Electronic Preprint for Journal of Information Processing Vol.27

Regular Paper

# A Demographic Perspective of Smartphone Security and Its Redesigned Notifications

Jema David Ndibwile[1,a) ] Edith Talina Luhanga[2,b)] Doudou Fall[1,c)] Youki Kadobayashi[1,d)]

Received: March 12, 2019, Accepted: September 11, 2019

**Abstract:** Billions of smartphones, globally, are running out-of-date Operating Systems (OS) which make them vulnerable to cyberattacks. Behaviours of users in updating their OS vary between different geographic locations considering various demographic factors. For instance, developing countries have a very different stance compared to developed ones on how their users perceive device updates. To assert our claim, we first investigated security behaviours among different demographics in Japan and Tanzania. The results indicate that demographic factors such as culture, income, and geographic location highly impact behaviours of participants on OS updating. However, education and awareness do not seem to have significant impact on security behaviours. Consequently, insecure behaviours were equally exhibited among most participants regardless of their education levels or awareness. We also found that most participants do not update their application software on their smartphones despite being aware. Moreover, in the developing country settings, most participants tend to avoid certain security advice because they necessitate incurring data charges that take up a high percentage of their incomes. Then, we surveyed and evaluated the participants' preferences for different re-designed security notifications for improving update compliance. Finally, we propose color-coded fear-appeal designs for persuading users into updating their devices' application software.

**Keywords:** smartphone security, operating system, device updates

## 1. Introduction

The popularity of smartphones and the amount of sensitive information they store make them attractive to attackers interested in exploiting them and obtaining sensitive information [1]. Apart from exploiting common human vulnerabilities through social engineering, attackers also exploit system vulnerabilities. In smartphones, the system exploitations are typically on phones that run obsolete applications such as the Operating System (OS) [2] since these have many security vulnerabilities.

About 99.6% of new phones are Android or iOS. Android dominates the market with a 72% share [3]. However, around 1 Billion active Android devices have been running an out-of-date OS for 2 years [4], and thus the OS has many security vulnerabilities [1]. The number of iOS-based devices that are vulnerable on the other hand, ranges from hundreds to thousands [5], [6], [9]. The number of smartphone users is forecast to grow from 2.1 billion in 2016 to around 2.5 billion in 2019. Just over 36 percent of the world's population was projected to use a smartphone in 2018, up from about 10 percent in 2011 [7]. With this pace of smartphone usage, it is important to identify the reasons why most smartphone users do not upgrade their software on time or at all. Doing so, would be an effective way to build a secure mobile ecosystem.

In both human and system exploitations, there are many theories as to why users do not follow security advice or comply with security guidelines. These theories range from users' personal characteristics and preferences, such as negligence, convenience, and usability to demographic factors such as culture, education levels (non-degree, undergraduate, and postgraduate) and economy [11]. Moreover, despite numerous campaigns about security vulnerability identification and software patches release, several studies indicate that most users worldwide tend to ignore security updates on their devices [12], [13], [14]. It has also been reported that users ignore the update messages because they are too confusing or generally annoying. For instance, a study by Fagan et al. [15] suggests that computer users are reluctant to apply software updates to their machines even though they care so much about their device privacy and security.

Despite the fact that cyberattacks relying on users' naivety such as phishing are persistent [8], the cybersecurity knowledge among many users globally is still low especially in developing countries [10], [16], [17]. Previous studies have only focused on users of similar or certain demographics: permanently residing in developed countries, certain age, certain socio-economic status etc., Refs. [11], [18], [19], [20]. Joinson et al. posit that, in order to properly protect cybersecurity, it is important to integrate culture, behaviour and the design of security tools and policies [21]. Few studies [22] have attempted to explore the security knowledge and behaviours of users in developing countries especially

[1] Nara Institute of Science and Technology, Graduate School of Information Science, Nara 630–0092, Japan
[2] The Nelson Mandela African Institution of Science and Technology, The School of Computational and Communication Sciences and Engineering, Arusha 23311, Tanzania
[a)] jema.ndibwile.je8@is.naist.jp
[b)] edith.luhanga@nm-aist.ac.tz
[c)] doudou-f@is.naist.jp
[d)] youki-k@is.naist.jp

pertaining to social engineering, nevertheless the participants in these studies have primarily been of high literacy. As smartphone penetration and Internet usage continue to rise in developing countries [23], along with online financial transactions e.g., use of mobile money services [24], it is important to understand the behaviours and knowledge of users of various educational and socio-economic levels in these countries comprehensively. Furthermore, a comparative analysis of how the knowledge and behaviours in developing and developed countries differ could guide security experts on whether existing social engineering solutions such as anti-phishing programs/applications in developed countries can be effectively ported with slight adjustments to developing countries, or whether novel approaches are needed to deal with the different demographic and geographical factors of these users. Unfortunately, such kinds of research works are understudied. Our study aimed at assessing both these factors.

To gain a better insight of what solution to propose, we conducted a user study with 206 participants to examine the differences and gaps in smartphone privacy and security perceptions in both developed and developing countries. We chose Tanzania to represent a developing country and Japan for a developed one. Both countries have high smartphone penetration rates [25]. We, as authors from these countries, also have the ability to communicate in the local languages (Swahili and Japanese) and have an understanding of the socio-cultural and economic situation of the regions. We believe that Japan and Tanzania smartphone usage habits as well as demographics are consistent with those in many other developed and developing countries respectively. For instance, most developed countries have a pay as you go and a contract basis for paying for phone charges while many developing countries focus only on pay as you go. Also, education levels, incomes (earnings per month), lifestyle etc., fall into the average range for developing and developed countries.

Furthermore, our interest towards these two countries is motivated by their cyber-uniqueness. Japan has been ranked the safest country in the world, with only 2% of its computers reporting a malicious program incident [26], [27]. Meanwhile, Tanzania is one of the leading countries in the world for mobile money, e.g., M-Pesa, transactions that are steadily replacing traditional banking systems [24], [28]. We examine how different groups (e.g., those with higher education vs. those without) perceive smartphone security updates and the general aspect of cybersecurity. We seek to verify our claims that apart from reasons such as usage of low-end devices or update delays by vendors, smartphone users' behaviours in updating their smartphone applications are highly influenced by factors such as financial capability, awareness, and priority. We also study other hidden individual differences between these two countries in the context of smartphone behaviour and general security attitudes. We had four research objectives:

- To determine users' knowledge in relation to software updates such as OS and smartphone security.
- To identify users' motivations for updating their smartphone application software.
- To identify users' distractions for updating their smartphone application software.
- To determine factors that may predict users' OS update behaviours.
- To assess users' security behaviours such as password choices, phishing knowledge, Wi-Fi usage etc.

Our findings revealed that there are some security and privacy similarities and differences among participants of different demographics. Most of them are aware that software updates in general improve security, however, it does not translate into their security-conscious behaviours. In addition, we found some unique cyber-concern patterns. For instance, Japanese participants are more security-conscious than Tanzanian participants as the majority of them mentioned "*security*" as the major motivation for updating their smartphone application software while the majority of participants in Tanzania mentioned improved "*performance and user interface*" as the main motivation. Other demographic factors such as income and time affect how our participants behave towards updating their smartphone application software. For instance, the majority of the Tanzanian participants are reluctant to update their smartphone software because they tend to have a very limited mobile data plan. They would be motivated to do so if their phones would improve in terms of performance and new or fancy user interface (UI) features. On the other hand, in Japan similar behaviour is determined by the desire for new security features. However, conserving device battery power and Wi-Fi hotspots prevalence distract users from updating their smartphones instantly upon receiving a notification. Lastly, we noticed that education levels do not significantly influence users' behaviours in application software update, phishing, and password choices.

Based on our findings, we believe that users would benefit more from user-friendly and psychological appealing notifications for easy update compliance. We propose several approaches and reveal the cybersecurity gap among participants of the two countries. Our contributions are summarized as follows:

1. Extended novel notification designs which integrate security updates with other free information services for increasing security awareness and update compliance.
2. Persuasive smartphone designs for fear appeals (color-coded notifications) to increase update compliance.
3. Analytical results of cybersecurity behaviour differences between Tanzania and Japan.

## 2. Background and Related Work

### 2.1 An Overview of Devices' Software Update Notifications

In usable security, human beings are regarded as the main point of weakness in the security chain and lead to most security setbacks [29], [30]. As a result, it is difficult to automate security decisions since users must perform a part of the task such as responding to security notifications (e.g., SSL, Phishing [31], [32]). Several models have been proposed to help analyze why humans make poor security decisions and researchers have used those models to offer recommendations [33], [34], [35], [36]. For instance, users tend to ignore messages that appear too frequently and with a poor timing [34]. Also, users' decisions might be highly influenced by various factors. For example, sending a security update notification to a smartphone user can be viewed as

one way to enforce security update compliance. However, highly customized notifications that are based on individual traits and are at a user locus of attention are more likely to influence users' decisions than ordinary update notifications. Most studies focus on improving security by examining average human behaviours and offering guidance for how interfaces used by all users could be improved [14]. In that case, Egelman et al. [34] posit that there could be only an average gain of results because the improvement could only be effective to a subset of users. The improvement might only resonate with a small number of a population and not with the general population.

