Human Factors in Cybersecurity, Vol. 127, 2024, 127–136
https://doi.org/10.54941/ahfe1004772

Exploring User Perspectives on Prioritizing Security Through Software Updates

Mahzabin Tamanna[1], Joseph D Stephens[2], Abdolhossein Sarrafzadeh[3], and Mohd Anwar[4]

[1]Department of Computer Science, Collage of Engineering, North Carolina State University, Raleigh, NC, USA
[2]Department of Psychology, Collage of Health & Human Sciences, North Carolina Agricultural and Technical State University, Greensboro, NC, USA
[3]Center of Excellence in Cybersecurity Research, North Carolina Agricultural and Technical State University, Greensboro, NC, USA
[4]Department of Computer Science, Collage of Engineering, North Carolina Agricultural and Technical State University, Greensboro, NC, USA

ABSTRACT

Security vulnerabilities can expose users to risk if they do not promptly install necessary security updates. To minimize risk, software developers regularly release security updates that address known or potential vulnerabilities. The National Vulnerability Database (NVD) has demonstrated the severity of different attacks that can be prevented by installing updates. However, previous studies have revealed many users avoid installing software updates due to numerous reasons. In this study, we examined users' behaviors towards software updates by analyzing their perceptions and prioritization of software regarding installing security updates. We also explored to what extent the users trust these updates. The goal of this study is to gather insights into user attitudes toward software updates to benefit developers, analysts, and users. To achieve the goal and gain a comprehensive understanding of users' perspectives, we conducted a survey consisting of questions designed to uncover valuable insights into individual behaviors, attitudes, and preferences related to software updates. The questionnaire featured seven categories of software, such as web browsers, multimedia players, and antivirus software, where participants ranked their preferred software categories for security updates. The survey also collected information about user trust in software updates for enhancing security. Our analysis showed that users prioritize the software updates that are essential to running the system, such as OS updates. Among the survey respondents, 29% of users prioritized antivirus updates, 26% prioritized OS updates, and 20% prioritized web browsers. Only 3.52% considered multimedia software updates important. Despite 48% of users think software updates can enhance security, only 16% rarely or never rely on them. In addition, approximately 40% reported having adverse experiences with software updates. These reasons have resulted in a lack of trust in updates, making it difficult for software to achieve higher adoption. To enhance security through, it is important to develop better strategies and reliable updates that build users' trust in the software update.

Keywords: Human factors, Cybersecurity, Software update, Trust, Human behaviour

INTRODUCTION

Software updates involve modifying existing software to address issues, improve functionality, and enhance security. Software with vulnerability makes the system vulnerable and causes a security risk for the users. Neglecting updates for identified vulnerabilities can cause severe security breaches. However, many users do not install all updates and do not consider all updates equally important or significant or have high priority (Khan, Bi & Copland, 2012; Nappa *et al.,* 2015). While users often accept some software updates, many updates are ignored (Mathur *et al.,* 2018; Vaniea, Rader & Wash, 2014).

In 2021, the Log4j vulnerability, also known as Log4Shell, affected numerous systems and applications. According to the National Vulnerability Database NVD (NVD, 2021), the Log4shell attack had a severity score of 10 and was labelled as critical. The attack could have been prevented by applying the available software update. (IBM, 2021). Based on a 2022 study, many security breaches occur due to vulnerabilities for which updates were available but remain uninstalled (Software Patching Statistics, 2022). Some updates remain uninstalled for more than two years (Symantec, 2016), causing numerous systems to remain at risk of being attacked. The installation of updates is a crucial aspect of maintaining security (Reeder, Ion & Consolvo, 2017). However, it is often neglected by users.

