Nudging Adoption: Creating Awareness in Antivirus Software

Jacqueline White
University of North Carolina at Charlotte

Heather Richter Lipford
University of North Carolina at Charlotte

Abstract

Users often lack awareness of potential security risks on their smartphones and the protective security mechanisms available for securing their devices and information. One way of raising awareness in users is through the use of notifications and nudges. To that end, we designed two notifications for antivirus software, encouraging users to install antivirus software on another platform, namely a smartphone. We first developed the designs through feedback from a semi-structured interview conducted with 12 participants, then further evaluated the designs through a user study with 36 participants. Our preliminary results indicate that notifications on one device, such as a laptop, may be effective in raising awareness of security tools on other device platforms. Our results also highlight the motivators influencing adoption of antivirus software on another device platform and design guidelines for user attention to and implementation of notifications suggesting security behaviors.

1 Introduction and Related Work

Users generally perceive that their traditional computers (e.g. desktops and laptops) are more likely to be vulnerable to security risks than their smartphones, and generally trust their smartphone applications [9, 11, 14, 15] to be secure and safe. Additionally, users are more likely to use protection mechanisms on their computers than on their smartphones [3, 9, 11, 14]. Thus, while users do care about their smartphone security, they sometimes lack awareness of the appropriate mechanisms and behaviors to secure their devices [9, 10, 15]. As a result, educating users about suggested security actions, such as through the use of notifications and nudges, can be effective in increasing awareness and secure behaviors [2, 5, 6, 13, 16]. A major question then is how and when to deliver such guidance, to raise awareness of security tools and encourage their use. In our research, we are investigating whether we can use notifications on one platform where users are already using a security tool, namely a traditional computer, to raise awareness of and motivate adoption of similar tools on another platform, namely a smartphone.

Notices have been used in a variety of situations, most relevantly in security risk awareness as well as security tool notifications, such as reminders to run system scans in antivirus software or alerting of potential phishing websites. Key criteria in providing security advice are that the advice is effective, easy to execute, consistent across notifications, and concise [1, 7, 12]. Additionally, notifications should have easy to understand language and avoid technical jargon [14]. Nudges have also been used to influence behavior when faced with a choice, such as making default choices the more secure option [1, 4, 8, 12, 13, 16]. Zimmerman and Renaud explain, "Nudges activate automatic cognitive processes, such as biases and heuristics, to encourage people to decide in a particular way [16]." With these guidelines in mind, we are designing and evaluating two notifications for anti-virus software on a computer, which recommends the use of that same software on a smartphone.

This poster presents a two-phase user study of a notification to encourage users of antivirus software on a laptop/desktop to also adopt usage of antivirus software on a smartphone. We chose anti-virus software as the tool due to wide-spread understanding of its function and purpose as well as its universal applicability to both traditional computing devices and smartphones. Our research questions are as follows [1] Could notifications in existing security tools be utilized to nudge existing users to adopt the tools on a different platform, and [2] What are the user suggested design guidelines for such a notification to encourage attention and adoption?

2 Methodology

This study operated in two phases, with the first being a design phase to determine the most effective design and placement for a notification in a laptop-based anti-virus interface. The second phase consisted of a user study to evaluate the notification designs and their perceived effectiveness.

2.1 Design Phase

During the first phase of the study, we tested three iterations of notification phrasing, design, and placement with a focus group of 12 university student participants to determine the most effective combination for catching users' attention and prompting them to read the notification. During this step, various types of notifications, such as subtle nudges, active warnings, and banners, were designed for an antivirus software in a laptop/desktop environment following design guidelines previously outlined [1, 1, 7, 12, 12, 14]. Each design was shown to participants who were then interviewed regarding what they liked or disliked, and potential changes. At the conclusion of the design phase, two notification designs were chosen and redesigned for the second phase of the user study.

2.2 Evaluation Phase

We then conducted a user study with 36 participants to evaluate the perceived effectiveness of the notifications. First, participants completed a demographics survey which included questions about their current usage and perceptions of antivirus software on their laptop/desktop and smartphone. Participants were then shown a prototype of an antivirus software in a laptop/desktop environment and asked to explore the prototype to familiarize themselves with the application. We utilized an A/B methodology, where half of the participants saw no nudge, while half saw an active notification and a passive nudge, within the prototype. Participants were then interviewed to determine if they were interested in installing antivirus software on their smartphone. Group A was then given the time to explore the prototype again with the notifications included. All participants were then shown the two notifications and asked their impressions, likes and dislikes, and suggestions for improving the notifications. We also asked for their perceptions regarding whether and how such a notification could prompt them to install antivirus software on their smartphone. Transcripts of the interviews from the second phase of the study were qualitatively analyzed using grounded-theory methodology to identify key themes regarding notification design preferences and motivators for installing antivirus software on a smartphone.

3 Preliminary Results

In the pre-study survey, we found that 22 participants were already using antivirus software on their laptops/desktops, while only 5 participants were using antivirus software on their phones. The three most common reasons for installing, or considering installing, antivirus software on the laptop/desktop and smartphone were that the software was useful, the software was pre-installed on the device, or that the participant was required to install the software. Still, most of the participants viewed antivirus software as beneficial to their device, with 28 participants agreeing with this statement on their smartphone and 29 participants agreeing on their laptop/desktop. However, we also found that more participants would recommend antivirus software to others on the laptop/desktop (30 participants) than the smartphone (21 participants).

