Journal of Information Processing Vol.30 841–858 (Dec. 2022)

[DOI: 10.2197/ipsjjip.30.841]

Regular Paper

Experiences, Behavioral Tendencies, and Concerns of Non-Native English Speakers in Identifying Phishing Emails

Ayako A. Hasegawa[1,a)] Naomi Yamashita[2,4,b)] Mitsuaki Akiyama[2,c)] Tatsuya Mori[3,1,5,d)]

Received: March 8, 2022, Accepted: September 2, 2022

Abstract: Phishing, a form of online fraud, remains a huge cybersecurity threat. Recent research in cybersecurity and risk management revealed the possibility that non-native speakers of the language used in phishing emails are more susceptible to such attacks. Although many studies have focused on the behaviors that native English speakers use to avoid phishing attacks, little is known about the behaviors of non-native speakers. Therefore, we conducted an online survey with 862 non-native English speakers (284 Germans, 276 South Koreans, and 302 Japanese). We showed that non-native English speakers are regularly exposed to English phishing emails. Through our scenario-based roleplay task, we found that participants, especially those who lacked confidence in English, had a higher tendency to ignore English emails without careful inspection than emails in their native languages. Furthermore, both the German and South Korean participants generally followed the instructions in the email in their native languages without careful inspection. Finally, our qualitative analysis revealed five main concerns in identifying English phishing emails: difficulty understanding email content, difficulty identifying errors and unnatural language, unfamiliarity with phishing emails, decreased attention, and difficulty finding similar cases. These findings highlight the importance of providing non-native speakers with specific anti-phishing interventions that differ from those for native speakers.

Keywords: usable security, phishing, non-native English speakers, security behavior

1. Introduction

Phishing is a frequently employed cyberattack that masquerades as a legitimate business or reputable individual to acquire sensitive data, such as account credentials or credit card information. Since the mid-90s, a vast body of research in the fields of cybersecurity and risk management has led to the development of countermeasures [2], [3]; however, phishing remains a huge cybersecurity threat [4]. It is noteworthy that COVID-19 has caused a further massive increase in phishing attacks [5].

Among Internet users, non-native speakers of the language used in phishing emails are more susceptible to such attacks. Recent work has shown that their English proficiency level significantly affects the ability of the users to identify English phishing emails, and evidently lower English proficiency levels lead to increased phishing susceptibility [6]. Although research shows that non-native speakers are more susceptible to phishing attacks, little is known about their coping behaviors: we still lack an understanding of the differences in behavior (or reactions) of people when they receive an email containing instructions to click on a URL link or open an attachment in a non-native language compared with when they receive it in their native languages.

In the fields of psychology and cognitive science, research has shown that people tend to behave differently (i.e., perform more poorly) when using a non-native language compared with their native language [7], [8]. However, research suggests somewhat incongruous results. First, previous research on risk and uncertainty shows that people tend to be risk-averse in the face of uncertainty [9]. This implies that people may become more risk-averse when dealing with emails written in a non-native language because they are less confident about being able to identify phishing attacks written in a non-native language. As a result, people may simply ignore such emails without careful inspection. In contrast, other research has shown that people tend to make more risk-prone decisions when using a non-native language [10], [11]. Therefore, a non-native speaker may follow the instructions written in the email without careful inspection, which could lead to unwanted consequences, such as breaches of critical sensitive information.

To help non-native speakers defend themselves against phishing attacks, we must understand their current practices of dealing with emails written in a non-native language. In particular, we are interested in understanding the concerns of non-native speakers when they are involved in phishing attacks and the differences in the ways they deal with emails (with links and attachments)

[1] NICT, Koganei, Tokyo 184–0015, Japan
[2] NTT, Musashino, Tokyo 180–8585, Japan
[3] Waseda University, Shinjuku, Tokyo 169–8555, Japan
[4] Kyoto University, Kyoto 606–8501, Japan
[5] RIKEN AIP, Chuo, Tokyo 103–0027, Japan
[a)] a.hasegawa@nict.go.jp
[b)] naomiy@ieee.org
[c)] akiyama@ieee.org
[d)] mori@nsl.cs.waseda.ac.jp

This paper is the extended version of the paper presented at SOUPS'21 [1].

depending on whether they are written in their native language or in a non-native language.

In order to explore behavioral tendencies of non-native English speakers (NNESs) and their concerns about identifying English phishing emails, we conducted an online study with 862 NNESs (284 Germans, 276 South Koreans, and 302 Japanese) who are full-time workers exposed to the risks of phishing attacks in English. We recruited NNESs because English remains the dominant language on the Internet [12]. Although German, South Korean, and Japanese peoples are all NNESs, their average English proficiency levels differ; Germans have the highest, while the Japanese have the lowest [13]. We studied participants' behavior toward emails and their experiences and concerns about identifying English phishing emails.

We found that NNESs are regularly exposed or perceive that they are exposed to English phishing emails. In our scenario-based roleplay task, participants adopted more security-risk-averse behaviors (i.e., ignoring emails without careful inspection) when the emails were written in English rather than in their native languages. This tendency was salient for those who lacked confidence in reading English. Furthermore, both the German and South Korean participants generally adopted more security-risk-prone behaviors (i.e., following the instructions in the email without careful inspection) when the emails were written in their native languages than the Japanese participants. In addition, qualitative analysis of their open-ended answers revealed five main factors that formed their concerns in identifying English phishing emails, which differ from the concerns they have in identifying phishing emails in their native languages. These findings highlight the importance of providing non-native speakers with specific anti-phishing interventions that differ from those for native speakers.

This study makes the following contributions:

(1) This work is among the first that systematically explores the relationship between users' English proficiency levels and their reactions/behaviors when receiving an email that includes links and attachments.
(2) Our results show that users have specific concerns about identifying a phishing email written in their non-native language (English) and that they adopt different strategies when receiving emails written in their native and non-native languages.
(3) Our findings provide design implications that help users combat phishing attacks in their non-native languages (English).

2. Background and Research Questions

In this section, we review the literature that is closely related to this study. We first review studies that explored the factors that influence users' susceptibility to phishing emails. Next, we review previous works that examined the effect of users' language and culture on their susceptibility to phishing emails. Finally, we highlight the research questions of this study.

2.1 Factors Related to Phishing Susceptibility

The factors related to susceptibility to phishing (including spear phishing) emails found by previous studies can be classified into three categories: (i) user demographics, (ii) anti-phishing strategies, and (iii) contents and contexts of phishing.

User Demographics. Many researchers have found that basic demographics such as age and gender are related to phishing susceptibility [14], [15], [16], [17]. However, some studies yielded incongruous results because they used different methods and studied different populations. For example, Sheng et al. [15] reported young people were most susceptible to phishing whereas Li et al. [14] concluded that older people were the most susceptible. Research has also revealed that users' attributions or traits such as personality traits (Big Five) [18], [19], cognitive impulsivity [20], [21], employment department and position [14], and education level [20], [22] were related to phishing susceptibility. In terms of user skills, studies have reported that user security knowledge, awareness, behavior, and previous anti-phishing training experience were significantly related to phishing susceptibility [15], [23], [24], [25]. Vishwanath et al. [26] found that a heavy email load (i.e., the number of received emails) had a strong and significant influence on phishing susceptibility.

Anti-phishing Strategies. Several studies indicated that people often did not pay attention to reliable phishing cues and their strategies failed to identify phishing emails or suspicious URLs [19], [25], [27], [28], [29], [30]. For instance, Downs et al. [28] reported that participants in their study used various strategies to determine the validity of emails, primarily centered around interpreting the email text rather than focusing on more reliable phishing cues in headers or the URLs associated with the links. On the other hand, Vishwanath et al. [26] and Wang et al. [31] found that individual attention to email sources, grammatical errors, and misspellings were significantly negatively related to phishing susceptibility. They also concluded that individual attention to urgent cues and subject lines were significantly positively related to phishing susceptibility. Wash et al. explored anti-phishing strategies of IT expert [32] and non-expert users [33], and found that non-expert users have many properties in common with how IT experts identify phishing emails.

Contents and Contexts of Phishing Emails. Given that users' anti-phishing strategies center around interpreting email texts, researchers have studied how users' behaviors are affected by email contents. Researchers have classified the contents of phishing emails based on a seminal work by Cialdini [34], which identified principles that triggered people's decisions to comply with requests (called "principles of persuasion"). They found that the presence of authority cues [21], [35], consistency [36], and scarcity [36] increased users' phishing susceptibility. From the viewpoints of contexts, participants are more susceptible when phishing messages are specific to their situations [37], [38], [39]. Unsurprisingly, several studies revealed that the contents and context of phishing emails to which participants were more susceptible depend on the demographics of participants [14], [16], [40].

2.2 Impact of Culture and Language

Culture. Cross-cultural studies are positioned as a crucial theme in the field of cybersecurity because culture directly impacts security-related phenomena [41]. Recently, many re-

searchers have conducted a variety of cross-cultural security studies, such as those on the security behavior intentions scale (SeBIS) [42], generated passwords [43], smartphone unlocking [44], and account security incident response [45]. Some of these cross-cultural studies adopted Hofstede's cultural dimensions [46] to interpret the observed differences in security behavior by linking them to the national characteristics, such as the individualism-collectivism dimension [45].

The cross-cultural approach has also attracted interest in phishing research. Butavicius et al. [23] and Tembe et al. [47] recruited participants from multiple countries and showed that those with higher individualism scores (e.g., the U.S. participants) were less likely to be phished. Both works suggest that low levels of individualism may fuel a desire to respond to requests from others to maintain group harmony, which includes requests in phishing emails (especially from an authority figure). Flores et al. [24] reported that factors (individual demographics) that were significantly correlated with phishing susceptibility differed among countries.

Language. Although language is known to have a considerable influence on one's thoughts and behavior, few studies in cybersecurity have focused on language. A broad body of research in the fields of psychology and cognitive science shows that people face various interpretation and reasoning problems when using a non-native language [7], [8], [48], [49]. For instance, Takano and Noda [7] demonstrated that using a foreign language caused a temporary decline in thinking task performance. Rear [8] compared the critical thinking skills of Asian students in their native language and English contexts and argued that using a foreign language considerably interfered with critical thinking. Some researchers have also identified problems that non-native speakers face during Internet use, such as online searches [49]. On the other hand, some psychological researchers demonstrated that using a foreign language reduced decision-making bias, that is, the loss aversion bias that people have in their native language contexts was reduced in foreign language contexts [10], [11].

Although studies have explored the impact of culture on users' phishing susceptibility, the impact of language (especially language barriers) on this phenomenon is not yet fully understood. So far, little work has addressed the impact of language barriers of NNESs on their susceptibility to phishing emails. Among the few studies that investigated language issues in cybersecurity, Alseadoon et al. [6] and Kävrestad et al. [50] conducted a phishing identification task in Saudi Arabia and Sweden, respectively. They revealed that the NNESs' self-perceived English proficiency level significantly affected their ability to identify phishing English emails [6] and legitimate English emails [50], respectively.

2.3 Research Questions

In summary, although previous works suggest that NNESs may be more susceptible to phishing attacks, it remains unclear how language affects non-native speakers' strategies to combat phishing attacks. To help non-native speakers defend themselves against phishing attacks, it is critical to understand their current practices of dealing with emails written in their non-native language. In this paper, we ask:

RQ1: Are NNESs exposed to English phishing emails?

