Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 9, No. 3, September 2023, pp. 632-648
ISSN: 2338-3070, DOI: 10.26555/jiteki.v9i3.26557

The Usage of Password Generators to Enhance Data Security in Most Used Applications

Erwin Halim [1], Angelia Hartanto Teng [1], Marylise Hebrard [2], David Sundaram [3], Placide Poba-Nzaou [4]
[1] Bina Nusantara University, Jl. Kebon Jeruk 27, Jakarta 11480, Indonesia
[2] Institut Des Usages, Montpellier, France
[3] University of Auckland, Auckland, New Zealand 1010
[4] University of Quebec in Montreal, Montréal, H3C 3P8, QC, Canada

ARTICLE INFO

Article history:

Received June 30, 2023
Revised July 14, 2023
Published July 20, 2023

Keywords:

Password Generator;
Classified Information;
Hackable;
Data Breaches;
Data Security

ABSTRACT

One of the world's global issues is data breaches. These crimes can happen because most people use hackable passwords such as their birthdates and sequencing numbers or alphabets so they would not be easily forgotten. Setting weak passwords in almost or all accounts certainly raises issues and increases the possibility that classified information is hacked and leaked. When it happens, classified data can be misused and taken advantage. This research will help spread awareness to society on how important data security is and how helpful password generators can be to reduce and prevent the probability of data security crimes from happening. This quantitative research uses SMART-PLS as a statistical tool to process the data gathered and random sampling to determine its population. SMART-PLS is variance-based structural equation modeling that uses the partial squares path modeling method. Overall, researchers successfully gathered 114 datasets. Google Forms was used to gather the data. A potential limitation of the study is that all respondents are primarily based in Jakarta. Expanding the geographic focus for further study to gain more insights is highly recommended. 48% of the respondents came from the age group of under 20, occupation as students. Factors significantly affecting people's intention to comply with password generators are perceived password effectiveness, perceived ease of use, subjective norms, and attitude. Eventually, the intention to comply may arouse actual compliance. The result of the study can be used to raise educational campaigns on the usefulness of password generators to promote data security. Based on the result, 78.9% of the respondents are willing to increase their data security. This research contribution is to see how aware people are of data security, how well they know password generators as a technology to generate strong passwords, and how welcome they are with the idea of using password generators.

Corresponding Author:

Erwin Halim, Bina Nusantara University, Jl Kebon Jeruk Raya No. 27, Jakarta 11480, Indonesia
Email: erwinhalim@binus.ac.id

1. INTRODUCTION

Data security is essential to maintain the confidentiality of sensitive information. Data security is necessary for websites, devices, and applications. Users must use strong passwords to lock down data in order for it to be secured [1]. As the world is globalized, technologies evolve. Data security demand fluctuates high. Data security is necessary for social media, messaging services, e-commerce, and entertainment apps [2]. Users should get creative in determining their passwords. Creating solid passwords could be troublesome for most people. Generally, several characteristics determine a good password. First, a good password should contain at least 12 characters and mix uppercase and lowercase letters, numbers, and special symbols [3]. Next, strong passwords should not contain memorable keyboard paths [3]. Lastly, it

should not be based on people's personal information [3]. People should also make sure that passwords are unique for each account.

Users use the same password for many platforms since practically everything requires a password, which makes it easier to remember [4]. In order to remember passwords more quickly and easily, most people pick straightforward passwords like their birthdays or a sequence of digits [5]. These factors made it easy for hackers to breach classified data and information because passwords are considered weak. Weak passwords have led to many cases in the world reporting crime for data leakages. A report revealed that weak passwords were to blame for 80% of data breach crimes [6]. There have been other breaches from Cupid Media's database, which had more than 42 million user passwords, to the parent firm of the New York Sports Club, which kept records of its customers and financial information [7]. As a result, lots of parties felt scathed. Information secretly released to the public could be abused for selfish gain [8]. Another case was about healthcare data breaches. Many practitioners reported that 24.09 million individuals were affected by data breaches from 2005 to 2019 [9].

A data breach is unauthorized access to and disclosing sensitive data worldwide [10]. Data breaches pose severe threats to their victims, from reputational damage to financial losses [11]. Nowadays, people can easily find data on the internet. It indicates a growth in the volume of data. It creates a problem because data volume increases exponentially, and data breaches happen more frequently [11]. In 2022, global cyber-attack numbers increased by 38% compared to 2021 [12]. It is simply because of the pandemic. Due to the pandemic, people faced quarantine. All education and work-related activities were done online. In order to facilitate the activities, collaboration tools such as OneDrive and Google Drive were used [12]. It gives hackers more opportunities to hack and conduct data breaches. Some steps people can take to minimize data breaches are storing data more securely, having a clear desk policy, naming documents more clearly and consistently, and reviewing access control and backup systems [13].

This research aims to observe how willing users are to use a password generator and how much of the population has started using it. The research focuses on determining factors significantly affecting people's use of password generators. The results of this research could be used to create educational campaigns on increasing data security. Overall, this research proposes 15 hypotheses. All of the hypotheses are significant. The research was quantitative, with a total of 161 respondents and a usable dataset 114. Of which mostly live in Jakarta. Expanding the geographic coverage for further study to gain more insights is highly recommended. Respondents' responses were considered valid if they had social media and were interested in using a password generator. Datasets are collected using random sampling and a tool called Google Forms. SMART-PLS, a variance-based structural equation modeling that uses the partial squares path modeling method, is used in this research as a statistic tool to process the data gathered. PLS-SEM was chosen because the structural model is complex, and it includes many constructs, indicators, and model relationships. This research contribution is to see how aware people are of data security, how well they know password generators as a technology to generate strong passwords, and how welcome they are with the idea of using password generators.

2. LITERATURE REVIEW

2.1. Perceived Ease of Use

Perceived ease of use refers to when a person or a group believes using a password generator in practice is relatively easy [5], [14]. According to TAM, perceived ease of use is defined as "the degree" to which an individual believes that by using a particular system, they would be able to enhance their job performance [15]. In this case, an individual or a group must believe that when they use a password generator, this tool can help them enhance their data security. Previous research has also established that perceived ease of use is a crucial factor influencing user acceptance and usage behavior of information technologies [16].

2.2. Perceived Usefulness of Protection

Protection is guaranteed by the usage of security mechanisms [17]. Security refers to providing physical, logical, and procedural safeguards [17]. Therefore, the perceived usefulness of protection talks about users' intention to comply is determined by their beliefs about the roles and responsibilities of information technology. This technology can protect their data assets and improve their work output [5]. In this case, users need to believe that password generators will be able to safeguard their data resources by increasing the security level. By then, their job performance will be enhanced.

2.3. Self-Efficacy

Self-efficacy is a "subjective probability that one can execute a certain course of action" [18]. It influences people regarding how people interpret persuasive messages in which those messages are intended to encourage behavioral change [19]. The impact of self-efficacy is an increase in an individual's commitment, endeavor, and perseverance [20]. Another study defined self-efficacy as a belief that people can successfully execute and perform specific tasks [21]. In this case, self-efficacy refers to when users feel confident with their abilities, skills, and knowledge when using password generators. When users feel confident, strong tendencies to use the technology continuously evoke.

2.4. Intention to Comply

An individual or a group's readiness to commit to forming a habit is referred to as having the intention to comply [8]. Password generator compliance is vital to an individual's information security [22]. The stronger the intention to commit, the more likely the behavior will be carried out. In this case, the stronger the intention of users to comply with password generators, the more likely these users will comply with password generators. A previous study has shown that intention of compliance arises when there is a detection for certainty in which certainty is influenced by security awareness [23] and self-efficacy [24].

2.5. Attitude

Attitude refers to the degree to which the performance of the compliance behavior is positively valued [25]. Assessing attitude helps researchers diagnose which factors affect people's decision on whether or not they will comply with password generators and help researchers identify possible solutions [26]. The attitude of an individual can be measured and evaluated [27]. Attitude refers to the tendency to evaluate objects favorably or unfavorably [28] and is usually defined as permanent mental or neural willingness gained from experience [29]. GISA and security policy change awareness significantly impact this variable. If users can positively value GISA and are aware of security policy changes, they have an attitude. This attitude also will have a significant impact on the intention of users to comply.

