Analysis of the Relationship Between Psychological Manipulation Techniques and Personality Factors in Targeted Emails

Analysis of the Relationship between Psychological Manipulation Techniques and Personality Factors in Targeted Emails

Kota Uehara[1], Hiroki Nishikawa[1,2], Takumi Yamamoto[2],
Kiyoto Kawauchi[2], Masakatsu Nishigaki[1]
[1] Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011 Japan
E-mail: nisigaki@inf.shizuoka.ac.jp
[2] Mitsubishi Electric, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, Japan

Abstract. The damage from targeted email attacks continues to be an acute issue for Internet users. Several recent studies have demonstrated that psychological manipulation techniques (e.g. Cialdini's principles) are used effectively in phishing mails, the susceptibility to Cialdini's principles correlates with the personality factors (so-called Big Five), and the use of AI can serve to facilitate the assessment of the personality factors based on social media information. Based on the results outlined in the aforementioned studies, this paper considers the possibility of a new type of attack that uses open source intelligence (OSINT) tools to obtain social media information about the target and then misuse personality estimation tools and psychological manipulation techniques to create malicious emails with a highly effective level of psychological manipulation for each specific target. In this paper, to estimate the possibility of such attack, investigation and analysis in relation to such questions as whether Cialdini's principles work in targeted emails, and whether the effectiveness of Cialdini's principles in targeted email correlates to personality factors was performed through conducting a user experiment.

1 Introduction

In recent years, the damage due to targeted e-mail attacks have increased rapidly. Targeted e-mail attacks are a typical example of social engineering causing damage (for example, exploiting information and money or manipulating PCs illegally) to the targets by deceiving them. To accomplish a targeted e-mail attack, it is essential to convince the target that the malicious e-mail is a regular e-mail, and consequently, the attacker attempts to collect sensitive information about the target.

Currently, it is a common practice for companies and users to send information about themselves over the Internet, through owned media and social media. It has been reported that the web and social media is overflowed with information pertaining to companies and individuals. Moreover, personally identifiable information and privacy information can be obtained by consolidating publicly available personal information

[1], [2]. This method of gathering information is called Open Source Intelligence (OSINT), and there are several tools that facilitate OSINT activities. Attackers can use OSINT tools to obtain information related to the identified targets (e.g., their organizations, direct managers, the names of their friends, email addresses, related events, and personal interests) and then, to incorporate this information in creating specialized emails for each target with a high level of the mimicry precision (that is, a malicious email whose legitimacy cannot be easily determined by a receiver) [3], [4].

Moreover, a recent study has revealed that information obtained from social media can be used to estimate the psychological tendencies of users, and that tools are actually being used to estimate the personality related to a users' personality factors (Big Five [5]) based on information extracted from their tweets and blog posts [6]. As further research in conducted this field, it is expected that OSINT will become capable of estimating other psychological characteristics in addition to personality factors.

It is evident that human behavior is susceptible to psychological manipulation to some extent. Experiments have shown that Cialdini's principles [7] can be used to improve the effectiveness of psychological manipulation of phishing emails [8]. It has also been demonstrated that based on each user's personality factors, Cialdini's principles can differently affect the ease with which a user is influenced by psychological manipulation [9].

Hence, it is important to forearm ourselves against new types of attacks that may use OSINT tools to obtain social media information on the target and then, misuse personality estimation tools and psychological manipulation techniques to create malicious emails for each target with a highly effective level of psychological manipulation (that is, creating targeted emails that easily influence targets).

To estimate the possibility of such an attack, a user experiment was performed during this study to investigate and analyze, whether Cialdini's principles work in targeted email creation, and whether the effectiveness of Cialdini's principles in targeted emails correlates to personality factors, with the goal of anticipating the danger arising from such attacks and defending against them. The user experiment revealed that Cialdini's principles are effective when used within the text of targeted emails, but did not allow revealing correlation between the effects of Cialdini's principles and the human personality factors. With regard to the latter, the paper of Egelman and Peer demonstrates that behavioral characteristics (rather than personality factors) tend to have a stronger effect on human ideas on privacy [10]. Therefore, it may be possible to obtain an insight on which types of people could be easily influenced by psychological manipulations using Cialdini's principles in targeted emails by analyzing both personality factors and behavioral characteristics.

