The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan

Nissy Sombatruang*, Youki Kadobayashi†, M. Angela Sasse‡, Michelle Baddeley§ and Daisuke Miyamoto†
*Department of Security and Crime Science
University College London, London, UK
E-mail: uctznso@ucl.ac.uk
†Laboratory for Cyber Resilience
Nara Institute of Science and Technology, Nara, Japan
E-mail: {youki-k, daisu-mi}@is.naist.jp
‡Department of Computer Science
University College London, London, UK
E-mail: a.sasse@ucl.ac.uk
§Institute for Choice
University of South Australia, Adelaide, Australia
E-mail: michelle.baddeley@unisa.edu.au

***Abstract*—Many people find public Wi-Fi networks convenient but these networks harbor security and privacy risks. As public knowledge of these risks becoming common, we investigated whether the risks were still at large and what factors influenced users to use the networks — being the first study to draw evidence from Japan. Adapting the methodology from a previous study in the UK, we first set up an experimental open public Wi-Fi network at 11 locations in downtown Nara and captured Internet traffic. From approximately 7.7 million packets captured from 196 unique mobile devices during a 150-hour experiment, we found private photos, emails, documents, and login credentials being transmitted in clear text without encryption — confirming that not only did many applications still fail to encrypt data-in-motion but also did many users continue to use unsecured public Wi-Fi networks. We then used a scenario-based survey to examine factors affecting the users' decision to use the networks. From 103 participants, we found that the desire to conserve mobile data — a form of resource preservation heuristic — instigated a risk-taking attitude and influenced participants, especially among those usually having a small monthly data plan, to use unsecured public Wi-Fi networks. Female and those having finish high-school only, were also more likely to use the networks.**

***Index Terms*—Public Wi-Fi Security, Human-Centered Security, Users Decision-Making, Resource Preservation Heuristic**

I. Introduction

Public Wi-Fi networks provide access to many services for users on the move. However, while offering convenient access at little to no cost, most public Wi-Fi networks harbor security and privacy risks — especially open networks which required no authentication and provided no encryption. Numerous stories have appeared in the media (e.g. [4], [27], [36], [26], [28]). Many theoretical studies also support such claims ([1], [3], [32], [38], [40]); so does empirical evidence ([5], [6], [9], [16], [19], [33]).

Despite growing public knowledge about the risks, public Wi-Fi networks continue to expand. In Japan, there were about 500,000 hotspots in 2016 [39], are 800,000 in 2018 [13], and are expected to grow further, especially in the anticipation of the 2020 Tokyo Olympics [23]. But to date, no previous studies have investigated either the risks or the factors influencing users to use unsecured public Wi-Fi in this country. We are the first to address this gap.

To this end, we adapted and improved upon the work of Sombatruang *et al.* [33] originally conducted in the UK in 2016 in the Japanese town of Nara. We set up our own experimental free open public Wi-Fi network for 150 hours during November and December 2017, and inspected the traffic for sensitive information that was transmitted insecurely. Our findings confirmed that the risks of public Wi-Fi in Japan were still at large — worrying that despite the country has done well in many aspects of cyber security such as having one of the lowest malware infection rates [35], public Wi-Fi risks may have been overlooked.

Understanding the factors influencing users to use these unsecured networks is an important first step to mitigate the risks. We again adapted a scenario-based survey from the same previous study [33], adopted part of their analysis method, and added new tests to examine factors in more depth.

First, we investigated the role of the desire to preserve mobile data, hereafter called *resource preservation heuristic*. Sombatruang *et al.* [33] originated this idea, showing that female preferred public Wi-Fi to save mobile data. However, their study did not investigate this heuristic in depth — disabling us to observe its true effect in the decision-making. We aimed to address this gap. We considered this heuristic important, especially now that many people have mobile data, a more secure means to use the Internet — but the trade-off mechanism for choosing between mobile data and a potentially unsecured public Wi-Fi network is not very well understood.

We consulted the literature from economic and psychology which have previously examined how the constraint of re-

sources captures the attention, triggers intrusive thoughts, and creates cognitive loads which could lead to myopic decision-making ([31], [42], [20], [25], [34], [24], [29]). Our findings support this notion. The constraint of mobile data instigated resource preservation heuristic, leading to the decisions to use a potentially unsecured public Wi-Fi.

Next, we examined how the perceived risks public Wi-Fi affected the decision-making. Evidence from previous studies are limited and inconsistent. One study argued that users of public Wi-Fi networks were not aware of the risk [19]. Others show that users were aware of the risks but did not think the risks would be realised ([30], [37], [21]). Sombatruang *et al.* [33] did not statistically test this factor either and so we did and found that it did not significantly affect the decision-making.

We also investigated the roles of demographic factors and found a significant relationship between gender and education level and the tendency to use public Wi-Fi.

The paper is structured as follows: Section II and III introduced related work and methodology, respectively. The results are in Section IV. We discussed the application of our work, its limitation, and possible future work in Section V, before presenting the conclusion in Section VI.

II. Related Work

Our study related to the study of public Wi-Fi risks and of factors affecting user's decisions to use the networks.

A. Security and privacy risks of unsecured Wi-Fi networks

The security and privacy risks of unsecured public Wi-Fi networks are not new. The wireless transmission nature of Wi-Fi makes the data travelling through these networks vulnerable to various types of attack such as man-in-the-middle ([1], [3], [32], [38]) and eavesdropping ([19], [16]), especially when the networks do not use encryption. Many free public Wi-Fi fall into this category [2]. Even with an encryption standard such as WPA2, Wi-Fi is not immune from vulnerabilities [40].

Empirical evidence is also mounting. Cheng *et al.* [6] found leaked sensitive user information while using public Wi-Fi at various airports — worrying given that many travelers use public Wi-Fi at airports. Chen *et al.* [5] also found sensitive data such as medical history and family income leaking from a Wi-Fi side channel. Some of these data are highly sensitive in nature and could be subject to data protection law in many jurisdictions. F-Secure [9] provided further evidence, capturing one username and password in the clear during a 30-min free Wi-Fi experiment in central London (UK) in 2014. Sombatruang *et al.* [33] also found one online dating app transmitted information such as name, date of birth, and sexual orientation unencrypted, in a similar experiment in 2016.

We wanted to investigate whether these risks were still at large in Japan, given the growing knowledge of public Wi-Fi risks and many media reports (e.g. [4], [27], [36], [26], [28]). Being the first study in Japan would also give local insight, especially useful to the Japanese authorities whose interest in cyber security have grown substantively in the past few years.

B. Factors affecting a user's decision to use public Wi-Fi

Understanding factors influencing users to use unsecured public Wi-Fi is an important first step to mitigate the risks. The perceived risk of using the networks is a good starting point. Klasnja *et al.* [19] found that public Wi-Fi users did not know the risk involved. But public knowledge may have evolved since their study in 2009. Seigneur *et al.* [30] gave an alternative view. Only 10% of their participants responded "*No*" when asked whether they knew that a Wi-Fi hotspot could be easily impersonated. But 58.4% responded "*I don't care*". Perhaps, public Wi-Fi users did know about the risks but they simply did not care. McShane *et al.* [21] supported the claim; 25% of their participants admitted to have used unsecured public Wi-Fi for financial purpose despite security concern being the top most common reason for not using it.