"*Color is present in every aspect of human life, and color is driving our decisions*" [37]. It also represents a very important design element in the digital warnings, which aim at influencing decisions and actions of users. Color appeal has an influence in behavioural intentions among people with various demographics. Unfortunately, this subject has not been fully studied in a cybersecurity perspective. Currently, most warning and notification messages are based on the "*trial-and-error*" approach rather than "*persuasion or communication theories*" [37]. According to color-in-context theory, the influence of color on affect, cognition and behaviour is a function of the psychological context in which the color is perceived [38]. However, the effectiveness of using color in security notifications and compliance to security behaviours has not been fully studied.

### 2.2 General User Characteristics on Devices' Software Update: Individually, Geographically and Demographically

In less developed settings, users typically tend to be cost-conscious with regards to their data usage due to low income, despite data charges being low or reasonable. For instance, Marthur et al. did a large-scale study of mobile data usage in South Africa [39]. They found that people tend to be cost-conscious when the data charges are unaffordable and employ different strategies to optimize their data usage, such as actively disconnecting their devices from mobile Internet. These tendencies are similar across most Sub-Saharan African (SSA) countries including Tanzania, which is under our study. Most mobile users in those countries are on pre-paid plans, and mobile service costs comprise a significant portion of their monthly income [40].

Furthermore, demographics such as age, gender and levels such as technical expertise influence security behaviours of users [11]. For instance, Garg et al. found that there is a significant difference in terms of risk behaviours and attitudes between older and younger people [41]. Similarly, a study by Sheng et al. found that women participants are more susceptible to phishing than men and participants between the ages of 18 and 25 are more susceptible to phishing than other age groups [11]. Furthermore, the evidence from several studies suggests that users' beliefs, psychology, and decision-making influence security attitudes and behaviours [34], [42], [43]. For instance, Wash et al. found that demographic differences in beliefs about security pose challenges for helping users to become more informed about security [44].

Multiple system vulnerabilities in Android phones could easily be solved by applying automatic system updates (auto-update) [45]. However, most users tend to avoid auto-update for a variety of reasons. Several studies focusing on PC software updating behaviour outline reasons for software auto-update avoidance [30], [46], [47]. In those lines of works, authors point out that users tend to avoid software auto-update due to the past negative experiences such as interface alteration and incompatibility issues. Other studies indicate that some users do not update their devices or do not set them to auto-update mode because the update messages are either confusing or they rely on free Wi-Fi due to limited Internet data plan in both mobile and PC [15], [39], [48]. Other concerns for avoiding auto-update are task interruption and device reboot necessity [30].

While most studies focus on PCs, we recognize and compliment the few other existing works focusing on smartphone users' software updating attitudes and behaviours [49], [50], [51]. However, those lines of works do not address our research questions, rather they give an insight to our study. For instance, Möller et al. found that users have a tendency of using vulnerable apps from *Google Play* for up to seven days after the patches have been released [50]. Similarly, Tian et al. studied how users make decisions in managing their Android apps and found that users consider managing apps as a non-trivial task and they would benefit more from additional information [51]. They proposed a mechanism that displays crowd sourced reviews of updated apps to help mobile users in making privacy-conscious decisions. In their most recent work, Marthur et al. realized that there are several differences that distinguish mobile users who auto-update their applications from those who do not [49]. Those differences are past negative experiences in software updates, propensity to engage in risk taking behaviours, and proactive awareness about their online security.

### 2.3 Risk-taking Behaviours: Password and Wi-Fi Usage

Most studies only point out some technical usages of public Wi-Fi related to security, privacy and behaviour [52], [53]. However, little or no user study has been concerned with policy enforcement such as terms and conditions of Wi-Fi usage. For instance, Kindberg et al. [52] only examined trust issues in Wi-Fi hotspots and realized that users willingly provided personal information to the service provider in order to access the Internet. This can be viewed as an economic rationale or as just a mere desperation of users to get connected. Similarly, Kowitz et al. [54] realized that many users do not firmly understand Wi-Fi security issues such as their data could easily be intercepted or sent in clear texts. Moreover, many other researchers pointed out the vulnerabilities related to Wi-Fi, which are technical in nature [54]. Several lines of works have demonstrated flaws and vulnerabilities in Wi-Fi hotspots that can be cracked by attackers [52], [53], [55], [56]. Wi-Fi users believe that there are sufficient protections on their systems to be secure [53] and as a result, they do not hesitate to engage in risk-taking behaviours and ignore terms and conditions established by a service provider. Surprisingly, some users believe that the potential Wi-Fi attacks will not harm them despite being aware of the risks of using public Wi-Fi [54].

Most users also tend to choose weak passwords or reuse the

same password for multiple applications [57]. Despite strict policies and guidelines about password usage, users still violate those rules for a variety of reasons such as naivety or impulsivity. Existing studies show that password perception is categorized based on either "*convenience*" or "*security*" [58]. Apart from poor knowledge about password choices, many users choose bad passwords because they are convenient to remember. Those who choose good passwords are more conscious about security. In a user study about password usage, Notoatmodjo et al. [57] realized that more than half of their participants reused their passwords on different applications because of "*password overload*" i.e., inability to handle or remember multiple passwords for multiple applications. Users tend to avoid secure passwords due to difficulty in remembering them over time because of the length and the randomness of secure password characters. Therefore, they tend to choose short and insecure passwords [59]. It makes more sense to use biometric authentication, graphical or master passwords, however, those methods somehow necessitate incurring more cost, training and prone to single point of failure. Thus, traditional alphanumeric password system remains prevalent for decades despite facing the issues related to theft or forgetfulness [60].

## 3. Part 1 of Survey Study

In this section, we show how we conducted the first part of the survey study and the subsequent data analysis and findings are shown in Section 4.

### 3.1 Recruitment

A total of 206 participants, 100 from Tanzania (69% males, 31% females, average age: 30 years, $\sigma$ = 7.15) and 106 from Japan (55.7% males, 44.3% females, average age: 33 years, $\sigma$ = 13) took part in the study. The participants were recruited online by the global market research company, Macromill Group [84] from December 1st – 28th, 2017.

Table 1 shows the proportion of participants with no degree, with an undergraduate degree, and with a postgraduate degree. In both countries, we used the same pre-screening criteria for eligible participants to take part in the survey. Questions were in a random order and translated into the two main languages spoken in Tanzania and Japan (Swahili and Japanese). Participants in both countries were compensated for their time. Participants were required to meet the following criteria to be eligible to take the survey:

- Own either an Android- or an iOS-based smartphone.
- Have experience with basic smartphone operations including OS updating.
- Be literate in English, Swahili or Japanese.
- Primarily reside in Tanzania or Japan.

We also ensured a roughly equal mix of participants with different levels of education as shown in **Table 1**.

### 3.2 Methodology

This part of the survey consisted of open-ended and multiple-choice questions about participants' knowledge, attitudes and behaviours regarding smartphone security. It also aimed at assessing participants' knowledge on the relationship between smartphone application software updates and their security, their attitudes towards those updates, and their response to update notifications. We asked our participants whether updates affect security of their smartphones. We also asked them whether they set their devices to auto-update mode, and if they did not, we asked them to provide the main reason for that. In addition, we asked what motivates them the most into either setting their devices into auto-update mode or updating their application software. We also examined their immediate reactions upon receiving update notifications. Furthermore, we asked if there are any specific reasons that hinder their choices. **Table 2** shows the summarized format of some key questions that match our objectives.

**Table 1** Participants' Demographics.

| | **Japan** | **Tanzania** |
|---|---|---|
| Non-graduate | 24.5% | 25% |
| Undergraduate | 48.0% | 49.0% |
| Postgraduate | 27.5% | 26.0% |

**Table 2** Sample Questions for Participants.

| |
|---|
| Q1. Do OS updates improve security of your smartphone? |
| Q2. Android users: Is your smartphone set into OS auto update mode? iPhone users: Do you let your smartphone automatically update its OS when no action is taken? |
| Q3. If the answer is NO for Q2, what is the main reason? |
| Q4. What motivates you the most into updating your smartphone OS? |
| Q5. Upon receiving a notification prompt for OS updating, what is your instant reaction? |
| Q6. If the answer for Q5 is either "ignore them" or "install later", what is the main reason? |
| Q7. How much is your monthly Internet plan or usage (estimate) and what is the maximum data file you are willing or likely to download for OS updates? |
| Q8. If the answer for Q7 is below 250MB, what is the main reason for that? |

We also asked the participants to rank their own cybersecurity knowledge, e.g.

1. How much do you know about information security? a) I know enough to protect my information b) I don't know c) I know very little d) I am an expert.
2. If the answer is not b), where & how did you learn about it? a) In school/college b) Self-learning c) At work place d) At workshops/conferences.

We then contrasted their responses with our own assessment based on their responses to questions about phishing knowledge, password choices, Wi-Fi usage and general cybersecurity knowledge.

## 4. Results for Part 1

All the data collected were purely nominal or ordered. We therefore used summary tables to tabulate frequencies of each response and plotted frequency graphs to visually explore the data. We also calculated summary statistics (mean, standard deviation) for the ordered data. We then applied Chi-test in order to explore

the differences in responses between Tanzanian and Japanese respondents and performed a Pearson correlation test. The test aimed to determine whether a correlation existed between self-assessed information security knowledge, actual information security knowledge and education level, age and source of information security education. The detailed results of this analysis are elaborated in the following subsections. These results are arranged based on the order of our research objectives in Section 1.