2.6. General Information Security (GISA)

General Information Security, or GISA, is defined as an individual or a group's self-learning knowledge obtained by personal efforts regarding issues related to information security and their ramifications [30]. It is often referred to as a state of consciousness and knowledge about security issues and is frequently found to impact security compliance behavior [31]. The knowledge obtained can be from various sources such as the internet, magazines, experiences, or other available sources. In this case, it refers to users' efforts to obtain information regarding data security and password generators.

2.7. Perceived Password Effectiveness

Perceived password effectiveness is defined as users' expectations that following the suggested password recommendations will shield them against dangers involving passwords [4]. In this case, if users believe that a password generator is one of the recommended password guidelines for increasing data security, users will be prevented from password-related threats. The more users feel that the password generator is effective, the higher the chances they will eventually comply [32]. A previous study has shown that perceived password effectiveness significantly influences someone's intention to comply with password guidelines [33].

2.8. Security Policy Change Awareness

Before they can put the anticipated change into practice, an individual or organization must understand the modifications made to security policies [1]. Users must follow security rules because they need more awareness [1]. In this case, users must know security controls to comply with password generators. Password generators are connected with security policies because to secure users' data, users need strong passwords, which password generators can assist by generating strong passwords. Awareness of security policy changes becomes one of the crucial aspects of protection against undesirable information security behaviors [34].

2.9. Subjective Norms

Subjective norms are defined as people's perception of social pressure on whether to perform or not to perform particular behavior after going through several considerations [18]. Therefore, this subjective norm's causal process is likewise regarded as compliance [5]. People may decide to comply with the requirements when behavioral expectations cause it. Some examples of behavioral expectations are essential referents as executives, colleagues, and managers [25].

2.10. Actual Compliance

The variable of actual compliance is linked to the intention to comply. Actual compliance assesses people's willingness and the degree to which their intentions were transformed into compliance-related actions [4]. It is more likely that people will engage in certain conduct the more strongly they plan to commit themselves to doing so [8]. Previous studies stated that actual compliance deals with all regulations individually [35], resulting in disjointed results [35].

2.11. Technology Awareness

Technology awareness concerns individuals' self-consciousness and interest regarding technologies [36]. When dealing with technology, technological awareness becomes mandatory [37]. Whenever people raise their consciousness and are interested in knowing more about technical issues and strategies, these people are aware of the technology. Increasing technology awareness should be one of their efforts [36]. People can obtain information from the internet, magazines, or other resources.

3. METHOD

Data is collected using several filter questions. Responses are only considered valid if respondents have social media accounts and are interested in using a password generator. If respondents qualify for all filter questions, they can proceed with answering the questionnaires. Questionnaires are collected using Google Forms. Statistical analysis was done by looking at the respondent section that Google form has generated. In the respondent section, google form provides statistics according to respondents' responses.

3.1. Analysis Method and Data Source

Structural Equation Modeling (SEM) data analysis techniques are used in this study. Aside from using SEM as a data analysis technique, this study also uses SMART-PLS. SMART-PLS is a statistical tool used for testing hypotheses made. Structural Equation Modeling (SEM) and SMART-PLS in this paper function as data analysis techniques. It is used because research models are built based on previous studies. The research conducted is quantitative and involves complex structuring models. Not only SMART-PLS but the tool named SPSS is also used in this study to eliminate datasets considered outliers. Overall, this study gathered 161 datasets, with usable data from 114 datasets. All respondents come from Indonesia, primarily based in Jakarta. Therefore, it is considered a limitation and threat to validity as responses may contain subjectivity or fail to represent the population. These data are collected online, to be specific, using google forms as the questionnaire, with purposive sampling in January 2023 in Indonesia.

3.2. Research Methodology

Fig. 1, shown above, explains this research's methodology. This research started with problem definition. After a problem was identified, researchers started their literature review. Then, researchers build the research model and construct questionnaires. When everything was ready, researchers collected data using google forms. The responses of the respondents were further checked for their validity. If the respondents do not have social media and are not interested in using a password generator, their responses will not be used. However, the research continued with data entry and analysis if the responses were valid. Then, a further literature survey was conducted. For the last step, researchers will write and edit a journal based on their findings.

3.3. Model Building

Fig. 2 shows the model path coefficient output or this research's model. The model was built by combining several research models from various research conducted. There are eleven variables in total, with 15 hypotheses connecting these variables.

3.4. Hypotheses

Hypothesis 1 (H1): There is a significant impact of perceived password effectiveness on intention to comply. *Hypothesis 2 (H2)*: A significant impact of perceived ease of use on self-efficacy exists. *Hypothesis 3 (H3)*: A significant impact of perceived ease of use on intention to comply exists. *Hypothesis 4 (H4)*: A significant impact of perceived ease of use on the perceived usefulness of protection exists. *Hypothesis 5 (H5)*: Subjective norms significantly impact the perceived usefulness of protection. *Hypothesis 6 (H6)*: There is a significant impact of the perceived usefulness of protection on the intention to comply. *Hypothesis 7 (H7)*: There is a significant impact of the perceived usefulness of protection on self-efficacy. *Hypothesis 8 (H8)*: There is a significant impact of intention to comply on self-efficacy. *Hypothesis 9 (H9)*: Subjective norms significantly impact the intention to comply. *Hypothesis 10 (H10)*: General Information Security

(GISA) significantly impacts self-efficacy. *Hypothesis 11 (H11)*: There is a significant impact of technology awareness on self-efficacy. *Hypothesis 12 (H12)*: General Information Security (GISA) significantly impacts attitude. *Hypothesis 13 (H13)*: Security policy change awareness significantly impacts attitude. *Hypothesis 14 (H14)*: There is a significant impact of attitude on the intention to comply. *Hypothesis 15 (H15)*: There is a significant impact of intention to comply on actual compliance.