Research has provided reasons and recommendations to increase user awareness and improve update application rates. According to the findings (Marconato, Nicomette & Kaâniche, 2012; Wash *et al.,* 2014) users hesitate to update software for several reasons, which include a lack of understanding of update importance and concerns about potential disruptions. Additionally, users sometimes do not fully understand the necessity or functionality of updates, leading them to avoid updating software (Zhang-Kennedy, Chiasson & Biddle, 2014; Fagan, Khan & Nguyen, 2015). Furthermore, Vaniea & Rashidi (2016) found some users do not like the changes that a software update brings, such as changes in user interface or navigation processes. Although software updates are important for enhancing system security, user reluctance undermines this essential protection, and it remains unclear whether users' attitudes toward all software updates are consistent. Moreover, it is unknown how much users trust software updates. These gaps in knowledge create obstacles to providing developers with effective, evidence-based advice to improve users' update behaviour. Thus, in our study, we investigated how end-users prioritize software updates and their trust level in these updates for system security. To achieve this, our structured research questions are as follows:

RQ1: Which type of software do users prioritize when considering updates?

RQ2: To what extent do users trust these software updates?

By answering the research question, our goal was to understand user behaviour and decision-making in willingness to apply software updates. This study has been organized as follows. Section 2 presents a review of related work, Section 3 describes the methodology, Section 4 presents the results, and Section 5 offers the conclusion of the study.

RELATED WORK

Although updates are essential for ensuring the security and proper functioning of the software, users frequently fail to install them (Vaniea & Rashidi, 2016; Redmiles, Malone & Mazurek, 2016). While users with some expertise follow security practices, the majority of non-experts do not consider software updates to be important (Ion, Reeder & Consolvo, 2015). Not just among non-expert end users, even system administrators are also reluctant and face difficulties with processing software updates (Tiefenau *et al.,* 2020). Previous research on user behavior regarding software updates has shown that users frequently ignore and delay the updates (Nicholson, Coventry & Briggs, 2018; Möller *et al.,* 2012;). Some users tend to overlook the significance of updates and may not fully comprehend the potential security risks associated with outdated software versions (Vitale *et al.,* 2017; Wash *et al.,* 2016). Users often have difficulties understanding the need for updates if their current version appears to be working fine (Fagan & Khan, 2016; Mathur et al., 2018; Vaniea & Rashidi, 2016). Similar disparities between users' perceptions and actions regarding software updates have been found in studies focused on Android (Rosen, Qian & Mao, 2013), smartphones (Fassi *et al.,* 2020), and smart homes (Haney & Furman, 2023). One potential reason for the hesitation could be the disruptive nature of software updates, which can take a long time to complete and interrupt ongoing tasks (Fassi et al., 2021).

Various solutions have been proposed to address the issue of delayed updates, including automatic (Sarabi *et al.,* 2017) and silent updates (Duebendorfer & Frei, 2009). While some users prefer automatic updates for convenience and to ensure their software is up-to-date, others desire more control over the update process (Wash *et al.,* 2014). According to Mathur & Chetty (2017), users who choose to enable automatic updates may have lower risk tolerance and less trust in applications. Additionally, users want to know what the update entails to determine whether they want the changes or not. Thus, Farik *et al.* (2018) recommended that developers clearly communicate the significance of updates and improve notification messages. Besides, user-centered solutions like providing more information and designing better notifications have been frequently suggested to improve compliance rates further. Mathur & Chetty (2017) proposed providing more information, and Tian et al. (2014) emphasized the importance of designing better notifications.

METHODOLOGY

Participants Requirement

For our research study, we utilized Qualtrics to conduct an online survey and gather data from 63 participants. The participants were required to be at least 18 years old and have experience with the Windows operating system. To ensure ethical research practices, the study was approved by the author's institution's Institutional Review Board (IRB). All survey participants voluntarily participated in the survey without any compensation. The

Qualtrics software was chosen as it has been widely used in security-related research to gain insights into user perspectives. The survey was designed to collect data without collecting any personal information that could potentially breach participants' privacy or security. Therefore, the survey responses were anonymous and non-traceable.

Survey Design

The survey was designed to collect valuable insights and feedback from participants regarding their attitudes and actions toward software categories and software updates. The survey used purposive non-probability sampling. The questionnaire was a set of quantitative questions to gather user information on behaviours and preferences related to software updates. In addition, the survey encompassed demographic questions, inquiries about computer usage patterns, and users' emotional and rational information. Participants rated their responses to these questions on a 5-point Likert scale, from Never = 1 to Always = 5.

