Smart Home Cybersecurity Awareness and Behavioral Incentives

Anon

***Abstract*—— *Purpose* – Smart-home security involves multi-layered security challenges related to smart-home devices, networks, mobile applications, cloud servers, and users. However, very few studies focus on smart-home users. This paper aims to fill this gap by investigating the potential interests of adult smart-home users in cybersecurity awareness training and non-financial rewards that may encourage them to adopt sound cybersecurity practices.**

***Design/methodology/approach* – A total of 423 smart-home users between the ages of 25 and 64 completed a survey questionnaire for this study, with 224 participants from Japan and 199 from the UK.**

***Findings* – Cultural factors considerably influence adult smart-home users' attitudes toward cybersecurity. Specifically, cultural differences impact their willingness to participate in cybersecurity awareness training, their views on the importance of cybersecurity training for children and senior citizens, and their preference for non-financial rewards as an incentive for good cybersecurity behavior. These results highlight the need to consider cultural differences and their potential impact when developing and implementing cybersecurity programs that target smart-home users.**

***Originality/value* – The paper investigates whether adult smart-home users are willing to spend time and money to engage in cybersecurity awareness training and to encourage their children and elderly parents to participate in training, as well. In addition, the paper examines incentives, especially non-financial rewards, that may motivate adult smart-home users to adopt cybersecurity behaviors at home. Furthermore, the paper analyses demographic differences among smart-home users in Japan and the UK.**

***Practical implications* – This research has two main implications. First, it provides insights for information security professionals on the importance of designing cost-effective and time-efficient cybersecurity awareness training programs for smart-home users. Second, the findings may assist governments in establishing non-financial incentives to encourage greater uptake of cybersecurity practices among smart-home users.**

***Keywords*—security awareness, smart home, cybersecurity hygiene behaviors, incentives**

I. Introduction

THE frontier between human and computer security is increasingly blurry. Recent technologies, such as the Internet of Things (IoT), have brought users' personal lives closer to cyberspace. Emerging technologies, such as augmented and virtual reality, bring cyberspace to users' reality and *vice-versa*. This collaborative mixed-reality exposes users to cyber attacks that might impact not only their privacy and cybersecurity, but possibly also their personal safety and security. Happa *et al.* [1] assumed that the attack on collaborative mixed-reality applications might include personal data leaks, loss of trust, and physical, psychological, and reputational harm. Attack impacts could be noticeable in smart homes, one of the most prominent IoT usage contexts.

A smart home is a branch of ubiquitous computing that incorporates smartness into dwellings for a better quality of life [2]. We suspect that smart homes will include collaborative mixed-reality applications to improve users' experience of services such as healthcare, energy management, and entertainment. In addition to the security issues already present in mixed-reality collaboration applications, cyber attacks on smart homes are becoming common. A recent experiment using a fake smart home identified more than 12 000 scanning or hacking attempts in a single week [3]. Furthermore, the number of smart-home users is expected to exceed 77 million by 2025 [4]. The increase of smart-home users could drastically raise the number of victims in case of a low level of user information security awareness and preventative measure adoption.

It is worth noting that user awareness of security countermeasures, while not the only factor, decreases information system misuses, which could lead to a reduction in the success rate of cyber attacks [5]. Thus, there is a strong case to promote cybersecurity awareness training for smart-home users. However, higher costs of these efforts may deter smart-home users. For instance, Aldawood and Skinner [6] pointed out that monetary costs and resources are a critical obstacle to deployment of cybersecurity education programs. Furthermore, Douha *et al.* [7] highlighted the importance of time constraints, in addition to monetary costs, when discussing cybersecurity awareness training of smart-home users. Consequently, investigating the inclination of smart-home users to allocate both financial resources and time toward cybersecurity awareness training could furnish a novel and practical understanding of the most affordable and efficient training course that would fit the needs of the average user.

To improve users' information security awareness and pro-cybersecurity behavior, incentives such as rewards can be useful. Lu [8] indicated that rewards could positively influence users' intentions to adopt information system security policies. Rewards could also be effective in incentivizing pro-cybersecurity behavior among smart-home users, as demonstrated by Douha *et al.* [7]. However, the effectiveness of rewards as incentives might depend on the users' environment, as Coventry *et al.* [9] highlighted the influence of environmental factors on cybersecurity behavior. For instance, non-financial incentives, particularly those related to social norms, could have a strong impact on household behavior, according to Lindbeck [10]. Despite the literature on the importance of incentives in cybersecurity behaviors [11], [12], research on the use of non-financial rewards for pro-cybersecurity behavior among smart-home users is currently lacking.

With the above in mind, we aimed to discover the potential interests of adult smart-home users in cybersecurity awareness training and also the non-financial rewards that may encourage them to adopt pro-cybersecurity behaviors. We used an online survey to collect data from 426 smart-home users aged between 25 and 64 years living in Japan and the United Kingdom of Great Britain and Northern Ireland (UK). The choice of Japan and the UK is motivated by the expansion of the smart-home market in these countries and the multiple cultural differences between them, as discussed in Section II-A. The pole positions of Japan and the UK in the fight against cyber attacks in Asia and Europe is another reason to conduct this comparative study.

We denote the research questions to be addressed in this paper as follows:

- ***Research Question 1:*** Is there a relationship between adult smart-home users' citizenship and their interest in cybersecurity awareness training?
- ***Research Question 2:*** Is there a relationship between adult smart-home users' citizenship and their interest in non-financial rewards?
- ***Research Question 3:*** Do Japanese and British adult smart-home users agree that it is imperative to educate children on cybersecurity to ensure that they do not inadvertently endanger the security of smart homes?
- ***Research Question 4:*** Do Japanese and British adult smart-home users agree that it is imperative to educate senior citizens on cybersecurity to ensure that they do not inadvertently endanger the security of smart homes?

Previous research has proposed a game-theoretic approach to analyze the cost-benefit of security investments for smart-home users (i.e., adults, children, and senior citizens). In particular, incentivizing users to engage in cybersecurity awareness training and good cybersecurity practices has been shown to enhance overall security awareness. In the present paper, we make several important contributions to the field, including:

1) Investigating the impact of national cultures on smart-home users' interest in cybersecurity awareness training, an area that has received limited research attention.
2) Proposing non-financial rewards as a valuable incentive to encourage smart-home users to adopt good cybersecurity behavior at home.
3) Conducting a survey questionnaire to collect and analyze the opinions of Japanese and British adult smart-home users regarding their potential interests in cybersecurity awareness training and desired non-financial rewards towards good cybersecurity behavior at home.
4) Discovering whether adult smart-home users intend to engage in cybersecurity awareness training, and are willing for children and senior citizens to get trained.
5) Examining the influence of national cultures on smart-home users' interests in non-financial rewards.
6) Identifying the most prominent non-financial reward that may motivate smart-home users to adopt good cybersecurity hygiene at home.

We present related work in Section II. We describe our methodology to address the identified research gap in Section III. We present our results in Section IV. Lastly, we discuss our findings in Section V and conclude this paper in Section VI.

II. Background & Related Work

Cross-cultural studies aim at understanding human behaviors throughout different cultures. This section, through Subsection II-A, first explains the choice of Japan and the UK to conduct our cross-cultural study. We describe the socio-economic and cultural differences between these countries. In addition, we highlight the national cybersecurity policies and recent strategies adopted by each country to improve IoT security. Furthermore, Subsection II-B analyzes the previous research on home users' cybersecurity awareness training and non-financial rewards.

A. Motivation for Comparing Japan and the UK

The choice of Japan and the UK in this work aims to analyze eastern and western smart-home users' opinions on cybersecurity awareness training and rewards for compliance behavior. Japan and the UK are two leading nations for innovation and technologies that differ in many factors, such as socio-economy, culture, and cybersecurity strategies, which could lead to several cross-cultural issues when discussing cybersecurity awareness and security compliance behavior of smart-home users.

1) Socio-Economy: Socioeconomic status (SES) typically comprises economic status, social status, and work status, which are measured by income, education, and occupation, respectively [13]. In Japan and the UK, SES exhibits some differences. Firstly, a study by Ballas *et al.* [14] found that the UK has higher income inequality than Japan. This confirms earlier research by Wilkinson and Pickett [15], showing that Japan has lower income inequality and better health and social well-being than the UK. Secondly, Japan has a more homogeneous education system, with nine years of compulsory education for all students, whereas the UK has a more diverse system, with eleven years of compulsory education. Lastly, in Japan, there is a strong emphasis on job security and lifetime employment, while the UK has a more flexible labor market. However, both countries have high employment rates, with most workers being full-time employees aged 25-64.

2) Culture: Hofstede's six dimensions of national cultures illustrate the cultural disparities that exist between Japan and the UK, as depicted in Figure 1 [16]. The findings reveal that Japan scores higher than the UK in *Power Distance*, *Masculinity*, *Uncertainty Avoidance*, and *Long-Term Orientation*, while scoring lower in *Individualism* and *Indulgence*. These scores imply that the Japanese tend to adhere to hierarchical positions in society more than the British, with collectivism, conformity, and harmony being their primary focus. In contrast, the British prioritize individualism, and competitiveness between groups is more apparent in Japan. Additionally, the British prioritize short-term goals and are less concerned with cultural heritage, while the Japanese experience more stress and uncertainty about the future. Furthermore, the British prioritize personal freedom, whereas the Japanese feel constrained by social norms. These cultural differences could significantly impact cybersecurity policies and their implementation in both countries.

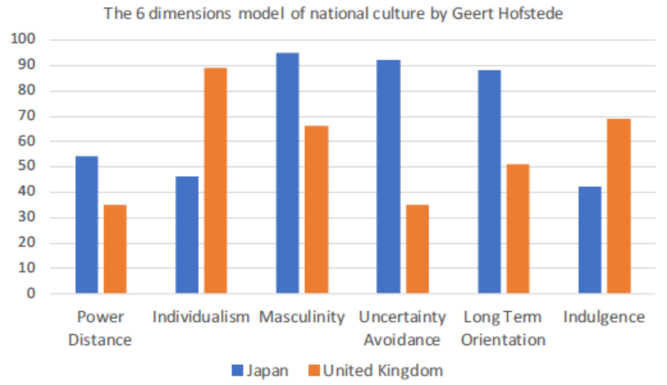

Fig. 1. Cultural differences between Japan and the UK based on Hofstede's cultural dimensions

3) National Cybersecurity Policy: IBM reported that Japan was the top-attacked country in Asia and the UK was among the most-attacked European countries in 2020 [17]. Japan and the UK have upgraded their cybersecurity policies in response to emerging technologies and complex threats. Japan's new strategy [18] aims to achieve three policy goals: (1) "*enhancing socio-economic vitality and sustainable development,*" (2) "*realizing a digital society where the people can live with a sense of safety and security,*" and (3) "*contributing to the peace and stability of the international community and Japan's national security.*" The strategy envisions creating a society where people can choose digital services that suit their needs and achieve diverse forms of happiness. The UK's new strategy [19] has five goals: (1) "*strengthening the UK cyber ecosystem*", (2) "*building a resilient and prosperous digital UK,*" (3) "*taking the lead in the technologies vital to cyber power,*" (4) "*advancing UK global leadership and influence for a more secure, prosperous and open international order,*" and (5) "*deterring adversaries to enhance UK security in and through cyberspace.*" The vision for the UK in 2030 is to remain a leading democratic cyber power, able to protect and promote its interests in cyberspace and support national goals.

