Lessons in Prevention and Cure

A User Study of Recovery from Flubot Smartphone Malware

Geers, Artur; Ding, Aaron; Gañán, Carlos Hernandez; Parkin, Simon

DOI
10.1145/3617072.3617109

Publication date
2023

Document Version
Final published version

Published in
Proceedings - EuroUSEC 2023

Lessons in Prevention and Cure: A User Study of Recovery from Flubot Smartphone Malware

Artur Geers
Aaron Ding
Carlos Hernandez Gañán
Simon Parkin
Delft University of Technology
Delft, Netherlands

ABSTRACT

The smishing-based malware Flubot was taken down in mid-2022, yet there is little understanding of how it directly impacted smartphone users. We engage with customers of a partner Internet Service Provider (ISP), who have suffered a Flubot infection on their smartphones. We surveyed 87 ISP customers who had been notified of a Flubot infection, in the months around and preceding the take-down of Flubot. We found that slightly over half of respondents were unaware of the malware infection before being notified, though many others had suspicions. We also observe that just over half of respondents experienced non-technical harms from the malware, with many experiencing harms before notification and several experiencing unwanted or aggressive activity from users of other infected devices. Many respondents reported not having removed the malware, while some discarded the infected device or stopped using online services in their efforts to be more secure afterwards. We offer recommendations, including that clearer guidance be sought to help users identify a malware infection (and not a focus only on prevention), and support provided for recovery from personal harms caused by mobile malware, as the impacts are not only technical.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

smartphone malware, Flubot, user notification study

ACM Reference Format:
Artur Geers, Aaron Ding, Carlos Hernandez Gañán, and Simon Parkin. 2023. Lessons in Prevention and Cure: A User Study of Recovery from Flubot Smartphone Malware. In *The 2023 European Symposium on Usable Security (EuroUSEC 2023), October 16–17, 2023, Copenhagen, Denmark*. ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3617072.3617109

EuroUSEC 2023, October 16–17, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0814-5/23/10.
https://doi.org/10.1145/3617072.3617109

1 INTRODUCTION

Smishing is a type of phishing attack that uses Short Messaging Service (SMS) or simple text messages on mobile phones to steal a victim's Internet credentials. The increased occurrence of smishing attacks constitute a considerable threat for consumers, businesses and networks [36].

Flubot, a specific type of smishing-based malware, is a recent large-scale example of smishing, which has affected millions of consumers and businesses in a fairly short time [74]. Fortunately for users, Flubot was taken down in early June of 2022 by a global cooperation of cyber police forces [24]. However, the risks posed by Flubot and other active smishing-based malware types (e.g., SMSControllo and Anatsa) are still present [24, 43, 45, 55, 65].

To our knowledge, the impacts of smishing and smartphone-based malware on affected users have not been directly examined before. To understand the impacts upon smartphone users, we partnered with an Internet Service Provider (ISP), based in the same country as the authors. We engaged with customers who have suffered a Flubot infection on their smartphones. We surveyed 87 ISP customers who had been notified of a Flubot infection, in the months around and preceding the takedown of Flubot. Although Flubot has been taken down, lessons must be learned – while there is still an opportunity – about how to support those users impacted by mobile malware.

We explore the research question *"How has Flubot impacted consumers who have an infected mobile phone (as detected and signaled by their ISP)?"*

We examine this research question in more detail with specific sub-questions: (SQ1) Are mobile end-users aware of being infected by Flubot, including potential harms?; (SQ2) How have end-users acted on the Flubot infection?; (SQ3) How have end-users perceived the remediation assistance?

Framing the sub-questions within the B-MAP behavior model [25], The first two questions explore the Ability of end-users to notice Flubot (SQ1) and to respond to it (SQ2), while also capturing related Motivation factors. The third question (SQ3) considers the ISP notification, considered here as a facilitating Prompt to act.

We find that a little over half of the 87 respondents were unaware of the malware infection before they were notified (SQ1). Just over half of the respondents reported experiencing harms as a result; many experienced harms before notification, and several experienced aggressive behavior from other infected users. Many users also had their suspicions that there was an infection (SQ2). Many users reported not having removed the malware (SQ3), while some

discarded the infected device, or took (potentially inappropriate) action afterwards in their efforts to be more secure; this included ceasing to use specific services such as online banking.

The rest of the paper is arranged with the background of Flubot presented in Section 2. We detail our Methodology in Section 3 and Results in Section 4. Discussion of the implications of our findings are in Section 5, consideration of related work in Section 6, and concluding remarks in Section 7.

2 BACKGROUND

One goal of our work is to examine the effects of mobile malware – specifically Flubot – as compared to 'traditional' malicious software, such as IoT malware [9, 62] or ransomware [69]. In this section we elaborate on how Flubot mobile malware functions, as well as current activities to reduce and mitigate mobile malware.

Flubot sends out messages to other phone numbers (generally in the same country), infecting other smartphones from the moment the text is opened; messages include a link within the text that when clicked on will often download a malicious external application. Similar to phishing, Flubot messages would commonly imitate package delivery services. Such services have become increasingly popular in the last several years, even more so in the wake of the Covid-19 pandemic. Smishing campaigns are seen as becoming more effective [23, 59, 70].

Flubot (formerly known as Cabassous) functions as both a banking Trojan and spyware. Financial credentials may be logged, raiding any financial accounts including cryptocurrency applications. Activities comparable to spyware are also seen, including storage of contact information and sending of fraudulent texts to contacts, all while hiding this activity from the user of the infected device [19, 36, 57]. Figure 1 shows the process of a Flubot infection, from the victim's perspective. Flubot in particular targets Android phones; if an iPhone is detected, a URL-borne attack vector is limited to stealing credit card information, rather than installing malware.

As at the start of the infection – left-hand side of Figure 1 – a user would receive a text message which includes a hyperlink (for example embedded in a message purporting to be from a delivery service). Figure 1 depicts the process leading to device infection, where after infection the phone connects to a Command and Control (C&C) server. The device informs the server of which applications are installed on the smartphone, and all the contacts [75]. The C&C server returns a list with instructions on how to capture information from the different relevant applications. It also shares a list with phone numbers to send SMS texts to (to spread the malware), and provides the specific text that should be sent (including a malicious link).

Flubot also modifies phone behavior. As well as capturing all the data on the phone, the phone infection turns battery-save mode off, starts sending malicious SMS texts, and shares the information gathered from keylogging and screen-capturing features, especially financial information. This process keeps repeating, unless the victim realizes that the phone is infected and performs a factory reset to remediate the infection. The more recent versions of Flubot can perform a range of activities, some of which are performed constantly [51, 53, 65]. This includes intercepting notifications (e.g., passcodes), sending and intercepting SMS texts, logging contacts, and disabling power-saving features.

Flubot has been taken down, but the sharing of malicious links through SMS texts, for the purpose of infecting smartphones, has been used by multiple other social engineering malware types since 2017. These include [64, 65, 68]. Teabot, Anatsa, BRATA, SMSControllo, Anubis, Cerberus, Oscorp and Ubel (which is most likely a more developed version of Oscorp), and the latest addition, ERMAC 2.0 (based on Cerberus). These are examples of mobile malware – generally targeting Android phones – that use multiple ways of infecting mobile phones, including smishing [7, 16, 17, 34, 42–44, 63, 77, 80].

Flubot not only shares an infection vector with other Android malware families, but also presents similarities with other malware families in terms of phone feature manipulation. Other types of mobile malware, such as Triada [83], Ztorg [47], and Joker [67], can also gain root access to Android devices and modify system components, to hide their presence and evade detection. In addition to this, they can also steal personal information, display unwanted ads, and even subscribe users to premium services without their knowledge. These types of mobile malware can cause significant financial damage and can be difficult to remove once installed on a device.

2.1 Detection methods

Internet Service Providers (ISPs) – such as the ISP we partnered with for this research – may use either or both of two automated measures to automatically detect phones infected with Flubot. One is based on the Internet traffic between the infected device and an infected C&C server. The other is based on the SMS traffic. The latter method is based on monitoring the spike of SMS texts being sent as a result of the Flubot infection, to determine if it meets a threshold. If the amount of sent texts meets the threshold, the device is marked as infected, and blocked; the owner receives an email notification about the block for further information and to remediate the infection.

2.2 Preventive measures

A range of measures are currently available to prevent users from becoming victims of malware, which have been adapted for smartphone users and smishing-based malware. **Informing and educating mobile phone users** is a common tactic to limit the effectiveness of phishing attacks, similar to smishing attacks [14, 32]. Even if a malware infection is suspected, it is still difficult to determine which malware it specifically is, and what the appropriate response is [59]. Furthermore, to keep advice concise and actionable for the end-user, there is a risk that crucial aspects of the advice are left out [30, 60]. Regarding **measures on the device** itself, Android OS and iOS account for 66.77% and 32.55% of smartphones globally [72]. Android has been updated to make it more difficult to download from outside the Google App Store [13, 79], though some end-users continue to download external software [37]. We consider features of smishing malware in reflection upon our findings, in Section 5.

