Stop clicking on "update later": Persuading users they need up-to-date antivirus protection

Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle

Carleton University, Ottawa, Canada
leah.zhang@carleton.ca, chiasson@scs.carleton.ca, robert_biddle@carleton.ca

Abstract. Online security advice aims to persuade users to behave securely, but appears to have limited effects at changing behaviour. We propose security advice targeted at end-users should employ visual rhetoric to form an effective, memorable, and persuasive method of communication. We present the design and evaluation of infographics and an online interactive comic developed to persuade users to update their antivirus software. Results show superior learning and behavioural outcomes compared to mainstream text-only security advice.

Keywords: Antivirus, Persuasive Visualization, Usable Security

1 Introduction

While automated detection systems should be used as the first line of defence against security threats, user education offers a complementary approach to secure computer systems. Online security advice is common and abundant, but typically has little persuasiveness to change behaviour. Persuasive strategies embedded in authentication mechanisms were found to be effective at motivating users to create stronger passwords [11], but little research has investigated whether theories in Persuasive Technology (PT) could be successfully applied to instructional interventions in security.

In this paper, we show that security advice is more persuasive (both perceived and actual) for end-users if it employs visual rhetorical devices that aid in mental model building of secure behaviour. A *mental model* is users' simplified internal concept of how something works in reality [6], and is used in decision making and problem solving. We present the design strategies and prototypes composed of infographics and an online interactive comic that motivate the correct use of antivirus protection. First, we frame the problem in context of computer security and explain how PT strategies in the design can be used to address the challenges. Secondly, we report our user studies that assess the perceived persuasiveness of our prototypes, and the actual persuasiveness at changing users' antivirus management behaviour after one week. Results show that our prototypes provide superior learning outcomes than mainstream text-only security advice. Participants showed high retention, reported an enjoyable learning experience, and demonstrated changes in antivirus management behaviour.

Authors' copy. Published in PERSUASIVE 2014, Springer LNCS

2 Challenges of Motivating Antivirus Protection

Fogg's *Functional Triad* identifies *media* as one way that PT can operate to change behaviour [9] — to persuade people by allowing them to explore cause-and-effect relationships, or to provide them with vicarious experiences that motivate or help people to rehearse a behaviour. Work in usable security to address phishing threats (e.g., [14]), privacy policies (e.g., [13]), and data leaks on smartphones (e.g., [2]) has exemplified that media can have positive effects on motivating secure behaviour. Other work successfully applied PT theory in authentication systems to persuade users to create stronger passwords (e.g., [4,11]). The only theoretical exploration of comics in computer security is Security Cartoon [20] that uses short comic strips to explain various security risks. The main theoretical findings suggest that presenting serious topics like computer security as a comic could help users to overcome the "intimidation factor" associated with learning. However, the work does not explore the potential interactive components of web comics, which may help to enhance learning and engagement.

We focus our discussion on the effective use of media to persuade users to maintain an up-to date antivirus software. Antivirus (also known as "AV") prevents, detects, and removes malicious software programs (i.e., malware). *Signature-based* antivirus software scans the contents of the program against a library of known virus signatures, and is effective against existing viruses that are contained in the antivirus database. *Heuristic-based* antivirus software examines programs based on a set of guidelines and rules identifying suspicious behaviour and characteristics. This method of detection is effective against variants of known viruses, and may also detect some *zero-day* viruses [1].

Although PT theory is generalizable in many domains, some unique challenges in computer security require special consideration [11]. We define the main challenges and frame them in terms of antivirus protection:

1) Security is a secondary task [23] that users may choose to bypass if it impedes the completion of a more relevant primary task: Running regular updates and renewing antivirus software subscriptions is a preventative measure that may not directly relate to any specific threat. Most antivirus software checks for updates automatically and sends users reminders, but installing updates, renewing the software, and payment may still require users' attention. Unfortunately, users may ignore prompts and reminders to updates.