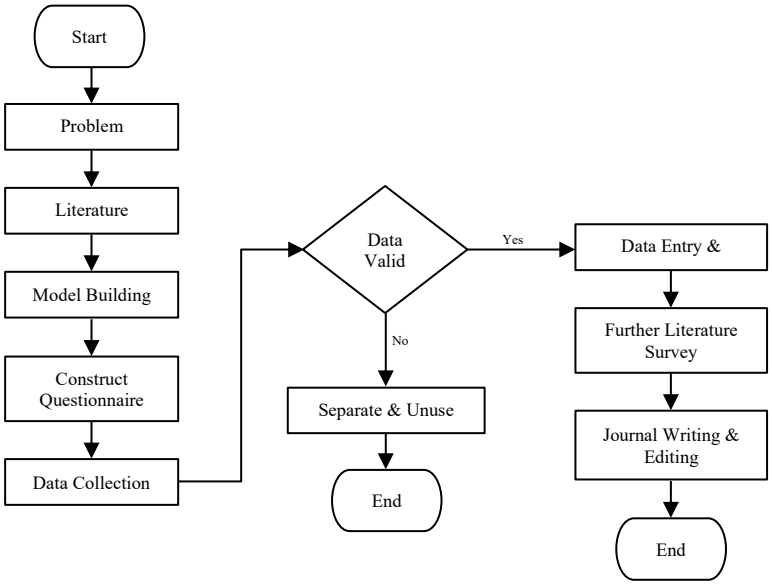

Fig. 1. Research Methodology

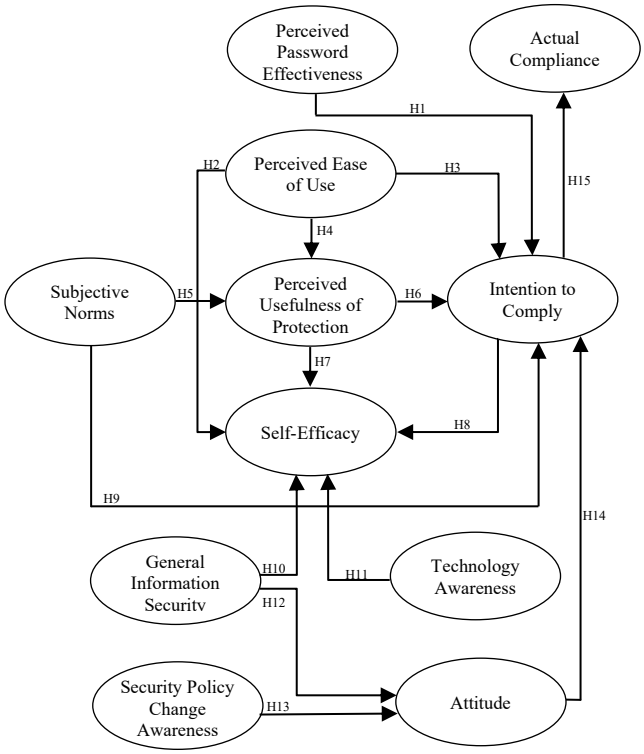

Fig. 2. Model Path Coefficient Output

3.5. Variables and Indicators

In this research, a total of eleven variables are used. Those are perceived ease of use, perceived usefulness of protection, self-efficacy, subjective norms, perceived password effectiveness, intention to comply, actual compliance, General Information Security (GISA), technology awareness, attitude, and

security policy change awareness. Look at the Table 1 for more explanations of these variables and indicators.

Table 1. Variables and indicators

Questionnaire	Code	Ref
Perceived Ease of Use (PU)		
I find it easy to recover from errors encountered when complying with my organization's ISP.	PU1	[5]
Compliance with the requirements of my organization's ISP requires a lot of mental effort.	PU2	[5]
I find it easy to comply with my organization's ISP	PU3	[5]
Perceived Usefulness of Protection (PP)		
Complying with my organization's ISP addresses my job-related security needs.	PP1	[5]
Complying with my organization's ISP saves me time	PP2	[5]
Complying with my organization's ISP enables me to accomplish tasks more securely.	PP3	[5]
Self-Efficacy (SE)		
I have the necessary skills to fulfill the requirements of the ISP	SE1	[2]
I would feel comfortable following my organization's ISP on my own	SE2	[2]
If I wanted to, I could easily comply with my organization's ISP on my own	SE3	[2]
Intention to Comply (IC)		
intend to comply with the requirements of the ISP of my organization	IC1	[2]
I intend to protect information resources according to the requirements of the ISP of my organization.	IC2	[2]
I intend to protect technology resources according to the requirements of the ISP of my organization.	IC3	[2]
Attitude (AT)		
I support the process requiring me to change my password	AT1	[1]
This required change of password will make working with my [university] account saver	AT2	[1]
Mandating this change of password is a good idea	AT3	[1]
General Information Security (GS)		
Overall, I am aware of the potential security threats and their negative consequences.	GS1	[2]
I have sufficient knowledge about the cost of potential security problems	GS2	[2]
I understand the concerns regarding information security and the risks they pose in general.	GS3	[2]
Perceived Password Effectiveness (PE)		
I believe the recommended password guidelines will prevent password-related threats.	PE1	[4]
The likelihood of compliance increases when individuals perceive the recommended response as effective	PE2	[4]
Security Policy Change Awareness (SP)		
I am aware of the requirements prescribed by [university] to change my PID password	SP1	[1]
I understand the rules and requirements regarding the PID password change prescribed by [university]	SP2	[1]
I know my responsibilities to change my PID password as prescribed by [university]	SP3	[1]
Subjective Norms (SN)		
I think my classmates and/or colleagues believe I should change my PID password	SN1	[1]
People who influence my behavior think that I should change my PID password	SN2	[1]
People who are important to me think I should change my password	SN3	[1]
Technology Awareness (TA)		
I follow news and developments about the security related technologies	TA1	[5]
I discuss internet security issues or anecdotes with friends and people around me	TA2	[5]
I read about the problems of malicious threats attacking users' computers	TA3	[2]
Actual Compliance (AC)		
You have already changed your PID password in accordance with the requirement [stated above]	AC1	[4]

4. RESULT and DISCUSSION

4.1. Measurement Model: Validity and Reliability

Validity and reliability are the two most crucial factors in conducting research. Both validity and reliability act as standards of acceptance. It ensures that all data gathered can be considered valid and reliable. The two are used to determine the loading factor obtained from the calculated results of the SMART PLS. In general, the ideal loading factor value ranges from 0.7 and above. As much as possible, the loading factor cannot be lower than 0.7. However, if the loading factor equals or exceeds 0.5, it can still be considered ideal [38]. Aside from the loading factor, another important factor used in this research is the Average Variance Extracted (AVE). AVE describes the relationship between each indicator and its latent variable. The ideal value of AVE should be at least 0.5 [39]. Fig. 3 shows the original path coefficient output before changes are made. Some loading factors and AVE need to meet the standards. For an in-depth explanation of each value, refer to Table 2. Table 2 shows the variables and indicators' validity based on their cross-loading, Average Variance Extracted (AVE), Composite Reliability (CR), and Cronbach Alpha (CA) values.

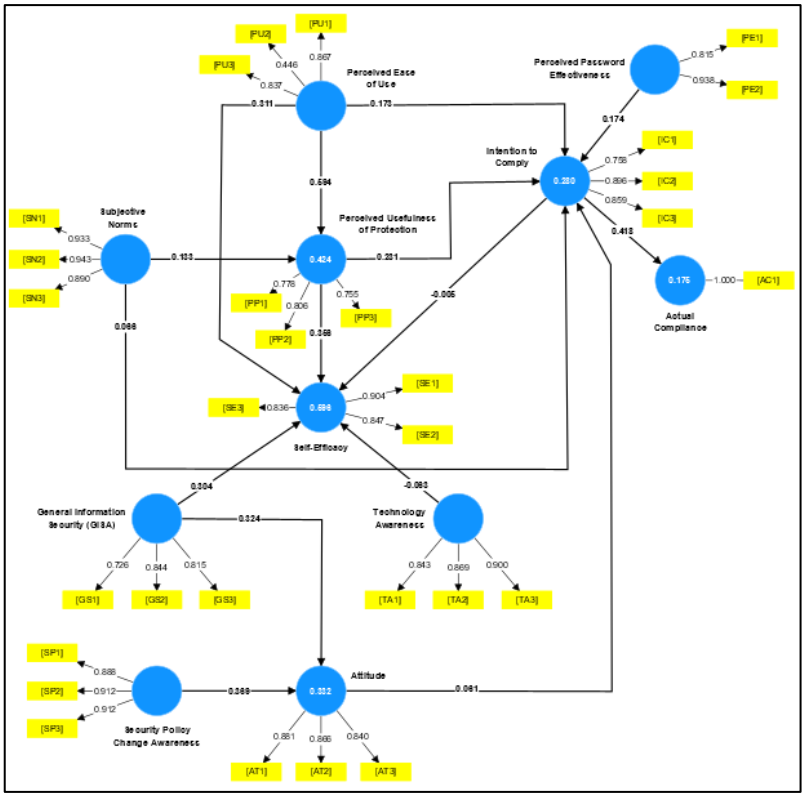

Fig. 3. Path Coefficient Output (Before)

Based on Table 2, all variables have the ideal AVE value ranging from 0.550 to 0.850. Besides all indicators having an excellent AVE value, they must also pass through the ideal cross-loading factors of 0.7. Only one indicator does not pass the minimum standard of cross-loading factor, variable PU2, with a cross-loading value of 0.446. As a result, the variable's CA is affected. Variable PU's CA falls short of the recommended standard CA value [40]. Variable PU has a CA value of 0.580. Aside from variable PU, variable PP's CA also does not pass the minimum standard of CA value. The perceived usefulness of protection (PP)'s CA value is 0.680.

Fig. 4 shows bootstrapping result before changes are made using SMART-PLS software. Looking at the p-values, only eight hypotheses proposed from this model can be considered valid or significant. P-values are considered valid when their values are equal to or below 0.05. Most p-values and the t-values also need to pass the excellent standard value. For an in-depth explanation of each proposed hypothesis's significance, refer to Table 3.

