Asia Pacific Journal of Information Systems
Vol. 33 No. 3 (September 2023), 603-623

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2023.33.3.603

Affective Response to Feelings of Password Fatigue by Password Change Requirements

Sang Cheol Park*

Associate Professor, College of Business, Daegu University, Korea

ABSTRACT

While prior work has conducted individuals' password security behavior, there is a relatively neglect to examine individuals' affect and feelings of password fatigue in password change context. Therefore, this study explicated individuals' affective response to the feelings of password fatigue by drawing on several theoretical lens. Survey data collected from 267 users were used to test the model using partial least square analysis. This study found that feelings of password fatigue positively affected the negative password fatigue-induced affect, and also both the feelings of password fatigue and the negative password fatigue-induced affect were negatively related to attitude toward changing passwords, which in turn, leads to the intention to change passwords. Furthermore, this study found that shadow work recognition negatively moderated the relationship between attitude and behavioral intention. This study could offer a new theoretical perspective to understand an individual's security behavior and provide empirical evidences for practitioners in charge of IT security in organizations.

Keywords: Feelings of Password Fatigue, Negative Affect, Shadow Work Recognition

Ⅰ. Introduction

Password changes have been one of the most long-standing of all best practices for securing information systems. Numerous studies have investigated the extent to which an individual creates a strong password by password change requirements (e.g., Kaleta et al., 2019; Khern-am-nuai et al., 2022; Merdenyan and Petrie, 2022; Zviran and Haga, 1999).

While there are doubts on the effectiveness of the password changes, there are still security advantages to requiring users to change their password periodically (e.g., Gulenko, 2014; Hartwig and Reuter, 2022; Merdenyan and Petrie, 2022). However, requiring users to change their password generates individuals' password fatigue which may lead to minimize their level of security effort (Cram et al., 2021). Such password changes could accumulate individuals' password fatigue and exhaustion resulting from new combinations of passwords containing a particular

*Corresponding Author. E-mail: sangch77@gmail.com

set of charaters, numbers, symbols, and uppercase letters.

Meanwhile, individuals' affective feelings play a crucial role in human motivation and influences perception, cognition, social judgments, and behaviors (e.g., Forgas, 1995; Forgas and George, 2001). Even though there are previous studies on the affective concept in psychology and organizational behavior (e.g., Brockner and Higgins, 2001; Forgas and George, 2001; Martin et al., 1998; Schaubroeck and Jones, 2000), there is a lack of systematic examinations on the affective response that involves human behavior in password changes context (e.g., Renaud et al., 2021).

Hence, this study examines the relationship between the feelings of password fatigue and the affective response, which influences individuals' attitudes and behavior for password changes. This study also considers shadow work as a silent moderator in the relationship between attitude and behavioral change. According to Illich (1981), shadow work was initially defined as "entirely different form of unpaid work which an industrial society demands as a necessary complement to the production of goods and services." Lambert (2015) also argues that consumers in digital era may feel fatigued when they feel enforced to perform shadow work, such as managing their passwords. It also refers to all unpaid tasks people do on behalf of businesses and organizations (Lambert, 2015).

Password changes are close to shadow work because organizations and IT departments pass their work on to end-users. For instance, the password change requests by orgnizations push end-users through the cycle of inventing a new paswords, remembering them for a certain period of time, then forgetting them while devising and memorizing new ones. Such cycle open a factory of shadow work (Lambert, 2015). Thus, this study examines how shadow work can affect the relationship between attitudes toward password changes and the intention to change it. In light of the above, this study addresses the following research questions:

How do users' feelings of password fatigue influence their affective response when they are forced to change their passwords by organizations and how does the shadow work play in their security behavior?

To address the above questions, this study draws upon theories, such as fatigue (e.g., Cameron, 1973; Cram et al., 2021), affective event theory (e.g., Weiss and Cropanzano, 1996), theory of planned behavior (e.g., Ajzen and Fishbein, 2000), and shadow work recognition (Lambert, 2015). In addition, this study tests a theory-based model of how both feelings of password fatigue and affective response affect individuals' attitude, and how it influences their password change behavior.

Ⅱ. Literature Review

2.1. Password Security

To date, password security research has employed a variety of theoretical perspectives, yet there are commonalites in how people feel and behave when they are forced to change their password periodically. For example, Kaleta et al. (2019) dealt with individuals' use of online passwords by using construal level theory to understand how people create and use strong passwords. Mainly, research streams on IT/password security are divided into two aspects: cognitive/affective perspective (e.g., D'Arcy and Teh, 2019) and security/usability trade-off (e.g., Kaleta et al., 2019; Kim and Kang, 2008; Park and Oh, 2016). <Table 1> lists the studies that have conducted in

either cognitive or affective aspects and summarized their findings.

As indicated in <Table 1>, much of work has neglected to explore the affective aspects as well as security-focus. Building on this stream of literature, this study attempts to further explicate individuals' affective response to the feelings of password fatigue in password change settings by drawing on several theoretical lens such as fatigue, affective event theory, theory of reasoned action, and shadow work recognition.

2.2. Fatigue and Password Fatigue

While numersous definitions on the fatigue have been existed in literature, there are no consensus definitions (e.g, Shen et al., 2006). However, the fatigue has been often refered to a subjective lack of physical and/or mental energy which is perceived by the individuals to interfere with usual and desired activites (Béthoux, 2006; Cameron, 1973). Fatigue is a phenomenon studied in various research fields including cognitive neuroscience, exercise physiology, psychology, and the medical sciences. For example, different studies have shown the phenomenon of decreased cognitive performance after a period of activity as; central fatigue (e.g., Kluger et al., 2013), cognitive fatigue (Ackerman and Kanfer, 2009), and mental fatigue (Inzlicht et al., 2014). Such research on fatigue dealt with almost with variation in productive output which resulted from prolonged work. As a type of security fatigue, password fatigue can be mental fatigue that pertains to the individual's unwillingness to adhere to password-based security

<Table 1> Summary of Research on Password Security (a chronological order)

Authors	Research Focus	Major Findings	Perspective	Trade-off Focus
Keith et al. (2009)	Improving password strength	Demonstrating that well-designed passphrases do not increase login failures and generate positive user perceptions.	Cognitive-oriented	Usability Focus
Gulenko (2014)	Examining the influence of emotions on security behavior	Finding that there is a significant effect of positive emotions on security behavior.	Affective-oriented	Usablility Focus
Stobert and Biddle (2014)	Suggesting the password life cycle for users to keep track of many accounts and passwords.	Identifying a password life cycle that follows users' password behavior.	Cognitive-oriented	Usability Focus
Greene and Choong (2017)	Investigating ambiguous terminology in password rules.	Finding that users are confused by the terms "non-alphanumeric", "symbols", "special characters", and punctuation marks" in password rules.	Cognitive-oriented	Usabliilty Focus
Furnell et al. (2018)	Addressing problems that users tend to ignore security guidelines.	Suggesting that users actually respond to the "nudges" (i.e., indirect advice) as their behavior is significantly improved.	Cognitive-oritented	Security Focus
Wei et al. (2018)	Observing how often passwords are specific to the services for which they were created.	Finding service-specific passwords can reveal other shared interests or demographics of that service's user-base.	Cognitive-oritented	Usability focus

<Table 1> Summary of Research on Password Security (a chronological order)(Cont.)

