information

Article

Does an Information System Security Notice Format Influence Users' Compliance Willingness from the Perspective of the Framing Effect?

Linhui Sun [1], Xun Li [1,*], Jie Gao [2,*] and Fangming Cheng [3]

[1] School of Management, Xi'an University of Science and Technology, Xi'an 710054, China
[2] School of Management, Xi'an Jiao Tong University, Xi'an 710049, China
[3] School of Safety Science and Engineering, Xi'an University of Science and Technology, Xi'an 710054, China
* Correspondence: lx15914231728@163.com (X.L.); gaoj@mail.xjtu.edu.cn (J.G.)

Abstract: Information security issues have triggered both academic and practical circles to think about operation management and the sustainable development of information systems. Based on the theory of framing effect, this study constructs a theoretical model of the presentation framework of security notice information on users' compliance willingness and empirically tests the proposed research hypotheses using a combination of behavioral experiments and questionnaires to analyze the mechanism of the information presentation framework on compliance willingness. The results show that (1) the information presentation framework has a significant effect on users' decision to comply, but it varies according to specific frameworks. While the attribute and risk frameworks have a significant effect on users' decision to comply, the goal framework does not have a significant effect on users' decision to comply. (2) The security notice situation moderates the relationship between the security notice information presentation frame and users' compliance willingness, but this varies according to the specific situation of the specific framework. The security notice situation moderates the relationship between the attribute framework, the risk framework, and users' compliance willingness but not the relationship between the goal framework and users' compliance willingness. (3) Information security cognition has a moderating effect on the relationship between the security notice presentation framework and users' compliance willingness, but it varies by the specific frameworks. Information security cognition moderates the relationship between attribute frames, risk frames, and users' compliance willingness but not the relationship between goal frames and users' compliance willingness.

Keywords: framing effect; security notice; compliance willingness; notice format; information system

Citation: Sun, L.; Li, X.; Gao, J.; Cheng, F. Does an Information System Security Notice Format Influence Users' Compliance Willingness from the Perspective of the Framing Effect? *Information* **2023**, *14*, 39. https://doi.org/10.3390/info14010039

Academic Editor: Costas Vassilakis

Received: 4 December 2022
Revised: 2 January 2023
Accepted: 6 January 2023
Published: 9 January 2023

1. Introduction

Information systems are frequently used by a variety of businesses and organizations to support their own operational management, to conduct enterprise resource planning, and to view information systems as playing a crucial part in the management of production activities. Systems for handling the collection, processing, transfer, storing, and utilization of information are known as information systems. Today, information systems are a crucial and advantageous tool for organizational management and enterprise resource management. Indeed, various information systems have merged with communication and computer technologies, and the term "information system" now most often refers to the system that enables human and computer coexistence.

System equipment will continuously provide users with a variety of feedback prompts in a variety of methods during the functioning of the information system. When a user performs a job within the system, the system responds to their actions by sending feedback

prompts. These prompts include requests for personal information, security notices regarding the system's operational state, etc. Of these, security notices are one of the most common categories of feedback prompts.

The purpose of security notices is to inform users of the implications of their current actions, including the preservation of system identification numbers (IDs) or passwords, the backup of key customer data, and the encryption of classified files. Generally speaking, compliance and confirmation are the decision content required from users in the face of these security notices, which include users' determination of whether some user privileges are available to the system, whether users' current operations are in line with their actual intentions, whether they will choose to comply with the system specifications required by the security notices, and whether they will choose to share key information. Security notices often play a guiding role in users' information security behaviors and have been shown to have an impact on the effective and stable operation of information systems [1].

In the case of information systems, security notices can provide good information feedback to users by making the user more aware of the system's operations, reducing waiting anxiety, improving users' experience, and increasing users' compliance willingness. By creating psychological expectations, security notices help users form compliance expectations by letting them know whether their operations have been executed, if they have been undone, what impact they will have after execution, where the execution results could be checked, and how to resolve current system problems, all of which will increase users' compliance willingness with the next system operation. Meanwhile, the user's compliance willingness influence information security, personal property protection, and privacy assurances if they are willing to comply with the system requirements. Clearly, security notices and compliance willingness are interrelated, and the importance of security notices and compliance willingness for information systems is self-evident.