### 4.1 General findings

In both Tanzania and Japan, a majority (62.75%, $n = 129$) of the participants were aware that smartphone application software updates improve device security. However, the majority of participants in both countries (69%, $n = 69$ for Tanzania and 58.5%, $n = 62$ for Japan) had not enabled automatic OS updates which, according to several studies, is the best practice for security patches [45]. Despite the low usage of auto-update, the majority of Android participants in both countries (84%, $n = 42$ out of 50 in Tanzania and 86.84%, $n = 33$ out of 38 in Japan), and the majority of iOS participants in Japan (82.61%, $n = 19$ out of 23) currently have an OS version that is supported. In Tanzania, however, most iOS participants have an unsupported OS version (54.54%, $n = 12$ out of 22).

### 4.2 Motivation for updating OS (Motivators)

This subsection introduces the findings of our second objective which highlights the main reasons that motivate the participants of both countries to update the operating systems of their smartphones.

As indicated in **Fig. 1**, in Japan, around 33% of smartphone participants are primarily motivated to update their OS due to security reasons, which is a significantly higher percentage than participants in Tanzania (16%) ($p < 0.001$, Welch's t-test). Another 30% install updates because they view them as generally important, and 21.7% install updates to acquire better performance. In Tanzania meanwhile, the top two motivators for updating the OS are to get an improved user interface (38.6%) and better performance (23.9%), with only 16% updating primarily for security reasons. Another 17% of participants view updates as generally important.

### 4.3 Distraction for updating OS (Distractors)

This subsection describes in details the main reasons for the participants to avoid updating the operating systems of their smartphones.

As depicted in **Fig. 2**, financial consideration is the main reason participants avoid auto-update in Tanzania. In Japan meanwhile, participants are generally ambivalent towards timely (immediate) updating with 24.2% explicitly stated that "*updates are not a priority*" while others seem to imply the same by viewing auto-update as troublesome, not bothering to change the default settings, and viewing updates as less important than conserving battery power.

Only around 14% of participants in Japan, and 13% of participants in Tanzania, choose to instantly install OS updates when notified, while 16% of participants in Japan and 11% in Tanzania

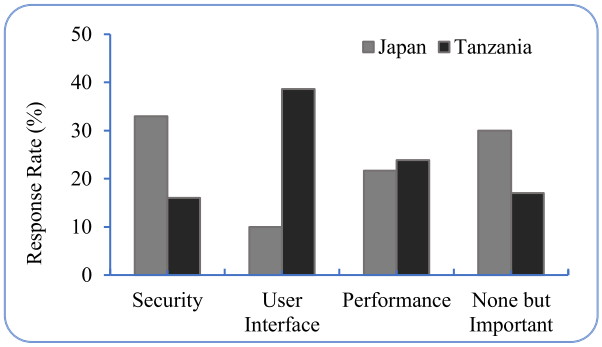



**Fig. 1** Motivators for OS updating.

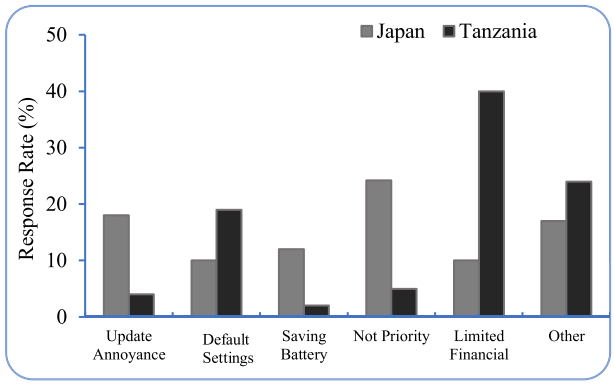



**Fig. 2** Reason for avoiding auto-updates.

completely ignore the notifications. Generally, the majority of participants in Tanzania (43%) check the remaining mobile data or the update file size before making a decision about updating their OS. A majority of the participants (58%) reported being comfortable spending 250 MB or less of their mobile data plan on these updates, while another 28% were willing to spend 500 MB–2 GB of their data plans. About 30% were willing to spend 2 GB or more.

Meanwhile in Japan, participants were significantly less concerned about the data usage or the size of the update file compared to those in Tanzania ($p < 0.001$, Welch's t-test), with only 12% consider these two factors. However, most of them (30.5%) opt to delay installing OS updates due to distractions from other activities on their phones e.g., conserving battery during transit (12%) or waiting for Wi-Fi connection to update their devices (10%). In Tanzania, where Wi-Fi is not as prevalent as in Japan, only 2.8% choose to delay updates until they are connected to free Wi-Fi.

### 4.4 Statistical significance for updating behaviours

By auto-update behaviour, we hereby refer to it as a tendency of a user to set her device into automatic update mode for application software. Similarly, by instant-update behaviour, we hereby refer to it as a tendency of a user to update her device immediately after she receives the update notification.

We summarize the variables that may have impacts on users' behaviours in updating their smartphones' OS as follows.

In a one-way Multivariate Analysis of Variance (MANOVA), results indicate that income and motivators have a statistically significant impact on auto- and instant-update behaviour for both countries ($p < 0.001$, Hotelling Lawley test). Tanzania has sim-

**Table 3** Multivariate analysis of variance (one way).

| Coefficients | Value | F | Hypoth dif | Sig |
|---|---|---|---|---|
| *(Intercept)* | 11.296 | 474.4 | 2.000 | 0.001 |
| Education | 0.030 | 0.615 | -4.000 | 0.652 |
| Income | 0.467 | 3.23 | 12.000 | 0.001** |
| Distractor | 0.059 | 0.817 | 6.000 | 0.558 |
| Motivator | 0.324 | 04.47 | 6.000 | 0.001** |

*Summary:* The *Sig* column indicates significance level of the data where the two asterisks mean the variable data has higher significance level where $p < 0.001$. *F* column is another statistic test for checking whether means between two populations are significantly different. *Hypoth dif* column is the number of degrees of freedom in the model and *Value*-column represents test statistics.

ilar results i.e., income together with motivators have a statistically significant impact on auto- and instant-update behaviour ($p < 0.001$, Hotelling Lawley test). However, with the same test we found that distractors and education levels have no significant impact on the same behaviour ($p > 0.05$) in Tanzania. In Japan, only a motivator variable has a statistically significant impact on both auto- and instant-update behaviour ($p < 0.001$, Hotelling Lawley test), while education, distractors and income have a low or no statistically significant impact ($p > 0.05$). **Table 3** shows a summary of a one-way MANOVA of independent variables over continuous dependent variables (auto- and instant-update) for both countries.

### 4.5 Participants Assessments on Privacy and Security Knowledge

Privacy seems to be important for a vast majority of participants in both countries, and this is reflected by the high proportion of participants who use screen lock authentication on their smartphones (80% in Tanzania, 80.2% in Japan). However, in both countries, self-confidence on privacy and security knowledge was average. Around half of participants, 49% in Tanzania and 51.9% in Japan, felt they did not know enough about information security, and around a quarter of them, 26.1% in Tanzania and 26.4% in Japan, felt that they knew just enough to protect their data, $p < 0.001$ Student's t-test.

Our assessment of information security knowledge (characteristics of strong passwords, email phishing awareness and other online behaviours) revealed participants' self-assessment on their knowledge levels is probably accurate. Overall, only 34% of Tanzanian and 18% of Japanese participants managed to identify the strongest password correctly in the multiple-choice questions. The significant number, $p < 0.001$ Student's t-test, of both Tanzanian and Japanese participants chose the longest password instead of the one with at least a minimum of required length and with the combination of all important characters such as variation of letter cases, numbers, and special characters. **Figure 3** shows the password choices of the participants.

A significant number of participants in Tanzania were also likely or very likely, 48% and 20% respectively, to open links from unknown emails and 3% were not sure, meaning a majority are susceptible to phishing attacks. Although most Japanese participants, 60%, were unlikely to open such links, more than a quarter (33%) were still likely to do so, 0.9% very likely and

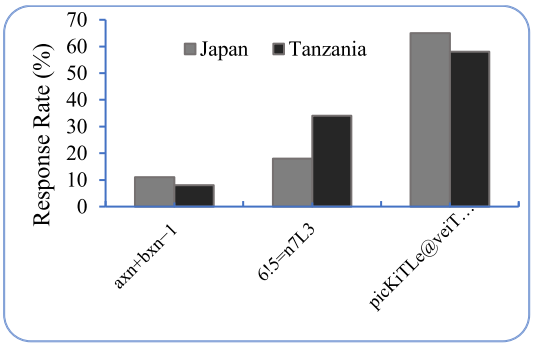



**Fig. 3** Participants' concept of a strong password.

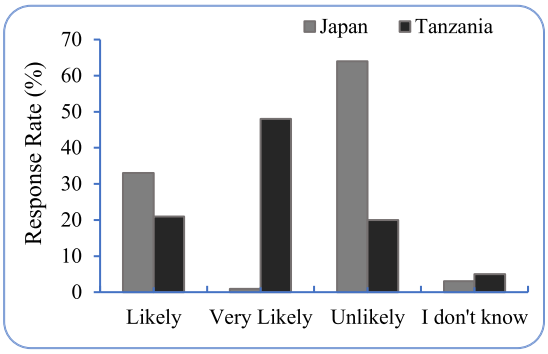



**Fig. 4** How likely a participant would open an email attachment from unfamiliar source or sender.

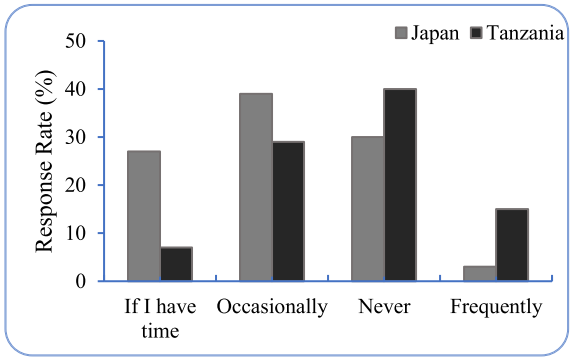



**Fig. 5** How often the participants read Wi-Fi terms and conditions on public network connections?

5% unsure, which is also a significant number of participants ($p < 0.001$, Student's t-test). **Figure 4** summarizes the knowledge of the participants pertaining to phishing.