RESULTS

Participants Descriptive Analysis

Our survey received a total of 63 responses to the questionnaire. However, 15 responses were excluded due to incomplete answers, leaving us with a group of 48 participants. It is worth noting that the group had a balanced distribution in terms of gender, with 54.17% of the participants being male and 45.83% being female. Furthermore, the majority of participants belonged to the age group of 26–34 and possessed a higher level of education. All participants reported spending at least one hour on the computer every day. While selecting the size of our population for the survey, we considered previous user behaviour studies (Fugard & Potts, 2015; Jiang, He, & Allan, 2014).

Priorities of Users Concerning Software Updates

RQ1: Which type of software do users prioritize when considering updates?

To address our first research question and gain deeper insights into the preferences and priorities, we asked users to prioritize the categories of software they feel are important to update and have significance. The categories provided are antivirus/anti-malware, Windows (OS), web browser, email and digital communication, word processing, graphics software, and multimedia software.

Figure 1 illustrates our findings to answer the research question. Results have revealed that almost one-third of the participants, which is approximately 29%, give the highest priority to antivirus updates when it comes to selecting software categories for security purposes. Additionally, around 26% of the respondents consider operating system updates to be important for maintaining security, while roughly 20% of them prioritize web browser updates. It's worth noting that only a small fraction of the participants, about 3.52%, believe that multimedia software updates are of significant importance for security purposes.

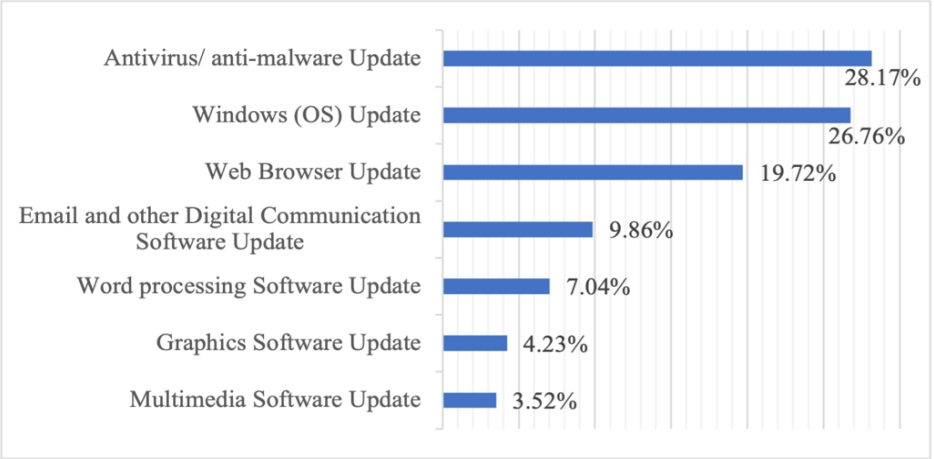

Figure 1: Users' response for software category prioritization.

Users' Trust in Software Update

RQ2:To what extent do users trust these software updates?

To answer our second research question, we constructed four broader questions to find out what users trust in the software update. As we were focused on observing the behavioral changes of users, we utilized a widely used behavioral model, Affect-Reason-Involvement (ARI) model (Buck *et al.*, 2004). This model's purpose is to understand the emotional and rational behaviour of a user and to understand how users make decisions.

How often do you feel a software update can make your system secure?

This question focuses on the effect aspect of the ARI model to identify users' trust in software updates. Respondents were expected to provide the rational and emotional reasons behind updating software to improve system security based on their knowledge and trust. This question also helped us to understand the significance to users of keeping software up-to-date for security purposes.

How often do you worry about not updating your software will make your system vulnerable for attack?

This question aims to assess both the emotional and logical aspects of the ARI model. It captures the emotional aspects by asking about concerns related to system vulnerability while also prompting the respondents to consider the logical relationship between software updates and system vulnerability.

How often do you know the reason for the software update?

This question addresses the reason aspect of the ARI model, focussing on users' reliability and understanding of software updates. Responses to this question reflected their awareness of the reasons provided by software developers for implementing updates, such as bug-fix, security patches, or feature enhancements.

How often have you had a negative experience after you applied a software update?

This question focuses on the emotional component of the ARI model by asking respondents to reflect on their feelings or experiences after installing software updates. Responses indicated that experiencing adverse or negative experiences is not unusual. Events like system crashes, data loss, or compatibility issues can cause inconvenience and difficulties, which leads to distrust of software updates.