Swanson *et al.* [37] offered another explanation. Their participants said they used public Wi-Fi because, despite awareness of certain risks, they did not believe the risks would be realised. Participants in Klasnja *et al.* [19]'s study echoed this feeling of invincibility, believing their devices had sufficient security measures to mitigate the risks — worrying as many users do not update their software ([17], [41], [43]).

Other studies show that trust in public Wi-Fi lies in the cues — the environment when the users connect to the networks. Ferreira *et al.* [11] found that the name of Wi-Fi affected user's trust. Kindberg *et al.* [18] found that users could be influenced by location-relevant images displayed on the log-in page. Ferreira *et al.* [10] and Jeske *et al.* [15] also showed that a security padlock next to the Wi-Fi name promoted trust.

Another important factor is the constraint of mobile data but it was largely overlooked until the work of Sombatruang *et al.* [33]. They initially tested whether users' decision to use public Wi-Fi aligned with the expected utility theory. But they also found that more females than males preferred public Wi-Fi to save mobile data — shedding new light of the importance of mobile data preservation heuristic. However, their study did not investigate this heuristic in depth — disabling us to understand the true effect and the situation which prompts the heuristic. We wanted to address this gap. Data from Japan would also test if the heuristic has a universal nature.

To pave a foundation, we consulted the economic and psychology literature studying decision-making of those with constrained financial resources. We considered them and the users with constrained mobile data to be most comparable.

Previous studies found that scarcity — the state of not having enough — has many hidden costs including the reduced cognitive bandwidth needed to think clearly and effectively ([42], [25], [24], [29]). Shah *et al.* [31] used lab experiments and showed that financial difficulties created a cognitive load which could lead poor participants to make riskier sub-optimal financial decisions. This may explain the findings from Sombatruang *et al.* [33]'s study. The thought of running out of data may also create a similar cognitive load which led participants to take risks from using a potentially unsecured public Wi-Fi.

Mani *et al.* [20] provided another evidence. In the lab experiments, they found inducing thoughts about finances reduced cognitive performance among poor participants. Their fieldwork experiments in India confirmed the theory. The same sugarcane farmer did worse on a cognitive performance test before the harvest when money was scarce. Being poor was stressful and so cognitive load was diverted towards worrying about the difficult circumstances at hands. Spears [34] also noted similar findings. Participants, assigned to receive one or two household items for free, did worse in the cognitive tests than did those assigned to get more free items. Having a small budget taxed their minds (from having to choose items they wanted most), leading to poor cognitive performance.

These related works all point to one notion. The constraint of resources introduces cognitive load and trigger intrusive thoughts that could lead to sub-optimal decision-making. Hence, we hypothesized that the constraints of mobile data too would trigger an intrusive thoughts and influence participants to take risks of using potentially unsecured public Wi-Fi.

In this section, we present the related work. The next section, Section III, discusses the methodology.

III. Methodology

Our study has two parts: the risks of public Wi-Fi and factors influencing users to use it. We adapted and improved the methodology from the work of Sombatruang *et al.* [33].

A. Security and privacy risks of unsecured public Wi-Fi

We set up a free open public Wi-Fi network (SSID = *.Free JP Wi-Fi*) and monitored traffic for 150 hours during November and December 2017 at 11 locations in downtown Nara (Appendix A). The network consisted of a laptop running on Kali Linux OS (4.13.0-kali1-686-pae), an iPad (OS 10.3.3), a data sim card by IIJmio, a USB cable for connecting an iPad to a laptop, and a customized Python-based captive portal application[1]. We replaced a Windows-based setup previously used in Sombatruang *et al.*'s study with a Unix-based as many newer mobile OS did not detect Windows-based hotspots. No registration or authentication was required to use our network. However, potential users were routed to a login page which forced a user to accept the terms and conditions of usage before using the network. We considered this setup the closest design to many real-life open unsecured public Wi-Fi.

We used Wireshark (v.2.4.1), a network analyser software, to capture and analyse the traffic passing through our Wi-Fi network. We also used Network Miner (v.2.2.0.0), a forensic software not previously used in the work of Sombatruang *et al.* to reconstruct data traffic more effectively. We examined traffic that was transmitted via HTTP, an unencrypted protocol, and via Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP), the last three of which could reveal the content and the credentials of emails if not configured properly.

[1]Adapted from www.github.com/AloysAugustin/captive_portal

B. Factors affecting users' decisions to use unsecured Wi-Fi

We used a scenario-based online survey which asked participants to decide whether they would use public Wi-Fi in hypothetical scenarios. We launched the survey in November 2017 and completed the data collection in the same month.

1) Recruitment and participants: We hired Macromill[2] to recruit participants. The firm has a diverse demographic of 10 million participants nationwide which would allow well-balanced samples. Eligible participants were restricted to only those living in Japan and aged at least 18, all of whom had at least one mobile device, and had used public Wi-Fi in the past, according to the self-assessed pre-screening questions. Each participant received a reward[3] for their participation. A total of 103 participants with diverse background were recruited (Appendix B), all of them have Japanese nationality.

2) Survey questions and platform: We adopted the eight scenarios from Sombatruang *et al.*'s study [33] but changed some elements to accommodate local environment e.g. replaced Whatsapp with LINE, a more popular app in Japan. We translated the survey to Japanese and pilot tested it with a student and a staff at the institution, and with Macromill staff.

The eight scenarios covered different transaction types, degree of urgency, and location of the scenario (Table I), allowing us to examine how participants made decision in different contexts. All participants were given the same eight scenarios but the order of the cases were randomized by the system to minimize the anchoring effect and response biases.

In each scenario, we asked participants to choose whether they would use the Internet and, if so, by free open public Wi-Fi or mobile data plan/roaming, supposing they have 100%, 75%, 50%, and 25% left on data allowance. These constraints would allow us to examine how resource preservation heuristic influenced the decision to use unsecured public Wi-Fi.

The descriptions and the rationale for each scenario are listed below. Paragraphs I, II, and the questions from scenario I applied to all other scenarios, except for 1GB data plan (¥1500) was replaced with 20MB (¥2000) data roaming plan and the transaction size of 100MB was replaced with 2MB in scenario V-VIII which placed participants outside Japan.

Scenario I:"*You are waiting at a train station in Japan. When you arrive, you see that the train is running 1 hour late.*

[2]A Japanese marketing research firm (www.group.macromill.com)

[3]The amount is commercial data and is kept confidential by Macromill

TABLE I SCENARIOS TYPES

Scenario	Type of Transaction	Urgency	Location
I	Non-financial	Non-urgent	In Japan
II	Non-financial	Urgent	In Japan
III	Financial	Non-urgent	In Japan
IV	Financial	Urgent	In Japan
V	Non-financial	Non-urgent	Outside Japan
VI	Non-financial	Urgent	Outside Japan
VII	Financial	Non-urgent	Outside Japan
VIII	Financial	Urgent	Outside Japan

You want to check messages on messaging apps (e.g. LINE) or emails but you do NOT urgently need to contact anyone in particular. You last checked your messages 2 hours ago."