2) Security systems are often too complex and abstract for end-users to form proper mental models and use accurately [5]: Most antivirus software automates the virus detection process "behind the scenes" without user interaction. Although automated systems can unburden users from making security decisions, such systems lack vigilant human oversight and therefore cannot handle exceptions and novel patterns. When automation fails, users may be left unprepared to analyze available information, find causality, and take actions to enable system recovery.

[1] Unknown malware for which specific antivirus signatures are not yet available.

3 Visual Rhetoric as a Facilitator for Learning

To address the challenges, we aim to use PT as media to persuade users to maintain an up-to-date antivirus software. Specifically, we employ visual rhetoric [18] in security information to construct arguments. Visual rhetoric can be thought of as the analysis of graphical devices using traditional vocabulary from rhetorical theory, such as pathos, logos, and ethos. The construction of images in advertising to make a point or argument is a example of visual rhetoric in practice.

The use of visual rhetoric could work in three ways: 1) foster good mental models; 2) construct arguments to persuade the need for security; 3) overcome the "intimidation factor" associated with security learning. The first two strategies correspond to the traditional mode of Greek rhetoric, logos, and the third strategy to pathos. Images appeal to the users' emotions and help to give reason to our argument of *why* they should follow the advice.

Fogg's behaviour model (FBM) emphasizes that motivation alone may not get people to perform a behaviour if they do not have the ability [10]. When users are unaware or have incomplete mental models of security threats, they may underestimate the risks involved. Furthermore, if security information appears overly technical, time consuming, or uninteresting, users may have low motivation to learn. The FBM model implies that making a behaviour easy to do may be a viable approach to increase behaviour performance [10].

We argue that learning from infographics and interactive comics are relatively easier than other alternatives due to their graphical nature. Infographics are visual representations of information, data, or knowledge [19]. Comics are a form of "sequential art" [8] that use a series of images and text to tell a story. Webcomics with interactivity are capable of persuading users through visual and *procedural rhetoric* [3] by incorporating interactive elements. The media acts as a "facilitator" [10] to signal users that learning about security is easy. Furthermore, infographics and interactive comics have low production costs, and are quicker to produce than film, animation, or games. These characteristics are important as new materials need to be produced rapidly to meet evolving security threats.

4 Prototype Design

The design of our prototypes was guided by the 5-phase ADDIE (Analyze, Design, Develop, Implement, and Evaluate) instructional design model [12]. The *analysis* phase consists of gathering and consolidating information. The *design* phase identifies a "blueprint" of activities and materials required. In the *development* phase, the content and the design are assembled and iterated. Next, the *implementation* phase ensures all material is fully functional before it is revealed to audience. Since ADDIE is an iterative process, evaluation is involved at every stage and may be formal (e.g., pilot study) or informal (e.g., feedback). A final *evaluation* is involved after the *implementation* phase to monitor learning outcomes after a particular time has passed.

Infographic Design: We created two infographics. In the *analysis* phase of the ADDIE process, we reviewed popular online antivirus protection resources as well as antivirus and risk communication literature in computer security. We chose to provide users with practical actionable advice on how to stay safe — explaining the basics of how antivirus software works, why regular updates are necessary, and common myths surrounding malware protection. We selected two metaphors from well-known concepts in security literature, *Surveillance* and *Medical*, to help users build mental models of antivirus protection. *Surveillance* is inspired by physical security metaphors (e.g., [17]), and *Medical* is inspired by biological models used to predict computer virus outbreaks (e.g., [16]). We iterated the two concepts during the *design* and *development* phase and presented sketches to members of our lab for feedback. Each concept was implemented as a infographic (see Figure 1A and 1B) to test its effectiveness against existing text-only advice with no visuals and metaphors. Evaluating two different infographics help to ensure that our findings are not specific to one design. We provided identical textual information on both infographics, first describing how antivirus software works, followed by a tips and myths section.

