to look at the poster for a moment, I would at least walk away with the message that weak passwords are bigger targets for hackers." For the *Lock* infographic, participants said the visuals successfully captured the intentions of hackers, and depicted password strength well. In general, participants commented that they liked the graphics in the *Target* and *Lock* poster and thought the metaphors were effective. Participants thought average users would not read the text condition with interest on their own time. Some participants found the information "a lot to take in at once", "too technical", or "boring" to read.

2) Usefulness of the information: We received positive evaluations across all three infographics on the usefulness of the material. Novice users found the information particularly helpful. Knowledgeable users agreed that the information would be suitable to teach average home users. One participant said "I already know most of the information, but I think something like this would be great for my parents."

Responses to the Likert scale question about the usefulness of the information are available in Figure 4. Based on the responses, we could not determine which infographic participants found to be the most useful. Kruskal-Wallis test showed no statistically significant difference in the perceived usefulness of the information between the three infographics ($H(3) = 2.66$ with $p = 0.26$). However, when comparing the three infographics to text-based information, participants perceive the infographics to be significantly more useful ($H(3) = 16.53$ with $p = 0.001$). Mann-Whitney tests show the difference between each of the infographic when compared to the text-based condition are ($U = 9.5, p < 0.001, r = -0.745$) for *Target*, ($U = 23, p = 0.003, r = -0.586$) for *Lock*, and ($U = 21.5, p = 0.004, r = -0.579$) for *Lifespan*.

During open-ended feedback, participants commented that depicting password strength visually through various sizes of combination locks in the *Lock* infographic is very informative. They thought the graphic successfully "depicts what the hacker is trying to do". The *Target* infographic demonstrated password strength on a more abstract level, linking weak passwords with bigger targets. Although participants thought the message was straightforward and clear, they did not learn what constitutes password strength. Once again, participants found the *Lifespan* infographic visually complex, and took more effort to decipher the message. Participants also found that *Lifespan* is not a familiar concept to describe passwords. The text-based document took longer and more effort to read than all three infographics. Participants commented that it would be challenging for users to remember information from text descriptions.

3) Likelihood to update current passwords: Participants evaluated how likely they were to update their passwords after reading the material. We found a significant difference between the persuasiveness of the 4 conditions ($H(3) = 8.186, p = 0.042$). Mann-Whitney tests show that the *Target* and *Lock* infographics are significantly more persuasive than text-based information, ($U = 23.5, p = 0.004, r = -0.577$) and ($U = 36, p = 0.029, r = -0.4376$). We found no statistical difference between the *Lifespan* infographic and text-alone conditions ($U = 55.5, p = 0.272, r = -0.22$). Results of the Likert scale question are provided in Figure 5.

During the study session, we heard comments such as "I need to change my passwords", and "I will Google more about this". The evaluations show that *Target* and *Lock* infographics have greater potential to be more persuasive than text advice.

4) Memorability of information: Participants rated the likelihood of remembering learnt information. A Kruskal-Wallis test showed a statistically significant difference between the memorability of the four conditions ($H(3) = 20.369, p <$

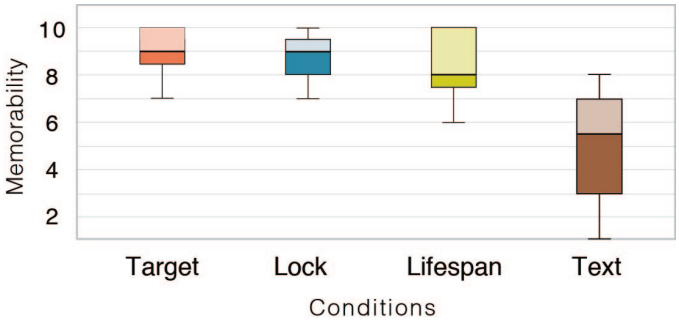

Fig. 6. Likert scale responses assessing *how likely participants will remember the information* (10 = most likely, 1 = least likely)

0.001). Mann-Whitney tests show that all three infographics are significantly more memorable than text-alone information, $(U = 3.5, p < 0.001, r = -0.161)$ for *Target*, $(U = 16.5, p = 0.001, r = -0.131)$ for *Lock*, and $(U = 12, p < 0.001, r = -0.142)$ for *Lifespan*. Results of the Likert scale question are provided in Figure 6. We assess the actual information retention of the four conditions in the following section.