Japan and the UK have recently introduced new national cybersecurity strategies that aim to raise public awareness of cyber risks and promote a free, open, peaceful, and secure cyberspace. Nevertheless, due to their cultural differences, they may adopt distinct approaches to implement and achieve these policy objectives.

4) Recent Strategies for IoT Security: In 2016, Japan developed two guidelines, i.e., (1) the "IoT Security Guidelines" [20] and (2) "IoT Safety/Security Development Guidelines" [21], suggesting required security strategies on IoT devices and services based on the security-by-design principle. The guidelines promote the awareness of IoT stakeholders (e.g., manufacturers, service providers) of the necessity of ensuring IoT security. However, they do not clarify all the legal responsibilities of IoT stakeholders when they are involved in a cybersecurity incident. Furthermore, Japan has contributed significantly, through its IoT security guidelines mentioned above, to the publication of a new international standard called ISO/IEC 30147:2021 that provides system life cycle processes to implement and maintain trustworthiness in an IoT system or service [22]. As for the UK, at the end of 2021, the UK Government introduced the Product Security and Telecommunications Infrastructure (PSTI) Bill to Parliament to promote security by design for consumer IoT security–where consumers are the end-users of IoT products and services [23]. The PSTI Bill bans default passwords, requires manufacturers, importers and distributors to comply with new security requirements for IoT security, and creates an enforcement regime with civil and criminal sanctions to prevent insecure products on the UK market.

The implementation of new IoT security policies by Japan and the UK to safeguard end-users of IoT applications is commendable. However, it is crucial to acknowledge that relying solely on secure technologies is insufficient to guarantee the security of these devices. The human factor plays a significant role in the security chain, particularly in a smart home, where end-users continuously interact with numerous IoT devices. While the push to remove default passwords from manufacturers is beneficial, it would require IoT owners to remember each device's private password in their smart home. This situation may lead to coping strategies that would inevitably weaken the security of devices and smart homes. Thus, additional initiatives are necessary to strengthen smart-home users' cybersecurity knowledge and skills through cybersecurity awareness training.

5) Smart-Home Adoption: The expansion of the smart-home market is an essential motive for conducting this study. In Japan, household penetration was estimated to be 23.6% in 2022 and is expected to reach 70.2% by 2027 [24]. The number of active smart-home users is expected to reach 40.17 million by 2027 in Japan. As for the UK, household penetration was estimated to be 45.8% in 2022 and is expected to reach 98.8% by 2027 [25]. The number of active smart-home users is expected to reach 29.70 million by 2027 in the UK. Smart-home usage is growing fast in both countries, with a more significant population in Japan but greater penetration in the UK. Investigating cybersecurity awareness education of smart-home users becomes crucial to prevent an uncontrollable escalation of cyberattack victims.

B. Related Work

To identify the most relevant related work, we used the following databases: ACM Digital Library, IEEE Xplore Digital Library, Web of Science and Google Scholar. We searched for the keywords in publication titles:

- *(cross-cultural OR multi-national OR cultural OR cross-national OR cross-country) AND (comparative OR comparison OR analysis OR differences) AND (security OR cybersecurity OR (cyber AND security)) AND (human OR user) AND awareness*

- *survey AND (security OR cybersecurity OR (cyber AND security)) AND (education OR awareness OR training) AND (home OR (connected AND home) OR (smart AND home)) AND (user OR children OR adult OR parent OR elderly OR (senior AND citizen))*

We selected only relevant cross-cultural studies related to cybersecurity awareness published from 2011 to date. In addition, we considered relevant research in psychology that focused on non-financial rewards.

1) Cross-National Research on Users' Cybersecurity Awareness: The literature suggests that users' awareness of cybersecurity issues, and their intentions to behave securely, depend on their cultural background. Harbach *et al.* [26] revealed variations in smartphone unlocking attitudes across national cultures. For instance, participants in Japan reported inconvenience as the main reason for not using a secure lock screen, while participants in the UK stated the absence of perceived threats was the reason. This suggests that cultural factors can shape secure technology usage.

Sawaya *et al.* [27] investigated the differences in security behaviors among individuals from diverse cultures and observed that individuals in Asia (e.g., Japan) demonstrated less secure behavior, as compared to those in Western countries (e.g., France). However, this pattern cannot be assumed to hold for all Eastern and Western countries, as the study was limited to specific regions and cultures. Further research is required to carry out pairwise comparisons of the levels of cybersecurity awareness and secure behavior among individuals from different cultures. This study explores the interest in cybersecurity awareness training among smart-home users from Japan and the UK.

- *H_1: Cultural differences influence smart-home users' interests in cybersecurity awareness training.*

Previous research has demonstrated the importance of considering cultural differences in the customization of security tools [27]. For example, Ndibwile *et al.* [28] found significant differences in security perception between Japanese and Tanzanian smartphone users, leading the authors to suggest the redesign of security notifications to better align with each country's cultural norms. This was supported by the findings of Argyris *et al.* [29], who demonstrated the importance of customizing picture passwords based on cultural differences.

Our study builds upon this existing body of work by exploring the influence of national culture on users' interest in non-financial rewards for cyber hygiene in smart homes. By examining this issue, we aim to deepen our understanding of how to incentivize smart-home users with tailored non-financial rewards and to encourage the adoption of safe and secure behaviors in a rapidly digitalizing world.

- *H_2: Cultural differences influence smart-home users' interests in non-financial rewards.*

Further cross-national research is required to gain a better understanding of users' intentions and behaviors toward cybersecurity in smart homes. The impact of user knowledge on their security intentions has been discussed in previous research [30], [31]. However, the study by Sawaya *et al.* [27] suggested that users' self-confidence in their cybersecurity knowledge had a greater positive impact on their security behaviors compared to their actual cybersecurity knowledge. Non-financial rewards, which are known to impact users' intrinsic motivation [32], may be useful in building users' self-confidence and encouraging secure behavior in smart homes. Lay users who reside in smart homes may require both education and confidence-building measures to adopt secure behavior in their homes.

2) Home Users' Cybersecurity Literacy: In this study, we distinguish between two categories of internet user. The first is home computer users (HCUs) –individuals who access Internet services through conventional terminals such as desktops, laptops, smartphones, and tablets within their homes. The second is smart-home users (SHUs), a new generation of Internet users who not only use internet services but also remotely control Internet of Things (IoT) devices such as smart thermostats and smart speakers. They might use various terminals and voice commands to enhance their comfort and overall quality of home life.

The increasing popularity of smart home technology has raised concerns regarding the security and privacy of users. Zheng *et al.* [33] investigated users' perceptions of smart-home privacy risks from the perspective of external actors. The study interviewed eleven smart-home owners from the United States (US) through Skype video calls, revealing that American smart-home users value the convenience and connectedness of IoT devices more than obsolescence and security issues. Participants were more concerned with the government and Internet Service Providers (ISPs) having access to their smart home data than other external entities such as manufacturers and advisers. Participants' opinions about external entities depended on perceived benefits from these entities. Although most participants were fairly affluent, technically skilled, and highly interested in new technology, they were unaware of privacy risks from non-audio/video IoT devices. We note that the number of participants in the study is not significant, and the results may only apply to smart-home users living in the US.

This study aligns with the motivation to investigate the cybersecurity literacy of SHUs and to find new solutions to help SHUs be more aware of security and privacy issues and behave more securely at home. Cybersecurity education has emerged as a crucial factor in enhancing the attitudes of smart-home users toward security. One recent study that emphasizes the importance of cybersecurity education is the research conducted by Li *et al.* [34], which demonstrates the significance of online discourse about security and privacy risks and protections in educating smart-home users and shaping their individual and collective attitude development.

Cybersecurity education is an essential factor in enhancing cybersecurity literacy. The literature on cybersecurity literacy suggests that all user groups, including senior citizens, children, and adults, should have a minimum level of cybersecurity literacy to protect themselves from cyber attacks. For example, Blackwood-Brown, Levy, and D'Arcy [35] show that cybersecurity awareness training improved senior citizens' cybersecurity skills, allowing them to take proactive measures against cyber attacks. Similarly, Quayyum, Cruzes, and Jaccheri [36] highlight the need for cybersecurity education for children to ensure they develop safe and responsible online habits.

In their investigation into parental responsibility for children's online security, Ahmad *et al.* [37] survey 872 parents with children aged 17 and under. The study indicate a considerable lack of awareness among parents regarding cybersecurity threats that children face online. Sun *et al.* [38] conduct a study by interviewing 23 parents who live in smart homes across Canada and the US via Zoom video calls. They show that parents' perceptions and mitigation strategies regarding their children's safety in smart homes encompassed physical and digital aspects. However, the study has several limitations. Firstly, the authors acknowledged that some parents may have exhibited social desirability bias during the interviews–as they attempted to portray themselves as responsible parents. Additionally, the sample size was relatively small; the authors did not collect critical demographic information, such as gender and education level, that could have yielded deeper insights into the parents' responses. Finally, the study included participants from two Western countries that share similar national cultures based on Hofstede's cultural dimensions [39].

To fill the gap in the existing literature, our study addresses the need for a more diverse sample by recruiting and surveying smart home users from various national cultures using an online questionnaire. Furthermore, instead of focusing solely on parents, we broaden our research scope by focusing on adults in general, acknowledging that not all adults have children. Previous studies have mainly considered parents' cybersecurity awareness solely in relation to the safety of their children, overlooking the needs and safety of senior citizens. Therefore, our study aims to explore the willingness of adults to educate both children and senior citizens on cybersecurity, recognizing their responsibility for care for those who might not have the knowledge in their households.