It has been demonstrated that the notice format (textual description) of information system security notices has an impact on individuals' behavioral willingness [2]. In other words, different methods of presenting information would affect people's behavior choices. However, the influence of information descriptions on users' behavioral choices in real life has often been neglected, leading to the development of hidden issues relating to information security behavior and the development of security issues. Considering this, it is highly useful to investigate the impact of notice formats on compliance willingness of users regarding security notices, in order to enhance users' compliance willingness with information system security notices, as well as to improve users' attitudes toward security notices. For reference, the security notice interface of the information system used in the actual situation in the current study is shown in Figure 1.

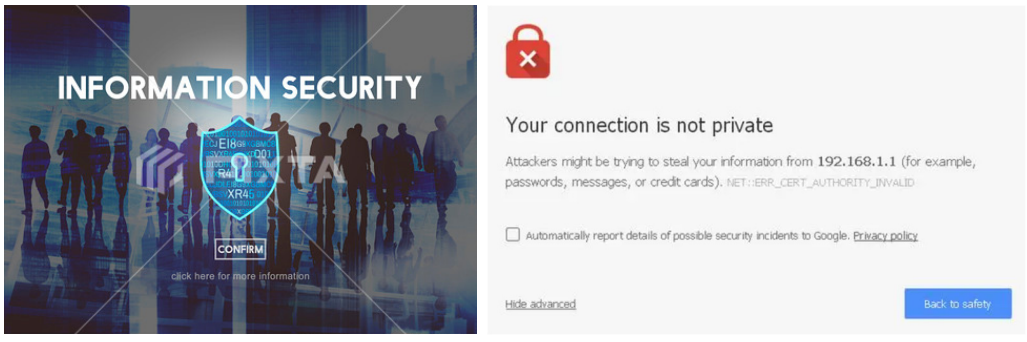

Figure 1. Security Notice Interface.

2. Literature Review

The framing effect refers to the possibility that alternative formulations of the same issue may influence people's choices [3]. Its existence was discovered by Tversky and Kahneman in their "Asian Disease Problems" study. Furthermore, after an interdisciplinary meta-analysis, Levin et al. (1998) found that there are three distinct categories into which

framing effects can be subdivided: risk framing effects, attribute framing effects, and goal framing effects. Each of these categories has a different information description focus [4].

Numerous studies have shown that the framing effect has two division dimensions: the external framing effect and the internal framing effect. The internal framing effect is also known as the self-framing effect, as used by Levin (1998) and Wang (2004) [4,5]. Additionally, Wang (1996) also proved the existence of the two-way and one-way framing effects as further dimensional divisions [6].

The framing effect phenomenon has attracted the attention of numerous scholars, and it continues to be discussed and explored in a variety of different research fields, including the real estate market [7], purchase intention [8], donor decision [9], perceived credibility [10], public attitude [11], and more. A framing effect has also been found in the area of information security [12]. As the information security of a system is often reflected in the specific results brought by the user after the operation or the online security behavior of the user, a framing effect may also exist in the compliance decisions in response to security notices. It is worth noting that after clarifying the classification of the framing effect, subsequent scholars have jointly or separately discussed its influence or application in specific scenes or situations based on either three types or a single type in different research fields based on this classification.

2.1. Research on the Attribute Framing Effect

The attribute framing effect affects evaluations about the characteristics of an object or event, and a positive attribute framing effect occurs when a key characteristic of a thing or event is placed in a positive light. In general, people prefer things described with positive framing in the attribute framing effect. For instance, when Levin and Gaeth (1998) classified beef as having a composition of either 75% lean or 25% fat, individuals preferred beef with a 75% lean composition (i.e., beef described with a positive format) [4]. Negative attribute framing effects occur when the key features of a thing or event are placed under negative framing. The research on the attribute framing effect is concentrated primarily in the field of marketing. According to the research by Wen et al. (2021), a negative framing format can increase customers' readiness to acquire and spend while making the decision to purchase personalized vacation packages when compared to a positive framing format [13]. Meanwhile, customers are more likely to pay a higher stated price when prices are presented in a positive format, according to Dixit (2014), than when prices are presented in an unframed or a negative framing format [14].