Table 2. Variables and indicators validity (before)

No.	Variable & Indicators	Cross Loading	AVE	CR	CA
	AT		**0.744**	**0.897**	**0.829**
1.	AT1	0.881			
2.	AT2	0.866			
3.	AT3	0.840			
	GS		**0.635**	**0.839**	**0.711**
4.	GS1	0.726			
5.	GS2	0.844			
6.	GS3	0.815			
	IC		**0.705**	**0.877**	**0.789**
7.	IC1	0.758			
8.	IC2	0.896			
9.	IC3	0.859			
	PU		**0.550**	**0.774**	**0.580**
10.	PU1	0.867			
11.	PU2	0.446			
12.	PU3	0.837			
	PE		**0.771**	**0.870**	**0.720**
13.	PE1	0.815			
14.	PE2	0.938			
	PP		**0.609**	**0.823**	**0.680**
15.	PP1	0.778			
16.	PP2	0.806			
17.	PP3	0.755			
	SP		**0.818**	**0.931**	**0.889**
18.	SP1	0.888			
19.	SP2	0.912			
20.	SP3	0.912			
	SE		**0.745**	**0.897**	**0.828**
21.	SE1	0.904			
22.	SE2	0.847			
23.	SE3	0.836			
	SN		**0.850**	**0.945**	**0.912**
24.	SN1	0.933			
25.	SN2	0.943			
26.	SN3	0.890			
	TA		**0.759**	**0.904**	**0.841**
27.	TA1	0.843			
28.	TA2	0.869			
29.	TA3	0.900			

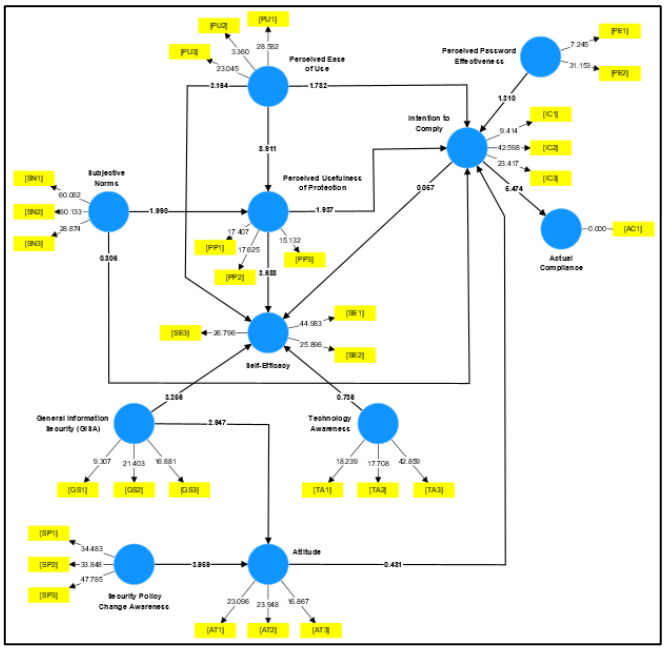

Fig. 4. Bootstrapping Result (Before)

Table 3. Path coefficient (before)

Relation and Hypotheses	Ori Sample	Sample Ave.	Stand. Dev	t-stat	p-value
PE to IC (H1)	0.174	0.192	0.133	1.310	0.190
PU to SE (H2)	0.311	0.308	0.098	3.164	0.002
PU to IC (H3)	0.173	0.170	0.097	1.782	0.075
PU to PP (H4)	0.594	0.596	0.067	8.911	0.000
SN to PP (H5)	0.133	0.136	0.067	1.990	0.047
PP to IC (H6)	0.231	0.210	0.119	1.937	0.053
PP to SE (H7)	0.356	0.355	0.097	3.688	0.000
IC to SE (H8)	-0.005	-0.002	0.084	0.057	0.955
SN to IC (H9)	0.066	0.074	0.082	0.806	0.420
GS to SE (H10)	0.304	0.305	0.093	3.256	0.001
TA to SE (H11)	-0.063	-0.059	0.086	0.736	0.462
GS to AT (H12)	0.324	0.331	0.110	2.947	0.003
SP to AT (H13)	0.369	0.381	0.093	3.959	0.000
AT to IC (H14)	0.061	0.067	0.128	0.481	0.630
IC to AC (H15)	0.418	0.422	0.076	5.474	0.000

According to the theory of Argumentum ad hominem, the digressions are due to acceptance or rejection of the hypotheses made [41]. Rejection or acceptance of the hypotheses made is due to the respondents' circumstances and how they respond to the questions in the questionnaire made by the researcher. The responses could vary for different individuals. The researcher's way of explaining the concept of a password generator or asking respondents to answer the questionnaire might be subjective and eventually affect their responses [41]. Hence, it may lead to digressions made and, eventually, the insignificance of hypotheses. Subjectivity can be caused by several factors, such as people's race, gender, position, and other factors.

For instance, there was discrimination in South Africa [41]. Where white-skinned and black-skinned people were not given the same right when it came to giving opinions and arguments. When debate happens, most of the time, black-skinned people's arguments are not taken seriously. Other examples include, during trials, the plaintiff and the defendant's family members are not allowed to give testimonies [41]. This theory can then be applied to this research paper's insignificant hypotheses. Respondents' responses may contain subjectivity. For example, the respondents mostly are researchers' friends, families, relatives, or someone close to the researcher. It may affect the reliability and validity of the responses. During trials, someone close to the victims cannot give testimonies to prevent subjectivity, whereas this research does not implement the same action. This research is open to the public without any exclusions. Therefore, relatives or close ones are allowed to give responses, whether it being subjective or not. In addition, the data gathered and used in this research was only 114, mostly domiciliated in Jakarta. The datasets may fail to represent the whole population. It adds to the research's validity limitations.

Variables are written in abbreviations to shorten their form of writing. For instance, the variable perceived password effectiveness is PE, and intention to comply is IC. Based on previous studies, all hypotheses proposed in this research are proven significant or valid. Refer to the list below for in-depth explanations of each hypothesis proposed. H1: According to a previous study, perceived password effectiveness significantly impacts the intention to comply [4]. H2: According to a previous study, perceived ease of use significantly impacts self-efficacy [5]. H3: According to a previous study, perceived ease of use significantly impacts the intention to comply [5]. H4: According to a previous study, perceived ease of use significantly impacts the perceived usefulness of protection [5]. H5: According to a previous study, subjective norms significantly impact the perceived usefulness of protection [5]. H6: According to a previous study, the perceived usefulness of protection significantly impacts the intention to comply [5]. H7: According to a previous study, the perceived usefulness of protection significantly impacts self-efficacy [5]. H8: According to a previous study, intention to comply significantly impacts self-efficacy [2]. H9: According to a previous study, subjective norms significantly impact the intention to comply [2]. H10: According to a previous study, General Information Security (GISA) significantly impacts self-efficacy [2]. H11: According to a previous study, technology awareness significantly impacts self-efficacy [2]. H12: According to a previous study, General Information Security (GISA) significantly impacts attitude [2]. H13: According to a previous study, security policy change awareness significantly impacts attitude [1]. H14: According to a previous study, attitude significantly impacts the intention to comply [2]. H15: According to a previous study, intention to comply significantly impacts actual compliance [4].

Acknowledging the limitations of the research, researchers decided to base this research on previous studies that had been conducted. According to previous studies, all hypotheses proposed in this research should yield significance. Therefore, researchers make some changes and upgrades to the research model. Changes and upgrades were made to the research model in the hope that it would produce better and more acceptable outcomes despite this research's limitations. Some of the changes and upgrades done are

eliminating data considered outliers and reconstructing the variables and indicators used in this research. All changes and upgrades were done to minimize subjectivity and failure in representing the geographic population. For future research, it is highly recommended that researchers collect more respondents from various geographical areas. It is done to minimize or even eliminate subjectivity from happening. More data is gathered to increase the percentage of validity and reliability as it can better represent the population. In total, there are seven insignificant hypotheses and eight significant hypotheses. Insignificant hypotheses are almost 50% of the significant ones. Compared to previous studies, this finding surely contradicts previous studies. Hence, changes and upgrades should be made in this research. This research's validity and reliability may be maintained if changes and upgrades are made.

