Using Comics to Teach Users About Mobile Online Privacy

Leah Zhang-Kennedy
School of Computer Science
Carleton University
Ottawa, Ontario
leah.zhang@carleton.ca

Sonia Chiasson
School of Computer Science
Carleton University
Ottawa, Ontario
chiasson@scs.carleton.ca

ABSTRACT

Users' privacy is increasingly being jeopardized by images uploaded using smartphones. These images have detailed metadata that can be used maliciously. We designed an online interactive comic to study whether this kind of teaching media can effectively communicate to end-users about the risks associated with mobile online privacy. We present the learning outcomes of our comic prototype based on comparisons of a pretest questionnaire with a follow-up questionnaire one week later. We found significant improvements in participants' understanding and the majority of users reported positive changes in mobile privacy behaviour.

1. INTRODUCTION

Smartphones equipped with GPS are able to track and transmit users' location, oftentimes without users' explicit knowledge. These location-based services may be enabled by default and many apps take advantage of this functionality. For example, photos taken with most smartphones have location-based data attached as metadata; this process is known as *geo-tagging* [6]. Furthermore, permission to share location information (and other tracking data) is typically requested when apps are installed, leading users to believe that these settings cannot be changed.

Many users are unaware of this type of tracking and those who are aware resent the privacy violation. The collected information may be used for online behavioural advertising, may be sold to others for unspecified purposes, or may be used with malicious intent such as in identity theft or stalking [8][5]. When surveyed, users were increasingly opposed to allowing even their phone carrier to track their location [16] and refused to "sell" this information in exchange for discounted apps [15]. Unfortunately, many users still unknowingly reveal significantly more personal details online than they realize [6]. We are faced with this contradictory scenario where users express concern for their privacy yet still share details that could potentially endanger themselves. We argue that users lack the knowledge needed to adequately protect themselves against geo-tagging and understand the risks of online tracking.

Our goal with this online comic is to increase users' awareness of geo-tagging risks and persuade users to act in a more privacy-aware manner when using their mobile devices. In a previous study [11], we evaluated metaphors for risk communication about mobile online privacy through the design of two infographics [1], each using a distinct metaphor, and conducted a between-subject study to test their effectiveness at educating users on this subject. Users reported that information represented visually was easier to digest, learn and remember than text-only information.

In this study, we investigate whether an interactive comic can further enhance the communication and understanding of the topic of mobile online privacy and persuade users to change their privacy behaviour. Technical topics such as security and privacy can be intimidating to users who do not have technical expertise. Earlier work [14, 17, 18] has shown that comics could help users overcome the "intimidation factor". One early effort using this approach is *Security Cartoon*, which uses short static comic strips to explain various security risks [14]. We have recently created interactive online comics for educating users about password guessing attacks [17] and malware/antivirus [18]. Our current prototype uses a similar approach and delivers the information in a 9-page online interactive comic book that offers a comprehensive overview of mobile online privacy. We conducted a user study with 18 participants to evaluate its effectiveness. We also tested whether participants subsequently modified their smartphone geo-tagging and applications settings as an indicator of the persuasiveness of our materials. We have made available our two mobile privacy infographics and the interactive comic accessible online [1].

2. BACKGROUND

In this section, we provide background on the threats faced by users as a result of geo-tagging and summarize studies addressing the issue of mobile privacy. We further discuss previous use of comics in the context of teaching about computer security and privacy.

2.1 Threats from geo-tagging

Henne et al. [9] examined privacy implications of geo-tagging. The results showed that most users are interested in protecting their own as well other people's privacy. Furthermore, users lack the proper understanding of the risks of geo-tagging and usually share more information than they wish by sharing their location information with every image

Technical report TR-14-02, School of Computer Science, Carleton University. April, 2014.

captured and uploaded by their smartphones. A study performed by Friedland et al. [5] discussed how users are usually unaware of how much information they share online and how third-party sites can use this information to gather information about their identities. Balebako et al [3] designed an app providing feedback to users each time apps transmitted geo-location from their phone. Users were previously unaware of the amount of data being transmitted and expressed significant concern once they became aware. Goga et al. [8] performed a study that was able to find users' social network accounts, based on the geo-location information of users' different posts on three popular social network sites: Yelp, Flickr and Twitter. The two most common risks for geo-tagging are identity theft and online tracking that could lead to physical stalking.