B. Information retention

Prior to viewing the study material, we gave participants the opportunity to describe, in their own words, the ways in which hackers try to guess passwords. For comparison, this question was also asked verbatim one week later in an emailed online questionnaire. We received 52 completed responses in the pretest, and 54 completed responses one week later. Blank answers were considered as "I don't know."

We evaluated the answers based on correct descriptions of attacks, not based on participants' ability to define technical terms used in computer security. We assigned a corresponding meaning unit to each correct statement. For example, we attributed participants' answer to "targeted attack" when they wrote "birthdays, names of close family member, and pets", even though they did not identify the name of the attack.

In the pretest, our results show that password guessing attacks are primarily understood among home-users as targeted attacks. 41 (75%) out of the 55 participants were able to identify targeted attacks correctly, compared to 16 (29%) for brute-force attacks, and 15 (27%) for dictionary attacks (see Figure 7). Three users skipped the pretest question and were unable to provide answers.

We conducted McNemar tests to analyze participants' ability to describe password guessing attacks pretest compared to one week later. Refer to Table I for a summary of the results. We found a statistically significant increase in participants' ability to describe brute-force and dictionary attacks across "Target", "Lock", and "Lifespan" prototypes after one week. For the text-alone condition, we found no significance. We expected little or no increase in participants' ability to describe targeted attacks, since the pretest showed that most participants were already knowledgeable. The statistics were in line with our prediction, showing no statistically significant differences for any of the conditions for targeted attacks. Most participants already had no trouble explaining the idea of targeted attacks, and therefore user education has little influence. We further conclude that prior to viewing our infographics, participants have very limited knowledge of brute-force and dictionary attacks. All three infographics were able to raise awareness about these types of attacks and results show that participants were able to remember this information one week later (Figure 7).

Brute-Force Attack	Target	$(\chi 2(1) = 1.364, p = 0.008)$
	Lock	$(\chi 2(1) = 3.636, p = 0.063)$
	Lifespan	$(\chi 2(1) = 2.727, p = 0.031)$
	Text	$(\chi 2(1) = 5.625, p = 0.25)$
Dictionary Attack	Target	$(\chi 2(1) = 2.5, p = 0.031)$
	Lock	$(\chi 2(1) = 2.727, p = 0.031)$
	Lifespan	$(\chi 2(1) = 3.636, p = 0.063)$
	Text	$(\chi 2(1) = 4.286, p = 0.5)$
Targeted Attack	Target	$(\chi 2(1) = 10.313, p = 1)$
	Lock	$(\chi 2(1) = 15, p = 1)$
	Lifespan	$(\chi 2(1) = 15, p = 1)$
	Text	$(\chi 2(1) = 15, p = 1)$

TABLE I. SUMMARY OF MCNEMAR TEST COMPARING PARTICIPANTS' ABILITY TO DESCRIBE ATTACKS ON THE PRETEST AND ONE WEEK LATER

In the one-week follow-up questionnaire, we also asked participants to generate two unique passwords. We did not specify the length of the password or how to create them. We emphasized that the password should be something they can remember. 98% of the participants who viewed an infographic prototype created passwords that were at least 7 characters long. Most created strong passwords using a personally meaningful passphrase. None replicated our example *"My sister Peggy's 29 years old"* from the infographics, although three participants used a passphrase with references to a sister's name and age. 60% of participants who viewed the text condition used variations of passphrases to create passwords that are at least 7 characters long. Half of these participants created passphrases from whole words and sequential numbers. Other participants who viewed the text condition created passwords from combinations of people's names, strings of unrelated words, and non-English words combined with numbers and special characters.

VI. DESIGN OF THE INTERACTIVE COMIC

The infographic study highlighted that most users prefer to learn visually. Building on this idea, we explored whether a richer visual experience would enhance learning. We chose a comic book format as the teaching medium, and developed a 14-page online comic to educate users [15]. In addition to metaphors, we included stimuli to engage the user; for example, characters, narrative, humor, and interactivity. See Figure 8 for two example pages from the comic.

To the best of our knowledge, the only extensive exploration of the comic medium in computer security education is *Security Cartoon* [14]. It uses a series of comic strips to improve non-expert users' understanding of various risks [14]. Mainstream comics that have security advice include Dilbert [37] and XKCD [38]. Another related example is the online Google Chrome comic [39]. The 39-page instruction manual, delivered entirely in comic book format, teaches users about the inner workings of the Google Chrome browser, including key security concepts and benefits.

There are several advantages to the comic medium. First, it offers an enormous breadth of control to create customized content through a full range of visual symbols, and pairing of words and images to construct a convincing story [34].

