TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Shiori Yamazaki 184084IVSB

# A Training Module of Social Engineering For Japanese Non-Technical Users

Bachelor's thesis

Supervisor: Kaido Kikkas, PhD

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Shiori Yamazaki 184084IVSB

# SOTSIAALMANIPULATSIOONI ÕPPEMOODUL JAAPANI TAVAKASUTAJATELE

bakalaureusetöö

Juhendaja: Kaido Kikkas,
tehnikateaduste doktor

Tallinn 2021

# Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Shiori Yamazaki

# Abstract

Japan has one of the largest numbers of Internet users in the world, and accordingly, the number of cyber-attacks has been increasing in recent decades. Research has shown that the Japanese with free access to the Internet, however, are not always provided with sufficient education against preventable cyber-attacks such as phishing. In short, ordinary Internet users in Japan are often not aware of good security practices, nor implementing security measures against attacks. This attitude has helped increase the number of successful cyber-attacks targeting Japanese non-technical Internet users.

The main objective of this study is to raise awareness of cybersecurity and prevent social engineering attacks by providing adequate training to Japanese non-technical Internet users. This study also focuses on the factors contributing to the vulnerability of the Japanese from both technical and cultural aspects. The analysis of the pre-survey confirmed that most of the respondents were concerned about security and did not take appropriate security measures. In addition, more than 90% were not given opportunities to participate in security training in the past, and many of them showed interest in security training if it is 1. free 2. short 3. online. The training prototype used in this study reflected the user feedback from the survey to satisfy their needs. As a result, 100% of the participants had a positive effect on their awareness and knowledge after the training. The paper includes the improvements in training efficiency analysed from the participants' feedback and such results can be referred for later implementation of a large scope.

This thesis is written in English and is 47 pages long, including 7 chapters, 10 figures and 10 tables.

# Annotatsioon

Jaapan on üks suurima internetikasutajate arvuga riike maailmas ning viimastel aastakümnetel on küberrünnakute arv pidevalt kasvanud. Nagu uuringud näitavad, ei ole jaapanlaste puhul vaba ligipääsuga Internetti alati kaasnenud piisav koolitus kalastusrünnete ja muude, tegelikult välditavate küberohtude vastu. Üldjuhul ei ole Jaapani tavakasutajad sageli teadlikud headest turvatavadest ega kasuta rünnete vältimiseks kaitsemeetmeid. Selline suhtumine suurendab tõenäosust nende langemiseks sotsiaalmanipulatsiooni ohvriks.

Käesoleva uurimistöö peaeesmärgiks on pakkuda välja piisava mahuga turvakoolitus harilikele Jaapani internetikasutajatele, vältimaks manipulatsioonründeid. Siin uuritakse erinevaid tehnilisi ja kultuurilisi aspekte, mis muudavad jaapanlased haavatavateks, lisaks pakutakse välja ka veebipõhise turvakoolituse prototüüp ning analüüsitakse erinevaid tõhusa väljaõppe viise. Prototüüpi ja kasutajate tagasisidet sellele on kavas edaspidi kasutada koolituse läbiviimiseks juba suuremate organisatsioonide kontekstis.

Küsitlused Jaapani internetikasutajate seas viidi läbi veebipõhiselt. Esimese küsitluse tulemused näitasid, et enamik vastanutest ei kasutanud piisavaid turvameetmeid, ent olid samas ohtudest teadlikud ja olid huvitatud lisakoolitusest. Koolituse prototüübi koostamisel lähtuti kasutajate tagasisidest - näiteks uuriti, milliseid lünki avastati senises teadmistepagasis ning mida soovitakse tulevikus veel juurde õppida.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 47 leheküljel, 7 peatükki, 10 joonist, 10 tabelit.

# List of abbreviations and terms

| | |
|---|---|
| 2FA | Two-Factor Authentication |
| AR | Augmented Reality |
| CERT | Computer Emergency Response Teams |
| EU | European Union |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| IPA | Information-technology Promotion Agency |
| ISP | Internet service provider |
| IT | Information technology |
| JAIST | Japan Advanced Institute of Science and Technology |
| METI | Ministry of Economy, Trade and Industry |
| MEXT | Ministry of Education, Culture, Sports, Science and Technology |
| MIC | Ministry of Internal Affairs and Communications |
| MPD | Metropolitan Police Department |
| NGO | Non-governmental organizations |
| NIER | National Institute for Educational Policy Research |
| NISC | National center of Incident readiness and Strategy for Cybersecurity |
| PC | Personal Computer |
| USA | The United States of America |

# Table of contents

# List of figures

# List of Tables

# 1 Introduction

Digital safety has become one of the most essential concepts to know in the digital era. It is no longer enclosed between the security professionals or IT workers, but also to be shared among the normal users as the world has seen a dramatic rise in the number of Internet users and cyber-crimes concurrently. Japan is no exception.

Despite the drastic rise, the general public has been ignorant of such topics. Insufficient security knowledge leads to more cyber-crimes as security education was never prioritized in public institutions such as schools or companies. Education opportunities must be at every user's reach to reduce the number of preventable cyber-attacks and improve their digital literacy.

This thesis aims to solve the problem of insufficient security education by providing an online training module. As a first step, the current situation is carefully analysed from the statistics, surveys, and interviews in order to understand the users' struggles and challenges. The training module consists of common cyber-attacks in Japan and educates participants on how to protect themselves from attacks. The prototype of the training module (Chapter 5) is in Japanese and held completely online.

After collecting the feedback from the course participants, this study suggests the ideal method of security education to help Japanese non-technical Internet users understand better of cybersecurity so that they can take security measures to protect themselves. Future work must be done to educate a larger group of people in schools, universities, and companies. Its implementation can be supported by the analysis and prototype in this thesis.

# 2 Background

## 2.1 IT security in Japan

Japanese people are immersed in internet-based activities. The statistics by MIC [1] reveals that Internet usage was 89.8% in 2019. The working population aged between 20 and 60 had nearly 100% of Internet usage. There was a big gap between generations, however, the year 2019 witnessed a significant increase in the number of those aged above 80 from 21.5% to 57.5%, which calculates that the majority uses the Internet regularly regardless of their age. The smartphone was more frequently used as much as 63.3% of the population whereas PC was 50.4% The most common purpose among all age groups was sending and receiving emails. By contrast, the young and the elderly showed different levels of interest in using video posting, sharing sites, and using online games. The results also emphasised that as many as 75% of the respondents were concerned about their Internet usage, which breaks down into information breach (88.4%), computer virus infections (62.6%), and online fraud (51.9%). And almost 70% of households have implemented some security measures such as updating software (57.2%), installing anti-virus software (55.9%), setting a password on the device (49.6%).

Accordingly, the number of cybercrimes shows a rising trend. The insight report of Norton in 2019 [2] recorded that 23% of Japanese people in the past year experienced cybercrimes, 5 million of whom became victims of data breach, doubling the previous year's score. This rise made 42% of the Japanese who have experienced any cybercrimes in the past. The most worrying subject regarding data privacy was data breach, followed by misuse of data by a third party. At the same time, the Japanese were most pessimistic about their capacity; a large proportion of the people think that it is too late to protect or control their privacy. With such a negative view, the ratio of Japanese people who are actively looking for a solution to protect their data and privacy remained only 48% while the average of the other countries was 66.3%. A similar pattern was found in the response to the question of not knowing how to protect their privacy; Japan 66%; the rest 55%. Furthermore, despite a low score in the government trust, the majority think that data protection and data privacy must be secured by the government, not by an individual. The

results concluded that the Japanese are most reluctant to their own security among the 10 participating countries; they do feel insecure but are not actively looking for security measures to take.