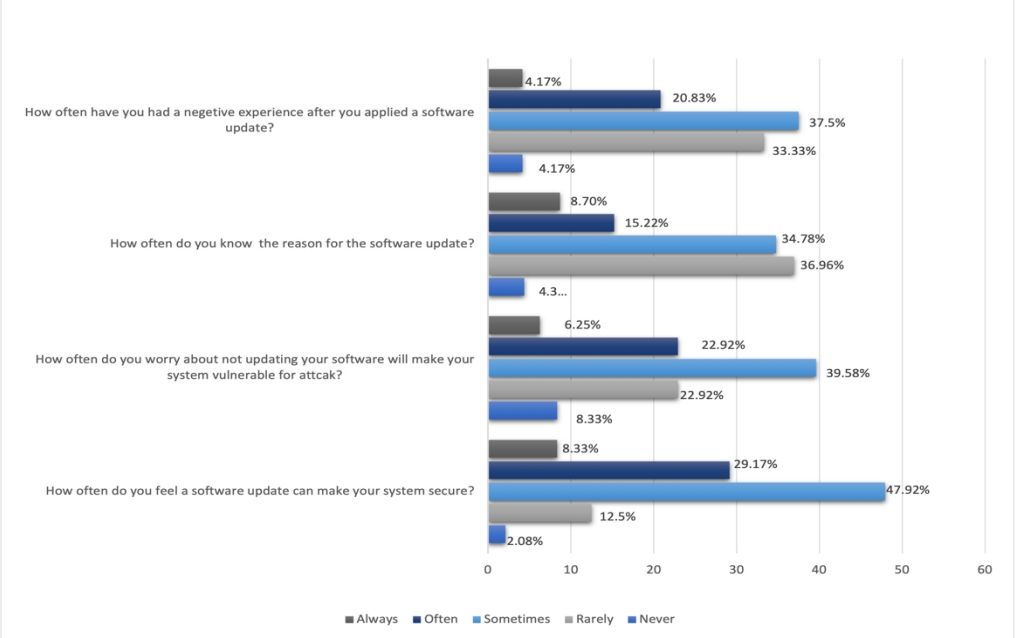

Figure 2: Users' perceptions of software updates.

Figure 2 displays our findings on the aforementioned research question two and shows the results of users' perceptions of software updates. Almost half of the respondents, 48%, acknowledge the importance of updating their software for increased security. However, the results showed that these users still have some confusion about the trustworthiness of these updates. On the other hand, a small percentage of respondents (16%) rarely or never utilize software updates. Furthermore, nearly 40% of users have had negative experiences with software updates in the past. This may explain their reluctance to rely on software updates.

DISCUSSION

Our research has revealed a range of user behaviour-related issues that require attention from software developers, vendors, or companies. The analysis of user preferences and behaviours regarding software updates for security illuminates several useful insights. Firstly, the high priority given to antivirus updates by nearly one-third of participants underscores the widely acknowledged importance of antivirus software in combating malware and ensuring system security. This prioritization reflects users' recognition of antivirus

updates as a primary defence against evolving cyber threats. The varying importance placed on different software categories highlights the complexity of security considerations. Next, respondents prioritized operating system and web browser updates over multimedia software updates for security. This indicates the need for tailored approaches to software maintenance and security based on users' differing needs and perceptions across different software domains.

Furthermore, many users showed uncertainty and hesitancy about trusting software updates, which has important implications for software development and cybersecurity practices. Addressing user concerns through enhanced transparency, communication, and user education initiatives is essential for fostering trust and confidence in update mechanisms. One of our results is aligned with (Vaniea, 2014) and found the prevalence of adverse experiences with software updates still exists. A significant number of survey participants emphasized the importance of considering user experience in software maintenance practices. Minimizing disruptions, ensuring compatibility, and providing adequate support are important for mitigating user dissatisfaction and fostering a culture of proactive software maintenance. Overall, our findings highlight the complex interplay between user perceptions, experiences, and behaviours regarding software updates for security purposes. Effective cybersecurity strategies must not only focus on technological solutions but also consider the human factor, addressing user attitudes, concerns, and preferences to provide better security.