- *H_3: SHUs agree that educating children on cybersecurity is crucial for protecting smart homes.*
- *H_4: SHUs agree that educating senior citizens on cybersecurity is crucial for protecting smart homes.*

There is strong convergent evidence for investigating SHUs' cybersecurity literacy toward the smart-home security because SHUs might interact with vulnerable and unreliable IoT devices and adversaries are interested in compromising these devices and users' data. Zeng, Mare, and Roesner [40] conducted interviews with 15 SHUs through phone or Skype calls. The participants in the study included women (approximately 27%) and men (approximately 73%). They were mostly aged 25 years and above (only three participants aged 18-24 years). The researchers found that participants had a large variety of IoT devices (e.g., 10 out of 15 SHUs owned at least six types of IoT devices). They also found that SHUs had limited personal concerns about security and privacy. In addition, participants' threat models often depended on the sophistication of their technical mental models, which demonstrated the importance of providing SHUs with technical security skills. Moreover, the researchers showed that smart homes with multiple users posed unique security and privacy issues, especially when the primary SHU has higher knowledge and control of the system than other SHUs. This result supports our research investigation of every group of SHUs.

Furthermore, we fill certain limitations of the work of Zeng, Mare, and Roesner [40] Firstly, previous research used a qualitative approach with a limited sample (i.e., 15 participants), whereas we propose a quantitative study with a significant sample of SHUs (i.e., 423 participants). Secondly, previous research did not give considerable attention to gender balance what we do in our research. Lastly, previous research did not specify participants' regions. Thus, it may not be reasonable to generalize the results. To cope with this limitation, we propose a cross-cultural study.

Previous studies have emphasized the importance of educating smart-home users (SHUs), including children, adults, and senior citizens, about cyber hygiene to foster the security of smart homes and ensure the safety of SHUs. However, further research is necessary to address the challenges related to SHUs' attitude toward cybersecurity and improve the security of smart homes. One critical obstacle to implementing effective cybersecurity education programs is the financial costs and resources involved [41]. The cost of cybersecurity education can be particularly challenging for average families.

In extended families, adults are often responsible for making decisions regarding the well-being of senior citizens and children. Therefore, our study focuses on the intention of adult smart-home users to participate in cybersecurity awareness training and their willingness to extend the training to other family members. Additionally, we investigate the use of non-financial incentives as a potential solution to promote long-term cybersecurity awareness among smart-home users.

3) Importance of Non-Financial Rewards: A reward is typically something given in exchange for good behavior. Rewards can be either financial, such as cash, or non-financial, such as awards and acknowledgments. As described in [42], extrinsic motivation (e.g., financial rewards) decreases the perception of intrinsic motivation, which implies the decreasing of actual intrinsic motivation. From a neuroscience perspective, extrinsic and intrinsic rewards trigger the same chemical reactions in the brain [43]. However, from a cost perspective, the former is expensive because of the financial aspect, whereas the latter is free. Furthermore, Gneezy, Meier, and Rey-Biel [44] noted that financial incentives may motivate users to change their behavior in the short run and even in the middle run. However, the desired change in users' lifestyle habits may disappear in the long run, i.e., when the incentives are removed. In contrast, non-financial rewards significantly impact intrinsic motivation [32]. Therefore, non-financial rewards may be more effective than financial rewards for promoting long-term behavior changes toward good cybersecurity hygiene among smart-home users.

III. Methodology

A. Survey Design

Our research collected quantitative data using online survey platforms. The survey took approximately 10 minutes to complete. We used a Japanese crowdsourcing platform called CrowdWorks [45] to recruit online participants from

Japan. Moreover, we used Prolific [46], a UK-based online crowdsourcing platform, to recruit UK respondents. We paid 1,000 Japanese Yen (about 7 Pounds Sterling) per hour for each participant. This is a standard rate that our institution pays to research participants.

We designed two survey questionnaires to align the survey results when considering the national language of Japan and the UK. We validated the translation correctness in three steps. Firstly, native Japanese speakers translated the questionnaire from English to Japanese. Then, another Japanese speaker who did not have knowledge of the original English questionnaire translated the previously translated questionnaire from Japanese back to English. Lastly, we compared the original English questionnaire with the translated one and found that the questionnaires were identical with the same semantics. Previous research articles [47], [48] used the same approach to verify translation correctness.

We piloted the survey questionnaires with 14 volunteers, six from Japan (50% female, 50% male) and eight from overseas (12.5% female and 87.5% male). We tested and revised the questionnaires accordingly. As described in the Appendix, our survey collected data using several constructs across the following five categories:

1) Demographics were measured using seven constructs (Dem_i, where $i = 1, \ldots, 7$)
2) Knowledge of smart homes was measured using two constructs (KSH_1 and KSH_2)
3) Smart-home security was measured using three constructs (SHS_1, SHS_2, and SHS_3)
4) Cybersecurity awareness training was measured using five constructs (CAT_j, where $j = 1, \ldots, 5$)
5) Non-financial rewards for pro-cybersecurity behavior were measured using four constructs (NFR_k, where $k = 1, \ldots, 4$)

On the other hand, we looked at the compliance of the questionnaires with ethical standards and procedures for research with human participants before distributing the survey to the target audience. It is noteworthy that we received our institution's Institutional Review Board (IRB) approval, which demonstrated that our research aligned with regulations and ethics in research studies involving human subjects.

Participants took the survey on a completely voluntary basis. We clarified the purpose of the study and the usage of the participants' responses before they took the survey. Eligibility criteria included being between the ages of 25 and 64 and either Japanese residents of Japan or British residents of the UK. Moreover, we provided informed consent to the participants. The participants who agreed to take the survey were requested to answer questions related to demographic information, knowledge about smart homes and their security, and interests in cybersecurity awareness training and non-financial rewards for good cybersecurity behavior at home.

B. *Pre-Selection Criteria of Participants*

We collected 434 responses between June 08 to June 22, 2022, from individuals living in smart homes. To ensure that participants were familiar with IoT devices while accounting for the heterogeneity of smart homes, we only considered those who owned and used at least five IoT devices from at least two device types at home. To ascertain this information, we asked two questions (see *Appendix A.2*):

1) *(KSH_1) How many IoT devices do you own?*
2) *(KSH_2) Please select all the types of IoT devices used in your house.*

After screening for eligibility, we excluded seven respondents who did not meet the ownership criteria and four who did not disclose essential information, such as their citizenship or education levels. Our final sample size was 423 participants. For the purpose of this study, we use the term "citizenship" to refer to both citizenship and nationality.

C. *Statistical Analysis*

We first conducted a descriptive statistical analysis of the collected data to examine the demographics and background of the sample population. We presented the data using tables, summarizing categorical variables with frequencies (%) and numerical variables with measures of central tendency (mean: μ) and dispersion (standard deviation: σ). Afterward, we made predictions about the larger population of smart-home users through the application of inferential statistical methods on the collected data, thus providing a comprehensive understanding of the sample population and its relationship to the population of smart-home users. We performed data analysis using R.

To enhance data analysis, we combined or classified some categories due to limited data. Specifically, we grouped age categories 45-54 and 55-64 into a single category 45-64, and education was categorized into two levels: secondary education (junior and high school) and higher education (bachelor's, master's, and doctorate degrees). We also combined "very insecure" and "insecure" into "insecure". and "very secure" and "secure" into "secure" for the perception of security levels. In terms of employment status, we categorized individuals as "unemployed" if they were not "employed full-time", "self-employed", or "employed part-time". Additionally, the number of IoT devices owned was classified as 5-10 or more than 10, and known cyberattacks were classified into three groups: 0-2, 3-4, and 5-6. These modifications allowed for a more comprehensive and in-depth analysis of our data.

The subsequent section presents the statistics of the variables of interest.

IV. Results

A. *Descriptive Statistics*

We surveyed 423 participants (52.96% from Japan and 47.04% from the UK), including 224 participants from Japan (46% female, 54% male) and 199 participants from the UK (45.2% female, 54.8% male). The ages of participants ranged from 25 to 64 years old. In the UK, the majority of participants were in the 25-34 age range (35.7%), followed by 33.2% in the 35-44 age range, and 31.2% in the 45-64 age range. In Japan, the majority of participants were in the 35-44 age range (45.1%), followed by 31.7% in the 25-34 age range, and 23.2% in the 45-64 age range.

TABLE I
DESCRIPTIVE STATISTICS

	Japan		UK	
	Obs	% μ (σ)	Obs	% μ (σ)
Citizenship	224	52.96%	199	47.04%
Age group				
25 - 34	71	31.7%	71	35.7%
35 - 44	101	45.1%	66	33.2%
45 - 64	52	23.2%	62	31.2%
Gender				
Female	103	46%	90	45.2%
Male	121	54%	109	54.8%
Level of education				
Secondary Education	67	29.9%	73	36.7%
Higher Education	157	70.1%	126	63.3%
Employment status				
Unemployed	38	17%	25	12.6%
Employed full-time	121	54%	151	75.9%
Employed part-time	35	15.6%	12	6%
Self-employed	30	13.4%	11	5.5%
Number of household members under 18 years old	224	1 (1.1)	199	0.9 (1.0)
Number of household members aged 65 and older	224	0.4 (0.8)	199	0.1 (0.4)
Number of IoT devices owned				
5-10	213	95.1%	146	73.4%
More than 10	11	4.9%	53	26.6%
Number of distinct categories of IoT devices owned	224	5.7 (1.8)	199	5.6 (1.9)
Cybersecurity experience				
No	173	77.2%	141	70.9%
Yes	51	22.8%	58	29.1%
Number of known cyberattacks				
0 - 2	102	45.5%	43	21.6%
3 - 4	100	44.6%	105	52.8%
5 - 6	22	9.8%	51	25.6%
Perception of the security level of your smart home				
I don't know / Unsure	129	57.6%	87	43.7%
Insecure	50	22.3%	23	11.6%
Secure	45	20.1%	89	44.7%

Table I provides more information about our sample. The majority of participants from Japan (70.1%) and the UK (63.3%) had a higher education, while the remaining participants had completed their secondary education. Regarding employment status, the majority of participants from Japan (54%) and the UK (75.9%) were full-time employees, with the remainder being part-time employed, self-employed, or unemployed.