As indicated in **Fig. 5**, in both countries the number of participants who read public Wi-Fi terms and conditions on a daily basis was significantly low, 12% in Tanzania and 2.8% in Japan ($p < 0.001$, Student's t-test). However, Japanese participants were more likely to read the terms when they had free time (26.4% vs. 6.8% of Tanzanian participants) or on an occasional basis (29.5% vs. 39.6% of Tanzanian participants). Few participants, 35%, were aware that they are responsible for data breaches on public Wi-Fi. In such situations, most Japanese participants, 46.2%, would blame themselves while most Tanzanian participants, 34.1%, would either not know whom to blame or, 28.41%, would blame a service provider. In general, users could easily understand the risks associated with public Wi-Fi usage if they could read terms and conditions for the subsequent Wi-Fi connection.

**Table 4** Likert Scale about Information Security Education.

| Question | Tanzania | | Japan | |
|---|---|---|---|---|
| Mean & Standard Deviation | μ | σ | μ | σ |
| 1. People ought to receive information security education | **3.85** | 1.18 | **4.03** | 0.77 |
| 2. Individuals ought to teach themselves about info security | **3.53** | 1.21 | **3.88** | 0.81 |
| 3. I would like to be taught about information security | **4.17** | 0.85 | **3.66** | 0.88 |
| 4. Cybersecurity education is not needed if security software is used | **2.68** | 1.41 | **2.34** | 1.05 |
| 5. I would like to receive security tips about my smartphone | **4.12** | 0.93 | **3.83** | 0.82 |

*Scale: 1-Strongly disagree, 2-Disagree, 3-Neutral, 4-Agree, 5-Strongly agree.
*Data significance, Tanzania: $p = 0.0020$, Japan: $p = 0.0025$, Chi-square t-test.

Terms and conditions seem trivial because users do not face the consequences immediately, however apart from that, language barrier could be one of the reasons that people do not bother to read them. It might not be the case in Japan where the native language, Japanese, is used for almost everything whereas in Tanzania, this is likely the major factor. English being the official language means all official documentations are in English, which favours only the few who are elites.

In Tanzania, among all participants who claimed to have knowledge about information security, 58% learned about it by themselves through online articles, news and other resources. However, 35% acquired it from schools, colleges and universities. The remaining percentage (4) acquired the knowledge from work places through various capacity building programs. Unlike in Tanzania, in Japan, among all participants who claimed to have knowledge about information security, only 29.4% learned about it by themselves through various ways such as the Internet. About 67% learned about information security at schools, universities and workplaces. Among participants with no university degrees, the majority of them, 73.7%, learned about information security by themselves, the remaining 26.3% learned about it at schools, work places and by other means. Overall, the number of participants who rated themselves low in information security knowledge is significant (49% in Tanzania and 52% in Japan), while a small number of the participants know just enough to protect their data.

In questions 3 and 5 of **Table 4**, participants were asked whether they would like to receive or to be taught about information security. Tanzanian participants showed higher desire to acquire such knowledge than the Japanese participants did. This phenomenon is the evidence of the information-security knowledge gap between the two countries as verified on the global cybersecurity indexes by ITU 2017 report [61].

We used non-parametric test (Chi-square test) to categorically (Tanzania vs. Japan) compare the participants' responses in Likert scale numbers. More participants in Japan than in Tanzania generally believe that people ought to receive information security education, $\mu$ (4.04 vs. 3.85). Although the difference is marginal, in Japan, information-security education facilities and policies are more structured than in Tanzania, thus this concept is more realistic and practical in Japan than it is in Tanzania. As a result, more participants in Japan than in Tanzania, $\mu$ (3.9 vs. 3.5), believe that people ought to seek and teach themselves about information security. However, both Japanese and Tanzanian participants disagree that information security is unnecessary when security software is used ($\mu = 2.3$), in which Japanese participants disagree more, $\mu$ (2.3 vs. 2.7).

## 5. Part 2 of Survey Study

### 5.1 Overview

We propose redesigned smartphone security notifications for OS update compliance. The proposed notifications are intended to persuade users into complying with the provided security advice. The notifications initially come to the attention of the users as a social information service with the security advice embedded. Our goal is to have notifications that are less compelling and nagging than the existing ones. Thus, we design our notifications to give a user much more freedom of choice such as accepting or rejecting them. They also provide an option on how frequent a recipient would wish to receive them. As a second part of the survey, we tested the preference of our notification mock-ups with the same participants of the first part of the survey (Ref. Section 3.2).

### 5.2 Methodology

We provided 5 pairs of the security notification mock-ups to each participant. Each pair had two options for a participant to choose. The mock-ups specifically intend to simplify the update process, warning users about malicious updates/apps, and providing extra information with the consideration of a source credibility. We included the information that guides a user on how to perform a certain task such as updating the OS, together with the counterpart notification without such information. We also designed other mock-ups that give a control to the users on how frequent they would like to receive them. We asked the participants to choose their preferred security notification designs compared with ordinary or plain notifications. In summary, the notifications showed participants:

- Different information services, such as real-time traffic updates, weather information and news headlines that could be integrated with ordinary update notifications.
- Different messages to warn users of the risks of running an out of date application software, where to get further information, and how to update the current software.
- Different subscription/unsubscribe options.

We chose these types of information services because we believe they could positively affect and benefit the majority of the recipients based on the relevance of their geographic locations.

## 6. Results for Part 2

At every pair of mock-ups, we show a visualized graph of the participants' preferences.

### 6.1 Mock-up 1

**Figure 6** shows a first pair sample which comprised of two

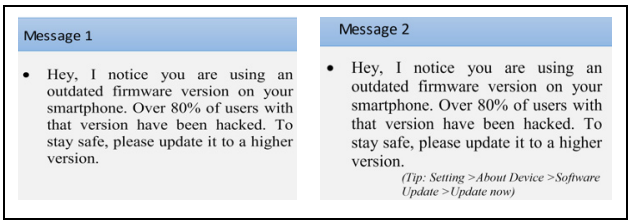



**Fig. 6** Tip on how to update a devices' application software.

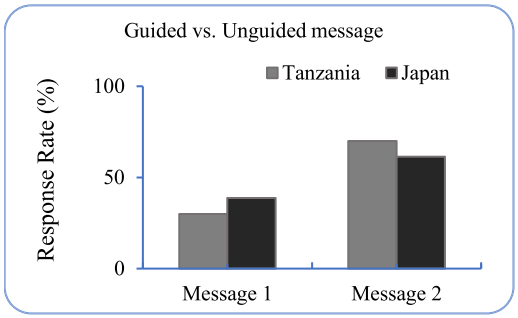



**Fig. 7** Participants' preferences for notification mock-up 1.

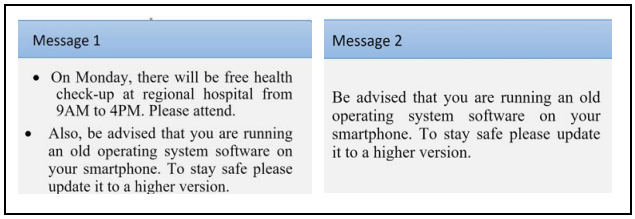



**Fig. 8** Information service on top of security advice.

notifications. The first notification (Message 1) informs a participant about her outdated application software and the consequences of not updating it. However, it does not tell the participant, for instance a novice one, on how to perform the update. On the contrary, the second notification (Message 2) contains the same message with additional information, i.e., a tip of how the participant can update her device by following the outlined procedure.

**Preference**: Most participants in both countries chose the notification (Message 2) that has a tip on how to perform the actual update and claimed that it is more appealing and persuasive than the first notification (Message 1) as shown in **Fig. 7**.

### 6.2 Mock-up 2

**Figure 8** shows a second pair sample which comprised of two notifications. The first notification (Message 1) informs the participant on details about free health check-up at a regional hospital and advices her to attend. Meanwhile the same message explains about a potential vulnerability that may be present on the device due to the outdated version of application software running on the device. On the contrary, the second notification (Message 2) only advices the participant about a potential vulnerability due to an outdated application software running on the device.

**Preference**: The most expected choice on this result outcome would obviously be Message 1 which gives the participant a benefit of extra information on top of the security advice. However, most Japanese participants (61%) chose Message 1 while most

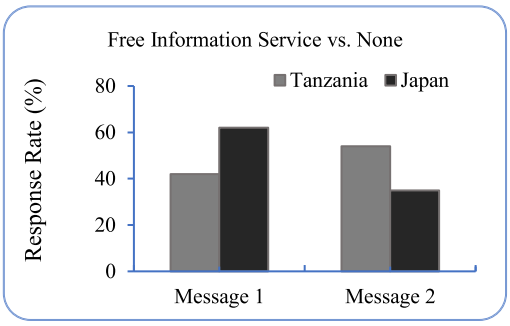



**Fig. 9** Participants' preferences for notification mock-up 2.

Tanzanian participants (52%) chose Message 2 as indicated in **Fig. 9**. The rationale in this case would be the fact that the two countries have different healthcare systems. The reality and practicality of the service might have influenced the participants' preferences.