Comic Design: We expanded the conceptual models included in the infographic designs and explored Fogg's definition of media as interactive technologies that can use both interactivity and narrative to create persuasive experiences that support rehearsing a behaviour or exploring casual relationships [9]. We designed and developed a 10-page online interactive comic that showcases these characteristics. The full comic is available online at [22].

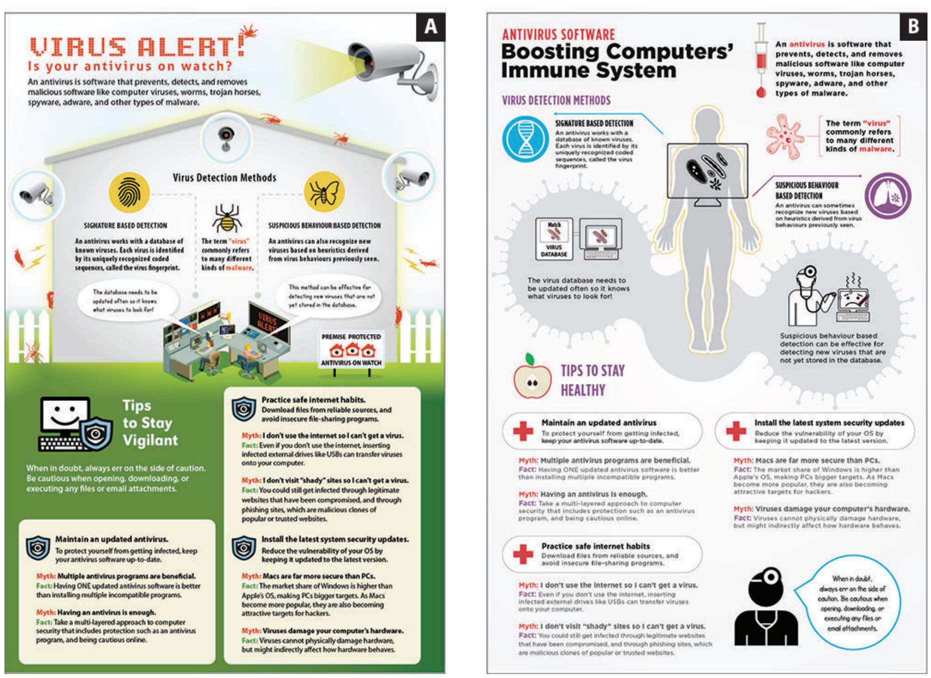

Fig. 1. Infographic prototypes. A) Surveillance. B) Medical.

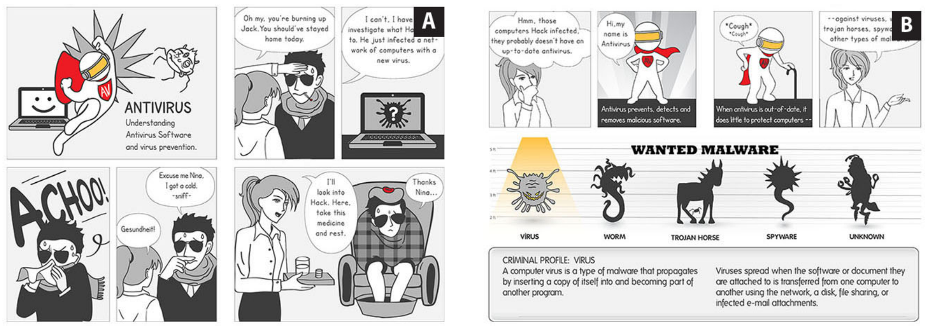

Fig. 2. Individual panels from the comic. A) pg 2 of 10. B) pg 3 of 10.