METI [3] reported that human resources in the field of cybersecurity play an important role in the IT industry. Japan, however, is facing a problem that the shortage in the workforce is estimated to grow up to 193,000. They also claim that the country needs levelling up in the general knowledge in IT; this tendency presumably derives from low level of satisfaction with job training and low active learning by employees. The research on security education in school by NIER [4] points out the challenges at each stage of school education. They have concluded that education on information ethics is never sufficient at all stages and there is a gap in students' information literacy when they graduate from junior high school because only a few of the IT-related subject are taught in their curriculum. In order to avoid various harms on the internet, the need for security education was proposed for a variety of stakeholders, including teachers, students, parents and communities.

Additionally, IPA [5] described the top 10 security threats of 2021 elected by security specialists. For individuals, the rankings were the following:

1. unauthorized use of mobile payment
2. data breach by phishing
3. online defamation and slander
4. threatening and fraudulent requests for money via emails and social media
5. mishandling of credit card information
6. unauthorized use of internet banking
7. data breach by online services
8. fake web alerts
9. harmful mobile applications
10. unauthorized logins to online services

Most of the threats in the ranking are preventable with enough caution, except when the system or application has unintended vulnerabilities.

## 2.2 Similar initiatives in other countries

While many countries have struggled with a growing threat of cyber-attacks, USA has always been taking lead in this domain since the late 1990s and the world's first national level security training was launched in 2003. Almost simultaneously, EU has been discussing the need to improve national information security literacy and ENISA was established in 2004. [6] Their initiatives continued to grow and there are several laws in effect in the listed countries. In USA, HIPAA, enacted in 1996, has enforced all health care providers and their business associates to take security awareness training who have access to health data. [7] Similarly, EU has made an impactful strategy to reach young people with various actions and campaigns. [8] And such methods have been allegedly effective in educating a larger group of people.

On the other hand, many people in developing countries are suffering from inequality of education. The study [9] claims that women in South Africa, who are generally less educated than men, are more vulnerable to cyber-attacks and only those who received proper IT education are aware of risks and preventions of cyber-attacks. And in order to educate people across the country, it is essential to provide education to everyone from an early age, i.e., elementary school.

## 2.3 Related work

Despite the need for individually distributed education, little has been studied in this domain. Alaul [10] emphasized the need for security awareness training among normal users. The non-technical are, in many cases, neglected or thought lightly of compared to the efforts which companies put into security professionals; as a result, lack of education has allowed cybercriminals to take advantage of the human vulnerabilities of ordinary users. The key factors suggested in their study are that many entities must be involved to educate ordinary users: governments, CERT, police departments, enterprises, ISPs, media, users, NGOs, schools, universities. Each of them has their own roles and responsibilities to keep up to date with security. Beuran et al [11] focused on training for cybersecurity personnel. The contributions of the thesis are the analysis of the current major cyber

training programmes in Japan, current best practices and methodologies for cybersecurity training, requirements for effective training, and so on. They suggested that effective security training must 1. be appropriate for the knowledge level of the target audience 2. be in accordance with the skills as the program aims to develop 3. include hands-on activities 4. reach audience large audience 5. be cost-effective and sustainable. They also proposed that cybersecurity education must be provided to not only IT or security-related professions but also ordinary people, who make up the vast majority of Internet users. Continuously, Tan et al [12] suggested an adaptive method for security awareness training with stress that almost 95% of cybersecurity attacks come from human error. Their study provided adaptive online training of the proper level to an individual learner with fewer constraints of time and place as the content is generated by the algorithm. They concluded that such adaptive training worked effectively to educate participants in the domain of cybersecurity.

For general e-learning, several features have been suggested in previous studies. Yukawa et al [13] found that implementing a sense of connectedness or seeing other participants' progress increases the motivation of learners. The other research by Kogo [14] has studied online learning for adults, and there are often barriers in the current style of education, which are high tuition cost, small spare time, and low matching to the need. These can be often solved by online training, however, the knowledge in andragogy is not shared in Japan's education; the training must apply their characteristics of adults; they are often goal-oriented and focused on practical skills; they have rich and diverse life experiences; they can make their decisions on learning in contrast to mandated school education. Nevertheless, they expect that the needs for online learning expand more in the foreseeable future for its flexibility as long as their motives are kept high.

It must be acknowledged that many training programmes are available online with fees, most of which target employees from an enterprise. Being a competitive market, the variation of the training contents and styles are, without a doubt, beneficial to users. However, only a few programmes are offered fully in Japanese, and the Japanese users are still isolated from proper security awareness training.

## 2.4 Current challenges

Although the importance of security education has been discussed in the previous studies, Japan has multiple blocking factors on implementation. Firstly, Japan is experiencing a lack of a cybersecurity workforce, which makes it hard to find skilled educators in the field. As the situation is expected to be worsened in the coming years, it is irrefutable that on-site training programmes for all users are not viable. Secondly, language barriers are commonly found in the Japanese society. For instance, the majority do not have the ability to reach online resources in a foreign language. Although education promotion plan by MEXT [15] targeted A2 level of English for more than 50% of high school students at graduation, the end-result report showed that only 40.2% reached A2 level, half of whom achieved more than A2 level. Since it is said that at least B2 level is needed to attend lectures in a target language, most people are limited to the Japanese language when choosing learning materials. And the last resort of machine translation is still far from being useful due to the inaccuracy caused by the complex structure of the language. Another language issue that must be addressed is the complexity of the Japanese writing system. Written Japanese consists of three components: *hiragana*, *katakana*, *kanji*. *Kana*, a combination of *hiragana* and *katakana* represent phonological units of Japanese writing, each contains 46 base letters. All *kana* letters are taught to first-year students in elementary school. *Kanji*, on the other hand, are logographic characters, most of which are adopted from Chinese characters. This component contains thousands of characters and 2,136 of them are considered *jōyō kanji*, or the guideline for daily used *kanji* on official documents by MEXT. According to school guidelines, students learn the *jōyō kanji* from 1st grade to 12th grade. With such a long period of learning, unlearnt kanji may limit young Internet users' understandings on the Internet. (Table 1) The language complexity expands not only in the writing system but also in grammatical expressions including honorifics. However, being one of the most difficult languages to learn as a foreign language creates high resistance to online scams from overseas as it is often easy to spot phishing text written by a non-native speaker.

Table 1. Example of Japanese young Internet users' understanding

| | |
|---|---|
| Original text | 外部から不正ログインが検知されました。直ちにパスワードを変更してください。 |

| | |
|---|---|
| Translated Text | An unauthorized login has been detected from outside. Please change your password immediately. |
| Original text to 2nd graders' understanding | [Unknown] から [Unknown] ログインが [Unknown] されました。<br>[Unknown]ちにパスワードを[Unknown]してください。 |
| Translated text to 2nd graders' understanding | An [Unknown] login has been [Unknown] from [Unknown]. Please [Unknown] your password [Unknown]. |

All in all, cybersecurity education is in high demand. The solution suggested in this thesis is to provide an online training module for free. By this means, the constraints of time, place, and cost found in the current training modules can be nullified, and such training can be developed at once with regular maintenance. And the training content should be enhanced with hands-on activities as suggested. Therefore, this method satisfies the requirements to tackle the challenges pointed out in previous studies. This study later implements a prototype of the training module, which is provided to prospective users. The expected outcome is to become the foundation of future cyber education in Japan, by taking multiple factors such as cultures and attitudes. .