Paragraph I: "*...You then scan for Wi-Fi hotspots and find a free open public Wi-Fi network you never used before. This network is working properly. No registration or password is required to use it. You can use the Wi-Fi as long as you like.*"

Paragraph II: "*Suppose you also have a 4G data plan. You have paid ¥1500 for 1GB which has no expiration date. The 4G network works properly. Using the Internet will use about 100MB of your data plan (i.e. 10% of 1GB allowance). (To illustrate, 1 min of a standard video clip is 5MB.)*"

Question: "*Would you use the Internet and by which mean?*"

1) You have **1GB** left on your mobile data plan
   - Yes, via free Wi-Fi.
   - Yes, via the data plan.
   - No, I will not connect to the Internet.
2) You have **0.75GB** (75% of 1GB) left on data plan
3) You have **0.50GB** (50% of 1GB) left on data plan
4) You have **0.25GB** (25% of 1GB) left on data plan

In scenario I, we placed participants in Japan, a familiar environment. We asked whether they would make non-urgent non-financial transactions and, if so, by which mean. We hypothesized that as data allowance decreased, participants would exhibit a risk-taking attitude and choose public Wi-Fi.

Scenario II: "*You are waiting for a train home (in Japan) late in the evening when you realise you have lost the keys to the apartment you share with a friend. You know the friend will leave the flat before you arrive to catch a flight on a 2-week vacation. You call her but she does not answer. You can call a locksmith service but it will be expensive. You can contact your friend via a messaging app on her iPad.*"

In scenario II, we also placed participants in Japan, and asked them whether they would make non-financial transactions. But with time pressure, we hypothesized that they would be unable to assess the situation effectively and be more likely to take risks from a potentially unsecured public Wi-Fi.

Scenario III: "*You are working in a town in Japan away from home and have decided to catch a movie at a cinema close to where you work. You buy a ticket an hour before the show starts, and want to use the time to have a dinner. While eating, you recall that you have to pay for a holiday package, else it will be cancelled and you will lose expensive deposit. It is due in 5 days. You can pay via Internet banking only.*"

In this scenario, we asked participants whether they would make financial transactions in a non-urgent scenario. As in scenario I, we hypothesized that participants would choose public Wi-Fi as data allowance depleted. But the sensitivity of financial transactions would made them more cautious about the risks and less likely to choose public Wi-Fi.

Scenario IV: "*You are working in a town in Japan away from home and have decided to catch a movie at a cinema close to where you work. You buy a ticket an hour before the show starts, and want to use the time to have a dinner. While eating, you recall that you have to pay for a holiday package, else it will be cancelled and you will lose an expensive deposit. It is due today and will be too late by the time you arrive back at the hotel. You can pay via Internet banking only.*"

In scenario IV, we asked participants whether they would use public Wi-Fi to make financial transactions under time pressure. We hypothesized that the pressure would affect their decision but the sensitivity of transactions would deter them.

Scenarios V-VIII were similar to scenarios I-IV, except that participants were placed in Madagascar, allowing us to assess the effect of surrounding environments on the decision-making. We hypothesized that participants would be cautious of the risks in Madagascar and hesitated to choose public Wi-Fi, despite expensive data roaming. But as the data allowance depleted, we expected more participants to take the risks.

Scenario V: "*You are on a 2-week holiday in Madagascar. When you arrive at a train station, you see that the train you want to catch is running 1 hour late. You want to check messages on messaging apps (e.g. LINE) or emails but you do NOT urgently need to contact anyone in particular. You last checked messages about 2 hours ago.*"

Scenario VI: "*You are waiting for a train at a station in Madagascar late in the evening when you realise you lost the keys to a friend's house you stay. You know the friend will leave his house before you arrive to catch his flight for a 3-day business trip. You call him but he does not answer. You can call a locksmith service but will be expensive. Suppose you can contact your friend via a messaging app on his iPad.*"

Scenario VII: "*You have decided to join a walking tour in Madagascar. You arrive at a meeting point 1 hour early and want to use the time to have lunch. While eating, you recall that you have to pay for your next holiday, else it will be cancelled and you will lose an expensive deposit. It is due in 5 days. You can pay via Internet banking only.*"

Scenario VIII: "*You have decided to join a walking tour in Madagascar. You arrive at a meeting point 1 hour early and want to use the time to have lunch. While eating, you recall that you have to pay for your next holiday, else it will be cancelled and you will lose an expensive deposit. It is due today and will be too late by the time you get back at the hotel. You can pay via Internet banking only.*"

At the end of each scenario, we asked participants to rate how they perceived the risk that their data could be compromised via mobile data, and via free public Wi-Fi on a scale of 0% to 100%, 0% being not very likely and 100% being very likely. This would allow us to assess the effect of the perceived risks on decision-making.

To optimize data quality, we embedded rules such as making questions mandatory and attaching a picture related to the scenario to make it more intuitive. We also tested the survey on different platform (i.e. laptop, tablet, and smart phones).

3) Statistical analysis methods: We analyzed three factors potentially affecting the decisions to use public Wi-Fi: mobile data preservation heuristic, perceived risks of unsecured public Wi-Fi, and demographic factors. The first two factors were not statistically tested in depth in Sombatruang *et al.*'s study, and so we added a Cochran's Q Test and an independent samples T-Test. The same binary logistic regression was used on demographics factors. We ran all analysis using SPSS.

C. Ethics Approval

We seeked approval from the IRBs of the institutions. For the Wi-Fi experiment, permission was granted provided that participants gave consent by accepting the terms and conditions of using our Wi-Fi network through a captive portal, explaining that they agree they were at least 18 years old and data such as IP address, MAC address, and network traffic would be collected. The collected data, stored in an encrypted drive, were accessible only to the research team.

For the survey, permission was granted given that data were collected anonymously and participants were explained about the study and gave consent. None of our questions asked for personally identifiable information. We also showed details about our study and a consent form at the start of the survey.

IV. Results

We reported findings from the public Wi-Fi experiment and the survey in this section. Each is discussed in turn.

A. Security and privacy risks of unsecured public Wi-Fi

From approximately 7.7 million Wi-Fi packets captured from 196 mobile devices, we found data, which we considered sensitive, transmitted insecurely without encryption. Some of these data are highly sensitive and hence have been obscured.

1) Images: We found one online dating app transmitted images using HTTP which provided no encryption. We reconstructed the traffic and found 108 photos of the app users (an example in Fig. 1). Although these images can be viewed by anyone using the online dating application, some users may not want to share them with non-users of the app — especially in Japan where online dating is not common [8].

2) Search history: We found a stock checking system of one company transmitting its product search history without encryption via HTTP (Fig. 2). This system was for private use; hence, data could be commercially sensitive. We also found the credentials of the user making this search (Section IV-A4).

3) Emails and documents: We captured 57 email messages being transmitted in clear text using Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) (examples in Fig. 3) — among which attached 4 MS Word files (Fig. 4).

4) Credentials: We captured various forms of credentials. First, we found a password, in clear text, to open an encrypted file attached in one of the emails captured (Fig. 5). We also found one server's authentication token being sent using HTTP Basic Authentication (Fig. 6). This scheme transmits credentials as user ID/password pair, encoded using base64 which takes binary data and turns it into text. The encoded text is embedded unencrypted in the HTTP header.