2 Related Work

A brief overview of the previous studies related to the targeted email attacks using OSINT is provided in this section from the perspective of mimicry precision and the effectiveness of psychological manipulation. With regards to the former, it was demonstrated by Ball et al., [3] that the threats to social engineering using OSINT have been increasing dramatically. Additionally, Uehara et al. in their study [4], proposed a

model of the state transition diagram to demonstrate how attackers make use of OSINT tools during the creation of targeted emails with high-precision mimicry to obtain targeted individual information in a state transition manner. The latter is broadly classified by the previous studies into the following main groups: the character estimation of the target using OSINT; the effect of psychological manipulation according to the character; and the deterioration of social engineering due to psychological manipulation.

Earlier study related to ascertaining the personality of targeted individuals using OSINT include active research of a user's five major personality factors (Big Five) extrapolated from information posted to the social media. The remarkable results of this research have already been implemented in IBM Watson's Personality Insights [6]. The Personality Insights tool employs a user's tweets published on Twitter and their blog posts to calculate their Big Five score. Several related studies show the presence of correlation between the Big Five of the psychological test subjects and the text written by those subjects. Personality Insights is an AI-based tool that employs machine learning techniques to identify the presence of correlation between the results of a psychological test (questionnaire) on the Big Five administered to several thousand users, and social media texts and posts (tweets or blog posts). Personality Insights is publicly available as an API module, hence, just by uploading social media texts of a user, it calculates a Big Five score for this individual.

Previous study on the effect of psychological manipulation based on personality factors has demonstrated that certain personality factors are more easily affected by Cialdini's principles [9]. Cialdini's principles (proposed by Dr. Robert Cialdini) are the psychological principles that make another party susceptible to external influence [7]. Alkış et al. clarified that Cialdini's principles are effective on people of all types, and performed experiments demonstrating that a user's personality factors affect "the degree of influence" of Cialdini's principles. Specifically, they administered psychological tests (questionnaires) related to the Big Five proposing subject answer questionnaires to determine the response rate to Cialdini's principles, and then investigated the correlation between the specific Big Five score of each user and various Cialdini's principles. The investigation showed several cases of significant correlation between the Big Five scores and users' response rates for each of Cialdini's principles.

Furthermore, considering the existing studies on psychological manipulation, Wright et al. [8] and Akbar [11] in their papers illustrated the results of the misuse of Cialdini's principles in phishing emails. Wright et al. sent a phishing email incorporating the six Cialdini's principles and an email without incorporating them to a group of university student test subjects, and then, compared the difference in response rates (rate of students who followed the instructions in the phishing email) [8]. The results of the experiment showed a higher response rate from subjects that received the phishing email incorporating any of Cialdini's principles (at least one) compared to those who received an email created without applying the principles, which demonstrated the effectiveness of Cialdini's principles in phishing emails. Akbar developed a flow chart to identify whether or not an email text incorporated Cialdini's principles, and investigated how frequently phishing emails actually employ Cialdini's principles [11]. The results showed that 96.1% of phishing email data sets studied by Akbar incorporated "Authority", and 41.1% used "Scarcity" principles, and that a high percentage of phishing emails also complied with other principles.

Akbar's study demonstrated that currently Cialdini's principles are widely used in phishing emails, and it can be inferred that Cialdini's principles will work effectively in targeted malicious emails. Therefore, it should be taken into consideration that new types of attacks may be invented to make use of OSINT tools to obtain social media information on the target and thereafter, to misuse personality estimation tools and psychological manipulation techniques seeking to automatically create specialized emails for each target with a highly effective level of psychological manipulation (that is, targeted emails that easily influence targets).

3 Targeted Emails with a Highly Effective Level of Psychological Manipulation by Using OSINT

3.1 Big Five

The Big Five, as proposed by Goldberg is a type of personality evaluation scale, also known as the "five major factor personality model" [5]. It is considered a comprehensive, clear model that provides an understanding of personalities, and is often used in many fields such as healthcare and consumer preference surveys. The Big Five is based on the following five elements used to evaluate personalities:

- Openness;
- Conscientiousness;
- Extroversion;
- Agreeableness;
- Neuroticism.

3.2 Obtaining Big Five Score Using OSINT

Recent developments in AI have made it possible to extrapolate the Big Five of individuals from their social media information (tweets and blog posts). Machines have no human biases and therefore, are able to extrapolate the Big Five objectively.

Representative examples include IBM Watson's Personality Insights [6]. Personality Insights is openly available as an API in the IBM Watson Developer Cloud. The API was used to build a program that analyzes the user's tweets to estimate the user's Big Five scores.