# 3 Methodology

Most of the previous studies in security awareness training are usually aimed at the design of the training or the development of the training. As this thesis aims to cover both sides, the method is a combination of previous studies in aspects of training design and development. For training design, this research employed conventional qualitative and quantitative methods to sample user data, and Google Forms has been chosen as a platform to distribute the questionnaire on various social media sites so as to reach a larger scope of the Japan's community. This approach is often used in research for a general view of the situation. The development of the training follows an ordinary modern web application since web applications are already accepted by many non-technical users. Considering that the development of the study is scoped to a prototype, the final outcome must be determined with feedback after the training.

To make the suggested solution effective, the implementation process of the training prototype involves four steps:

1. Analyse the current situation with collected data
2. Design an online training module according to users' need
3. Develop the training
4. Seek for improvements from user feedback

The first survey or pre-survey was conducted via Google Forms from 8th to 12th of March in 2021. The aim was to understand the current situation to make the training more meaningful for the future targets. The survey consisted of two sections: the general Internet usage and knowledge, and security concerns and measurements. Both included multiple-choice questions, free-text questions, linear questions measured on a 5-point Likert scale. (Appendix 2 – Pre-survey) Conclusively, 80 anonymous responses were included in the later analysis in Chapter 4.3. Due to the short time frame, the development of the training focused the most on the delivery time while considering the required features. After the training was given to the test subjects, the second survey or post-survey

was conducted via Google Forms from 29th of March to 2nd of April in 2021. The main goal was to reflect on feedback in future work. Primarily, the participants were asked to share comments on changes in their security awareness before and after the course as well as the course content itself. This survey included similar measurements to the first survey such as Likert scale questions, and more free-text style questions were used to collect individual-specific answers. (Appendix 3 – Post-survey) The collected feedback from 9 course participants who completed the training are analysed to make the course more effective and suggested steps are concluded in Chapter 6.

# 4 Analysis of the current situation

## 4.1 Case study

Cybercrimes are allegedly common in Japan. This section provides three real-life examples to have a closer look into what is happening in the Japanese society. On collecting data, a 1:1 interview was conducted for 10-30 minutes. And each interviewee was asked their technical background including how long they were using the Internet, their context regarding the use of the Internet, what happened, how they found out the crimes, and what actions they took after the discovery. After reviewing each case, analysis is made for the causes and preventions.

### 4.1.1 Case A

The victim was an 8-year-old elementary school girl. She recently started using the Internet although she could not read most of the text as it was written in *kanji*. In the given context, reading everything online was difficult for her without the help of a dictionary but she kept using it by guessing how to read or what an unknown word meant. She spent many hours playing an online computer game where users interact with others. Playing the computer game was free for anyone but the system also allowed users to pay for rare items. She did not have money to buy these items for herself, but she wanted to play it better with paid rare items. One day, she found a blog article that said that she could get a reward for the in-game currency worth 10,000 yen ($100). She immediately clicked the link in the article and visited the website. It was exactly what she wanted so that she could buy herself rare items without paying money. The website had a simple form asking username and password in return for the 10,000-yen ($100) reward. She did not read full text nor think deeply but only believed that this claim was real, and she could buy rare items without paying money. Right after she typed her credentials, she found out that she could no longer log in to her account. Then she realised that her account was stolen, and the next day she decided to go to the police station. She was very eager to get her account back for game data. It was not too difficult for the police to track the traffic since this criminal was only an amateur. One month later, the police announced that the phishing

website was managed by a 17-year-old high school girl and her account was happily back again after learning an important lesson.

There are multiple factors that encouraged this crime. The main factor was that she was too young and innocent to understand the existence of phishing or general fraud. Her digital illiteracy greatly caused her to fall into such fraud by telling her password to a third person. Her parents could have helped the situation by restricting services or the school could have taught her how to correctly handle credentials on the Internet. This crime could have been stopped from happening by keeping the credentials to herself. It could be referred that the lack of knowledge in *kanji* lowered her understandings of the content. As she was used to guessing everything, she never learnt to read with caution. Such deficiency could have been solved with a dictionary.

### 4.1.2 Case B

The victim was an ordinary 20-year-old university student. She used social media frequently and did online shopping occasionally. One day, she logged in to her Amazon account from her brother's smartphone. Several days after, she received an SMS from 'Amazon' that her activities violated their policy. It just came to her mind that logging into Amazon from someone else's device was an illegal action to take so she clicked the link and visited 'Amazon'. She followed instructions on the screen to re-enter account credentials and her credit card details. Later, she became sceptical about it and called her mother because the credit card was her mother's. Her mother checked the details and they found out that her credit card reached the limit of 800,000 yen ($ 8,000) within half an hour from the phishing. Several home appliances were bought with her money until the limit, and they could not cancel the purchase even after calling the card company to stop the transactions.

This case had a rather large amount of money loss and was not compensated by anyone. She was surely a victim of phishing, but she violated the rules of not telling credentials to any third party. What could have saved her was to disable the card before it was used. However, it took a while to confirm activities and all the transactions were made in such a short period of time. She wished to know how to detect phishing websites or navigate herself to authentic websites, in this case, Amazon.

### 4.1.3 Case C

The victim was a 52-year-old owner of a car dealership. He was using the Internet for more than 20 years but never got deep into it. If he ever needed to fix a computer, he would call a computer repair technician. His main use of the Internet was to browse websites and play online game on his smartphone. He was a big fan of Pokémon GO, an AR mobile game application first published in 2016 by Niantic. Since it is a globally popular mobile application, it has such a feature that friending someone from overseas will bring benefits. Once he visited an online forum in English to find international Pokémon GO friends, he clicked a link to see detailed information. It redirected him to log in to 'Google' and asked for authentication. He was a little sceptical because the page was in English and did not know why it required him to authenticate this way. A few days later, he noticed that an unknown person was added to his friend list on the application, so immediately removed the suspicious friend. At the same time, he started noticing a weird trace of somebody else logging in to his Facebook from a different geographical location in his login history. He checked Facebook settings and removed any suspicious linking to other services. He quickly asked for help from somebody with technical and security knowledge. The expert gave him advice that he should change the password and turn on 2FA. After these taking effect, no suspicious events were detected.

It was originally a phishing website to illegally gain Google account credentials. However, this leakage had a larger effect on multiple services because he was linking his Google account credentials with Facebook and Pokémon GO, which allowed the attacker to use any of these. When this event took place, 2FA was not turned on. Such authentication could have prevented all these logins by a third person.