LIMITATIONS

We acknowledge some limitations in our study. Firstly, we focused only on users running the Windows operating system and did not investigate other operating systems like Ubuntu or iOS. Secondly, our participants were mostly educated and had expertise in computers, so our results may not be representative of non-expert users. However, we did include some participants who lacked significant computer expertise. It is worth noting that all our participants identified as male or female, and we did not consider other gender identities. Nevertheless, gender was not a factor in our study and was beyond its scope. To better understand the impact of gender, further studies can expand on this topic.

CONCLUSION

In conclusion, our findings highlight user preferences and factors that influence their decisions regarding which software categories they prioritize for updates based on security considerations. Users often prioritize updates for software that is essential to run their computing systems, such as antivirus and OS updates. Though antivirus updates ranked highest, it is only contain around 29% of response. Furthermore, many users have had negative experiences and do not believe that updates can ensure or improve security, leading to a lack of trust in software updates. Achieving higher adoption rates of software updates remains an open challenge due to a persistent lack of trust.

To improve security through software updates, it is not enough to progress only on the technological front; it is also essential to develop more effective strategies to make the updates reliable and win the trust of users.

ACKNOWLEDGMENT

We would like to express our deep appreciation to the National Science Foundation (NSF) for their generous funding (NSF grant 2007662), which has been instrumental in advancing our research and contributing to the scientific community. We also express gratitude to the Human-Cantered AI research group at North Carolina A&T State University for their invaluable support in this paper.

REFERENCES

Arunesh Mathur, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. Quantifying users' beliefs about software updates. In Workshop on Usable Security (USEC), 2018.

Buck, R., Anderson, E., Chaudhuri, A. and Ray, I., 2004. Emotion and reason in persuasion: Applying the ARI model and the CASC Scale. Journal of Business Research, 57(6), pp. 647–656.

Duebendorfer, T. and Frei, S., 2009. Why silent updates boost security. TIK. ETH Zurich, Tech. Rep, 302.

Edwards, W. K., Poole, E. S. and Stoll, J., 2008, July. Security automation considered harmful?. In Proceedings of the 2007 Workshop on New Security Paradigms (pp. 33).

Fagan, M., Khan, M. M. H. and Buck, R., 2015. A study of users' experiences and beliefs about software update messages. Computers in Human Behavior, 51, pp. 504–519.

Fagan, M., Khan, M. M. H. and Nguyen, N., 2015. How does this message make you feel? A study of user perspectives on software update/warning message design. Human-centric Computing and Information Sciences, 5(1), pp. 1–26.

Fagan, M. and Khan, M. M. H., 2016. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In Twelfth symposium on usable privacy and security (Soups 2016) (pp. 59–75).

Fassl, M., Neumayr, M., Schedler, O. and Krombholz, K., 2021, October. Transferring update behavior from smartphones to smart consumer devices. In European Symposium on Research in Computer Security (pp. 357–383). Cham: Springer International Publishing.

Frik, A., Egelman, S., Harbach, M., Malkin, N. and Peer, E., 2018. Better late (r) than never: Increasing cyber-security compliance by reducing present bias. In Symposium on Usable Privacy and Security (pp. 12–14).

Fugard, A. J., & Potts, H. W. (2015). Supporting thinking on sample sizes for thematic analyses: A quantitative tool. International journal of social research methodology, 18(6), 669–684.

Haney, J. M. and Furman, S. M., 2023, May. User perceptions and experiences with smart home updates. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 2867–2884). IEEE.

Ion, I., Reeder, R. and Consolvo, S., 2015. {"... No} one Can Hack My {Mind"}: Comparing Expert and {Non-Expert} Security Practices. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (pp. 327–346).

IBM, What is the Log4j vulnerability? https://www.ibm.com/topics/log4j, 2021

Jiang, J., He, D., & Allan, J. (2014, July). Searching, browsing, and clicking in a search session: Changes in user behavior by task and over time. In Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval (pp. 607–616).

Khan, M., Bi, Z. and Copeland, J. A., 2012, October. Software updates as a security metric: Passive identification of update trends and effect on machine infection. In MILCOM 2012–2012 IEEE Military Communications Conference (pp. 1–6). IEEE.