The characters *Jack* and *Nina* are agents of computer security. They solve computer security crimes and protect users against *Hack*, whose mysterious demeanour is symbolic of all computer security crimes. Jack and Nina take on the role of mentors who teach users about antivirus protection. Conceptually, we extended the medical theme that was found to be successful in the infographic study (discussed in section 6). For example, we subtly allude to the medical theme at the start of the comic, when agent Jack catches a cold, while Hack infects a network of computers with a computer virus (See Figure 2A). The medical concept was used repetitively throughout the comic to strengthen the message. We explored interactivity to offer users additional insights and reinforce learning through exploration. For example, in the "types of malware" section, users can rollover malware silhouettes to learn more about them (See Figure 2B). At the end of the comic, users have the option to play two "test your knowledge" mini games to review and practice important concepts that were taught in the comic.

The prototypes use original artwork conceptualized and drawn by us. We first created written scripts of the narrative at the *design* phase, created the characters, and produced storyboards. During the *development* phase, the storyboards were scanned and imported into Adobe Photoshop and overlaid with text dialogues, tested, and iterated. Each screen was then hand drawn and coloured with a graphic tablet in Adobe Illustrator and implemented in Adobe Flash.

5 Methodology and Research Design

We conducted two ethics approved, between-subject, one-on-one user studies to evaluate the infographic and comic prototypes. 40 university students and staff with diverse academic backgrounds participated in the infographic study, and an additional 16 students and staff participated in the comic study.

Infographic study: Participants were randomly assigned to one of three study conditions: *"Surveillance"* infographic ($n = 15$), *"Medical"* infographic ($n = 15$), and a text-only condition that we will refer to as *"Text"* ($n = 10$). Due to randomized assignment, the participants' self-reported experiences with antivirus software were skewed between conditions. Mean self-ratings on a 6 point scale (1 - novice, 6 - expert) were 3.4 for *Surveillance*, 2.7 for *Medical*, and 2 for *Text*. Each infographic was presented on a 20 by 30 inch poster, and the text condition was presented on a letter size printout in 12pt font. We searched for the best written publicly available online advice, and determined that the most relevant content came from Wikipedia [24], Logical PC Solutions [15] and a security blog [21]. The material was assembled to correspond to the written content of our infographics. We kept all basic text formatting such as headings, indents, and paragraphs to maintain good readability.

Comic study: After the infographic results were analyzed, we designed a interactive comic and conducted a second study. The infographic study provided valuable insights on the types of content and stimulus that should be included in the interactive comic. The purpose of the second study is to investigate whether our comic with a richer interactive user experience helps to further enhance the learning process and effect positive behavioural change. The static infographics were quick to read and provided helpful actionable advice, while the comic uses persuasive technology that incorporates interactivity, a narrative, and mini-games. During the study, participants viewed the comic as a .swf file on a Macintosh laptop computer. The average self-rating participants gave on a scale of 1 to 6 (1 - novice, 6 - expert) for prior experience with antivirus software was 2.

Instruments for both studies: Participants first completed a *demographic questionnaire* to collect information like age, gender, education, and background, then a *pretest questionnaire* for evaluating current knowledge and behaviour. We inquired about antivirus management, malware, and how antivirus software works. Next, participants were given as much time as they needed to view the prototype. Average viewing times were 2 minutes per infographic, 4 minutes for *text*, and between 5 to 8 minutes for the comic. Afterwards, participants were asked to openly comment on their experience and to point out any difficulties they had with the prototype. To elicit further feedback, participants completed a *prototype evaluation questionnaire* based on Likert scales for measuring the perceived effectiveness and usefulness of the prototypes. In classical models of attitude change, messages are presented, received, processed, and if successful, users' attitudes shift towards the advocated position [7]. However, the measurement of behavioural intentions is not always a good predictor of behaviour [1]. To minimize this intention-behaviour gap, we distributed a *followup questionnaire* one week later to assess information retention and behaviour change.