3.3 Cialdini's Principles

Cialdini's principles are the psychological principles proposed by Dr. Cialdini that coerce a person to be susceptible to external influence [7]. Cialdini's principles consist of the following six elements outlined below:

- Liking

This psychological principle explains that people actively respond to requests made by those they like. The person does not necessarily have to know the other party, but the principle of Liking includes a "likable personality" or a "polite tone."

- Reciprocation

This psychological principle explains that people want to repay favors to others (feel like they have to repay favors). Even if the favor is forced upon the person in a one-sided fashion, they feel obligated to return the favor. In other words, the person receiving the favor is psychologically motivated to return the favor whether they are happy to or not.

- Social Proof

This psychological principle explains that people want to follow what other people around them are doing. This psychological motivator arises from the desire to use the behavior of others (third parties) as judgment criteria for decision making in different situations.

- Commitment and Consistency

This psychological principle explains that people want their behavior to be consistent (want to become consistent). People tend to justify their decisions. In other words, when faced with similar situations from the past, people execute the same actions that were effective before. The principle of Commitment and Consistency also says that people attempt to keep the promises they have made.

- Authority

This psychological principle explains that people trust those in positions of authority with titles or experience. It results in the psychological motivation to follow those who are or seem to be above one's station or experts in a certain field.

- Scarcity

This psychological principle explains that the rarer something is, the more value is placed on it. It results in the psychological motivation to obtain something quickly before it is finished; this usually refers to things with pressing time limits or limited quantities.

3.4 Relationship between Big Five and Cialdini's Principles

Although Cialdini's principles apply to all people, it has been demonstrated that the degree of susceptibility to these principles is differently affected by one's personality [9]. For example, the persons with a high Big Five extroversion score are more susceptible to Reciprocation, Scarcity, and Liking, whereas the persons with a high conscientiousness score are more susceptible to reciprocation, liking, and commitment and Consistency, but less susceptible to Liking as shown in the experiments. Therefore, the attacker can use the methods explained in the previous section to obtain the Big Five of the target, thereby, learning, about the exposure to Cialdini's principles most effective for the targeted individual. Afterwards, the attacker can use the method, which is explained in the next section to incorporate the principles into an email seeking to create a targeted email with a highly effective level of psychological manipulation for the target.

3.5 Application of Cialdini's Principles in Targeted Emails

As demonstrated by Uehara et al. in their study [4], attackers can employ OSINT tools to increase the mimicry precision of targeted emails. Fig. 1 shows a sample targeted email attack perpetrated by using OSINT to obtain the target's email address and organization from their name. The email is spoofed to appear as if it originated from the technical department of the organization where the target works, recommending that the target install an antivirus software, and prompting the user to click a malicious URL. Fig. 2 and Fig. 3 show emails to which the attacker applied the Cialdini's principles Social Proof and Authority, respectively.

As explained in section 3.3, the principle of Social Proof is a psychological principle that causes people to "want to follow what others around us are doing." This is misused by the attackers to insinuate that "other employees have already installed this antivirus software." The principle of Authority is a psychological principle, in which people trust those in 'authority' with titles or experience. This can be misused by attacker through using the name of a manager in the organization. Because many companies currently list investor relations (IR) information on their websites, it is comparatively easy to obtain the names of executives using OSINT. It is thought that this information included in the text of an email will result in the high possibility of a user following the instructions.

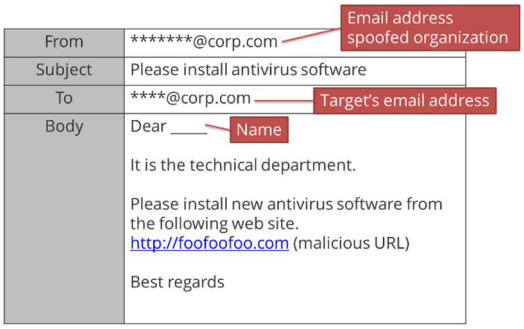

Fig. 1. Example of targeted email

From	*******@corp.com
Subject	Please install antivirus software
To	****@corp.com
Body	Dear ____ It is the technical department. Please install new antivirus software from the following web site. http://foofoofoo.com (malicious URL) Almost all of the other employees have already installed it, but you haven't done yet, so we contacted. Best regards

Fig. 2. Example of targeted email using Social Proof

From	*******@corp.com
Subject	Please install antivirus software
To	****@corp.com
Body	Dear ____ It is the technical department. Mr. XXX, the manager, requested to install new antivirus software. Please install it from the following web site. http://foofoofoo.com (malicious URL) Best regards

Fig. 3. Example of targeted email using Authority

Other Cialdini's principles aside from Authority can be incorporated into the text to utilize other human psychological principles to create targeted emails with a highly effective level of psychological manipulation. The attacker's cost effectiveness is considered extremely high as a result of adding just a small chunk of text that has a certain extent of effectiveness in psychological manipulation.