Identity theft: Identity theft is a risk associated with geo-tagging, where a malicious person is able to collect users' information such as their home, work, and kids' school addresses by gathering the location information from the images uploaded from the user's smartphone. Attackers use this information as well as other personal details to impersonate victims' identities, which could then be used in fraudulent activities such as financial transactions.

Online tracking: Online tracking occurs when a malicious site or user tracks a victim by collecting and mining information posted online. Victims could also be tracked through the images they upload to different online sites. Information gathered can range from home, work locations to specific details like kids' school address and favourite restaurants, fitness clubs, and other locations. In extreme cases, attackers who learn users' regular activities through uploaded photos may use this information for physical attacks such as stalking or abduction [7, 5].

2.2 Comics in security and privacy

Prior to our work on interactive comics [17, 18], the only extensive exploration of the comic medium to teach about computer security is *Security Cartoon* [14]. The cartoons consist of comic strips intended to improve non-expert users' understanding of various security risks [14]. The topic is also briefly addressed in mainstream comics such as Dilbert [2] and XKCD [12]; both of which occasionally provide security advice for end-users.

The mobile privacy comic presented in this paper is the third in a series of interactive comics to teach end-users about privacy and security topics. Our first comic [17] taught users about three types of password guessing attacks and provided a strategy for creating strong, memorable passwords that are resistant to guessing attacks. The intention was to persuade users to chose secure password by first teaching *how* the attacks work so that users can reason about strong passwords for themselves. Our experiment showed that users initially had very poor understanding of the attacks, but one week after viewing the online comic they demonstrated understanding of the attacks and 80% of users reported that they were influenced to update their current passwords as a result of viewing the comic.

Our second interactive comic taught users about different types of malware and how antivirus software works to protect computers against these threats [18]. In the pretest, only 13% of users could describe how antivirus software works. One week after viewing our comic, 88% of users could describe its operation. Furthermore, 69% of users reported sharing their knowledge with others, 38% became more cautious when browsing online and 33% updated their antivirus software.

3. DESIGN OF THE INTERACTIVE COMIC

We developed a 9-page online comic to educate users [1]. The comic used similar metaphors to those explored in the earlier mobile privacy infographics [11]. In the comic, we also included attributes specifically intended to increase reader engagement. For example, we made extensive use of characters, narrative, humour, and interactivity. Figure 1 provides two example pages from the comic.

The comic medium allows for highly customized content that takes advantage of a full range of visual symbols, and pairing of words and images to construct a convincing story [10]. The juxtaposition of images and text aids in breaking down complex concepts into manageable chunks that facilitate learning and comprehension. The use of narrative and characters further helps to progressively guide users towards understanding complex subjects. Furthermore, there is evidence that comics are more accessible to non-technical audiences than traditional educational materials because they are viewed as easy to read and are less intimidating [14].

The use of humour has been shown to ease the social, emotional, and cognitive challenges of addressing serious topics [4]. Humour can also enhance persuasion, and increase the comprehension and retention of information [4]. When designing our comic, we intentionally added humorous dialog and placed the characters in humorous situations in an effort to increase reader enjoyment, comprehension, and information retention.

We designed three main characters for the comic. *Jack* and *Nina* are agents of computer security. Their mission is to solve computer security and privacy crimes and protect users from *Hack*. As the name implies, Hack is a mysterious character who embodies all computer security crimes. Jack and Nina act as mentors who teach users about various attacks and protection strategies. In this particular case, they are teaching users about the risks of mobile geo-tagging and how to protect themselves against these threats. All of the characters are designed with a sense of humour to make them well-rounded, interesting, and believable [13].

We added interactive components to the comic to give users the opportunity to explore. For example, in the "Geo-tagging" section of the comic, users can roll over silhouettes of people to read about specific consequences of sharing photos online. The user follows a day in the life of "Jane", a character who fell victim to Hack.

The online comic consists entirely of original artwork drawn by us in Adobe Illustrator and programmed in Flash. During the study, participants viewed the comic as a .swf file on a Macintosh laptop computer. After study completion, we publicly released the comic on our website dedicated to teaching about computer security and privacy [1].