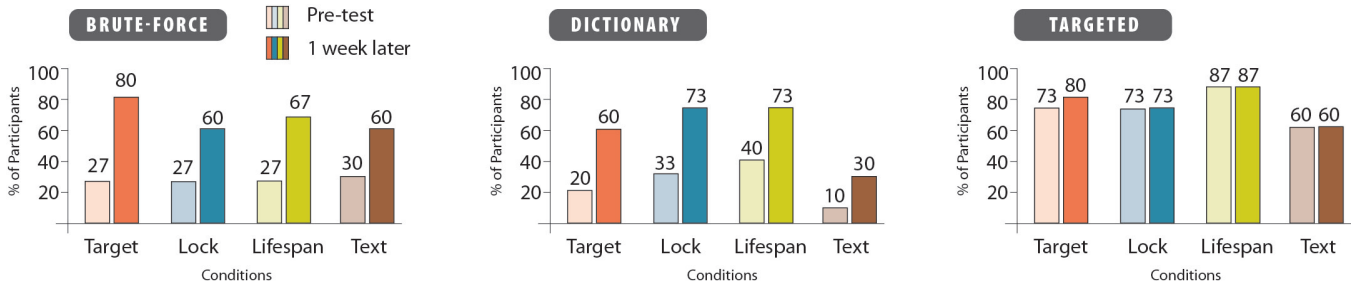

Fig. 7. Participants' ability to describe different types of attacks before and after viewing instructional material from the infographics

Fig. 8. Four individual panels from the online educational comic

Similar to infographics, the juxtaposition of images and text can help to break down complex concepts to aid in learning and comprehension. Secondly, comics are able to demonstrate complex processes progressively, through the use of stories and characters. Thirdly, it has a greater potential to reach non-technical Internet users than traditional educational efforts, because the reading format is lightweight, easy to consume, and appears less intimidating [14]. Comics can draw on the functions of humour to enhance communication of serious topics. Research in serious games has found that the use of humor can ease the social, emotional, and cognitive challenges of serious topics, and enrich the overall user experience [40]. Using humour can also enhance persuasion, and increase the comprehension and retention of information [40]. With this in mind, we incorporated humorous moments into the story when appropriate, as an effort to make the lessons light and pleasurable to learn.

We designed three main characters for the comic. *Jack* and *Nina* are agents of computer security. They solve computer security crimes and protect users against *Hack*. As the name implies, Hack's mysterious character embodies all computer security crimes. Jack and Nina take on the role of mentors who teach users about password guessing attacks. Characters are designed with a sense of humour to make them well-rounded, interesting, and believable [41].

As part of the online comic, we explored interactivity to offer users additional insights. For example, in the "Types of Attacks" section of the 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. The prototype uses original artwork drawn by us in Adobe Illustrator and programmed in Flash. Participants viewed the comic as a .swf file on a Macintosh laptop computer during the study. After study completion, we made the comic accessible to the public online [15].

VII. Interactive Comic User Study

For the comic study, we followed the same study protocol and used identical questionnaires as the infographic study, except the comic took longer to read. Most participants completed the comic in 8 to 10 minutes.

A. Participants

An additional 21 participants were recruited for the comic user study. To prevent overlap in the learning outcome, participants from the infographic study were excluded. 20 out of 21 participants reported having difficulties remembering passwords (95%). 11 (52%) participants practice password reuse, 8 (38%) use personal information, 7 (33%) write down passwords, 2 (10%) use a password manager, and 1 (5%) stores passwords in email.

In the pretest questionnaire, we received answers from 20 out of 21 participants who self-rated their current knowledge of password guessing attacks. 9 participants considered themselves to be somewhat knowledgeable, and another 10 believed they knew very little. Only one declared to be very knowledgeable. Nine participants reported that the typical length of the passwords they were using is 6 to 8 characters, and an additional eight said they were using passwords that are longer than 8 characters. Two participants said the length of their passwords depends on the minimum allowed by the site. Six participants said they are currently using alphanumeric characters, and an additional 11 are using alphanumeric with special characters. Only two participants reported regularly using weak passwords (e.g., numbers only).