We used non-parametric Kruskal-Wallis and Mann-Whitney U significance tests to analyze participants' Likert scale evaluations. McNemar significance tests were used to assess whether knowledge about the antivirus protection significantly changed before and one week after the experiment. In all cases, $p < 0.05$ is considered significant. In the results, all Likert-scale data is presented positively for readability, with $6 =$ most positive and $1 =$ least positive.

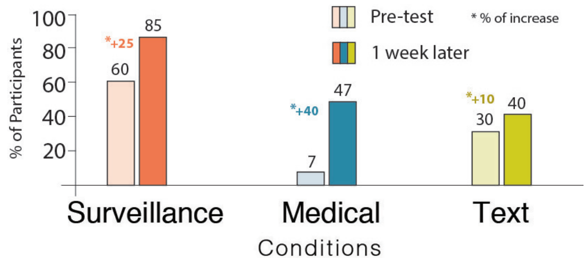

Fig. 3. Participants' ability to describe how antivirus software works before and one week after viewing the infographics and text material

6 Infographic Study Results

Information retention: In the *pretest questionnaire*, 40 participants described how antivirus software works to detect malware. The goal was not to test participants' ability to describe technical aspects of detection methods, but to identify their basic mental model of the detection process. We tabulated number of correct responses. Random assignment of participants to conditions led to a varied distribution of correct responses across conditions. 60% (9/15 participants) of correct responses were received for *Surveillance*, 7% (1/15 participants) for *Medical*, and 30% (3/10 participants) for *Text*. The same question was asked verbatim one week later in the *followup questionnaire*, where we received 38 completed questionnaires. We tabulated correct responses, then compared these to the *pretest questionnaire*, which was completed prior to viewing the educational materials (Figure 3 summarizes the results). McNemar significance tests were used to analyze the number of correct responses between the two questionnaires. Statistically, there was a significant increase in knowledge for the *Medical* condition ($\chi 2(1) = 1.224, p = 0.031$), but not for *Surveillance* or *Text*.

Perceived effectiveness of the media: In the *prototype evaluation questionnaire*, participants evaluated the perceived effectiveness of the media based on their experience with the prototype. Our results suggest that communicating security risks through infographics is perceived to be more effective than conveying the information through plain text. *Surveillance* (mean 4.8) and *Medical* (mean 5.3) infographics received higher Likert ratings than the *Text* condition (mean 3.3). Figure 4 (left) shows a Box and Whisker plot[2] that summarize participants' ratings. A Kruskal-Wallis test showed a statistically significant difference between perceived effectiveness of the three conditions ($H(3) = 17.85$ with $p < 0.001$). To determine where the differences lay, Mann-Whitney tests with a Bonferroni corrected p-value of ($p < 0.05/2 = 0.025$) was used. Participants perceived both infographics to be more effective than the *Text* condition: ($U = 18, p = 0.001, r = -0.648$) between *Surveillance* and *Text*, and ($U = 6.5, p < 0.001, r = -0.783$) between *Medical* and *Text*.

[2] Middle line is the median, whiskers represent the $1st$ and $4th$ quartiles. Outliers are plotted as individual points.

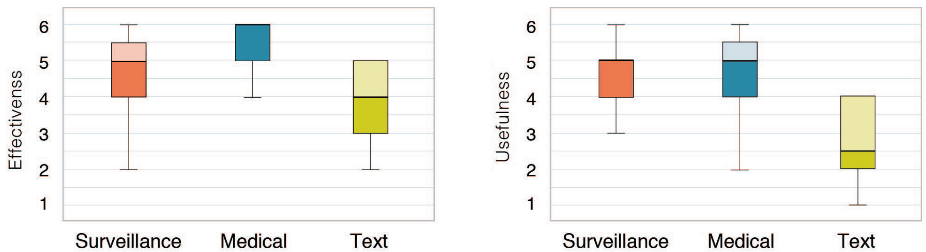

Fig. 4. Likert scale responses assessing the *effectiveness of the prototype at conveying information* (left) and *usefulness of the presented information* (right)