**Rationale**: The two countries have quite different healthcare systems that may have influenced the participants' preferences in this case. For instance in Japan, even though the healthcare system requires a patient to contribute some percentage, the annual health check-up is provided for free to employees and students [79]. Meanwhile the Tanzanian one requires a patient to pay unless she is fully covered by the insurance [76]. Thus, the free check-up notification could have not resonated beyond doubt among the Tanzanian participants. In Tanzania, the National Health Insurance Fund (NHIF) was established by the Act of Parliament No.8 of 1999 and began its operations in June 2001. The scheme was initially intended to cover public servants. It's only recently there have been some provisions which allow private membership [75]. However, the coverage is still low according to the global innovation lab, UNLESH and WHO [75], [77]. As of June 2013, the NHIF was estimated to be covering about 6.6% while Community Health Fund (CHF) covers about 7.3% of the population based on 2012 Census [75]. Other prepayment schemes cover less than 1% of the population [76]. On the contrary, Japanese healthcare system provides its services with the patient accepting responsibility for 30% of these costs while the government pays the remaining 70% [78], [80]. Payment for personal medical services is offered by a universal health care insurance system that provides relative equality of access, with fees set by a government committee. Moreover, all residents of Japan are required by the law to have health insurance coverage. People without insurance from employers can participate in a national health insurance programme, administered by local governments. Patients are free to select physicians or facilities of their choice and cannot be denied coverage. Hospitals, by law, must be run as non-profit and be managed by physicians. For-profit corporations are not allowed to own or operate hospitals. Clinics must be owned and operated by physicians [78], [79], [80].

### 6.3 Mock-up 3

**Figure 10** shows a third pair sample which comprised of two notifications. The first notification (Message 1) advises the participant about the usage of alternative road route due to traffic jam on a usual route. Meanwhile, the notification gives security

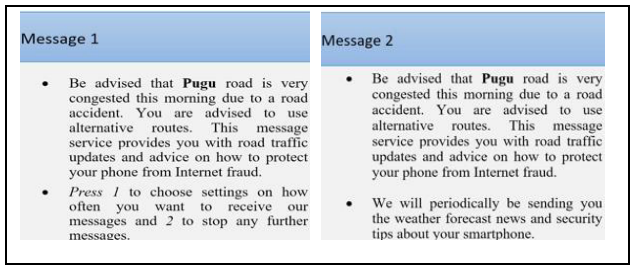



**Fig. 10** A control over how to receive a notification.

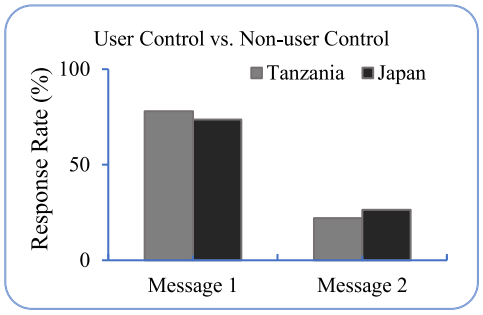



**Fig. 11** Participants' preferences for notification mock-up 3.


**Fig. 12** Government vs. general domain notification source.

advice to the participant and an opt-out or frequency option for future notifications. That means the participant has control on how often she wants to receive those kinds of notifications. The second notification (Message 2) gives no option to the participant and it is one of those typical kinds of nagging messages that most users dislike.

**Preference**: Most participants in both countries, as indicated in **Fig. 11**, chose Message 1 that gives them either control over how frequent they would like to receive those messages or an option to not receive them at all.

### 6.4 Mock-up 4

**Figure 12** shows a fourth pair sample which comprised of two notifications. The first notification (Message 1) advises the participant to update her application software to the latest version. The notable aspect of this notification is the source. The source indicates that it is a government entity, hence the "*.go*.", on the URL. The second notification (Message 2) indicates that the source is a commercial website domain, "*.com*".

**Preference**: It is easier to trust government sources than the "*.com*" URLs. However, this notification resonated more with Tanzanian participants because the "*.go.tz*" is the domain for Tanzanian government, thus it is familiar to them. Japanese participants probably were not sure what the "*.go.tz*" is, hence they preferred the domain that is familiar to them (Message 2) among the two as shown in **Fig. 13**. This case is one of the reasons why we

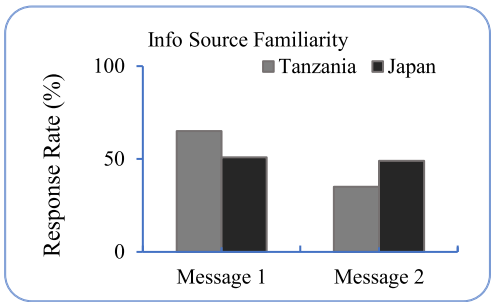



**Fig. 13** Participants' preferences for notification mock-up 4.

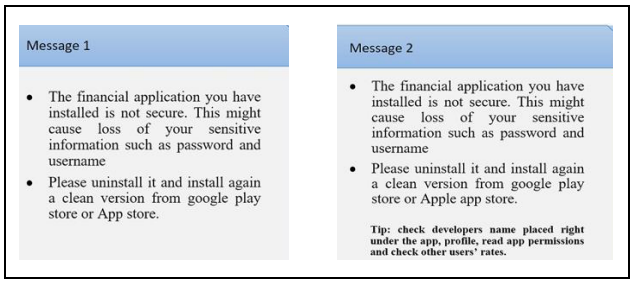



**Fig. 14** The notification with the guidance on how to identify a malicious application against the one without the guidance.

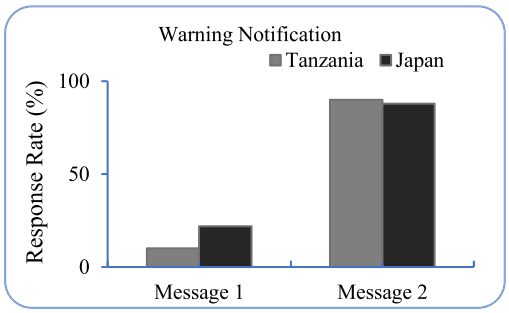



**Fig. 15** Preferences for notification mock-up 5.

ought to have different notification designs catered for a specific group of users instead of a general notification and expecting the same level of compliance.

**Rationale**: Government documents and government websites are generally considered authoritative and credible sources of information [81]. Many are scholarly, and some are even peer-reviewed. However, not all government orders are elite or peer-reviewed. Government agencies provide various publications, for different purposes. Depending on the instructions of your research, assignment, or any other purpose, some documents may be better than others but generally are more reliable [85], [86].

### 6.5 Mock-up 5

**Figure 14** shows a fifth pair sample which comprised of two notifications. The first notification (Message 1) warns the participant of a potential malicious transaction app that the participant might have downloaded from an unverified source. Message 2 does the same as Message 1 but with additional information that enlightens the participant on how to identify a malicious app.

**Preference**: This result is probably much anticipated regardless of other demographic factors. Most participants with a very basic understanding of smartphone operations would choose Message 2 which alerts and guides the participant about a mali-

cious app her device is running as shown in **Fig. 15**.

## 7. Color-coded Fear appeals Proposal

In this section, we propose the color-coded fear appeals for persuading users into updating their smartphones' OS. As suggested by the results in Section 4, few participants are generally motivated by the security reasons to update their OS. Other participants are more willing to update their devices' OS if they would benefit from features other than security. Moreover, some participants didn't know how to check their OS versions, thus they may not be able to associate the version number with certain vulnerabilities. Therefore, we believe that the color-coded fear appeals might be a better way to persuade such kinds of users to update their devices' software. We believe that a mere statement about a device vulnerability may not be as effective as a visual statement such as a color-coded warning.

### 7.1 Overview

As we discussed earlier, the security meltdown of a phone could be due to many factors such as;

- Self-inflicted: clicked a wrong link or app.
- Running an out-of-date or latest vulnerable version.

Despite the fact that most outdated OS versions are vulnerable, recently it has been revealed that even some newest versions are vulnerable [62]. However, those newest versions' vulnerabilities are due to manufacturers who accidentally or purposely put a bug into both Android and iOS [5], [6], [62].

To persuade users into making quick decisions on the software update of their devices, from the psychological point of view, we propose color-coded fear appeals that indicate the status of an OS. Hypothetically, it is easy to be conscious on making a quick decision if a certain color presented on your device indicates a certain level of threat. For example, an indicator of device battery power. The power level diminishes gradually until the device goes off. Most users would immediately react by charging their devices unless they do not have the means. They would do so because they know the consequences of ignoring the indicator. Thus, a visual indicator can help us know the level of risk of the devices. If smartphones and other devices had no battery power visual indicator like in **Fig. 16**, it could be difficult to anticipate or predict when the device goes off.