In the debate of attribute framing effect and individual willingness, Gasteiger (2020) discovered that framing strongly influenced participants' desire to convert to biosimilar drugs, with positive framing being more likely to do so than negative framing [15]. It can be seen that there is a correlation between the attribute framing effect and individual willingness. In view of this, in the process of designing information systems, system developers should pay attention to the security notices of different notice formats so that they might develop and utilize security notices with particular attribute frameworks to better guide the users' compliance decisions.

2.2. Research on the Goal Framing Effect

The goal framing effect refers to the ability to change the decision-making behavior of individuals by affecting the persuasiveness of communicated information. When persuasive messages focus on the positive consequences of an action, or when they focus on negative consequences, the messages will have a different level of attractiveness, resulting in the goal framing effect. The goal framing effect can be divided into a framework that may achieve gains (i.e., gain framework) and a framework that may face losses (i.e., loss framework). Meyerowits and Chaiken's (1987) Breast Self-Examination study, which encouraged women to voluntarily submit to breast examinations, is one particularly known example of goal framing effect research [16]. Although research on the goal framing effect has also been concentrated in the field of marketing, it has also been discussed in other fields.

For instance, Yang (2020) discovered that media persuasion influenced residents' green buying behavior by simultaneously activating a three-dimensional goal framework [17]. Wang (2022) observed that individuals with high (vs. poor) self-esteem had increased destination visit intent in response to gain-framework (vs. loss-framework) statements [18].

Tanford (2019) integrated framing and anchoring effects to evaluate the relationship between price anchoring, framing, and metric compatibility on one's willingness to pay for holiday accommodations when examining the goal framing impact on individual willingness [19]. When presented with reading materials that focused on the advantages for everyone in society rather than only those of the individual, Ceylan (2021) discovered that citizens considered the information more persuasive and were more motivated to help others [20]. DeGolia (2019) discovered that in order to acquire political and public support for environmental management, communicating within a loss framework was more effective than communicating within a gain framework [21]. Meanwhile, participants' opinions regarding vaccination were more favorable when the topic was framed in a positive format, according to a study by Altay (2020) [22]. Furthermore, punitive framing was shown to diminish information sharing willingness and affective commitment while enhancing effort-related commitment, according to the findings of Fehrenbacher (2019) [23].

In view of this, to return to the process of information systems, security notices encountered by users may have different goal frameworks, and users may also have different information security cognition levels. It is therefore worthwhile to draw on existing research paradigms to analyze and test the combination of the above variables in the field of information security to determine what influence mechanisms exist between the users' information security cognition level and their compliance willingness under the goal framework and whether similar differences in influence exist in other types of notice formats.

2.3. Research on the Risk Framing Effect

The risk framing effect refers to the framing effect first proposed by Tversky and Kahneman in 1979. The study of risk framing effects has a long history, and is connected to numerous research fields. The risk framing effect shows how the value function affects risk preferences, and suggests that different risk preferences emerge according to whether the outcome of a risky action is framed positively or negatively, as was demonstrated in the "Asian disease problem" study, which showed that a preference for either benefit or loss avoidance depends on how the question is framed and phrased. More specifically, when presented information with a beneficial framework, people tend to be risk-averse, and when presented information with a loss framework, they tend to be risk-seeking.

Channa (2021) discovered that people with higher levels of risk aversion were marginally more prepared to pay for risk-reducing devices when making risk-based decisions [24]. Li et al. (2020) found that farmers' perceived risk had a substantial negative effect on agricultural green production intentions [25]. Through research into event-related potential, Xu et al. (2020) discovered that, while making risky decisions in the face of uncertainty, gain framing improved behavioral and brain sensitivity to decision failure [26]. In addition, some scholars have discussed the framing effect of risk decision-making within the fields of medicine [27], economics [28], sports science [29], and college students' income control [30,31] and have verified the impact of the risk framing effect on behavioral decision-making in a wide variety of fields.