RQ2: Do NNESs show different behavioral tendencies (e.g., security-risk-prone vs. security-risk-averse) toward native language and English emails?

RQ3: What are the NNESs' concerns about identifying English phishing emails?

Following the suggestion of Lastdrager et al. [51], who addressed anti-phishing interventions designed specifically for children, we advocate for anti-phishing interventions designed specifically for NNESs.

3. Methods

We designed an online survey to understand NNESs' past experiences (**RQ1**), behavioral tendencies (**RQ2**), and concerns (**RQ3**) about English phishing emails.

3.1 Survey Design

Figure 1 summarizes the design of our survey and corresponding research questions [*1]. Our survey consisted of four parts. In Part 1, we asked the participants about their demographics; next in Part 2, we explored their behavior and attention toward emails (**RQ2**); then in Part 3 we asked the participants about their past experiences (**RQ1**); and finally in Part 4, we asked the participants with low confidence in identifying English phishing emails about their concerns. (**RQ3**).

In Part 2, randomly selected half of the participants from each country were shown a set of English emails that included phishing emails. The other half were shown the same set of emails translated into their native languages. All participants were provided with a scenario that described the background of receiving the emails and asked how they would respond to them. To minimize the effects of email content, we adopted a between-subjects design for Part 2. In Part 3, all participants were asked about their past experiences of being deceived by phishing emails, and in Part 4, they were asked about their confidence in identifying phishing emails in their native languages and in English. We adopted a within-subject design for Part 3 and 4 because we were interested in understanding whether people had different experiences and confidence levels when the language of the emails differed. Furthermore, it is worth noting that we conducted Part 3 and 4 (RQ1 and RQ3) after Part 2 (RQ2) because we were concerned that the participants' behavior (in Part 2) may be affected if they knew the focus of our study was phishing (as revealed in

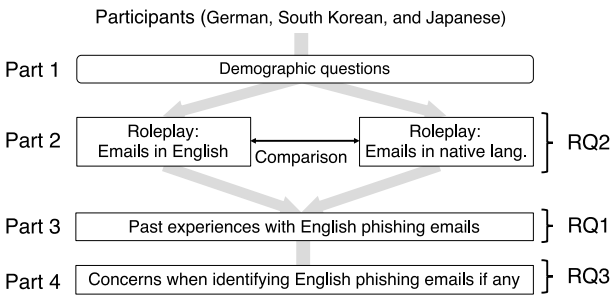

Fig. 1 Overview of our survey design and research questions (RQs).

[*1] The entire study was approved by our Institutional Review Board.

Part 3). A previous study showed that revealing such information would improve the participants' performance to identify phishing emails during the experiment [20]. We did not inform the participants that they were participating in a phishing study in Part 2. The demographics questions in Part 1 also did not include questions about their phishing experiences.

The questionnaire items (including the email materials) were translated into German, Korean, and Japanese by two professional translators of the respective language to ensure their validity.

3.2 Procedure

In this subsection, we introduce the procedure of our study and the preventive measures that protected the privacy of our participants during the study.

Screening Survey. To recruit eligible participants, we implemented a short screening survey prior to our main survey. The screening survey included four demographic questions: age, self-identified gender, occupational status, and native language. In the middle of the screening survey, we asked an attention check question. Those who were deemed eligible for our survey (participation eligibility is described in Section 3.4) proceeded to our survey. Our screening survey included a consent form and instructions. In the instructions, participants were provided with the survey title, estimated time, compensation, and confidentiality of the survey data. Our survey title was "Survey of emails written in <participants' native language> or English". Based on other security-related studies that conducted online surveys [29], [52], we did not use security-related terms (e.g., phishing) in either the survey title or instructions to avoid recruiting biased participants who were only interested in computer security.

All participants were required to complete consent forms before starting the main survey (Parts 1 to 4).

Part 1: Demographics. In addition to the basic demographic questions from the screening survey, we asked the following six questions: education level, whether they were IT professionals, confidence level in their English reading skills (6-point Likert scale), total years spent learning English, and the average number of emails they received each working day in their native language and English.

Part 2: Behavioral Tendencies (RQ2). Based on previous phishing studies, we measured the participants' behaviors based on their performances in a scenario-based roleplay task [15], [20], [28], [53], [54], [55]. The roleplay enables researchers to study phishing without conducting an actual simulated phishing attack [15].

We first gave participants fictitious profile information about the email recipient for roleplay in their native language. We then showed screenshots of four emails that included phishing emails and asked them to answer how they would respond if they received each email by selecting provided options. At the end of Part 2, we asked the participants about the email elements to which they usually paid attention when they received emails. They chose their top 3 email elements from a list of representative elements (e.g., sender's email address, subject line, grammatical errors and misspellings), which were adopted from Vishwanath et al. [26].

Part 3: Confidence and Concerns about English Phishing Emails (RQ1). In Part 3, we asked participants questions about their confidence and concerns about identifying English phishing emails. To avoid misunderstandings, we defined "phishing attacks" at the beginning of Part 3. Then, we asked how often they received both work-related and personal suspicious emails (except company phishing training). We specifically asked them how often they received such emails written in both their native language and English.

Next, we asked about their experiences of being deceived by phishing in both work-related and personal emails, except for training. We asked about clicking on a link or opening an attached file in phishing emails written both in their native language and English, regardless of the damage. If participants answered that they had been deceived by English phishing emails, we asked them to explain the contents of the phishing emails using an open-ended form (optional).

Part 4: Confidence and Concerns about English Phishing Emails (RQ3). Participants were then asked about their confidence levels for identifying phishing emails. They assessed their agreement or disagreement with these two statements: "I can always identify a phishing email written in <participant's native languages>" and "I can always identify a phishing email written in English" on a 6-point Likert scale from "strongly disagree" to "strongly agree." Depending on their answers about their level of confidence, participants were asked either why they thought that they could or could not identify English phishing emails in an open-ended question.

For a manipulation check, we included a question in the middle of Part 3 that asked about the definition of phishing. This was to confirm their understanding of phishing emails. They were asked to choose the best definition of phishing from three options: the definitions of phishing, ransomware, and distributed denial-of-service (DDoS). An attention check question was also included in the middle of Part 4. Participants who answered either the definition check or the attention check incorrectly, or both, were excluded from our dataset to ensure the quality of our analysis results. All participants received compensation, even if they did not pass these checks.

3.3 Materials for Roleplay Task

For our roleplay task, we carefully examined previous phishing studies as mentioned in Section 3.2 and finally prepared four emails: an *obvious-phishing* email, two *uncertain* emails, and a *genuine* email (**Table 1**). As shown in **Fig. 2**, all used screenshots of the emails follow the format of Gmail. The obvious-phishing email contained features that appeared to be undeniably illegitimate. The genuine email contained no features that suggested phishing. Because we were interested in how NNESs behave when they are faced with a high level of uncertainty, we prepared uncertain emails separately from obvious-phishing emails [*2]. The uncertain emails contained some features that suggested the possibility of phishing; however, such information alone did not pro-

[*2] Some prior studies treated them altogether as phishing emails [53], [54].

Table 1 Features of four emails used in roleplay task.

	Sender	Legitimacy	Phishing cues
(a)	PayPal (Card expiration notice)	Uncertain	· Impersonal greeting · Hidden URL (HTML button) · Request for sensitive information · Request for urgent action
(b)	LinkedIn (Login notification)	Obvious phishing	· Suspicious sender's email address · Impersonal greeting · Suspicious URL · Request for urgent action
(c)	Coworker (Meeting invitation)	Genuine	N/A
(d)	IT service staff (Alert notice)	Uncertain	· Attached zip file · Request for urgent action

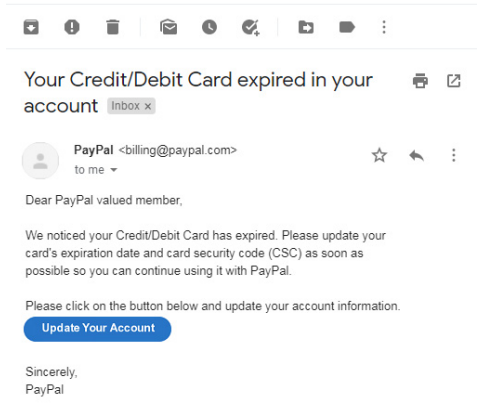

Fig. 2 Example of email screenshots shown to participants in the roleplay task (Email (a), English version).

vide sufficient evidence to identify whether the email was phishing based only on the appearance of the screenshots. The contents of the emails of our roleplay task must resemble those received by NNESs on a daily basis. If NNESs receive an email in English from a service that is unavailable in their country, they are likely to ignore it based on the unnatural context. Therefore, the senders (or spoofed senders) of the emails must be well-known, worldwide services (e.g., PayPal and LinkedIn) or business acquaintances to increase the feeling of verisimilitude in NNESs about an email in English. The obvious-phishing and uncertain emails were collected from an online archive of phishing emails (MillerSmiles.co.uk [56]) and the dataset used by Canfield et al. [53], [54]. The genuine email was taken from an inbox of one of the authors. We then arranged them for this study (e.g., displayed names and dates). We kept the survey short by providing a limited number of emails for this roleplay task that could be completed in a few minutes in order to reduce participants' fatigue.

Recent studies examined spear phishing emails applying the psychological principles of persuasion [16], [36] as mentioned in Section 2.1. Instead of covering various scenarios concerning such psychologically persuasive contexts, our roleplay task focuses on phishing cues that might be fundamental metrics when users identify phishing emails. As summarized in Table 1, the obvious-phishing and uncertain emails contained two or more features often associated with such practices as phishing cues: suspicious sender email addresses, suspicious URLs, impersonal greetings, hidden URLs, attached files, requests for sensitive information, and requests requiring urgent action [28], [53], [54], [57]. We did not use an email that contained obvious grammatical errors or misspellings. This is because it would be impossible to replicate them accurately across languages and we wanted to minimize experimental variability. In the obvious-phishing email (b) (Table 1), a suspicious URL was displayed, which Canfield et al. [53] described as the most valid cue for identifying phishing emails. The sender's email address in phishing email (b) was also suspicious. Although the name of a well-known service (LinkedIn) appeared in the URL and in the sender's email address, their positions in the URL and email address structure were inauthentic. The uncertain email (a) contained a hidden URL, and the URL was hidden by an HTML button that displayed text. The URL must be uncovered by hovering over it with a mouse to identify whether it was phishing or genuine. In the uncertain email (d), a zip file was attached, which could contain harmful files such as malware.

The participants played the role of a male employee who was given a prevalent name in each country (e.g., Japanese participants were given an identity of "Taro Yamada") working at the ABC Company. Each participant was informed that he had PayPal and LinkedIn accounts, which, respectively, corresponded to the senders of emails (a) and (b). We also informed the participants of the email addresses of his boss and the company's IT staff, which, respectively, corresponded to the senders of emails (c) and (d).