It is critical for smartphone users to take precaution against threats which may come from adversaries or their own negligence. Previous studies indicate that smartphone users lack good security awareness and proper adoption of its controls. Demographics such as ethnicity, language, and gender are associated with adoption of security controls. Thus, it is necessary to use a *simple* and *non-technical* design for encouraging the widespread awareness and adoption of those controls [63]. Since a good number of participants neither knew how to check the OS version nor to interpret its vulnerability severity, waiving off this users' effort could catalyze the update compliance. And this could be done programmatically by retrieving OS version and associating it with its safety level.

**Fig. 16** Variations of smartphone battery power levels [74].

**Table 5** Western color stereotypes [64].

| Color | Stereotypical Meaning |
|---|---|
| Red | hot, stop, aggression, *error, warning,* fire, daring |
| Yellow | happy, sunny, cheerful, slow down, *caution* |
| Green | envy, jealousy, a novice, spring-like (fertile) |

**Fig. 17** Preliminary prototype for OS fear appeals.

### 7.2 Color Stereotypes and Perceptions

Colors are perfectly suitable to boost the visual appeal of various products such as software and ads. Often, people associate certain colors with a specific meaning as shown on **Table 5**. These stereotypes can suitably be leveraged when designing a UI.

However, these stereotypes may not be relevant to every demographic. Different people from different demographics have different stereotypes on these colors. For instance, the colors in Table 5 are cultural-dependent, they are more prevalent to the western culture than they are to the rest of the world. For instance, red means "*death*" in Egypt whereas it means "*creativity*" in India, and "*happiness*" in China [65]. However, red is still universally known to attract attention, thus it can be used as a negative or positive connotation depending on where it is used (industry, medical, infrastructure, personal etc.).

### 7.3 Proposed Design

We propose that the status of OS security be displayed on a top rectangular bar of a device's screen with a relevant color. For instance, four different colors of a perceived level of threat severity can be used based on the current OS version running on a smartphone as indicated in **Fig. 17**.

Each color indicates a level of security of the OS in an orderly manner. Suppose, one of the latest two versions of OS is running on a device, it can be presented by a bar/icon showing green color. According to most emergency systems such as Healthcare - color code warning system [66], color-coded threat level advisory under attack for homeland security and others [67], the standard colors used are depicted as shown in **Fig. 18**.

We adopt the same color patterns as they are universally accepted in emergency situations. The level of threat or safety could trigger the OS visual bar to display a relevant color as shown in **Fig. 19**.


**Fig. 18** The US department of homeland security color scheme for threat-level system [67].


**Fig. 19** Design "A" for smartphone update fear appeals.

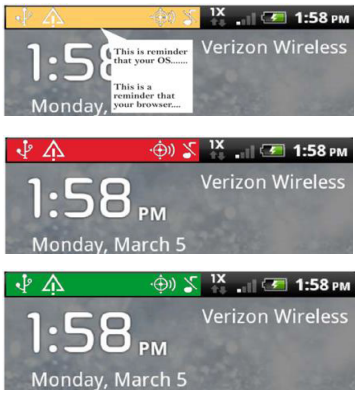



**Fig. 20** Design "B" for smartphone update fear appeal.

**Counter Argument**: Despite having an android icon to represent the status of security level of a device's Operating System, there could be other unrepresented obsolete applications within a device such as a Web browser. Furthermore, there could be an OS other than Android, e.g., Apple, Windows, Blackberry etc. It could be tedious to have a custom design for every device and for every application software. Nevertheless, the designed icons can easily be confused with the battery power icons since they are somehow similar in appearance and colors as it appears in Fig. 19.

**Alternative Design**: Following the above counter argument, a quarter or a half bar changing color can be used instead and could be more consistent with any smaller device. The bar could be flashing periodically and go to indicate a certain status of an application. It can either flash with text or present itself as a clickable bar that can open up in a small window explaining the issue associated as presented in **Fig. 20**.

## 8. Discussion and Future Work

### 8.1 Design Issues

We made simple message windows for summarized contents. We avoided long messages as many users would not like to read long sentences. As a result, we ended up having texts with very small font sizes. To improve the style of the notifications, the message window can be enlarged so as to have large text fonts. Furthermore, important information within texts such as key words is advised to be bolded or italicized to make it easy for the reader to quickly understand the theme of the message [82], [83]. For instance, "*road **X** has **congestion***", "*use alternative route*", "*please **update your device***."

### 8.2 Compliance Issues

Based on our results on OS update behaviour, immediate compliance is difficult. A time frame during which response is desired should be set e.g., 24–48 hours. During this time, efforts to educate a user on the security updates through system notifications should be provided. Moreover, at this point, our designed color-coded fear appeals can be utilized to subtly remind a user of the need to act.

Furthermore, to minimize the barriers to updates e.g., altered interfaces, OS updates can be redesigned to allow users to opt out of downloading or installing certain modules e.g., performance, UI but make security ones mandatory. Normally, current update notifications are too generic which include security, improved performance, improved UI etc., thus the update file tends to be very huge (200 MB up to 1 GB). In this case, the security module can be made mandatory and other modules being optional to waive off download issues which is one of the barriers to updates.

### 8.3 Demographics Factors

Despite the ambivalence in OS update among Japanese participants, security is still viewed as an important aspect by more participants than those in Tanzania. Some reports indicate that online users are highly conscious and concerned about the potential risk in online activities due to technology advancement and e-commerce prevalence [71]. Meanwhile in Tanzania, where technology is less advanced and with little usage of e-commerce [50], fewer Internet users might be conscious about security practices than Japanese users. This phenomenon can be attested by the 2017 ITU's Global Cybersecurity Index (GCI), where Tanzania scores 0.317 and ranked 88th globally while Japan scores 0.786 and ranked 11th globally [61]. Furthermore, our survey results indicate that significantly more Japanese participants than Tanzanians avoided updates in order to conserve their smartphone batteries. We believe this may be due to the different smartphone usage and phone ownership behaviours in the two countries. With mobile game industry being the biggest source of App economy in Japan, studies show that much of the time spent on smartphones is on mobile games and video streaming [72], which might be the biggest concern for battery power.

As previously mentioned, Japanese smartphone users tend to have access to high-bandwidth, the majority of them can afford such data plans. However, the data are mostly spent when the users are away from public or private Wi-Fi hotspots.

In Tanzania on the other hand, owing to limited data plans, much of the time spent on smartphones is in perusing light web contents on social media [73], which consume much less battery power. Many users also periodically turn off their data when not

browsing, in order to avoid background uploads and downloads, which take up a big portion of their pre-paid bundle [39]. This behaviour also limits battery power consumption.

### 8.4 Extended Applicability

A search engine like Shodan [68] has the ability of retrieving a lot of information from multiple online devices without compromising them. It is mostly used for research in cybersecurity around the Internet of Things (IoT) and other small-sized smart devices, since there are billions of them online that 1) have specific vulnerabilities that need to be fixed, and 2) can be identified quickly by their banner information [69]. With the use of filters, Shodan can display banners with specific information such as city, country, geo coordinates, hostname, Internet Protocol (IP) address, port number, operating systems etc.

Japan is the first country to pass a law that allows the National Institute of Information and Communications Technology (NICT) to scan IoT devices with generated user IDs and passwords and warn owners of breached devices to bolster their security. Although controversial, the idea has some merits in that, it allows at-risk users to be notified earlier. The re-designed notifications we presented earlier, as well as color-coded fear appeal concept, can be applied to make the notifications issued more persuasive to users.

Alternatively, government agencies such as CERT (Computer Security Emergency Response Team) in Japan [70] and/or telecommunication network operators could issue notifications with statistics on the estimated number or percentage of vulnerable devices within the geographical location that a user is in. The user could then be prompted to either choose 1) having their device's vulnerability scanned for them or 2) be directed via link to a page on the official agency's website that teaches users on how to scan and assess their devices' vulnerabilities through Shodan.

As we explored in our survey, source of information matters to recipients, i.e., government agencies seemed to be more reliable [81]. Thus, agencies such as CSERT that are predominantly owned by governments in various countries would make more impact to the recipients in terms of compliance. Moreover, this concept can be extended and applied beyond mobile devices. It can be applied to vulnerable software/platforms such as web/email applications, protocols, SSL certificates etc.

### 8.5 Limitations and Future Work

Our survey focused on analyzing the behaviours and the proposed design preferences based on the self-reported data. We cannot confirm the accuracy of these data. Also, our sample was limited to 206 participants which may not reflect the general population. Thus, we are limited to make a firm conclusion based on these results. In the future, we intend to test the effectiveness of the color-coded fear appeals and the redesigned notifications in a real-situation experiment with more participants.

## 9. Conclusion

In a nutshell, in the realm of personal computers, the security awareness of users is relatively higher than in smartphones. The skills needed by a user to interact responsibly with her smartphone is very different from those needed to interact with personal computers. Therefore, evaluating various reasons for different behaviours of smartphone users and advocating the security awareness can be an effective method for mitigating various cyberattacks on those devices.

Thus, we investigated the security perceptions, attitudes and behaviours among different smartphone users in Tanzania and Japan. We assessed the participants' preferences for our redesigned warning notifications to realize important persuasive aspects towards update compliance. We also proposed color-in-context theory for smartphone application software status. We believe that color is an important antecedent for persuading a user into making a quick and sound decision on her smart device.