Fig. 5, shown above, shows the path coefficient output after several changes are made. Overall, 13 datasets considered outliers are removed, four insignificant hypotheses are removed from the model, and the indicator PU2 is removed because its cross-loading value did not meet the standard ideal value. In addition, the variable TA, technology awareness, is also removed from the model. Variable TA is considered an unreliable variable. It is because its indicators all resulted in excellent cross-loading values. The variables AVE, CA, and CR all passed the ideal standard values. It shows that the variable is valid. However, if the t-stat and p-value are considered, the TA to SE's hypotheses are insignificant and, therefore, should be removed. The variable TA is only connected to one variable, variable SE. Therefore, removing the hypotheses connecting the two means that the variable TA should also be removed from the model.

Based on the result of Table 4 above, the conclusion that all variables in the table are valid can be made. All variables have an AVE value ranging from 0.630 to 0.874, higher than 0.5. On top of that, all of the loading factors succeeded in passing the ideal range, which is 0.7.

Table 4. Variables and indicators validity (after)

No.	Variable & Indicators	Cross Loading	AVE	CR	CA
	AT		**0.701**	**0.875**	**0.788**
1.	AT1	0.842			
2.	AT2	0.852			
3.	AT3	0.817			
	GS		**0.638**	**0.841**	**0.717**
4.	GS1	0.767			
5.	GS2	0.807			
6.	GS3	0.821			
	IC		**0.681**	**0.865**	**0.764**
7.	IC1	0.783			
8.	IC2	0.881			
9.	IC3	0.808			
	PU		**0.781**	**0.877**	**0.720**
10.	PU1	0.893			
11.	PU2	0.875			
	PE		**0.774**	**0.872**	**0.714**
12.	PE1	0.840			
13.	PE2	0.917			
	PP		**0.630**	**0.836**	**0.709**
14.	PP1	0.796			
15.	PP2	0.798			
16.	PP3	0.788			
	SP		**0.771**	**0.910**	**0.851**
17.	SP1	0.864			
18.	SP2	0.880			
19.	SP3	0.890			
	SE		**0.712**	**0.881**	**0.797**
20.	SE1	0.886			
21.	SE2	0.837			
22.	SE3	0.807			
	SN		**0.874**	**0.954**	**0.929**
23.	SN1	0.947			
24.	SN2	0.956			
25.	SN3	0.900			

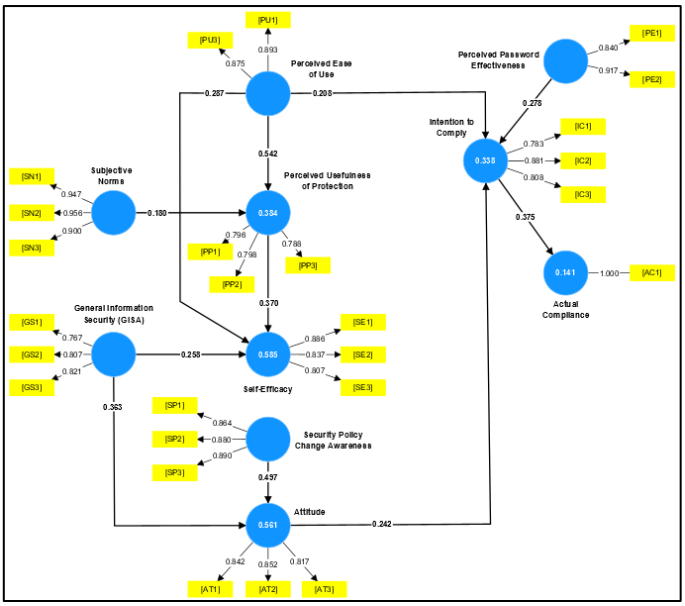

Fig. 5. Path Coefficient Output (After)

Above are the results of bootstrapping using SMART PLS software. All indicators shown above are valid. The T-values are above 1.96, ranging from 2.342 to 7.464, and the P-values below 0.05, ranging from 0 to 0.019. Below is Table 5, which shows the final path coefficient of this research. The results shown in Table 6 conclude that all eleven hypotheses are significant. If all hypotheses are now considered significant, then all variables are also crucial and will impact the usage of password generators. For instance, if people know perceived password effectiveness, they will likely have the intention to comply with the usage of password generators. Eventually, this research paper has proven and points out all factors affecting people's decision on whether or not they will comply and use password generators to enhance their data security. In order to comply with and use password generators, users need to feel perceived password effectiveness, perceived ease of use, and perceived usefulness of protection from password generators. Aside from that, users alone should be aware of security policy changes and general information security and have subjective norms. This way, it creates a positive attitude toward the usage of password generators. Hence, it will lead to users' intention to comply. When there is the intention to comply, it eventually leads to actual compliance.

Table 5. Path coefficient (after)

Relation and Hypotheses	Ori Sample	Sample Ave.	Stand. Dev	t-stat	p-value
PE to IC (H1)	0.278	0.282	0.103	2.714	0.007
PU to SE (H2)	0.287	0.284	0.103	2.779	0.005
PU to IC (H3)	0.208	0.212	0.088	2.365	0.018
PU to PP (H4)	0.542	0.545	0.073	7.464	0.000
SN to PP (H5)	0.180	0.182	0.072	2.507	0.012
PP to SE (H7)	0.370	0.375	0.098	3.782	0.000
GS to SE (H10)	0.258	0.260	0.093	2.766	0.006
GS to AT (H12)	0.363	0.367	0.080	4.554	0.000
SP to AT (H13)	0.497	0.496	0.075	6.620	0.000
AT to IC (H14)	0.242	0.242	0.103	2.342	0.019
IC to AC (H15)	0.375	0.378	0.084	4.464	0.000

4.2. Indicators and Variables

The value of cross-loading for the variable attitude ranges from 0.817 to 0.852, more or less similar. The highest value goes to AT2. All indicators have similar relevancy in this research. A variable attitude is needed for potential users to start using a password generator. Potential users should have a supportive attitude towards changing passwords, believe that password generators will make their accounts more secure, and have a positive attitude that states that changing the password is a good idea.

This research aims to discover how aware people are of data security and how welcome they are to using password generators. Fig. 6 shows the final bootstrapping result. It indicates that people are aware of data security. It can be further proven by looking at the variable security policy change awareness (SP),

which is significant. Aside from fulfilling the first research objective, this paper also successfully figures out how welcome people are with the idea of using a password generator. With all variables being significant, it eventually leads to the conclusion that people are willing or intend to comply with the usage of password generators. Hence, the intention to comply will become actual compliance.

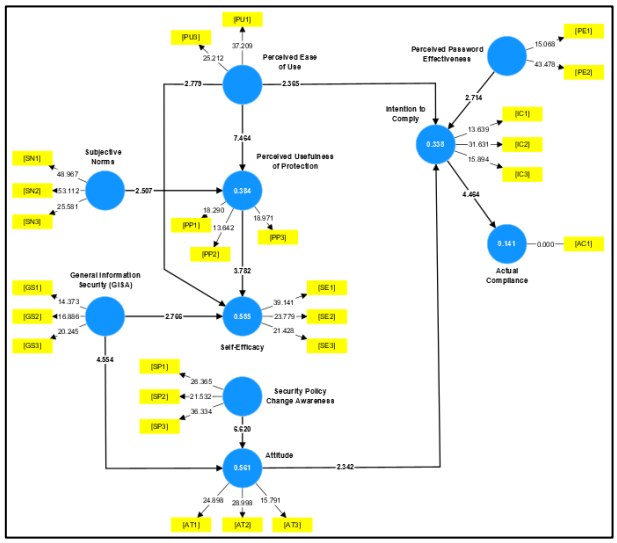

Fig. 6. Bootstrapping Result (After)

It also applies to the variable General Information Security (GISA). Variable GS's cross-loading value ranges from 0.767 to 0.821, with GS3 as the highest value among other variable indicators. In conclusion, people are considered potential users of password generators if they are interested in GISA. Potential users are considered interested if they know the security threats and their negative consequences, have sufficient knowledge of the disadvantages of potential security problems, and understand the concern for information security and the risk.