Remaining preventive measures are mostly based on SMS-text analysis, where an application downloaded on the phone, or an algorithm used by the telecom provider, acts to detect smishing texts based on the content [13]. It is unclear how effective any SMS filtering applications are against smishing-based malware, as Flubot

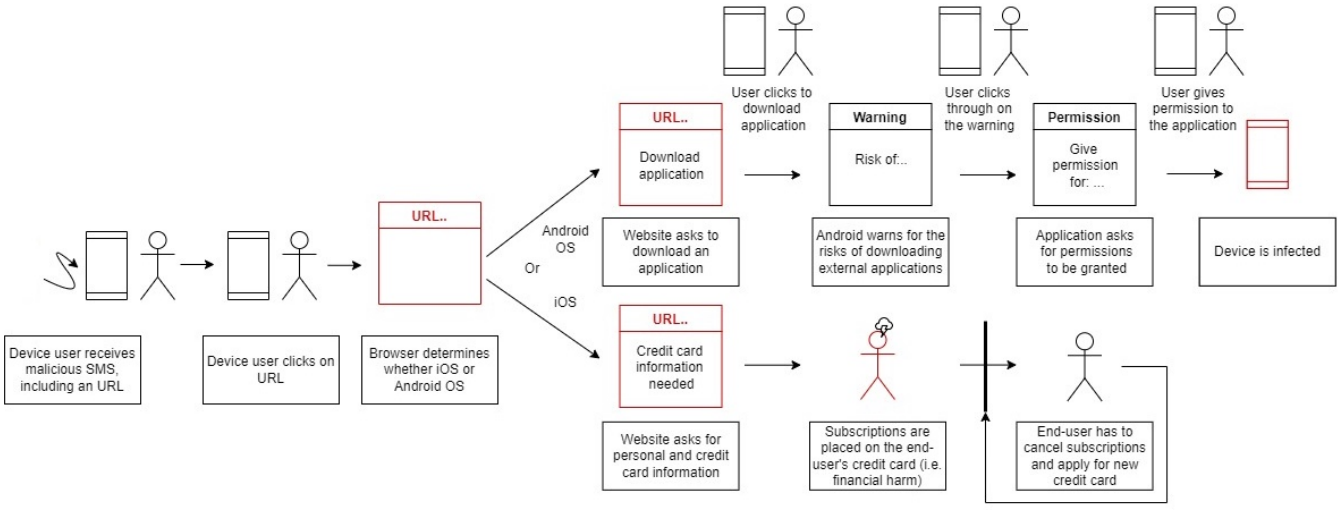

Figure 1: The sequence of a Flubot infection (for Android phones) or subscription scam (for iPhones) from a victim's perspective.

changes messages to avoid detection [33]. URL blocklisting relies on a database of websites, suspected of involvement in phishing and smishing, to trigger warnings to the user or prohibit loading of a web-page [13].

2.3 Reactive measures

The responsibility of avoiding and removing mobile phone malware inevitably falls, in part, upon the user [2, 35]. With Flubot, the user is less capable of determining whether an infection has occurred, due to Flubot's ability to hide itself and its operations [2, 5, 35]. A **notification** from a user's ISP – after detecting malware – can include advice on how to address mobile malware such as Flubot. The majority of research on notifying users with advice is focused on internet users in general and computer users more specifically [3, 4]. It is arguable that there is no one-size-fits-all way of notifying and educating computer users effectively [60, 82].

One method for notifying users who have a malware infection on their device is by email, as seen previously with IoT devices [11]. Another approach is a **walled garden notification**, i.e., restricting the connections the user can make on the Internet, and notifying them as part of the process. It is, however, difficult to contact large populations efficiently, where mail can be effective but does not reach everyone [11], or get their attention immediately [62].

3 METHODOLOGY

A survey was deployed to a large sample of users identified by a partner ISP [*in country removed during review*] as having Flubot infections. The focus on the customer base of a specific ISP is not assured to provide a representative picture of Flubot effects upon the wider population. However, it allows us to explore how users interact with the mechanisms of Flubot, and the potential impact Flubot has upon users (which we relate to other forms of mobile malware in Section 5).

The survey determined whether participating respondents were aware of an infection, and if so, whether the infection was remedied and how remediation was experienced. The survey also queried whether any non-technical harm was experienced as a result of the malware infection.

3.1 Recruitment

Given the exploratory nature of the research, an original intention was to conduct an interview study with users of infected devices. Recruitment occurred via a customer forum. However, this resulted in only one response; several others who indicated interest did not respond to repeated contact to arrange an interview. The one respondent was no longer using the listed contact address, so had not seen the malware notification from the ISP. The limited response reflects restrictions in the engagement method, which can arise within the customer service model of an ISP [9].

From IP-CC cases provided by Shadowserver [66], we identified cases of interest among the broadband customers of the partner ISP, based on connections to home networks managed by the ISP. The selection and tracking method for these cases can locate malware cases to an individual network. However, in the case of multiple smartphones connecting to the same home network, exactly which mobile device in a home is infected cannot be determined.

To obtain a sample of sufficient size, we examined cases across a time-span of seven months before the point of data collection. This started from November 2021, amounting to 1,532 cases. The further back cases go, the less reliable the responses will generally be, so we did not seek to look further back indefinitely. We also need to consider that we were interacting with the customer base of an ISP, rather than e.g., a dedicated academic survey platform such as Prolific. However, if there was any impact that the infection had on the respondent, the impact might be recollected more accurately. Notably, around the beginning of November 2021, a spike of cases was recorded by the partner ISP, which itself accounted for 684 cases.

Users had been sent notifications of the infection by the ISP according to the ISP's schedule, prior to the invitation to complete the

questionnaire (as detailed in Appendix A, also sent to notified customers within the remit of customer support). Potential respondents received at most two notifications, and 88 potential respondents completed and submitted a survey. The original ISP notification includes instructions to first "try to find out which Android devices have been connected to your internet connection", and then to back up "all files such as photos and contact information", and perform a factory reset. The notification also states that if no action is taken, that the internet connection will be blocked.

3.2 Survey structure

If a recipient of the survey invitation accessed it, an opening statement would inform the subject of the implications. This would inform the data subject of the purpose of the survey, and what is done with completed survey data.

After this, the main questions are asked. The survey design also benefited from feedback from staff at the partner ISP, who had experience with the notification process and prior interactions with affected customers (in place of a pilot). The conditions of the survey are followed with questions about remediation. Demographics questions were included in opening – the data subject was asked to give their profession, age and perceived technical ability (from 1 to 5); previous studies have shown that these demographics factors have the potential to skew outcomes [27, 38, 48, 62, 82], therefore it is important to record them for use alongside survey analysis. The full set of questions is listed in Appendix A.

Causes and suspicions. Each respondent was asked questions to determine whether they knew about Flubot or any smishing-based malware before being notified, and any suspicions that the mobile phone may be infected. Potential causes were queried, especially as the ISP notification focuses on detection rather than causes.

Remediation. The respondent was asked if they believed the infection was remediated successfully, and if so how long it took them (and if not, to detail any obstacles). The nature of Flubot means that it is difficult to determine whether a remediation was successful, relying here on user perception (similar to challenges with IoT device malware [9]).

Harm. The impact of malware goes beyond financial and data loss [33, 53, 76, 78]. A short description of the different types of harm was given (as in Appendix A). The first question was about whether harm was experienced prior to or after having been notified, if at all. If harm was experienced, the respondent could choose multiple types of harm, adapted from the harm framework of Agrafiotis et al. for managed (organization) infrastructures [1]. We considered the ISP ecosystem as analogous, as a managed system. For every type of harm that the respondent indicated having experienced, they were asked to elaborate. We combined physical harms and digital harms into one category, as a framing that acknowledges how these categories are intertwined in the use of a mobile smartphone device.

Remediation assistance. The respondent was asked to rate and elaborate on the information provided in the ISP notification and the support from the ISP. The respondent was also asked whether they changed how they interact with and make use of their mobile phone.

3.3 Analysis

For the purpose of analysis and to filter out unusable data, a first review of all the responses found that one respondent did not provide serious answers, and was excluded (e.g., declaring their occupation as 'crook'). The remaining 87 submissions are used for analysis and in the remainder of the paper.

In the survey a number of different questions were asked, from which statistical and empirical insights were drawn (as in Appendix A) and used to support the Discussion (Section 5). Spearman's Rank Correlation Coefficient was used to analyze ordinal and interval/ratio variables for correlations. Descriptive identifiers are given to the responses to separate questions (see Appendices B and C). By using Spearman's Rank Correlation Coefficient, when analyzing ordinal and interval/ratio variables, it is possible to determine strong and weak correlations between the set of variables.

For further analysis, ordinal and scale variables are used to determine whether significant correlation coefficients exist in the sample, as an indication for the larger population. Descriptive identifiers are given to the responses to separate questions (see Appendices B and C). Respondent age was treated as a ratio scale variable. Throughout the survey there are two more ratio scale variables, namely 2_DaysTakenRemediation and 1_AverageWeeklySMS.

There is a multiple choice question included, 1_Source (Q4), converted into 1_SourceFamily, 1_SourceFriends, 1_SourceNews, 1_SourceSocialMedia, 1_SourceTelco, 1_SourceEmployer, and 1_SourceGov, which, for analysis, was turned into nominal scale variables for all the different options included and suggested by respondents, in the last option it is possible to fill in one's own category [37, 81].

Ranked variables included a set of Likert scale questions were asked: Demo_SkillLevelSmartphone (Q3), 1_LikelihoodClickingUnknownSender (Q11), 3_Harm (Q14) converted into 3_HarmPhysicalDigital, 3_HarmPhysicalDigital, 3_HarmEconomic, 3_HarmPsychological, 3_HarmReputational, and 3_HarmSocietal. There is also 4_SatisfactionInformationProvision (Q18A), and 4_SatisfactionSupport (Q18B). These are treated as interval scale variables.

In the survey a number of yes or no questions were posed 1_PriorKnowledge (Q4), 1_Suspicion (Q6), 1_InclinationCauseInfection (Q8), 2_Remediation (Q12), 4_ChangedPhoneInteraction (Q20). These were often followed by open-ended questions for elaboration, as has been used in prior studies (e.g., [84]). The answers were converted to nominal variables, zero for "no" or one for "yes". A similar setup is used for 3_HarmWhen (Q15), where the answers are either "No harm", "Harm experienced prior to being notified" and "Harm experienced after being notified", with the answers being translated into values 0, 1 or 2, respectively.