We then provided the following four options to participants in each email: "I'd ignore it without referring to any other information than this screenshot;" "I'd follow its instruction without referring to any other information than this screenshot;" "I'd refer to some other information than this screenshot to decide how to respond [*3];" and "Other." Although, in reality, users could perform multiple actions (e.g., they ignore an email after checking the validity of sender address), to reduce the complexity of our user study, our roleplay tasks ask participants to choose their *initial reaction* rather than an email response procedure. We also asked the participants who chose "I'd refer to some other information..." or "Other" to specify the information they would refer to or what actions they would take in an open-ended form. Since we wanted to protect our participants from accessing phishing websites but did not want them to think that those emails are phishing, we asked them to answer the questions without searching any information contained in the emails.

Although we designed our roleplay tasks according to the aforementioned prominent literature, the ecological validity of the anti-phishing study of user behavior needs further improvement (Please see Section 5.2).

We provide the full questionnaire in Appendix A.1.

3.4 Participants

We recruited participants from three non-native English-speaking countries to cover three different English levels (high, moderate, and low). The English skills of the citizens of the countries and their confidence in English might affect their responses to English emails. We used the EF English Proficiency Index (EF EPI) 2019 [13] and selected one country from each English pro-

[*3] Hovering over links is included in this option.

Table 2 Basic and extensive demographics of our participants.

Country		Germany		South Korea		Japan	
Language used in our roleplay task		German (N=140)	English (N=144)	Korean (N=141)	English (N=135)	Japan (N=148)	English (N=154)
Age	18-29	24.3%	20.8%	29.8%	25.9%	23.6%	25.3%
	30-39	24.3%	27.1%	22.0%	25.9%	25.7%	21.4%
	40-49	26.4%	27.1%	24.1%	24.4%	25.0%	26.6%
	50-59	22.1%	20.8%	19.1%	19.3%	23.0%	20.1%
	60 or over	2.9%	4.2%	5.0%	4.4%	2.7%	6.5%
Self-identified gender	Male	55.0%	56.3%	59.6%	57.8%	60.1%	55.8%
	Female	45.0%	43.8%	40.4%	42.2%	39.9%	44.2%
Level of education	No high school/High school	25.0%	23.6%	9.9%	11.1%	19.6%	26.0%
	Assoc. degree/Tech. degree	39.3%	45.1%	12.8%	9.6%	20.3%	18.8%
	Bachelor's degree	33.6%	29.2%	71.6%	68.9%	52.7%	46.1%
	Graduate degree	2.1%	2.1%	5.7%	9.6%	7.4%	8.4%
IT professionals	% Professionals	30.7%	27.1%	19.9%	19.3%	8.1%	6.5%
Confidence of English-reading	% Positive (6-point scale)	77.9%	77.8%	41.1%	42.2%	12.2%	14.3%
Years of English learning	Ave.	8.9	8.4	11.6	12.4	8.4	8.2
Received emails per day	Ave.: Native language	25.3	23.1	13.5	14.2	28.7	33.1
Received emails per day	Ave.: English	6.5	4.7	3.0	2.7	1.4	2.2

ficiency level group: Germany from with the very high or high level, South Korea from the moderate level, and Japan from low or very low level.

In each country, we limited the participants to full-time workers who were at least 18 years old and native speakers of the country's official language (e.g., German samples only consisted of native German speakers). We recruited workers to improve the ecological validity of our study. For NNESs, workers face higher potential risks of phishing attacks written in English because they are more likely to be exposed to English than non-workers. We recruited a broad array of participants with quota sampling to match the demographics of working populations.

We recruited participants and conducted our survey through a survey company (Macromill [58]) that has large-scale, global online panels. The participants received a compensation, which roughly equals US$4.7. This survey was done in July and August, 2020.

We analyzed valid responses from 862 participants: 284 Germans, 276 South Koreans, and 302 Japanese. Participants finished our survey in 7.5 minutes (median), including the screening survey. **Table 2** shows the demographics of our participants. Their age and gender distributions were similar in all three countries. Although there were some differences among the three countries in demographics other than age and gender, the distributions of the demographics between the two groups divided by language in our roleplay task (native language group and English group) were similar in each country. The percentages of participants who were confident in their English reading skills were high in Germany, followed in descending order by South Korea and Japan.

3.5 Data Analysis

For RQ2, we categorized participants' behaviors toward phishing in a roleplay task based on two typical indexes introduced in Section 1: security-risk-prone and security-risk-averse behavioral tendencies.

- Security-Risk-Prone Behavior. We defined security-risk-prone behavior as potentially problematic behavior towards obvious-phishing or uncertain emails, specifically, participants following the instructions from the sender (e.g., clicking a link or opening an attached file) without any inspection. In our analysis, we counted the participants who answered, "I'd follow its instruction without referring to any other information than this screenshot," to the obvious-phishing or uncertain emails ((a), (b), and (d) in Table 1).
- Security-Risk-Averse Behavior. We defined security-risk-averse behavior as potentially problematic behavior towards genuine or uncertain emails, specifically, participants ignoring instructions from the sender without any inspection. We counted the participants who answered, "I'd ignore it without referring to any other information than this screenshot," to the genuine or uncertain emails ((a), (c), and (d) in Table 1).

For each email, we tested whether there was a significant difference between the percentages of participants who engaged in risk-prone behavior toward emails in their native language and those in English (Chi-square tests with Bonferroni correction for multiple comparisons). We tested security-risk-averse behavior in the same manner. Furthermore, to explore factors that affect an individual's security-risk-prone/risk-averse behavioral tendency, we performed ordinal logistic regression analyses. Specifically, we used the following model: security-risk-prone/averse behavior ~ age group + IT expertise + confidence in reading English + Email load + culture. These independent variables were selected based on the findings of the existing literature [14], [15], [26]. Specifically, we selected the variables that were generally used in prior studies and that were found to be significant. We confirmed that each pair of our independent variables had no multicollinearity and that the proportional odds assumption was satisfied.

For RQ3, we explored the participants' concerns about identifying English phishing emails in open-ended questions. Original open-ended comments were collected in participants' native languages and professional translators translated them into English. Two independent coders then rated them through an inductive thematic analysis method, which identifies, analyzes, and reports patterns (themes) within data [59]. The coders practiced rating a subsample of users' responses and discussed differences until they reached a consensus before rating the remainder of

the data. Because participants sometimes provided multiple concerns, we allowed multiple themes per response. Accordingly, we calculated the inter-rater reliability using the Kupper-Hafner statistic [60].

4. Results

In this section, we aim to answer our research questions by analysing the results of our roleplay task and survey questions. We first addressed **RQ1** by studying participants' past experiences of phishing. Next, we addressed **RQ2** by studying participants' behavior toward emails. Then, we addressed **RQ3** by studying participants' confidence and concerns about identifying English phishing emails. This study aims to unveil the differences in participants' behavior and perceptions between their native languages and English. Please note that national or cultural differences are out of our scope (see Section 5.2 for more details).

4.1 RQ1: Experiences with English Phishing Emails

Experience of Receiving Suspicious Emails. **Figure 3** shows the frequencies with which participants received suspicious emails, excluding "I don't know" responses. Although the frequency of receiving suspicious emails was lower in English compared to the participants' native languages in all three countries, at least a quarter of the participants received suspicious emails in English at least once a month. This indicates that NNESs are regularly exposed to or perceive that they are exposed to English phishing emails.

Experience of Being Deceived by Phishing Emails. **Table 3** depicts NNESs' experiences of being deceived by phishing emails. More than 10% of participants in Germany and Korea, and approximately 1.3% in Japan, had been deceived by English phishing emails. The percentage of participants who had been deceived by phishing emails in English was also lower than in their native language. This result may be influenced by the fact that they receive more suspicious emails in their native languages than in English. Among the participants who reported that they had been deceived by English phishing emails, the average number of times of being deceived was 1.7, 1.2, and 1.3 times in Germany, South Korea, and Japan, respectively.

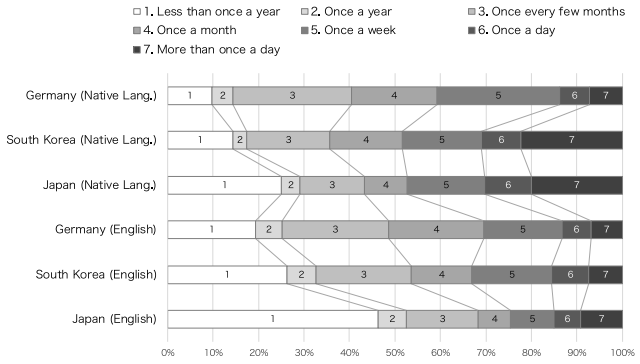

Fig. 3 Frequency of receiving suspicious emails.

Table 3 Percentage of participants who had been deceived by phishing emails.

Country	Native Lang.	English
Germany	25.4%	14.1%
South Korea	14.5%	10.1%
Japan	6.0%	1.3%

Contexts of Phishing Emails. We identify some contexts in which NNESs are likely to be deceived by English phishing emails based on comments from participants who have been deceived. We found that the majority of victims had been deceived by emails from well-known, worldwide services (e.g., PayPal, Amazon, eBay, Apple, and Google). They tended to click on the malicious URLs in security-alert emails without noticing anything strange even when the emails were written in English: "*The email was about my Amazon account. It stated that there was an unusual activity and that because of that, my account had been restricted. I clicked the link in a hurry to check and unblock my account.*" Participants also seem not to be suspicious when worldwide services send emails in English to notify customers of a lottery win or gift offer. Some participants reported that they had been deceived by English phishing emails spoofing international delivery services. NNESs who used international online shopping services or had family and friends living overseas were likely to accept English phishing emails spoofing international delivery services: "*I received an email stating that a package had arrived from overseas but could not be delivered to my home unless I paid the customs duty. My friend sometimes sends me packages, so I clicked the link, thinking that the email was regarding a package from my friend.*" Two participants reported that they had been deceived by English phishing emails spoofing an international-donation organization. Several participants received sophisticated spear-phishing emails written in English, although the number of participants who reported being deceived in such cases was lower than in typical phishing emails. They reported that they had not doubted the emails because it contained the name and email address of an acquaintance, such as a boss or customer (overseas customer).

In the next section (Section 4.2), we explore the differences in users' susceptibility between the contexts of their native languages and English when they actually receive phishing emails.

4.2 RQ2: Behavior toward the Emails

4.2.1 Security-Risk-Prone/Averse Behavioral Tendency

Table 4 shows the percentages of the participants with security-risk-prone/averse behavioral tendencies for each email in our roleplay task (see Table A·1 in Appendix A.2 for more details). In Germany and South Korea, the percentage of participants who engaged in security-risk-prone behaviors was lower in English contexts than in their native language contexts. Especially in South Korea, the difference was large and statistically significant for all three emails ($p < .05$). In contrast, in Japan, more participants engaged in security-risk-prone behavior in English contexts than in Japanese contexts. In all three countries, the percentages of participants who engaged in security-risk-prone behavior in response to the obvious-phishing email (b) with the suspicious URL and to the uncertain email (a) were similar. Participants did not seem to look for and rely on a suspicious URL for their decision-making, although Canfield et al. [53] described it as the most valid cue for identifying phishing emails.

Table 4 Percentage of participants who engaged in security-risk-prone/averse behaviors in our roleplay task.