On average, Japanese households had one person under the age of 18 ($\sigma = 1.1$), while British households had an average of 0.9 persons ($\sigma = 1.0$) in this age group. Regarding persons aged 65 and older, Japanese households had an average of 0.4 persons ($\sigma = 0.8$), whereas British households had an average of 0.1 persons ($\sigma = 0.4$).

Most participants from Japan (95.1%) and the UK (73.4%) owned between five to ten IoT devices. On average, Japanese participants owned 5.7 ($\sigma = 1.8$) distinct categories of IoT devices, while British participants owned an average of 5.6 ($\sigma = 1.9$) categories.

The participants in the study had limited experience with cybersecurity, with only a minority of British (29.1%) and Japanese (22.8%) respondents reporting having received formal training or having worked or studied in the field.

When asked about their knowledge of different types of cyberattacks, 78.4% of British participants were able to recognize at least three out of the six common attack types presented, while 54.4% of Japanese participants had a similar level of knowledge.

Furthermore, the results showed that only 20.1% of Japanese participants perceived their smart-home as secure, compared to 44.7% of British participants. These findings suggest that there may be cultural differences in smart-home's users attitudes toward cybersecurity.

B. Inferential Statistics

The present section analyzes the regression results obtained from the dependent variables aligned with our research questions. To visually showcase the findings, we provide a graphical comparison of the responses from Japan and the UK. Afterward, we present the results of logit models, along with their respective regression coefficients. Finally, we analyze and interpret the marginal effects.

1) SHUs' Interest in Cybersecurity Awareness Training: We analyze SHUs' interest in cybersecurity awareness training (CAT) using three dependent variables: need of CAT (CAT_1),

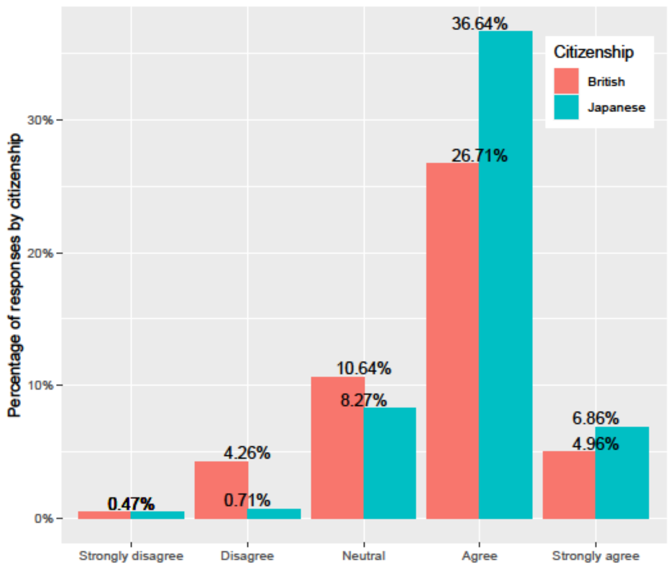

Fig. 2. Agreement on the necessity of cybersecurity awareness training for securing smart homes effectively.

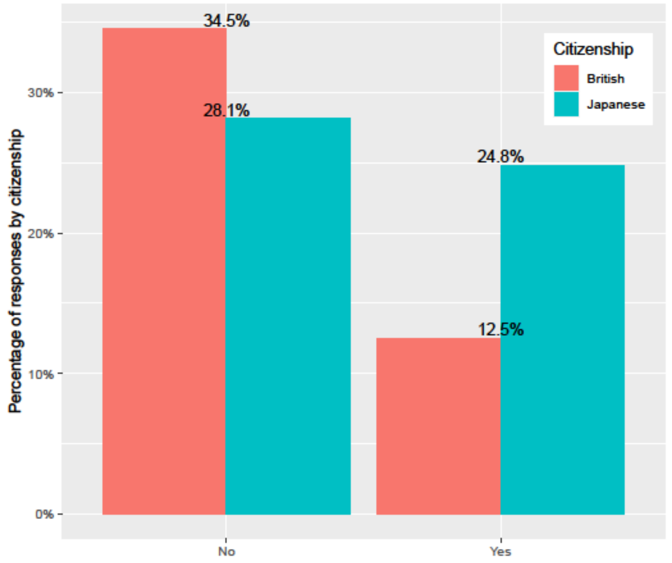

Fig. 3. Willingness to spend money on cybersecurity awareness training.

willingness to spend money on CAT (CAT_2), and willingness to spend time on CAT (CAT_3).

Figures 2, 3, and 4 show that a majority of British and Japanese respondents recognized the importance of cybersecurity awareness training to secure smart homes, with 75.17% expressing agreement or strong agreement. However, despite this recognition, 62.6% were not willing to invest money in such training. Conversely, 80.6% of respondents agreed that spending time on cybersecurity awareness training is a worthwhile endeavor.

Table II summarizes the results of the logit and ordered logit models on British and Japanese respondents. The analysis shows that the variable *citizenship* significantly impacted the perceived need for cybersecurity awareness training for smart home security ($p < 0.01$, column 2), willingness to spend money on training ($p < 0.01$, column 3), and willingness to allocate time for training ($p < 0.05$, column 4).

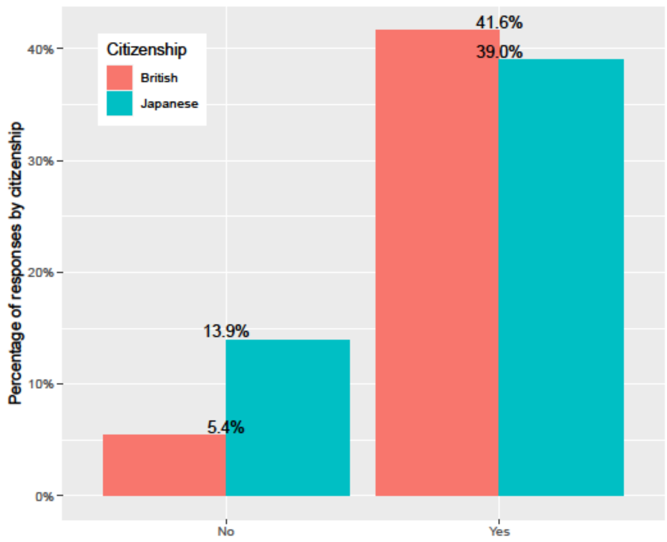

Fig. 4. Willingness to spend time on cybersecurity awareness training.

Table III summarizes the marginal effects resulting from the ordered logit regression analysis, which were estimated for the independent variable *citizenship*. The comparison between British and Japanese respondents revealed differences in their perceptions regarding the importance of cybersecurity awareness training for securing smart homes. Japanese respondents demonstrated a 0.8% decrease in the likelihood of expressing a strong disagreement, a 4% decrease in the likelihood of expressing disagreement, a 12.3% decrease in the likelihood of holding a neutral stance, an 8.3% increase in the likelihood of expressing agreement, and an 8.8% increase in the likelihood of expressing strong agreement when compared to British respondents. These findings suggest that Japanese respondents generally recognized the significance of cybersecurity awareness training more than British respondents.

Table IV presents the marginal effects resulting from the logit regression analysis. The analysis compared the spending behavior of British and Japanese respondents regarding cybersecurity awareness training. The findings showed that, in comparison to British respondents, Japanese respondents were 26.8% more likely to allocate financial resources toward cybersecurity awareness training. Conversely, Japanese respondents were 9.8% less likely to allocate time toward cybersecurity awareness training compared to British respondents. These results highlight the disparities in the resource allocation patterns between Japanese and British respondents in regard to cybersecurity awareness training.

2) Cybersecurity Awareness Training for Children: Our analysis of SHUs' opinions on the significance of cybersecurity awareness training for children, using the construct CAT_4, revealed noteworthy results.

As shown in Table II, the independent variable *citizenship* has a statistically significant impact on SHUs' opinions regarding the importance of cybersecurity awareness training for children in maintaining the security of smart homes ($p < 0.01$).

The findings are further visualized in Figure 5, which

TABLE II
REGRESSION RESULTS OF THE LOGIT AND ORDERED LOGIT MODELS

	Dependent variables							
	CAT_1	CAT_2	CAT_3	CAT_4	CAT_5	NFR_1	NFR_2	NFR_3
	Ordered Logit	Logit	Logit	Ordered Logit	Ordered Logit	Ordered Logit	Ordered Logit	Ordered Logit
Citizenship (Japanese)	0.953*** (0.243)	1.287*** (0.268)	−0.717** (0.325)	−0.899*** (0.228)	−1.219*** (0.229)	−0.955*** (0.221)	0.588*** (0.204)	1.050*** (0.205)
Age (25 - 34)	0.141 (0.265)	0.516* (0.295)	0.343 (0.353)	0.221 (0.257)	0.750*** (0.254)	0.190 (0.253)	0.127 (0.232)	−0.057 (0.234)
Age (35 - 44)	0.133 (0.255)	0.250 (0.281)	0.349 (0.331)	0.418* (0.250)	0.610** (0.243)	−0.221 (0.245)	−0.030 (0.223)	−0.043 (0.221)
Gender (Male)	−0.310 (0.220)	−0.005 (0.234)	−0.086 (0.289)	−0.390* (0.210)	−0.309 (0.207)	0.174 (0.206)	0.053 (0.190)	0.288 (0.190)
Level of education (Higher Education)	−0.082 (0.220)	−0.045 (0.240)	0.152 (0.285)	−0.231 (0.214)	−0.230 (0.211)	−0.047 (0.212)	−0.209 (0.196)	−0.101 (0.197)
Employment status (Employed full-time)	0.426 (0.292)	1.162*** (0.367)	0.335 (0.379)	0.281 (0.285)	0.170 (0.286)	0.061 (0.288)	0.369 (0.256)	0.238 (0.262)
Employment status (Employed part-time)	−0.138 (0.389)	0.743 (0.457)	−0.260 (0.470)	0.330 (0.385)	−0.554 (0.387)	−0.040 (0.385)	−0.094 (0.346)	0.409 (0.350)
Employment status (Self-employed)	−0.114 (0.404)	0.945* (0.483)	−0.414 (0.480)	0.018 (0.392)	0.146 (0.394)	−0.454 (0.398)	−0.267 (0.366)	−0.398 (0.351)
Number of household members under the age of 18	−0.087 (0.097)	0.041 (0.103)	0.090 (0.130)	0.081 (0.095)	0.070 (0.092)			
Number of household members over the age of 65	−0.046 (0.169)	0.073 (0.177)	−0.255 (0.200)	0.093 (0.166)	0.280* (0.163)			
Number of IoT devices owned (More than 10)	0.487 (0.317)	0.225 (0.329)	−0.389 (0.435)	0.386 (0.291)	0.424 (0.297)	0.248 (0.292)	0.942*** (0.281)	0.123 (0.277)
Cybersecurity experience (Yes)	0.356 (0.249)	0.087 (0.259)	0.208 (0.353)	0.315 (0.234)	0.329 (0.234)	0.044 (0.224)	0.288 (0.211)	0.073 (0.208)
Number of known cyberattacks (3 - 4)	0.587** (0.233)	0.654** (0.254)	0.845*** (0.291)					
Number of known cyberattacks (5 - 6)	0.166 (0.337)	0.436 (0.366)	0.881* (0.473)					
Perception of the security level of your smart home (Insecure)	0.835*** (0.291)	0.465 (0.297)	0.735* (0.390)	0.680** (0.277)	0.230 (0.268)	0.040 (0.267)	0.191 (0.247)	0.375 (0.248)
Perception of the security level of your smart home (Secure)	0.047 (0.238)	0.479* (0.261)	0.490 (0.328)	0.081 (0.229)	0.282 (0.227)	0.642*** (0.234)	0.606*** (0.211)	0.595*** (0.211)
Constant		−3.179*** (0.528)	0.701 (0.503)					
Observations	423	423	423	423	423	423	423	423