4. STUDY DESIGN

We conducted a user study with 18 participants to test the effectiveness of the comic and evaluated its perceived effectiveness, usefulness, and memorability. Our objective was to assess whether users demonstrated improved understanding after viewing the comic, and evaluate information retention and behaviour after one week.

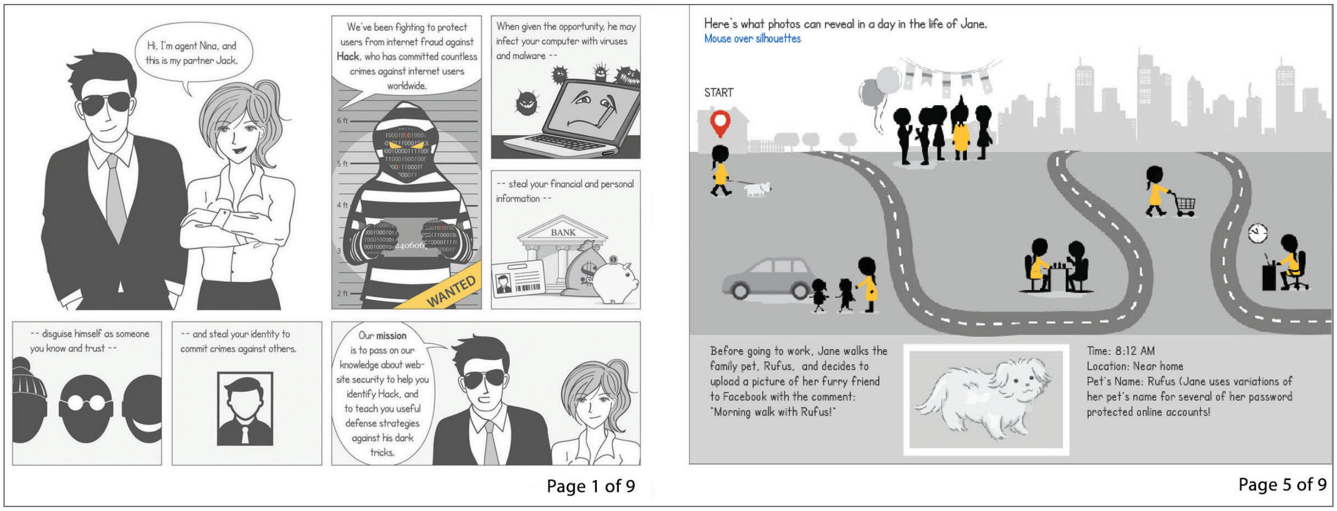
Hi, I'm agent Nina, and this is my partner Jack.
We've been fighting to protect users from internet fraud against **Hack**, who has committed countless crimes against internet users worldwide.
6 ft
5 ft
4 ft
3
2 ft
WANTED
When given the opportunity, he may infect your computer with viruses and malware --
-- steal your financial and personal information --
BANK
-- disguise himself as someone you know and trust --
-- and steal your identity to commit crimes against others.
Our **mission** is to pass on our knowledge about web-site security to help you identify Hack, and to teach you useful defense strategies against his dark tricks.
Page 1 of 9
Here's what photos can reveal in a day in the life of Jane.
Mouse over silhouettes
START
Before going to work, Jane walks the family pet, Rufus, and decides to upload a picture of her furry friend to Facebook with the comment: "Morning walk with Rufus!"
Time: 8:12 AM
Location: Near home
Pet's Name: Rufus (Jane uses variations of her pet's name for several of her password protected online accounts!
Page 5 of 9

Figure 1: A page from our mobile privacy interactive comic [1]

The study received approval from our University's Ethics review board. Participant were Carleton University students and staff recruited through an email mailing list. Participants were compensated $20 for their time.