Behavioral tendency	Country	Language	(a) Uncertain	(b) Obvious phishing	(c) Genuine	(d) Uncertain
Security-risk-prone behavior	Germany	Native	27.1%	30.7%	N/A	53.6%
		English	22.2%	23.6%		45.8%
	South Korea	Native	**41.8%***	**43.3%***		**50.4%***
		English	**25.9%***	**25.2%***		**31.1%***
	Japan	Native	8.8%	8.8%		23.6%
		English	14.3%	14.9%		24.7%
Security-risk-averse behavior	Germany	Native	48.6%	N/A	19.3%	32.1%
		English	61.8%		24.3%	40.3%
	South Korea	Native	**20.6%****		21.3%	30.5%
		English	**41.5%****		28.9%	37.0%
	Japan	Native	44.6%		18.9%	46.6%
		English	56.5%		29.2%	48.7%

Bold font indicates that the difference between the two groups (native language and English) is statistically significant (Chi-square tests). Significance levels are ***p <.001; **p <.01; *p <.05, whose p-values are corrected for multiple testing using the Bonferroni method.

Table 5 Regression analysis for Security-risk-prone/averse behavioral tendencies in English contexts.

Independent variables	Security-risk-prone				Security-risk-averse			
	Coefficients	Std. Err.	p-values		Coefficients	Std. Err.	p-values	
Age group	−.2702	.0814	<.001	***	.2068	.0745	.0055	**
IT professional	.2602	.2555	.3086		−.1440	.2375	.5443	
Confidence in reading English	.2504	.0867	.0039	**	−.3263	.0844	<.001	***
Num. Received English emails	−.0234	.0152	.1245		−.0294	.0159	.0641	
Korean	−.0717	.2362	.7616		−.3981	.1176	.0473	*
Japanese	−.5300	.2794	.0578		.0635	.2068	.7589	

p-values test the hypothesis that coefficients are zero, i.e., independent variables do not affect security-risk-prone/averse behavior. Significance levels are ***p <.001; **p <.01; *p <.05. Security-risk-prone/averse behavior (dependent variables): the number of emails the participants engaged in security-risk-prone/averse behaviors (0 to 3). Age group: 18–29, 30–39, 40–49, 50–59, or ≥60. IT professional: professional or non-professional (we set the non-professional as the baseline). Confidence in reading English: 6-point Likert scale 0 (strongly disagree) to 5 (strongly agree). Culture: Germany, South Korea, or Japan (we set Germany as the baseline).

As Table 4 shows, in all three countries, the percentage of participants who engaged in security-risk-averse behavior was higher for emails in English than for emails in their native languages. For the genuine email (c), which contained no phishing cues, 24–29% of the participants engaged in security-risk-averse behavior in English contexts. We found that the differences in the percentages of participants with security-risk-averse behavior between their native language and English contexts were larger for email (a), which was sent from PayPal, than emails (c) and (d), which were respectively sent from the coworker and company staff. This tendency was common in all three countries. In other words, participants appear more likely to ignore an email from a service with which they have no personal relationship than one from a sender with whom they have an established relationship in English contexts. This result suggests that the expected extent to which relationships are impacted by ignoring emails may be negatively related to security-risk-averse behavior in English contexts.

As shown in **Table 5**, age groups and confidence in reading English had significant effects on participants' security-risk-prone/averse behaviors in English contexts; younger participants with more confidence in reading English were more likely to follow the instructions in obvious-phishing and uncertain emails written in English, and they were also less likely to ignore the instructions in genuine and uncertain emails written in English. The result indicating that factors related to participants' self-perceived English proficiency level significantly affect their behavior toward English emails is consistent with previous phishing studies that examined NNESs [6], [50]. Contrary to the expectations from previous phishing studies [15], [24], [26], IT expertise and the number of received emails did not significantly affect participants' behavior in English contexts. A prior work [61] in language communication reported that NNESs' behavior was more influenced by their self-perceived English fluency than objective English fluency. Our results seems to support that conclusion: confidence in English reading (self-perceived English index) did affect NNESs' behavior more than the number of received English emails (the objective English index relates to familiarity with English).

4.2.2 Participants' Inspection Behaviors

We analyzed the open-ended responses of participants who reported that they would refer to some other information than the screenshot. The most frequent inspection behaviors were the same regardless of whether the participants were shown emails in English or their native language: participants would log in to the website without clicking the link in the email, which is generally recommended as an anti-phishing reaction [62], for emails (a) and (b), and they would ask their coworkers for emails (c) and (d). In all three countries, the percentages of participants who reported that they would use Internet search were higher in their native language environment than in English. In English contexts, 0.4% of German, 4.8% of Korean, and 6.5% of Japanese reported that they would use an online translator (on average of four emails). Please see Appendix A.2 for more details.

4.2.3 Attention to Email Elements

Previous studies found that individual attention to email sources and grammatical errors/misspellings were significantly and negatively related to phishing susceptibility, and that atten-

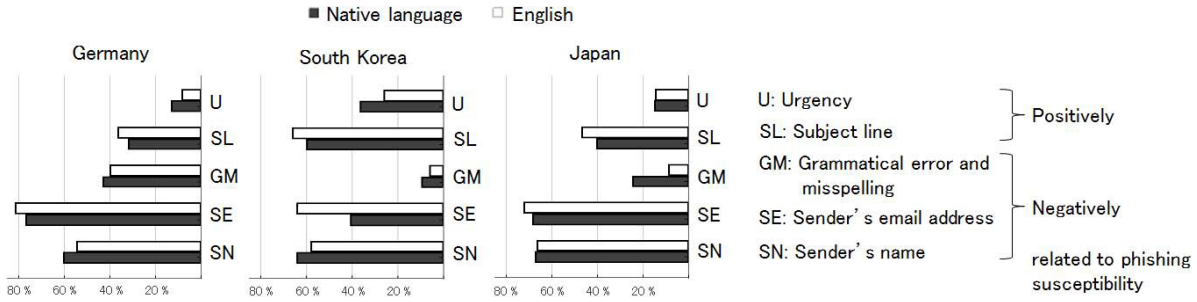

Fig. 4 Email elements to which our participants pay attention.

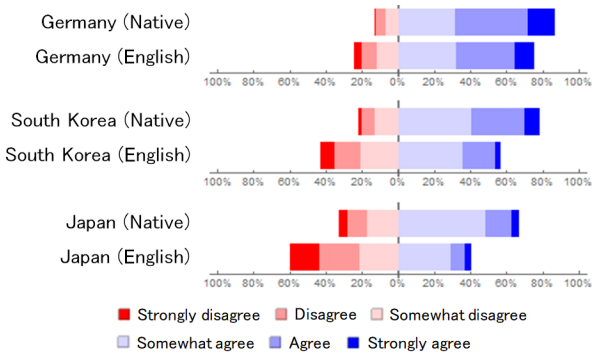

Fig. 5 Participants' confidence in identifying phishing.

tion to urgency cues and subject lines were significantly and positively related to phishing susceptibility [26], [31]. **Figure 4** shows the percentages of the participants who usually paid attention to each email element in their native language and English contexts. Although there were some differences in elements that participants paid attention to between the three countries, we focus on the common differences between their native languages and English. In all three countries, participants paid less attention to grammatical/misspelling errors and more attention to the sender's email addresses and subject lines in English contexts. This indicates that participants tended to rely more on information recognized at a glance to roughly grasp the content and context of the emails in English contexts. We note that excessive reliance on subject lines for phishing identification is risky because they often serve as a lure in phishing emails [26]. In countries with relatively low English proficiency (i.e., Korea and especially Japan), the percentage of participants who focused on grammatical errors and misspellings was markedly lower in English contexts than in native language contexts. This reflects the fact that participants with low confidence in their English reading skills believed that they were unable to detect such errors in English.

4.3 RQ3: Confidence and Concerns about English Phishing Emails

4.3.1 Confidence in Identifying Phishing Emails

Figure 5 shows participants' degree of confidence in identifying phishing emails. The percentages of participants who were not confident in identifying English phishing emails (i.e., answered "strongly disagree" to "somewhat disagree.") were 24.6% (70/284) in Germany, 43.5% (120/276) in Korea, and 60.0% (181/302) in Japan. In all three countries, the percentage of participants who were confident that they can identify phishing was lower in English than in their native language. We conducted a correlation analysis and found that participants' degree of confidence in identifying English phishing emails was positively correlated with their confidence in their English reading skills (Germany $\rho = .378$, $p < .001$; South Korea $\rho = .456$, $p < .001$; Japan $\rho = .452$, $p < .001$). Conversely, following the several previous studies that showed that the participants' confidence in identifying phishing did not explain their phishing identification performance in the native language contexts [52], [63], [64], we also found that confidence in identifying English phishing was not significantly correlated with participants' security-risk-prone/averse behavioral tendencies in English contexts in any of the three countries.

4.3.2 Concerns about Identifying Phishing in English

Of the 862 participants, 371 participants who were not confident in identifying English phishing emails (as described in Section 4.3.1) were asked about their concerns. Since we aimed to explore their specific problems to determine anti-phishing interventions for NNESs, we excluded 144 unclear responses such as "Because I am not good at English." As a result, we conducted thematic analysis of 227 responses and found five main concerns (themes) as shown in **Table 6**. The final inter-rater reliability was 0.84. A value greater than 0.75 is considered to be an excellent level of agreement [65]. Comments from German, South Korean, and Japanese participants are indicated with (G), (K), and (J), respectively. The discussion of each concern follows, and design implications based on these concerns will be presented in Section 5.1.

Difficulty Understanding English Email Content. The majority of participant concerns contained anxiety about identifying English phishing emails because the participants struggled to understand the content of English emails. Comments from such participants indicated that the fundamental cause of this concern is their lack of English skills: "*Because my English skills aren't very good, I can't understand English emails at all*" (J) and "*I'm not good at English. Even when I did roughly understand the email, I couldn't grasp its details in English...*" (J). Especially, older participants expressed strong concerns: "*It's been a long time since I learned English, so I can't read it very well*" (K). As a strategy to address this concern, some participants used an online translator. However, they also complained about its inaccuracy: "*I tried to use an online translator, but unfortunately, its translations aren't very good, and they are sometimes very confusing...*" (K). Participants who felt that they could not understand the English emails admitted that they often ignored them:

Table 6 Five main concerns of participants in identifying English phishing emails.

Concerns	Germany	South Korea	Japan	Total
Difficulty understanding English email content	69.0% (20/29)	84.4% (65/77)	61.2% (74/121)	70.0% (159/227)
Difficulty identifying errors and unnatural language in English	20.7% (6/29)	2.6% (2/77)	21.5% (26/121)	15.0% (34/227)
Unfamiliarity with English phishing emails	6.9% (2/29)	5.2% (4/77)	12.4% (15/121)	9.3% (21/227)
Decreased attention in English contexts	3.4% (1/29)	3.9% (3/77)	11.6% (14/121)	7.9% (18/227)
Difficulty finding similar cases in English on the Internet	0.0% (0/29)	0.0% (0/77)	5.8% (7/121)	3.1% (7/227)

Note that a single participant may have mentioned multiple concerns. Please also note that because we asked participants with the open-ended question, we cannot conclude that the participants who did not mention a particular concern in our study were not concerned about it.

"*Since I can't read English, I usually just ignore English emails*" (J). This is typical security-risk-averse behavior and can certainly prevent English phishing emails, but such biased behavior also creates a risk of opportunity loss by inhibiting communication in English. We conclude that NNESs need support to reduce two distinct risks: English phishing emails and opportunity loss of English communication.