Authors	Research Focus	Major Findings	Perspective	Trade-off Focus
D'Arcy and Lowry (2019)	Identifying the role of affect in judgment and decision for IS security.	Developing employee compliance model that explains cognitive beliefs on the consequences of compliance and noncompliance as well as state-based affective constructs.	Affective-oriented	Secuirty Focus
Kaleta et al. (2019)	Examining choice of online passwords.	Finding people with a high construal level created or showed intention to choose stronger passwords.	Cognitive-oriented	Usabliilty Focus
Yıldırım and Mackie (2019)	Introducing a new user-friendly guideline approach to password creation	Offering a reliable solution by encouraging users to create their own formula to compose passwords.	Cognitive-oritented	Security Focus
Woods and Siponen (2019)	Improving password memorability.	Finding small changes to the password verification stage can affect password memorability.	Cognitive-oritented	Security Focus
Zimmermann and Gerber (2020)	Suggesting password authentication schemes.	Finding that the password followed by fingerprint authentication scored highest in terms of preference, usability, and intention to use.	Cognitive-oritented	Usability focus
Cram et al. (2021)	Investigating how security fatigue affects employee security policy compliance and non-compliance.	Developing security fatigue concept and finding its antecedents and consequences.	Affective-oriented	Security Focus

behavior.

Despite some studies on security fatigue in IS areas (e.g., Cram et al., 2021; Furnell and Thomson, 2009; Stanton et al., 2016), there has been no attempt to examine the relationship between password fatigue and password security behavior. In the absence of academic research on password fatigue, previous research suggested that users often perceived security as an obstacle that hindered their productivity (e.g., Cram et al., 2021; Stanton et al., 2016). Subsequently, this fatigue was coined to describe the threshold of acceptance beyond which it becomes too burdensome for users to maintain IT security (Furnell and Thomson, 2009). Security fatigue can be referred to "*users' weariness or reluctance to experience more of something* (Stanton et al., 2016, p. 26)." Cram et al. (2021) focused on security fatigue as a socio-emotional state experienced by a user disillusioned with security guidelines and procedures. Therefore, in this study, password fatigue is defined as an individual's feelings of weariness or reluctance to deal with changing passwords.

2.3. Affective Events Theory and Affective Response

Affective events theory (hereafter, AET) is a theory that demonstrates how various moods and emotions affect job performance in the workplace (Weiss and Cropanzano, 1996). According to the AET, perception and the experience of salient and relevant work events cause reactions in employees that can shape their momentary actions and create an ongoing emotional tone in the workplace (Weiss et al., 1993). The AET is compatible with this research context because the individuals' affective response is influ-

enced by the feature of a specific event (e.g., forcing users to change their existing passwords). Furthermore, many disciplines, such as organizational behavior, marketing, social psychology, and information systems, provided strong evidences that affect was a critical factor in job satisfaction (Forgas, 2008; Weiss et al., 1999), decision-making (Mittal and Ross, 1998; Slovic et al., 2004), work motivation (Seo et al., 2004), and employees' IS compliance (D'Arcy and Lowry, 2019).

While there are several studies on password security policy (e.g., Hartwig and Reuter, 2022; Li et al., 2019; Merdenyan and Petrie, 2022; Tam et al., 2010), they still neglect 'affect' in existing IS security that provides detailed explanations about why and how individuals behave in a particular way. Thus, based on previous work employing 'affect' in IS security, this study has regarded the affect response as a consequence of the feelings of password fatigue because it can fluctuate individuals' attitudes, beliefs, and behaviors (D'Arcy and Lowry, 2019; Judge et al., 2006). Based on the above findings, this study predicts that affective response, which is tapped into AET, could result from the feelings of password fatigue and the antecedent of individuals' attitudes and behavioral intentions.

2.4. Theory of Planned Behavior and Shadow Work

The theory of planned behavior (hereafter, TPB) postulates that an individual's behavior is influenced by attitude, subjective norms, and perceived behavioral control (Ajzen, 1991). The TPB is intuitive, parsimonious, and insightful to explain behavior (Bagozzi, 1982). Previous studies have confirmed that the intention to comply with IS compliance is strongly influenced by the attitude, and perceived behavioral control (Bulgurcu et al., 2010; D'Arcy and Lowry, 2019; Venkatesh et al., 2003). Most of IS literature verified the relationship between attitude and behavioral intention as well as provided a consistent pattern of emprical evidences (Venkatesh et al., 2003). Namely, positve attitude toward IS security polices increases behavioral intention to comply with IS security rules. Conversely, negative attitude will decrease an individual's compliance behavioral intention. In summary, the TPB has been widely used in explaining individuals' decision to adopt acceptable computer security (e.g., Lee and Kozar, 2005) or comply with IS security policies (D'Arcy and Lowry, 2019; D'Arcy and Teh, 2019).

Additionally, this study regards that shadow work recognition plays a moderating role in the relationship between attitude and behavioral intention. Shadow work has been referred to all the unpaid tasks people do for businesses and organizations (Lambert, 2015). The term shadow work was presented by Illich (1981), an Austrian philosopher and social critic. He mentioned that shadow work was all the unpaid labor done in a wage-based economy. Later then, Lambert (2015) presented a new perspective on shadow work in the service economy. He highlighted that the 'service' of many service sectors disappeared. For example, most people pump their gas and fill the tank by themselves, and pay their bills by swiping a credit card. In addition, airport travelers should issue their tickets using self-service check-in kiosks. Shadow-working travelers do all of this themselves on their computer/smartphone screens. It represents replacing the past paid work of travel agents with the unpaid work of customers.

In this study, a typical example of shadow work is shown in the password change context. In general, individuals have long lists of digital keys such as username and passwords among their favorite web

sites/applications. They must update and protect their lists at all times. Most applications force users to create or recall usernames and passwords for even the most unimportant tasks. Another problem is when every new password stupulates specific requirements (e.g., numbers of characters, capitalizatios, punctuation marks). Such requirements could accelerate the shadow work. Password expiration can also cause shadow work. This pushes individuals through the cyle of inventing a password, remembering it for three months, then forgetting it while devising and memorizing a new one. Based upon the above example, the concept of shadow work could be applied to this study. Therefore, this study has considered shadow work a psychological trigger in the current manner of doing or thinking about changing passwords.

