2FA SMSs: Influence of Cybersecurity Behavior & OTP Message Content on Security

KEVIN LAKSANA ISKANDAR, University of Twente, The Netherlands

Two-factor authentication or 2FA for short is a common security measure used to verify one's identity. One method of 2FA is the use of SMS messages, called 2FA SMSs, containing a token as the second form of authentication. Although 2FA SMSs are widely used and accepted as a form of 2FA, it has multiple vulnerabilities which may be exploited through different schemes and methods in order to bypass 2FA. This paper conducts a survey to elaborate on the contents of 2FA SMSs and uses quantitative data analysis to investigate the relationship between an individual's cybersecurity knowledge/behavior and susceptibility to 2FA via SMS security breach.

Additional Key Words and Phrases: Human Factor, Short Message Service (SMS), Security, Two-Factor Authentication (2FA)

1 INTRODUCTION

Before the rapid development of the internet, account security was not too strict. A simple password was enough for most accounts to be accessed [5], but now times have changed. Computer and Information Security (CIS) has become a very important aspect due to the amount of essential data and information now stored on one's account or device [10]. As it became prevalent that a simple password is no longer sufficient to provide security for important accounts such as emails & online banking accounts, additional measures needed to be taken in order to make them secure. One of these additional measures used for authentication and authorization is two-factor authentication (2FA) [5]. Two-factor authentication involves the use of two different factors to authenticate a user. Traditionally, one factor is a password and the second factor may be many different things that the user knows, have or are [12]. However, the focus of this paper will be on SMS (Short Message Service) as a second factor of authentication.

2FA via SMS using One-Time Passwords (OTP) was initially created to mitigate phishing and other types of attack on user's account authorization and authentication [9] and is still widely used by many at the present time as a second factor of authentication as a majority of people owns a mobile phone [12]. 2FA via SMS works by having an account (such as email or bank account) be linked to a mobile phone number. This way, when the account owner would like to perform a process that requires authorization/authentication, aside from the password, the user would have to enter the verification code or the OTP token sent to the user's mobile phone number via SMS to validate the user. In other words, 2FA via SMS works to ensure that the user using the account also possesses the phone number linked to the account and as the mobile phone number linked to the account should belong to the user, the identity of the user is authenticated [9].

Although 2FA via SMS is widely used, there exists methods and schemes to bypass it [5, 7]. Methods involving Stingray and rogue base stations, SS7 protocol & mobile phone trojans/malware require high technical knowledge to perform while others such as sim swapping & Verification Forwarding Attacks (VCFA) [13] are less technical and can be considered a 'social engineering attack' [5]. As human factors heavily contribute towards 'social engineering attacks', this paper will investigate the relationship between the level of user IT knowledge and security of 2FA SMS through data collection and analysis. And as the information sent in different 2FA SMSs differ, this paper will also aim to analyze the contents of 2FA SMS messages as it may affect 2FA SMS security.

2 PROBLEM STATEMENT

A lot of different research has been done in the field relating to human factors and cybersecurity in general. However, there is a lack of research focused on how human factor, which in the case of this paper is user's IT knowledge/background, may influence 2FA SMS security specifically. As there are some unique attacks designed specifically to bypass 2FA SMS, this paper will investigate whether a user's IT knowledge may affect the success rate of these attacks. Some research deem 2FA SMSs to be insecure and obsolete [9], thus this investigation will reveal whether the this is due to the users of 2FA SMS or if the fault lies within others or if perhaps the contents of 2FA SMSs may play a role as not much research has been done regarding the contents of different 2FA SMS messages.

2.1 Research Questions

Main research question:

Does the content of 2FA SMS messages or user IT knowledge play a role in the security of 2FA SMSs?

From the problem statement & main research question, the following research questions are formulated:

1. What can be used to measure user IT knowledge and security of 2FA SMS?

TScIT 37, July 8, 2022, Enschede, The Netherlands

2. What information is contained within a 2FA SMS message? To what extent does information compromise 2FA SMS security or otherwise?
3. Is there a relationship between an individual's IT knowledge/behavior and the security of 2FA SMS through personal experiences?

3 RELATED WORK

Through literature search via Scopus and Google scholar using keywords such as "2FA SMS", "human factor", "IT background" and "security" (among others), several related papers in this field have been found. However, since no paper was found which focuses specifically on the role of human factor on 2FA SMS security, the related works found can be classified into two main categories. The first category of papers focuses on SMS and 2FA[5, 6, 9, 11, 12, 14]. These papers elaborate on the functionality and workings of SMS, the use of SMS for 2FA, how 2FA works using SMS, the vulnerabilities & security risks of 2FA using SMS, methods & schemes to bypass 2FA SMS and methods to prevent these attacks. The attacks may be in the form of SIM swapping, rogue base stations, SS7 protocol, trojans/malware and etc. [5, 9] These papers provide the foundation of knowledge required to understand the workings & details of 2FA SMS. The second category of papers focuses on human factor and its impact on cybersecurity [7, 10]. These papers elaborate on how human factor may lead to security breaches, loss of data and other cybersecurity vulnerabilities. These papers also elaborate and validate the importance of human factor in the area of cybersecurity and how it affects information security. Aside from the two categories, there may be some papers which are more closely related to the topic [15]. This paper focuses on the contents of 2FA SMSs and human factor to determine whether it may pose a risk to security. The paper conducted an analysis on 50 different OTP messages sent via SMS. According to [15], the results suggested that information present in an SMS OTP may affect the security of 2FA via SMS, however it was stated that the study was limited and required further research.

4 METHODOLOGY

This research will be done in a few main stages. The first stage is literature review. A literature review of papers connected to methods of bypassing 2FA SMS, the methods to prevent them and papers regarding 2FA SMS security in general will be conducted. This will provide a deeper understanding of the workings of 2FA SMS, its security and the methods/schemes used to bypass 2FA SMS. By getting a deeper understanding, better questions and reasoning may be formulated in order to answer the following research questions. This should already be done prior to the creation of the survey.