Difficulty Identifying Errors and Unnatural Language in English. Baki et al. [19] found that users generally investigated such language information as writing styles and grammar to identify phishing emails. However, our participants believed that they could not adopt this strategy for emails in English: "*For Japanese emails, I can obviously identify incongruities caused by grammar, nuances, and honorific expressions. However, in English, although I can understand the surface contents of emails, I cannot grasp any language nuances*" (J). Indeed, the result of Section 4.2.3 shows that participants paid less attention to grammatical errors and misspellings in English contexts. This concern is not a simple problem because many participants mentioned not only errors in sentences but subtle unnatural nuances in the language. Participants believed that they needed a high level of English knowledge to overcome this concern: "*Phishing emails are not always obvious. Further English knowledge is necessary to more certainly recognize them*" (G).

Unfamiliarity with English Phishing Emails. Sheng et al. [15] reported that the participants with a high degree of prior exposure to anti-phishing education (i.e., familiarity with phishing) were significantly less susceptible to phishing. However, participants were concerned about their unfamiliarity with English phishing emails: "*... I'm not familiar with the formats and patterns of English phishing emails*" (J) and "*... Compared to Korean ones, English phishing emails are more varied and sneaky, which increases the odds that they will be confusing*" (K). A participant noted the difference in the amount of experience receiving phishing emails written in their native language and those in English as well as the amount that can be learned from familiar media: "*I think that there is a general type of phishing email that is written in Korean. It's an advantage to experience more phishing emails in Korean than similar emails in English. All kinds of media deal with (Korean) phishing emails, so there are more chances to figure out if it's phishing compared to those in English...*" (K).

Decreased Attention in English contexts. Although it is evident that users' attention is essential to identify phishing emails, several participants were concerned that their attention would be reduced in reading English emails: "*... I can't understand the contents of English emails. Thus, I practically panic and worry that I won't make the right decision when I receive it*" (J), and "*Since I can't read English, I blindly open a phishing email to understand the contents*" (J). These concerns reflect security-risk-prone behaviors of NNESs. One participant noted that their attention was decreased because the language of the URLs is English.: "*... If Korean emails provide a link, since its language is different, I might not click on it because it looks different. But for English emails, since the contents are in English and the link is also English, it does not stand out so much. Therefore, I might click on the link more easily than in Korean emails*" (K). It seems to be unique to NNESs to focus on the discrepancy between the languages used in the body of the email and the link (i.e., URL that can use Unicode) respectively, however English emails do not have this feature, suggesting that it is not an effective behavior against English phishing emails.

Difficulty Finding Similar Cases in English on the Internet. In our roleplay task, some participants told us that they used Internet search engines to find similar cases of received suspicious emails in their native language contexts. This means searching on the Internet is an important strategy for identifying phishing emails. However, participants mentioned that they encountered a problem when they searched for similar cases in English: "*When I Google the text of a phishing email in Japanese, I can see if it is phishing by viewing the posted experiences by people who received a similar email. However, for English, I cannot see if it is phishing because it's difficult for me to read the contents of websites from a Google search*" (J); and "*... Even if I can search websites related to the phishing email, it is difficult to determine which information is correct in English contexts*" (J). This matches the findings of Chu et al. [49], [66] who reported that NNESs struggle when viewing and skimming online search results. Although only few participants mentioned this concern (3.1%), we infer that participants who mentioned that they struggled to understand the content of English emails (70.0%) would also have difficulty when searching for similar cases.

On the other hand, the following are three main reasons collected from participants who were confident in identifying English phishing emails: their attention improves due to a lack of opportunities to receive English emails in their daily life, they can read the elements needed to identify phishing in English, and they believe the mailer and in-house system will detect it. However, regarding the mailer and in-house system, one participant reported that such systems make decisions that lead to lost opportunities: "*Since distinguishing between good and phishing emails is often difficult, you often automatically anticipate phishing or spam in the case of English emails. So sometimes an important email might easily get lost*" (G).

5. Discussion

In a society where native and non-native speakers coexist, it is desirable that there is a minimal discrepancy in communication between native and non-native speakers. The capability of non-native speakers to respond appropriately to emails written in English is a typical example; that is, NNESs are expected to be able to read and understand genuine emails, while correctly ignoring phishing emails even when they are written in English. Through our experiments, we found that NNESs were more prone to engaging in undesirable behaviors when they handled English emails, whether phishing or genuine, and that this tendency varied across countries. We also found that NNESs could not adopt their strategies for identifying phishing emails written in their native languages for English phishing emails. Specifically, they had difficulty in identifying errors and unnatural language and searching similar cases in English contexts. In this section, we first discuss the design implications that aim at supporting NNESs in taking the appropriate action when they need to deal with an email written in English. We then discuss the limitations and future extensions of our study.

5.1 Design Implications

Our findings suggest the need to develop assistive technologies to help NNESs handle English emails correctly. In this section, we present specific design implications (**D1**–**D4**) based on our findings. We also discuss their effectiveness and limitations.

D1: Language-agnostic phishing knowledge base. As a strategy for identifying phishing emails written in their native language, some participants reported that they use Internet search engines to obtain information about similar phishing cases, as shown in Section 4.2.2. At the same time, they raised a concern that it would be difficult to take the same approach for identifying English phishing emails, as we derived in Section 4.3.2 – Difficulty Finding Similar Cases in English on the Internet. The common challenges derived from our participants' comments and previous studies of information searches in non-native language [49], [66], [67] are as follows. First, for NNESs, obtaining information in English is a difficult task. Second, even when they find correct information in English, they may not be able to interpret it correctly. Moreover, it is not straightforward for NNESs to ascertain the reliability of information sources. Based on these observations, we propose to develop a *phishing knowledge base*, which (1) is operated by a globally authorized, neutral organization such as an international standardization organization, (2) collects and maintains phishing cases in various languages, and (3) provides *language-agnostic notations* so that NNESs can understand the phishing content. As a previous study on the design of a security indicator implies [68], adopting graphical notations would be effective for solving this problem.

D2: Auto follow-up mechanism Our survey revealed that some NNESs tended to engage in security-risk-averse behavior primarily because the email was written in English, as described in Section 4.2.1. While this behavior may help to reduce the threat of phishing, it could lead to the increase of the risk of losing important opportunities by ignoring all incoming emails written in English. We believe that introducing an auto follow-up mechanism is useful in solving this problem. Gmail [69] has adopted a functionality to provide both an email sender and recipient with a quick reminder that nudges them to follow-up or respond to a potentially important email. For instance, the Gmail inbox displays the message "Received *X* days ago. Reply?" for the receiver and "Sent *X* days ago. Follow up?" for the sender.

D3: Training on anti-phishing emails for NNESs Some participants reported that they were confident in identifying phishing emails written in their native language, but it was difficult for them to identify phishing emails written in English because they were unfamiliar with the patterns of English phishing emails, as shown in Section 4.3.2 – Unfamiliarity with English Phishing Emails. They also reported a concern that their attention was reduced when reading English emails compared to reading their native language emails. One promising strategy to solve such a problem is to provide training. As previous studies have reported, providing a training program is known to be effective in encouraging appropriate action toward received emails, which could contain phishing [15], [70], [71]. Participants in the training program can learn what to watch for in an email and the intrinsic wording to help them identify a phishing message. There are no studies that have shown that important points for identifying phishing emails, e.g., the domain name of a URL in the email, vary greatly across languages. Therefore, it may seem that it is sufficient for non-English speakers to take phishing training in their native language. However, the essential elements in identifying phishing emails are not only the technical points such as domain names in URLs, but also the correct understanding of the content and context of the email, which must be learned through specific examples in English. Therefore, it is desirable for NNESs to participate in English Phishing training. Moreover, because our regression analysis revealed that confidence in English reading increases security-risk-prone behaviors, we believe that English language lessons alone would not be sufficient and that specialized English phishing training for NNESs would be needed. Assessing the effectiveness of such an educational approach is a challenge for the future.

D4: Machine translation as an assistive tool. Machine translation (MT) services are expected to help NNESs with concerns about their inability to understand English emails, as mentioned in Section 4.3.2 – Difficulty Identifying Errors and Unnatural Language in English. In recent years, the accuracy of MT as well as existing MT services, such as DeepL [72] and Google Translate [73], which are known to generate very natural translations, has improved drastically due to advances in deep learning technology. In fact, many participants mentioned that they relied on MT services when they needed to read emails in English. As it is expected that the quality of MT technology will continue to improve in the future, adoption of MT as an assistive tool could help NNESs identify English phishing emails.

MT is expected to provide the advantages mentioned above; however, the advancement of MT may raise two new concerns: (i) it could interfere with the commonly used phishing identification practice, i.e., detecting grammatical typos/errors in phishing emails, and (ii) if the phishing email sender uses advanced

MT and sends the translated phishing emails written in the recipient's native language, the recipients could be fooled by phishing scams because the emails are written with natural text in their native languages. These observations imply that the strategy that many participants use to fight against phishing emails, i.e., detecting grammatical typos/errors, will no longer be promising in the future. As MT technology improves, strategies for identifying phishing emails that rely solely on grammatical errors should be avoided, and other essential features associated with phishing should be considered.

Because NNESs' concerns in identifying English phishing were not specific to a particular language/culture, we believe the above design implications are generalizable to non-native speakers of other languages.

5.2 Limitations and Future Work

While our survey provides much insight into the challenges faced by NNESs when they receive English emails, there are several limitations.

The purpose of this study was to examine how language barriers impact users' susceptibility to phishing emails. The reason we recruited participants from three countries varying in English proficiency was not to compare cultural effects but to confirm the robustness of our findings. However, in addition to language, cultural differences may have influenced the results of this study. Sawaya et al. [42] and Harbach et al. [44] examined "active" attitudes for the secure use of devices or services (e.g., updating software, strengthening passwords, and locking smartphones) and reported that the Japanese participants exhibited less secure behavior compared with participants from other countries. We cannot conclude that those results are inconsistent with our result indicating that Japanese participants are less likely to engage in security-risk-prone behavior, as shown in Table 4. People's behavior may vary depending on the context, thus our work focused on revealing behavioral tendencies in the context of phishing email. Furthermore, demographic differences may have influenced the results of this study. The high proportion of IT professionals among German participants may have influenced our survey results, although our regression analysis revealed that IT expertise did not significantly affect participants' security-risk-prone/averse behaviors. The different types of prior training provided in each country also may have influenced the participants' behaviors. It is complicated to conduct a survey of susceptibility to phishing emails that completely separates the effects of language from the effects of cultural and demographic differences. To reduce such effects, we adopted a between-subjects design for each country instead of directly comparing participants' results per country in our roleplay task.

Through our user study, we tested whether participants were willing to follow the instructions (i.e., clicking on the links or opening the attachment files) in the phishing emails. However, after accessing a website in an actual phishing attack, users may see an alerting security indicator and realize that the website is a phishing website, and the attack may not be successful. This study did not take such cases into account. To determine the likelihood of NNESs falling victim to a phishing attack, it is necessary to observe the overall decision-making process of NNESs after reading a phishing email written in English and visiting a website. The "natural" contexts in which NNESs receive an email in English depend on their work and life, and accurately replicating it in roleplay task is difficult. Conducting user studies with more strict ecological validity is a challenge for future research. In addition, further research is needed to investigate NNESs' behavior when they receive more sophisticated spear-phishing emails that are highly aligned with their personal contexts.