The remaining questions Demo_PROFESSION (Q2), 1_SuspicionElaboration (Q7), 1_InclinationCauseElaboration (Q9), 2_RemediationElaboration (Q13), 3_HarmElaboration (Q17), 4_SatisfactionElaboration, (Q19) 4_ChangedInteractionElaboration (Q21) are open-ended questions which are not meant for statistical analysis but for empirical insights – these are discussed in detail in the next Section.

Regarding qualitative analysis, the answers provided in the questions would in the first instance be divided into groups by the immediate indication of a condition (e.g., indicating 'yes' for a harm having been experienced, or 'no' if not). This served to group responses. Given the survey format, elaborations upon conditional responses were grouped only when they were very similar, as an application of a thematic analysis approach [10].

One of the authors applied a 'codebook'-style approach, which Braun & Clarke regard as reasonable to conduct with one coder [10]. The codes and themes (including sample excerpts attached to codes) were discussed among the authors at weekly intervals, adding, removing, or revising codes as necessary. A final codebook was produced, with themes and codes detailed in Table 1 and Table 2. Attention was given here to capturing a range of responses without losing meaningful detail when consolidating codes (such as different harms, etc.). Coding identified seven themes, as detailed in the codebook tables: Indicators (of Flubot), Suspected causes, (reasons for) Failure to remediate, Harms pre-notification, Harms post-notification, and Impact on phone interaction.

3.4 Ethics

The principles of the Menlo Report for ethical assessment of ICT Research are followed [22]. Regarding **Respect for Persons**, the study protocol was reviewed and approved by the human research ethics committee of the authors' institution. All respondents were given informed consent for participating, i.e., aggregated response data being analyzed and published afterwards. Respondents were informed that they were free to stop participating at any moment. Survey responses were anonymized, separating them from customer records at the partner ISP.

For **Respect for Stakeholders**, the partner ISP's safety, privacy and security guidelines and policies were adhered to when using their data, tools, programs and facilities. No data left the ISP's facilities until it was generalized, anonymized, and approval given for using it in the research. For **Justice**, no groups have been excluded based on prejudice. Attributes of persons have only been included for this research if deemed relevant for analysis, such as age. No respondent selection was based on specific attributes. **Beneficence** has been a fundamental aspect of this research; no processes at the partner ISP were disturbed. Some detection details are obfuscated, so as not to benefit malicious parties involved in smartphone malware.

4 RESULTS

4.1 Demographics

The average age of survey respondents is 63, ranging between 36 and 81. The distribution of ages over the whole respondent group, including the normal curve is shown in Figure 2. The respondent group is skewed toward older adults. A US study of adults aged 50 and over indicates that older adults may make only marginally less use of smartphone text-messaging features than younger age groups [6], and that such features still see a 92% popularity among older age groups. However, older adults are noted as potentially limiting their use of technology as a means to avoid security threats [29, 46]. Frik et al. [28] found that older adults are only marginally less likely to configure smartphone settings relating to security and privacy. The 2022 US Internet Crime Complaint Centre (IC3) report detailed a year-on-year decrease in the number of both reported malware cases and reported phishing cases among older adults [52].

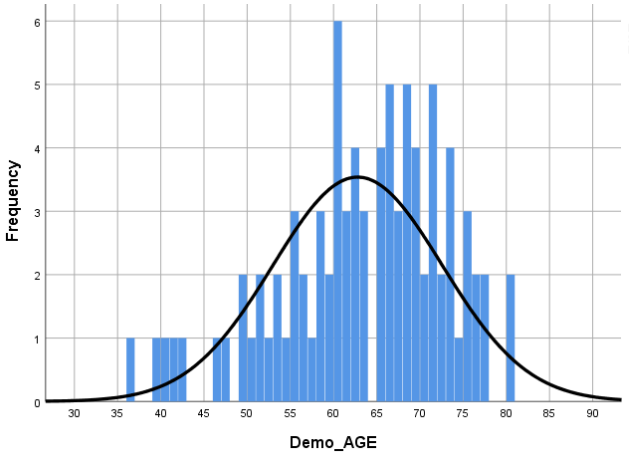

Figure 2: Histogram of the age distribution of the survey respondents, including the normal distribution *(Mean = 62.78, Std Dev. = 9.808, N = 87).*

The professions listed by respondents can be grouped in three categories, namely unemployed or without a recognised profession (17 respondents, of which a portion answered with being a housewife, and others had submitted working disability as their profession); retired (32 respondents), or; working (38 respondents).

Of all respondents, only one subject indicated working in IT / computing, which was also reflected in their perceived smartphone usage and remediation capabilities as it is rated the highest (5 out of 5). Regarding perceived ability of using and fixing smartphones, respondents on average rate their experience regarding use and recovery of smartphones to be moderate (3.06 out of 5). Only 10 respondents (11.5% of respondents) consider themselves to be very inexperienced.

4.2 Causes and Suspicions

Around half the sample (48.3%) indicated already knowing about Flubot or other malware before being notified. The question was posed as multiple choice, meaning that each respondent was able to select multiple answers: the most popular source for hearing about Flubot is news outlets (34.5%); the second most popular source is social media (20.7%), and the third most popular source is friends (18.4%). Figure 3 shows the different categories listed in the survey and how often they were selected. Looking at prior research of information sources [58], these trends align more with sources of knowledge about cybercrime than malware and phishing. Considering the relative older age of our respondents, Das et al. [21] found that older adults were more likely to report hearing about data breaches from news sources (as also with [29]), and we see a similar trend, as in Figure 3.

The majority of the respondents (59.8%, i.e. 52 respondents) did not suspect the presence of malware on their phone before being notified. Of the 35 respondents with a suspicion, 34 replied with

Table 1: Main themes and emerging from analysis of survey results (Part 1 of 2).

Theme	Code	Count
Indicators		
Text-message activity	Increased texts being sent (7); Texts and calls from unknown senders (10)	17
Phone/OS behaviour	Weird notifications (2); Lost control over phone (4); Slower phone (2)	8
Application characteristics	Unable to delete installed application (2); Downloaded suspicious application (4)	6
Non-technical indicators	(Un)known contacts asking/informing user of being hacked (2); High phone bill (2)	4
Suspected causes		
Malicious link	Courier/DHL text (waiting for a parcel) (10); courier text (16); Courier email (6)	25
Malicious download	Downloaded malicious app through SMS	9
Failure to remediate		
Lack of knowledge	Unaware (11); Did not know how to fix (2); No way of knowing (2)	15
Non-technical barriers	Unusable phone (2); Fixing cost too much money (1); Unused (2); Not my phone (1)	6

an elaboration (the 'Indicators' theme at the top of Table 1). The answers are quite diverse and not always unrelated to each other. Four respondents relate the infection to having downloaded a suspicious application, and two suspected something after not being able to delete an application they had just downloaded. The latter also implies existing suspicion, to want to remove the application.

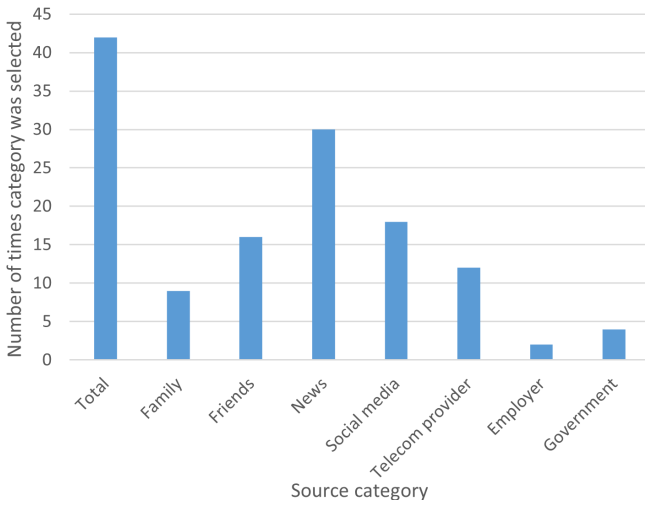

Figure 3: Sources from which the 87 respondents came to know about Flubot and/or other mobile malware.

Phone activity itself was also suspicious: "Increased texts being sent", "Texts and calls from unknown senders", and "(un)known contacts asking/informing whether the respondent was hacked" are very much related to each other, as is "High phone bill". To reiterate, as a consequence of a Flubot infection, a phone sends additional texts, and sometimes calls others without the knowledge of the owner of the infected smartphone; this can lead to a high phone bill and receivers (of the secretly sent SMS texts) potentially responding to the texts, e.g., asking whether the sender of the malicious texts was hacked. Not all answers can be attributed solely to the presence of Flubot. For instance, losing control over the phone is not necessarily a consequence of Flubot – such an answer does not make the suspicion less true or applicable, however the suspicion of the four respondents answering "Lost control over phone", could well have been caused by something that is not Flubot. All other suspicions can potentially be attributed to Flubot.

Regarding the cause of the malware infection, a slight majority of the respondents (52.9%) had an idea of what had caused the infection. This does, however, also mean that almost half the respondents (47.1%) indicated having no idea about the cause. Of the respondents having replied in the positive to having a sense of what caused the Flubot infection (second code theme in Table 1, 'Suspected causes'), two answers are unlikely to have been the actual cause of the infection: "Foreign number through WiFi" and "Called back to unknown number". The latter two factors are not known causes of Flubot infections or other similar smishing-based malware. These two answers can be symptoms of the infection, and the second of these can be the cause for an increased phone bill, but that is not how Flubot or smishing-based malware is spread. Also, "Malicious (DHL) email (about parcel)" is also not related to Flubot. The answers then point to confusion between cause and consequence.