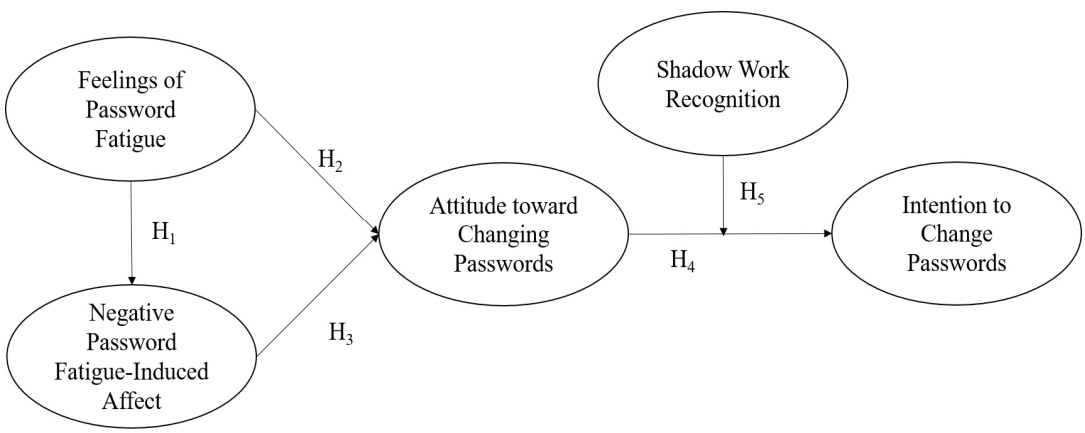
Ⅲ. Research Model and Hypotheses

3.1. Research Model

As shown in <Figure 1>, when individuals are forced to change their existing passwords, their affective response will become negative because they suffered from password fatigue. Feelings of password fatigue and affective response will also negatively affect the individuals' attitudes toward changing passwords. Furthermore, the effect of attitude on behavioral intention might be weakened if individuals recognize password change as shadow work, even though they have positive attitudes. Based on above assessment, this study has proposed the research model in <Figure 1>.

3.2. Research Hypotheses

The feelings of password fatigue are defined as the feeling of exhaustion resulting from the request for password change. Cram et al. (2021) have identified antecedents and consequences of security fatigue. They reported that the security fatigue was related to feelings of frustration, tiredness, and hopelessness, which were a kind of 'affect'. The affect plays a crucial role in organizational behavior, and it helps shape an individual's overall experience and behavior (Oreg et al., 2011; Seo et al., 2004). Even though there is no research which directly elucidated the relation-



<Figure 1> Research Model

ship between feelings of password fatigue and affective response, previous work indicated that password management might cause an affective or emotional response (e.g., Cram et al., 2021; D'Arcy and Lowry, 2019; Gulenko, 2014). Since it is reasonable to assume that the feelings of password fatigue could affect negative password fatigue-induced affect. Thus, this study states the following hypothesis:

H1: Feelings of password fatigue are positively related to the negative password fatigue-induced affect.

In security-usability trade-off, changing the password composition (i.e., increasing the length of password characters or removing the need for special characters) could make it more complicated for individuals (e.g., Greene and Choong, 2017; Kaleta et al., 2019; Zviran and Haga, 1999). For example, common password requirements enforce that a password cannot match the username, must be of a certain length, and contain various characters, including upper/lowercase letters, numbers, and special characters (Zviran and Haga, 1999). Such a password requirement with mandatory changes has led to considerable confusion and stress for those trying to keep track of passwords in both work and personal settings. Therefore, password fatigue can negatively influence attitude toward changing passwords. Based on the logic, this study could present the following hypothesis:

H2: Feelings of password fatigue are negatively related to attitude toward changing passwords.

Previous studies reported that the affective response influenced attitudes (D'Arcy and Lowry, 2019; Derbaix, 1995). For example, D'Arcy and Lowry (2019) conceptualized positive and negative mood in terms of both positive and negative affectivity. They reported that both positive and negative affectivity leads to compliance attitudes. Prior work also explained that 'affect' encompassed moods and emotions regarding feeling states (Lowry et al., 2014; Zhang, 2013). Thus, if individuals are in a positive mood, they are more likely to have a positive attitude toward changing passwords, whereas the attitude could become more negative as people are in a negative mood. Based on previous work, this study assumes that a higher negative password fatigue-induced affect is associated with a more negative attitude toward changing passwords.

H3: Negative password fatigue-induced affect is negatively related to attitude toward changing passwords.

An attitude is a strong predictor of an individual's intention to engage in that behavior, whereby intention is a behavioral action tendency (Ajzen, 1991; Ajzen and Fishbein, 2000). The attitude results from one's cognitive values, expressing whether a person feels positively or negatively about performing a specific behavior (Ajzen and Fishbein, 2000). Prior studies showed consistent patterns of results which found the significant relationship between the attitude and intention to use in a variety of research contexts (e.g., D'Arcy and Lowry, 2019; Ilies et al., 2006; Judge et al., 2006). Thus, this study posits the following hypothesis:

H4: Attitude toward changing passwords is positively related to the intention to change passwords.

While there is a positive relationship between the attitudes toward changing passwords and intention

to change passwords, the direction of the relationship might be changed because of the effect of shadow work. Specifically, in password change context, individuals must put their time and effort into typing the password to execute the action. It becomes troublesome and time-consuming when individuals make optimal combinations to meet the criteria by password policies (e.g., Keith et al., 2009). In this case, it leads to a negative impact on usability (e.g., Kaleta et al., 2019). Hence, this study posits the following hypothesis:

H5: Shadow work recognition will moderate the relationship between attitude and intention to change passwords such that the strength of the relationship will be weaker when the shadow work recognition is higher.

3.3. Construct Operationalization

This section describes how it operationalized each of the constructs. The feelings of password fatigue were operationalized by capturing the extent to which the individuals feel fatigued, bored, and exhausted under the situation that forces the end-users to create passwords (Cram et al., 2021). These ones form the basis for three of the measurement items (PF1 – PF3). The negative password fatigue-induced affect was operationalized by creating seven measures from affective response construct (AR1 – AR7) (Feldman and Russell, 1998; Seo et al., 2004; Zhang 2013). According to D'Arcy and Lowry (2019), the attitude toward changing passwords was operationalized using three scales. Intention to change passwords was operationalized using a four-item scale to determine if the end-users intend to make new passwords in the near future (Ajzen and Fishbein, 2000). Lastly, for the shadow work recognition, this study developed a simple yes/no-based question because there is no theoretical background in academic area so far. To avoid agreement bias from a nature of a simple yes/no-based question, this study rephrased to remove the positive and negative sentiments, thus answer options are neutral (Callegaro et al., 2015). In this study, the final answer options on asking shadow work are the follows: 'Yes, it is a shadow work', 'No, it is not a shadow work', and 'I have no idea'. <Table 2> shows the actual measurement items in this study.