## 4.2 User attitudes and knowledge

From 80 responses on the pre-survey, it is a positively skewed distribution when it comes to the confidence level in their knowledge in IT. (Figure 1) It is abundantly clear that many people have concerns about cyber-attacks from the weak negative skew. (Figure 2) And those who have taken security training only remained 7.5% of the respondents, and 3.8% have been victimised of cyber-attacks. The majority, namely 77.5% of the respondents, confirmed that they do not have enough knowledge in security nor take

security measures at their best (Figure 3) while the points of interests in security training remained 41.3%. (Figure 4)

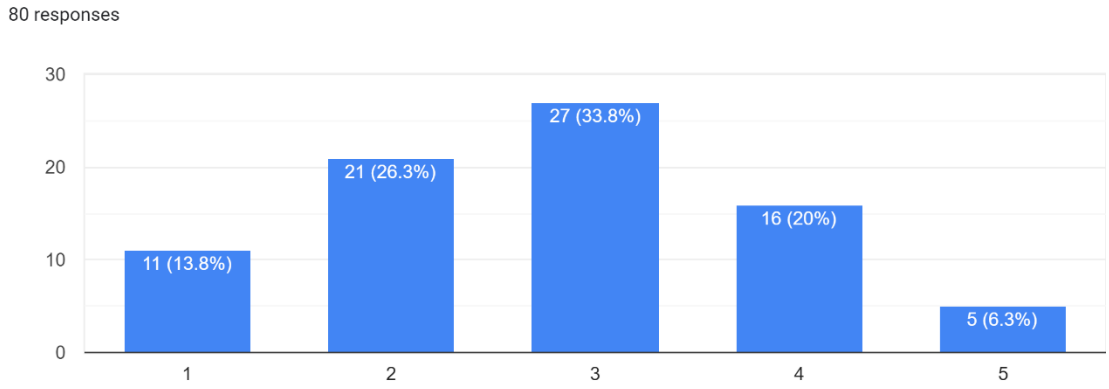


Figure 1. Question "I have knowledge in computers and the Internet"

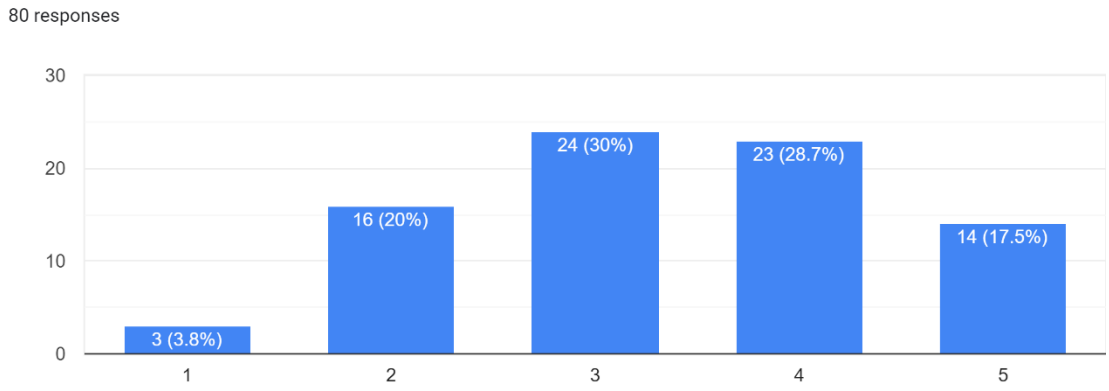


Figure 2. Question "I have concerns about cyber-attacks"

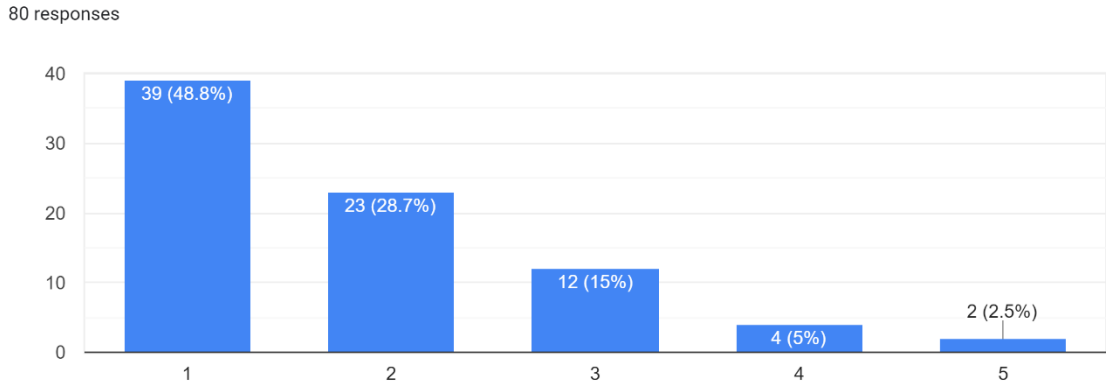


Figure 3. Question "I have knowledge in social engineering and am always taking best security measures"

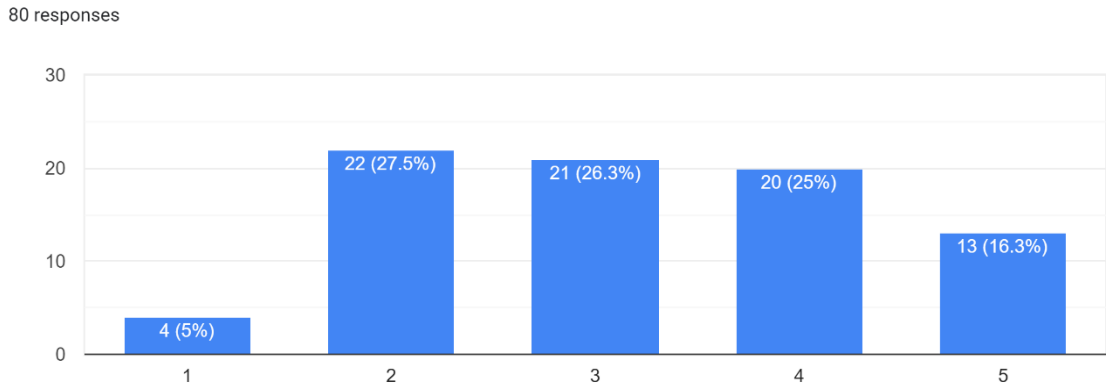


Figure 4. Question "I am interested in security training"

With these figures combined, an interesting relation was found. Those who have participated in training showed 2.83 points in concerns about security in contrast to 3.41 points by people who have not. Similarly, the training participants had nearly double the score of 3.33 in their security measures of the others being 1.72. This concludes that security training contributes a rise to security measures and thus relieves their concerns about security. People who are confident in IT knowledge showed more interests in taking training with a score of 3.7 while the others with 2.8. They are slightly less concerned about security as they take more measures, however, the difference between the two groups is relatively small, and the best influence comes from training.

Table 2. Analysis of security by groups

| **Group** | **Concerns about security** | **Security measures** | **Interests in security training** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Those who have participated in training | 2.83 | 3.33 | 3.20 |
| Those who have not participated in training | 3.41 | 1.72 | 3.17 |
| Those who are confident in IT knowledge | 3.28 | 2.52 | 3.67 |
| Those who are not confident in IT knowledge | 3.10 | 1.44 | 2.78 |

## 4.3 Training design

There has been guidance for developers or administrators, but there has been little research from a participant's point of view. The report [11] has suggested that training must satisfy the requirements for cyber training; the content level is appropriate for the target audience; the training includes hands-on activities; The training scopes as large audience as possible; The training has good cost-performance characteristics. The research [13] stresses the importance of the feel of connection with other participants.

As this study conducted the pre-survey, its results have helped understand prospective users' needs. For a style of the training, online training is the most popular answer with 82.5%, where off-line training received 26.3%. A few suggested text-based learning such as books. This relates to the majority preferring 'no constraints on time (62.5%)', 'no constraints on place (55.0%)', and 'self-paced learning (40.0%)', showing that learning has become an individual activity than a conventional group activity. The tuition fee is often a big part of the consideration. 46.2% of the respondents would take part in the training only for free of charge, resulting in only one out of four would take the training for more than 1,000 yen ($10). Another question on the length of the lecture tells that 68.8% of the users would take the course only if it is less than one hour, and only 6.2 % want to be in training that lasts more than 5 hours. From the results, the majority has the intention of taking training only when the training is 1. online 2. free 3. short. Positive votes on requested features are listed in the table below.