***p<0.01; **p<0.05; *p<0.1

TABLE III
MARGINAL EFFECTS OF CITIZENSHIP FOR ORDERED LOGIT MODELS CAT_1, CAT_4, CAT_5, NFR_1, NFR_2, AND NFR_3

		Strongly disagree (Very dissatisfied) (Not at all)	Disagree (Dissatisfied) (Slightly)	Neutral (I don't know/ Unsure) (Moderately)	Agree (Satisfied) (Very)	Strongly agree (Very satisfied) (Extremely)
Citizenship (Japanese)	CAT_1	-0.008*	-0.040***	-0.123***	0.083***	0.088***
	CAT_4	0.002	0.007*	0.077***	0.116***	-0.201***
	CAT_5	0.004	0.034***	0.109***	0.111***	-0.259***
	NFR_1		0.024***	0.192***	-0.141***	-0.075***
	NFR_2	-0.122***	-0.024**	0.070***	0.054***	0.022**
	NFR_3	-0.183***	-0.072***	0.059***	0.124***	0.072***

*** p <0.01; ** p <0.05; * p <0.1

highlights that a significant majority of British and Japanese respondents concurred that educating children on cybersecurity is critical for ensuring the security of smart homes, with 87.72% indicating agreement or strong agreement.

On the other hand, Table III indicates that Japanese respondents had a slightly different attitude towards the issue compared to British respondents. They were 0.2% more likely to express strong disagreement, 0.7% more likely to express disagreement, 7.7% more likely to express a neutral stance, 11.6% more likely to express agreement, and 20.1% less likely to express strong agreement.

3) Cybersecurity Awareness Training for Senior Citizens: The analysis of SHUs' opinions regarding the importance of cybersecurity awareness training for senior citizens, using the construct CAT_5, revealed meaningful insights.

As presented in Table II, our findings indicated that the independent variable *citizenship* has a statistically significant effect on SHUs' views about the significance of cybersecurity awareness training for senior citizens in securing smart homes ($p < 0.01$).

In addition, Figure 6 shows that a substantial proportion of British and Japanese respondents considered that educating senior citizens on cybersecurity is crucial for ensuring the security of smart homes, with 82.97% of respondents indicating agreement or strong agreement.

However, Table III reveals that compared to British respondents, Japanese respondents showed a slightly different attitude towards the issue. They were 0.4% more likely to express strong disagreement, 3.4% more likely to express disagreement, 10.9% more likely to hold a neutral stance, 11.1% more likely to express agreement, and 25.9% less likely to express strong agreement.

4) SHU's Interest in Non-Financial Rewards for Promoting Cybersecurity Behavior: The analysis showed that the

TABLE IV
MARGINAL EFFECTS OF LOGIT MODELS CAT_2 AND CAT_3

	Dependent variables	
	CAT_2	CAT_3
Citizenship (Japanese)	0.268 *** (0.050)	-0.098 ** (0.043)
Age (25 - 34)	0.107 * (0.060)	0.050 (0.051)
Age (35 - 44)	0.051 (0.056)	0.050 (0.049)
Gender (Male)	-0.001 (0.049)	-0.012 (0.040)
Level of education (Higher education)	-0.009 (0.050)	0.021 (0.041)
Employment status (Employed full-time)	0.221 *** (0.059)	0.046 (0.055)
Employment status (Employed part-time)	0.132 (0.082)	-0.042 (0.076)
Employment status (Self-employed)	0.174 * (0.090)	-0.069 (0.081)
Number of household members under the age of 18	0.008 (0.022)	0.013 (0.018)
Number of household members over the age of 65	0.015 (0.037)	-0.036 (0.028)
Number of IoT devices owned (More than 10)	0.047 (0.070)	-0.058 (0.069)
Cybersecurity experience (Yes)	0.018 (0.055)	0.028 (0.046)
Number of known cyberattacks (3 - 4)	0.134 *** (0.050)	0.127 *** (0.045)
Number of known cyberattacks (5 - 6)	0.087 (0.074)	0.131 ** (0.063)
Perception of the security level of your smart home (Insecure)	0.097 (0.063)	0.098 ** (0.046)
Perception of the security level of your smart home (Secure)	0.100 * (0.054)	0.069 (0.044)
Observations	423	423

*** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$

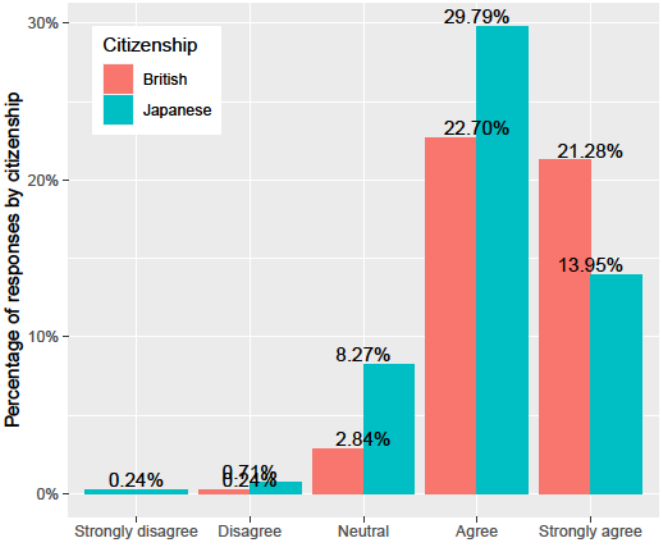

Fig. 5. Cybersecurity awareness training for children.

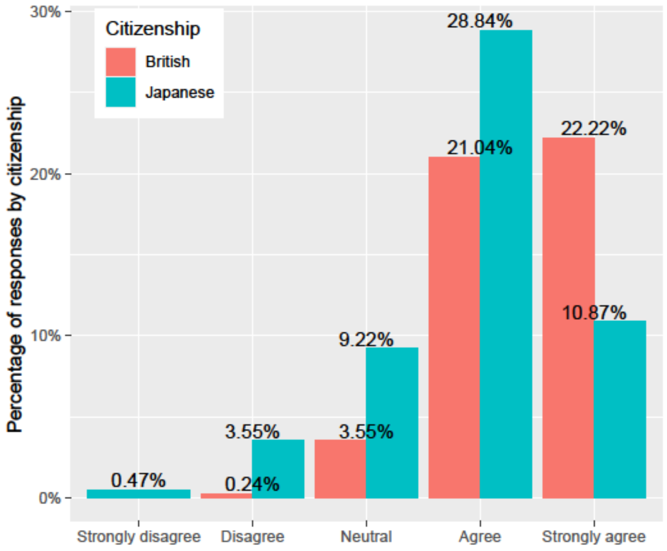

Fig. 6. Cybersecurity awareness training for senior citizens.

independent variable *citizenship* had a statistically significant impact on SHUs' satisfaction with non-financial rewards for good cybersecurity behavior in smart homes. Specifically, the significance level was $p < 0.01$ for the constructs NFR_1, NFR_2, and NFR_3, as shown in Table II.

Figure 7 provides additional insights into participants' attitudes towards non-financial rewards. Most respondents,

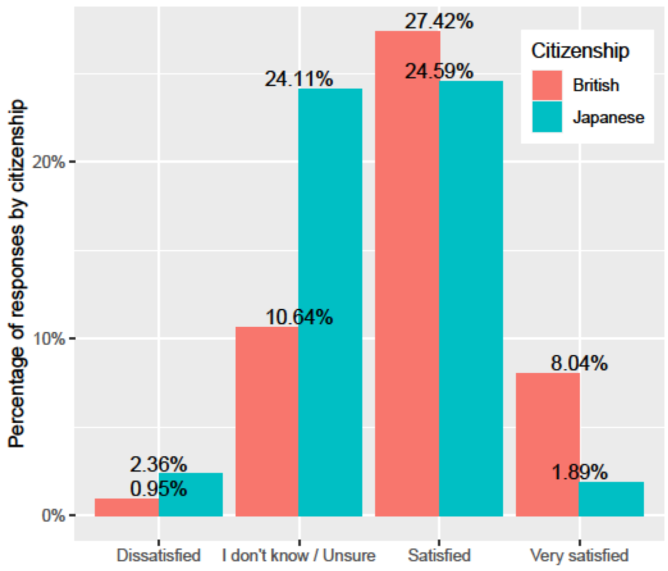

Fig. 7. Level of satisfaction with non-financial rewards for promoting cybersecurity hygiene at home.

61.94%, reported feeling satisfied or very satisfied with these types of rewards. Meanwhile, 34.75% of respondents were unsure about their feelings towards non-financial rewards, and 3.31% reported feeling dissatisfied.

As presented in Table III, Japanese respondents had a 2.4% higher probability of being dissatisfied, a 19.2% higher probability of holding a neutral stance, a 14.1% lower probability of being satisfied, and a 7.5% lower probability of being very satisfied with non-financial rewards for cybersecurity behavior in smart homes compared to British respondents.

The investigation of non-financial rewards, such as awards and virtual reality (VR) services, revealed notable findings. Japanese respondents demonstrated a higher level of interest in the "Certificate of Achievement for Good Cybersecurity Behavior at Home" than British respondents, with decreases of 12.2% and 2.4% in the "not at all interested" and "slightly interested" categories, respectively, and increases of 7%, 5.4%, and 2.2% in the "moderately interested", "very interested", and "extremely interested" categories, highlighting the cultural differences in the perceived value of this specific reward.