Mathur, A., Malkin, N., Harbach, M., Peer, E. and Egelman, S., 2018. Quantifying users' beliefs about software updates.arXiv preprint arXiv:1805.04594.

Mathur, Arunesh, and Marshini Chetty. "Impact of user characteristics on attitudes towards automatic mobile application updates." In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), pp. 175–193. 2017.

Marconato, G. V., Nicomette, V. and Kaâniche, M., 2012, October. Security-related vulnerability life cycle analysis. In 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS) (pp. 1–8). IEEE

Möller, A., Michahelles, F., Diewald, S., Roalter, L. and Kranz, M., 2012. Update behavior in app markets and security implications: A case study in google play. In Research in the Large, LARGE 3.0: 21/09/2012-21/09/2012 (pp. 3–6)

Nappa, A., Johnson, R., Bilge, L., Caballero, J. and Dumitras, T., 2015, May. The attack of the clones: A study of the impact of shared code on vulnerability patching. In 2015 IEEE symposium on security and privacy (pp. 692–708). IEEE.

Nicholson, J., Coventry, L. and Briggs, P., 2018. Introducing the cybersurvival task: Assessing and addressing staff beliefs about effective cyber protection. In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018) (pp. 443–457).

National Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2021-44228, 2021.

Reeder, R. W., Ion, I. and Consolvo, S., 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. IEEE Security & Privacy, 15(5), pp. 55–64.

Redmiles, E. M., Malone, A. R. and Mazurek, M. L., 2016, May. I think they're trying to tell me something: Advice sources and selection for digital security. In 2016 IEEE Symposium on Security and Privacy (*SP)* (pp. 272–288). IEEE.

Rosen, S., Qian, Z. and Mao, Z. M., 2013, Appprofiler: A flexible method of exposing privacy-related behavior in android applications to end users. In Proceedings of the third ACM conference on Data and application security and privacy (pp. 221–232).

Sarabi, A., Zhu, Z., Xiao, C., Liu, M. and Dumitraş, T., 2017. Patch me if you can: A study on the effects of individual user behavior on the end-host vulnerability state. In Passive and Active Measurement: 18th International Conference, PAM 2017, Sydney, NSW, Australia, March 30–31, 2017, Proceedings 18 (pp. 113–125). Springer International Publishing.

Software Patching Statistics: Common Practices and Vulnerabilities, https://heimdalsecurity.com/blog/software-patching-statistics-practicesvulnerabilities/, June 23, 2022.

Symantec. Internet Security Threat Report. Network Security, 21, 2016.

Tian, Y., Liu, B., Dai, W., Cranor, L. F. and Ur, B., 2014. Study on user's attitude and behavior towards android application update notification. Usenix, Menlo Park, CA.

Tiefenau, C., Häring, M., Krombholz, K. and Von Zezschwitz, E., 2020. Security, availability, and multiple information sources: Exploring update behavior of system administrators. In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020) (pp. 239–258).

Vaniea, K. E., Rader, E. and Wash, R., 2014, April. Betrayed by updates: how negative experiences affect future security. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 2671–2674).

Vaniea, K. and Rashidi, Y., 2016, May. Tales of software updates: The process of updating software. In Proceedings of the 2016 chi conference on human factors in computing systems (pp. 3215–3226).

Vitale, F., McGrenere, J., Tabard, A., Beaudouin-Lafon, M. and Mackay, W. E., 2017, May. High costs and small benefits: A field study of how users experience operating system upgrades. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 4242–4253).

Wash, R., Rader, E., Vaniea, K. and Rizor, M., 2014. Out of the loop: How automated software updates cause unintended security consequences. In 10th Symposium On Usable Privacy and Security (SOUPS 2014) (pp. 89–104).

Zhang-Kennedy, L., Chiasson, S. and Biddle, R., 2014. Stop clicking on "update later": Persuading users they need up-to-date antivirus protection. In Persuasive Technology: 9th International Conference, PERSUASIVE 2014, Padua, Italy, May 21–23, 2014. Proceedings 9 (pp. 302–322). Springer International Publishing.