4.1 Survey Population & Demographics

This section will discuss the survey mentioned in further detail. With the purpose of limiting the amount of variables, the respondents for this survey will be restricted to individuals from or formerly from the EEMCS (Electrical Engineering, Math & Computer Science) department of the University of Twente. This target population was chosen as it is to be believed that most individuals in this group have basic knowledge of 2FA and basic technical knowledge on IT. The respondents age, IT background, level of study, gender and other information will be recorded as demographic information in order to find possible abnormalities or similarities in certain results with regard to specific demographic items.

4.2 Survey Scales (RQ1)

To answer RQ1, two scales will be required. The first to measure an individual's cybersecurity behavior and the second to measure an individual's use of 2FA SMS. These scales will both use a 5-point Likert scale (from "never" to "always", scoring from 1 to 5 respectively). Multiple scales exist to measure Cybersecurity behavior thus the survey will use one of these scales. The scale chosen for this purpose is SeBIS (Security Behavior Intentions Scale)[1] , a cybersecurity scale that is accepted and has been validated. This scale consists of four subscales consisting of 3-5 items each, with a total of 16 items. These subscales are *Device Securement, Password Generation, Proactive Awareness and Updating*. The full scale is shown in *Appendix C.1*. This scale is reliable with a Cronbach's Alpha of 0.801 and all subscales having greater than 0.6 and most greater than 0.7.

In order to construct a scale to measure 2FA SMS security, the subscales *Device Securement* and *Proactive Awareness* of the SeBIS scale were used and its items adapted to create a new scale. The *Device Securement* SeBIS subscale had items altered to specifically measure the device securement of mobile phone which are used for 2FA via SMS, while the *Proactive Awareness* SeBIS subscale had its questions altered to measure the susceptibility of an individual to different methods which may expose 2FA to security breaches. As a result, a 5-point Likert, 8 item scale was created (see *Appendix C.2* for full scale). These two scales are the answer to RQ1 and will be used to answer RQ3.

4.3 Survey Considerations

The order of blocks in the survey are as follows:

1. Informed Consent
2. Demographic
3. Cybersecurity Scale
4. 2FA Security Scale
5. OTP Entry

The order of measurements in the survey was intentional and meticulously planned. The first block to be accessed by respondents will be the Informed Consent block. The block informs the respondent about the study and usage of their data, thus giving them a choice to either participate or not participate in the study. Afterwards, the demographic items were placed with the intention of gathering respondents data that may still be used in the case that the respondent does not complete the survey. The two scales are then placed next, the order of these two scales do not matter much as one does not influence the results of the other as they should not have an affect on the respondent's thought process. The final block is the OTP entry block which was placed last due to the complexity and difficulty of the question. It was expected that some respondents may not continue with the survey if this block was to come before the others (through testing). Aside from the order of blocks, the consideration was also made to give definitions and examples of uncommon terms and difficult questions.

4.4 Survey Procedure

Before the survey was officially published, a pilot testing of the survey was done on a small group of EEMCS Bachelor students with the goal of ensuring that the survey was not too difficult and to estimate the time it took to complete the survey. As a result of this testing, it could be concluded that the survey took approximately 10-15 minutes at most to complete. It was also concluded that some questions were difficult to understand and were too demanding for the respondents. Thus definitions for acronyms and uncommon terminology were provided within the survey questions and some questions (mainly from the OTP entry block) were revised, simplified and made less demanding to increase the chance of the respondent completing the survey. The survey was then published and distributed through various online means to EEMCS members. The survey was distributed to various EEMCS discord groups, WhatsApp groups, MicrosoftTeams chats and distributed through personal chat to EEMCS students.

4.5 OTP Analysis (RQ2)

Answering RQ2 may be partially be done via literature review, but as there is not much papers that go into specific detail about the contents of 2FA SMSs or in this case the OTP message sent via SMS, an analysis of different OTP SMSs used for 2FA will be collected first-hand (through a survey) and studied. A minimum of 30 different OTP SMSs will be collected and analyzed. An analysis will be conducted to identify the different information that are present in these OTP SMSs. Specific categories to classify the information present within an OTP message will be created and their presence will be documented for each OTP message. As an example, if an OTP SMS for a certain account contains the verification code/token and a warning which reminds the user not to share the token with anyone, the category of warning and token can be marked as present for that OTP SMS. This stage then requires two steps, the first step is to finalize the categories of classification for information commonly found in 2FA SMS messages (OTP messages) and a second step of conducting the analysis of different OTP SMSs used for 2FA using the categories and determine whether the information present may be a security risk.

In order to assist in the data collection, a block will be added into the survey after the two scales. The purpose of this block will be to collect data of different OTP messages sent via SMS. Respondents will be asked to enter OTP message entries with the token being replaced as to ensure that no possible risk may come to the respondents as this may be sensitive data.

4.6 Data Analysis (RQ3)

After respondents have been gathered, multiple statistical analysis methods will be applied to the results to validate the scales, verify the results and answer the research questions. Firstly, to ensure the scale and results can be accepted and are reliable, a reliability test will be conducted on them. The reliability test will include the measurement of Cronbach's alpha and scale item-total correlation. Afterwards, to answer RQ3 a simple linear regression will be conducted on the result of the two scales (SeBIS and 2FA security scale) with the cybersecurity scale as the independent variable (x-axis) and 2FA security as the dependent variable (y-axis).

In order to perform data analysis, a minimum of 80 participants are required. This is so as is the minimum amount that satisfies the recommendation given by *Hair et al.* [4] to use a minimum of 5 respondents per item in the scale when accessing a scale as the SeBIS scale (which has the most items) has a total of 16 items which would require a minimum of 80 respondents.