Our results also identified multiple preliminary motivations for installing antivirus software on a smartphone. One of these motivators is the **functionality** of the software, where participants were considering if the antivirus software would actually protect their device and their information, which could both motivate or dissuade installation. The **ease of installation**, with participants expecting the process to be quick and easy, could also persuade or dissuade installation. Another motivator was **awareness** of the mobile version of antivirus software, with the lack of awareness of the availability of mobile antivirus software a stated reason for not installing. Participants also stated that **promotions** offered by the company would potentially motivate them to install the mobile version, even if just to test it. Some of these promotions included the cost of the software, if it was included in the existing cost of their coverage plan, or the offer of a free trial. Participants also considered their perceptions of **risk** to viruses on smartphones when deciding if it was even necessary to install antivirus software on their phones to protect against viruses.

Overall reaction to both designs was positive, and users indicated they could potentially be effective. Participant feedback indicated that such notifications should have a **minimalist** design with only necessary buttons and text. To ensure the notification is **user-friendly**, participants wanted one that was easy to understand, navigate (including returning to the main interface), and follow any instructions if necessary. Participants also wanted there to be sufficient **information** included in the notification to communicate the potential security risks users face on smartphones and how the antivirus software helps prevent these risks.

Inclusion of the notifications in existing antivirus software on the laptop/desktop led to 24 out of 36 participants indicating they would be interested in installing antivirus software on their smartphone. However, 10 participants who saw the prototype without nudges expressed their intent, prior to seeing and commenting on the notification designs. Thus, increasing awareness of the security tool is likely a primary motivator for installation with notifications being a potentially effective method of doing so.

4 Conclusion

While our analysis is ongoing, preliminary results indicate that there is potential to raise awareness and motivate adoption of smartphone security tools by utilizing notices on traditional computers. Our results provide guidance on the design of such notices, to inform future quantitative studies evaluating potential effectiveness and impact.

References

[1] ACQUISTI, A., ADJERID, I., BALEBAKO, R., BRANDIMARTE, L., CRANOR, L. F., KOMANDURI, S., LEON, P. G., SADEH, N., SCHAUB, F., SLEEPER, M., WANG, Y., AND WILSON, S. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv. 50*, 3 (aug 2017).

[2] BAVEL, R. V., RODRÍGUEZ-PRIEGO, N., VILA, J., AND BRIGGS, P. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies 123* (2019), 29–39.

[3] BREITINGER, F., TULLY-DOYLE, R., AND HASSENFELDT, C. A survey on smartphone user's security choices, awareness and education. *Computers Security 88* (2020), 101647.

[4] CARABAN, A., KARAPANOS, E., GONÇALVES, D., AND CAMPOS, P. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2019), CHI '19, Association for Computing Machinery, p. 1–15.

[5] EBERT, N., ALEXANDER ACKERMANN, K., AND SCHEPPLER, B. Bolder is better: Raising user awareness through salient and concise privacy notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2021), CHI '21, Association for Computing Machinery.

[6] GLUCK, J., SCHAUB, F., FRIEDMAN, A., HABIB, H., SADEH, N., CRANOR, L. F., AND AGARWAL, Y. How short is too short? implications of length and framing on the effectiveness of privacy notices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (Denver, CO, June 2016), USENIX Association, pp. 321–340.

[7] KITKOWSKA, A., WARNER, M., SHULMAN, Y., WÄSTLUND, E., AND MARTUCCI, L. A. Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (Aug. 2020), USENIX Association, pp. 437–456.

[8] MICALLEF, N., JUST, M., BAILLIE, L., AND ALHARBY, M. Stop annoying me! an empirical investigation of the usability of app privacy notifications. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction* (New York, NY, USA, 2017), OzCHI '17, Association for Computing Machinery, p. 371–375.

[9] MYLONAS, A., KASTANIA, A., AND GRITZALIS, D. Delegate the smartphone user? security awareness in smartphone platforms. *Computers Security 34* (2013), 47–66.

[10] NDIBWILE, J. D., LUHANGA, E. T., FALL, D., MIYAMOTO, D., AND KADOBAYASHI, Y. A comparative study of smartphone-user security perception and preference towards redesigned security notifications. In *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities* (New York, NY, USA, 2018), AfriCHI '18, Association for Computing Machinery.

[11] OPHOFF, J., AND ROBINSON, M. Exploring end-user smartphone security awareness within a south african context. In *2014 Information Security for South Africa* (2014), pp. 1–7.

[12] REEDER, R. W., ION, I., AND CONSOLVO, S. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security and Privacy* (2017).

[13] SHARMA, K., ZHAN, X., NAH, F. F.-H., SIAU, K., AND CHENG, M. X. Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People 1*, 1 (Jan. 2021), 69–91.

[14] TAHA, N., AND DAHABIYEH, L. College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies 26*, 2 (Mar. 2021), 1721–1736.

[15] WU, D., MOODY, G. D., ZHANG, J., AND LOWRY, P. B. Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. *Information Management 57*, 5 (2020), 103235.

[16] ZIMMERMANN, V., AND RENAUD, K. The nudge puzzle: Matching nudge interventions to cybersecurity decisions. *ACM Trans. Comput.-Hum. Interact. 28*, 1 (jan 2021).