The variable IC, intention to comply, has a cross-loading value ranging from 0.783 to 0.881. The highest cross-loading value goes to indicator IC2. IC2 has a more significant impact on this research than the other two indicators. In order for potential users to use a password generator, they need to have the intention to comply, whether it is the intention to comply with the requirements needed or the intention to protect information resources along with any technology resources that a password generator possesses.

The range of cross-loading value for the variable perceived ease of use is 0.875 to 0.893. The lowest cross-loading value goes to indicator PU2. That said, indicator PU2 has the lowest impact on this research compared to the other indicator in this variable. Potential users need to feel the perceived ease of using a password generator to decide whether to use it. The easier the usage and the less effort required, the higher the chances that potential users will use the password generator.

The variable PE, perceived password effectiveness, has a similar cross-loading value. Both indicators have the same impact on this research. Potential users should feel the perceived password effectiveness before deciding whether to use a password generator. If the generated passwords are considered ineffective and increase the potential risks of security threats, users will not use a password generator.

PP variable, perceived usefulness of protection, has a cross-loading value ranging from 0.788 to 0.798. Indicator PP2 has a slightly more excellent loading value than the other two indicators. It means that PP2 has a more significant impact on this research. Without feeling the perceived usefulness of protection while using the generated password that the password generator created, potential users will not be willing to use the password generator.

The variable security policy change awareness, SP, has a similar cross-loading value that ranges from 0.864 to 0.890. Users are considered potential users of password generators if they are aware of security policy changes. No awareness means that users do not care or pay attention to their account's security. They will not be interested in software such as password generators.

Variable self-efficacy, SE, has a cross-loading value ranging from 0.807 to 0.886. The highest loading value goes to indicator SE1. Therefore, SE1 has a slightly more significant impact on this research. Self-efficacy is about an individual's skills and comfort when using a password generator. Potential users should

have self-efficacy before they start using a password generator to ensure they feel confident about their skills using a password generator.

The value of cross-loading for the last variable, subjective norms, more or less are similar. It ranges from 0.900 to 0.956. It means that all indicators have a similar impact on this research. Subjective norms refer to people's perceptions. Due to its social pressure, people may decide on whether or not they will be using a password generator. Hence, this variable is very much needed because it plays a crucial role. It is also proven that the hypotheses concerning this variable are all significant.

4.3. Perceived Password Effectiveness to Intention to Comply

Based on the statistical result, perceived password effectiveness significantly impacts the intention to comply with a t-value of 4.068. This sign shows that users know and agree with how password generators can generate effective passwords, lowering the risk of security threats. Hence, it increases the percentage of users intending to comply.

4.4. Perceived Ease of Use to Self-Efficacy

Based on the statistical result, perceived ease of use significantly impacts self-efficacy, with a t-value of 2.779. It demonstrates that if potential users think using a password generator is simple, it instantly lowers their self-efficacy [5]. It boosts potential users' confidence in using password generators because they feel like they can master and easily use them in the future.

4.5. Perceived Ease of Use to Intention to Comply

Based on the statistical result, perceived ease of use significantly impacts the intention to comply with a t-value of 2.365. When potential users feel the perceived ease of use while using a password generator, there are higher chances that they will eventually try out and use a password generator. With that said, they will grow the intention to comply with all requirements and regulations that password generator possesses.

4.6. Perceived Ease of Use to Perceived Usefulness of Protection

Based on the statistical result, perceived ease of use significantly impacts the perceived usefulness of protection with a t-value of 7.464. Among other hypotheses, this hypothesis has the highest number of t-value. When potential users think they can utilize password generators efficiently to improve their work output, they are said to sense the perceived ease of usage [5]. However, protection is viewed as valuable when potential users believe that employing a password generator would be effortless [5]. Therefore, through the t-value proposed, this hypothesis can be proven significant.

4.7. Subjective Norms to Perceived Usefulness of Protection

Based on the statistical result, subjective norms significantly impact the perceived usefulness of protection with a t-value of 2.507. As mentioned, the perceived usefulness of protection talks about how potential users may gain self-confidence while using a password generator because they know its benefits. Therefore, it is closely related to subjective norms, as subject norms discuss people's perceptions and social pressure. People's perception of password generators will be significantly impacted if they perceive the usefulness of protection while using password generators.

4.8. Perceived Usefulness of Protection to Self-Efficacy

Based on the statistical result, the perceived usefulness of protection significantly impacts self-efficacy, with a t-value of 6.453. As explained above, self-efficacy talks about users' confidence because they have gained skills in operating something, in this case, a password generator. How simple it is for consumers to operate or use password generators is discussed by the various perceived utility of protection [5]. With that said, the two variables are linked.

4.9. General Information Security (GISA) to Self-Efficacy

Based on the statistical result, General Information Security (GISA) significantly impacts self-efficacy with a t-value of 3.782. From the questionnaires gathered, most respondents are already aware of GISA, so they gain confidence when new software, a password generator, concerning information security is introduced. With that being said, GISA is closely related to self-efficacy as it is proven that with GISA, people gain self-efficacy.

4.10. General Information Security (GISA) to Attitude

Based on the statistical result, General Information Security (GISA) significantly impacts attitude with a t-value of 5.649. The results gathered from the questionnaires show that users are already aware of general information security and have sufficient knowledge about security threats. That is why they develop the right positive attitude and can welcome password generators well as one of the solutions to reduce the risk of security threats.

4.11. Security Policy Change Awareness to Attitude

Based on the statistical result, security policy change awareness significantly impacts attitude with a t-value of 7.381. The results gathered from the questionnaires show that people are aware of the changes made in security policies. Due to this awareness, people develop positive and welcoming attitudes toward password generators because they can help reduce any threats regarding security from happening.

4.12. Attitude to Intention to Comply

Based on the statistical result, attitude significantly impacts the intention to comply with a t-value of 3.666. This t-value agrees with the outcome of [2]. The research shows that users have the right attitude toward password generators. They are willing to support changes made to their passwords to increase the security levels of their accounts. Therefore, these users can be said to have the intention to comply.

4.13. Intention to Comply with Actual Compliance

Based on the statistical result, the intention to comply significantly impacts the actual compliance with a t-value of 4.464. As mentioned earlier, the intention to comply is tightly related to actual compliance and is proven true by the significant hypotheses. Potential users of password generators can develop intentions to finally use password generators due to several factors, such as the perceived ease of use in using password generators and perceived password effectiveness from passwords generated by password generators. Hence, most respondents finally agreed to use a password generator.

The data gathered from questionnaires proved all of the hypotheses significant in this research. All variables and indicators pass the ideal standards. The p-values all do not pass the limit, which is 0.05, and the t-values all pass through 1.96 as its boundary. Moreover, all indicators pass through the excellent cross-loading value of 0.7. Lastly, to ensure the credibility of this research's validity and reliability, all variables have an AVE value of more than 0.5 and a CA value of 0.7 and above.

5. CONCLUSION

The most used social media are YouTube and Instagram, while the least used is Facebook. From the questionnaires gathered, people often use passwords containing numbers, capital letters, and small letters. Besides that, people also use birthdays quite frequently as their passwords. Whereas for their key password reminders, the majority of people, approximately 34.6%, use their family members' names. Overall, people generally use a 7-to-8-character password. Looking at the respondents' answers to the descriptive questions, people still use simple passwords that they can easily remember. A tiny percentage of people use strong passwords for their social media accounts. It can be seen that only minors are using an "out of the box" type of password, such as combining famous people's names with numbers. Most people use guessable, simple passwords and critical reminder passwords such as birthdays, names, and family surnames. Weak passwords or key password reminders increase the chance of users getting involved in various security threats, such as data breaches. Leakage of private data may lead to more crimes, such as theft and cyberattacks.