In addition, Japanese respondents showed a higher level of interest in having virtual reality services in smart homes as a non-financial reward, with a lower percentage of being categorized as "not at all interested" or "slightly interested", and a higher percentage of being categorized as "moderately interested", "very interested", or "extremely interested", as compared to British respondents. Specifically, Japanese respondents displayed a decrease of 18.3% for the "not at all interested" category, 7.2% for the "slightly interested" category, and an increase of 5.9% for the "moderately interested" category, 12.4% for the "very interested" category, and 7.2% for the "extremely interested" category, as compared to British respondents.

Figure 8 presents the results of our survey regarding the most desirable non-financial rewards. The two most popular rewards were "cyber insurance discounts" (31.44%) and "virtual point rewards" (26.24%). Interestingly, there were some differences in preferences between British and Japanese respondents. British respondents showed a greater interest in "cyber insurance discounts" as a reward (16.31%), while Japanese respondents were more interested in "virtual point rewards" (21.04%).

V. Discussion

Our study investigated whether adult smart-home users had an interest in cybersecurity awareness training and non-financial rewards for good cybersecurity behaviors. To achieve this objective, we formulated research questions related to citizenship, interest in cybersecurity awareness training, interest in non-financial rewards, and opinions on educating children and senior citizens on cybersecurity. Our analysis suggests that citizenship plays a significant role in shaping the interests of adult smart-home users in cybersecurity awareness training and their perceptions of its importance for children and senior citizens. Moreover, our analysis reveals that cultural differences influence the interest of smart-home users in non-financial rewards.

In the following sections, we will delve into the details of our results, discussing significant findings. We will also present the implications of our findings, as well as the limitations of our study and suggestions for future work.

A. Users' Cybersecurity Awareness for Home Security

1) Adult SHUs' Interest in Cybersecurity Awareness Training: Our results suggest that there is a significant correlation between citizenship and interest in cybersecurity awareness training. Specifically, Japanese respondents are more likely than British respondents to recognize the importance of cybersecurity education and allocate money toward it. However, they are less likely to allocate time for cybersecurity awareness training.

The data suggests that while most Japanese and British respondents expressed interest in cybersecurity awareness training, there were differences in the level of interest between the two groups. These differences are consistent with previous studies that have highlighted the crucial role of cultural differences in shaping users' attitudes towards cybersecurity [26], [27]. Our study further supports the hypothesis that cultural differences influence adult smart-home users' interest in cybersecurity awareness training. Hofstede's cultural dimensions suggest that Japanese prioritize collectivism, while British people focus on individualism. These cultural differences may have influenced the perceived importance of cybersecurity awareness training for each group of respondents. It is possible that Japanese respondents were more likely to acknowledge the importance of cybersecurity awareness training due to their cultural attitudes towards safety and security, which emphasize collective responsibility. In contrast, British respondents may be less interested in cybersecurity awareness training due to their individualistic cultural attitudes. Additionally, the higher level of insecurity among Japanese respondents regarding the security of their smart homes compared to British respondents could also explain the difference in interest levels.

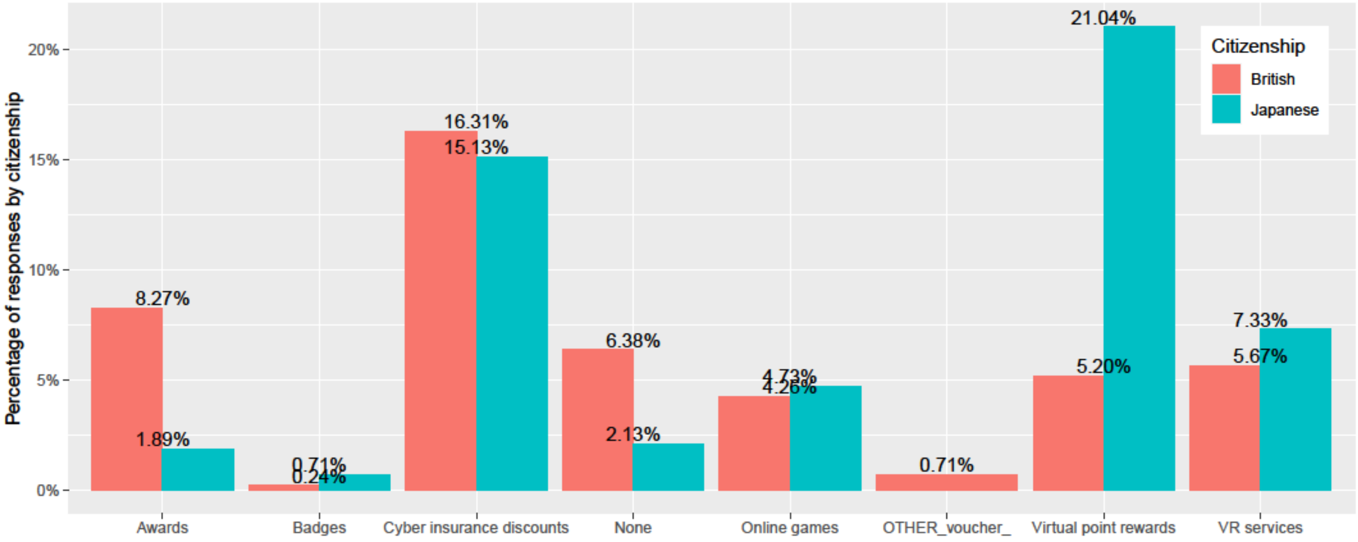

Fig. 8. Non-financial rewards for secure behavior in smart homes.

The findings indicate that there were significant differences in the willingness of Japanese and British respondents to allocate money toward cybersecurity awareness training, which could be influenced by socio-economic and cultural factors. While both groups demonstrated limited willingness to invest money in training, the extent of their allocation varied. Prior research has shown that Japan has lower income inequality and higher social well-being than the UK [14], [15]. These factors could impact the resources that individuals are willing or able to allocate toward cybersecurity awareness training. Furthermore, Japanese respondents may be more likely to prioritize spending on cybersecurity education due to cultural values of collective responsibility and a stronger social safety net. Conversely, British respondents may have less disposable income and less motivation to spend money on cybersecurity education due to higher income inequality.

The data reveals that British respondents were more willing to allocate time to cybersecurity awareness training compared to their Japanese counterparts. Nonetheless, it is worth noting that both groups demonstrated a willingness to invest some time in training. The disparity could be attributed to Hofstede's cultural dimensions theory, which suggests that Japanese people tend to experience more stress and uncertainty about the future than the British due to their higher level of uncertainty avoidance. Consequently, Japanese people may exhibit a greater reluctance to invest time in training that is not directly related to their primary occupation. Our findings are consistent with previous research highlighting the importance of considering both time and monetary costs when designing effective education programs for household security [7].

2) Cybersecurity Awareness Training for Children: The findings indicate that the majority of adults surveyed believe that providing education on cybersecurity to children is crucial for smart home security. This result aligns with the previous research of Ahmad *et al.* [37], who identified a lack of parental awareness regarding their children's online activities. Providing children with cybersecurity awareness training could address the issue of parental unawareness, as it would help children understand the risks posed by cyber threats and learn how to behave safely on the Internet.

In addition, our study shows a significant relationship between the citizenship of adult smart-home users and their attitudes towards the importance of cybersecurity awareness training for children in maintaining the security of smart homes. Specifically, the results indicate that cultural differences between Japan and the UK influence adults' appreciation of children's training toward safe online activities in smart homes. Our findings differ from those of Sun *et al.* [38], who investigated smart-home users from two countries with similar cultural backgrounds according to Hofstede's cultural dimensions.

3) Cybersecurity Awareness Training for Senior Citizens: The findings of our study indicate that both Japanese and British participants share a common belief in the importance of cybersecurity awareness training for senior citizens to protect themselves against cyber threats. These results are consistent with prior research conducted by Blackwood-Brown, Levy, and D'Arcy [35], who have also shown that cybersecurity awareness training can empower senior citizens to defend against cyber attacks proactively.

However, our analysis shows a significant correlation between the nationality of adult smart-home users and their perception of the importance of cybersecurity awareness training for senior citizens to secure smart homes. This result suggests that cultural differences between the two groups could influence their overall attitudes towards this issue, with Japanese participants less inclined than their British counterparts.

A potential reason for this gap in perception could be that British participants may possess a more comprehensive knowledge of the different types of cyber threats than their Japanese counterparts. The lack of awareness of cyber threats may make the Japanese less concerned about the dangers that older adults face from cyber attacks. This emphasizes the importance of increasing awareness about cyber threats in

Japan, particularly among senior citizens, to ensure that they can effectively protect themselves and their smart homes from potential cyber threats.

B. Non-Financial Reward for Cybersecurity

The findings of our study contribute to understanding the influence of national cultures on smart-home users' interests in non-financial rewards. The result validates our hypothesis that cultural disparities can affect the inclination of smart-home users towards non-financial rewards for demonstrating secure behavior. This outcome is in line with the work of Ndibwile *et al.* [28], who found significant differences in security perception between smartphone users from Japan and Tanzania, two countries with different cultural backgrounds based on Hofstede's cultural dimensions.

The results also suggest that the most significant non-financial incentives for participants are cyber insurance discounts and virtual point rewards. It is worth noting that there were differences in the preferences of British and Japanese participants, with the former expressing a greater interest in cyber insurance discounts and the latter in virtual point rewards.

With regard to cyber insurance discounts, it is worth noting that insurance solutions for cyber risks are not a recent development in the United Kingdom, particularly within the corporate sector. It is possible that the inclination of British SHUs towards cyber insurance discounts, as indicated by our study, could be linked to the fact that our participants were mostly employees. Nonetheless, promoting similar initiatives for individuals, including smart-home users, is advisable to create a safe and secure smart environment and cyberspace.

On the other hand, the preference of Japanese participants for virtual points is not arbitrary. Instead, it reflects the common practice in Japan of earning points for purchases, which can be redeemed for future transactions. The promotion of cashless payment services based on point reward systems by the Japanese government further supports this trend. Specifically, the government launched the Individual Number Card Points initiative, also known as MyNa Points, in 2020, which is ongoing. The widespread adoption of these systems in Japan emphasizes the significance of recognizing cultural norms when implementing reward programs.