There is no statistical difference between *Surveillance* and *Medical* infographics. However, participants' feedback indicate that the medical concept is the most intuitive to understand. One participant noted, "everybody understands how germs and viruses can affect the human body, so they can make meaningful comparisons with how computer viruses work." Another said, "comparing the computer with the human body is vivid and makes it easy to consider the importance of protecting our computer from viruses." Participants said that the bugs in the *Surveillance* infographic are recognizable imagery for viruses, and the surveillance camera is a well understood concept of physical security, but bugs seem "less threatening" than burglars in context of a "home invasion."

Perceived usefulness of knowledge gained: When comparing participants' responses for usefulness of the information (see Figure 4, right), we found a significant difference: $H(3) = 10.394$ with $p < 0.004$. Mann-Whitney tests show a statistical significance between *Surveillance* and *Text* ($U = 27, p = 0.013, r = -0.503$), and *Medical* and *Text* ($U = 20, p = 0.001, r = -0.627$), but not between *Surveillance* and *Medical*. This suggests that participants perceived the information shown on both infographics to be more useful than the information shown in the *Text* condition.

Participants' feedback indicates that users would be more likely to remember the main take-away message from the infographics, which is to keep their antivirus up-to-date, even if they could not remember the textual details. A participant said, "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." Another said, "I definitely think it would be a lot more interesting to read, which would subsequently make the information more memorable. Text can be very daunting to read, so a more visually interesting method of display with pictures and colours would be a lot more useful."

7 Antivirus Comic Results

Information retention: The *pretest questionnaire* showed that most users do not keep an updated antivirus, and highlighted misconceptions about malware

Effects of Learning	# of Participants
Shared knowledge	8 (69%)
More cautious when browsing and downloading	6 (38%)
Updated antivirus within one week	5 (33%)
More conscious of security warnings	3 (19%)
No effect	2 (13%)

Table 1. Antivirus comic: effect of learning on user behaviour

protection. One-week after interacting with the comic prototype, 88% of participants were able to describe how antivirus software works, compared to just 13% in the *pretest* (See Figure 6). In addition, 81% of the participants were able to describe why it is important to perform regular updates. A participant said, "I didn't know that by updating it's actually able to catch more things," and "the comic allowed me to understand how it worked and why is it so important to keep it up to date." Even though the malware terms sound familiar to participants in the *pretest questionnaire*, many could not describe them. One week after interacting with the comic, most participants were able to distinguish various types of malware. 6 participants used scenes from the comic to describe how antivirus software works, such as describing virus signatures as "DNA sequences", and referring to hackers as the "villains." This suggests that visual narratives of Hack helped to emphasize hackers' malicious intentions. Participants found the interactive elements in the comic useful to reinforce concepts learned.

Behavioural outcomes: Participants reported positive behavioural changes one week later. Table 1 provides a summary of the results. 31% of participants performed updates during the week. One participant explained, "I updated 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." Another said, "It made me realize that I need to be more aware. You know I went back to my computer and looked at my antivirus software that I had (at work) and went home and looked at my antivirus and made sure that it was up to date. I made sure everything was working on it."

38% of participants said that learning about malware had made them more cautious when web surfing and/or downloading files. Another 19% said they became more aware of reading the contents of security warnings before performing an action. An encouraging result is that 69% of participants shared the information they learned with family and friends within a week. A participant said "I was explaining it to my parents, especially my dad who has a whole bunch of antivirus on the computer so it made it really slow. So I was trying to explain to him that he doesn't need that many antivirus, he only needs one."