In preparation for data analysis, some data need to be altered in preparation for data analysis. This is so as some items in the SeBIS scale [1] were reverse-scored questions, meaning that their score needed to be reversed before conducting data analysis (5 should be 1 and 4 should be 2, vice versa). The items of the SeBIS scale that were reverse-scored were items 5, 8, 9, 10, 11 and 13.

5 RESULTS

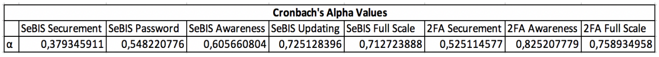
After 3 weeks of gathering respondents, the survey has gathered a total of 91 respondents from the EEMCS department of the University of Twente. Approximately 75% of respondents are male and 25% are female. The average age of respondents is 21.65 and standard deviation of 5.07 with a minimum of 18 and a maximum of 25. Approximately 95% of these respondents are students while the remaining 5% are either a faculty member or have graduated from an EEMCS course. A vast majority of the respondents have an education level or are currently pursuing their Bachelors degree leaving only 2 respondents from Masters studies and 1 pursuing a Phd. Thus the survey result does not represent the whole EEMCS population well in regards to the level of education as the proportion of Bachelor students to Master & Phd students is improper.

One very interesting piece of demographic data was one which asked respondents whether they have ever taken any sort of cybersecurity training. It was expected that a high proportion (perhaps around 90%) of respondents would answer “yes” to this question, however according to the results only around 58% of respondents answered “yes” for this demographic item. This is highly unusual as I believe that the University of Twente offers students cybersecurity training on a voluntary basis via email, thus it was expected that most respondents would have some sort of cybersecurity training.

Any data that may compromise the identity of the respondents are deleted (IP address & location, as *Qualtrics* record these automatically). Before conducting any tests and data analysis using the results of the survey, the integrity and completeness of the data must first be ensured. Thus, responses with incomplete data (deemed complete if the two scales are completed) and respondents who claim not to use 2FA via SMS are removed from the final data set. 11 responses were deemed incomplete and did not satisfy the requirements leaving only 80 responses left to be processed.

5.1 Reliability Test & Validation (RQ1)

The reliability of the two scales used in this study will be assessed through the analysis of two values. This will be through the calculation of the Cronbach’s alpha and item-total correlations of each scale. Although the cybersecurity scale (SeBIS) being used for this survey has been validated [1], it must still be tested for this study due to the difference in survey population.

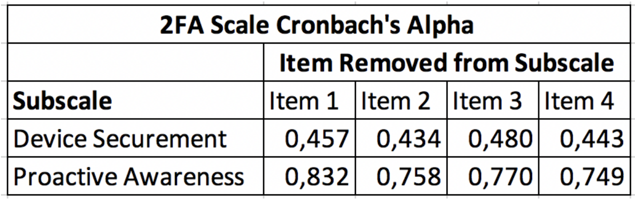


Cronbach's Alpha Values								
	SeBIS Securement	SeBIS Password	SeBIS Awareness	SeBIS Updating	SeBIS Full Scale	2FA Securement	2FA Awareness	2FA Full Scale
α	0,379345911	0,548220776	0,605660804	0,725128396	0,712723888	0,525114577	0,825207779	0,758934958

Table 1. Cronbach’s Alpha.

According to McKinley et al. [8], a multicomponent scale is reliable if the Cronbach’s alpha value for all subscales is greater than 0.6 and if the Cronbach’s alpha value for a majority of subscales is greater than 0.7. Unfortunately, in this study, this condition is satisfied for neither the cybersecurity nor the 2FA security scale. This is due to the low values of Cronbach’s alpha on the subscales *SeBIS Securement* (α = 0.38)*, SeBIS Password* (α = 0.54) *and 2FA Securement* (α = 0.53). However, according to *Bland & Altman* [2], Cronbach’s alpha values between 0.7 and 0.8 are satisfactory when comparing groups. Since the full scale Cronbach’s alpha for the two scales are 0.71 (for SeBIS) & 0.76 (for 2FA) and this study will be comparing the two scales through a simple linear regression, the two scales will be deemed acceptable and reliable to a certain extent in regards to the value of Cronbach’s alpha. (See *Table 1* for full alpha values)

For the next step of validation and reliability analysis, the item-total correlation will be used. “Item-total correlation measures how well the responses to one item correlate with the other items in the scale. Questions are deemed to not represent the rest of the scale when their item-total correlations are below 0.2” [1, 3]. For this study, the correlation between the item and the average of all other items in the scale and subscales will be calculated. According to *Everit* [3], it is recommended that all items have an item-total correlation of over 0.2. This is satisfied for all items except for *SeBIS Securement 1* (0.17) and *SeBIS Password 1* (0.02) for their item-total correlation with the full scale. However, since the values of item-total correlation with their respective subscales are over 0.2 (0.64 for Securement 1 & 0.41 for Password 1), the scale will still be accepted. Through these two reliability tests, it can be said that the two scales are acceptable and reliable enough to use. (see *Appendix A* for full item-total correlation values)



2FA Scale Cronbach's Alpha				
	Item Removed from Subscale			
Subscale	Item 1	Item 2	Item 3	Item 4
Device Securement	0,457	0,434	0,480	0,443
Proactive Awareness	0,832	0,758	0,770	0,749

Table 2. Cronbach’s Alpha of 2FA with an item removed.