Our results indicate that customizing non-financial rewards to users' cultures is crucial in motivating good cybersecurity hygiene practices in smart homes. This finding is consistent with Argyris *et al.* 's research [29], highlighting the importance of tailoring picture passwords to cultural differences.

These findings are consistent with the work of Argyris *et al.* [29], who demonstrated the importance of customizing picture passwords based on cultural differences. Similarly, our results emphasize the importance of customizing non-financial rewards to users' cultures to increase their effectiveness in motivating good cybersecurity hygiene practices in smart homes.

C. Implications

Our study highlights the importance of cultural factors in shaping adult smart-home users' attitudes toward cybersecurity awareness training. It is essential to design training programs that are tailored to the target audience's cultural and socio-economic backgrounds.

Moreover, cost and time constraints must be considered when designing effective cybersecurity awareness training programs. Additionally, Governments should support these programs by offering non-financial incentives, such as cyber insurance discounts in the UK and virtual point rewards in Japan.

Our study also emphasizes the need for training programs that address the unique cybersecurity challenges faced by children and senior citizens in smart-home environments. Ensuring that these groups have the knowledge and skills needed to maintain the security of their smart homes would promote safe and secure smart homes.

In addition, this study emphasizes the importance of developing and providing cyber insurance solutions and virtual rewards tailored to the distinct needs of smart-home users in the UK and Japan, respectively.

Finally, our study suggests the need for further research to understand the role of cultural differences in shaping users' attitudes toward cybersecurity. In addition, future work should implement and evaluate the effectiveness of non-financial incentives for promoting good cybersecurity hygiene practices in smart homes.

D. Limitations

It is important to recognize the limitations of this study. Firstly, while our research findings provide insights into the relationship between adult smart-home users' citizenship and their perceptions of the importance of cybersecurity awareness training and non-financial rewards, the underlying reasons that explain our results were not investigated in detail. Although our study provides some possible motivations, future research should focus on building and evaluating constructs that could provide a more detailed explanation of our findings.

Secondly, our study has limitations related to the profile of participants. Specifically, we were unable to verify whether participants possessed and used IoT devices in their homes. Additionally, the criteria used to define "smart-home users" in our study may be questionable because the exact number and types of IoT devices required to qualify a house as a "smart home" are currently unknown. Therefore, future studies may need to refine the definition of "smart-home users" to ensure the high quality of data collected.

Finally, our study is limited to participants from only two countries and cultures. Investigating a more diverse range of cultures could provide valuable insights into the relevance and applicability of our study findings.

VI. Conclusion

Smart-home users who lack cybersecurity awareness are at risk of cyberattacks that can disrupt the functioning of their smart homes and compromise their safety and privacy. Providing cybersecurity awareness training to smart-home users can equip them with the necessary knowledge and skills to prevent IoT misuse and security breaches. However, research indicates that users are often unwilling or unable to bear the costs of cybersecurity education.

Thus, we surveyed British and Japanese individuals between the ages of 25 and 64 living in smart homes to investigate this issue further. The results showed that while most participants recognized the importance of cybersecurity education and considered spending time on cybersecurity awareness training worthwhile, they were not willing to pay for such training. Additionally, participants agreed that educating children and senior citizens on cybersecurity was crucial for protecting smart homes. We also found that non-financial incentives for good cybersecurity practices in smart homes would satisfy most participants. British participants were particularly interested in cyber insurance discounts, while Japanese participants showed greater interest in virtual point rewards.

The findings of this study indicate noteworthy cultural differences between British and Japanese attitudes toward cybersecurity awareness training and non-financial incentives for securing smart homes. However, further research is necessary to comprehensively understand the cultural factors influencing smart-home users' inclination toward cybersecurity services. This knowledge will be valuable in implementing personalized solutions that encourage good cybersecurity practices in smart homes. Additionally, we recommend designing cost-effective and time-efficient cybersecurity awareness training programs for smart-home users to ensure the widespread adoption of these training programs.

ACKNOWLEDGMENTS

REFERENCES

[1] J. Happa, M. Glencross, and A. Steed, "Cyber security threats and challenges in collaborative mixed-reality," *Frontiers in ICT*, vol. 6, p. 5, 2019, https://doi.org/10.3389/fict.2019.00005.

[2] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes—Past, present, and future," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 1190–1203, 2012, https://doi.org/10.1109/TSMCC.2012.2189204.

[3] A. Laughlin, "How a smart home could be at risk from hackers," 2021, accessed 6 March 2023. [Online]. Available: https://www.which.co.uk/news/2021/07/how-the-smart-home-could-be-at-risk-from-hackers/

[4] Statista, "Smart Home Report 2021," 2021, accessed 6 March 2023. [Online]. Available: https://www.statista.com/study/42112/smart-home-report/

[5] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research*, vol. 20, pp. 79–98, 03 2009, https://doi.org/10.1287/isre.1070.0160.

[6] H. Aldawood and G. Skinner, "Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering," in *Cybersecurity and Cyberforensics Conference (CCC)*, 2019, pp. 111–117, https://doi.org/10.1109/CCC.2019.00004.

[7] N. Y.-R. Douha, B. O. Sane, M. Sasabe, D. Fall, Y. Taenaka, and Y. Kadobayashi, "Cost-benefit analysis toward designing efficient education programs for household security," in *The Fifteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE)*, November 2021, pp. 59–68.

[8] Y. Lu, "Cybersecurity research: A review of current research topics," *Journal of Industrial Integration and Management*, vol. 3, no. 04, p. 1850014, 2018, https://doi.org/10.1142/S2424862218500148.

[9] L. Coventry, P. Briggs, J. Blythe, and M. Tran, *Using behavioural insights to improve the public's use of cyber security best practices.* Government Office for Science, May 2014, available under an Open Government Licence, terms and conditions available here - http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/.

[10] A. Lindbeck, "Incentives and social norms in household behavior," *The American Economic Review*, vol. 87, no. 2, pp. 370–377, 1997. [Online]. Available: http://www.jstor.org/stable/2950948

[11] S. Goel, K. J. Williams, J. Huang, and M. Warkentin, "Can financial incentives help with the struggle for security policy compliance?" *Information & Management*, vol. 58, no. 4, p. 103447, 2021, https://doi.org/10.1016/j.im.2021.103447.

[12] Y. J. Li and E. Hoffman, "Behavioral compliance theory: An experimental and behavioral economics approach to information security policy compliance," *SSRN*, 2021. [Online]. Available: https://ssrn.com/abstract=3252742

[13] N. E. Adler, T. Boyce, M. A. Chesney, S. Cohen, S. Folkman, R. L. Kahn, and S. L. Syme, "Socioeconomic status and health: the challenge of the gradient." *American Psychologist*, vol. 49, no. 1, p. 15, 1994, https://doi.org/10.1037/0003-066X.49.1.15.

[14] D. Ballas, D. Dorling, T. Nakaya, H. Tunstall, and K. Hanaoka, "Income inequalities in japan and the uk: A comparative study of two island economies," *Social Policy and Society*, vol. 13, no. 1, p. 103–117, 2014.

[15] K. Pickett and R. Wilkinson, *The spirit level: Why equality is better for everyone.* Penguin UK, 2010.

[16] G. Hofstede, "Dimensionalizing cultures: The Hofstede model in context," *Online Readings in Psychology and Culture*, vol. 2, no. 1, pp. 2307–0919, 2011.

[17] IBM, "X-Force Threat Intelligence Index 2021," 2021, accessed 6 March 2023. [Online]. Available: https://www.ibm.com/downloads/cas/M1X3B7QG

[18] The Government of Japan, "Cybersecurity Strategy," 2021, accessed 6 March 2023. [Online]. Available: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf

[19] GOV.UK, "National Cyber Strategy 2022," 2022, accessed 6 March 2023. [Online]. Available: https://www.gov.uk/government/publications/national-cyber-strategy-2022

[20] IoT Acceleration Consortium, "IoT Security Guidelines Ver. 1.0," 2016, accessed 6 March 2023. [Online]. Available: http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf

[21] IPA, "IoT Safety/Security Development Guidelines (Second Edition)," 2016, accessed 6 March 2023. [Online]. Available: https://www.ipa.go.jp/files/000053920.pdf

[22] Ministry of Economy, Trade and Industry, "New International Standard for Safe Use of IoT Products and Systems Issued," 2021, accessed 6 March 2023. [Online]. Available: https://www.meti.go.jp/english/press/2021/0621_003.html

[23] UK Parliament, "Product Security and Telecommunications Infrastructure Bill," 2021, accessed 6 March 2023. [Online]. Available: https://bills.parliament.uk/bills/3069/publications

[24] Statista, "Smart Home: Japan," 2023, accessed 6 March 2023. [Online]. Available: https://www.statista.com/outlook/dmo/smart-home/japan

[25] ——, "Smart Home: United Kingdom," 2021, accessed 6 March 2023. [Online]. Available: https://www.statista.com/outlook/dmo/smart-home/united-kingdom

[26] M. Harbach, A. De Luca, N. Malkin, and S. Egelman, "Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, ser. CHI '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 4823–4827, https://doi.org/10.1145/2858036.2858273. [Online]. Available: https://doi.org/10.1145/2858036.2858273

[27] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada, "Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 2202–2214, https://doi.org/10.1145/3025453.3025926.

[28] J. D. Ndibwile, E. T. Luhanga, D. Fall, D. Miyamoto, and Y. Kadobayashi, "A Comparative Study of Smartphone-User Security Perception and Preference towards Redesigned Security Notifications," in *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, ser. AfriCHI '18. New York, NY, USA: Association for Computing Machinery, 2018, https://doi.org/10.1145/3283458.3283486.

[29] A. Constantinides, A. M. Pietron, M. Belk, C. Fidas, T. Han, and A. Pitsillides, *A Cross-Cultural Perspective for Personalizing Picture Passwords.* New York, NY, USA: Association for Computing Machinery, 2020, p. 43–52, https://doi.org/10.1145/3340631.3394859.

[30] S. Egelman and E. Peer, "The Myth of the Average User: Improving Privacy and Security Systems through Individualization," in *Proceedings of the 2015 New Security Paradigms Workshop*, ser. NSPW '15. New

York, NY, USA: Association for Computing Machinery, 2015, p. 16–28, https://doi.org/10.1145/2841113.2841115.

[31] M. Hull, L. Zhang-Kennedy, K. Baig, and S. Chiasson, “Understanding individual differences: factors affecting secure computer behaviour,” *Behaviour & Information Technology*, vol. 41, no. 15, pp. 3237–3263, 2021, https://doi.org/10.1080/0144929X.2021.1977849.