3.4. Research Approach and Data Collection

Given that this study evaluates how password fatigue engages in intention to change passwords via affective response, this study adopted a survey approach to test the proposed research model. The survey was developed and refined as follows. First, this study developed an initial questionnaire in which each subject was asked to respond based on their most recent experience on changing passwords. The survey was developed in English and two experts who were fluent in both English and Korean translated it into Korean. After that, they performed a backward translation to ensure consistency between Korean version of the measurement items and the original English version. Then, forty-nine undergraduate students in one of universities in South Korea completed the hard-copy-based survey. This served as a pilot test of the modified version of the questionnaire. After the pilot test, this study conducted a web-based survey in July 2022 that targeted employed professionals in organizations with having recent experience on changing passwords. This study instructed a research firm to collect responses and it paid participants a small amount for respondents' participation. Since the research involves human research participants, this study obtained the formal ap-

<Table 2> Measurement Items for Key Constructs

Construct	Items	Sources
Feelings of Password Fatigue	1. I feel fatigued due to changing passwords.	Cram et al. (2021)
	2. I feel bored due to changing passwords	
	3. I feel rather exhausted due to changing passwords.	
Negative Password Fatigue-induced Affect	Changing passwords is…	Seo et al. (2004); Zhang (2013)
	1. impassive – irritated	
	2. desirable – annoying	
	3. comfortable – fed up with	
	4. delightful – embarrassed	
	5. relaxed – nervous	
	6. satisfied – unsatisfied	
	7. pleasant – unpleasant	
Attitude toward Password Change	Changing passwords is…	Ajzen and Fishbein (2000)
	1. bad-good	
	2. unfavorable-favorable	
	3. negative- positive	
Intention to Change Passwords	1. I intend to change passwords from now on.	Ajzen and Fishbein (2000)
	2. I plan to change passwords in the future.	
	3. I prefer to change passwords.	
	4. My willingness to change passwords is quite high.	
Shadow Work	Do you think that your password change is considered as shadow work?	Developed

proval from DU-IRB committee of Daegu University in South Korea, before collecting data from respondents (approval number: 1040621-202205-HR-035).

For the sampling frame, this study adopted simple a random sampling method that allows the sampling error to be calculated and reduced selection bias. The random sampling method is the most straightforward method of probability sampling (Bryman, 2016). Based on this frame, this study collected two hundred and eighty survey respondents and finally two hundred and sixty-seven survey respondents were retained for the analysis due to screening out one of answering options of questioning the shadow work.[1)]

For the research method approach, the partial least square (PLS) technique is adopted to test the measurement and structural models. One advantage of PLS is that it can examine all of the paths in the proposed model including both measurement model and structural model simultaneously. Furthermore, the PLS parameter estimates reveal the strength and direction (i.e., positive or negative) of the relationships among variables compared to correlation coefficients. It also avoids parameters estimation biases common in regression analysis (Henseler et al., 2015). Hence, it is well suited for the predictive nature of this study. In this study, using Smart PLS 3.0, a bootstrap analysis

1) Frequency/ratio of responding the shadow work are follows: '1 = yes, it is a shadow (n = 131, 46.78%)', '2 = No, it is not a shadow work (n = 136, 48.57%)', and '3 = I have no idea (n = 12, 4.28%)'.

was performed with 300 subsamples, with a sample size set equal to the number of respondents in the sample (n = 267).

Ⅳ. Data Analysis and Results

4.1. Descriptive Analysis

<Table 3> lists the demographics for the sample. In the sample, 68.54% of respondents were female, and approximately 88.9% were in the 21 – 50 age group. The highest experience on recent password change was observed for less than three months (n = 156, 58.43%), followed in decreasing order by three – six months (n = 65, 23.21%), six-12 months (n = 24, 8.57%), one-two years (n = 15, 5.36%), and more than two years (n = 7, 2.62%).

4.2. Measurement Model

The measurement model was tested by examining the convergent and discriminant validity (Hair et al., 1998; Hair et al., 2012; Hair et al., 2017). Generally, two different assessments were made for convergent validity: (1) individual item reliability and (2) construct reliability. Individual item reliability was assessed by examining the item-to-construct loadings for each construct measured with multiple indicators. For the shared variance between each item and its associated construct to exceed the error variance, the standardized loadings should be greater than 0.80. As shown in <Table 4>, all the item-to-construct loadings exceeded the desired threshold.

The next step involved examining the composite reliability, Cronbach's alpha, the average variance extracted (AVE), and Rho_A for each block of measures. As shown in <Table 5>, each measure appears to be more than acceptable by established criteria.

As shown in <Table 5>, all the constructs exceeded the established criteria for AVE. Thus, all the constructs exceeded the threshold judged acceptable for construct reliability. Having established convergent validity, this study then turned to discriminant validity. This study conducted three tests for discriminant validity. First, this research calculated each indicator's loading on its construct and its cross-loading on all other constructs (see <Table 3>). In the columns of the <Table 4>, the loadings for the indicators for each construct were higher than the cross-loadings for other construct indicators. In addition, across the rows, each indicator has a higher loading with its construct than cross-loading with any other construct. This provides evidence of discriminant validity (Fornell and Larcker, 1981). As a second test of discriminant validity, this study also considered whether the AVEs of the latent constructs were greater than the square of the correlations among the latent constructs (see <Table 6>). When true, more variance is shared between the latent construct and

<Table 3> Sample Demographics

Items	Category	Frequency	Ratio (%)
Gender	Male	84	31.46%
	Female	183	68.54%
Age	21 – 30	67	23.92%
	31 – 40	99	37.07%
	41 – 50	78	27.86%
	Over 50	23	8.21%
Recent Experience on Password Change by Organizations	Less than 3 months	156	58.43%
	3 – 6 months	65	23.21%
	6 – 12 months	24	8.57%
	1 – 2 years	15	5.36%
	More than 2 years	7	2.62%

<Table 4> Item-Factor Loadings and Cross-Loadings

Construct	Items	AR	FP	AC	IT	SW
Negative Password Fatigue-Induced Affect	AR1	**0.860**	0.482	-0.344	-0.323	0.299
	AR2	**0.832**	0.434	-0.290	-0.267	0.317
	AR3	**0.853**	0.465	-0.379	-0.286	0.339
	AR4	**0.816**	0.379	-0.256	-0.234	0.345
	AR5	**0.860**	0.433	-0.346	-0.219	0.351
	AR6	**0.831**	0.416	-0.275	-0.202	0.258
	AR7	**0.847**	0.411	-0.252	-0.189	0.303
Feelings of Password Fatigue	FP1	0.357	**0.827**	-0.268	-0.341	0.214
	FP2	0.472	**0.917**	-0.302	-0.307	0.315
	FP3	0.501	**0.866**	-0.216	-0.196	0.242
Attitude toward Changing Passwords	AC1	-0.361	-0.285	**0.933**	0.666	-0.212
	AC2	-0.357	-0.296	**0.939**	0.579	-0.198
	AC3	-0.303	-0.254	**0.919**	0.561	-0.151
Intention to CHANGE PASSWORDS	IP1	-0.253	-0.233	0.518	**0.881**	-0.204
	IP2	-0.209	-0.249	0.500	**0.885**	-0.167
	IP3	-0.254	-0.284	0.604	**0.925**	-0.284
	IP4	-0.324	-0.356	0.676	**0.892**	-0.259
Shadow Work		0.375	0.298	-0.202	-0.260	**1.000**