Next, we captured a login credential from a stock checking system of one company being transmitted via HTTP (Fig. 7). Finally, we found three pairs of unencrypted login credentials via POP, SMTP, and IMAP email protocols (Fig. 8).

B. Factors affecting users decision

1) Mobile data allowance: First, we tested whether participants would be more inclined to use unsecured public Wi-Fi as the data allowance depleted in each scenario. We performed a Cochran's Q test 1, to test whether the observed differences in the proportion of participants deciding to use public Wi-Fi as data allowance depleted (from 100% to 75%, 50%, and 25%) were statistically different. We checked that our data met the four[4] assumptions needed for Cochran's Q Test.

$$T = k(k-1)((\sum_{j=1}^{k}(x_j - (N/k))^2)/(\sum_{i=1}^{b} x_i(k-x_i))) \quad (1)$$

Where k is the number of proportion to be observed (i.e. 1.0, 0.75, 0.50 and 0.25), b is the number of participants, X_j is the column total for the j^{th} proportion, X_i is the row total for the i^{th} participant, N is the grand total.

We found that the proportion of participants choosing public Wi-Fi (W_{WiFi}) generally increased as the mobile data allowance depleted (Fig. 9-10). But, the differences observed were statistically significant only in scenario IV and VIII which involved urgent financial transactions. For the remaining scenarios, the increased proportions could be due to chance.

In scenario IV which placed participants in Japan, the W_{WiFi} increased from 52.43% to 53.40%, 56.31%, and 59.22% as the remaining data allowance decreased from 100% to 75%, 50%, and 25%, respectively (Fig. 9). Cochran's Q test determined that the differences observed were statistically significant ($x^2(3) = 10.55$, $p < 0.01$). In scenario VIII which placed participants outside Japan, fewer participants chose public Wi-Fi — aligning with our hypothesis that participants would be wary of the risks in Madagascar. As the data allowance decreased from 100% and 75% to 50%, and 25%, the W_{WiFi} increased from 44.66% to 49.51%, and 55.34% ($x^2(3) = 8.95$, $p < 0.05$), respectively (Fig. 10).

However, an interesting pattern emerged. The increased in W_{WiFi} were statistically significant pervasively among the

[4]1. One dependent with two possible dichotomous values (i.e. using or not-using public Wi-Fi), 2. At least three categorical related groups (i.e. 1.0, 0.75, 0.50 and 0.25), 3. Random samples, 4. Sufficiently large samples ($n = 103$).

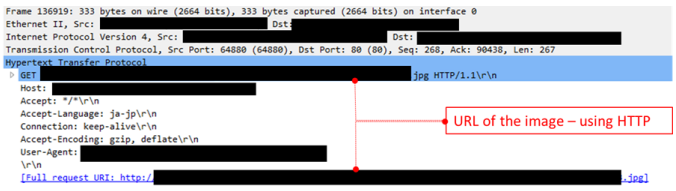

Fig. 1 Wi-Fi traffic of an image from one online dating app

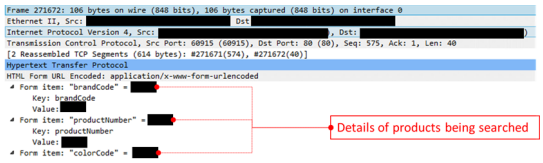

Fig. 2 An example of Wi-Fi traffic containing product search history

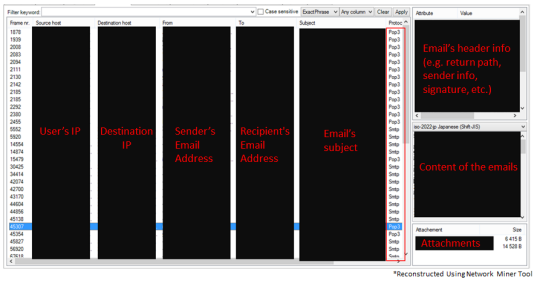

Fig. 3 Email messages reconstructed from traffic captured

Fig. 4 Attached documents among the email messages captured

Fig. 5 A password of an encrypted document sent via an email

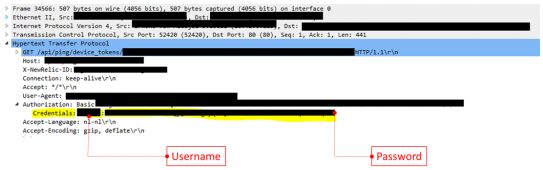

Fig. 6 A pair of credentials embedded in the HTTP header

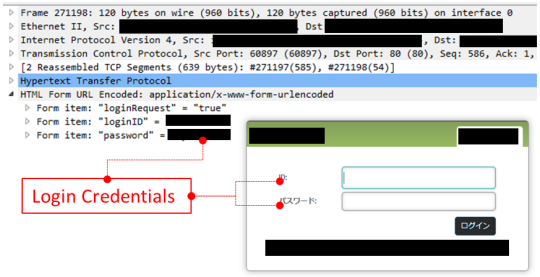

Fig. 7 A pair of username and password from a web-based stock checking system being transmitted in clear text via HTTP

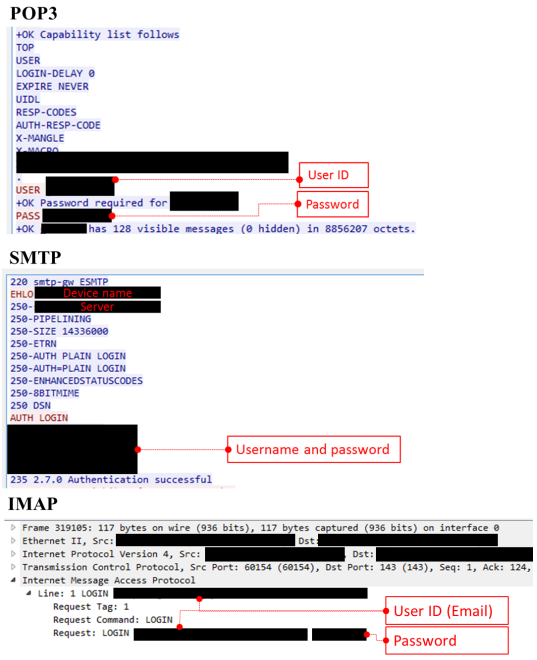

Fig. 8 Three pairs of email account's username and password transmitted in clear text via POP3, SMTP, and IMAP

data poor (those having less than 4 GB/month data on their real-life mobile device) but not among the data rich (those having at least 4GB/month). The 4GB/month cut-off is the median in our data set and we considered this data plan to be

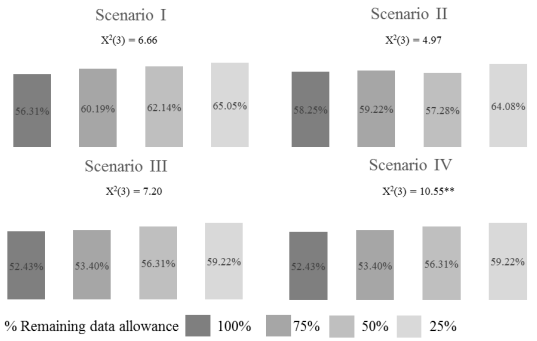

Fig. 9 Proportion of W_{WiFi} in scenario I-IV (**significant at $p < 0.01$)

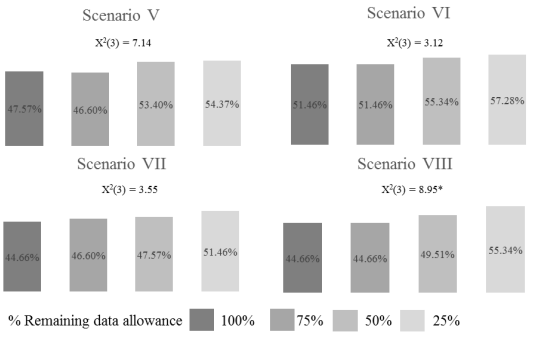

Fig. 10 Proportion of W_{WiFi} in scenario V-VIII (*significant at $p < 0.05$)

large enough for an ordinary user to not be too worry about data preservation.