The Cronbach’s Alpha values for when an item is removed from a subscale of the 2FA scale was also calculated in order to improve the scale by removing items that may negatively affect the Cronbah’s Alpha, results are shown in *table 2*. As seen, only the removal of item 1 from the subscale Proactive Awareness increases the Cronbach’s Alpha of a subscale (Original = 0.825, Item 1 removed = 0.832). However, although removing item 1 of Proactive Awareness increases the alpha of the subscale, it decreases the alpha of the full scale from 0.759 to 0.708. The removal of Item 4 from the Device Securement decreases the subscale alpha from 0.525 to 0.443, however it may bring a positive impact to the full scale’s alpha. This is so as removing item 4 from Device Securement subscale increases the full scale Cronbach’s alpha value from 0.759 to 0.760. This is a very small increase of Cronbach’s alpha but nevertheless still a slight improvement in the value.

5.2 OTP Message Analysis (RQ2)

Out of the initial 91 responses received by the survey, only 47 responses entered OTP(one-time password) message entries. This was to be expected as the question was demanding and may take the most time out of the whole survey. From the 47 responses, a total of exactly 100 entries were acquired. From the 100, only 88 contained a token and the SMS message while the other 12 only contained the token. Most entries did not follow the proper entry format given by the question thus some initial elements will be neglected.

Before conducting analysis of the OTP message entries, the categories for the common elements present in an OTP message that will be used for this study must be decided. These categories are as follows: Character (whether token contains at least one character), Digit (whether token contain at least one digit), Time (whether the message states that there is a time limit to validity of token), Warning (whether message contains a warning related to 2FA security), Action (whether the message states what action the token will be used for) and finally Identifiable (whether the OTP sender/issuer is identifiable through the message). To ensure that the results are to be as reliable as possible, only the category of Digit and Character will be recorded for responses with only a token and no message entries. As there was no way to automate the process of analysis due to the lack of consistency in the format of responses, manual analysis of the data was conducted. The results are as follows:

- Out of 100 tokens, 24% contained at least one character.
- Out of 100 tokens, 100% contained at least one digit.
- Out of 88 entries, 16% mentioned a time limit to token validity.
- Out of 88 entries, 25% gave a warning concerning 2FA/OTP security.
- Out of 88 entries, 41% mentioned the action the token is used for.
- In 72% out of 88 entries, the sender/issuer of the token was identifiable through the message

From the results of the analysis, it would appear that only a low amount (24%) of OTP tokens used for 2FA via SMS actually use characters while digits are present in all tokens. In other words, a majority (76%) of OTP message tokens only contain digits. In a way, this may increase the chances of 2FA being breached as having only digits in a token means that it may be relatively easier for an attacker to brute force or guess the OTP as a limited number of combinations can be created from digits (as there are only 0 to 9). However, by using both characters and digits in a token, it will be significantly harder for an attacker to brute force or guess the token as the amount of combinations are much higher. It can also be observed that the amount of messages that has (or at least mention) a time limit and has a warning are both relatively low (16% and 25% respectively).

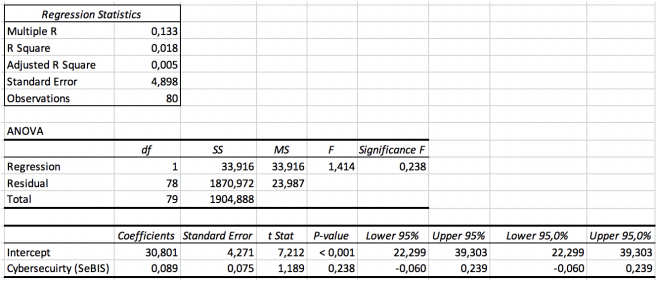
5.3 Linear Regression (RQ3)

Now that the scales and data have been validated, a simple linear regression comparing the results of the two scales will be conducted with the cybersecurity scale as the independent variable and 2FA security as the dependent variable. The scales were assigned this way as this study's goal is to investigate how cybersecurity behavior/knowledge may affect the security of 2FA and not the other way around. This simple linear regression will answer RQ3 as it will prove whether a relationship exists between the two scales of cybersecurity behavior and 2FA security.

Before the test is conducted, several assumptions when performing linear regression must be confirmed. The assumptions are as follows[16]:

1. There is a linear relationship between the variables.
2. Normal distribution
3. No or little multicollinearity
4. Homoscedasticity

To prove assumption 1, a hypothesis test is conducted. The null hypothesis of this test will be: "There is no linear relationship between cybersecurity behavior and 2FA security". And the alternative hypothesis: "There is a linear relationship between cybersecurity behavior and 2FA security".



Regression Statistics	
Multiple R	0,133
R Square	0,018
Adjusted R Square	0,005
Standard Error	4,898
Observations	80

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	33,916	33,916	1,414	0,238
Residual	78	1870,972	23,987		
Total	79	1904,888			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95,0%*	*Upper 95,0%*
Intercept	30,801	4,271	7,212	< 0,001	22,299	39,303	22,299	39,303
Cybersecuirty (SeBIS)	0,089	0,075	1,189	0,238	-0,060	0,239	-0,060	0,239

Fig. 1. Linear regression statistics.

From the ANOVA table in *Fig 1*, a p value of 0.238 is obtained. This p value means that at a 95% significance level, there is not enough evidence to reject the null hypothesis. Thus, the results suggest that there is not enough evidence to establish a linear relationship between the cybersecurity scale and the 2FA security scale. Thus unfortunately, the first assumption is not satisfied.

Although assumption one is not satisfied, assumptions two, three and four are true for this case. The graph in Appendix C.1 suggests that the data is normally distributed as a straight line may be plotted across it, thus satisfying assumption 2. Assumption 3 can be satisfied through a correlation matrix of all scale items (*Appendix C.2*). As no items have a correlation with absolute value of 1 or greater with another item other than itself, this assumption is satisfied. The final assumption can be satisfied through the inspection of the residual plot graph (*Appendix C.3*). As seen the residuals are scattered relatively randomly and are present above and below the x-axis thus satisfying this assumption.