3.6 Research Questions

Sections 3.1 through 3.5 describe new possible types of attacks that may use OSINT tools to obtain social media information on the target and misuse personality estimation tools and psychological manipulation techniques to create targeted malicious emails for each target with a highly effective level of psychological manipulation (that is, targeted emails that easily influence targets).

To evaluate the possibility of such an attack, the user experiment was performed to investigate and analyze "whether Cialdini's principles work in targeted emails" and "whether the effectiveness of Cialdini's principles in targeted emails correlates to personality factors."

The research questions addressed in this paper are defined as follows.

RQ1: Can Cialdini's principles be applied in writing the text of a targeted email to easily convince a recipient to open the targeted email?

RQ2: Would a Cialdini's principle that is effective on an individual show different trends based on personality factors in targeted emails?

4 User Experiment

To answer the RQ1 and RQ2, this section describes the user experiment conducted to investigate the correlation between the response rate (i.e., the ratio at which targets followed instructions written in the targeted emails) to targeted emails that utilized each of Cialdini's principles and personality factors. OSINT tools and Personality Insights enable a smooth estimation of personality factors. However, to ensure participation of a large number of subjects and because of concerns over handling personal information on social media, subjects filled out personality survey questionnaires instead.

4.1 User Experiment Overview

In our user experiment, subjects took personality surveys and afterwards, received pseudo targeted emails that did not employ Cialdini's principles and pseudo targeted emails that included phrases corresponding to each of Cialdini's principles. Subjects then indicated on a scale from one to five how likely they were to obey the instructions within each email. Finally, the effectiveness of Cialdini's principles in the targeted email and the correlation between Cialdini's principles and personality factors were both statistically analyzed.

4.2 User Experiment Process

The LimeSurvey [12] web questionnaire system was used along with the Lancers [13] crowdsourcing platform to recruit test subjects, and the user experiment was then performed according to the following procedure:

i. Last name input
   Subjects input their own last names but their surnames were only used for embedding in the address of the email text used for the experiment.
ii. Attribute information survey
   Subjects entered information such as their age range, occupation, duties, and type of IT usage.
iii. Personality survey via a personality test (Big Five)
   The personality test proposed by Namikawa et al., [14] was performed by subjects.
iv. Questionnaire on the effects of the Cialdini's principles using a pseudo targeted email
   Subjects selected the degree of obedience to instructions included in the email.

The subjects responded to the questionnaire after the preliminary explanation about information that we were going to collect was provided and their consent was received. The explanation also included the following:

> Because the experiment was designed for the company employees, non-company employees are not supposed to take part.

However, the Lancers system does not have a specification to accurately identify the occupation of participants. Therefore, it should be noted that the results of this user experiment may include responses from non-company employee participants.

4.3 Questionnaire for Personality Test

Japanese language versions of the Big Five questions have been preciously analyzed by Wada [15]. Based on the study [15] and applying methods that take into consideration the burden on users, a shortened version of a personality survey consisting of 29 questions was administered by Namikawa et al. [14]. In our user experiment, the Big Five scores were measured for each user using the shortened version of questions. Subjects were asked to respond to each question on a scale from one to five: "1: Disagree," "2: Disagree a little," "3: Neither agree nor disagree," "4: Agree a little," and "5: Agree." Then the score for each of the Big Five was calculated based on the responses obtained.