Each participant completed two one-on-one lab sessions. The first session was structured as follows:

- Participants completed a pre-test questionnaire assessing their current knowledge of smartphone geotagging and photo sharing behaviours.
- Participants viewed and interacted with the online comic. They were allowed as much time as needed to view the comic to learn about smartphone geotagging.
- Participants completed a questionnaire providing their perceptions and opinions of the prototype. The questionnaire included 5-point Likert scale questions, ranging from 1 (strongly disagree) to 5 (strongly agree). Some questions were reversed to avoid bias. The questionnaire also re-tested their knowledge of smartphone geotagging and photo sharing.

Participants were scheduled to return approximately one week later to complete the second session. It included a follow-up questionnaire and interview about the information they learned and their experience during the study.

5. STUDY RESULTS

Participants: Eighteen participants completed session one and 15 returned to complete the follow-up session. Participants included eight females and ten males with a mean age of 22. Most were undergraduate students, with the exception of two graduate students and two university stuff. In the pretest questionnaire, participants self-evaluated their knowledge of smartphone geo-tagging on a Likert scale from 1 (novice) to 5 (expert). 90% (16/18 participants) considered themselves to have low knowledge of the topic and gave ratings between 1 and 2. The remaining two participants gave a moderate rating of 3. Sixteen participants reported uploading photos from their smartphones on a regular basis. The top sites used to upload photos from their smartphones were Facebook (13/18), Twitter (10/18), Instagram (12/18). All participants expressed some concern regarding their online privacy.

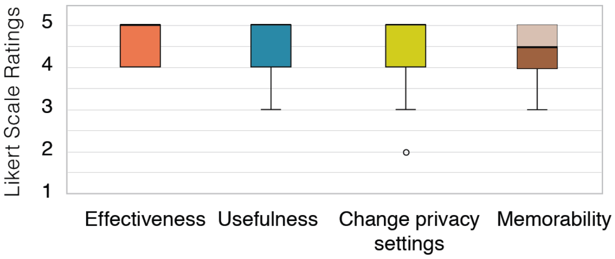

Figure 2: Likert scale responses (5 = most positive)

We begin by discussing users' Likert scale responses summarizing their perceptions and opinions of the comic at the end of session one. Figure 2 illustrates these responses.

Effectiveness for learning: Most users said that learning about smartphone geo-tagging visually is an effective method to communicate to users about this topic. The mean Likert-scale rating was 4.6/5. There is consensus among our participants that the graphics were very helpful in enhancing their understanding of geo-tagging. One participant commented that although she did not personally like reading comics on her own time, the mobile online privacy comic was able to get the message across and she did indeed learn useful information about geo-tagging. Most of our participants emphasized the entertainment value of the comic as a learning tool. They also mentioned that graphics enhanced their understanding and were impressed with the speed with which they were able to learn the information. For example, VPC5 said, "the graphics were an easy, fun, and fast way of teaching the information and sure helped enhance my understanding of the topic."

Usefulness of the advice: Most of the participants found that they have gained useful knowledge about smartphone geo-tagging ($Mean = 4.7$). VPC2 said, “People love posting and sending pictures and videos to one another without knowing the consequences, they seem to believe that it is safe since they believe only their friends can see the post/image.” Many participants expressed that they were unfamiliar with the risks associated with geo-tagging of photos on smartphones. For example, VPC1 stated “had I not have come to the session today, I wouldn’t have known about geo-tagging. I would like to see what other ways our privacy online can be compromised”, and VPC9 mentioned “I never really considered all the harm that could be done by uploading a simple photo from my phone”.

Likelihood to change location settings: Participants rated whether the comic has convinced them to change the location information settings of the apps they use on their smartphones. The majority thought the comic was convincing ($Mean = 4.4$) and prompted them to change the settings on their phone to prevent these risks. VPC7 said, “I never knew what geo-tagging was and I never knew it could be dangerous. I will definitely try to be careful from now on.” Some participants suggested that providing additional resources on how to change the settings would be very helpful. We did not offer this information in-depth because the procedure is different across smartphone models and apps, but providing links to external resources is possible.