Table 3. Requested features

| **Features** | **Positive votes (max. 100%)** |
|---|---|
| Join with friends | 40.0% |
| Share on social media | 23.8% |
| Take quizzes or tests | 40.0% |
| Receive certificate | 28.7% |
| Communicate with other participants in real time | 40.0% |
| Communicate with teachers in real time | 20.0% |

# 5 Development of the training

## 5.1 Content

The subjects have been chosen regarding the common cyber-attacks in Japan, found in Information Security: Top 10 threats in 2021 by IPA [5]. Thus, preventable cyber-attacks can be broadly categorized into online fraud, account security and device security. On creating the content, the training aims to provide the causes and preventions suggested by NISC. [16] Additionally, the content includes practical examples of a real-life situation and background information such as vulnerabilities to improve users' understandings.

### 5.1.1 Online Fraud

Phishing is one of the most common attacks in Japan, ranked as second in the top 10 threats in 2021 while half of the threats also fall into the category of fraud. Despite the preventable nature, the number of phishing attacks has been continuously increasing.

This chapter is divided into 3 sections. The first section describes the common methods used in social engineering, or how to manipulate people so that users understand the main techniques of online fraud. It explains the techniques like name-drop, hurry-up, give-and-take, and friendship with live examples and reasons why people fall into such fraud.

The second section teaches how to detect and avoid fake websites by looking at SSL certificate and bookmarking the official pages. In the end, the test shows how difficult it is to see the difference between 'I' (capital I), 'l' (small L), '1' (number one) in the browser header and draws attention to the importance of bookmarking or simply not redirecting to another page without a second thought.

### 5.1.2 Account Security

Account security has been called out for securing user accounts, yet it is still the case that people use the same password for multiple websites or use insecurely short and simple passwords.

This chapter is divided into 3 sections. The first section describes what kind of attacks are often made to crack passwords. There are many methods revealed today but as the target is non-technical, it lists brute force attack, dictionary attack, and account list attack. It also suggests checking whether their account has been leaked before and changing passwords if leaked.

The second section teaches the requirements for a secure password, and the risks of repeated password, social login method, and honestly answered security question. It also brings a discussion on whether to change passwords regularly from a modern point of view. After learning securing password, this section also covers how to store or manage passwords securely. Solutions follow the best practices suggested by NISC and raise awareness of potential danger with sticky notes around PC monitor and browser saved passwords.

The third section discusses the need for securing the authentication method. The conventional method of entering username and password has been revealed weak and explains why multi-factor authentication is needed for logins or any financial activities.

### 5.1.3 Device Security

Many users are still optimistic about device security as this subject has been often discussed only inside IT personnel, and it seems too complex for non-technical users. However, device security is one of the most important components to protect users from attacks as NISC suggests in their handbook. [16]

This chapter is divided into 3 sections. The first section reminds users of physical security on their devices. A screen lock with the shortest period is needed for every device to minimise the risk of unexpected intrusion. This section also mentions the possible events of stolen or lost device and what users could prepare for such incidents. In any case, encryption is suggested to nullify the damage in the event the device is in the attacker's hand.

The second section talks about application security. Participants can learn how to find trusted resources and limit the installation of suspicious or unknown applications from the Internet. Similarly, it brings the idea of authorization and permission what applications should be using and how to check these from smartphones.

The third section is focused on network security. It explains the difference between HTTP and HTTPS and confirms the importance of encryption. Along with the overview of the SSL certificate, it introduces the EV-SSL certificate to verify who is running the website, which can be used to detect phishing websites in subchapter 5.1.1. After learning encryption, it teaches how to use Wi-Fi securely from both user and administrator's perspectives. Participants learn what kind of risks lie on public free Wi-Fi. This section also mentions Bluetooth security and usage of VPN.

## 5.2 Application Prototype

In the limited time frame, the prototype is a client-only web application. The chosen technologies and services are as follows:

- React [17]
- TypeScript [18]
- Ant Design [19]
- Netlify [20]

The frontend development of the application is built with React in TypeScript. React is the most popular JavaScript library for the frontend development maintained by Facebook. This library is chosen for its popularity so that it is easy to find resources on the Internet. The programming language used in this application is TypeScript, developed and maintained by Microsoft. TypeScript adds optional static typing to JavaScript, making the programme easy to read and debug. The application relies heavily on Ant Design for its simplicity and consistency in design. The UI looks clean and instinctive thanks to the components provided by Ant Design. The app is hosted in Netlify because their service allows developers to make CI/CD and deploy for free. The prototype of the training module can be found at https://cytrain.netlify.app.

The application contains four pages: 1. Welcome page 2. Lecture page 3. Test page 4. About page. Welcome page shows an overview of the application to draw users' attention and users can take courses under Lecture page. The lectures are semantically divided into three chapters as described in Chapter 5.1. After finishing the lectures, users can take tests.

The tests focus on practical problems in a real-life situation rather than theoretical as the training aims to provide hands-on practice. Many of the questions simulate a specific case where users must determine what actions to take. After all the questions are marked, users can check the correct answer(s) with a description so that they can see the reasoning behind each action. The questions are set with tags of relevant chapters. With the tags, users can always go back to the lecture page and review a particular area in which they are not confident. About page introduces the purpose of the training, the references used in creating the content and the details of the development.

From the analysis discussed in chapter 4, special features are added to the training, which includes 'progress bar', 'quiz', and 'SNS share button'. And the design follows Mobile First Design as prospective users are expected to visit the website on their smartphones. The demonstration and its translation can be found in Appendix 4 – Demonstration of the training and Appendix 5 – Translation of the Training Content respectively.

## 5.3 Feedback

The post-survey collected initially 13 responses, 4 of which were detected as spam due to the same value chosen for all questions along with the same senseless word in all fields. They have been removed from the analysis in order to reflect only genuine opinions. The questions on the training content revealed that the difficulty level was slightly too high for the majority 55.6%, while the amount of the content was evaluated as adequate. The contributions of the training were highly appreciated; everyone showed positive feedback on their awareness and knowledge after the training, resulting that 7 out of 9 participants would recommend this training to others. Comments were processed into sentiment analysis provided by MonkeyLearn [21] and the results (Table 4) turned out both positive and negative. The variety of the feedback to the same matter must be addressed as this indicates the scope of the audience was not set appropriate by their knowledge level. A definite improvement shall be adding more visual contents.

Table 4. Sentiment analysis of the feedback

| **Comments (Translated)** | **Classification** | **Confidence** |
|---|---|---|

| | | |
|---|---|---|
| I felt like there was too much text, and the content was too difficult for non-academic people. It'd be better if more videos were there. | Positive | 0.643 |
| The content was very informative, and since my password was leaked before, the topic was relevant to me. The amount of content was so much that I couldn't learn all at once. | Positive | 0.858 |
| It was a bit too difficult for non-technical people. | Negative | 0.65 |
| The lecture was well-organized and easy to understand in spite of the complex subject. I felt familiar with cybersecurity. I liked how the illustrations and diagrams were effectively inserted. | Positive | 0.998 |
| It would be easier to understand if I could see the intensity of the risk. | Negative | 0.6 |
| It was smooth to read. I think this service is friendly to beginners thanks to the images and citations. | Positive | 0.996 |

It is worth mentioning that the pre-survey and post-survey was given in the same period, each conducted from 8th to 12th of March and from 29th of March to 2nd of April. Twitter was one of the platforms where this survey was spread along with Instagram and Facebook. The tweets were similarly written, except for the expected time: 5 minutes and 30 minutes respectively. Despite the higher impression on the post-survey, the number of link clicks were still lower, collecting only 9 responses after 41 clicks. (Table 5) The possible indication is 1. many who saw the tweet were not interested in using their free time of 30 minutes 2. the first impression of the training was not appealing enough. However, the end of March and the beginning of April is admittedly one of the busiest times of the year, as April is the first month of school and company year in Japan; some move to a new place; some prepare for a new school or company. This cultural influence might have contributed to the low number of responses.