4.4 Questionnaire on The Effects of Cialdini's Principles

4.4.1 Procedures for Creating Pseudo Targeted Emails

The following procedures were used to create a pseudo targeted email data set that includes phrases corresponding with each Cialdini's principle.

i. The pieces of text from 21 types of different emails (called “original email”), which were shown to the public at the Japan Cybercrime Control Center (JC3) [16] and had been used in the actual targeted email attacks in Japan, were randomly selected. Then three sets of original email data set consisting of seven kinds of original emails were created.
ii. One set (seven kinds of emails) was selected from the three original email data sets.
iii. Phrases incorporating Cialdini’s principles were deleted in the original emails to create “plain email” data sets. Plain emails are pseudo targeted emails which did not incorporate any of Cialdini’s principles. Seven kinds of plain emails were created.
iv. By embedding phrases corresponding to each Cialdini’s principle in the email text, six different types of pseudo targeted emails were created for each plain email (called “Cialdini email”). This resulted in targeted email data sets consisting of 49 pseudo targeted emails including plain emails.
v. The text of the pseudo targeted emails was reviewed by the experimenters (the four authors). If even a single experimenter felt that the email seemed slightly unclear, the matter was collectively deliberated and the text was corrected. The phrases were appropriately corrected based on Cialdini’s principles to comprise of natural-sounding Japanese on the premise that the meaning of the original emails would not be changed.
vi. Another set was then selected from the remaining original email data sets and steps iii, iv, and v, were executed.
vii. The procedure was complete when targeted email data sets were created from all the three original email data sets.

4.4.2 Experiment Procedures

i. One set was selected from the three targeted email data sets.
ii. Seven individual emails were chosen randomly including plain emails and emails incorporating Cialdini’s principles, so that the content was not duplicated. Duplicated content was removed owing to the fact that the order effect (the first time a text is viewed influences the second response) occurs if the same type of text (content) appears two or more times.
iii. The seven emails were then placed in a random order on a single webpage so that they could be scrolled. Test subjects then responded with a five-grade evaluation for each email regarding the “Degree of obedience to instructions provided in an email (response score)” in the following manner: “1: Definitely wouldn’t obey,” “2: Wouldn’t obey,” “3: Can’t say either way,” “4: Would obey,” “5: Definitely would obey.” The subjects provided responses to all seven emails before proceeding further by clicking the “Next” button.
iv. Another set was then selected from the remaining targeted email data sets and steps ii and iii were executed.
v. The experiment was concluded once responses were submitted for all three targeted email data sets.

4.4.2 Test Subjects

For this user experiment, one-hundred test subjects were recruited using Lancers [13], which is a crowdsourcing service. The average response time among test subjects was 7 minutes 40 seconds, and the shortest response time was 2 minutes 52 seconds, while the longest response time was at 22 minutes 34 seconds. A quartile response time was adopted to remove outliers corresponding to overly large and small values from the distribution of test subject response times. The values that were 1.5 times smaller than the first interquartile range, and the values that were 1.5 times larger than the third quartile range were treated as outliers. When the outliers were removed, the results showed 96 effective responses. It should be noted that as the user experiment was administered using a web questionnaire, it was not possible for the test administrators to adequately control the test subjects.

5 Experimental Results and Analysis

To investigate the internal consistency of the scale used in this experiment, Cronbach's alpha for the subscales within the data set was calculated (Table 1). Each resulted in a value of at least 0.7, showing some degree of validity. Then, the results of the user experiments RQ1 and RQ2 were analyzed.

5.1 Analysis 1: Analysis for RQ1

To answer RQ1 ("Can Cialdini's principles be applied in writing the text of a targeted email to easily convince a recipient to open the targeted email"?), analysis was performed to investigate if using Cialdini's principles to create targeted emails would result in a higher tendency of recipients opening such targeted emails, similar to that of phishing emails. A one-sided test was administered using the following null hypothesis and alternative hypothesis to analyze if there was a significant difference between the response scores for the plain emails and the Cialdini emails. The significance level was set to 5%.

Null hypothesis: Response scores for targeted emails will not change if Cialdini's Principles are applied.

Alternative hypothesis: Response scores for targeted emails will increase if Cialdini's Principles are applied.

As each subject was required to provide their response scores for both the plain emails and Cialdini emails (for each principle), the two response scores are comparable (that is, data is obtained from corresponding samples). Therefore, a Wilcoxon signed-rank test was implemented for verification.

Table 2 illustrates the results of the test. A significant difference could not be confirmed for the principles of consistency and social proof, and hence, the null hypothesis cannot be rejected. A significant difference ($p < 0.01$, $p < 0.05$) could be confirmed for the principles of scarcity, reciprocation, authority, and liking. Therefore, the null hypothesis could be rejected, and the alternative hypothesis was adopted. This

reveals that some of Cialdini's principles are effective at convincing recipients to open targeted emails, and that RQ1 can be partially established.