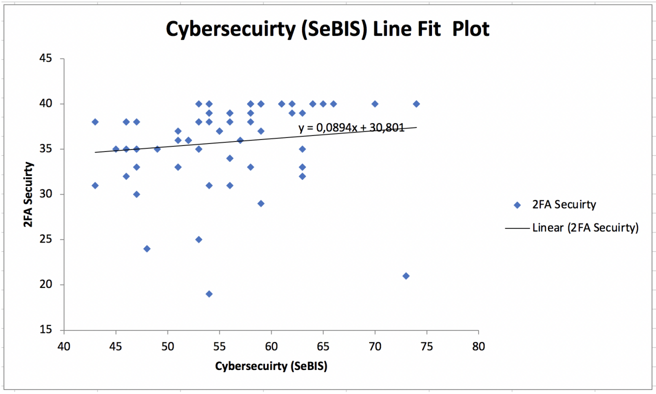


Fig. 2. Linear regression graph.

Fig 2 illustrates the linear regression of these two scales along with the line of best fit. The line of best fit has the formula y = 0.089x + 30.801, which is the regression equation, with x as Cybersecuirty and y as 2FA security. The gradient of the line is 0.089 when rounded thus suggesting that there is barely any correlation between the two from the data provided as this would mean that for every increase of one point in Cybersecurity, there will only be a 0.089 point increase in 2FA security, meaning that this is an incredibly weak correlation or no correlation at all.

The result of the graph is also supported by the coefficients table present in *Fig 1.* As seen in the graph, both the correlation coefficient and y-intercept match the gradient and the intercept in the formula presented in *Fig 2.* The results of the coefficient table can also be used in a null-hypothesis significance test where the null hypothesis is; “The intercept or slope equals 0” and the alternative hypothesis is; “The intercept or slope is not equal to 0”. Through the p values in the coefficient table, it can be stated that at a 95% significance level, there is not enough evidence to reject the null hypothesis. In other words, there is not enough evidence to prove that cybersecurity is a significant variable that impacts 2FA security. This is so as not both the p values are below the alpha value of 0.05 (Cybersecuirty has p value of 0.238).

6 DISCUSSION

In order to answer the question of whether the content of 2FA SMS messages or user IT knowledge play a role in the security of 2FA SMSs, we devised a survey which will both investigate the relationship between cybersecurity behavior and 2FA security. In this study cybersecurity behavior was used to represent IT knowledge and a validated scale was used to measure this. However, since there are no scales that measure 2FA security for a user specifically, we created a scale for 2FA security which mainly measures how susceptible to 2FA SMS security breaches a certain individual is. The survey also records OTP entries from respondents to analyze their contents.

From the data received in this study through the survey, it would suggest that the 2FA Scale that was created and used is a somewhat acceptable scale to be used to measure 2FA security. The Cronbach’s alpha of the whole scale is at an acceptable level and the item correlations of the scale is also at an acceptable level. However, perhaps some items may be added or removed to improve the scale. The scale may also need to be verified and validated even further with other methods such as factor analysis and Kaiser’s Criterion and using other survey populations to improve reliability and consistency.

The data pertaining to OTP message entries used for 2FA from the survey can be used to anwer RQ2. From the analysis, it would appear that there are not any blatant elements present in OTP messages to compromise the integrity of 2FA via SMS. However, there are certainly some elements that can be improved upon to minimize the possibility of a security breach. I believe that if a higher percentage of OTP messages contained a warning element, at least the success rate of *Verification Code Forwarding Attack (VCFA)*[13] would be decreased from its current success rate of 50%. This is so as for this type of social engineering attack to be successful, the user of 2FA must be tricked by the attacker into sharing their OTP token to the attacker through SMS by sending messages such as “Did you request a password reset for your Gmail account? Delete this message if you did. Otherwise, send Cancel + the verification code we sent you.” to the 2FA SMS user. If the user falls victim by believing this message and sends their OTP token, then the attacker will successfully obtain the token and breach 2FA SMS. However, if all legitimate OTP messages sent to 2FA users contained messages such as “Do not share this code. Klarna representatives will never reach out to you to verify this code over the phone or SMS.”, even if the user is not aware of VCFA, due to the warning provided in the OTP message, the chance of the user falling victim to the attack may decrease.

After validating the survey results and using the data to perform simple linear regression on the two scales which represents cybersecurity behavior and 2FA SMS security, it is concluded that there is not enough evidence, from the results, to suggest that there is a significant relationship between the two scales. Thus, as an answer to RQ3, there is no relationship between an individual’s IT knowledge/behavior and the security of 2FA SMS or susceptibility to 2FA SMS security breach to be exact as there is not enough evidence to suggest that a relationship does exist from the study.

6.1 Shortcomings & Future Work

There are many points in this study that may be altered and improved. The first point is the scale used to measure 2FA SMS security. As a widely used and validated scale for this does not exist, this study was forced to create a previously unvalidated scale and use it as part of a linear regression. This would mean one of the premises in which the linear regression is based upon is not validated yet. Thus, perhaps this study may be conducted once more using a reliable & validated scale to measure an individual's 2FA SMS security once one is created. This study also uses a relatively small number of participants thus results may be somewhat unreliable. Thus perhaps a similar study may be conducted with more participants and not using the EEMCS department of University of Twente as the survey population or at least not specific to one department so that different individual IT backgrounds/knowledge may be compared.

Another study may also be conducted with the focus of OTP content messages and how it may affect different *social engineering attacks* specifically. For example, a study may be conducted to investigate whether having a warning element in an OTP message will indeed decrease the success rate of *Verification Code Forwarding Attacks.* CIOs may also use the information from this study, especially the part of OTP content analysis (RQ2) to carefully choose the elements present in OTP messages to minimize the risk of 2FA security to be compromised and decrease the chances of a successful attack.