In the situation of an information system, when a security notice is delivered in a "gain" or a "loss" framework, users are informed of what they stand to gain or lose by obeying the security notice. The aforementioned studies into the impact of framing effects in various domains and the question of whether types of notification formats increase compliance willingness serve as theoretical benchmarks for research on information system security notices.

2.4. Research on Information Security Cognition

Research on information security cognition in recent years has primarily analyzed and discussed from the aspect of information security cognition. By considering the roles of the design and implementation of information security cognition, for instance, Ki-Aries (2017) developed a method for identifying security-related human elements [32]. Meanwhile, Hadlington (2019) demonstrated that job control position has a significant predictive role in calculating the overall information security cognition score [33]. Lh (2020) discovered that moral disengagement tendencies, particularly in the distribution of duty, play a significant influence in information security cognition [34]. Through case studies and questionnaires, Jaeger (2020) found that situational information security cognition improves the perception of risk and one's sense of reaction efficacy, which thereby increases actual behavioral response to phishing assaults [35]. To improve the level of information security cognition among employees in both private and public sector firms, Kk (2021) conducted a thorough assessment of the literature on the topic of information security cognition and recommended a set of advanced information security cognition methods and criteria [36]. Kvds (2021) investigated the role of information security cognition on some users' intentions to review their Facebook privacy settings, or, more specifically, how the Big Five personality qualities interacted with the desire to examine these settings, as mediated by information security cognition [37]. Overall, the introduction of the notion of information security cognition has allowed this study to delve deeper into the influential mechanisms and underlying mechanisms that influence users' willingness to make compliance decisions in the face of security notices.

2.5. Individuals Compliance Willingness Related Research

Social, organizational and individual elements have been shown to make up the three main contributing factors of compliance willingness [38]. Gurses (2018) examined the primary causes of non-compliance in the nursing sector and came to the conclusion that following evidence-based recommendations is essential for providing safe nursing care [39]. Enwereuzor (2020) investigated the relationship between moral leadership and safety compliance, finding that trust in the leader was a moderating component [40]. Meanwhile, Kilbane (2020) examined how staff members felt about using surgical safety checklists in small animal operating rooms, shedding light on the challenges to their utilization [41]. The existing studies are not comprehensive enough to discuss the analysis of information system users' compliance willingness with security notices and their influencing mechanisms.

2.6. Theoretical Analysis Framework

In summary, regardless of the information presentation framework (i.e., risk framework, attribute framework, or goal framework), each information presentation framework can be divided into two categories of positive and negative frameworks. Furthermore, in the situation of security notices, the content of security notices presented by these positive and negative frameworks are both positive and negative aspects of the same information description. Based on the implications of these three frame effects, framing effect theory was deemed to be a suitable theoretical paradigm to utilize to explore information descriptions, making this a reasonable and practical basis on which to build our theoretical model and experimental protocol design for the current study. Therefore, the information presentation framework based on the framing effect theory was used as the independent variable for the conceptual model of this study.

Information processing theory identifies two different systems and modes by which individuals can make decisions: intuitive inspiration and rational analysis. Specifically, when users make compliance decisions under different conditions and in the face of security notices in various situations, they may be influenced by their own information security cognitive level–that is, when a user has a high information security cognitive level, they will more often adopt the rational analysis mode when facing security notices, and make compliance decisions only after fully weighing the pros and cons. In contrast, when a user

has a low information security cognitive level, they will more often adopt the intuitive inspiration mode when facing security notices and make compliance decisions based on their intuitive experience, rather than thinking rationally. One's degree of cognition, or users' understanding and attention to information systems and security notices, will to some degree influence their desire to comply. The introduction of the idea of information security cognition facilitates the investigation of the influence mechanism and inner mechanism of users' readiness to make compliance decisions in the face of security notices.