Table 1. Reliability scores

Scale	Subscale	Cronbach's alpha	Number of items
Big Five	Extroversion (Ext)	0.850	5
	Agreeableness (Agr)	0.807	6
	Conscientiousness (Conc)	0.771	7
	Neuroticism (Neu)	0.784	5
	Openness (Ope)	0.811	6
Cialdini's principles	Reciprocation (Rec)	0.719	3
	Scarcity (Sca)	0.811	3
	Authority (Aut)	0.832	3
	Social Proof (SP)	0.829	3
	Liking (Lik)	0.800	3
	Consistency (Cons)	0.826	3

Table 2. Test results of response scores between plain email and Cialdini email

	p-value
Reciprocation	0.0411*
Scarcity	0.0306*
Authority	0.0038**
Social Proof	0.444
Liking	0.0014**
Consistency	0.37

† $p < 0.10$, * $p < 0.05$, ** $p < 0.01$

Table 3. Correlation between Big Five and Cialdini's principles

	Rec	Sca	Aut	SP	Lik	Cons
Ext	0.024	0.073	0.108	0.015	0.011	-0.079
Agr	-0.167	-0.143	-0.17	-0.138	-0.035	-0.122
Conc	-0.169	-0.103	-0.058	-0.143	-0.057	0.013
Neu	0.068	0.017	-0.005	0.072	0.053	0.057
Ope	0.01	0.046	0.096	0.005	0.03	-0.029

5.2 Analysis 2: Analysis for RQ2

To answer RQ2 ("Would a Cialdini's principle that is effective for a single individual show different trends based on personality factors in targeted emails"?), the correlation between the scores of each Big Five factor and the response scores for individual Cialdini's principles was considered, and analysis was performed whether any of Cialdini's principles notably influenced subjects with respect to each personality factor.

Table 3 shows the presence of correlation values between the Big Five and Cialdini's principles. The Spearman's rank correlation coefficient between each pair of Big Five factors measured using the questionnaires, and the response scores for Cialdini's principles were determined for the analysis.

The analysis was unable to determine a significant correlation between Cialdini's principles and any of the Big Five factors. Therefore, unlike the conclusions from the experimental results of the previous study by Alkış et al., this study did not succeed in confirming that the extent of influence of Cialdini's principles differs based on the user's personality factors.

6 Discussion of Analysis Results

6.1 Discussion on the results of analysis 1

In this section, the Cialdini's principles of consistency and social proof, for which no significant difference could be observed and confirmed, are discussed.

As described in the sections above, the principle of consistency is a psychological principle that states that people want their behavior to be consistent (want to become consistent). However, only a single email employing this principle was taken for analysis, although phrases suggesting that the recipient "did something similar before" were inserted when creating the targeted email, it is likely that the principle of consistency was not conveyed adequately in this experimental environment. For example, it may have been possible to make effective use of the consistency principle if the content of the targeted email suggested that the recipient "actually did this same thing before."

As noted earlier, the principle of social proof is a psychological principle stating that we want to follow what others around us are doing. Therefore, during this experiment, phrases were inserted in targeted emails asking the recipient to perform the following actions: "please open the attachment like everyone else", or "everyone else has already checked the attachment." However, the former could have been interpreted as follow: "please check the attachment using the same procedure/method as everyone else," while the latter could be interpreted as "someone else has already checked it for you." Subjects may therefore have misunderstood these emails, which meant that the principle of social proof did not work at a significant level.

6.2 Discussion on the results analysis 2

The research by Alkış et al. [9] showed the presence of correlation between personality factors and statistics related to the extent to which subjects are influenced in terms of all Cialdini's principles. This section examines why the results of the current experiment varied from those of Alkış et al.

Alkış et al. used the susceptibility to persuasive strategies scale (STPS) developed by Kaptein et al. to measure the extent, to which subjects were persuaded using Cialdini's principles [17]. When using STPS, researchers prepare in advance questions related to persuasion, and then, ask the subjects if they would obey. For example, one question on reciprocation is "when a family member does me a favor, I am very inclined to return this favor." Therefore, questions asked using STPS are not limited to targeted emails, but also include general requests and direct questions. In contrast, we, in this paper, included phrases corresponding to each of Cialdini's principles in the body of targeted emails and asked whether subjects would intentionally obey the text in these emails to evaluate responses within an experimental scenario that more closely resembled a targeted email. Elements such as the intrinsic suspicion people have of targeted emails, may have a direct effect on the judgment of the subjects, and hence, this may explain the differences in the obtained results compared with those of Alkış et al.