Perceived memorability of information: Most participants thought that they will likely remember what they have have learned weeks later. ($Mean = 4.3$). VPC2 particularly liked page 5 of the comic, where users could interact with a character named Jane to see how her actions could be used to jeopardize not only her own privacy but also those around her during the course of a day. The participant said, ”I believe this graphic should be used in schools to warn others about the dangers of geo-tracking.” We believe visual imagery of certain concepts helped participants to remember the information better. For example, participants used certain scenes of the comic to help explain their understanding of the concepts. On page 5 of the comic, one part shows a photo of Jane’s suitcase that she shared before going on vacation. The photo reveals some of her personal identifications and travel information. VP9 said, “I found the trail concept out of all the graphics the most fascinating... I guess that I am not a super sleuth in this way, but by looking at a photo of someone’s packed suitcase or someone’s milkshake, I would never think to gather such personal information about them!” Participants’ responses suggest that using graphical aids, characters and a narrative helped make difficult concepts easier for users to remember.

5.1 Information Retention

We tested information retention based on two concepts: geo-tagging and “EXIF”. At the beginning of session one, we asked the participants to describe the concepts in their own words. These questions were also asked verbatim in the follow-up questionnaire one week later. Figure 3 shows the results from the pre-test and follow-up questionnaires. For the analysis of information retention, only data from the 15 participants who completed both sessions is considered since the data must be paired. We evaluated the answers based on the correct description of the concepts, and not on participants’ ability to answer in the most correct technical terms. For example, some participants reported that “EXIF” is “a file that opens geo-tagging,” but the technical description would be: “file format for image files used by smartphone cameras which can also include GPS coordinates.” In this case, the participant’s answer would be considered correct. For each correct answer, we attributed a point and tabulated the pre- and post-test scores for each user.

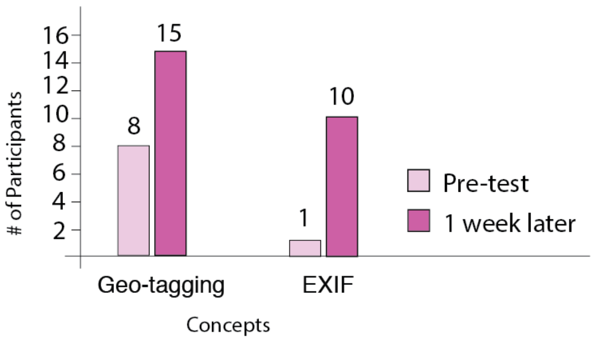

Figure 3: Participants’ ability to describe the geo-tagging and photo sharing risks before and one week after viewing the online comic

Geo-tagging concept: All of our participants were able to correctly describe what geo-tagging means in the follow-up questionnaire, compared to 53% (8/15 participants) in the pretest questionnaire. This demonstrates a significant increase in participants’ knowledge of the concepts, and excellent information retention after one week. Samples of participants’ definitions of geo-tagging include: “assigning geographical co-ordinant information to the metadata of a photograph, indicating where the picture was taken” (VPC14), and “Geo-tagging is a feature on smartphones where a photo uploaded to the web will contain information about what geo-location that photo was uploaded from” (VPC3). Such responses suggest that users had developed a reasonable understanding of the geo-tagging concept. Most participants were also able to recall prevention measures that were taught to them in the comic, such as turning off the GPS feature when not in use, not sharing pictures with personally identifiable information, and using an EXIF editor to remove location based information.

EXIF concept: Only one participant was able to identify or guess the meaning of “EXIF” in the pre-test questionnaire. After one week, 67% (10/15 participants) correctly described the concept in the follow-up questionnaire. They used descriptions like “the information that is provided on posts

Behaviour	# of participants
Changed location-based settings:	8
Cautious photo sharing behaviour:	4
No effect	3

Table 1: Summary of behaviour changes after one-week

and pictures on the time and location of where it was taken which pin points your exact location within 3m" (VPC2), and "It is a format in which your location and information is present for viewing and extraction when sharing images online" (VPC5).

Our pretest result indicate that our participants had very little knowledge of EXIF beforehand. Most defined EXIF as a file format that can be used on any device. We suspect that this occurred because the pre-test also included the words associated with the acronym, "Exchangeable Image File". In particular, the term "exchangeable," led participants to think about "cross-platform/device" compatibility of file format. Five participants still had some trouble defining the term in the follow-up questionnaire. Figure 3 summarizes users' knowledge of these two concepts from the pre-test and follow-up questionnaires.