VIII. Interactive Comic User Study Results

A. Post-viewing questionnaire results and feedback

Results of the three Likert scale questions, assessing the effectiveness, usefulness, likelihood to update current passwords, and perceived memorability of the information are presented in Figure 9. Overall, participants thought the comic was "enjoyable" and "fun". They thought people would identify with the characters and wanted to learn more about them. One

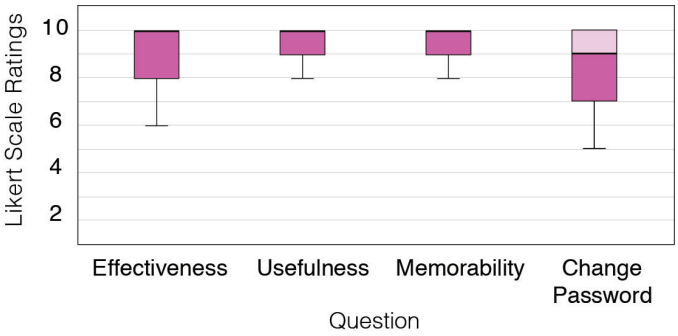

Fig. 9. Likert scale responses for the online comic (10 = most positive, 1 = least positive)

participant commented "I think it's great and some parts are really funny, I never thought that you could present security information like this before."

1) Effectiveness for learning: Teaching users about password guessing attacks through a comic book format was overall well received, with an average score of 9.2 for effectiveness. Visually, most participants found it to be appealing, and said it was enjoyable to read. A participant said "any time you have characters and a story, everything becomes more relatable." Several of the participants chuckled while reading the comic, which is a reassuring response that the use of humour was appreciated. A few participants were unsure of the reading direction at first, and offered layout suggestions for future iterations.

2) Usefulness of the advice: Users said they gained useful knowledge from reading the comic ($Mean = 9.2$). As explained by one participant, "I've heard some of this advice before, but never in a cohesive fashion like this." Many users were familiar with the advice concerning password strength, but gained practical information about password guessing attacks. Participants found the coping strategies to be particularity useful to help them remember passwords. They thought that prioritizing strong passwords for important accounts was practical advice, and that the passphrase is a "smart" technique.

3) Likelihood to update current passwords: Participants rated the likelihood to update their current password after viewing the comic. 80% participants said they would most likely update their current passwords. These participants thought that their current passwords are insecure, or moderately secure based on the information provided.

4) Memorability of information: The information provided in the comic was perceived to be strongly memorable ($Mean = 9.0$). Participants were surprised by the visualization of how quickly computers can crack weak passwords. Some said seeing how a single character can significantly increase the time to crack a password has motivated them to make their passwords longer in the future. Participants thought the tips and advice section to be particularly memorable, because it shows practical coping strategies that can be easily adopted.

B. Information Retention

Participants' ability to describe brute-force, dictionary, and targeted attacks was measured in the pretest and in the

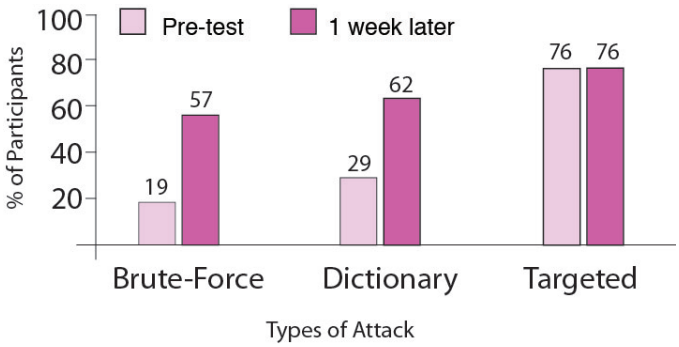

Fig. 10. Participants ability to describe different types of attacks before and after viewing instructional material

follow-up questionnaire (Figure 10). Again, most participants could describe targeted attacks on the pretest. On the follow-up questionnaire, most participants successfully described all three attacks.

We conducted a McNemar test to analyze participants' ability to describe the attacks pretest compared to one week later. Similar to the infographics study, we found a statistically significant increase in participants' ability to describe brute-force ($\chi 2(1) = 3.706, p = 0.004$) and dictionary attacks ($\chi 2(1) = 5.169, p = 0.008$) one week after viewing the prototypes. Participants were able to successfully describe targeted attacks on both occasions ($\chi 2(1) = 21, p = 1$) and the statistical test showed no difference.

IX. Discussion

Despite an abundance of password advice available to users, it seems insufficient to help users to create strong passwords. Ideally, users would not need to worry about security, but until security systems become completely automated, some user involvement is inevitable. As a first step, we believe motivating users to understand the process of security risks can help in harm reduction, and empower users to make informed security decisions. We choose to break down security concepts visually using the infographic and comic mediums to make the information easy to learn and enjoyable. In future work, we would like to partner with organizations and explore venues for deployment. At present, our goal is to first find the most appropriate ways of visualization the information. The next step would be to include lab measurements, such as users' reading time and eye-tracking, and see how this compares to the way users interact with the material in the real world through a field study.