The remaining answers (from 35 respondents, or 40.2%) are assumed to be accurate and the actual cause of the Flubot infection. 10 answers are "malicious DHL link while waiting for a parcel", showing that the timing of the Flubot campaigns has a significant

impact on the likelihood of the malicious links working. 16 are "Malicious link" (18.4%) and 9 are "Downloaded malicious app through SMS" (10.3%).

Messages from unknown senders. On average respondents reported receiving just over four SMS texts weekly (4.31) from unknown senders, excluding friends and family. 88.6% of the respondents receive between zero and five SMS texts weekly on average. Two texts per week is the most common number (37.9%), followed by 10 (4 respondents; 4.6%), 15 (2 respondents; 2.3%), 20 (1 respondents; 1.1%), 40 (1 respondents; 1.1%), or 60 (2 respondents; 2.3%) texts. This means that most respondents generally did not receive a large volume of unexpected or unfamiliar texts. This informs how much 'interference' there might have been between malicious and benign texts.

The respondents reported being unlikely to click on SMS texts from unknown senders, with the average score being 1.72 on a scale from 1 (very unlikely) to 5 (very likely). 50 respondents (57.5%) deemed it 'very unlikely' that they would click on a text from an unknown sender, and 19 respondents (21.8%) deemed it 'unlikely'. However, it is important to notice that 11 respondents (12.6%) are in between 'likely' and 'unlikely' to click on unknown texts (rating a three). Seven respondents were candid enough to state that they are 'likely' to click on unknown texts, of which one respondent even 'very likely'. This raises the issue that 20.7% of respondents (rated three or higher) self-report that there is some chance of them clicking on SMS texts from unknown senders, which may put these groups at substantial risk for further malware infections and harm. In a controlled study of user capacity to distinguish between genuine and phishing SMS messages, Clasen et al. [15] found that 73.4% of messages were categorized correctly.

4.3 Remediation

77% of the respondents (67 respondents) stated having remediated the malware, meaning that almost a quarter of the respondents (23%) had not remediated the infection – the third theme in Table 1, 'Failure to remediate'. 11 respondents (12.6%) were unaware of the infection, and possibly two more (2.3%), as their answer "No way of knowing" is ambiguous as to knowing of the infection or how to remediate. One respondent (1.1%) found the fixing cost to be too much; one respondent (1.1%) mentioned that it was not their phone; another two respondents (2.3%) did not know how to remediate, and; the remaining two respondents (2.3%) said that the infected phones were no longer in use.

If respondents remediated the Flubot infection, average self-reported clean-up time was 3.4 days. 52.9% of respondents reported remediating the infection in the first two days, while it took an additional 21.8% of respondents up to 7 days to remediate. There are two outliers, one (1.1%) who took 14 days, and one (1.1%) some 60 days.

4.4 Harm analysis

A slight majority of the respondents (52.9%) reported having experienced a type of harm, within the categories adapted from Agrafiotis et al. [1]. Some respondents named multiple aspects in their elaboration, hence more answers than respondents per category. Exactly half of the respondents that experienced harm experienced it prior to being notified, and the other half after being notified, as seen in the harm themes in Table 2, respectively.

The elaborations the respondents gave vary from discomfort (most common answer, 16 times answered; 18.4%) to financial harm (13 answers; 14.9%), as a result of an increased phone bill, to not trusting the smartphone or banking services anymore (8 answers; 9.2%), to loss of data (6 answers; 6.9%). Three respondents replaced their phone completely (which could constitute a notable financial burden). 6 respondents (6.9%) had received aggressive and/or threatening texts from the numbers their infected smartphones spread the Flubot infection to. This is also the biggest difference in the sample between experiencing harm before and after the notification: aggressive texts were reported as being experienced before being notified, when it may be that the respondent also does not know why it is happening. Other answers are comparable across the categories of pre- and post-notification.

46 respondents reported harms caused by Flubot, with ratings shown in Figure 4. Reputational and societal harm could be expected to be relatively close to each other in the context of home users, which is borne out by the results. These two categories score almost exactly the same, predominantly in the lower ratings. Physical/digital and economical harm follow similar trends, in that respondents reported experiencing these types of harm more heavily. Psychological harm has been experienced moderately, where the majority of respondents have awarded the harm a 2, 3 or 4 (on a scale from 1 to 5), with these three ratings having been awarded almost equally.

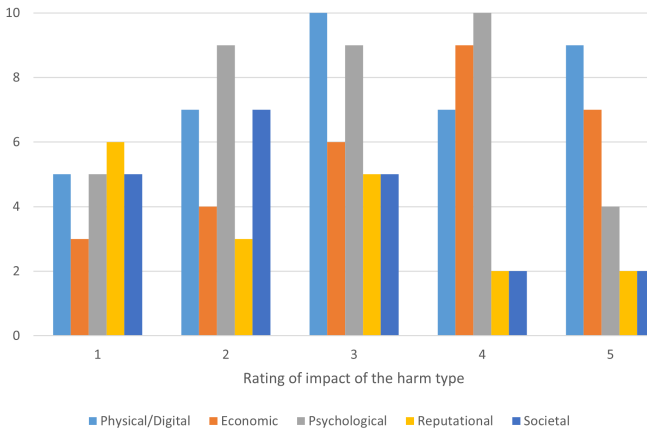

Figure 4: Chart of the harm types that have been selected (as different bars), with the rating (x-axis) of the impact that was associated to the harm types, and count of reported instances (y-axis).

Psychological harm has been experienced on average as a 3.0 (moderately impactful), and has been experienced by 42.5% of the respondents. The most experienced harm is physical/digital harm, being experienced by 43.7%, where this category also had the second highest impact, scoring 3.2 on average. The harm type that has the most impact is economic harm, scoring 3.45. The frequency of

Table 2: Main themes and codes emerging from analysis of survey results (Part 2 of 2).

Theme	Code	Count
Harms pre-notification		
Distress	Discomfort (9); Do not trust phone or banking app (6)	15
Loss of safety	Threatening/aggressive tests and unsafe	6
Monetary cost	Costs for phone bill	6
Disruption/Loss	Lost data (pictures) (3); Unable to work (properly) (1)	4
Harms post-notification		
Monetary cost	Costs for phone bill (7); Costs for new phone (3)	10
Distress	Discomfort (7); Do not trust phone or banking app (2); Stress (due to faulty reset) (1)	10
Disruption/Loss	Unable to work (properly) (1); Lost data (pictures) (3); Get a new number and change everywhere (1)	5
Impact on phone interaction		
Behaviour modified	More careful (24); ... with installing applications (2); Not clicking on (email) message unknown sender (22)	48
One-time action	Installed anti-virus (2); New phone (1)	3
Switch of behaviour	No longer use financial application (1); Only answer phone to known numbers (1)	2

having experienced economic harm is lower than the latter two types discussed, experienced by 33.3% of the respondents. Societal and reputational harm are reported less often (24.1% and 20.7% respectively) and the impacts of these types of harm are the least severe (with both rated around 2.5).

4.5 Support experience

We briefly summarize here the experiences with the ISP support (not featured in the codebook presented in the two tables, which focus on Flubot). The average satisfaction with the information and notification provided by the partner ISP is 3.17, which is slightly higher than the average satisfaction with the support provided (3.14). For both aspects, the ratings are relatively equally spread out over the five possible rating intervals, with the moderate rating (3) being the most popular for both information provision (28.7%) and support provision (25.3%). The elaborations provided by the respondents are categorized as positive, neutral, or negative, with answers spread relatively evenly over the three categories, albeit with a slight lean toward positive elaborations.

According to 13 respondents (14.9%), the ISP notification is clear, with 10 respondents (11.5%) describing the support as quick. 10 respondents (11.5%) have not remediated the issue themselves, while in contrast two respondents (2.3%) mentioned that neither the intervention of the ISP nor their notification was needed. Slowness and timing has been answered most frequently as a negative elaboration, such as with the ISP being regarded as slow to block the phone (5.7%) or slow to unblock it (1.1%).

4.6 Changes in phone usage after Flubot

For the last question posed in the survey, the majority of respondents (62.1%) changed their interaction with their phone because of the infection. This can be seen in the last code theme in Table 2, 'Impact on phone interaction'. This means 37.9% of respondents have not changed how they interact with their phone.

The elaborations given by respondents, as to how their interaction has changed, vary from a very broad and all-encompassing answer along the lines of being "More careful" (most frequent, 27.6%), to a more specific answer of "Not clicking on (email) message from unknown sender" (25.3%). Of the latter answer, 10% stated an intention to not click on email messages specifically, which is not effective in preventing smishing-based malware (i.e., the coping strategy does not fit the problem). Other precautions that respondents have taken following the infection are installing anti-virus software (2.3%); being more careful with installing applications (2.3%); buying a new phone (1.1%); ceasing use of financial applications (1 response; 1.1%), and; only answering the phone if it is a known number (1.1%). The latter measure is unrelated to Flubot malware, meaning that here too a respondent has been either wrongly informed of the cause, or has drawn an incorrect conclusion of what could have been the cause.

A study of actions after a ransomware infection [69] reported that of the 56% of victims that changed behaviors, this also includes more careful browsing, but also that users may change or adopt a behavior but not necessarily to one that would directly match the threat (which would be e.g., data backups in the case of ransomware).

5 DISCUSSION

Here we revisit our research questions, and explore recommendations which can serve as the basis for future work.

5.1 Revisiting research questions

SQ1: Awareness and Harms. Awareness of a device having a Flubot infection prior to notification was low, at 2.3% (SQ1). This

was predicated on already being suspicious of a downloaded application, and being unable to remove it.