In scenario I, which involved making non-urgent non-financial transactions, the proportions of the data poor deciding to use public Wi-Fi (W_{poor}) increased from 55.32% to 59.57%, 61.70%, and 68.09% ($x^2(3) = 9.78$, $p < 0.05$) as the data allowance decreased from 100% to 75%, 50%, and 25% (Fig. 11). In scenario II, which applied a time pressure, W_{poor} increased significantly from 59.57% to 68.09% ($x^2(3) = 9.00$, $p < 0.05$) as the data allowance depleted from 100% to 75%, and from 50% to 25% (Fig. 11). The 25% cut-off point seemed to heavily prompt the risk-taking attitude.

For financial transactions in scenario III, W_{poor} increased from 53.19% to 57.45%, and 61.70% ($x^2(3) = 9.43$, $p < 0.05$) as the allowance reduced from 100% and 75% to 50%, and 25% (Fig. 12). With a time pressure in scenario IV, W_{poor} increased from 55.32% to 57.45%, and 65.96% ($x^2(3) = 8.03$, $p < 0.05$) as the allowance reduced from 100% to 75%, and 50% and 25%. Again, the resource preservation heuristic reached its peak at 25% (Fig. 12). None of the differences among the data rich (W_{rich}) was statistically significant, suggesting the increase could be due to chance.

When the scenarios placed participants in Madagascar, both the W_{poor} and W_{rich} also generally increased as data roaming allowance depleted. But, as hypothesized, fewer of them did

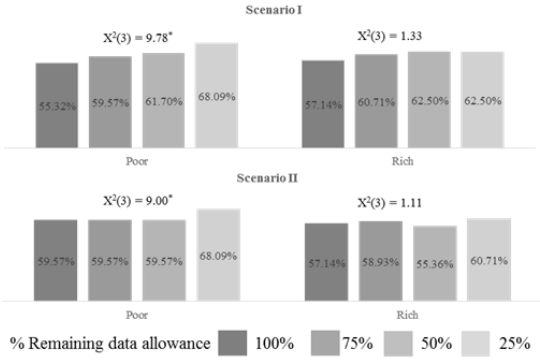

Fig. 11 Proportion of W_{poor} and W_{rich} in case I-II (*significant at $p < 0.05$, $n_{poor} = 47$, $n_{rich} = 56$)

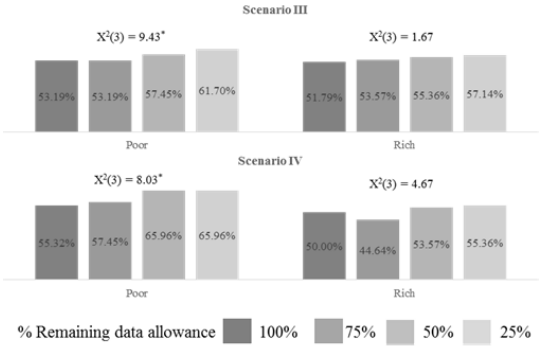

Fig. 12 Proportion of W_{poor} and W_{rich} in case III-IV (*significant at $p < 0.05$, $n_{poor} = 47$, $n_{rich} = 56$)

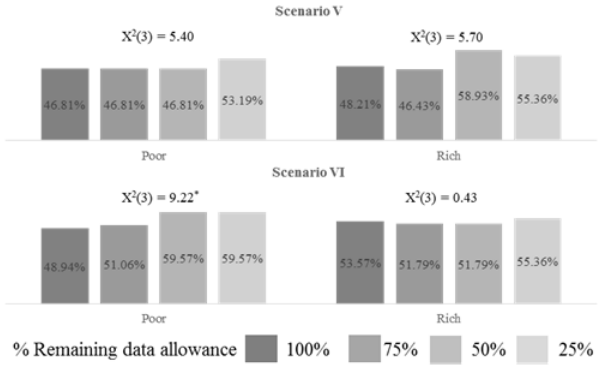

Fig. 13 Proportion of W_{poor} and W_{rich} in case V-VI (*significant at $p < 0.05$, $n_{poor} = 47$, $n_{rich} = 56$)

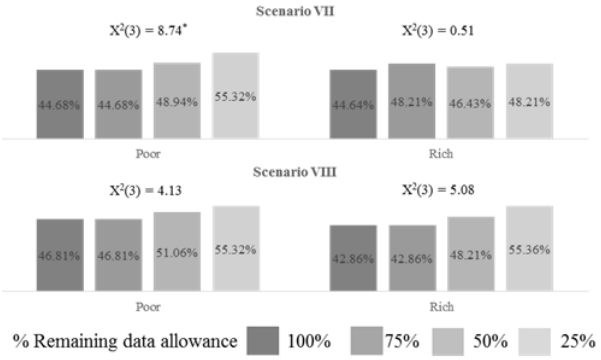

Fig. 14 Proportion of W_{poor} and W_{rich} in case VII-VIII (*significant at $p < 0.05$, $n_{poor} = 47$, $n_{rich} = 56$)

so compared to the scenarios in Japan. Again, the increased observed among the W_{rich} were statistically insignificant. The increased among W_{poor} were significant but in scenario VI and VII only (Fig. 13-14) — suggesting that the data poor and the data rich were not that different in an unfarmiliar environment.

2) Perceived risks of public Wi-Fi: Next, we examined whether the perceived risks that public Wi-Fi could be compromised affected the decisions to use the networks. We ran an independent samples T-Test ((2.1) or (2.2)) where equal variances were assumed, and not assumed, respectively) to test whether the perceived risks were statistically different between those deciding to use the network and those choosing not to.

$$t = (\mu_1 - \mu_2)/S\sqrt{1/n_1 + 1/n_2} \tag{2.1}$$

$$t = (\mu_1 - \mu_2)/\sqrt{s_1^2/n_1 + s_2^2/n_2} \tag{2.2}$$

Where μ_1 is the mean likelihood that participants deciding to use public Wi-Fi perceived the network can be compromised, μ_2 is the mean likelihood from participants deciding NOT to use the network, n_1 is the number of participants deciding to use public Wi-Fi, n_2 is the number of participants deciding NOT to, σ_p is the standard deviation (SD) of the total populations, σ_1 is the SD of n_1, and σ_2 is the SD of n_2.