6. Conclusion

Through our scenario-based roleplay task, we showed how non-native English speakers (NNESs) adopted security-risk-prone/averse strategies toward emails in their native language and English. Specifically, we found that participants adopted more security-risk-averse behaviors (i.e., ignoring emails without careful inspection) when the emails were written in English rather than in their native languages. In addition, our qualitative analysis of their open-ended answers revealed five main concerns in identifying English phishing emails: difficulty understanding email content, difficulty identifying errors and unnatural language, unfamiliarity with phishing emails, decreased attention, and difficulty finding similar cases. Our findings bring the unique insight that NNESs may have different concerns and strategies for avoiding phishing emails. It indicates the importance of considering language barriers when designing interventions to support people in combating phishing attacks. Implementing specific anti-phishing interventions for NNESs based on our findings is an important research effort to reduce communication difficulties between native and non-native English speakers.

References

[1] Hasegawa, A.A., Yamashita, N., Akiyama, M. and Mori, T.: Why They Ignore English Emails: The Challenges of Non-Native Speakers in Identifying Phishing Emails, *Proc. 17th Symposium on Usable Privacy and Security*, *SOUPS'21* (2021).

[2] Das, A., Baki, S., Aassal, A.E., Verma, R. and Dunbar, A.: SoK: A Comprehensive Reexamination of Phishing Research From the Security Perspective, *IEEE Communications Surveys & Tutorials*, Vol.22, No.1, pp.671–708 (2020).

[3] Shaikh, A.N., Shabut, A.M. and Hossain, M.: A literature review on phishing crime, prevention review and investigation of gaps, *Proc. 10th International Conference on Software, Knowledge, Information Management & Applications*, *SKIMA'16* (2016).

[4] Verizon: 2020 Data Breach Investigations Report (2020), available from ⟨https://enterprise.verizon.com/resources/reports/dbir/⟩ (accessed 2020-06-17).

[5] Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X.: Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, arXiv preprint arXiv:2006.11929 (2020).

[6] Alseadoon, I.M., Ramadan, R.A. and Khedr, A.Y.: Cultural impact on Users' Ability to protect themselves against Phishing websites, *International Journal of Computer Science and Network Security*, Vol.17, No.11 (2017).

[7] Takano, Y. and Noda, A.: A temporary decline of thinking ability during foreign language processing, *Journal of Cross-Cultural Psychology*, Vol.24, No.4, pp.445–462 (1993).

[8] Rear, D.: The language deficit: A comparison of the critical thinking skills of Asian students in first and second language contexts, *Asian-Pacific Journal of Second and Foreign Language Education*, Vol.2, No.13 (2017).

[9] Ross, S.A.: Some stronger measures of risk aversion in the small and the large with applications, *Econometrica: Journal of the Econometric Society*, pp.621–638 (1981).

[10] Keysar, B., Hayakawa, S.L. and An, S.G.: The foreign-language ef-

fect: Thinking in a foreign tongue reduces decision biases, *Psychological science*, Vol.23, No.6, pp.661–668 (2012).
[11] Costa, A., Foucart, A., Arnon, I., Aparici, M. and Apesteguia, J.: "Piensa" twice: On the foreign language effect in decision making, *Cognition*, Vol.130, pp.236–254 (2013).
[12] Web Technology Surveys: Usage statistics of content languages for websites (2021), available from ⟨https://w3techs.com/technologies/overview/content_language⟩ (accessed 2021-02-25).
[13] First, E.E.: EF English Proficiency Index (2019), available from ⟨https://www.ef.com/wwen/epi/⟩ (accessed 2020-06-13).
[14] Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B. and Laskey, K.: Experimental Investigation of Demographic Factors Related to Phishing Susceptibility, *Proc. 53rd Hawaii International Conference on System Sciences*, *HICCS'20* (2020).
[15] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J.: Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions, *Proc. 2010 SIGCHI Conference on Human Factors in Computing Systems*, *CHI'10* (2010).
[16] Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T. and Ebner, N.: Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing, *Proc. 2017 CHI Conference on Human Factors in Computing Systems*, *CHI'17* (2017).
[17] Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F.: Social phishing, *Comm. ACM*, Vol.50, No.10, pp.94–100 (2007).
[18] Halevi, T., Memon, N. and Nov, O.: Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks, *SSRN Electronic Journal* (2015).
[19] Baki, S., Verma, R., Mukherjee, A. and Gnawali, O.: Scaling and effectiveness of email masquerade attacks: Exploiting natural language generation, *Proc. 2017 ACM on Asia Conference on Computer and Communications Security*, *AsiaCCS'17* (2017).
[20] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C.: Phishing for the truth: A scenario-based experiment of users' behavioural response to emails, *Proc. 28th IFIP TC 11 International Information Security and Privacy Conference*, *IFIP SEC'13* (2013).
[21] Butavicius, M., Parsons, K., Pattinson, M. and McCormac, A.: Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails, *Proc. 26th Australasian Conference on Information Systems*, *ACIS'15* (2015).
[22] Moody, G.D., Galletta, D.F. and Dunn, B.K.: Which phish get caught? An exploratory study of individuals' susceptibility to phishing, *European Journal of Information Systems*, Vol.26, No.6, pp.564–584 (2017).
[23] Butavicius, M.A., Parsons, K., Pattinson, M.R., McCormac, A., Calic, D. and Lillie, M.: Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture, *Proc. 11th International Symposium on Human Aspects of Information Security & Assurance*, *HAISA'17* (2017).
[24] Flores, W.R., Holm, H., Nohlberg, M. and Ekstedt, M.: Investigating personal determinants of phishing and the effect of national culture, *Information & Computer Security*, Vol.23, pp.178–199 (2015).
[25] Harrison, B., Svetieva, E. and Vishwanath, A.: Individual processing of phishing emails, *Online Information Review*, Vol.40, No.2, pp.265–281 (2016).
[26] Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R.: Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model, *Decision Support Systems*, Vol.51, No.3, pp.576–586 (2011).
[27] Parsons, K., Butavicius, M., Pattinson, M., Calic, D., Mccormac, A. and Jerram, C.: Do users focus on the correct cues to differentiate between phishing and genuine emails?, *Proc. 26th Australasian Conference on Information Systems*, *ACIS'15* (2015).
[28] Downs, J.S., Holbrook, M.B. and Cranor, L.F.: Decision strategies and susceptibility to phishing, *Proc. 2nd Symposium on Usable Privacy and Security*, *SOUPS'06* (2006).
[29] Albakry, S., Vaniea, K. and Wolters, M.K.: What is This URL's Destination? Empirical Evaluation of Users' URL Reading, *Proc. 2020 CHI Conference on Human Factors in Computing Systems*, *CHI'20* (2020).
[30] Reynolds, J., Kumar, D., Ma, Z., Subramanian, R., Wu, M., Shelton, M., Mason, J., Stark, E. and Bailey, M.: Measuring Identity Confusion with Uniform Resource Locators, *Proc. 2020 CHI Conference on Human Factors in Computing Systems*, *CHI'20* (2020).
[31] Wang, J., Herath, T., Chen, R., Vishwanath, A. and Rao, H.R.: Phishing susceptibility: An investigation into the processing of a targeted spear phishing email, *IEEE Trans. Professional Communication*, Vol.55, No.4, pp.345–362 (2012).
[32] Wash, R.: How experts detect phishing scam emails, *Proc. 23rd ACM Conference on Computer-Supported Cooperative Work and Social Computing*, *CSCW'20* (2020).
[33] Wash, R., Nthala, N. and Rader, E.: Knowledge and Capabilities that Non-Expert Users Bring to Phishing Detection, *Proc. 17th Symposium on Usable Privacy and Security*, *SOUPS'21* (2021).
[34] Cialdini, R.B.: *Influence: The psychology of persuasion* (1984).
[35] Williams, E.J., Hinds, J. and Joinson, A.N.: Exploring susceptibility to phishing in the workplace, *International Journal of Human-Computer Studies*, Vol.120, pp.1–13 (2018).
[36] Van Der Heijden, A. and Allodi, L.: Cognitive triaging of phishing attacks, *Proc. 28th USENIX Security Symposium*, *SEC'19* (2019).
[37] Greene, K.K., Steves, M.P., Theofanos, M.F. and Kostick, J.: User context: an explanatory variable in phishing susceptibility, *Proc. 2018 Workshop on Usable Security*, *USEC'18* (2018).
[38] Hassandoust, F., Singh, H. and Williams, J.E.: How Contextualisation Affects the Vulnerability of Individuals to Phishing Attempts, *Proc. 23th Pacific Asia Conference on Information Systems*, *PACIS'19* (2019).
[39] Holm, H., Flores, W.R., Nohlberg, M. and Ekstedt, M.: An empirical investigation of the effect of target-related information in phishing attacks, *Proc. 11th IEEE International Enterprise Distributed Object Computing Conference Workshops and Demonstrations* (2014).
[40] Lin, T., Capecci, D.E., Ellis, D.M., Rocha, H.A., Dommaraju, S., Oliveira, D.S. and Ebner, N.C.: Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content, *ACM Trans. Computer-Human Interaction* (*TOCHI*), Vol.26, No.5, pp.1–28 (2019).
[41] Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R.: Future directions for behavioral information security research, *Computers & Security*, Vol.32, pp.90–101 (2013).
[42] Sawaya, Y., Sharif, M., Christin, N., Kubota, A., Nakarai, A. and Yamada, A.: Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior, *Proc. 2017 CHI Conference on Human Factors in Computing Systems*, *CHI'17* (2017).
[43] Mori, K., Watanabe, T., Zhou, Y., Hasegawa, A.A., Akiyama, M. and Mori, T.: Comparative Analysis of Three Language Spheres: Are Linguistic and Cultural Differences Reflected in Password Selection Habits?, *Proc. 2019 IEEE European Workshop on Usable Security*, *EuroUSEC'19* (2019).
[44] Harbach, M., De Luca, A., Malkin, N. and Egelman, S.: Keep on lockin' in the free world: A multi-national comparison of smartphone locking, *Proc. 2016 CHI Conference on Human Factors in Computing Systems*, *CHI'16* (2016).
[45] Redmiles, E.M.: "Should I Worry" A Cross-Cultural Examination of Account Security Incident Response, *Proc. 2019 IEEE Symposium on Security and Privacy*, *S&P'19* (2019).
[46] Hofstede, G.: National cultures in four dimensions: A research-based theory of cultural differences among nations, *International Studies of Management & Organization*, Vol.13, No.1-2, pp.46–74 (1983).
[47] Tembe, R., Zielinska, O., Liu, Y., Hong, K.W., Murphy-Hill, E., Mayhorn, C. and Ge, X.: Phishing in international waters: exploring cross-national differences in phishing conceptualizations between Chinese, Indian and American samples, *Proc. 2014 Symposium and Bootcamp on the Science of Security*, *HotSoS'14* (2014).
[48] Volk, S., Köhler, T. and Pudelko, M.: Brain drain: The cognitive neuroscience of foreign language processing in multinational corporations, *Journal of International Business Studies*, Vol.45, No.7, pp.862–885 (2014).
[49] Chu, P., Komlodi, A. and Rózsa, G.: Online search in english as a non-native language, *The Association for Information Science and Technology*, Vol.52, No.1, pp.1–9 (2015).
[50] Kävrestad, J., Pettersson, R. and Nohlberg, M.: The language effect in phishing susceptibility, *Proc. 6th International Workshop on Socio-Technical Perspective in IS Development*, *STPIS'20* (2020).
[51] Lastdrager, E., Gallardo, I.C., Hartel, P. and Junger, M.: How effective is anti-phishing training for children?, *Proc. 13th Symposium on Usable Privacy and Security*, *SOUPS'17* (2017).
[52] Nicholson, J., Coventry, L. and Briggs, P.: Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection, *Proc. 13th Symposium on Usable Privacy and Security*, *SOUPS'17* (2017).
[53] Canfield, C.I., Fischhoff, B. and Davis, A.: Quantifying phishing susceptibility for detection and behavior decisions, *Human Factors*, Vol.58, No.8, pp.1158–1172 (2016).
[54] Canfield, C., Davis, A., Fischhoff, B., Forget, A., Pearman, S. and Thomas, J.: Replication: Challenges in using data logs to validate phishing detection ability metrics, *Proc. 13th Symposium on Usable Privacy and Security*, *SOUPS'17* (2017).
[55] Rajivan, P. and Gonzalez, C.: Creative persuasion: A study on adversarial behaviors and strategies in phishing attacks, *Frontiers in Psychology*, Vol.9, p.135 (2018).
[56] MillerSmiles.co.uk: MillerSmiles.co.uk (2003), available from ⟨http://