Leveraging the statistically significant correlations as found in Appendix C, we saw significant correlation at the 0.01 level (2-tailed) between average weekly number of texts received and a higher likelihood of a respondent clicking on a text from an unknown sender. This suggests that noticing the initial infected text message is more difficult when mixed in with other, benign messages (which themselves may appear to come from an unknown sender).

A Flubot infection might otherwise be indicated alongside the financial harm of an (unexplainable) increase in phone bills (because of a surge of SMS texts being sent), or banking applications being taken over. Aggressive texts may also be received from users of other infected devices. A range of potential harms may then be experienced alongside technical indicators of Flubot infection, without direct evidence of the existence of Flubot on a device.

The importance of 'indirect' ways to become aware of a Flubot infection can be applied to other types of malware that exploit SMS messages. For example, many banking trojans, such as Anubis [50], Ginp [49], and Red Alert 2.0 [56], use smishing to trick users into downloading fake banking apps or visiting fake banking websites. Adware such as Hummingbad [41] also commonly spreads through smishing. Ransomware families also use smishing to trick users into downloading malicious files or visiting fake websites that contain ransomware (such as Android/Filecoder.C [39]).

Victims have variously experienced all five types of harm (SQ1), as categorized by Agrafiotis et al. [1]. The type of harm with the largest relative impact is economic harm, then physical/digital harm, psychological harm, ending with reputational and societal harm, respectively. Harms may be compounded if the user does not know what is triggering the harmful events (such as financial loss, aggressive messages, etc.). Experienced harm is often a very strong (negative) prompt [25], especially harm with a high impact such as financial loss or receiving aggressive texts. Existing research on fear appeals (e.g., [61]) could be translated to support ways to address fears experienced due to smishing malware.

SQ2: Remediation. Considering acting on Flubot (SQ2), it is difficult to determine which Android phone on a network needs to be remediated and whether the remediation was successful (as there is no direct feedback loop in the remediation process, just as with e.g., smart device malware [9, 62]). Comparing to IoT malware such as Mirai [9] and persistent IoT malware such as QSnatch [62], 35 of 87 respondents believed they had noticed something which may indicate the presence of mobile malware, but this included traits which are not associated with Flubot (such as malicious messages via email). In comparison, QSnatch [62] appears to generally not be noticed by users unless they are notified.

There is a chance that Mirai and similar forms of IoT malware may eventually be removed through 'natural clean-up' [9]. Just as with persistent QSnatch malware, Flubot appears to require direct user action to remove it. The lack of feedback when removing IoT malware has been shown, by Bouwmeester et al., to lead to despair and uncertainty regarding the success of the remediation [9]. As lack of feedback is an issue for Flubot remediation too, this should be taken into account when structuring instructions which act to 'boost' a user toward remediation [25].

Despite the initial Flubot notification(s) from the ISP, and any follow-up correspondence (and possibly the survey itself), a significant portion of the sample did not have a correct or sufficient understanding of Flubot or its causes (41 of 87 respondents). Exploratory research into user mental models [71] suggests that malware is less well-understood than the software that users may interact with it more regularly, implying that care is needed when assuming how much technical knowledge users have.

SQ3: Support. In general, the respondents were moderately satisfied with the information and support provided in remediation assistance (SQ3). A quarter of the respondents had not remediated at all, because the victims did not trust the notification, did not know how to remediate, or did not adequately read the notification. This implies that varied support strategies are necessary (as has been considered elsewhere [11]), and consideration given in communicating instructions to varying levels of trust and expertise. Most post-remediation respondents reported being more careful with how they interact with their phone, whereas some are more careful with clicking on unknown senders' messages and when downloading external applications. Unfortunately, a few respondents adopted behaviors which would not directly prevent a re-infection of their device (e.g., limiting use of banking apps or unexpected emails). This is comparable to consumers avoiding online banking after hearing of online scams [54] – users who feel it necessary to behave 'more securely' may need guidance on how to do so, relative to a specific security concern.

5.2 Limitations

This study was exploratory, focusing on articulating the impacts of Flubot infections (which had not previously been explored). This precedes determining the awareness of Flubot across a wider user base – including users or customers who have not experienced a Flubot infection (whether having received security advice or not) – which would be a next step. Future work would also explore the 'weightings' that impacted users place on different harms. Here we did not explore Flubot victim experiences through open discussion, as this was attempted but was not successful (as mentioned in Section 3.1); the dynamic with the ISP limited the demands we could put on customer time (a challenge noted elsewhere, e.g., [9]. Survey respondents suffered malware infections over seven months, which although not an especially long period of time, was balanced with asking respondents to recall specific details of events.

The source data was available due to the partner ISP's dedicated resourcing of a capability to detect Flubot infections and link them to customers, itself developed in response to the uniquely high proliferation of Flubot as compared to other forms of mobile malware with less dedicated/developed detection capabilities; this meant that comparison to other mobile malware 'in situ' would have been difficult (especially as, to our knowledge, there is no other research on the lived user experience of any kind of mobile malware). However, we have addressed this in Section 5.

Because the data provided by Shadowserver only shows whether the infected device is connected to broadband connection of the

partner ISP on that day, it could potentially mean that a device has not remediated while not being visible in more recent Shadowserver datasets (simply if the device does not connect to a broadband connection of the partner ISP again). Linking infections to home networks rather than specific phones is an issue in households, if more than one smartphone connects regularly with the network. This highlights the social factors in identifying an infection, as well as the ambiguity users face in diagnosing and remediating Flubot infections, where the dynamics of shared smart homes [31] can be built upon in future work with a focus on malware remediation efforts.

The survey cohort suffered malware infections over seven months, which although not an especially long period of time, was balanced with asking respondents to recall specific details of events.

5.3 Recommendations

Based on our findings, we provide the following as initial recommendations, which also complement each other:

Adaptive ISP notifications. An adaptive notification approach first sends an email (as we see here with the partner ISP), and switches to different approaches such as phone or letter [11], if there is no user response. There may also be promise in partnering with other entities – and communication channels – that customers engage with [73] (noting here that ISPs are already one such entity). Here we consider that adaption could also signal different (potential) consequences which may relate to what users have experienced (as detailed in our Results, and elaborated below with scenarios). An adaptive notification approach burdens an ISP (since it requires manual intervention) [12], but preemptive action could result in fewer ongoing cases and users avoiding their phone being blocked. In some jurisdictions – including the country where the study was conducted – ISPs are expected to provide a degree of customer protection. In such cases, a legal entity could be engaged to send an email or letter, as this also has the potential to be effective [40].

Scenarios for identifying the cause of an infection. One aspect that should be included in notifications to users is more of the (albeit weaker or indirect) indicators, as at the top of Table 1, for what may cause an (otherwise difficult to detect) Flubot infection. Many of the respondents did not notice anything suspicious before receiving the notification from the ISP. A few sentences or scenarios could describe e.g., an end-user having clicked on a link inside an SMS text, or having downloaded an application outside of the OS app marketplace. These would serve as identifiable precursor events to a malware infection. There is a connection also to the breaking and formation of habits [18, 26], and specifically what the ecosystem can do to reduce the exposure of users to 'bad' habits – in the case of Flubot this could, for example, include providing safer ways to access a wider range of apps; this would strengthen the capacity to assert that e.g., OS warnings are indicative of malicious apps.

Support for recovery from personal harms. Harms should be reduced as much as possible, but evidence of harms may serve as an *indirect, non-technical indicator* of the presence of mobile malware, and so could be useful specifically when messages with malicious payloads do not prompt suspicion (since, e.g., legitimate courier messages may be sent from unknown contacts as well). Additional information could also address what to do when having experienced economical loss as a result of the infection, or what to do when having experienced psychological harm – existing ISP notifications may already relay advice from other bodies (such as manufacturers) [62], which could be extended to include non-technical support expertise.

6 RELATED WORK

There are a number of knowledge gaps around mobile malware – no academic literature examines the efficacy of remediation (and advice) on mobile phone users infected by smishing-based malware, and little research exists on anti-phishing tools for smartphones [11, 13, 32]. Jörgensson deployed a questionnaire to analyze the emerging threat landscape for users and where they source mobile applications from [37]. Bosamia et al. identified unintentional installation of rogue and malware applications as one of the biggest financial threats [8]. When looking at why end-users click on malicious links, six reasons have been found for why smartphone smishing-based attacks are successful [32], including small screen size and the downloading of apps from third parties.

Looking at user behaviors generally, Das et al. [20] identified triggers for security and privacy behavior, influenced by the Fogg Behavior Model [25], while also examining the role of social interactions and outside information sources in prompting behavior change. Studies have found that (self-perceived) technical skill and technically aligned professions do not automatically translate into better security behavior. Forget et al. [27] and Wash and Rader [82] found in their studies on security behavior regarding computers (rather than smartphones), that misaligned perceptions of expertise and inaccurate knowledge about computer security often lead to negative impacts on computer security. However, no such studies have been performed in the smartphone landscape. We find, for instance, that having suspicions about particular events or actions (such as having downloaded applications outside of the OS app marketplace) can be useful for prompting users to consider their actions – and smartphone habits – to engage in preventative steps against the kinds of mobile malware that actively evades detection, such as Flubot.

7 CONCLUSION

In the greater context of smishing-based malware, it could be said with the take-down of Flubot that a battle has been won, but that the war against smishing-based malware is not necessarily over. We partnered with an Internet Service Provider (ISP) to survey 87 customers who had suffered a Flubot infection on their mobile device, to understand their experiences and reveal the harms, informing the response to future strains of mobile- and smishing-based malware.