We used the Levene's Test for equality of variances to determine whether the data sets were subjected to (2.1) or (2.2). If the Levene's test returns insignificant result ($p > 0.05$), we

assume equal variances and apply (2.1). We also checked that our data met the assumptions for the T-Test[5].

We found that although μ_2 was greater than μ_1 in 28 of 32 instances, the observed differences were statistically significant in only 2 of the 28 instances: in scenario IV which asked participants to make an urgent financial transaction in Japan when the remaining data allowance was at 75% ($t(101) = -2.10$, $p < 0.05$), and in scenario VII which asked participants to make an urgent non-financial transaction outside Japan when the remaining data allowance is at 25% ($t(101) = -2.02$, $p < 0.05$).

For the remaining 30 instances, the differences observed were statistically insignificant — suggesting the decisions to use or not to use public Wi-Fi were not significantly affected by the participants' perceived risks of using these networks.

We then analysed the perceived risks among the data rich and the data poor, using the same t-tests. For the data poor, μ_2 was greater than μ_1 in all 32 instances but only statistically significant in one instance asking participants to make urgent non-financial transactions in Japan when having 50% left of data allowance ($t(37) = -2.88$, $p < 0.05$). For the data rich, μ_2 was greater than μ_1 in 24 of 32 instances, of which only 7 were statistically significant (Table II). In the 8 instances where μ_2 was less than μ_1, none were statistically significant. The results suggested that, in most cases, the perceived risks played less of a role in the decision-making in both groups.

3) Demographic factors: We ran binomial logistic regressions (3) to predict the probability of participants deciding to use or not to use public Wi-Fi based on their demographic.

$$\Pr(Y_i = 1|X_i = x_i) = exp(\beta_0 + \beta_1 x_i)/(1 + exp(\beta_0 + \beta_1 x_i)) \quad (3)$$

Where Y is a binary response variable, $Y_i = 1$ if a participant decides to use public Wi-Fi, $Y_i = 0$ if a participant decides not to use public Wi-Fi, $X = (X_1, X_2, ..., X_k)$ is the independent variable (i.e. gender, income, education level, employment).

We found a statistically significant correlation between gender, education, and the decision to use public Wi-Fi.

[5]1. Dependent variables measured on a continuous scale, 2. Independent variable consist of two categorical independent groups (i.e. used vs. not used public Wi-Fi), 3. Independence of observations, 4. No significant outliers, 5. Normally distributed dependent variables, 6. Homogeneity of variances (tested and corrected in the Levene's Test)

TABLE II DIFFERENCES IN THE PERCEIVED RISKS OF THE DATA RICH DECIDING TO USE (μ_1) AND NOT USE (μ_2) PUBLIC WI-FI

Value	Scenario VI		Scenario VII			Scenario VIII	
	Data Level						
	75%	25%	100%	75%	50%	100%	50%
μ_1	56.48	55.97	52.64	54.19	52.54	52.58	54.00
σ_1	21.81	25.24	25.08	24.74	25.39	24.33	22.17
μ_2	70.30	69.09	69.57	69.27	70.30	66.32	66.72
σ_2	20.81	19.29	21.92	22.75	21.10	19.50	21.10
$\mu_1 - \mu_2$	-13.82*	-13.12*	-16.93*	-15.08*	-17.76*	-13.74*	-12.72*
t	-2.33	-2.05	-2.62 -	2.31	-2.77	-2.26	-2.12
$df^\star$	48.26	51.00	51.00	51.00	51.00	50.00	50.00

σ=Standard Deviation, t=t-test result, df=Degree of Freedom,$\star$ Excluded outliers, *Significant at $p < 0.05$.

a) Gender: Similar to the findings from the work of Sombatruang *et al.* [33], females were more likely than males to choose public Wi-Fi. We agreed with their explanation that women may be less obsessive with security advice and may have created a habit of saving data plan whenever possible. This could also be true for women in Japan.

When the scenario asked participants to make non-urgent financial activity in Japan, despite having 100% and 75% left of data allowance, females were 3.86 times ($\beta = 1.35$, $OR = 3.86$, $p < 0.05$, $R^2 = 0.26$) and 3.42 times ($\beta = 1.23$, $OR = 3.42$, $p < 0.05$, $R^2 = 0.28$), respectively, more likely. When the allowance depleted to 50%, the odds increased to 5.62 times ($\beta = 1.73$, $OR = 5.62$, $p < 0.05$, $R^2 = 0.37$), showing a stronger tendency to save data. In an urgent scenario, however, females were 3.2 times ($\beta = 1.16$, $OR = 3.20$, $p < 0.05$, $R^2 = 0.29$) more likely.

In Madagascar scenarios, we found a statistically significant result only when asking participants to make an urgent non-financial transaction — suggesting that gender played less of a role in an unfamiliar environment. In that one case, female were 3.68 times ($\beta = 1.30$, $OR = 3.68$, $p < 0.05$, $R^2 = 0.32$) more likely when having 50% left on data roaming allowance.

b) Education Level: Unlike the findings from Sombatruang *et al.* [33]'s study which found no significant relationship between education level and the decision to use, or not to use, public Wi-Fi, our participants holding a bachelor or postgraduate degree were less likely to do so than those having finished high-school only (reference group). One possible explanation is an exposure to cyber security awareness were mostly at university level onward in Japan.

When the scenarios placed participants in Japan and when they had 75%, 50%, and 25% left on data allowance, participants holding a bachelor degree were 0.15 times ($\beta = -1.89$, $OR = 0.15$, $p < 0.05$, $R^2 = 0.26$), 0.07 times ($\beta = -2.67$, $OR = 0.07$, $p < 0.01$, $R^2 = 0.43$), and 0.12 times ($\beta = -2.09$, $OR = 0.12$, $p < 0.05$, $R^2 = 0.32$) less likely to decide to use public Wi-Fi to make non-urgent non-financial transactions. In an urgent situation, they were 0.22 times ($\beta = -1.53$, $OR = 0.22$, $p < 0.05$, $R^2 = 0.26$), 0.20 times ($\beta = -1.64$, $OR = 0.20$, $p < 0.05$, $R^2 = 0.23$), and 0.21 times ($\beta = -1.58$, $OR = 0.21$, $p < 0.05$, $R^2 = 0.26$), less likely when having 100%, 75%, and 50% left on data allowance. For financial-related transactions, participants having a bachelor and postgraduate degree were 0.22 times ($\beta = -1.53$, $OR = 0.22$, $p < 0.05$, $R^2 = 0.29$) and 0.10 time ($\beta = -2.35$, $OR = 0.10$, $p < 0.05$, $R^2 = 0.29$), respectively, less likely to choose public Wi-Fi in urgent scenarios and when having 50% left on their data allowance.

However, the results from all scenarios placing parcitipants in Madagascar were statistically insignificant. Like gender, education level also played less of a role in the decision-making in an unfamiliar environment — suggesting participants were not that different when placed outside their comfort zone.

V. Discussion

We discussed the applications of our study, its limitations, and potential future work in this section.

A. Applications

Our study has two key messages. First, the risks of public Wi-Fi in Japan are still widespread, despite growing concern and public knowledge about them. Second, users are likely to keep using the networks as long as they are trapped in a resource preservation heuristic mindset. This finding can be applied in a number of ways that could improve security.