Furthermore, we realized some similarities and differences in both countries. The majority of the participants are equally aware that software updates improve security, however it does not translate into their security-consciousness levels. Additionally, we found that Japanese participants were more security-conscious than Tanzanian participants as most of them mentioned "*security*" as the major motivation for updating their smartphone OS while the majority of participants in Tanzania mentioned improved "*performance and user interface*" as the main motivation. Thus, in Tanzania, income and motivators such as improved user interface and performance predict whether a user will update her smartphone OS, while in Japan similar behaviour is predicted by the desire for new security features.

Additionally, in Japan conserving a device battery power and Wi-Fi hotspots prevalence may distract users from updating their smartphones instantly upon receiving a notification while in Tanzania this behaviour is again determined by the income. Overall, auto-update behaviour is dictated by income and motivators for both countries, while instant-update behaviour is dictated by distractors only.

Lastly, we noticed that education levels do not significantly influence users' OS update behaviours for their smartphones.

### References


[1] Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L. and Shabtai, A.: Taxonomy of mobile users' security awareness, *Computers & Security*, Vol.73, pp.266–293 (2018).

[2] Lange, M., Liebergeld, S., Lackorzynski, A., Warg, A. and Peter, M.: L4Android: A generic operating system framework for secure smartphones, *Proc. 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pp.39–50, ACM (2011).

[3] 99.6 percent of new smartphones run android or iOS, available from ⟨https://www.theverge.com/2017/2/16/14634656/android-iosmarket-share-blackberry-2016/⟩ (accessed 2018-01-17).

[4] 1 billion android devices are more than 2 years out of date, available from ⟨https://www.extremetech.com/mobile/258998-1-billionandroid-devices-two-years-date/⟩ (accessed 2017-10-12).

[5] Hundreds of iOS apps leaking data due to misconfigured Firebase backends, available from ⟨https://appleinsider.com/articles/18/06/29/hundreds-of-ios-apps-leaking-data-due-to-misconfigured-firebase-backends-report-says/⟩ (accessed 2018-03-27).

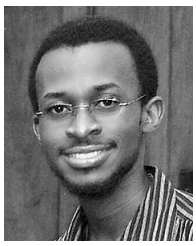
[6] Programming Error Exposes Thousands of iOS Apps to Hijacking, available from ⟨https://www.pcmag.com/news/361270/programming-error-exposes-thousands-of-ios-apps-to-hijacking/⟩ (accessed 2018-03-27).

[7] Number of smartphone users worldwide from 2014 to 2020 (in billions), available from ⟨https://www.statista.com/statistics/330695/number-ofsmartphone-users-worldwide/⟩ (accessed 2017-02-12).

[8] Ndibwile, J.D., Kadobayashi, Y. and Fall, D: UnPhishMe: Phishing Attack Detection by Deceptive Login Simulation through an Android Mobile App, *2017 12th Asia Joint Conference on Information Security*

(*AsiaJCIS*), pp.38–47, IEEE (2017).
[9] Ndibwile, J.D., Luhanga, E.T., Fall, D., Miyamoto, D. and Kadobayashi, Y.: Smart4Gap: Factors that Influence Smartphone Security Decisions in Developing and Developed Countries, *Proc. 2018 10th International Conference on Information Management and Engineering*, pp.5–15, ACM (2018).
[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, *Proc. 2nd African Conference for Human Computer Interaction: Thriving Communities*, p.17, ACM (2018).
[11] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J.: Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.373–382, ACM (2010).
[12] Egelman, S., Cranor, L.F. and Hong, J.: You've been warned: An empirical study of the effectiveness of web browser phishing warnings, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.1065–1074, ACM (2008).
[13] Vaniea, K.E., Rader, E. and Wash, R.: Betrayed by updates: How negative experiences affect future security, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.671–2674, ACM (2014).
[14] Wash, R., Rader, E., Vaniea, K. and Rizor, M.: Out of the loop: How automated software updates cause unintended security consequences, *Symposium on Usable Privacy and Security* (*SOUPS*), pp.89–104 (2014).
[15] Fagan, M., Khan, M.M.H. and Buck, R.: A study of users' experiences and beliefs about software update messages, *Computers in Human Behavior*, Vol.51, pp.504–519 (2015).
[16] Kortjan, N. and Von Solms, R.: A conceptual framework for cybersecurity awareness and education in SA, *South African Computer Journal*, Vol.52, No.1, pp.29–41 (2014).
[17] Kritzinger, E. and Von Solms, S.H.: A framework for cyber security in Africa, *Journal of Information Assurance & Cybersecurity*, Vol.2012, No.1 (2012).
[18] Griffin, R.: A Demographic Analysis to Determine User Vulnerability among Several Categories of Phishing Attacks (2018).
[19] Bullee, J.W., Montoya, L., Junger, M. and Hartel, P.: Spear phishing in organisations explained, *Information & Computer Security*, Vol.25, No.5, pp.593–613 (2017).
[20] Diaz, A., Sherman, A.T. and Joshi, A.: Phishing in an Academic Community: A Study of User Susceptibility and Behavior, arXiv preprint arXiv:1811.06078 (2018).
[21] Joinson, A. and Steen, T.V.: Human aspects of cyber security: Behaviour or culture change?, *Cyber Security: A Peer-Reviewed Journal*, Vol.1, No.4, pp.351–360 (2018).
[22] Flores, W.R. and Ekstedt, M.: Shaping intention to resist social engineering through transformational leadership, *Information Security Culture and Awareness, Computers & Security*, Vol.59, pp.26–44 (2016).
[23] Singer, P.W. and Friedman, A.: *Cybersecurity: What everyone needs to know*, Oxford University Press (2014).
[24] Economides, N. and Jeziorski, P.: Mobile money in Tanzania, *Marketing Science*, Vol.36, No.6, pp.815–837 (2017).
[25] Poushter, J., Bishop, C. and Chwe, H.: Social media use continues to rise in developing countries, but plateaus across developed ones, Washington: Pew Internet and American Life Project (2018).
[26] Emerging Asian countries among most exposed to malware (2017), available from ⟨https://news.microsoft.com/apac/2017/08/24/emerging-asiancountries-among-exposed-malware/⟩ (accessed 2017-06-23).
[27] Microsoft security intelligence report, volume 22 — January through march, available from ⟨https://download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5BE38A28368433/Security_Intelligence_Report_Volume_22.pdf/⟩ (accessed 2017-06-23).
[28] Mirzoyants, A.: Mobile Money in Tanzania: Use, Barriers and Opportunities, *Intermedia Financial Inclusion Tracker Surveys Project* (2013).
[29] Sasse, M.A., Brostoff, S. and Weirich, D.: Transforming the 'weakest link'—A human/computer interaction approach to usable and effective security, *BT Technology Journal*, Vol.19, No.3, pp.122–131 (2001).
[30] Mathur, A., Engel, J., Sobti, S., Chang, V. and Chetty, M.: They Keep Coming Back Like Zombies: Improving Software Updating Interfaces, *SOUPS*, pp.43–58 (2016).
[31] Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N. and Cranor, L.F.: Crying Wolf: An Empirical Study of SSL Warning Effectiveness, *USENIX Security Symposium*, pp.399–416 (2009).
[32] Wu, M., Miller, R.C. and Garfinkel, S.L.: Do security toolbars actually prevent phishing attacks?, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.601–610, ACM (2006).
[33] Cranor, L.F.: A framework for reasoning about the human in the loop (2008).
[34] Egelman, S. and Peer, E.: The myth of the average user: Improving privacy and security systems through individualization, *Proc. 2015 New Security Paradigms Workshop*, pp.16–28, ACM (2015).
[35] Ng, B.Y., Kankanhalli, A. and Xu, Y.C.: Studying users' computer security behavior: A health belief perspective, *Decision Support Systems*, Vol.46, No.4, pp.815–825 (2009).
[36] Wogalter, M.S. (Ed.): *Handbook of warnings*, CRC Press (2006).
[37] Silic, M., Cyr, D., Back, A. and Holzer, A.: Effects of Color Appeal, *Perceived Risk and Culture on User's Decision in Presence of Warning Banner Message* (2017).
[38] Meier, M.A., Hill, R.A., Elliot, A.J. and Barton, R.A.: *Color in achievement contexts in humans*, Cambridge University Press (2015).
[39] Mathur, A., Schlotfeldt, B. and Chetty, M.: A mixed-methods study of mobile users' data usage practices in South Africa, *Proc. 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp.1209–1220, ACM (2015).
[40] Gmsa: The mobile economy: Sub-Saharan Africa 2014, available from ⟨https://www.gsma.com/mobileeconomy/archive/GSMA-MESubSaharanAfrica-2014.pdf/⟩ (accessed 2018-04-11).
[41] Garg, V., Lorenzen-Huber, L., Camp, L.J. and Connelly, K.: Risk communication design for older adults, *ISARC, Proc. International Symposium on Automation and Robotics in Construction*, Vol.29, p.1, Vilnius Gediminas Technical University, Department of Construction Economics & Property (2012).
[42] Egelman, S. and Peer, E.: Scaling the security wall: Developing a security behavior intentions scale (sebis), *Proc. 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp.2873–2882, ACM (2015).
[43] Herrero, J., Urueña, A., Torres, A. and Hidalgo, A.: My computer is infected: The role of users' sensation seeking and domain-specific risk perceptions and risk attitudes on computer harm, *Journal of Risk Research*, Vol.20, No.11, pp.1466–1479 (2017).
[44] Wash, R. and Rader, E.J.: Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users, *SOUPS*, pp.309–325 (2015).
[45] Fahl, S., Harbach, M., Muders, T., Baumgärtner, L., Freisleben, B. and Smith, M.: Why Eve and Mallory love Android: An analysis of Android SSL (in) security, *Proc. 2012 ACM Conference on Computer and Communications Security*, pp.50–61, ACM (2012).
[46] Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L.F. and Telang, R.: Do or do not, there is no try: User engagement may not improve security outcomes, *12th Symposium on Usable Privacy and Security* (*SOUPS 2016*), pp.97–111 (2016).
[47] Vaniea, K.E., Rader, E. and Wash, R.: Betrayed by updates: How negative experiences affect future security, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.2671–2674, ACM (2014).
[48] Chetty, M., Banks, R., Brush, A. J., Donner, J. and Grinter, R.: You're capped: understanding the effects of bandwidth caps on broadband use in the home, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.3021–3030, ACM (2012).
[49] Mathur, A. and Chetty, M.: Impact of user characteristics on attitudes towards automatic mobile application updates, *Symposium on Usable Privacy and Security* (*SOUPS*) (2017).
[50] Möller, A., Michahelles, F., Diewald, S., Roalter, L. and Kranz, M.: Update behavior in app markets and security implications: A case study in google play, Research in the Large, LARGE 3.0: 21/09/2012-21/09/2012, pp.3–6 (2012).
[51] Tian, Y., Liu, B., Dai, W., Ur, B., Tague, P. and Cranor, L.F.: Supporting privacy-conscious app update decisions with user reviews, *Proc. 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, pp.51–61, ACM (2015).
[52] Kindberg, T., O'Neill, E., Bevan, C., Kostakos, V., Stanton Fraser, D. and Jay, T.: Measuring trust in wi-fi hotspots, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.173–182, ACM (2008).
[53] Klasnja, P., Consolvo, S., Jung, J., Greenstein, B.M., LeGrand, L., Powledge, P. and Wetherall, D.: When i am on wi-fi, i am fearless: Privacy concerns & practices in eeryday wi-fi use, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.1993–2002, ACM (2009).
[54] Kowitz, B. and Cranor, L.: Peripheral privacy notifications for wireless networks, *Proc. 2005 ACM Workshop on Privacy in the Electronic Society*, pp.90–96, ACM (2005).
[55] Aime, M.D., Calandriello, G. and Lioy, A.: Dependability in wireless networks: Can we rely on WiFi?, *IEEE Security & Privacy*, Vol.5, No.1 (2007).
[56] Gold, S.: Cracking wireless networks, *Network Security*, Vol.2011, No.11, pp.14–18 (2011).
[57] Notoatmodjo, G. and Thomborson, C.: Passwords and perceptions, *Proc. 7th Australasian Conference on Information Security*, Vol.98,