We found that a little over half of the respondents were unaware of the malware infection before they were notified; others claimed to have heard about it through news outlets, and social networks or personal contacts. By specifically exploring the harmful and non-technical effects of Flubot, we saw a majority of our respondents reporting having experienced harms caused by the malware, with many experiencing harms before notification and

several experiencing aggressive behavior from other infected users. Our recommendations focus around crafting support measures to reach affected users more effectively, with improved cues to help diagnose a Flubot or mobile-malware infection, and avenues for help and further information if harms do occur from such malware. The form and positioning of these recommendations will be explored as future work.

ACKNOWLEDGMENTS

The authors greatly appreciate the participation of the respondents, and the support of the partner ISP during the study. This publication is part of the RAPID project (Grant No. CS.007) financed by the Dutch Research Council (NWO).

REFERENCES

[1] Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *OUP Journal of Cybersecurity* (2018). http://kar.kent.ac.uk/69076/

[2] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. 2021. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science* 3 (3 2021). https://doi.org/10.3389/fcomp.2021.563060

[3] Ross Anderson, Chris Barton, Rainer Boehme, Richard Clayton, Carlos Ganan, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. 2019. Measuring the Changing Cost of Cybercrime. *The 18th Annual Workshop on the Economics of Information Security*. https://doi.org/10.17863/CAM.41598

[4] AppAnnie. 2021. State of Mobile 2021. https://www.data.ai/en/go/state-of-mobile-2021/

[5] Nikolay Atanassov and Minhaz Chowdhury. 2021. Mobile Device Threat: Malware. *2021 IEEE International Conference on Electro Information Technology (EIT)*, 007–013. https://doi.org/10.1109/EIT51626.2021.9491845

[6] Anabela Berenguer, Jorge Goncalves, Simo Hosio, Denzil Ferreira, Theodoros Anagnostopoulos, and Vassilis Kostakos. 2016. Are smartphones ubiquitous?: An in-depth survey of smartphone adoption by seniors. *IEEE Consumer Electronics Magazine* 6, 1 (2016), 104–110.

[7] Bitdefender. 2022. New FluBot and TeaBot Global Malware Campaigns Discovered. https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered

[8] Mansi Bosamia, Dharmendra Patel, Smt Chandaben, and Mohanbhai Patel. 2019. Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. *International Journal of Computer Sciences and Engineering Open Access Review Paper* (2019). Issue 7. https://doi.org/10.26438/ijcse/v7i1.810817

[9] Brennen Bouwmeester, Elsa Rodriguez, Carlos Gañán, Michel Van Eeten, and Simon Parkin. 2021. "The thing doesn't have a name": Learning from emergent real-world interventions in smart home security. USENIX Association, 493–512. www.usenix.org/conference/soups2021/presentation/bouwmeester

[10] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology* 18, 3 (2021), 328–352.

[11] Orcun Cetin, Carlos Ganan, Lisette Altena, Takahiro Kasama, Daisuke Inoue, Kazuki Tamiya, Ying Tie, Katsunari Yoshioka, and Michel van Eeten. 2019. Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai. *Proceedings 2019 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2019.23438

[12] Orcun Cetin, Carlos Ganan, Maciej Korczynski, and Michel van Eeten. 2017. Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning. In *Workshop on the Economics of Information Security (WEIS)*.

[13] Sharvari Prakash Chorghe and Narendra Shekokar. 2016. A survey on anti-phishing techniques in mobile phones. *2016 International Conference on Inventive Computation Technologies (ICICT)*, 1–5. https://doi.org/10.1109/INVENTIVE.2016.7824819

[14] Robert Choudhury, Zhiyuan Luo, and Khuong An Nguyen. 2022. Malware in motion. *8th International Conference on Information Systems Security and Privacy (ICISSP 2022)* (2 2022), 85. https://doi.org/10.2/JQUERY.MIN.JS

[15] Max Clasen, Fudong Li, and David Williams. 2021. Friend or foe: An investigation into recipient identification of sms-based phishing. In *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15*. Springer, 148–163.

[16] Cleafy Labs. 2021. Oscorp evolves into UBEL: an Android malware spreading across the globe. https://www.cleafy.com/cleafy-labs/ubel-oscorp-evolution

[17] Cleafy Labs. 2021. TeaBot, a new Android malware targeting banks in Europe. https://www.cleafy.com/cleafy-labs/teabot

[18] James Clear. 2018. *Atomic habits: An easy & proven way to build good habits & break bad ones*. Penguin.

[19] Radu Crahmaliuc. 2021. What is FluBot and why you need to start taking it seriously right now. https://www.bitdefender.com/blog/hotforsecurity/what-is-flubot-and-why-you-need-to-start-taking-it-seriously-right-now/

[20] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. https://www.usenix.org/conference/soups2019/presentation/das

[21] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A typology of security and privacy news and how it's shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[22] department of homeland security. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf

[23] Jason Dies. 2021. A Rapid Rise in Global Parcel Volumes Shows No Signs of Slowing. https://www.pitneybowes.com/us/shipping-index.html.

[24] Europol. 2022. Takedown of SMS-based FluBot spyware infecting Android phones | Europol. https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

[25] BJ Fogg. 2009. A behavior model for persuasive design. *ACM International Conference Proceeding Series* 350 (4 2009). https://doi.org/10.1145/1541948.1541999

[26] Brian J Fogg and Jason Hreha. 2010. Behavior wizard: A method for matching target behaviors with solutions. In *International Conference on Persuasive Technology*. Springer, 117–131.

[27] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. 2016. Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes. *Proceedings of the Twelfth Symposium on Usable Privacy and Security*. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/forget

[28] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' expectations about and use of smartphone privacy and security settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–24.

[29] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*. 21–40.

[30] Nathaniel H Fruchter. 2019. Enhancing ISP-Consumer Security Notifications. https://dspace.mit.edu/bitstream/handle/1721.1/122916/1126790910-MIT.pdf?sequence=1&isAllowed=y

[31] Christine Geeng and Franziska Roesner. 2019. Who's in control? Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[32] Diksha Goel and Ankit Kumar Jain. 2018. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security* 73 (3 2018), 519–544. https://doi.org/10.1016/j.cose.2017.12.006

[33] NZ Herald. 2022. FluBot: Nasty phone virus sends spam messages that can cost you thousands - NZ Herald. https://www.nzherald.co.nz/business/flubot-nasty-phone-virus-sends-spam-messages-that-can-cost-you-thousands/63SINI7ODSIZLKFCGUTMMZZLVA/

[34] Lidia Howler. 2021. UBEL – the successor of Oscorp Android credential stealing malware. https://howtoremove.guide/ubel-oscorp-android-malware/

[35] Markus Jakobsson. 2018. Two-factor inauthentication – the rise in SMS phishing attacks. *Computer Fraud & Security* 2018 (6 2018). Issue 6. https://doi.org/10.1016/S1361-3723(18)30052-6

[36] W Stuart Jones. 2021. Choose Your Own Compromise: Attackers Use Similar Lures to Deliver Both Smishing and Malware Attacks | Proofpoint US. *Proofpoint* (12 2021). https://www.proofpoint.com/us/blog/email-and-cloud-threats/choose-your-own-compromise-attackers-use-similar-lures-deliver-both

[37] Anton Jörgensson. 2018. Bachelor's Programme in IT-forensics and Information Security, 180 credits Malware in Mobile Devices. http://hh.diva-portal.org/smash/get/diva2:1248547/FULLTEXT01.pdf

[38] Nanda Kumar, Kannan Mohan, and Richard Holowczak. 2008. Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems* 46 (12 2008), 254–264. Issue 1. https://doi.org/10.1016/J.DSS.2008.06.010

[39] Yassine Lemmou, Jean-Louis Lanet, and El Mamoun Souidi. 2021. A behavioural in-depth analysis of ransomware infection. *IET Information Security* 15, 1 (2021), 38–58.

[40] Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, and Indra Spiecker. 2021. Effective notification campaigns on the web: A matter of trust, framing, and support. In *30th USENIX Security Symposium (USENIX Security 21)*. 2489–2506.