First, it helps us to advise the public more effectively. Telling them not to use public Wi-Fi networks at all is probably futile. Not everyone will have an unlimited data plan, and those with a small data plan will keep using the networks, despite awareness of certain risks. A more practical strategy is to urge the public to use a reliable virtual private network (VPN) — not just for sensitive transactions but making a habit of using it whenever they use public Wi-Fi. In Japan, policy makers could consider doing so in the existing security campaign such as the International Cyber Security Campaign[6] and the National Police Agency's Cyber Safety hotline[7]. Targeting the campaign on females and students in high school may be useful as they are more likely to use the networks. VPN providers could also help to make it easier for users by making the app starts automatically by default — the feature missing from many main VPN products such as Cisco AnyConnect.

Next, we may want to shift the focus from fixing the users to other more fixable elements. Encouraging public Wi-Fi providers to implement secured connections is one possible solution. Germany led an example, requiring authentication on all public Wi-Fi hotspots [**?**]. The Japanese Ministry of Internal Affairs and Communications have been discussing this possibility [22]. Providers in Japan can also apply for a certified *Secured Wi-Fi* badge from the *Safe Security ISP*[8], aiming to promote the security of Internet Service Providers (ISP). However, only 4 companies with a total of 70,000 hotspots have signed up so far[9]. Reducing the fees (¥40,000/year) and publicizing the initiative could be a good incentive.

We should also continue to promote app providers to encrypt sensitive data in transit. Failure to encrypt such data, as shown in our findings, could lead to data breaches that expose firms to fines and reputation damages, especially in light of the new 2017 Protection of Personal Information Act in Japan [14] and the EU General Data Protection Regulation [7]. The good news is many big names in the tech industry have started to take notice. For example, Apple encourages all iOS apps to use App Transport Security (ATS)[10]. Google Chrome, a web browser, also flags non-secured web sites — not only to warn users but also to encourage developers to implement HTTPS [12]. The local providers in Japan, however, need to catch up.

Telecom operators may help by offering packages that could dissuade users from using unsecured public Wi-Fi such as allowing subscribers to borrow data from next month when data allowance is low. Also, as many Japanese telecom operators offer free public Wi-Fi to subscribers, policy makers may consider encouraging them to offer secured Wi-Fi networks.

B. Limitations and possible future works

Our study has inherent limitations. For the public Wi-Fi experiment, there may be other sensitive data being transmitted insecurely but not captured in our analysis. However, we consider our findings sufficient to warrant the message that the risks of unsecured public Wi-Fi in Japan were still at large.

For the online survey, despite our efforts to elicit good quality responses such as using engaging scenarios, some participants might not fully pay attention. But, this is expected from all research using online survey. Some users may guess the intention of the survey and gave favourable answers; but we considered our pilot study provided sufficient rigor to detect such biases in the design. Our survey also used hypothetical scenarios; people may behave differently in real life. Possible future studies could investigate data in a naturalistic setting. For the econometric analysis, unravelling correlation and causation may reflect influences from underlying variables. Fuller exploration of larger data sets would give us more insight about the ultimate causal factors.

Moreover, the observed resource preservation heuristic may not be truly universal as Japan and UK are developed economies. Analysing data from developing economies would address this limitation. Future studies could also use our framework to investigate the effect of other resource preservation heuristic in a wider context of cyber security such as examining how the desire to save time or money influences people to forgo security. Finally, since users constrained by mobile data are likely to keep using unsecured public Wi-Fi, another useful future work is seeking interventions that help them to create a habit of using VPN.

VI. Conclusion

Our study shows a concerning but important conclusion. Despite growing knowledge and media reports about unsecured public Wi-Fi networks, the risks continued; many applications still did not encrypt sensitive data-in-motion and many users continued to use the networks for sensitive transactions.

We highlighted the resource preservation heuristic — the desire to save mobile data allowance — as a particular root cause for influencing users' decision-making. We also showed that the perceived risks of public Wi-Fi played less of a role in the decision-making. Our study is the first to have examined these two factors using rigorous statistical tests and provided a framework for future study wishing to investigate resource preservation in a wider context of cyber security.

[6] www.nisc.go.jp/security-site/campaign
[7] www.npa.go.jp/cybersafety
[8] www.isp-ss.jp
[9] Information obtained directly from a representative from ISP-SS
[10] forums.developer.apple.com/thread/6767

Our findings called for a more workable solution to mitigate the risks of unsecured public Wi-Fi. Urging users to make a habit of using a VPN when on public Wi-Fi is more plausible than stopping them from using it entirely. Greater emphasis is also needed on app providers to encrypt sensitive data-in-motion and on public Wi-Fi providers to offer secured Wi-Fi. Telecom operator could also help by offering data plan that allow users to borrow data from next month — essentially interfering the intrusive thoughts about running out of data that instigates the unwanted resource preservation heuristic.

REFERENCES

[1] M. D. Aime, G. Calandriello, and A. Lioy. Dependability in wireless networks: Can we rely on wifi? *IEEE Security & Privacy*, 5(1), 2007.

[2] A. V. Anastasia, S. V. Zareshin, I. S. Rumyantseva, and V. G. Ivanenko. Analysis of security of public access to wi-fi networks on moscow streets. In *Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian*, pages 105–110. IEEE, 2017.

[3] R. G. Brody, K. Gonzales, and D. Oldham. Wi-fi hotspots: secure or ripe for fraud. *Journal of Forensic Investigative Accounting*, 5(2):27–47, 2013.

[4] L. Change. Beware of hotel wi-fi - russian hackers are stealing info. www.digitaltrends.com/computing/russia-hotel-wi-fi-hack, Aug. 2017.

[5] S. Chen, R. Wang, X. Wang, and K. Zhang. Side-channel leaks in web applications: A reality today, a challenge tomorrow. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 191–206. IEEE, 2010.

[6] N. Cheng, X. O. Wang, W. Cheng, P. Mohapatra, and A. Seneviratne. Characterizing privacy leakage of public wifi networks for users on travel. In *INFOCOM, 2013 Proceedings IEEE*, pages 2769–2777. IEEE, 2013.

[7] E. U. Commission. Gdpr key changes. www.eugdpr.org/key-changes.html, May 2018.

[8] E. Dalton and L. Dales. Online konkatsu and the gendered ideals of marriage in contemporary japan. *Japanese Studies*, 36(1):1–19, 2016.

[9] F-Secure. The f-secure wi-fi experiment. www.fsecureconsumer.files.wordpress.com/2014/09/wi-fi_report_2014_f-secure.pdf, 2014.

[10] A. Ferreira, J.-L. Huynen, V. Koenig, and G. Lenzini. Socio-technical security analysis of wireless hotspots. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 306–317. Springer, 2014.

[11] A. Ferreira, J.-L. Huynen, V. Koenig, G. Lenzini, and S. Rivas. Do graphical cues effectively inform users? In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 323–334. Springer, 2015.

[12] Google Security Blog. Next steps toward more connection security. security.googleblog.com/2017/04/next-steps-toward-more-connection.html, Apr. 2017.

[13] iPass. Wi-fi growth map. www.ipass.com/wifi-growth-map, 2018.