[32] M. Silverman, “Non-financial recognition,” *The Most Effective of Rewards. Brighton: Institute for Employment Studies*, 2004.

[33] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, “User Perceptions of Smart Home IoT Privacy,” *Proc. ACM Hum.-Comput. Interact.*, vol. 2, no. CSCW, nov 2018, https://doi.org/10.1145/3274469.

[34] J. Li, K. Sun, B. Huff, A. Bierley, Y. Kim, F. Schaub, and K. Fawaz, ““It’s up to the Consumer to be Smart”: Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit,” in *2023 2023 IEEE Symposium on Security and Privacy (SP) (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, may 2023, pp. 380–396, https://doi.org/10.1109/SP46215.2023.00022.

[35] C. Blackwood-Brown, Y. Levy, and J. D’Arcy, “Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective,” *Journal of Computer Information Systems*, vol. 61, no. 3, pp. 195–206, 2021, https://doi.org/10.1080/08874417.2019.1579076.

[36] F. Quayyum, D. S. Cruzes, and L. Jaccheri, “Cybersecurity awareness for children: A systematic literature review,” *International Journal of Child-Computer Interaction*, vol. 30, p. 100343, 2021, https://doi.org/10.1016/j.ijcci.2021.100343.

[37] N. Ahmad, U. A. Mokhtar, W. Fariza Paizi Fauzi, Z. A. Othman, Y. Hakim Yeop, and S. N. Huda Sheikh Abdullah, “Cyber Security Situational Awareness among Parents,” in *Cyber Resilience Conference (CRC)*, 2018, pp. 1–3.

[38] K. Sun, Y. Zou, J. Radesky, C. Brooks, and F. Schaub, “Child Safety in the Smart Home: Parents’ Perceptions, Needs, and Mitigation Strategies,” *Proc. ACM Hum.-Comput. Interact.*, vol. 5, no. CSCW2, oct 2021, https://doi.org/10.1145/3479858.

[39] Hofstede Insights, “Compare Countries,” 2022, accessed 6 March 2023. [Online]. Available: https://www.hofstede-insights.com/product/compare-countries/

[40] E. Zeng, S. Mare, and F. Roesner, “End User Security and Privacy Concerns with Smart Homes,” in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, July 2017, pp. 65–80. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[41] H. Aldawood and G. Skinner, “Challenges of implementing training and awareness programs targeting cyber security social engineering,” in *2019 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 2019, pp. 111–117, https://doi.org/10.1109/CCC.2019.00004.

[42] B. J. Calder and B. M. Staw, “Interaction of intrinsic and extrinsic motivation: Some methodological notes,” *Journal of Personality and Social Psychology*, vol. 31, no. 1, p. 76–80, 1975, https://doi.org/10.1037/h0076167.

[43] Incentive Research Foundation, “Using Behavioral Economics Insights in Incentives, Rewards, and Recognition: The Neuroscience,” 2017, retrieved: October, 2022. [Online]. Available: https://theirf.org/wp-content/uploads/2017/05/final-neuroscience-study.pdf

[44] U. Gneezy, S. Meier, and P. Rey-Biel, “When and why incentives (don’t) work to modify behavior,” *Journal of Economic Perspectives*, vol. 25, no. 4, pp. 191–210, December 2011, https://doi.org/10.1257/jep.25.4.191.

[45] CrowdWorks, “Easy online ordering for any job.” 2019, accessed 6 March 2023. [Online]. Available: https://crowdworks.jp

[46] Prolific, “Quickly find research participants you can trust,” 2022, accessed 6 March 2023. [Online]. Available: https://www.prolific.co

[47] M. Harbach, A. De Luca, N. Malkin, and S. Egelman, “Keep on lockin’ in the free world: A multi-national comparison of smartphone locking,” in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, ser. CHI ’16. New York, NY, USA: Association for Computing Machinery, 2016, p. 4823–4827, https://doi.org/10.1145/2858036.2858273.

[48] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada, “Self-confidence trumps knowledge: A cross-cultural study of security behavior,” in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, ser. CHI ’17. New York, NY, USA: Association for Computing Machinery, 2017, p. 2202–2214, https://doi.org/10.1145/3025453.3025926.

APPENDIX

SURVEY QUESTIONNAIRE

A.1 Demographics

1) (Dem_1) What is your citizenship?
   - Japanese
   - British
   - Other:______
2) (Dem_2) What is your age?
   - 25 - 34
   - 35 - 44
   - 45 - 54
   - 55 - 64
3) (Dem_3) What is your gender?
   - Female
   - Male
   - Non-binary or non-conforming
4) (Dem_4) What is your level of education?
   - Japan
     - Junior high school
     - High school
     - Bachelor’s Degree
     - Master’s Degree
     - Doctorate Degree
     - Other:______
   - UK
     - GCSE / National 5 (O-level)
     - A-level / Higher / Advanced Higher
     - Bachelor’s Degree
     - Master’s Degree
     - Doctorate Degree
     - Other:______
5) (Dem_5) What is your current employment status?
   - Employed full-time
   - Employed part-time
   - Home duties (Full-time stay-at-home)
   - Retired
   - Self-employed
   - Student
   - Unable to work
   - Unemployed looking for work
   - Unemployed not looking for work
6) (Dem_6) How many members of your household are under the age of 18?
7) (Dem_7) How many members of your household are of age 65 years and above?

A.2 Knowledge about Smart Homes

A smart home is a house equipped with many internet-of-things (IoT) devices (e.g., smart bulbs, smart TVs, smart speakers, smart kitchen appliances, smart locks, smart IP cameras, and smart cars) that automate tasks normally handled by humans and are typically remotely controlled.

8) (KSH_1) How many IoT devices do you own?
   - None

- 1-4
- 5-10
- 11-15
- 16-20
- 21-25
- 26-30
- More than 30

9) (KSH_2) Please select all the types of IoT devices used in your house.
   - Smart bulbs
   - Smart cars
   - Smart displays (e.g., Google Nest Hub)
   - Smart fridges
   - Smart garage door openers
   - Smart hubs (smart-home hubs)
   - Smart IP cameras
   - Smart locks
   - Smart meters
   - Smart ovens
   - Smart plugs
   - Smart speakers
   - Smart thermostats
   - Smart TVs
   - Smart vacuum cleaners
   - Other:______

A.3 Smart-Home Security

A smart home is a convenient technology because it improves the quality of life at home. However, smart-home devices are not designed with security as a priority, and they collect and share private information targeted by cyber attackers. For instance, according to a recent experiment, smart homes could be exposed to more than 12,000 cyberattacks in a single week.

10) (SHS_1) Have you ever taken any formal cybersecurity awareness training, or have you worked or studied in the cybersecurity field? Please select "Yes" if any of these instances apply.
    - No
    - Yes

11) (SHS_2) Which of the following cyberattacks are you aware of?
    - Data and Identity theft
      Data generated by unprotected wearables and smart appliances provide cyberattackers with an ample amount of targeted personal information that can potentially be exploited for fraudulent transactions and identity theft.
    - Device hijacking
      The attacker hijacks and effectively assumes control of a device. It only takes one device to potentially gain access to an entire network and infect all IoT devices in the home.
    - Distributed Denial-of-Service (DDoS)
      A denial-of-service attack (DoS attack) attempts to render a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. In the case of a distributed DoS (DDoS), the incoming traffic flooding a target originates from multiple sources.
    - Man-in-the-Middle (MITM)
      An attacker breaches, interrupts, or spoofs communications between two systems. For example, an attacker can disable vulnerable HVAC systems during a heat wave, creating a disastrous scenario for service providers with affected models.
    - Permanent Denial of Service (PDoS)
      PDoS, also known as phlashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware. For example, the attackers can feed fake data to thermostats in an attempt to cause irreparable damage via extreme overheating.
    - Social engineering
      The attackers manipulate or trick people into divulging confidential information, transferring money, or downloading malware using social interactions (e.g., phone talking, email, social media).
    - Other:______
    - None / Not applicable

12) (SHS_3) How secure or insecure do you think your smart home is?
    - Very insecure
    - Insecure
    - I don't know / Unsure
    - Secure
    - Very secure

A.4 Cybersecurity Awareness Training

Cybersecurity awareness training may help households to prevent and protect their smart homes from cyberattacks.

13) (CAT_1) Do you agree or disagree that you need cybersecurity awareness training to learn how to secure effectively your smart home?
    - Strongly disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly agree

14) (CAT_2) Are you willing to spend **money** on cybersecurity awareness training every year in a personal capacity to protect your smart home?
    - No
    - Yes

15) (CAT_3) Are you willing to spend **time** on cybersecurity awareness training every year in a personal capacity to protect your smart home?
    - No
    - Yes

16) (CAT_4) Do you agree or disagree that children need cybersecurity awareness training?
    - Strongly disagree
    - Disagree

- Neutral
- Agree
- Strongly agree

17) (CAT_5) Do you agree or disagree that senior citizens need cybersecurity awareness training?
    - Strongly disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly agree

A.5 Non-Financial Rewards for Pro-Cybersecurity Behavior

We aim to provide non-financial rewards in smart homes to encourage users to adopt good cybersecurity behavior.

18) (NFR_1) How satisfied or dissatisfied would you be with receiving non-financial rewards to encourage you to practice good cybersecurity hygiene at home?
    - Very dissatisfied
    - Dissatisfied
    - I don't know / Unsure
    - Satisfied
    - Very satisfied
19) (NFR_2) Would you be interested in competing with other smart-home users to get the award of the "CERTIFICATE OF ACHIEVEMENT FOR GOOD CYBERSECURITY BEHAVIOR AT HOME"?
    - Not at all
    - Slightly
    - Moderately
    - Very
    - Extremely
20) (NFR_3) Would you be interested in having virtual reality (VR) services in your smart home as a reward? For instance, virtual aquarium tour, virtual beach tour, virtual city tour, virtual mountain climbing tour, virtual museum tour, virtual space station tour, virtual zoo tour
    - Not at all
    - Slightly
    - Moderately
    - Very
    - Extremely
21) (NFR_4) What non-financial reward would you like to get when behaving securely in your smart home?
    - Getting awards
    - Playing online games
    - Getting virtual point rewards
    - Getting access to virtual reality (VR) services
    - Getting cyber insurance discounts for households
    - Getting badges
    - Other:______
    - None of the above