It is evident from our pretest assessment of participants' password practices that mental models of password guessing attacks are primarily understood among novice home-users as targeted attacks. We believe this limited understanding can impact users' ability to create good passwords. In both studies, the majority of participants self-reported that they are using strong passwords outlined by standard password advice, such as creating passwords that are at least 7 characters long with uppercase, lowercase, numbers and special characters. There seem to be, however, confusion about what constitutes as a "good password". A participant commented "I think my passwords are strong by my own standards, but after reading [the comic] I don't feel they are very strong." Another participant admitted "things I thought were strong weren't. I use my name with a number at the end. I thought that was strong enough." This suggests that when users sometime choose weak passwords, they mistakenly think they are strong enough. Users justify passwords such as "Ashley10" as strong, based on the length and types of characters, not based on whether it is susceptible to password guessing attacks. We suggest that traditional password advice given to home users does not adequately explain why users should follow the advice or explain how the process of password cracking works, thus limiting users' ability to create strong passwords.

X. Conclusion

There is evidence from our study that home users have misconceptions about what constitutes a "good" password. Furthermore, our pretest questionnaire allowed us to gain valuable insights into home-users' mental model of password guessing attacks. Most users' knowledge is largely restricted to targeted attacks. We conclude that a lack of awareness of brute-force and dictionary attacks could impede users' ability to choose good passwords, and propose that more user education on *how* attacks work would be beneficial.

Our visualization prototypes are teaching tools intended to raise awareness about password guessing attacks, and provide users with practical information in pleasing, easy to understand formats. In our two-part study, we explored teaching users visually through infographic posters and an interactive comic. The visualization prototypes were perceived by participants to be more effective, useful, memorable, and persuasive than text-alone explanations. Participants who viewed either the infographics or comic were able to successfully describe brute-force, dictionary, and targeted attacks, identify weak passwords, and make strong sample passwords using strategies like a passphrase. However, the two teaching formats led to different user experiences. The infographics were quick to read and provided helpful actionable advice, while the comic provided users with an in-depth contextual understanding of the attacks and a richer user experience. We believe that both are valuable and effective teaching tools.

References

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: learning from the first twelve years," *ACM Computing Surveys*, vol. 44, no. 4, 2012.

[2] D. Florêncio and C. Herley, "Where do security policies come from," in *Proceedings of the 10th Symposium on Usable Privacy and Security*, 2010.

[3] D. Weirich and M. Sasse, "Pretty good persuasion: a first step towards effective password security in the real world," in *Proceedings of the New Security Paradigms Workshop (NSPW)*. ACM, 2001, pp. 137–143.

[4] R. Wash, "Folk models of home computer security," in *Proceedings of the 6th Symposium on Usable Privacy and Security*. ACM, 2010.

[5] C. Herley, "So long, and no thanks for the externalities," in *New Security Paradigms Workshop (NSPW)*, 2009.

[6] S. Görling, "The myth of user education," in *Virus Bulletin Conference*, vol. 11, 2006, p. 13.

[7] J. Nielsen, "User education is not the answer to security problems," *Alertbox, October*, 2004.

[8] R. Mayer, W. Bove, A. Bryman, R. Mars, and L. Tapangco, "When less is more: Meaningful learning from visual and verbal summaries of science textbook lessons." *Journal of educational psychology*, vol. 88, no. 1, p. 64, 1996.

[9] L. Chanlin, "The effects of verbal elaboration and visual elaboration on student learning." *International Journal of Instructional Media*, vol. 24, no. 4, pp. 333–39, 1997.

[10] ——, "Animation to teach students of different knowledge levels." *Journal of Instructional Psychology*, 1998.

[11] J. Risch, "On the role of metaphor in information visualization," *arXiv preprint arXiv:0809.0884*, 2008.

[12] P. Kelley, J. Bresee, L. Cranor, and R. Reeder, "A nutrition label for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, 2009, p. 4.

[13] P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, p. 7, 2010.

[14] S. Srikwan and M. Jakobsson, "Using cartoons to teach internet security," *Cryptologia*, vol. 32, no. 2, pp. 137–154, 2008.

[15] Zhang-Kennedy, L. and Chiasson, S. and Biddle, R., "Versipass," `http://www.versipass.com/edusec/`.