[14] P. I. P. C. Japan. Personal information protection act. www.ppc.go.jp/en/legal, May 2018.

[15] D. Jeske, L. Coventry, and P. Briggs. Decision justifications for wireless network selection. In *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on*, pages 1–7. IEEE, 2014.

[16] B. D. Kern. Whacking, joyriding and war-driving: Roaming use of wi-fi and the law. *Santa Clara Computer & High Tech. LJ*, 21:101, 2004.

[17] M. Khan, Z. Bi, and J. A. Copeland. Software updates as a security metric: Passive identification of update trends and effect on machine infection. In *MILCOM 2012-2012 IEEE Military Communications Conference*, 2012.

[18] T. Kindberg, E. O'Neill, C. Bevan, V. Kostakos, D. Stanton Fraser, and T. Jay. Measuring trust in wi-fi hotspots. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 173–182. ACM, 2008.

[19] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall. When i am on wi-fi, i am fearless: privacy concerns & practices in eeryday wi-fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1993–2002. ACM, 2009.

[20] A. Mani, S. Mullainathan, E. Shafir, and J. Zhao. Poverty impedes cognitive function. *Science*, 341(6149):976–980, 2013.

[21] I. McShane, M. A. Gregory, and C. Wilson. Practicing safe public wi-fi: Assessing and managing data-security risks. 2016.

[22] Ministry of Internal Affairs and Communications. Wireless-lan business guidelines 2nd edition. www.soumu.go.jp/main_content/000444788.pdf, 2016.

[23] Ministry of Land, Infrastructure, Transport and Tourism. New tourism strategy to invigorate the japanese economy, meeting of the council for a tourism vision to support the future of japan. www.mlit.go.jp/common/001172615.pdf, 2016.

[24] S. Mullainathan and E. Shafir. Savings policy and decision-making in low-income households. *Insufficient funds: Savings, assets, credit, and banking among low-income households*, 121:140–142, 2009.

[25] S. Mullainathan and E. Shafir. *Scarcity: the true cost of not having enough*. Penguin books, 2014.

[26] T. Murayama. Danger of free wi-fi. ascii.jp/elem/000/001/610/1610917, Jan. 2018.

[27] C. Osborne. Coffeeminer hijacks public wi-fi users' browsing sessions to mine cryptocurrency. www.zdnet.com/article/how-to-hack-public-wi-fi-to-mine-for-cryptocurrency, Jan. 2018.

[28] N. Sato. Argentina's starbuck wi-fi unauthorized mining. japan.cnet.com/article/35112098, Dec. 2017.

[29] F. Schilbach, H. Schofield, and S. Mullainathan. The psychological lives of the poor. *American Economic Review*, 106(5):435–40, 2016.

[30] J.-M. Seigneur, P. Kölndorfer, M. Busch, and C. Hochleitner. A survey of trust and risk metrics for a byod mobile working world. In *Third International Conference on Social Eco-Informatics*, pages 217–228, 2013.

[31] A. K. Shah, S. Mullainathan, and E. Shafir. Some consequences of having too little. *Science*, 338(6107):682–685, 2012.

[32] T. S. Sobh. Wi-fi networks security and accessing control. *International Journal of Computer Network and Information Security*, 5(7):9, 2013.

[33] N. Sombatruang, M. A. Sasse, and M. Baddeley. Why do people use unsecure public wi-fi?: an investigation of behaviour and factors driving decisions. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*, pages 61–72. ACM, 2016.

[34] D. Spears. Economic decision-making in poverty depletes behavioral control. *The BE Journal of Economic Analysis & Policy*, 11(1), 2011.

[35] Statistica. Countries with the lowest rate of malware infected computers as of 4th quarter 2016. www.statista.com/statistics/321852/lowest-malware-infection-rate-countries, 2016.

[36] A. Sulleyman. Coffee shop wi-fi most dangerous of all, warns security report. www.independent.co.uk/life-style/gadgets-and-tech/news/wifi-hotpots-coffee-shop-dangerous-security-risk-report-a7750091.html, May 2017.

[37] C. Swanson, R. Urner, and E. Lank. Naïve security in a wi-fi world. In *IFIP International Conference on Trust Management*, pages 32–47. Springer, 2010.

[38] C. Szongott, M. Brenner, and M. Smith. Metds-a self-contained, context-based detection system for evil twin access points. In *International Conference on Financial Cryptography and Data Security*, pages 370–386. Springer, 2015.

[39] Tefficient. Upsell and loyalty strategies of operators: Using public wi-fi as customer magnet. www.media.tefficient.com, 2016.

[40] M. Vanhoef and F. Piessens. Key reinstallation attacks: Forcing nonce reuse in wpa2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1313–1328. ACM, 2017.

[41] K. E. Vaniea, E. Rader, and R. Wash. Betrayed by updates: how negative experiences affect future security. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2671–2674. ACM, 2014.

[42] K. D. Vohs. The poor's poor mental power. *Science*, 341(6149):969–970, 2013.

[43] R. Wash, E. Rader, K. Vaniea, and M. Rizor. Out of the loop: How automated software updates cause unintended security consequences. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 89–104, 2014.

APPENDIX

A. Locations of public Wi-Fi experiment

- Kintetsu Nara Train Station

- JR Nara Train Station
- On a train from Yamato Saidaiji Station to Kintetsu Nara Station
- Nara Tourist Information Centre (within the vicinity of JR Nara Train Station)
- Higashimuki Shopping Street
- Sanjodori Shopping Street
- Konishi Sakura Dori Shopping Street
- Kohfukuji Temple
- Gangoji Temple
- Nara National Museum (outside)
- Sarusawa-Ike pond

B. Demographics of survey participants

Age			**Annual Income**	n	%
Mean	42.54		<¥2,000,000	5	5
Median	40.00		>2,000,000 but ⩽¥4,000,000	22	21
Mode	35.00		>¥4,000,000 but ⩽¥6,000,000	19	18
S.D.	12.46		>¥6,000,000 but ⩽¥8,000,000	16	16
Min	20.00		>¥8,000,000 but ⩽¥10,000,000	12	12
Max	75.00		>¥10,000,000 but ⩽¥12,000,000	4	4
			>¥12,000,000 but ⩽¥15,000,000	3	3
Gender	n	%	>¥15,000,000 but ⩽¥20,000,000	4	4
Male	58	56	>¥20,000,000	2	2
Female	45	44	Do not know	9	9
Total	103	100	No Answer	7	7
			Total	103	100
Education	n	%			
High school graduate	23	22	**Current Region of Resident**	n	%
Diploma/Vocation training	34	33	Tokyo	13	13
Bachelor degree	38	37	Kanto (but not Tokyo)	23	22
Postgraduate	8	8	Chubu	18	17
Total	103	100	Kansai	21	20
			Kyushu	9	9
Employment Status	n	%	Shikoku	5	5
Not working - Full time student	2	2	Chugoku	5	5
Not working - Sick/disable	2	2	Tohoku	3	3
Not working - Retired	3	3	Hokkaido	6	6
Not working - Others	17	17	Total	103	100
Working - Part time	15	15			
Working - Full time	61	59			
Working - Others	3	3			
Total	103	100			