In conclusion, the respondents in this research feel that the perceived ease of use of password generators will significantly impact how they feel about the perceived usefulness of protection of password generator and their self-efficacy. In addition, variables such as GISA, positive attitude, awareness towards security policy, and the feeling of perceived password effectiveness will eventually evoke a sense of intention to comply with any requirements or regulations the password generator possesses. Moreover, most famous and frequently used social media users, such as Instagram and YouTube, should increase their account security. Add more restrictions on people's passwords so that weak passwords are no longer allowed. For example, users should simultaneously use symbols, numbers, and uppercase and lowercase letters for their passwords. Hence, this will assist social media users in protecting and increasing their social media account security. Password generators could be the ideal solution if users feel that setting up stricter passwords is too troublesome. With the help of a password generator, users will have strong passwords that they can use for their account's security in no time as password generator functions to generate strong passwords.

This research ended with eleven significant hypotheses after upgrades and changes were made. Changes and upgrades should be made because of this research's subjectivity limitations and potential failure to represent the whole population. Therefore, this research bases its results on previous studies. Previous studies have proven that all hypotheses proposed in this research are supposedly significant. Therefore, researchers decided to make some changes and upgrades to the research model. After reconstruction, researchers yielded eleven significant hypotheses for this research paper. A summary of the variables' explanation is as follows: to comply with and use a password generator, users need to feel perceived password effectiveness, perceived ease of use, and perceived usefulness of protection from a password generator. Aside from that, users alone should be aware of security policy changes and general information security and have subjective norms. This way, it creates a positive attitude toward the usage of password generators. Hence, it will lead to users' intention to comply. When there is the intention to comply, it eventually leads to actual compliance.

Overall, this research has successfully pointed out crucial factors affecting people's decisions regarding the usage of password generators. The paper also proves that people are aware of data security and are willing to use a password generator to enhance data security. With that said, society can start conducting educational campaigns on password generators to encourage people to start using them. It is highly recommended that further study is conducted based on this research because this research still has limitations. The limitation of this paper includes subjectivity due to respondents' responses bases only in Indonesia, with the majority coming from Jakarta. Geographical area coverage should be expanded in future studies to gain more insights and perspectives. Aside from that, the limitation of this study also sources from the limited datasets gathered. In total, this research only uses a total of 114 respondents. Future studies are recommended to collect more data to increase the research's validity and reliability.

REFERENCES

[1] F. Bélanger, S. Collignon, K. Enget, and E. Negangard, "Determinants of early conformance with information security policies," *Information and Management*, vol. 54, no. 7, pp. 887–901, 2017, https://doi.org/10.1016/j.im.2017.01.003.

[2] A. Al-Omari, O. El-Gayar, and A. Deokar, "Information Security Policy Compliance: The Role of Information Security Awareness," *AMCIS 2012 Proceedings*, pp. 1-10, 2022, https://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/16/.

[3] F. Z. Glory, A. Ul Aftab, O. Tremblay-Savard, and N. Mohammed, "Strong Password Generation Based on User Inputs," *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0416-0423, 2019, https://doi.org/10.1109/IEMCON.2019.8936178.

[4] F. Mwagwabi, T. McGill, and M. Dixon, "Short-term and long-term effects of fear appeals in improving compliance with password guidelines," *Communications of the Association for Information Systems*, vol. 42, no. 1, pp. 147–182, 2018, https://doi.org/10.17705/1CAIS.04207.

[5] A. Al-Omari, O. El-Gayar, and A. Deokar, "Security Policy Compliance: User Acceptance Perspective," *2012 45th Hawaii International Conference on System Sciences*, pp. 3317-3326, 2012, https://doi.org/10.1109/HICSS.2012.516.

[6] Z. Hassanzadeh, R. Biddle, and S. Marsen, "User Perception of Data Breaches," in *IEEE Transactions on Professional Communication*, vol. 64, no. 4, pp. 374-389, 2021, https://doi.org/10.1109/TPC.2021.3110545.

[7] S. Raponi and R. D. Pietro, "A Longitudinal Study on Web-Sites Password Management (in)Security: Evidence and Remedies," in *IEEE Access*, vol. 8, pp. 52075-52090, 2020, https://doi.org/10.1109/ACCESS.2020.2981207.

[8] M. Siponen, M. Adam Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Information & Management*, vol. 51, no. 2, pp. 217–224, 2014, https://doi.org/10.1016/j.im.2013.08.006.

[9] A. H. Seh *et al.*, "Healthcare Data Breaches: Insights and Implications," *Healthcare*, vol. 8, no. 2, p. 133, 2020, https://doi.org/10.3390/healthcare8020133.

[10] S. Veena, M. Divyalakshmi, and V. Poornima, "Study of Cybersecurity in Data Breaching," *International Journal of Advance Engineering and Research Development*, vol. 5, no. 3, pp. 1513–1516, 2018, https://www.ijaerd.com/index.php/IJAERD/article/view/4975.

[11] L. Cheng, F. Liu, and D. D. Yao, "Enterprise data breach: causes, challenges, prevention, and future directions," *Wiley Interdiscip Rev Data Min Knowl Discov*, vol. 7, no. 5, p. e1211, 2017, https://doi.org/10.1002/widm.1211.

[12] C. V. Camp and W. Peeters, "A world without satellite data as a result of a global cyber-attack," *Space Policy*, vol. 59, p. 101458, 2022, https://doi.org/10.1016/j.spacepol.2021.101458.

[13] H. Hammouchi, O. Cherqi, G. Mezzour, M. Ghogho, and M. El Koutbi, "Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time," *Procedia Computer Science*, vol. 151, pp. 1004-1009, 2019, https://doi.org/10.1016/j.procs.2019.04.141.

[14] A. G. R. Amalia and A. N. L. I. Fahrudi, "The Relationship Between Perceived Ease of Use, Perceived Usefulness and Perceived Loss of Control with User Satisfaction in Mandatory Setting," In *3rd Annual International Conference on Public and Business Administration (AICoBPA 2020)*, pp. 171-173, 2021, https://doi.org/10.2991/aebmr.k.210928.034.