In information security management, the willingness of users of information systems to comply with security notices may be influenced by the security notice situation. The security notice situation can be understood as a security notice or description with different information content, which appears within the operating environment of an information system, depending on the immediate operating status of the system. In reality, security notices are immediate, multiple, and flexible, and they are important feedback prompts that users are often exposed to when using information systems. In the situation of information system security notices, the content of a security notice is specialized and complex. The decision to comply to a security notice is closely related to the situation of the security notice. In the situation of a security notice that may involve the users' property security, users may have a strong compliance willingness regardless of the nature of the framework in which the system presents the information because they attach special importance to their property security; however, in the situation of security notices that do not involve property security, the users' compliance willingness is more likely to be influenced by the different frameworks in which the information is presented. Therefore, differences in users' compliance willingness in various security notice situations merit further investigation. As such, the concept of the security notice situation was used as a moderating variable in the conceptual model of this study.

Regarding users' compliance willingness, generally speaking, willingness is a prerequisite for behavior formation. One study on policy shaping and behavior compliance noted that the compliance willingness of grassroots cadres to take charge of policy compliance was influenced by individuals' personal characteristics and psychological factors, and this willingness determined their choice of actual compliance behavior. In the field of information security, information security compliance behavior can be understood as the implementation compliance of system users or organization employees in the face of information security policies or information security systems, which is often premised on one's compliance willingness with information security. The individual human will of system users is therefore an important research concern in terms of information security compliance behavior. By analyzing users' compliance willingness in the face of security notices, the laws of user information security compliance behavior can be better understood, and the correlation and consistency between willingness and behavior can also be discussed, thereby enriching the research scope of compliance willingness and information security behavior. We therefore used the concept of users' compliance willingness as the dependent variable in the conceptual model used in this study.

The conceptual model of "information presentation framework–security notice situation–information security cognition–user's compliance willingness" was constructed in this study by synthesizing the above-mentioned theoretical derivation. The model used the security notice information presentation framework as the independent variable, security notice situation and information security cognition as the moderating variables, and users' compliance willingness as the dependent variable, reflecting the correlation and influence mechanisms between the security notice information presentation framework and users' compliance willingness. The conceptual model of this study is shown in Figure 2.

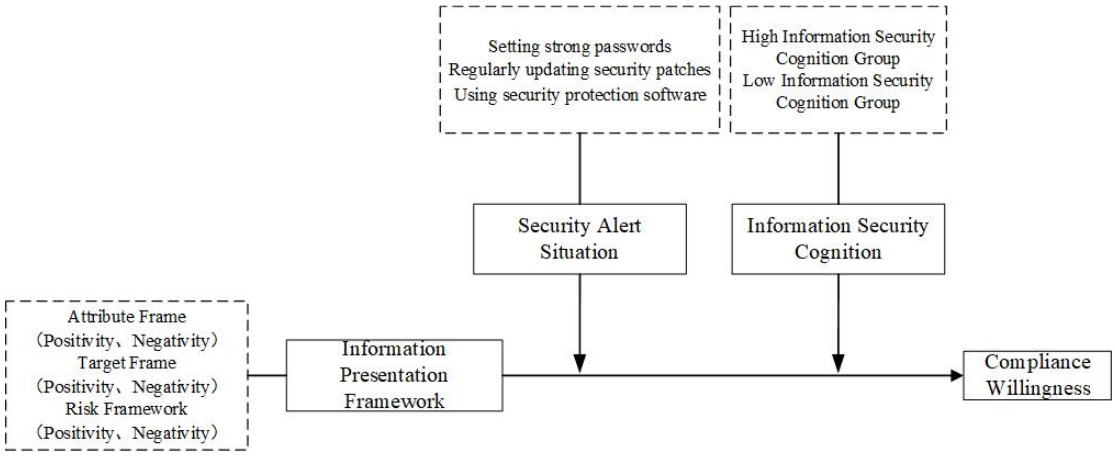

Figure 2. Theoretical Analysis Framework.