Perceived effectiveness of the media: Results from the *prototype evaluation questionnaire* (Figure 5) show that the comic was perceived to be effective. Feedback indicates that the comic was easy to understand, and may be suitable for an audience of all ages. Participants reported a pleasurable user experience, and described the comic as "fun", "cute," and "pleasant". Several participants

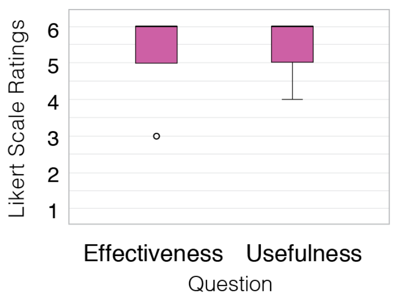

Fig. 5. Likert scale responses for the *effectiveness* and *usefulness* of the comic

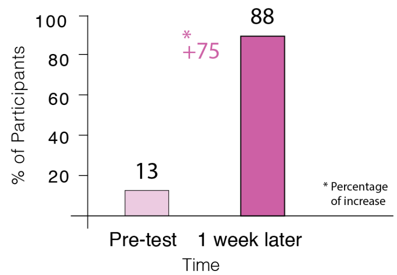

Fig. 6. Participants' ability to describe how antivirus works before and after viewing the comic

wanted to share the information with family and friends. The visual content and interactivity kept users entertained while they learned useful information. A participant said, "If I came across security information and it takes me 30 minutes to read, I probably wouldn't read it. This was quick and easy." Several commented that the characters in the comic made the topic more relatable.

Perceived usefulness of knowledge gained: Results from the *prototype evaluation questionnaire* (see Figure 5) suggest that participants perceived the information taught to them to be highly useful. Feedback indicates that the comic was most useful at clarifying common "myths" surrounding malware and antivirus software. The interactive elements and mini-games were useful to reinforce the information learned.

8 Discussion and Conclusion

In this paper, we show how PT can be used as media to persuade users to update antivirus software. We designed and formally evaluated infographics and a interactive comic that use visual rhetoric to construct arguments. We argue that the strategies proposed in this paper can help to improve computer security understanding, and provide an efficient method for end-user communication of many types of technical information. To summarize, our strategies were:

Use visual rhetoric to construct arguments: Educating users about how security works may increase motivation to practice secure behaviour because it helps to justify the need. For example, our studies show that learning about antivirus detection methods may motivate users to perform updates because they gained knowledge about *why* regular updates are necessary. Visuals also help to illustrate abstract concepts concretely, thus aid in comprehension.

Build mental models of security risks: Helping users build mental models of security risks is an important step towards developing long-term motivation and ability. Since not all security threats will occur in the same way each time (e.g., phishing emails), users with a robust mental model would be able to adapt to changing threats and make security conscious decisions.

Increase users' ability to learn (by making learning easy to do): Since computer security is often administered by end-users with low security knowledge, we show that visual methods of communication can help users overcome the intimidation associated with learning about security. Therefore, media may act as a facilitator to signal that learning is easy to do, and help users engage with the content.

Although PT offer many other potential channels of intervention, we aim to address the current state of mainstream security advice through media as the first step. Media is a widely used channel of communication to warn users about evolving security threats. We believe a more receptive approach than text-based security information is to increase the persuasiveness of the message through visual rhetoric, improve users' mental models of security, and to make the learning process easy to do. The infographics quickly helped users build mental models of how antivirus software works through metaphors and visually illustrating the threat of malware. The interactive comic took this one step further to enable procedural rhetoric through the use of narrative and interactivity to highlight cause and effect relationships. Results show superior perceived effectiveness and usefulness of the prototypes over mainstream text-based information, particularly for participants with low security experience. The pretest and followup results confirmed improvements in knowledge and behaviour after one week.

Our future work will address a few limitations, including context, scalability, the distribution of participants across conditions, and the control condition. First, a longitudinal study outside of the lab setting could possibly measure the prototypes' influences on behaviour over longer time periods and in various learning environments. Second, although we used randomization to assign participants to a condition to balance the groups, chance distribution of experienced versus inexperienced participants resulted an imbalance between groups in the infographic study. Third, we carefully adapted mainstream text information from well written online resources as the control condition, but text from different resources may have varying degrees of effectiveness.