<Table 5> Reliability of Each Construct

Construct	Mean	Std	Cronbach's Alpha	Composite Reliability	AVE	Rho_A
Negative Password Fatigue-Induced Affect	4.473	1.107	0.932	0.945	0.711	0.936
Attitude toward Changing Passwords	4.436	1.525	0.923	0.951	0.866	0.928
Feelings of Password Fatigue	4.896	1.417	0.840	0.904	0.758	0.853
Intention to Change Passwords	4.494	1.657	0.919	0.942	0.803	0.930
Shadow Work	N/A	N/A	1	1	1	1

its block of indicators than with another construct. As seen by reading across the rows of the <Tables 6>, the measures passed this test, providing additional evidence of discriminant validity.

Lastly, this study calculated the Heterotrait-Monotrait Ratio of correlation (HTMT) to assess the discriminant validity. The HTMT criterion measures the average correlations of the indicators across constructs. Henseler et al. (2015) suggested an acceptable level of discriminant validity (< 0.90). In this study, it provided good evidence of discriminant validity.

4.3. PLS analysis

Given the sample used in this study, statistical tests can be very sensitive and may detect spurious effects (Hair et al., 1998). Therefore, a strict significance level of 0.001 was used for all statistical

<Table 6> Squared Pairwise Correlations and Assessment of the Discriminant Validity

Construct	AR	FP	AC	IT	SW
Negative Password Fatigue-Induced Affect	**0.843**				
Feelings of Password Fatigue	-0.368	**0.930**			
Attitude toward Changing Passwords	0.514	-0.300	**0.871**		
Intention to Change Passwords	-0.295	0.650	-0.319	**0.896**	
Shadow Work	0.375	-0.202	0.298	-0.260	**1**

tests. The explanatory power of a structural model can be evaluated by looking at the R^2 value (variance accounted for) of the final dependent construct.

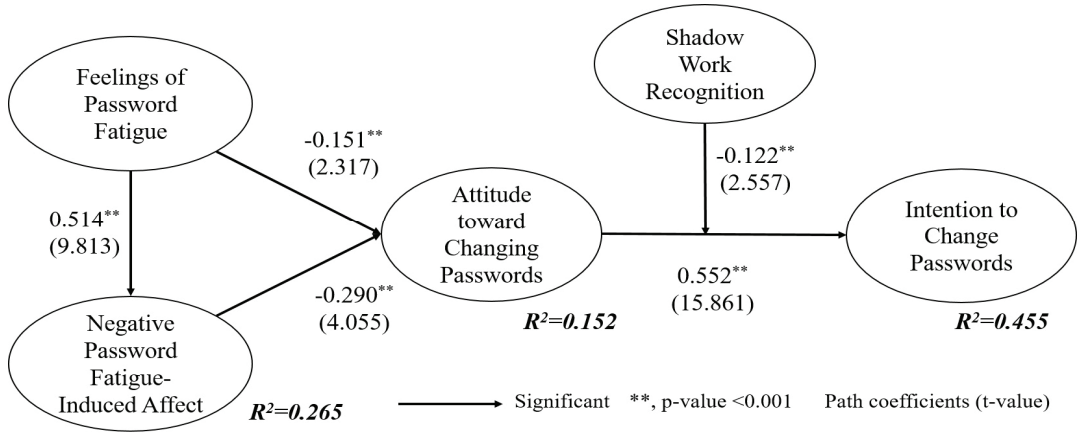
The final dependent construct in this study (IP) had an R^2 value of 0.455, indicating that the model accounts for 45.5% of the variance in the dependent variable. The R^2 values for attitude toward changing passwords and affective response were 0.152 and 0.265, respectively. These R^2 of 0.455, 0.151, and 0.265 values can be as a rule of thumb in empirical studies related to IS research in general, interpreted as substantial, weak and moderate respectively based on guidelines of coefficient of determination (Chin, 1998). Thus, R^2 values in this study are sufficient to interpret the path coefficients as meaningful.

The structural model was tested by examining the path coefficient's statistical significance and magnitudes (Chin, 1998). The magnitude of a path coefficient represents the strength of the direct effect and it carries meaning only if the path coefficient is statistically significant. According to prior work (e.g., Chin, 1998; Huber et al., 2008; Urbach and Ahlemann, 2010), path coefficient values close to 0.5 or greater were interpreted as corresponding to large effect sizes, value around 0.3 were interpreted as corresponding to medium effect sizes, and values near 0.1 as corresponding to small effect size. Huber et al. (2008) also suggested that path coefficient must be at least 0.100 and at a significance level of at least 0.05. As this study used bootstrapping technique to determine the significance level (Efron and Tibshirani, 1993; Wetzels et al., 2009), path coefficient values at the 0.001 level is meaningful.

As shown in <Figure 2>, the path between feelings of password fatigue and negative password fatigue-induced affect (β = 0.514, t = 9.813) was significant at $p < 0.001$. The path between feelings of password fatigue and attitude toward changing passwords (β = -0.151, t = 2.317), the path between negative password fatigue-induced affect and attitude toward changing passwords (β = -0.290, t = 4.055), and the path between attitude toward changing passwords and intention to change passwords (β = 0.552, t = 15.861) were all significant at $p < 0.001$. Lastly, the path between the interaction of shadow work recognition with attitude toward changing passwords and

<Table 7> Heterotrait-Monotrait Ratio of Correlation (HTMT) for Assessing the Discriminant Validity

Construct	AR	FP	AC	IT	SW
Negative Password Fatigue-Induced Affect					
Feelings of Password Fatigue	0.390				
Attitude toward Changing Passwords	0.572	0.341			
Intention to Change Passwords	0.310	0.693			
Shadow Work	0.388	0.209	0.158	0.229	



<Figure 2> Results of Testing the Hypotheses

intention to change passwords (β = -0.122, t = 2.557) was significant at $p < 0.001$. <Table 7> lists the results for all of the hypotheses tested.