ACKNOWLEDGMENTS

I would like to express my gratitude towards Fons Wijnhoven, the track chair, for this wonderful opportunity to conduct a study. I would also like to thank Jan-Willem Bullee, my supervisor, for all the guidance, help and recommendations. And I would finally like to thank all who participated in the study.

REFERENCES

[1] Egelman, S., & Peer, E. (2015). Scaling the Security Wall. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. https://doi.org/10.1145/2702123.2702249

[2] Bland, J. M., & Altman, D. G. (1997). Statistics notes: Cronbach's alpha. BMJ, 314(7080), 572. https://doi.org/10.1136/bmj.314.7080.572

[3] Everitt, B. S. The Cambridge Dictionary of Statistics. Cambridge University Press, Cambridge, UK, 2002.

[4] Hair, J. F., Tatham, R. L., Anderson, R. E., and Black, W. Multivariate Data Analysis, 6 ed. Prentice Hall, 2006

[5] Jover, R. P. (2020). Security analysis of SMS as a second factor of authentication. Communications of the ACM, 63(12), 46-52.

[6] Jr., B. B. B., & Vibar, J. C. N. (2021). Authentication Key-Exchange Using SMS for Web-Based Platforms. Journal of Computer and Communications, 09(08), 1–12. https://doi.org/10.4236/jcc.2021.98001

[7] Lartey, K.H., Li, M., Botchey, F.E. and Qin, Z. (2021) Human Factor, a Critical Weak Point in the Information Security of an Organization's Internet of Things. Heliyon, 7, Article No. E06522. https://doi.org/10.1016/j.heliyon.2021.e06522

[8] McKinley, R. K., Manku-Scott, T., Hastings, A. M., French, D. P., & Baker, R. (1997). Reliability and validity of a new measure of patient satisfaction with out of hours primary medical care in the united kingdom: development of a patient questionnaire. BMJ, 314(7075), 193. https://doi.org/10.1136/bmj.314.7075.193

[9] Mulliner, C., Borgaonkar, R., Stewin, P., Seifert, JP. (2013). SMS-Based One-Time Passwords: Attacks and Defense. In: Rieck, K., Stewin, P., Seifert, JP. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2013. Lecture Notes in Computer Science, vol 7967. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39235-1_9

[10] Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work, 24(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

[11] Reaves, B., Scaife, N., Tian, D., Blue, L., Traynor, P., & Butler, K. R. B. (2016). Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. 2016 IEEE Symposium on Security and Privacy (SP). https://doi.org/10.1109/sp.2016.28

[12] Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A Usability Study of Five {Two-Factor} Authentication Methods. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 357-370).

[13] Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., & Memon, N. (2017). Mind your SMSes: Mitigating social engineering in second factor authentication. Computers & Security, 65, 14–28. https://doi.org/10.1016/j.cose.2016.09.009

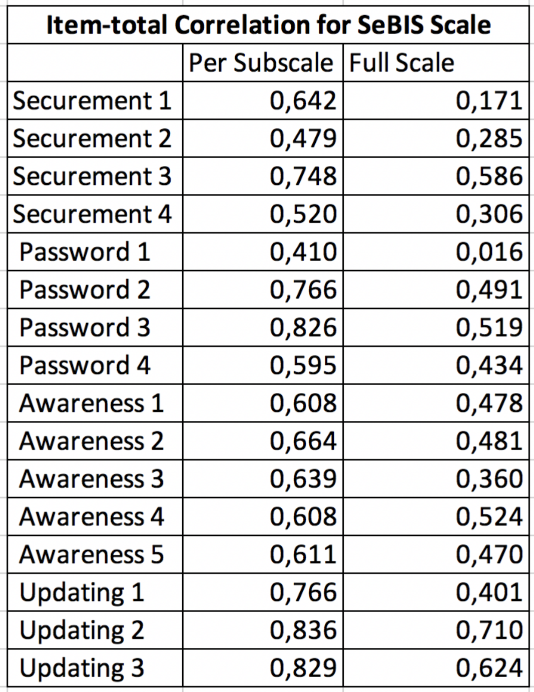
[14] Ulqinaku, E., Lain, D., & Capkun, S. (2019). 2FA-PP. Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. https://doi.org/10.1145/3317549.3323404

[15] Watters, P., Scolyer-Gray, P., Kayes, A., & Chowdhury, M. J. M. (2019). This would work perfectly if it weren't for all the humans: Two factor authentication in late modern societies. First Monday. https://doi.org/10.5210/fm.v24i7.10095

[16] Statistics Solutions. (2021, August 11). Assumptions of Linear Regression. https://www.statisticssolutions.com/free-resources/directory-of-statistical-analyses/assumptions-of-linear-regression/

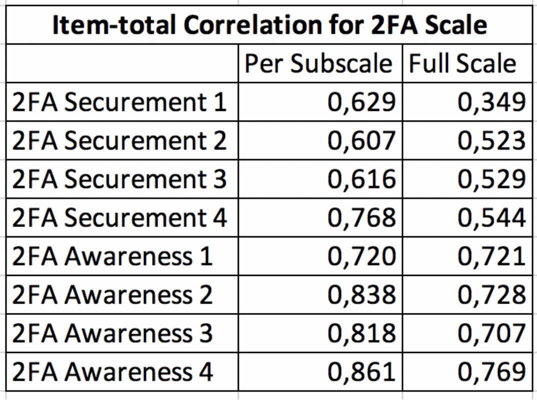
A APPENDIX

A.1 Appendix A.1



Item-total Correlation for SeBIS Scale		
	Per Subscale	Full Scale
Securement 1	0,642	0,171
Securement 2	0,479	0,285
Securement 3	0,748	0,586
Securement 4	0,520	0,306
Password 1	0,410	0,016
Password 2	0,766	0,491
Password 3	0,826	0,519
Password 4	0,595	0,434
Awareness 1	0,608	0,478
Awareness 2	0,664	0,481
Awareness 3	0,639	0,360
Awareness 4	0,608	0,524
Awareness 5	0,611	0,470
Updating 1	0,766	0,401
Updating 2	0,836	0,710
Updating 3	0,829	0,624