Table 5. Comparison of tweet activities

| **Survey** | **Impressions** | **Total engagements** | **Link clicks** | **Retweets** |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Pre-survey | 2041 | 234 | 56 | 16 |
| Post-survey | 5053 | 347 | 41 | 11 |

# 6 Future steps

This study has seen several challenges in development and implementation throughout the whole process. From the analysis of the feedback, there are some possible improvements that need consideration during the development as listed below:

- Encourage to start
    a. Divide into smaller sections
    b. Make it less frightening
- Enable customised styles
    a. Optimize the design for different learning styles
    b. Allow text helpers
- Improve efficiency
    a. Adopt adaptive training
    b. Add more practical / interactive contents

In essence, the training must be motivating enough for many users to start before going into further details. As described in Chapter 5.3, the training did not attract as many users as expected and their reactions to the announcement of the training prototype were low compared to the first survey. What can be inferred from the feedback is 1. users were not encouraged to take the training by its length of 30 minutes 2. users were hesitating to learn new things especially when the subject seemed too complex, or they were not familiar with technologies in general. Although the prototype of the training module was approximately 30-minute long with each lecture of 10-minute length and its target was clearly described as non-technical users, some participants found it excessively long or complex. Therefore, each section must be no longer than 10 minutes and the total training should not exceed an hour as revealed at the pre-survey in Chapter 4.3.

Another suggestion is to allow users to optimize the styles; some of the feedback highly appreciated the visual contents being effectively inserted while others felt the need for more visual contents. As everyone has different learning styles as text-oriented or visual-oriented, high customization must be the norm in the modern age. Additionally, it is critical to provide text helpers; not all Japanese can read well as mentioned in Chapter 2.4, so the training should adjust the content to their level of literacy. For example, adding hiragana alongside *kanji* can enlarge the scope of the audience to those who cannot read *kanji* or replacing rather academic words with kid-friendly ones can help children in kindergarten as it is not too early a starting age of the Internet nowadays. Cultural visualisation such as manga or anime should also be considered as it may potentially attract more users.

The efficiency can be enhanced with adaptive training proposed by the previous study [12]. The suggested approach improves the learning curve and makes it stick by generating the proper level of the content for each learner. Furthermore, there is no doubt that the training must contain more hands-on practice to polish their skills in cybersecurity [11]. Such practice is admittedly effective in a real-life situation as the case study in the prototype had a positive effect on some users. Since learning is a continuous process, more interactive contents should be effectively inserted to avoid boredom and add playfulness.

The ultimate goal is to reach as large an audience as possible so that security awareness is heightened on a larger scale, ideally nationwide. One possible solution is to mandate the training in schools and companies by law. This enaction, however, involves slugging processes of countless discussions and approvals and mandatory training might become dull to some group of people. Owing to that, one of the most accessible solutions is to take actions to increase social media shares such as Facebook and Twitter. This study followed this approach and successfully spread the training to many users, but the majority of them did not have the motive to take the training. Generally speaking, the Japanese enjoy using social media and tend to follow what others do for the country's collectivism. Nevertheless, it must be recalled that Japan has one of the world's largest ageing populations and they are hard to reach on social media but often victims of cybercrimes. Hence, further research is needed to deeply understand the nature of Japanese users and propose how to encourage active training across the country.

# 7 Summary

Despite the high rate of Internet usage across the country, cybersecurity education was not sufficiently provided to the general public. The research has proven that many Japanese Internet users do not have access to good security training resources or materials where the poor ability of language skills has narrowed the scope of accessible materials online. Within the first survey, the majority showed concerns about cyber-attacks and interests in learning cyber hygiene to protect themselves.

The goal of the work was to analyse Japanese-specific difficulties or vulnerability and develop a prototype of web-based security training for non-technical users in Japan as a solution to raise security awareness. The subjects of the content were chosen online fraud, account security, and device security, all of which together cover the common individual-scoped cyber-attacks in Japan. Additional features reviewed and suggested by the thesis such as social media share buttons and progress bars were implemented for the prototype training. The training was developed with users' reflection and is currently deployed at https://cytrain.netlify.app. The platform is semantically divided into 4 pages: Welcome page, Lecture page, Test page, and About page. Each page has user-friendly navigation, following the modern web design.

As a result, the training successfully played an important role in raising awareness and educating the participants on what security measures to be taken in their daily usage of the Internet. 100% of the training participants on the post-survey showed positive effects on their awareness and knowledge. However, it cannot be denied that the prototype has seen several challenges. Later possible improvements in the design are such as adding more interactive and practical activities, dividing the proper level of content, splitting into smaller sections.

For a future step, this study can be referenced as a prototype material along with the suggested improvements when an individual or an institution develops security training for any size of participants. Furthermore, it is of utmost importance to investigate a method to reach a larger audience to accomplish the objective of the study.

# References


[1] Ministry of Internal Affairs and Communication, "2020 WHITE PAPER Information and Communications in Japan," 2020. [Online]. Available: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2020/2020-index.html. [Accessed 13 May 2021].

[2] H. Furuya, "*Nōton Raifu Rokku Saibā sēfuti insaito repōto 2019* [NortonLifeLock Cyber Safety Insight Report 2019]," NortonLifeLock Inc., 1 April 2019. [Online]. Available: https://japan.norton.com/PR/NLCSIR2019.pdf. [Accessed 13 May 2021].

[3] Ministry of Economy, Trade and Industry, "*IT jinzai ikusei no jōkyō tō ni tsuite* [Status of IT human resource development]," [Online]. Available: https://www.meti.go.jp/shingikai/economy/daiyoji_sangyo_skill/pdf/001_s03_00.pdf. [Accessed 13 May 2021].

[4] A. Kohgo, "Information security education for students in Japan," National Institute for Educational Policy Research, Ministry of Education, Culture, Sports, Science and Technology, March 2014. [Online]. Available: https://www.nier.go.jp/English/educationjapan/pdf/201403ISE.pdf. [Accessed 13 May 2021].

[5] "*jōhō sekyuriti jūdai kyōi 2021* [Information Security: Top 10 threats in 2021]," Information-technology Promotion Agency, Japan, March 2021. [Online]. Available: https://www.ipa.go.jp/files/000088835.pdf. [Accessed 13 May 2021].

[6] W. Wang and L. Guo, “Cyber Security Training in Europe and America and its Enlightenment to China,” 2020.

[7] “Health Insurance Portability and Accountability Act of 1996,” the United States of America, 1996.

[8] European Union, “European Strategy for a Better Internet for Children,” 2012.

[9] I. M. Venter, R. J. Blignaut, K. Renaud and A. M. Venter, “Cyber security education is as essential as “the three R's”,” 2019.

[10] F. A. Alaul, “The Need for Effective Information Security Awareness,” American University of Sharjah, Sharjah, 2012.

[11] R. Beuran, K.-i. Chinen, Y. Tan and Y. Shinoda, "Towards Effective Cybersecurity Education and Training," Japan Advanced Institute of Science, 2013.

[12] Z. Tan, R. Beuran, S. Hasegawa, W. Jiang, M. Zhao and Y. Tan, “Adaptive security awareness training using linked open data datasets,” Japan Advanced Institute of Science and Technology, Nomi, 2020.