As indicated in <Table 8>, all hypotheses were statistically supported. This study examined how individuals' feeling of password fatigue influence their negative password fatigue-induced affect, which might lead to password change when they are forced to change by organizations. This research also examined the moderating effect of shadow work recognition in the relationship between attitude and the intention to change passwords.

By developing and testing a theoretical research model, this study showed that individuals' password changing behavior in organizations could be described by feelings of password fatigue, negative password fatigue-induced affect, and shadow work recognition. Specifically, individuals' affective response could result from feelings of password fatigue and a negative emotional driver of their attitude toward changing passwords. Furthermore, the positive relationship between attitude and intention becomes weakened due to shadow work recognition and somewhat influenced in a negative direction.

Ⅴ. Conclusion

This study examined the effects of individuals' password fatigue and negative password fatigue-in-

<Table 8> Summary of Testing Hypotheses

#	Hypothesis	Results
1	Feelings of password fatigue are positively related to negative password fatigue-induced affect.	Supported
2	Feelings of password fatigue are negatively related to attitude toward changing passwords.	Supported
3	Negative password fatigue-induced affect is negatively related to attitude toward changing passwords.	Supported
4	Attitude toward changing passwords is positively related to the intention to change passwords.	Supported
5	The shadow work recognition will moderate the relationship between the attitude toward changing passwords and the intention to change passwords such that the strength of the relationship will be weaker when the shadow work recognition is higher.	Supported

duced affect on their security behavior related to password change. This study also found that shadow work recognition could play a moderating role in the relationship between their attitude toward changing passwords and intention to change passwords. Based on the findings, this research offers a new theoretical perspective to understand an individual's password change behavior and provides empirical evidence for practitioners who are interested in IT security.

5.1. Implications for Research

This study has several implications for research.

First, this research offers a new theoretical concept to understand an individual's password creation behavior. Specifically, this study introduced the effect of password fatigue as a trigger for describing online security behavior. Prior research recognized the usability and security tradeoff problem and attempted to solve the tradeoff in passwords (e.g., Kaleta et al., 2019; Keith et al., 2009). This study could offer new insights regarding usability by focusing on password fatigue for understanding password creation behavior. Thus, this research contributes to the existing literature on a password management strategy from a psychological perspective.

Second, while password fatigues could be an interesting topic in IS security areas, there is no empirical evidence on the effect of password fatigue to individuals' security behavior. This study examined the effect of password fatigue on IS security behavior for explaining how individuals feel password change requirement. In addition, this study has regarded the negative password fatigue-induced affect as a consequence of password fatigue. Particularly, this research offers empirical evidence that a negative affective response leads to a negative attitude toward password creation.

Lastly, this study introduced the concept of shadow work and identified how this is relevant to security behavior. Specifically, this study tested how shadow work recognition play a moderating role in the relationship between attitude and behavioral intention in password security context. While many studies on password security have been conducted, no attempt has been made to explore individuals' psychological mechanisms on password creation by adopting shadow work recognition. By applying this new concept to the study, this is the first study that provides empirical evidence that shadow work can be a moderator in the relationship between attitude and behavioral intention. By introducing the shadow work concept, this study contributes to provide a unique theoretical ground for relevant researchers in IS security literatures.

5.2. Implications for Practice

This study also has some implications for practitioners. First, this study provided empirical evidences on that the feelings of password fatigue could be a critical factor to generate individuals' negative attitudes. The password fatigue poses a great cyber-security risk, apart from the mental effect and stress that comes with password fatigue. Since individuals get frustrated remembering many complex passwords, they have possibilities to use weak passwords and even repeat them without minor changes. Hackers can take advantage of this fatigue because weak and repeated passwords are vulnerable to cracking and dictionary attacks. Thus, practitioners must find a way to alleviate the password fatigue users experience to decrease organizations' time, money, and mental energy in their organizations. For example, single sign-on could be one of alternative ways

to alleviate the password fatigue.

Second, the results of this study indicated that the negative password fatigue-induced affect, attitude toward changing passwords, and intention to change passwords are influential in this regard. Thus, organizations are well advised to focus on managing employees' emotions induced by the interaction between employees and IT security polices in organizations. For instances, organizations could tailor password security policies to a contextual aspect of the job position and organizations. In addition, organizations should make an effort to stop forcing frequent password changes to prevent generating negative affective responses and attitudes.

Lastly, this study has provided an empirical evidence that shadow work recognition plays a moderating role in the relationship between attitude and behavioral intention. In this study, as the extent of shadow work is greater, the direction of the relationship between attitude and behavioral intention is changed from positive to negative. This finding suggest that individuals' perception shift could be a useful strategy to improve their password management. For IT security managers, it is necessary to create a work atmosphere that evokes the idea that changing or updating passwords is entirely the users' job they are willing to do so that they do not feel like they are performing shadow work.

5.3. Limitations and Suggestions for Future Research

This study is subject to limitations and it is important to point these out. This study asked respondents to recall their most recent experience. Recall bias can be a threat in these circumstances because respondents may not have an accurate recall of their experience. Common method bias (hereafter, CMB) can also be another limitation, given the design of this study. Hence, this study conducted a CMB test to guard against any error that could have arisen due to the self-report survey methodology. According to Kock (2015), the occurrence of a VIF greater than 3.3 indicates pathological collinearity and that a model may be contaminated by CMB. If all VIFs in the inner model resulting from a full collinearity test is equal to or lower than 3.3, the model can be considered free of common method bias. In this study, all the VIFs in the inner model were lower than 1.4 (see <Appendix A>). Hence, CMB was not a significant limitation in this study. Another limitation of this study is that this study did not explore additional variables because it focused on the parsimonious model. Thus, future research may explore additional predictors to expand the scope and explanatory power of the research model. Lastly, this study has employed TPB as one of several theoretical lens to explain an individual's behavior. Although the TPB had been a well-known theory to predict individuals' behavior, this study admitted that it was one of the old-fashioned theories. Therefore, future research needs to consider a different relevant theory to predict users' behavior in this study context.

Acknowledgments

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2021S1A3A2A02089809).

<References>

[1] Ackerman, P. L, and Kanfer, R. (2009). Test length and cognitive fatigue: An empirical examination of effects on performance and test-taker reactions. *Journal of Experimental Psychology: Applied*, *15*(2), 163-181. https://doi.org/10.1037/a0015719

[2] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

[3] Ajzen, I., and Fishbein, M. (2000). Attitudes and the attitude-behavior relation: Reasoned and automatic processes. *European Review of Social Psychology, 11*(1), 1-33. https://doi.org/10.1080/14792779943000116

[4] Bagozzi, R. P. (1982). A field investigation of causal relations among cognitions, affect, intentions, and behavior. *Journal of Marketing Research*, *19*(4), 562-584. https://doi.org/10.1177/002224378201900415

[5] Béthoux, F. (2006). Fatigue and multiple sclerosis. *Annales de Réadaptation et de Médecine Physique*, *49*(6), 355-360.