www.millersmiles.co.uk/⟩ (accessed 2020-06-18).
[57] Steves, M.P., Greene, K.K. and Theofanos, M.F.: A Phish Scale: Rating Human Phishing Message Detection Difficulty, *Proc. 2019 Workshop on Usable Security*, *USEC'19* (2019).
[58] Macromill: Macromill (2000), available from ⟨https://group.macromill.com/⟩ (accessed 2020-06-13).
[59] Braun, V. and Clarke, V.: Using thematic analysis in psychology, *Qualitative Research in Psychology*, Vol.3, No.2, pp.77–101 (2006).
[60] Kupper, L.L. and Hafner, K.B.: On assessing interrater agreement for multiple attribute responses, *Biometrics*, pp.957–967 (1989).
[61] Neeley, T.: Language Matters: Status Loss and Achieved Status Distinctions in Global Organizations, *Journal of Organization Science*, Vol.24, No.2, pp.476–497 (2013).
[62] Mossano, M., Vaniea, K., Aldag, L., Düzgün, R., Mayer, P. and Volkamer, M.: Analysis of publicly available anti-phishing webpages: Contradicting information, lack of concrete advice and very narrow attack vector, *Proc. 5th European Workshop on Usable Security*, *EuroUSEC'20* (2020).
[63] Dhamija, R., Tygar, J.D. and Hearst, M.: Why phishing works, *Proc. 2006 SIGCHI Conference on Human Factors in Computing Systems*, *CHI'06* (2006).
[64] Hong, K.W., Kelley, C., Tembe, R., Murphy-Hill, E. and Mayhorn, C.: Keeping Up With The Joneses: Assessing Phishing Susceptibility in an Email Task, *Proc. Human Factors and Ergonomics Society Annual Meeting*, Vol.57, pp.1012–1016 (2013).
[65] Fleiss, J.L., Levin, B., Paik, M.C., et al.: The measurement of interrater agreement, *Statistical methods for rates and proportions*, Vol.2, No.212-236, pp.22–23 (1981).
[66] Chu, P., Jozsa, E., Komlodi, A. and Hercegfi, K.: An Exploratory Study on Search Behavior in Different Languages, *Proc. 4th Information Interaction in Context Symposium*, *IIIX'20* (2012).
[67] Young, A.L., Komlodi, A., Rózsa, G. and Chub, P.: Evaluating the Credibility of English Web Sources as a Foreign-Language Searcher, *The Association for Information Science and Technology*, Vol.53, No.1, pp.1–9 (2016).
[68] Felt, A.P., Reeder, R.W., Ainslie, A., Harris, H., Walker, M., Thompson, C., Acer, M.E., Morant, E. and Consolvo, S.: Rethinking Connection Security Indicators, *Proc. 20th Symposium on Usable Privacy and Security*, *SOUPS'16* (2016).
[69] Google Workspace Center: 7.3 Remember to follow up (2020), available from ⟨https://support.google.com/a/users/answer/9259771#7.3⟩ (accessed 2020-09-17).
[70] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A. and Pham, T.: School of Phish: A Real-World Evaluation of Anti-Phishing Training, *Proc. 5th Symposium on Usable Privacy and Security*, *SOUPS'09* (2009).
[71] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E.: Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish, *Proc. 3rd Symposium on Usable Privacy and Security*, *SOUPS'07* (2007).
[72] DeepL: DeepL Translate (2020), available from ⟨https://www.deepl.com/translator⟩ (accessed 2020-09-17).
[73] Google: Google Translate (2020), available from ⟨https://translate.google.com/⟩ (accessed 2020-09-17).

Appendix

A.1 Questionnaire

Each participant read and answered the questionnaire in their native language. Participants were randomly assigned to a group where they were shown emails written in their native language or English. One asterisk (*) indicates that the sentences were arranged by the participant's country: Germany, South Korea, or Japan. Double asterisks (**) indicate that the sentences were dynamically arranged according to the participant's preceding answers.

Screening survey

Survey Title: Survey of emails written in German/Korean/Japanese* or English.

Number of questions: 5 in the screening survey and 17 in the main survey (time required: about 25 minutes).

Participation compensation: 4 EUR / 5500 KRW / 500 JPY (for those who participated in the main survey)

Data handling: This questionnaire is conducted anonymously. Responses to it will be used for academic research. The aggregated results of the answers to the multiple choice questions will be published in an academic journal, and the answers to the open-ended questions may be published in an academic journal with a non-personally identifiable form. The answers will be provided to requesting organizations, and translations may be outsourced to a third party. The answers will be protected as confidential information.

Note: This survey has several open-ended questions. To help us improve the quality of our research, please be as specific as possible about your opinions. This survey also includes several image-based questions.

I agree with the above information and agree to participate in this survey.

- ○ Yes, I agree with the above statement and I will participate in this survey.
- ○ No.

Q01. How old are you?

- ○ 18–29 years old
- ○ 30–39 years old
- ○ 40–49 years old
- ○ 50–59 years old
- ○ 60 years or older
- ○ Prefer not to answer

Q02. What is your gender (self-identified gender)?

- ○ Male
- ○ Female
- ○ Other
- ○ Prefer not to answer

Q03. Which of the following best describes your current occupational status? Please select the most applicable answer.

- ○ Work (full-time)
- ○ Work (part-time)
- ○ Student
- ○ Unemployed or retired (including homemaker)

Q04. This question is designed to verify that you have read the question carefully.
Please select both "No" and "Other".

- □ Yes
- □ No
- □ Other
- □ Prefer not to answer

Q05. What is your native language (the language you primarily spoke before you were 10 years old)?

- ○ German/Korea/Japanese*
- ○ English
- ○ Other

Main survey

Q01. Are you an expert in the fields of information technology (IT), computer engineering, or computer science?
- ○ Yes
- ○ No

Q02. Which of the following best describes your highest achieved education level? Please select the most applicable answer.
- ○ Some high school
- ○ High school graduate
- ○ Some college, no degree
- ○ Associate's degree
- ○ Bachelor's degree
- ○ Graduate degree
- ○ Other
- ○ Prefer not to answer

Q03. How confident are you in your ability to read English? Please select the most applicable answer.
- ○ Very unconfident
- ○ Unconfident
- ○ Somewhat unconfident
- ○ Somewhat confident
- ○ Confident
- ○ Very confident

Q04. How many years have you studied English in total, including self-study? Please round your answer down to the nearest whole number.
( ) years

Q05. How many emails (both work-related and personal) do you receive on average on a typical weekday? Please include auto-send emails. If you receive less than one email a day on average, answer "0".
Emails written in German/Korean/Japanese*: ( )
Emails written in English: ( )

From here, you will answer by looking at email screenshots. Answer by looking at the screenshots without actually searching or accessing the information in them. The recipient of the following email is Max Mustermann / Hong Gil-dong / Taro Yamada*. Please answer questions 6–9 as if you were Max Mustermann / Hong Gil-dong / Taro Yamada*.

Profile of Max Mustermann / Hong Gil-dong / Taro Yamada*
- · Name: Mr. Max Mustermann / Hong Gil-dong / Taro Yamada*
- · Country of residence: Germany / South Korea / Japan*
- · Occupation: office worker
- · Employer: ABC Company
- · Boss: Erika Müller (erika.mueller@abccompany.com) / Hong Gil-soon (gilsoon.hong@abccompany.com) / Hanako Tanaka (hanako.tanaka@abccompany.com)*
- · Email address of IT service department: it-service@abccompany.com
- · Online services he uses:
  - – PayPal
    - ∗ Online payments service. He uses this service for private online shopping. He registered his private email address and his credit card information with this service.
  - – LinkedIn
    - ∗ Online networking services. He uses this service to build his network. He registered his private email address with this service.
  - – Zoom
    - ∗ Video conferencing service. He uses this service for working from home. He registered his business email address with this service.

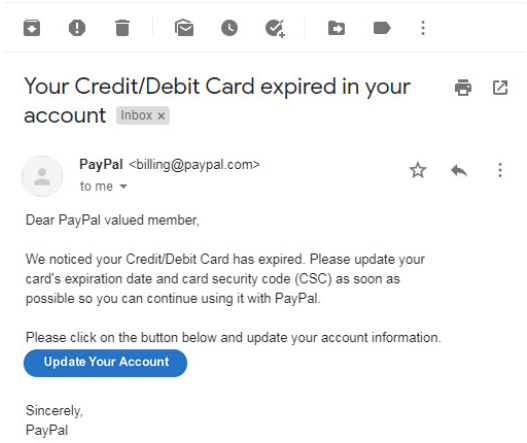

Fig. A·1 Email (a).

Email (a): An email sent to a private email address (see **Fig. A·1**).

Q06. How would you respond if you received email (a)?
- ○ I'd ignore it without referring to any other information than this screenshot.
- ○ I'd follow its instruction without referring to any other information than this screenshot.
- ○ I'd refer to some other information than this screenshot to decide how to respond.
  Please specify. ( )
- ○ Other
  Please specify. ( )

Email (b): An email sent to a private email address (see **Fig. A·2**).

Q07. How would you respond if you received email (b)?
- ○ I'd ignore it without referring to any other information than this screenshot.
- ○ I'd follow its instruction without referring to any other information than this screenshot.
- ○ I'd refer to some other information than this screenshot to decide how to respond.
  Please specify. ( )
- ○ Other
  Please specify. ( )

Email (c): An email sent to a business email address (see **Fig. A·3**).

Q08. How would you respond if you received email (c)?
- ○ I'd ignore it without referring to any other information than this screenshot.