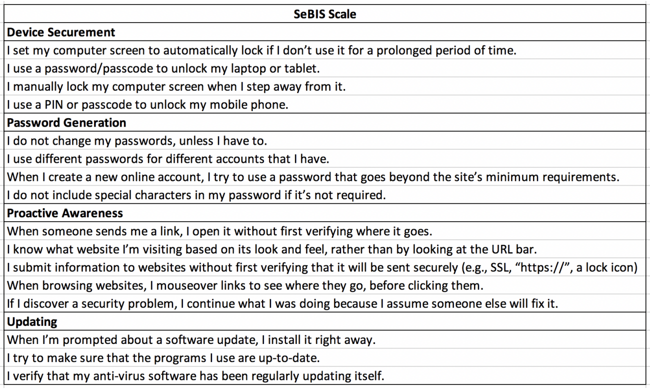
A.2 Appendix A.2



Item-total Correlation for 2FA Scale		
	Per Subscale	Full Scale
2FA Securement 1	0,629	0,349
2FA Securement 2	0,607	0,523
2FA Securement 3	0,616	0,529
2FA Securement 4	0,768	0,544
2FA Awareness 1	0,720	0,721
2FA Awareness 2	0,838	0,728
2FA Awareness 3	0,818	0,707
2FA Awareness 4	0,861	0,769

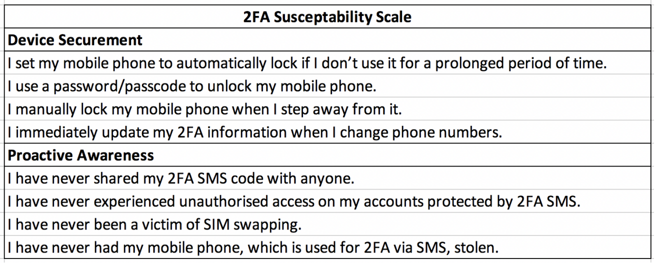
B APPENDIX

B.1 Appendix B.1



SeBIS Scale
Device Securement
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
I use a password/passcode to unlock my laptop or tablet.
I manually lock my computer screen when I step away from it.
I use a PIN or passcode to unlock my mobile phone.
Password Generation
I do not change my passwords, unless I have to.
I use different passwords for different accounts that I have.
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
I do not include special characters in my password if it's not required.
Proactive Awareness
When someone sends me a link, I open it without first verifying where it goes.
I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.
I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon)
When browsing websites, I mouseover links to see where they go, before clicking them.
If I discover a security problem, I continue what I was doing because I assume someone else will fix it.
Updating
When I'm prompted about a software update, I install it right away.
I try to make sure that the programs I use are up-to-date.
I verify that my anti-virus software has been regularly updating itself.

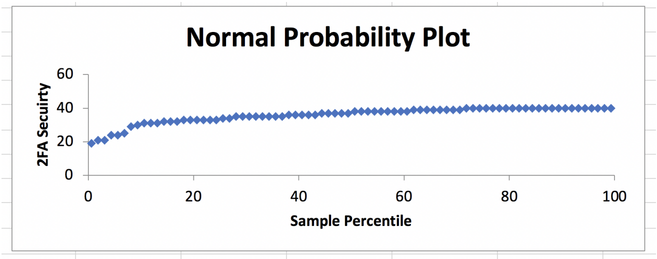
B.2 Appendix B.2



2FA Susceptability Scale
Device Securement
I set my mobile phone to automatically lock if I don't use it for a prolonged period of time.
I use a password/passcode to unlock my mobile phone.
I manually lock my mobile phone when I step away from it.
I immediately update my 2FA information when I change phone numbers.
Proactive Awareness
I have never shared my 2FA SMS code with anyone.
I have never experienced unauthorised access on my accounts protected by 2FA SMS.
I have never been a victim of SIM swapping.
I have never had my mobile phone, which is used for 2FA via SMS, stolen.

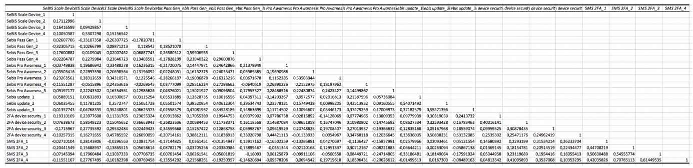
C APPENDIX

C.1 Appendix C.1



C.2 Appendix C.2

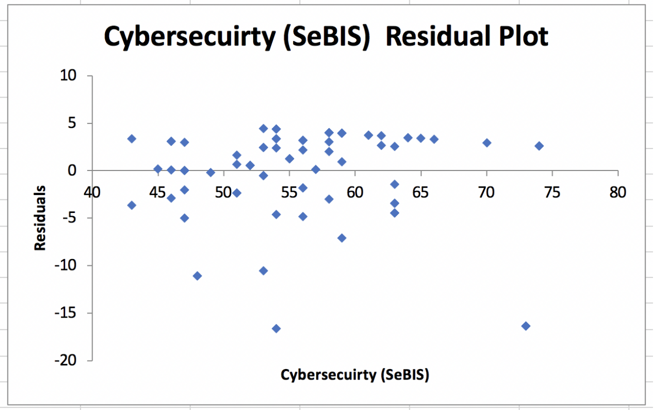
Correlation Matrix (Size was too big to fit)