[6] Brockner, J., and Higgins, E. T. (2001). Regulatory focus theory: Implications for the study of emotions at work. *Organizational Behavior and Human Decision Processes, 86*(1), 35-66. https://doi.org/10.1006/obhd.2001.2972

[7] Bryman, A. (2016). *Social Research Methods.* Oxford University Press.

[8] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

[9] Callegaro, M., Murakami, M. H., Tepman, Z., and Henderson, V. (2015). Yes‐no answers versus check-all in sself-administered modes: A systematic review and analyses. *International Journal of Market Research, 57*(2), 203-224. https://doi.org/10.2501/IJMR-2015-014a

[10] Cameron, C. (1973). A theory of fatigue. *Ergonomics, 16*(5), 633-648.

[11] Chin, W. W. (1998). *The Partial Least Squares Approach to Structural Equation Modeling.* Mahwah, NJ:Lawrence Erlbaum.

[12] Cram, W. A., Proudfoot, J. G., and D'Arcy, J. (2021). When enough is enough: investigating the antecedents and consequences of information security fatigue. *Information Systems Journal, 31*(4), 521-549. https://doi.org/10.1111/isj.12319

[13] D'Arcy, J., and Lowry, P. B. (2019). Cognitive affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43-69. https://doi.org/10.1111/isj.12173

[14] D'Arcy, J., and The, P. L. (2019). Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization. *Information & Management, 56*(7), 103-151. https://doi.org/10.1016/j.im.2019.02.006

[15] Derbaix, C. M. (1995). The impact of affective reactions on attitudes toward the advertisement and the brand: A step toward ecological validity. *Journal of Marketing Research, 32*(4), 470-479. https://doi.org/10. 1177/002224379503200409

[16] Efron, B., and Tibshirani, R. (1993). *An Introduction to The Bootstrap*. New York: Chapman Hall.

[17] Feldman, B. L., and Russel, J. A. (1998). Independence and bipolarity in the structure of current affect. *Journal of Personality and Social Psychology*, *74*(4), 967-984. https://doi.org/10.1037/0022-3514.74.4.967

[18] Forgas, J. P. (2008). Affect and cognition. *Perspectives on Psychological Science, 3*(2), 94-101. https://doi.org/10.1080/026999307 01437931

[19] Forgas, J. P. (1995). Mood and judgment: The affect infusion model (AIM). *Psychological Bulletin, 117*(1), 39-66. https://doi.org/10.1037/0033-2909.117.1.39

[20] Forgas, J. P., and George, J. M. (2001). Affective influences on judgments and behavior in organizations: An information processing perspective. *Organizational Behavior and Human Decision Processes, 86*(1), 3-34. https://doi.org/10.

1006/obhd.2001.2971

[21] Fornell, C., and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. https://doi.org/10.1177/002224378101800104

[22] Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., and Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security*, *75*(June), 1-9. https://doi.org/10.1016/j.cose.2018.01.016

[23] Furnell, S., and Thomson, K. L. (2009). Recognising and addressing 'security fatigue'. *Computer Fraud & Security*, *11*(Novermber), 7-11. https://doi.org/10.1016/S1361-3723 (09)70139-3

[24] Greene, K. K, and Choong, Y. Y. (2017). Must I, can I? I don't understand your ambiguous password rules. *Information & Computer Security, 25*(1), 80-99. https://doi.org/10.1108/ICS-06-2016-0043

[25] Gulenko, I. (2014). Improving passwords: influence of emotions on security behaviour. *Information Management & Computer Security*, *22*(2), 167-178. https://doi.org/10. 1108/IMCS-09-2013-0068

[26] Hair, J. F., Anderson, R. E., Tatham R. L., and Black, W. C. (1998). *Multivariate Data Analysis* (5th ed.). Upper Saddle River, NJ: Prentice-Hall.

[27] Hair, J. F., Hollingsworth, C. L., Randolph, A. B., and Chong, A. Y. L. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, *40*(3), 414-433.

[28] Hair, J. F., Sarstedt, M., Ringle, C. M., and Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, *40*(3), 414-433. https://doi.org/10.1007/ s11747-011-0261-6

[29] Hartwig, K., and Reuter, C. (2022). Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. *Behaviour & Information Technology, 41*(7), 1357-1380. https://doi.org/10.1080/0144929X.2021.1876167

[30] Henseler, J., Ringle, C. M., and Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135. https://doi.org/10.1007/s11747-014-0403-8

[31] Huber, F., Herrmann, A., Frederik, M., Vogel, J., and Vollhardt, K. (2008). *Kausalmodellierung Mit Partial Least Squares: Eine Anwendungsorientierte Einführung.* Springer-Verlag.

[32] Ilies, R., Scott, B. A., and Judge, T. A. (2006). The interactive effects of personal traits and experienced states on intraindividual patterns of citizenship behavior. *Academy of Management Journal*, *49*(3), 561-575. https://doi.org/10.5465/amj.2006.21794672

[33] Inzlicht, M., Schmeichel, B. J., and Macrae, C. N. (2014). Why self-control seems (but may not be) limited. *Trends in Cognitive Sciences*, *18*(3), 127-133. https://doi.org/10.1016/j.tics.2013.12.009

[34] Illich, I. (1981). *Shadow Work*. Salem, New Hampshire and London: Marion Boyars.

[35] Judge, T. A., Scott, B. A., and Ilies, R. (2006). Hostility, job attitudes, and workplace deviance: Test of a multilevel model. *Journal of Applied Psychology, 91*(1), 126-138. https://doi.org/10.1037/0021-9010.91.1.126

[36] Kaleta, J. P, Lee, J. S., and Yoo, S. (2019). Nudging with construal level theory to improve online password use and intended password choice: A security-usability tradeoff perspective. *Information Technology & People, 32*(4), 993-1020. https://doi.org/10.1108/ITP-01-2018-0001

[37] Keith, M., Shao, B., and Steinbart, P. (2009). A behavioral analysis of passphrase design and effectiveness. *Journal of the Association for Information Systems, 10*(2), 63-89.

[38] Khern-am-nuai, W., Hashim, M. J., Pinsonneault, A., Yang, W., and Li, N. (2022). Augmenting password strength meter design using the elaboration likelihood model: evidence from randomized experiments. *Information Systems Research,* Articles in Advance, 1-21.

[39] Kim, J., and Kang, D. (2008). A study on the factors

affecting the information systems security effectiveness of password. *Asia Pacific Journal of Information Systems*, *18*(4), 1-26.

[40] Kluger, B. M, Krupp, L. B., and Enoka, R. M. (2013). Fatigue and fatigability in neurologic illnesses: Proposal for a unified taxonomy. *Neurology, 80*(4), 409-416. https://doi.org/10.1212/WNL.0b013e31827f07be

[41] Kock, N. (2015). Common method bias in pls-sem: a full collinearity assessment approach. *International Journal of e-Collaboration*, *11*(4), 1-10.