[13] T. Yukawa, K. Kawano and Y. Fukumura, "*e-Learning ni okeru tsunagari kan no dounyū* [An e-Learning environment providing awareness of study progress and communication context]," *Japan journal of educational technology,* vol. 31, no. 13498290, pp. 61-64, 2007.

[14] C. Kogo, "*Shakaijin no manabinaoshi onrain kyōiku mp jittai to kadai* [Re-learning for Working Adults the reality and challenges of online education]," *The Japan Institute for Labour Policy and Training, The Japanese journal of labour studies,* vol. 721, pp. 15-25, Aug 2020.

[15] "*Heisei 30 nendo eigo kyōiku jisshi jōkyō chōsa gaiyō* [Overview of the survey on English Education Implementation Status]," Ministry of Education, Culture, Sports, Science and Technology, 2018. [Online]. Available: https://www.mext.go.jp/content/20200710-mxt_kyoiku01-100000661_2.pdf. [Accessed 13 May 2021].

[16] "*Intānetto no anzen anshin handobukku* [Internet Safety and Security Handbook]," National center of Incident readiness and Strategy for Cybersecurity, 31 March 2020. [Online]. Available: https://www.nisc.go.jp/security-site/files/handbook-all.pdf. [Accessed 13 May 2021].

[17] Facebook, "React," [Online]. Available: https://reactjs.org.

[18] Microsoft, "TypeScript," [Online]. Available: https://www.typescriptlang.org.

[19] Alibaba Group, "Ant Design," [Online]. Available: https://ant.design.

[20] Netlify Inc., "Netlify," [Online]. Available: https://www.netlify.com..

[21] MonkeyLearn Inc., "MonkeyLearn," [Online]. Available: https://monkeylearn.com.

# Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Shiori Yamazaki

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "A Training Module of Social Engineering For Japanese Non-Technical Users", supervised by Kaido Kikkas
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

# Appendix 2 – Pre-survey

Table 6. Survey of ordinary Internet users' attitudes towards social engineering

| Question | Answers (80)<br>[answer type] options (count) |
|---|---|
| What is your age range? | [Multiple choice]<br>- 10-19 (7)<br>- 20-29 (64)<br>- 30-39 (2)<br>- 40-49 (3)<br>- 50+ (4) |
| What is your gender? | [Checkboxes]<br>- Male (32)<br>- Female (46)<br>- Other (2) |
| What is your educational and occupational background? (multi-select) | [Checkboxes]<br>- IT-related school (9)<br>- IT-related job (4)<br>- None of the above (67) |
| Period of Internet usage | [Linear scale]<br>1-10 in years<br>(1, 0, 1, 0, 3, 2, 9, 8, 3, 53) |
| Time spent on the Internet per day | [Linear scale]<br>1-10 in hours<br>(1, 6, 13, 10, 15, 7, 9, 8, 6, 5) |
| I have knowledge in computers and the Internet | [Linear scale]<br>1-5<br>(11, 21, 27, 16, 5) |
| I have concerns about cyber-attacks | [Linear scale]<br>1-5<br>(3, 16, 24, 23, 14) |
| I know what social engineering is | [Multiple choice]<br>- Yes (18)<br>- No (62) |
| I have taken training on social engineering | [Multiple choice]<br>- Yes (6)<br>- No (74) |
| If yes, please provide the details of the training | [Short answer]<br>university (4), school (1), online course (1) |

| | |
|---|---|
| I have been victimized of a social engineering attack | [Multiple choice]<br>- Yes (3)<br>- No (77) |
| If yes, please provide the details of the attack | [Short answer]<br>Phishing SMS (1), Account hijacking (1) |
| I have knowledge in social engineering and am always taking best security measures | [Linear scale]<br>1-5<br>(38, 23, 12, 4, 2) |
| I am interested in security training | [Linear scale]<br>1-5<br>(4, 22, 21, 20, 13) |
| Preferred styles of learning | [Checkboxes]<br>- Online (66)<br>- In-person (21)<br>- Text (2)<br>- SNS (1) |
| Preferred cost of the training | [Checkboxes]<br>- Free (61)<br>- Less than 1,000 yen or $10 (28)<br>- Less than 5,000 yen or $50 (18)<br>- Less than 10,000 yen or $100 (3)<br>- More than 10,000 yen or $100 (1) |
| Preferred number of participants | [Checkboxes]<br>- Alone (32)<br>- 5 participants (40)<br>- 20 participants (27)<br>- More than 20 participants (13) |
| Preferred length of the training | [Multiple choice]<br>- Less than 1 hour (55)<br>- Less than 5 hours (20)<br>- Less than 10 hours (4)<br>- More than 10 hours (1) |
| Preferred features | [Checkboxes]<br>- Join with friends (32)<br>- Share on social media (19)<br>- Take quizzes or tests (32)<br>- Receive certificate (23)<br>- Take training at any time (50)<br>- Take training from any place (44)<br>- Communicate with other participants in real time (16)<br>- Communicate with teachers in real time (32) |

# Appendix 3 – Post-survey

Table 7. Survey of online security training for ordinary Internet users

| Question | Answers (13)<br>[answer type] options (count) |
|---|---|
| What is your age range? | [Multiple choice]<br>- 10-19 (0)<br>- 20-29 (6)<br>- 30-39 (1)<br>- 40-49 (0)<br>- 50-59 (2)<br>- 60-69 (0)<br>- 70-79 (0)<br>- 80-89 (0)<br>- 90+ (0) |
| What is your gender? | [Multiple choice]<br>- Male (4)<br>- Female (5)<br>- Other (0) |
| Your quiz score | [Multiple choice]<br>- 0-4 (0)<br>- 5-8 (3)<br>- 9-12 (6)<br>- 13-14 (0)<br>- 15 (0) |
| Difficulty level of the training | [Linear scale]<br>1-5<br>(0, 1, 2, 5, 1) |
| Amount of the training | [Linear scale]<br>1-5<br>(0,1, 5, 3, 0) |
| I have a higher awareness of cyber-attacks and security measures | [Linear scale]<br>1-5<br>(0, 0, 0, 4, 6) |
| I am more knowledgeable in cyber-attacks and security measures | [Linear scale]<br>1-5<br>(0, 0, 0, 1, 8) |
| Please provide what you have learnt | [Short answer]<br>Encryption (1), Storing password (1), |

| | |
|---|---|
| | Everything (2), Difference between HTTP and HTTPS, EV-SSL certificate (2) |
| Please provide what you want to learn more | [Short answer]<br>Safe environment (1), Auto generated password (1) |
| Preferred features | [Checkboxes]<br>- Share on social media (2)<br>- Quiz (9)<br>- Progress bar in lecture (3)<br>- Estimated time in lecture (0)<br>- Other (0) |
| Unnecessary features | [Checkboxes]<br>- Share on social media (1)<br>- Quiz (0)<br>- Progress bar in lecture (1)<br>- Estimated time in lecture (4)<br>- Other (0) |
| Missing features | [Short answer]<br>Auto analysis (1), Back button (1), Chapter quiz (1) |
| I would recommend this training to others | [Linear scale]<br>1-5<br>(0, 0, 2, 3, 4) |
| Any improvements or comments | [Short answer]<br>I felt like there was too much text, and the content was too difficult for non-academic people. It'd be better if more videos were there.<br><br>The content was very informative, and since my password was leaked before, the topic was relevant to me. The amount of content was so much that I couldn't learn all at once.<br><br>It was a bit too difficult for non-technical people.<br><br>The lecture was well-organized and easy to understand in spite of the complex subject. I felt familiar with cybersecurity. I liked how the illustrations and diagrams were effectively inserted.<br><br>It would be easier to understand if I could see the intensity of the risk.<br><br>It was smooth to read. I think this service is friendly to beginners thanks to the images and citations. |