pp.71–78, Australian Computer Society, Inc. (2009).
[58] Tam, L., Glassman, M. and Vandenwauver, M.: The psychology of password management: A tradeoff between security and convenience, *Behaviour & Information Technology*, Vol.29, No.3, pp.233–244 (2010).
[59] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N.: PassPoints: Design and longitudinal evaluation of a graphical password system, *International Journal of Human-computer Studies*, Vol.63, No.1-2, pp.102–127 (2005).
[60] Herley, C., van Oorschot, P.C. and Patrick, A.S.: Passwords: If we're so smart, why are we still using them?, *International Conference on Financial Cryptography and Data Security*, pp.230–237, Springer, Berlin, Heidelberg (2009).
[61] ITU. 2017: Global cybersecurity index (2017), available from ⟨https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx⟩ (accessed 2018-03-24).
[62] Millions of Android Devices are Vulnerable Right Out of the Box, available from ⟨https://www.wired.com/story/android-smartphones-vulnerable-out-of-the-box/⟩ (accessed 2018-03-24).
[63] Parker, F., Ophoff, J., Van Belle, J.P. and Karia, R.: Security awareness and adoption of security controls by smartphone users, *2015 2nd International Conference on Information Security and Cyber Forensics* (*InfoSec*), pp.99–104, IEEE (2015).
[64] Waters, C.: Web concept & design New Riders Publishing, *Indianapolis*, USA (1996).
[65] Russo, P. and Boor, S.: How fluent is your interface?: Designing for international users, *INTERCHI '93*, pp.342–347 (1993).
[66] A Guide to Emergency Codes – Emergency Preparedness & Response in Health Care, available from ⟨https://nhcps.com/emergency-preparedness-response-health-care-guide-emergency-codes/⟩ (accessed 2018-06-10).
[67] Chronology of Changes to the Homeland Security Advisory System, available from ⟨https://www.wired.com/2009/09/threatleveladvisory/⟩ (accessed 2018-06-10).
[68] The search engine for Security, available from ⟨https://www.shodan.io/⟩ (accessed 2019-01-05).
[69] A Shodan Tutorial and Primer, available from ⟨https://danielmiessler.com/study/shodan/⟩ (accessed 2019-01-05).
[70] Japan Computer Emergency Response Team Coordination -Center available from ⟨https://www.jpcert.or.jp/english/⟩ (accessed 2019-01-05).
[71] Three reasons why japan is falling behind in mobile commerce, available from ⟨https://blog.euromonitor.com/2017/04/threereasons-why-japan-falling-behind-mobile-commerce.html⟩ (accessed 2018-02-10).
[72] Top 5 smartphone app categories in japan, ranked by average number of apps used*, July 2014 and July 2016, available from ⟨http://www.emarketer.com/Chart/Top-5-Smartphone-App-Categories-Japan-Ranked-by-Average-Number-of-Apps-Used-July-2014-July-2016/202167/⟩ (accessed 2018-02-10).
[73] African millennials; mobile usage and media consumption, available from ⟨https://blog.geopoll.com/african-millennials-mobile-usageand-media-consumption/⟩ (accessed 2018-02-10).
[74] Top 10 Smartphones with Long Battery Life in Ghana (2018), available from ⟨https://itechghana.com/top-10-smartphones-with-long-battery-life-in-ghana-2018/⟩ (accessed 2019-06-10).
[75] Community Commodity Health Insurance Scheme, available from ⟨https://unleash.org/solutions/community-commodity-health-insurance-scheme/⟩ (accessed 2019-06-10).
[76] Mtei, G., Makawia, S., Ally, M., Kuwawenaruwa, A., Meheus, F. and Borghi, J.: Who pays and who benefits from health care? An assessment of equity in health care financing and benefit distribution in Tanzania, *Health policy and planning*, Vol.27, (suppl_1), pp.i23–i34 (2012).
[77] WHO, World Health Report: Health System Financing: The Path to Universal Coverage (2010).
[78] Health care system in Japan, available from ⟨https://en.wikipedia.org/wiki/Health_care_system_in_Japan/⟩ (accessed 2019-06-10).
[79] International Student Insurance, available from ⟨https://www.internationalstudentinsurance.com/japan-student-insurance/healthcare-in-japan.php/⟩ (accessed 2019-06-10).
[80] Nomura, H. and Nakayama, T.: The Japanese healthcare system, The BMJ Publishing Group Ltd. (2005).
[81] Are government documents scholarly or peer reviewed?, available from ⟨https://apus.libanswers.com/faq/139271⟩ (accessed 2019-06-10).
[82] Macaya, M. and Perea, M.: Does bold emphasis facilitate the process of visual-word recognition?, *The Spanish Journal of Psychology*, Vol.17 (2014).
[83] Emmott, C., Sanford, A.J. and Morrow, L.I.: Capturing the attention of readers? Stylistic and psychological perspectives on the use and effect of text fragmentation in narratives, *Journal of Literary Semantics*, Vol.35, No.1, pp.1–30 (2006).
[84] Macromil Group, available from ⟨https://group.macromill.com/⟩.
[85] Hong, H.: Government websites and social media's influence on government-public relationships, *Public Relations Review*, Vol.39, No.4, pp.346–356 (2013).
[86] Web Evaluation, available from ⟨http://library.sccsc.edu/tutorials/websiteevaluation/websiteevaluation-plainHTML.asp⟩ (accessed 2019-06-12).



**Jema David Ndibwile** received his M.Tech. degree in information security from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India, in 2015. He is currently pursuing his Ph.D. degree with the Nara Institute of Science and Technology (NAIST), Japan. His research interests include phishing countermeasures, the psychology of cybersecurity, and ethical hacking.

**Edith Talina Luhanga** received her B.Eng. degree in electronics and computer engineering and her M.Sc. degree in advanced computing science from the University of Nottingham, in 2010 and 2011, respectively, and her Ph.D. degree in information science from the Nara Institute of Science and Technology (NAIST), Japan. She is currently a Lecturer with the Nelson Mandela African Institution of Science and Technology (NM-AIST), Tanzania. Her research interests include health behavior change, understanding users, and human–computer interactions.

**Doudou Fall** received his M.E. degree in data transmission and information security from University Cheikh Anta Diop, Senegal, in 2009, and his M.E. and Ph.D. degrees in information science from the Nara Institute of Science and Technology (NAIST), Japan, in 2012 and 2015, respectively, where he is currently an Assistant Professor with the Graduate School of Information Science. His research interests include cloud computing security, vulnerability, and security risk analysis.

**Youki Kadobayashi** received his Ph.D. degree in computer science from Osaka University, Japan, in 1997. He is currently a Professor with the Laboratory for Cyber Resilience, Nara Institute of Science and Technology, Japan. His research interests include cybersecurity, Web security, and distributed systems. He is a member of the ACM and the IEEE Communications Society.