[42] Lambert, C. (2015). *Shadow Work: The Unpaid, Unseen Jobs That Fill Your Day*. Catapult.

[43] Lee, Y., and Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, *48*(8), 72-77.

[44] Li, Y., Zhang, N., and Siponen, M. (2019). Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation. *Behaviour & Information Technology*, *38*(5), 435-453. https://doi.org/10.1080/0144929X.2018.1539519

[45] Lowry, P. B., Twyman, N. W., Pickard, M., and Jenkins, J. L. (2014). Proposing the affect-trust infusion model (ATIM) to explain and predict the influence of high and low affect infusion on web vendor trust. *Information & Management*, *51*(5), 579-594. https://doi.org/10.1016/j.im.2014.03.005

[46] Martin, J., Knopoff, K., and Beckman, C. (1998). An alternative to bureaucratic impersonality and emotional labor: bounded emotionality at the body shop. *Administrative Science Quarterly*, *43*(2), 429-469. https://doi.org/10.2307/2393858

[47] Merdenyan, B., and Petrie, H. (2022). Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours. *Behaviour & Information Technology*, Article in Advance.

[48] Mittal, V., and Ross W. T. (1998). The impact of positive and negative affect and issue framing on issue interpretation and risk taking. *Organizational Behavior and Human Decision Processes, 76*(3), 298-324. https://doi.org/10.1006/obhd.1998.2808

[49] Oreg, S., Bartunek, J. M., Lee, G., and Do, B. (2018). An affect-based model of recipients' responses to organizational change events. *Academy of Management Review, 43*(1), 65-86. https://doi.org/10.5465/amr.2014.0335

[50] Oreg, S., Vakola, M., and Armenakis, A. (2011). Change recipients' reactions to organizational change: A 60-year review of quantitative studies. *The Journal of Applied Behavioral Science*, *47*(4), 461-524. https://doi.org/10.1177/0021886310396550

[51] Park, J., and Oh, C. G. (2016). Cognitive bias and information security research: Research trends and opportunities. *Asia Pacific Journal of Information Systems*, *26*(2), 290-298.

[52] Renaud, K., Zimmermann, V., Schürmann, T., and Böhm, C. (2021). Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, *8*(1), 1-17. https://doi.org/10.1057/s41599-021-00746-5

[53] Schaubroeck, J., and Jones, J. R. (2000). Antecedents of workplace emotional labor dimensions and moderators of their effects on physical symptoms. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior, 21*(2), 163-183. https://doi.org/10.1002/(SICI)1099-1379(200003)21:2<163::AID-JOB37>3.0.CO;2-L

[54] Seo, M. G., Barrett, L. F., and Bartunek, J. M. (2004). The role of affective experience in work motivation. *Academy of Management Review, 29*(3), 423-439.

[55] Shen, J., Barbera, J., and Shapiro, C. M. (2006). Distinguishing sleepiness and fatigue: Focus on definition and measurement. *Sleep Medicine Reviews*, *10*(1), 63-76. https://doi.org/10.1016/j.smrv.2005.05.004

[56] Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis, 24*(2), pp. 311-322. https://doi.org/10.1111/j.0272-4332.2004.00433.x

[57] Stanton, B., Theofanos, M. F., Prettyman, S. S., and

Furman, S. (2016). Security fatigue. *IT Professional*, *18*(5), 26-32.

[58] Stobert, E., and Biddle, R. (2014). The password life cycle: User behaviour in managing passwords. In *Paper presented at the 10th symposium on usable privacy and security (SOUPS 2014)*.

[59] Tam, L., Glassman, M., and Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology, 29*(3), 233-244. https://doi.org/10.1080/01449290903121386

[60] Urbach, N., and Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application, 11*(2), 5-40.

[61] Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425-478.

[62] Wei, M., Golla, M., and Ur, B. (2018). The password doesn't fall far: How service influences password choice. *Who Are You, 87*, 108-112.

[63] Weiss, H. M., Nicholas, J., and Daus, C. (1993). *Affective and Cognitive Influences on Job Satisfaction*. San Francisco, CA: Society of Industrial and Organizational Psychology.

[64] Weiss, H. M., and Cropanzano, R. (1996). Affective events theory: A theoretical discussion of the structure, causes and consequences of affective experiences at Work. In B. M. Staw, & L. L. Cummings (Eds.), *Research in Organizational Behavior: an Annual Series of Analytical Essays and Critical Reviews* (pp. 1-74). Greenwich, CT: JAI Press.

[65] Weiss, H. M., Nicholas, J. P., and Daus, C. S. (1999). An examination of the joint effects of affective experiences and job beliefs on job satisfaction and variations in affective experiences over time. *Organizational Behavior and Human Decision Processes, 78*(1), 1-24. https://doi.org/10.1006/obhd.1999.2824

[66] Wetzels, M., Odekerken-Schröder, G., and van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly, 33*(1), 177-195.

[67] Woods, N., and Siponen, M., (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies, 128*(6), 61-71. https://doi.org/10.1016/j.ijhcs.2019.02.003

[68] Yıldırım, M, and Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security, 18*(6), 741-759.

[69] Zhang, P. (2013). The affective response model: a theoretical framework of affective concepts and their relationships in the ICT context. *MIS Quarterly*, *37*(1), 247-274.

[70] Zimmermann, V., and Gerber, N. (2020), The password is dead, long live the password: A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies, 133*(January), 26-44. https://doi.org/10.1016/j.ijhcs.2019.08.006

[71] Zviran, M., and Haga, W. J. (1999). Password security: An empirical study. *Journal of Management Information Systems*, *15*(4), 161-185. https://doi.org/10.1080/07421222.1999.11518226

<Appendix A> Collinearity statistics (VIF)

Construct	AR	AC	FP	IP	SW	SW x AC
Negative Password Fatigue-Induced Affect (AR)		1.360				
Attitude toward changing passwords (AC)				1.081		
Feelings of password fatigue (FP)	1.000	1.360				
Intention to change passwords (IP)						
Shadow work recognition(SW)				1.044		
SW x AC				1.037		

◆ About the Authors ◆

Sang Cheol Park

Sang Cheol Park is currently an associate professor of College of Business at Daegu University in Korea. He received his Ph.D. in MIS from Sungkyunkwan University in Korea. He previously worked for Georgia State University as a post-doctoral researcher and joined in University of Tennessee (Knoxville) as a visiting scholar. His research focuses on the areas of judgment and decision making in technology usage context and digital platform work with shadow work. His research has appeared in the *JAIS, EJIS, ISJ, JGIM, CHB, JCIS*, and among others.

Submitted: January 11, 2023; 1st Revision: March 23, 2023; Accepted: May 24, 2023