We have successfully extended our proposed strategies to other security topics like password guessing attacks, and are currently working on prototypes for motivating online privacy. The research resulted in high quality educational materials fully accessible to the general public online [22]. We are actively pursuing deployment of the material at national and international venues.

Acknowledgements

This project has been 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. S. Chiasson acknowledges funding from NSERC for her Canada Research Chair in Human Oriented Computer Security.

References

1. C.J. Armitage and M. Conner. Efficacy of the theory of planned behaviour: A meta-analytic review. *British journal of social psychology*, 40(4):471–499, 2001.

2. R. Balebako, J. Jung, W. Lu, L.F. Cranor, and C. Nguyen. Little brothers watching you: Raising awareness of data leaks on smartphones. In *Symposium on Usable Privacy and Security*, 2013.
3. I. Bogost. *Persuasive games: The expressive power of videogames*. MIT Press, 2007.
4. S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot. Influencing users towards better passwords: Persuasive cued click-points. In *British HCI*, volume 1, pages 121–130. British Computer Society, 2008.
5. S. Chiasson, P.C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, 2006.
6. K. Craik and W. James. *The nature of explanation*. Cambridge Univ. Press, 1967.
7. W.D. Crano and R. Prislin. Attitudes and persuasion. *Annual Review of Psychology*, 57:345–374, 2006.
8. W. Eisner. *Comics & Sequential Art*. Poorhouse Press, Tamarac, FL, 1985.
9. B.J. Fogg. *Persuasive Technology: Using Computers to Change What We Think and Do*. Morgan Kaufmann, San Francisco, 2003.
10. BJ Fogg. A behavior model for persuasive design. In *Persuasive Technology*, page 40. ACM, 2009.
11. A. Forget, S. Chiasson, P.C. van Oorschot, and Biddle. Persuasion for stronger passwords: Motivation and pilot study. In *Persuasive Technology*, pages 140–150. Springer, 2008.
12. K .L. Gustafson and R. M. Branch. What is instructional design? *Trends and Issues in Instructional Design and Technology*, pages 16–25, 2002.
13. P.G. Kelley, J. Bresee, L.F. Cranor, and R.W. Reeder. A nutrition label for privacy. In *Symposium on Usable Privacy and Security*. ACM, 2009.
14. P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor, and J. Hong. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2):7, 2010.
15. Logical PC Solutions. 5 Popular Computer Virus Misconceptions, Accessed June 2013. `http://www.logicalpcs.com/2012/03/07/5-popular-computer-virus-misconceptions/`.
16. R. Pastor-Satorras and A. Vespignani. Epidemic spreading in scale-free networks. *Physical Review Letters*, 86(14):3200, 2001.
17. F. Raja, K. Hawkey, S. Hsu, K.L.C. Wang, and K. Beznosov. A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In *Symposium on Usable Privacy and Security*. ACM, 2011.
18. L.M. Scott. Images in advertising: The need for a theory of visual rhetoric. *Journal of consumer research*, pages 252–273, 1994.
19. M. Smiciklas. *The power of infographics: Using pictures to communicate and connect with your audiences*. Que Publishing, 2012.
20. S. Srikwan and M. Jakobsson. Using cartoons to teach internet security. *Cryptologia*, 32(2):137–154, 2008.
21. R. Tembhurne. 15 Myths and Misconceptions about Viruses and Security Applications, Accessed June 2013. `http://rakesh.tembhurne.com/15-myths-and-misconceptions-about-viruses-and-security-applications/`.
22. Versipass. Secure Comics. `http://www.versipass.com/edusec`.
23. A. Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*, 1999.
24. Wikipedia. Antivirus Software, Accessed June 2013. `https://en.wikipedia.org/wiki/Antivirus_software`.