[16] S. Gaw and E. Felten, "Password management strategies for online accounts," in *Proceedings of the 2nd Symposium on Usable Privacy and Security*. ACM, 2006, pp. 44–55.

[17] M. Devillers, "Analyzing password strength," *Radboud University Nijmegen, Tech. Rep*, 2010.

[18] F. Asgharpour, D. Liu, and L. Camp, "Mental models of security risks," *Financial Cryptography and Data Security*, pp. 367–377, 2007.

[19] L. Camp, "Mental models of privacy and security," *Technology and Society Magazine, IEEE*, vol. 28, no. 3, pp. 37–46, 2009.

[20] R. Wash and E. Rader, "Influencing mental models of security: A research agenda," in *Proceedings of the New Security Paradigms Workshop (NSPW)*. ACM, 2011, pp. 57–66.

[21] A. Paivio, "Dual coding theory: Retrospect and current status." *Canadian Journal of Psychology/Revue canadienne de psychologie*, vol. 45, no. 3, p. 255, 1991.

[22] V. Gyselinck and H. Tardieu, "The role of illustrations in text comprehension: What, when, for whom, and why?" 1999.

[23] H. M. Cuevas, S. M. Fiore, and R. L. Oser, "Scaffolding cognitive and metacognitive processes in low verbal ability learners: Use of diagrams in computer-based training environments," *Instructional Science*, vol. 30, no. 6, pp. 433–464, 2002.

[24] G. Lakoff and M. Johnson, "The metaphorical structure of the human conceptual system," *Cognitive Science*, vol. 4, no. 2, pp. 195–208, 2010.

[25] F. Raja, K. Hawkey, S. Hsu, K. Wang, and K. Beznosov, "A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings," in *Proceedings of the 7th Symposium on Usable Privacy and Security*. ACM, 2011.

[26] A. Marcus, "Metaphors and user interfaces in the 21st century," *interactions*, vol. 9, no. 2, pp. 7–10, 2002.

[27] Royal Bank of Canada, "Don't be a Target," Accessed March 2013, `http://www.rbc.com/privacysecurity/ca/popup-dont-be-a-target.html`.

[28] Fontana, J., "Password life expectancy down to seconds," Accessed March 2013, `http://www.zdnet.com/password-life-expectancy-down-to-seconds-7000009851`.

[29] Microsoft Developer Network, "Password Policy," Accessed March 2013, `http://msdn.microsoft.com/en-us/library/ms161959.aspx`.

[30] Deloitte, "P@$$1234: the end of strong password-only security," Accessed March 2013, `http://deloitte.com/view/en_GX/global/industries/ technologymedia-telecommunications/tmt-predictions-2013`.

[31] G. Notoatmodjo and C. Thomborson, "Passwords and perceptions," in *Proceedings of the 7th Australasian Conference on Information Security-Volume 98*. Australian Computer Society, Inc., 2009, pp. 71–78.

[32] M. Keith, B. Shao, and P. Steinbart, "A behavioral analysis of passphrase design and effectiveness," *Journal of the Association for Information Systems*, vol. 10, no. 2, pp. 63–89, 2009.

[33] M. Smiciklas, *The Power of Infographics: Using Pictures to Communicate and Connect With Your Audiences*. Que Publishing, 2012.

[34] S. McCloud, *Reinventing comics: How imagination and technology are revolutionizing an art form*. William Morrow Paperbacks, 2000.

[35] Wikipedia, "Password Cracking," Accessed March 2013, `http://en.wikipedia.org/wiki/Password_cracking`.

[36] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *Security & Privacy, IEEE*, vol. 2, no. 5, pp. 25–31, 2004.

[37] Adams, S., "Dilbert," Accessed December 2012, `http://search.dilbert.com/comic/Security`.

[38] Munroe, R., "XKCD: a webcomic of romance, sarcasm, math, and language," Accessed December 2012, `http://xkcd.com/936/`.

[39] Google Chrome Team, McCloud, S., "Google Chrome," Accessed June 2012, `http://www.google.com/googlebooks/chrome`.

[40] C. Dormann and R. Biddle, "A review of humor for computer games: Play, laugh and more," *Simulation & gaming*, vol. 40, no. 6, pp. 802–824, 2009.

[41] A. Nijholt, "Embodied agents: A new impetus to humor research," in *The April Fools' Day Workshop on Computational Humour*, ser. Twente Workshops on Language Technology, vol. 20. University of Twente, 2002.