[41] Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone, and Gigliola Vaglini. 2020. Model checking and machine learning techniques for HummingBad mobile malware detection and mitigation. *Simulation Modelling Practice and Theory* 105 (2020), 102169.
[42] McAfee. 2019. The Cerberus Banking Trojan: 3 Tips to Secure Your Financial Data. https://www.mcafee.com/blogs/privacy-identity-protection/cerberus-banking-trojan/
[43] T Meskauskas. 2022. Anatsa Trojan (Android) - Malware removal instructions (updated). https://www.pcrisk.com/removal-guides/23778-anatsa-trojan-android
[44] T Meskauskas. 2022. ERMAC 2.0 Trojan (Android) - Malware removal instructions (updated). https://www.pcrisk.com/removal-guides/23920-ermac-20-trojan-android
[45] T Meskauskas. 2022. SMSControllo Malware (Android) - Malware removal instructions. https://www.pcrisk.com/removal-guides/23607-smscontrollo-malware-android
[46] Benjamin Morrison, Lynne Coventry, and Pam Briggs. 2021. How do Older Adults feel about engaging with Cyber-Security? *Human Behavior and Emerging Technologies* 3, 5 (2021), 1033–1049.
[47] Ashawa Moses and Sarah Morris. 2021. Analysis of mobile malware: a systematic review of evolution and infection strategies. *Journal of Information Security and Cybercrimes Research* 4, 2 (2021), 103–131.
[48] James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. 2021. Training and Embedding Cybersecurity Guardians in Older Communities. *Association for Computing Machinery* (2021), 86. https://doi.org/10.1145/3411764.3445078
[49] Baodi Ning. 2021. *Analysis of the Latest Trojans on Android Operating System*. Ph. D. Dissertation.
[50] Baodi Ning, Guanqin Zhang, and Zexin Zhong. 2020. An evolutionary perspective: a study of Anubis Android banking trojan. In *2020 7th International Conference on Dependable Systems and Their Applications (DSA)*. IEEE, 141–150.
[51] Dor Nizar and Roy Moshailov. 2022. FluBot's Authors Employ Creative and Sophisticated Techniques to Achieve Their Goals in Version 5.0 and Beyond | F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/flubots-authors-employ-creative-and-sophisticated-techniques-to-achieve-their-goals-in-version-50-and-beyond
[52] Federal Bereau of Investigation (FBI) (US). 2022. Internet Crime Complaint Center (IC3) Elder Fraud Report. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf
[53] Pierluigi Paganini. 2022. FluBot malware continues to evolve. What's new in Ver 5.0 and beyond? https://securityaffairs.co/wordpress/126451/malware/flubot-ver-5-0-improvements.html
[54] Simon Parkin, Elissa M. Redmiles, Lynne Coventry, and M. Angela Sasse. 2019. Security When it is Welcome: Exploring Device Purchase as an Opportune Moment for Security Behavior Change. Internet Society. https://doi.org/10.14722/usec.2019.23024
[55] Politie. 2022. Politie stopt internationaal verspreiding FluBot malware | politie.nl. https://www.politie.nl/nieuws/2022/juni/1/02-politie-stopt-internationaal-verspreiding-flubot-malware.html
[56] Andrea Possemato, Dario Nisi, and Yanick Fratantonio. 2021. Preventing and Detecting State Inference Attacks on Android.. In *NDSS*.
[57] Attia Qamar, Ahmad Karim, and Victor Chang. 2019. Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems* 97 (8 2019), 887–909. https://doi.org/10.1016/j.future.2019.03.007
[58] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (2015), 121–144.
[59] Nikki Ralston. 2021. Flubot Threat Bulletin – Allot blocks over 140M C&C connection attempts - Security Boulevard. https://securityboulevard.com/2021/05/flubot-threat-bulletin-allot-blocks-100m-cc-connection-attempts/
[60] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64.
[61] Karen Renaud and Marc Dupuis. 2019. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop*. 42–56.
[62] Elsa Rodríguez, Max Fukkink, Simon Parkin, Michel Van Eeten, and Carlos Gañán. 2022. Difficult for Thee, But Not for Me: Measuring the Difficulty and User Experience of Remediating Persistent IoT Malware. (3 2022). https://doi.org/10.1109/EuroSP53844.2022.00032
[63] Ruik. 2021. Anatsa Android Malware Uses Fake Delivery Notifications to Infect Victims. https://www.cyclonis.com/anatsa-android-malware-uses-fake-delivery-notifications-to-infect-victims/
[64] Hank Schless. 2021. FluBot: Malware as a Service Meets Mobile Phishing. https://resources.lookout.com/blog/flubot-malware-as-a-service-meets-mobile-phishing
[65] Alberto Segura and Rolf Govers. 2022. Flubot: the evolution of a notorious Android Banking Malware – Fox-IT International blog. https://blog.fox-it.com/2022/06/29/flubot-the-evolution-of-a-notorious-android-banking-malware/amp/
[66] Shadowserver. 2019. Drone/Botnet-Drone Report | Shadowserver. https://www.shadowserver.org/what-we-do/network-reporting/drone-botnet-drone-report/
[67] Chen Shi, Chris Chao-Chun Cheng, and Yong Guan. 2021. Forensic Analysis on Joker Family Android Malware. In *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 403–406.
[68] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, and Nasir Memon. 2017. Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers & Security* 65 (3 2017). https://doi.org/10.1016/j.cose.2016.09.009
[69] Camelia Simoiu, Christopher Gates, Joseph Bonneau, and Sharad Goel. 2019. "I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 155–174.
[70] Saskia Speelman. 2021. ACM: Parcel delivery market grows even faster as a result of the pandemic | ACM.nl. https://www.acm.nl/en/publications/acm-parcel-delivery-market-grows-even-faster-result-pandemic
[71] Eric Spero, Milica Stojmenović, Zahra Hassanzadeh, Sonia Chiasson, and Robert Biddle. 2019. Mixed pictures: Mental models of malware. In *2019 17th International Conference on Privacy, Security and Trust (PST)*. IEEE, 1–3.
[72] Statcounter. 2022. Mobile Operating System Market Share Worldwide | Statcounter Global Stats. https://gs.statcounter.com/os-market-share/mobile/worldwide
[73] Ben Stock, Giancarlo Pellegrino, Frank Li, Michael Backes, and Christian Rossow. 2018. Didn't you hear me?—Towards more successful web vulnerability notifications. *Network and Distributed Systems Security (NDSS) Symposium 2018* (2018).
[74] André Tavares. 2022. FluBot Malware Persists: Most Prevalent In Germany and Spain. https://www.bitsight.com/blog/flubot-malware-persists-most-prevalent-germany-and-spain
[75] Techtarget contributor. 2017. What is command-and-control server (C&C server)? https://www.techtarget.com/whatis/definition/command-and-control-server-CC-server
[76] Telecompaper. 2021. KPN waarschuwt voor smishingmalware Flubot. https://www.telecompaper.com/news/kpn-waarschuwt-voor-smishingmalware-flubot--1384249
[77] Bill Toulas. 2021. Anubis Android malware returns to target 394 financial apps. https://www.bleepingcomputer.com/news/security/anubis-android-malware-returns-to-target-394-financial-apps/
[78] Filip Truta. 2022. Rejuvenated FluBot Campaign Moves to Finland; iPhone Users Also Targeted. https://www.bitdefender.com/blog/hotforsecurity/rejuvenated-flubot-campaign-moves-to-finland-iphone-users-also-targeted-2/
[79] Shailen Tuli. 2020. Developing an Accessibility Service for Android. https://codelabs.developers.google.com/codelabs/developing-android-a11y-service#0
[80] Vishnu Varadaraj. 2021. Beware of BRATA: How to Avoid Android Malware Attack. https://www.mcafee.com/blogs/mobile-security/beware-of-brata-how-to-avoid-android-malware-attack/
[81] Rick Wash, Norbert Nthala, and Emilee Rader. 2021. Knowledge and Capabilities that Non-Expert Users Bring to Phishing Detection. *Proceedings of the Seventeenth Symposium on Usable Privacy and Security*. (8 2021). www.usenix.org/conference/soups2021/presentation/wash
[82] Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. *Symposium on Usable Privacy and Security (SOUPS) 2015*. https://bitlab.cas.msu.edu/papers/security-survey.pdf
[83] Fengguo Wei, Yuping Li, Sankardas Roy, Xinming Ou, and Wu Zhou. 2017. Deep ground truth analysis of current android malware. In *Detection of Intrusions and Malware, and Vulnerability Assessment: 14th International Conference, DIMVA 2017, Bonn, Germany, July 6-7, 2017, Proceedings 14*. Springer, 252–276.
[84] Mei-Ling Yao, Ming-Chuen Chuang, and Chun-Cheng Hsu. 2018. Research on the User Attitudes and Behaviors of Mobile Security and Antivirus. *International Journal of Liberal Arts and Social Science* 6 (6 2018). Issue 5. www.ijlass.org

APPENDIX A – SURVEY QUESTIONS

Demographics

(1) Enter your age
(2) Enter your profession
(3) How experienced are you in using and restoring your smartphone? Give an estimation of hardly any experience (1) to expert (5).

Awareness: cause and suspicions

(4) Before you we're informed by [partner ISP], did you have any experience with sms-phishing malware, like Flubot. [Yes / No]
(5) How did you learn about sms-phishing malware, like Flubot? (multiple answers possible) [work, family, friends, news, government, telecom provider, social media, previous infection, other]
(6) Before you we're informed, did you experience something different or suspicious on your phone. [Yes / No]
(7) Explain what you noticed.
(8) Do you have an idea what caused the infection. [Yes / No]

(9) What do you think caused the infection?
(10) How often do you receive SMS messages on average per week? Without counting friends and family.
(11) How likely are you to click on a URL link in a text message that is not from friends or family? Give an estimate from very unlikely (1) to very likely (5).

Remediation

(12) Did you fix the Flubot infection? [Yes or No]
(13) How many days did it take you to clear up the Flubot infection after you were informed? Explain why not.

Harms

Harm descriptions: (1) Physical or digital distress: a physical or digital negative effect on someone or something (for example, losing your phone or data, or getting physically hurt); (2) Economic distress: negative financial or economic consequences; (3) Psychological distress: a negative effect on mental well-being; (4) Reputational distress: a negative effect on the general opinion of someone or something; (5) Social and societal suffering: a negative effect in a social or societal context.

(14) Different types of suffering;
1. Physical or digital suffering:
2. Economic suffering:
3. Psychological suffering:
4. Reputational suffering:
5. Social suffering:
(15) Given the types of distress, have you experienced any distress as a result of the Flubot infection? [Yes, before I was informed; Yes, after I was informed; No.]
(16) What type of suffering have you experienced as a result of the Flubot infection? Please estimate the impact the suffering has had on you, from low impact (1) to high impact (5) or "No impact" if that type is not applicable.
(17) Explain what kind of suffering you have experienced (including the seriousness of the suffering you have experienced).

Remediation experience

(18) On a scale from very bad (1) to very good (5), how did you experience the Flubot infection and its resolution, regarding: [(A) The information in the original email about how to resolve the Flubot infection; (B) The available support and resources provided by [partner ISP]]
(19) Explain your experience.
(20) Since the Flubot infection, has it changed how you use your smartphone? [Yes or No]
(21) Explain the change in use of your smartphone.