[15] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, vol. 13, no. 3, p. 319-340, 1989, https://doi.org/10.2307/249008.
[16] V. Venkatesh, "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model," *Information Systems Research*, vol. 11, no. 4, pp. 342–365, 2000, https://doi.org/10.1287/isre.11.4.342.11872.
[17] R. Mekovec and Ž. Hutinski, "The role of perceived privacy and perceived security in online market," *2012 Proceedings of the 35th International Convention MIPRO*, pp. 1549-1554, 2012, https://ieeexplore.ieee.org/abstract/document/6240857.
[18] D. T. Amijaya, S. Sulhaini, and L. E. Herman, "Influence of Trust, Subjective Norm, and Perceived Usefulness on the Intention of Using Contraceptives with Education Level as Moderation Variables," *International Journal of Multicultural and Multireligious Understanding*, vol. 8, no. 8, pp. 125-137, 2021, http://dx.doi.org/10.18415/ijmmu.v8i8.2848.
[19] N. Wilde and A. Hsu, "The influence of general self-efficacy on the interpretation of vicarious experience information within online learning," *International Journal of Educational Technology in Higher Education*, vol. 16, no. 1, p. 26, 2019, https://doi.org/10.1186/s41239-019-0158-x.
[20] A. A. Hayat, K. Shateri, M. Amini, and N. Shokrpour, "Relationships between academic self-efficacy, learning-related emotions, and metacognitive learning strategies with academic performance in medical students: a structural equation model," *BMC Med. Educ.*, vol. 20, no. 1, p. 76, 2020, https://doi.org/10.1186/s12909-020-01995-9.
[21] H. Wu, S. Li, J. Zheng, and J. Guo, "Medical students' motivation and academic performance: the mediating roles of self-efficacy and learning engagement," *Medical education online*, vol. 25, no. 1, p. 1742964, 2020, https://doi.org/10.1080/10872981.2020.1742964.
[22] A. Kanta, I. Coisel, and M. Scanlon, "Smarter Password Guessing Techniques Leveraging Contextual Information and OSINT," *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1-2, 2020, https://doi.org/10.1109/CyberSecurity49315.2020.9138870.
[23] J. Goo, M. -S. Yim, and D. J. Kim, "A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate," in *IEEE Transactions on Professional Communication*, vol. 57, no. 4, pp. 286-308, 2014, https://doi.org/10.1109/TPC.2014.2374011.
[24] W. Li, R. Liu, L. Sun, Z. Guo, and J. Gao, "An Investigation of Employees' Intention to Comply with Information Security System—A Mixed Approach Based on Regression Analysis and fsQCA," *Int. J. Environ. Res. Public Health*, vol. 19, no. 23, p. 16038, 2022, https://doi.org/10.3390/ijerph192316038.
[25] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, vol. 34, no. 3, p. 523, 2010, https://doi.org/10.2307/25750690.
[26] P. Muthuswamy, R. Vanitha, C. Suganthan, and P. S. Ramesh, "A study on attitude towards research among the doctoral Student," *International Journal of Civil Engineering and Technology*, vol. 8, no. 11, pp. 811-823, 2017, https://iaeme.com/Home/article_id/IJCIET_08_11_083.
[27] D. Abun, T. Magallanes, S. L. Foronda, and M. J. Incarnacion, "Investigation of Cognitive and affective Attitude of Teachers toward Research and their behavioral Intention to conduct Research in the Future," *Journal of Humanities and Education Development (JHED)*, vol. 1, no. 5, 2021, https://ssrn.com/abstract=3818096.
[28] J. S. Kesenheimer and T. Greitemeyer, "Going green (and not being just more pro-social): do attitude and personality specifically influence pro-environmental behavior?," *Sustainability*, vol. 13, no. 6, p. 3560, 2021, https://doi.org/10.3390/su13063560.
[29] M. Ham, M. Jeger, and A. F. Ivković, "The role of subjective norms in forming the intention to purchase green food," *Economic Research-Ekonomska Istrazivanja*, vol. 28, no. 1, pp. 738–748, 2015, https://doi.org/10.1080/1331677X.2015.1083875.
[30] J. D'Arcy and A. Hovav, "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics*, vol. 89, no. S1, pp. 59–71, 2009, https://doi.org/10.1007/s10551-008-9909-7.
[31] L. Li, L. Xu, and W. He, "The effects of antecedents and mediating factors on cybersecurity protection behavior," *Computers in Human Behavior Reports*, vol. 5, p. 100165, 2022, https://doi.org/10.1016/j.chbr.2021.100165.
[32] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, 1975, https://doi.org/10.1080/00223980.1975.9915803.
[33] F. Mwagwabi, T. McGill, and M. Dixon, "Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines," *2014 47th Hawaii International Conference on System Sciences*, pp. 3188-3197, 2014, https://doi.org/10.1109/HICSS.2014.396.
[34] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Comput. Secur.*, vol. 106, p. 102267, 2021, https://doi.org/10.1016/j.cose.2021.102267.
[35] A.-M. Ghirana and V. P. Bresfelean, "Compliance Requirements for Dealing with Risks and Governance," *Procedia Economics and Finance*, vol. 3, pp. 752–756, 2012, https://doi.org/10.1016/S2212-5671(12)00225-0.
[36] T. Dinev and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *J. Assoc. Inf. Syst.*, vol. 8, no. 7, pp. 386–408, 2007, https://doi.org/10.17705/1jais.00133.

[37] M. Hendawi, "Students' technological awareness at the College of Education," *Cypriot Journal of Educational Sciences*, vol. 15, no. 4, pp. 749–765, 2020, https://doi.org/10.18844/cjes.v15i4.5057.
[38] S. Ammad, W. S. Alaloul, S. Saad, and A. H. Qureshi, "Personal protective equipment (PPE) usage in construction projects: A systematic review and smart PLS approach," *Ain Shams Engineering Journal*, vol. 12, no. 4, pp. 3495-3507, 2021, https://doi.org/10.1016/j.asej.2021.04.001.
[39] P. M. dos Santos and M. Â. Cirillo, "Construction of the average variance extracted index for construct validation in structural equation models with adaptive regressions," *Communications in Statistics-Simulation and Computation*, vol. 52, no. 4, pp. 1639-1650, 2023, https://doi.org/10.1080/03610918.2021.1888122.
[40] A. F. Hayes and J. J. Coutts, "Use omega rather than Cronbach's alpha for estimating reliability. But…," *Communication Methods and Measures*, vol. 14, no. 1, pp. 1-24, 2020, https://doi.org/10.1080/19312458.2020.1718629.
[41] A. P. S. Shofi and W. Widyastuti, "Ad Hominem Fallacy in the Second US Presidential Debate 2020: Donald Trump, the King of Ad Hominem," *Edulitics (Education, Literature, and Linguistics) Journal*, vol. 7, no. 2, pp. 76-80, 2022, http://www.e-jurnal.unisda.ac.id/index.php/edulitic/article/view/3525.

BIOGRAPHY OF AUTHORS

Erwin Halim, Dr. Erwin Halim is a Lecturer at Bina Nusantara University in the Information Systems department. He also serves as Executive Director of the Indonesian Information Systems Association (ASII). Graduated with a Master of Management, University of Indonesia and a Master of Administration from Pierre Mendes France University, also from Bina Nusantara University in Business Information Systems. In between his busy schedule, he writes and has been a consultant for the Kontan Kompas Gramedia daily since 2007. Email: erwinhalim@binus.ac.id.

Angelia Hartanto Teng, she holds a Bachelor's degree in Business Analytics from BINUS University, where she gained expertise in various areas such as Java programming, SQL, UI/UX design using Figma, data analysis with Tableau, and project management. Angelia's skills in communication, problem-solving, and leadership contribute to her success in diverse roles. Her dedication to student development and her involvement in various organizations showcase her commitment to personal and professional growth. Email: angelia.teng@binus.ac.id.

Marylise Hebrard, Marylise Hebrard is Professor in Business Law. She an experienced professional with an impressive career in various roles. Previously served as the Director of France at the Sino-French Center, she has been responsible for organizing training sessions, conferences, and research seminars while leading the bilingual journal of the center. Her role also involves developing relationships with Chinese institutions and administrations and promoting their activities in other Asian countries. Marylise holds a Doctorate in Public Law from the University of Montpellier, where her research focused on the training and function of lawyers in China. She also has a DEA in Chinese Language and Civilization from the National Institute of Oriental Languages and Civilizations (INALCO) and a Bachelor's degree in Philosophy from the University of Montpellier III. Her diverse educational background and extensive experience in various sectors reflect her versatility and ability to navigate complex international environments. Email: marylh9889@outlook.fr.

David Sundaram, Professor in Business School, Information Systems and Operations Management, New Zealand. Professor David Sundaram is a highly accomplished researcher and lecturer at the University of Auckland. He obtained his Ph.D. in Computer Science from the University of California, Los Angeles (UCLA). His research interests lie in the areas of data management, databases, and data mining. He has published extensively in renowned scientific journals and conferences, contributing to the advancement of these fields. Professor Sundaram's expertise encompasses various aspects of data management, including query optimization, indexing techniques, and distributed databases. He has collaborated with industry partners on projects related to big data analytics and database systems. As an educator, Dr. Sundaram is dedicated to fostering the next generation of computer scientists, teaching courses on databases, data science, and information systems. Email: d.sundaram@auckland.ac.nz.

Placide Poba-Nzaou, Full Professor, ESG School of Management, University of Quebec in Montreal. Placide Poba-Nzaou is a professor and researcher at the University of Quebec in Montreal (UQAM), specializing in machine learning, data mining, and artificial intelligence. He holds a Ph.D. in computer science from the University of Montreal and has made significant contributions to these fields. Poba-Nzaou's research focuses on developing innovative algorithms and models to solve complex problems in various domains, such as bioinformatics, finance, and social networks. He has published extensively in reputable scientific journals and has presented his work at international conferences. Additionally, Poba-Nzaou actively engages in teaching and mentoring students, sharing his expertise in machine learning, data analysis, and algorithm design. Email: poba-nzaou.placide@uqam.ca.