However, the results of this experiment suggest that some human personality factors may affect Cialdini's principles used in targeted emails. There is the existing research pertaining to this and illustrating that behavioral characteristics (rather than personality factors) tend to have a stronger effect on human ideas on privacy [10]. Hence, it may be possible to gain an insight on "which types of people would be more easily influenced by psychological manipulation using Cialdini's principles" in targeted email rather than analyzing both personality factors and behavioral characteristics.

7 Conclusion

This study considered the hypothesis that "an attacker may use OSINT tools to obtain social media information on the target and then, to misuse personality estimation tools and psychological manipulation techniques seeking to create targeted emails aimed for each target with a highly effective level of psychological manipulation based on the existing studies on correlation between personality estimation tools (which estimate an individual's personality from social media information), and psychological manipulation techniques (Cialdini's principles). To test this hypothesis, an experiment, which confirmed the effectiveness of Cialdini's principles in composing targeted emails, was performed involving 100 users. However, the results of this experiment were unable to demonstrate the presence of correlation between human personality factors and the effect of using Cialdini's principles in targeted emails. In future research, analysis performed from the perspective of both personality characteristics and behavioral characteristics should be considered. Further research will also be required to assess if the same effect is obtained for English language emails, as the experiment in the present study was performed using the emails written in Japanese.

References

1. Acquisti, A., Gross, R., Stutzman, F.: Face recognition and privacy in the age of augmented reality. Journal of Privacy and Confidentiality 6.2, (2014) 1-20
2. Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., Dabbish, L.: Anonymity, privacy, and security online. Pew Research Center, (2013)
3. Ball, L.D., Ewan, G., Coull, N.J.: Undermining-social engineering using open source intelligence gathering. In: Proc. of 4th International Conference on Knowledge Discovery and Information Retrieval (KDIR), SciTePress-Science and Technology Publications, (2012) 275-280
4. Uehara, K., Mukaiyama, K., Fujita, M., Nishikawa, H., Yamamoto, T., Kawauchi, K., Nishigaki, M.: Basic Study on Targeted E-mail Attack Method Using OSINT. International Conference on Advanced Information Networking and Applications, (2019) 1329-1341
5. Goldberg, L.R.: An alternative "description of personality": the big-five factor structure. Journal of personality and social psychology 59.6, (1990) 1216-1229
6. IBM, "Personality Insights," https://www.ibm.com/watson/services/personality-insights/, [Accessed 25 Mar. 2019]
7. Cialdini, R.B. Influence. Vol. 3. Port Harcourt: A. Michel, (1987)
8. Wright, R.T., Jensen, M.L., Thatcher, J.B., Dinger, M., Marett, K.: Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. Information systems research 25.2, (2014) 385-400
9. Alkış, N., Temizel, T.T.: The impact of individual differences on influence strategies. Personality and Individual Differences 87, (2015) 147-152
10. Egelman, S., Peer, E.: The myth of the average user: Improving privacy and security systems through individualization. In Proceedings of the 2015 New Security Paradigms Workshop, (2015) 16-28
11. Akbar, N.: Analysing persuasion principles in phishing emails. Master's thesis, University of Twente, (2014)
12. LimeSurvey, https://www.limesurvey.org/, [Accessed 24 Mar. 2019]
13. Lancers, https://www.lancers.jp/, [Accessed 24 Mar. 2019] (In Japanese)
14. Namikawa, T., Tani, I., Wakita, T., Kumagai, R., Nakane, A., Noguchi, H.: Development of a short form of the Japanese Big-Five Scale, and a test of its reliability and validity. The Japanese Journal of Psychology 83.2, (2012) 91-99 (In Japanese)
15. Wada, S.: Construction of the Big Five Scales of personality trait terms and concurrent validity with NPI. The Japanese Journal of Psychology 67.1, (1996) 61-67 (In Japanese)
16. Japan Cybercrime Control Center (JC3), https://www.jc3.or.jp/, [Accessed 20 Mar. 2019] (In Japanese)
17. Kaptein, M.: Personalized persuasion in ambient intelligence. Journal of Ambient Intelligence and Smart Environments 4.3, (2012) 279-280