# Appendix 4 – Demonstration of the training

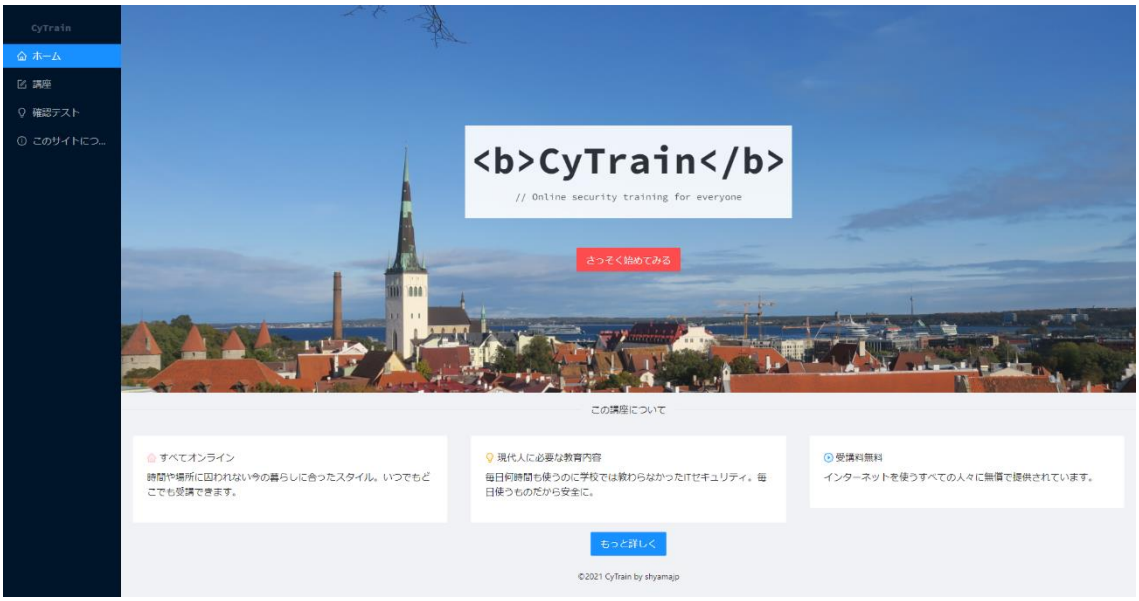


Figure 5. Welcome Page (PC)

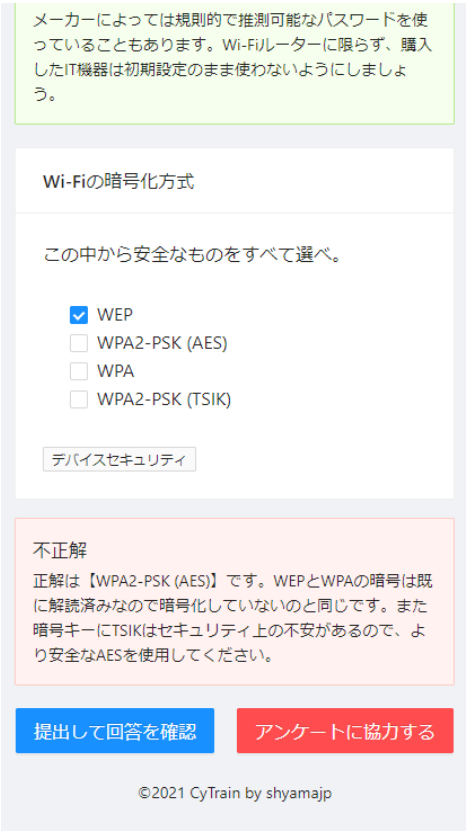


Figure 6. Quiz Answer Page with description (Mobile)

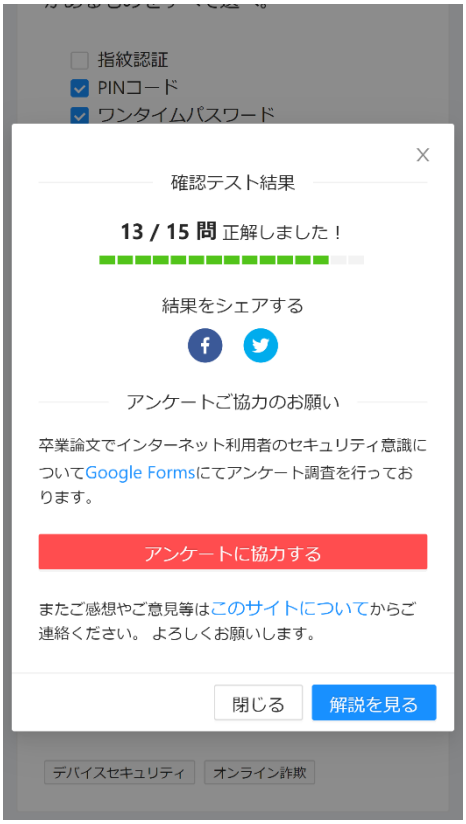


Figure 7. Quiz Result Page with share button (Mobile)


Figure 9. Lecture List Page (Mobile)


Figure 8. Welcome Page (Mobile)


Figure 10. Lecture Page with illustration and progress bar (Mobile)

# Appendix 5 – Translation of the Training Content

Table 8. Welcome Page in English

| | |
|---|---|
| Red button text | Start now |
| Divider text | About this training |
| Box 1 | Everything Is Online<br><br>There is no constraints of time or place suited for today' lifestyle. You can take the training from anywhere at your own pace. |
| Box 2 | Essential Content in the Modern Age<br><br>IT security is not taught in school despite the large spread of the Internet use. Learn how to protect yourself for your daily risks. |
| Box 3 | Free Tuition<br><br>This training is provided for anyone who has access to the Internet. |
| Blue button text | Show more |

Table 9. Lecture List Page in English

| | |
|---|---|
| Page Header | List of Lectures |
| Box 1 | Online Fraud<br><br>Can you verify who you are connecting with over the Internet? Learn how to spot authentic materials and avoid various online scams.<br><br>2 Lectures (8 minutes)<br><br>- Basics of online fraud<br><br>- How to spot authentic materials |

| | |
|---|---|
| Box 2 | Account Security<br><br>Is your account secure? Learn how to secure your account with special authentication.<br><br>3 Lectures (13 minutes)<br><br>- Various methods of attacks<br><br>- How to create secure password and store password securely<br><br>- Secure authentication methods |
| Box 3 | Device Security<br><br>Is your connection protected? Learn how to use browser and network in a secure way.<br><br>3 Lectures (20 minutes)<br><br>- Device Security<br><br>- Application Security<br><br>- Network Security |
| Blue button text | Check out this lecture |

Table 10. Quiz Result Page in English

| | |
|---|---|
| Divider text 1 | Your test results |
| Paragraph 1 | You got 13 out of 15.<br><br>Share your results on social media. |
| Divider text 2 | Please leave feedback |
| Paragraph 2 | I am researching for my graduation thesis on the attitude towards security through Google Forms. |
| Red button text | Go to survey |

| | |
|---|---|
| Paragraph 3 | Please share your opinions via contacts on About page. Thank you for your cooperation. |