	SeBIS Scale Device	IS Scale Device	IS Scale Device	IS Scale Device	ebis Pass Gen_	ebis Pass Gen_	ebis Pass Gen_	ebis Pass Gen_	is Pro Awarnes	is Pro Awarnes	is Pro Awarnes	is Pro Awarnes	is Pro Awarnes	Sebis update_1	Sebis update_2	Sebis update_3	device securit	device securit	device securit	device securit	SMS 2FA_1	SMS 2FA_2	SMS 2FA_3	SMS 2FA_4
SeBIS Scale Device_1	1																							
SeBIS Scale Device_2	0,17112996	1																						
SeBIS Scale Device_3	0,16416599	0,09429857	1																					
SeBIS Scale Device_4	0,10050387	0,5307298	0,15156542	1																				
Sebis Pass Gen_1	0,02607706	-0,33107358	-0,26307725	-0,17820781	1																			
Sebis Pass Gen_2	-0,32305715	-0,10266799	0,08871213	0,118542	0,18521078	1																		
Sebis Pass Gen_3	-0,17600882	-0,0109045	0,02007462	0,06887743	0,26580312	0,59906955	1																	
Sebis Pass Gen_4	-0,02204787	0,2279984	0,23646723	0,13403591	-0,17828199	0,23940322	0,29600876	1																
Sebis Pro Awarness_1	-0,03749838	0,19686942	0,33488278	0,16236315	-0,21720075	0,14447971	0,24642866	0,31379949	1															
Sebis Pro Awarness_2	-0,03503416	0,22893598	0,20698564	0,13196092	-0,02248031	0,16132375	0,24035471	0,05985685	0,19690986	1														
Sebis Pro Awarness_3	0,23263561	0,38312659	0,34310571	0,1225546	-0,28266107	-0,19006879	-0,16323216	0,00671678	0,1152285	0,53503944	1													
Sebis Pro Awarness_4	-0,11551287	-0,0515896	0,24353616	-0,0269545	0,03777099	0,28516224	0,27298662	-0,0640619	0,26890226	0,2152975	0,18197962	1												
Sebis Pro Awarness_5	0,09197177	0,22243502	0,16354561	0,12985626	0,04376021	0,15021927	0,09096504	0,17953527	0,28488526	0,22480874	0,2423427	0,14499862	1											
Sebis update_1	0,05889151	0,00632893	0,16500657	0,03115294	0,05531889	0,12628735	0,10016556	0,04397311	-0,14203367	0,0972577	0,02016813	0,21387596	0,05736084	1										
Sebis update_2	0,06035455	0,11781205	0,3572747	0,15061728	0,05501574	0,39520954	0,40612304	0,29534743	0,23378131	0,15749428	0,00998205	0,43513932	0,09160555	0,54071492	1									
Sebis update_3	-0,01357743	-0,04768335	0,35248801	0,06625373	-0,02558579	0,47081952	0,34528189	0,14863699	0,11714502	0,10094607	0,03446173	0,37479259	0,17009973	0,37182579	0,55471396	1								
2FA device security_1	0,19310109	0,23977608	0,11331765	0,23055324	0,09913862	0,17055389	0,19944753	0,09379902	0,07786738	-0,02815892	-0,14128069	0,07774965	0,13809353	0,09779939	0,30319039	0,2413732	1							
2FA device security_2	0,07638673	0,58549223	0,15045652	0,36663943	-0,26823636	0,00684453	0,11738371	0,16118568	0,14687084	0,08651858	0,16747046	0,10980802	0,14745692	0,08627334	0,32593428	0,16783463	0,40016141	1						
2FA device security_3	-0,1715967	0,27735592	0,29532484	0,02449423	-0,34559668	0,15257422	0,12868758	-0,05998767	0,09619529	0,20748825	0,19708407	0,27013937	-0,19366632	-0,12835168	0,05167968	0,18559074	0,09959525	0,30878435	1					
2FA device security_4	-0,10257315	0,16271655	0,45785592	0,26090059	-0,20714161	0,38812111	0,31838913	0,33020798	0,44421113	-0,01133933	0,0054967	0,34768118	0,12036645	0,13636035	0,50838231	0,53132085	0,2535302	0,25471176	0,24962419	1				
SMS 2FA_1	-0,02710104	0,28143806	-0,0296563	0,10831754	-0,17144825	0,0361451	-0,01354947	0,13917162	-0,16502259	-0,13286891	0,04270697	-0,1136427	-0,15837991	0,02579966	0,02093461	0,05121554	0,14680892	0,2293199	0,31534214	0,36233704	1			
SMS 2FA_2	-0,20441549	0,15688937	-0,13865515	0,05658614	-0,08782179	-0,03705256	-0,20380384	-0,13899467	-0,0351344	-0,02120168	0,12951337	0,30712167	-0,08221883	-0,06644211	-0,00263094	-0,05867138	0,01369145	0,18154781	0,20514519	0,22434477	0,44708219	1		
SMS 2FA_3	-0,07145394	0,17960484	-0,13037333	0,07706735	-0,00701454	-0,06261541	-0,05001819	-0,16093	0,06125879	-0,09911106	-0,0500558	-0,08449721	-0,24714805	-0,33186481	-0,18149064	-0,17591924	0,05344958	0,23119689	0,1954416	0,16055413	0,50630488	0,54555774	1	
SMS 2FA_4	-0,11551107	0,27767495	-0,10182398	-0,00769458	-0,13554292	-0,21568261	-0,19250357	-0,14620694	-0,09378206	0,0694542	0,19719618	0,18596431	-0,20626612	-0,01499513	0,0167303	-0,08489163	0,04813342	0,41095893	0,3537008	0,10353295	0,42035826	0,70765113	0,61449535	1

C.3 Appendix C.3

Residual Plot


Cybersecuirty (SeBIS) Residual Plot
Residuals
Cybersecuirty (SeBIS)