APPENDIX B – STATISTICAL ANALYSIS

Correlation significant, at the 0.01 level (2-tailed)):

- Demo_SkillLevelSmartphone and 4_SatisfactionInformationProvision: a correlation of 0.324 and a 2-tailed significance of 0.002 with a N of 87.
- 1_AverageWeeklySMS and 1_LikelihoodClickingUnknownSender: a correlation of .402 and a 2-tailed significance of 0.000 with a N of 87.
- 1_LikelihoodClickingUnknownSender and 3_HarmReputational: a correlation of 0.444 and a 2-tailed significance of 0.002 with a N of 48.
- 3_HarmEconomic and 3_HarmReputational: a correlation of 0.434 and a 2-tailed significance of 0.002 with a N of 48.
- 3_HarmEconomic and 3_HarmSocietal: a correlation of 0.492 and a 2-tailed significance of 0.000 with a N of 48.
- 3_HarmPsychological and 3_HarmReputational: a correlation of 0.517 and a 2-tailed significance of 0.000 with a N of 48.
- 3_HarmPsychological and 3_HarmSocietal: a correlation of 0.538 and a 2-tailed significance of 0.000 with a N of 48.
- 3_HarmReputational and 3_HarmSocietal: a correlation of 0.879 and a 2-tailed significance of 0.000 with a N of 48.
- 4_SatisfactionInformationProvision and 4_SatisfactionSupport: a correlation of 0.620 and a 2-tailed significance of 0.002 with a N of 87.

Correlation significant, at the 0.05 level (2-tailed)):

- 10. Demo_SkillLevelSmartphone and 4_SatisfactionSupport: a correlation of 0.221 and a 2-tailed significance of 0.040 with a N of 87.
- 11. 1_LikelihoodClickingUnknownSender and 3_HarmPsychological: a correlation of 0.348 and a 2-tailed significance of 0.015 with a N of 48.
- 12. 1_LikelihoodClickingUnknownSender and 3_HarmSocietal: a correlation of 0.299 and a 2-tailed significance of 0.039 with a N of 48.
- 13. 3_HarmEconomic and 3_HarmPsychological: a correlation of 0.341 and a 2-tailed significance of 0.018 with a N of 48.

APPENDIX C – SPEARMAN'S CORRELATION ON SURVEY RESULT VARIABLES

Correlations

			Demo_AGE	Demo_SkillLevelSmartphone	1_AverageWeeklySMS	1_LikelihoodClickingUnknownSender	2_DaysTakenRemediation
Spearman's rho	Demo_AGE	Correlation Coefficient	1.000	.110	.204	.002	.182
		Sig. (2-tailed)	.	.311	.059	.988	.140
		N	87	87	87	87	67
	Demo_SkillLevelSmartphone	Correlation Coefficient	.110	1.000	.082	-.057	-.164
		Sig. (2-tailed)	.311	.	.448	.600	.184
		N	87	87	87	87	67
	1_AverageWeeklySMS	Correlation Coefficient	.204	.082	1.000	.402**	.115
		Sig. (2-tailed)	.059	.448	.	.000	.352
		N	87	87	87	87	67
	1_LikelihoodClickingUnknownSender	Correlation Coefficient	.002	-.057	.402**	1.000	-.228
		Sig. (2-tailed)	.988	.600	.000	.	.064
		N	87	87	87	87	67
	2_DaysTakenRemediation	Correlation Coefficient	.182	-.164	.115	-.228	1.000
		Sig. (2-tailed)	.140	.184	.352	.064	.
		N	67	67	67	67	67
	3_HarmPhysicalDigital	Correlation Coefficient	-.089	-.061	-.155	-.279	.189
		Sig. (2-tailed)	.550	.681	.294	.055	.225
		N	48	48	48	48	43
	3_HarmEconomic	Correlation Coefficient	.157	.059	-.088	.083	-.248
		Sig. (2-tailed)	.288	.689	.553	.576	.110
		N	48	48	48	48	43
	3_HarmPsychological	Correlation Coefficient	.162	.016	.119	.348*	.044
		Sig. (2-tailed)	.273	.912	.421	.015	.779
		N	48	48	48	48	43
	3_HarmReputational	Correlation Coefficient	-.023	.048	.256	.444**	.009
		Sig. (2-tailed)	.879	.748	.079	.002	.955
		N	48	48	48	48	43
	3_HarmSocietal	Correlation Coefficient	.034	.071	.198	.299*	.044
		Sig. (2-tailed)	.818	.633	.176	.039	.780
		N	48	48	48	48	43

Figure 5: Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 1 of 4.

Correlations

			3_HarmPhysicalDigital	3_HarmEconomic	3_HarmPsychological	3_HarmReputational	3_HarmSocietal
Spearman's rho	Demo_AGE	Correlation Coefficient	-.089	.157	.162	-.023	.034
		Sig. (2-tailed)	.550	.288	.273	.879	.818
		N	48	48	48	48	48
	Demo_SkillLevelSmartphone	Correlation Coefficient	-.061	.059	.016	.048	.071
		Sig. (2-tailed)	.681	.689	.912	.748	.633
		N	48	48	48	48	48
	1_AverageWeeklySMS	Correlation Coefficient	-.155	-.088	.119	.256	.198
		Sig. (2-tailed)	.294	.553	.421	.079	.176
		N	48	48	48	48	48
	1_LikelihoodClickingUnknownSender	Correlation Coefficient	-.279	.083	.348*	.444**	.299*
		Sig. (2-tailed)	.055	.576	.015	.002	.039
		N	48	48	48	48	48
	2_DaysTakenRemediation	Correlation Coefficient	.189	-.248	.044	.009	.044
		Sig. (2-tailed)	.225	.110	.779	.955	.780
		N	43	43	43	43	43
	3_HarmPhysicalDigital	Correlation Coefficient	1.000	.056	.190	.086	.141
		Sig. (2-tailed)	.	.706	.195	.563	.340
		N	48	48	48	48	48
	3_HarmEconomic	Correlation Coefficient	.056	1.000	.341*	.434**	.492**
		Sig. (2-tailed)	.706	.	.018	.002	.000
		N	48	48	48	48	48
	3_HarmPsychological	Correlation Coefficient	.190	.341*	1.000	.517**	.538**
		Sig. (2-tailed)	.195	.018	.	.000	.000
		N	48	48	48	48	48
	3_HarmReputational	Correlation Coefficient	.086	.434**	.517**	1.000	.879**
		Sig. (2-tailed)	.563	.002	.000	.	.000
		N	48	48	48	48	48
	3_HarmSocietal	Correlation Coefficient	.141	.492**	.538**	.879**	1.000
		Sig. (2-tailed)	.340	.000	.000	.000	.
		N	48	48	48	48	48

Figure 6: Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 2 of 4.

Correlations

			4_SatisfactionInformationProvision	4_SatisfactionSupport
Spearman's rho	Demo_AGE	Correlation Coefficient	-.033	-.059
		Sig. (2-tailed)	.763	.589
		N	87	87
	Demo_SkillLevelSmartphone	Correlation Coefficient	.324**	.221*
		Sig. (2-tailed)	.002	.040
		N	87	87
	1_AverageWeeklySMS	Correlation Coefficient	.060	-.069
		Sig. (2-tailed)	.581	.523
		N	87	87
	1_LikelihoodClickingUnknownSender	Correlation Coefficient	-.003	.003
		Sig. (2-tailed)	.981	.980
		N	87	87
	2_DaysTakenRemediation	Correlation Coefficient	-.022	-.130
		Sig. (2-tailed)	.858	.294
		N	67	67
	3_HarmPhysicalDigital	Correlation Coefficient	-.098	-.089
		Sig. (2-tailed)	.506	.549
		N	48	48
	3_HarmEconomic	Correlation Coefficient	-.158	-.015
		Sig. (2-tailed)	.283	.917
		N	48	48
	3_HarmPsychological	Correlation Coefficient	-.036	.001
		Sig. (2-tailed)	.806	.997
		N	48	48
	3_HarmReputational	Correlation Coefficient	.116	-.028
		Sig. (2-tailed)	.434	.853
		N	48	48
	3_HarmSocietal	Correlation Coefficient	.124	-.066
		Sig. (2-tailed)	.400	.656
		N	48	48

Figure 7: Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 3 of 4.

Correlations

		Demo_AGE	Demo_SkillLevelSmartphone	1_AverageWeeklySMS	1_LikelihoodClickingUnknownSender	2_DaysTakenRemediation
4_SatisfactionInformationProvision	Correlation Coefficient	-.033	.324**	.060	-.003	-.022
	Sig. (2-tailed)	.763	.002	.581	.981	.858
	N	87	87	87	87	67
4_SatisfactionSupport	Correlation Coefficient	-.059	.221*	-.069	.003	-.130
	Sig. (2-tailed)	.589	.040	.523	.980	.294
	N	87	87	87	87	67

Correlations

		3_HarmPhysicalDigital	3_HarmEconomic	3_HarmPsychological	3_HarmReputational	3_HarmSocietal
4_SatisfactionInformationProvision	Correlation Coefficient	-.098	-.158	-.036	.116	.124
	Sig. (2-tailed)	.506	.283	.806	.434	.400
	N	48	48	48	48	48
4_SatisfactionSupport	Correlation Coefficient	-.089	-.015	.001	-.028	-.066
	Sig. (2-tailed)	.549	.917	.997	.853	.656
	N	48	48	48	48	48

Correlations

		4_SatisfactionInformationProvision	4_SatisfactionSupport
4_SatisfactionInformationProvision	Correlation Coefficient	1.000	.620**
	Sig. (2-tailed)	.	.000
	N	87	87
4_SatisfactionSupport	Correlation Coefficient	.620**	1.000
	Sig. (2-tailed)	.000	.
	N	87	87

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Figure 8: Correlations, significance and N per variable correlation in SPSS for all ordinal and ratio variables, page 4 of 4.