5.2 Behavioural Outcomes

During session two, we asked participants whether they took any actions to protect their online privacy since viewing the educational material. 53% of participants (8/15) changed location-based settings on their smartphones such as disabling GPS functionality and/or removing location information from photos. For example, VP8 said, "Since viewing the material, I definitely took actions online (and on my smartphone) to protect my privacy online. I changed my settings on my phone... and I am also careful when uploading pictures in case there is anything in the background of the photo that could be used like my drivers licence or a credit card." An additional four participants (27%) said that although they did not make any physical changes during the course of one week, reading the comic made them more aware of their own privacy and therefore more cautious about online privacy in general. Interestingly, several participants also shared the information they learned with a family member. For instance, VPC7 said, "I didn't personally take any actions to protect my online privacy since I don't usually upload pictures but I told my sister about it and if I ever do upload pictures more frequently I will take precautions to ensure important information cannot be extracted from the picture." Table 1 summarizes the behaviour changes reported one week after viewing the comic.

6. CONCLUSIONS

We designed a comic prototype that teaches users about mobile online privacy and conducted a user study to evaluate the effectiveness, usefulness, memorability, and persuasiveness of the comic to convince users to change privacy settings on their mobile devices. Participant evaluations of the comic and feedback suggest that most thought the prototype was an effective learning tool that had helped them with the understanding of the concepts. Many commented that the comic was fun, engaging, and quick to read. We assessed users' pre-test knowledge and compared it to their knowledge one week after viewing the comic. We found significant improvements in participants' understanding. Furthermore, more than half of the participants took actions to improve their privacy settings and a further 27% reported more cautious behaviour.

A common theme in our research is the idea that empowering users with security knowledge of specific threats and advice on how to protect themselves will persuade users to behave more securely. This current study provides further supporting evidence for our visual and entertaining approach to security and privacy education.

7. 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.

8. REFERENCES

[1] Versipass. http://www.versipass.com/edusec/.

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

[3] 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 (SOUPS)*. ACM, 2013.

[4] C. Dormann and R. Biddle. A review of humor for computer games: Play, laugh and more. *Simulation & gaming*, 40(6):802–824, 2009.

[5] G. Friedland, G. Maier, R. Sommer, and N. Weaver. Sherlock holmes' evil twin: On the impact of global inference for online privacy. In *New Security Paradigms Workshop (NSPW)*, 2011.

[6] G. Friedland and R. Sommer. Cybercasing the joint: On the privacy implications of geo-tagging. In *USENIX Workshop on Hot Topics in Security (HotSec)*, 2010.

[7] G. Friedland and R. Sommer. Cybercasing the joint: on the privacy implications of geo-tagging. In *Proc. USENIX Workshop on Hot Topics in Security*, 2010.

[8] O. Goga, H. Lei, S. H. K. Parthasarathi, G. Friedland, R. Sommer, and R. Teixeira. Exploiting innocuous activity for correlating users across sites. In *International Conference on World Wide Web (WWW)*, 2013.

[9] B. Henne, C. Szongott, and M. Smith. Snapme if you can: privacy threats of other peoples' geo-tagged media and what we can do about it. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pages 95–106. ACM, 2013.

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

[11] C. Mekhail, L. Zhang-Kennedy, and S. Chiasson. Visualizations to teach about mobile online privacy. In *Persuasive Technology Conference (poster)*, 2014.

[12] Munroe, R. XKCD, Accessed December 2012. http://xkcd.com/936/.

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

[14] S. Srikwan and M. Jakobsson. Using cartoons to teach internet security. *Cryptologia*, 32(2):137–154, 2008.

[15] TRUSTe. Uk 2013 consumer data privacy study, mobile edition. http://www.truste.com/

about-TRUSTe/press-room/news_uk_truste_customers_concerned_about_mobile_privacy, 2013.

[16] J. Urban, C. Hoofangle, , and S. Li. Mobile phones and privacy. *Public Law Research Paper*, 2012.

[17] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. Password advice shouldn't be boring: Visualizing password guessing attacks. In *APWG eCrime Summit*. IEEE, 2013.

[18] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. Stop clicking on "update later": Persuading users they need up-to-date antivirus protection. In *Persuasive Technology Conference*. Springer, 2014.