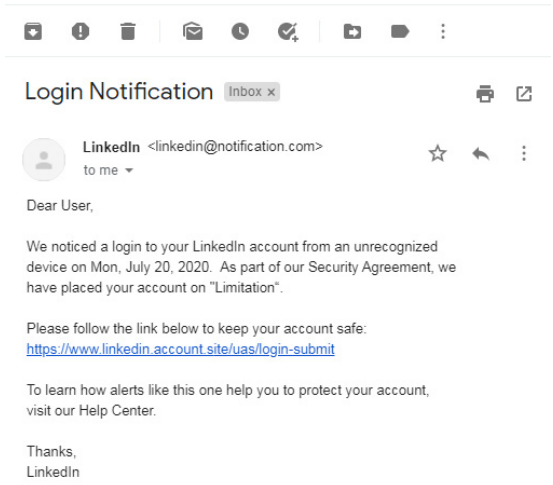

Fig. A·2 Email (b).

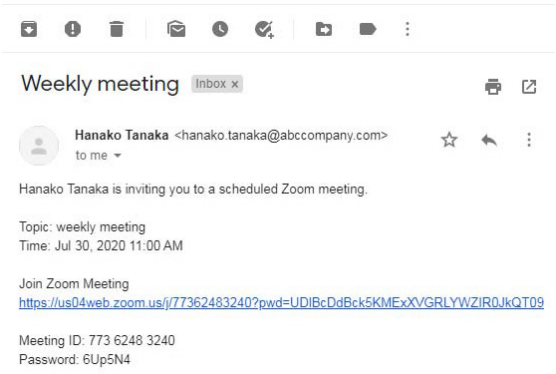

Fig. A·3 Email (c).

- I'd follow its instruction without referring to any other information than this screenshot.
- I'd refer to some other information than this screenshot to decide how to respond.
  Please specify. ( )
- Other
  Please specify. ( )

Email (d): An email sent to a business email address (see **Fig. A·4**).

Q09. How would you respond if you received email (d)?

- I'd ignore it without referring to any other information than this screenshot.
- I'd follow its instruction without referring to any other information than this screenshot.
- I'd refer to some other information than this screenshot to decide how to respond.
  Please specify. ( )
- Other
  Please specify. ( )

Q10. When you receive an email written in English/German/Korean/Japanese* [*4], to which parts do you usually pay attention?

[*4] We displayed the language which corresponded with the emails that the participant was presented in Q06–Q09.

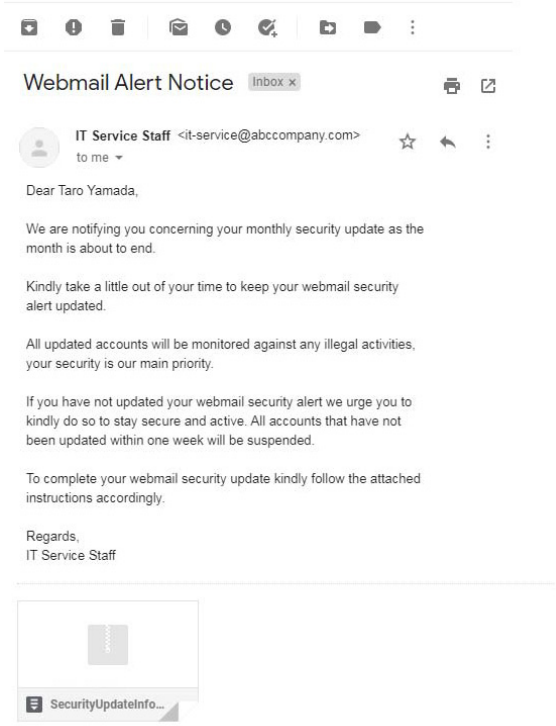

Fig. A·4 Email (d).

Choose the three items from the list below to which you pay the most attention.

- □ Sender's name
- □ Sender's email address
- □ Subject line
- □ Grammatical errors/misspellings in the language
- □ Formality of language
- □ Urgency of message
- □ Your involvement with the email
- □ URLs
- □ Attachment file

Q11. This question is designed to verify that you have carefully read the question.
Please select both "No" and "Prefer not to answer".

- □ Yes
- □ No
- □ Other
- □ Prefer not to answer

From here, we will ask about your experience and perception of phishing. Phishing is online fraud that acquires sensitive information primarily by masquerading as a legitimate business or a reputable person.

Q12. How often do you receive both work-related and personal emails that are assumed to be phishing? Do not include phishing-training emails from your company. Please select the most applicable answer.
Phishing emails written in German/Korean/Japanese*:

- Less than once a year
- Once a year
- Once every few months
- Once a month

Table A·1 Detailed results of the roleplay task.

			N	% Ignore	% Follow	Other				
						% Check the website without a link	% Ask a related person	% Internet search engine	% Online translator	% Other
(a)	Native	Germany	140	48.6%	27.1%	17.1%	0.0%	2.1%	0.0%	5.0%
		South Korea	141	20.6%	41.8%	22.0%	0.0%	8.5%	0.0%	7.1%
		Japan	148	44.6%	8.8%	26.4%	0.0%	15.5%	0.0%	4.7%
	English	Germany	144	61.8%	22.2%	10.4%	0.0%	1.4%	0.0%	4.2%
		South Korea	135	41.5%	25.9%	21.5%	0.0%	2.2%	5.2%	3.7%
		Japan	154	56.5%	14.3%	11.7%	0.6%	7.8%	6.5%	2.6%
(b)	Native	Germany	140	50.7%	30.7%	10.0%	0.0%	2.1%	0.0%	6.4%
		South Korea	141	29.8%	43.3%	11.3%	0.0%	7.1%	0.0%	7.8%
		Japan	148	55.4%	8.8%	19.6%	0.0%	11.5%	0.0%	5.4%
	English	Germany	144	61.8%	23.6%	8.3%	0.0%	0.0%	0.0%	6.3%
		South Korea	135	46.7%	25.2%	8.9%	0.0%	3.7%	5.9%	8.9%
		Japan	154	57.8%	14.9%	9.7%	0.6%	5.8%	5.2%	5.8%
(c)	Native	Germany	140	19.3%	68.6%	4.3%	5.0%	0.0%	0.0%	2.9%
		South Korea	141	21.3%	57.4%	3.5%	9.9%	0.7%	0.0%	7.1%
		Japan	148	18.9%	56.1%	3.4%	12.8%	0.0%	0.0%	8.8%
	English	Germany	144	24.3%	63.9%	2.1%	5.6%	0.0%	0.0%	4.2%
		South Korea	135	28.9%	43.7%	3.0%	11.9%	0.0%	2.2%	10.4%
		Japan	154	29.2%	43.5%	5.2%	8.4%	0.0%	5.2%	8.4%
(d)	Native	Germany	140	32.1%	53.6%	0.0%	11.4%	0.7%	0.0%	2.1%
		South Korea	141	30.5%	50.4%	0.0%	10.6%	1.4%	0.0%	7.1%
		Japan	148	46.6%	23.6%	0.0%	16.9%	4.1%	0.0%	8.8%
	English	Germany	144	40.3%	45.8%	0.0%	7.6%	0.0%	1.4%	4.9%
		South Korea	135	37.0%	31.1%	0.0%	13.3%	0.7%	5.9%	11.9%
		Japan	154	48.7%	24.7%	0.0%	9.1%	1.3%	9.1%	7.8%

- Once a week
- Once a day
- More than once a day
- I don't know

Phishing emails written in English:

- Less than once a year
- Once a year
- Once every few months
- Once a month
- Once a week
- Once a day
- More than once a day
- I don't know

Q13. Have you ever been deceived by a phishing email? Being deceived by a phishing email means that you visited a website linked in the phishing email or opened a file attached to the phishing email, regardless whether you were directly damaged. Please answer the total number of work-related and personal experiences. Do not include your experience with phishing-training emails from your company.

Experience with phishing emails written in German/Korean/Japanese*:

- I have been deceived
  Approximately ( ) times
- I have been deceived, but I don't remember how many times
- I have never been deceived
- I don't know

Experience with phishing emails written in English:

- I have been deceived
  Approximately ( ) times
- I have been deceived, but I don't remember how many times
- I have never been deceived
- I don't know

An optional question for participants who answered "I have been deceived" or "I have been deceived, but I don't remember how many times" in Q13-2.

Q14**. If you remember the content of the phishing email in English, describe it as specifically as possible (e.g., the company/service/person the attacker masqueraded, the purpose and its requests, and why you were unable to identify it as a phishing email). If you have been deceived more than once, please tell us about the most recent phishing email you received.

Q15. This question is designed to verify that you are carefully reading the question. Please choose one of the following statements that fits the definition of phishing:

- An attacker encrypts files on your device
- An attacker masquerades as a legitimate company/service/person and asks for sensitive information
- An attacker sends a massive amount of traffic to a target website to disable it.

Q16. To what extent do you agree with the following statements? Please select the most applicable answer.

"I can always identify a phishing email written in German/Korean/Japanese*."

- Strongly disagree
- Disagree
- Somewhat disagree
- Somewhat agree
- Agree
- Strongly agree

"I can always identify phishing email written in English."

- Strongly disagree
- Disagree
- Somewhat disagree

- Somewhat agree
- Agree
- Strongly agree

Q17. Please specify why you think you can/cannot** identify a phishing email written in English. Answer by comparing it with the German/Korean/Japanese* case.

A.2 Results of the Roleplay Task

Table A·1 shows the detailed results of our roleplay task. This table provides a breakdown of the coded results of open-ended descriptions regarding their behaviors of participants who selected "*I'd refer to some other information than this screenshot to decide how to respond.*"

Ayako A. Hasegawa received her B.S. and M.S. degrees in information science from Ochanomizu University in 2013 and 2015, respectively. She also received her B.S. degree in human science from Musashino University in 2019. She is currently a researcher at NICT. Her current research interests are mainly on usable security and privacy. She is a member of IPSJ and IEICE.

Naomi Yamashita is a Distinguished Researcher at NTT Communication Science Laboratories and a visiting professor at Kyoto University. Her current projects focus on the design, development and evaluation of technologies for mindful inclusion in various domains such as global teams and mental healthcare.

Mitsuaki Akiyama received his M.E. and Ph.D. degrees in information science from Nara Institute of Science and Technology in 2007 and 2013. Since joining Nippon Telegraph and Telephone Corporation (NTT) in 2007, he has been engaged in research and development on cybersecurity. He is currently a Senior Distinguished Researcher at NTT Social Informatics Laboratories. He received the Cybersecurity Encouragement Award of the Minister for Internal Affairs and Communications in 2020, the ISOC NDSS 2020 Distinguished Paper Award in 2020, and the IPSJ/IEEE Computer Society Young Computer Researcher Award in 2022. His research interests include cybersecurity measurement, offensive security, and usable security and privacy. He is a senior member of IPSJ and a member of IEEE and IEICE.

Tatsuya Mori is currently a professor at Waseda University, Tokyo, Japan. He received B.E. and M.E. degrees in applied physics, and Ph.D. degree in information science from the Waseda University, in 1997, 1999 and 2005, respectively. He joined NTT lab in 1999 and moved to Waseda University in 2013. From Mar 2007 to Mar 2008, he was a visiting researcher at the University of Wisconsin-Madison. He has engaged in the research of network measurement, security, and privacy. He has received many best paper awards including NDSS 2020 and EuroUSEC 2021. Dr. Mori is a member of ACM, IEEE, IEICE, and IPSJ.