2.7. Experimental Hypothesis

The question of whether users' compliance willingness regarding security notices differs across various situations depending on the information presentation framework used, current research is not thorough enough to analyze this issue, but this question has already received the attention of scholars in related fields (e.g., information system, human-computer interaction, and cybersecurity). The content of security notices can greatly influence the understanding and judgment of users in the lead-up to making operational decisions. System users tend to make compliance decisions based on the text headings and content of security notices, so there may be a causal relationship between the information presentation framework and users' compliance willingness.

In the closed loop of "human–machine–environment" management, users are the key detail that can affect the trend of information system security issues, and their compliance willingness with security notices involves a process that begins with a psychological reaction and leads to a behavioral choice, which requires the invoking of their individual information security cognition. Faced with an information system security notice, users will go through the process of weighing pros and cons to make a judgment based on the content of the security notice information presented by the system. Therefore, users' information security cognition level may affect their compliance willingness. To ensure the effective operation of information systems, then, it is necessary to explore the impact of users' information security cognition on the compliance willingness with security notices in order to understand users' cognition and its impact on their evaluation of information security and information systems.

According to the technology–organization–environment framework, an individual's adoption or acceptance of information technology is influenced by both internal forces and the external environment. The security notice is an important environmental factor in information systems. Studies have been conducted in the field of marketing to investigate the moderating effect of purchasing in green advertising appeals and green purchase intentions, confirming the moderating role of the situation in the relationship between appeals and intentions. As a system appeal format, variations in information presentation frameworks in security notices can be integrated with known understandings of their impacts to affect compliance willingness, with consideration of information security cognition. Therefore, this study proposes the following hypotheses, as shown in Table 1.

Table 1. Research Hypothesis.

Experimental Hypotheses for the Attribute Framework
H1: Subjects experience framing effects for all three attribute frameworks when presented with security notice situations.
H1-1: Participants' compliance willingness choices in the positive and negative format conditions differ significantly when prompted to set up a strong password.
H1-2: Participants' compliance willingness choices within the positive and negative format conditions differ significantly when prompted to update security patches regularly.
H1-3: Participants' compliance willingness choices in the positive and negative format conditions differ significantly when prompted to use security protection software.
Experimental Hypotheses for the Goal Framework
H2: Information security notices presented in all three goal-framed situations demonstrate framing effects.
H2-1: Participants' compliance willingness differs significantly according to whether a positive or negative format is used to prompt them to set up a strong password.
H2-2: Participants' compliance willingness differs significantly according to whether a positive or negative format is used to prompt them to regularly update their security patches.
H2-3: Participants' compliance willingness differs significantly according to whether a positive or negative format is used to prompt them to use security protection software.
Experimental Hypotheses for the Risk Framework
H3: Participants demonstrate framing effects when confronted with security notice situations across all three risk frameworks.
H3-1: Participants' choice in deterministic and uncertain scenarios differ significantly according to whether a positive or negative format is used to prompt them to set up a strong password.
H3-2: Participants' choice in deterministic and uncertain scenarios differ significantly according to whether a positive or negative format is used to prompt them to regularly update their security patches.
H3-3: Participants' choice in deterministic and uncertain scenarios differ significantly according to whether a positive or negative format I used to prompt them to use security protection software.
Information Security Cognition Hypotheses
H4: Subjects with different levels of information security cognition differ in their compliance willingness with different types of security notice situations according to the different attribute framework used.
H4-1: Participants with high information security cognition differ in their compliance willingness with security notices depending on the attribute frameworks condition.
H4-2: Participants with low information security cognition differ in their compliance willingness with security notices depending on the attribute frameworks condition.
H5: The compliance willingness of participants with different information security cognitive levels differs when presented with different goal frameworks of security notice situations.
H5-1: Participants with high information security cognition differ in their compliance willingness when presented different goal frameworks of security notice situations.
H5-2: Participants with low information security cognition differ in their compliance willingness when presented different goal frameworks of security notice situations.
H6: Participants with different cognitive levels of information security demonstrate different levels of compliance willingness when presented with security notice situations of different risk frameworks.
H6-1: When faced with security notices of different risk frameworks, users in the high information security cognition group exhibit a different level of compliance willingness.
H6-2: When faced with security notices of different risk frameworks, users in the low information security cognition group exhibit a different level of compliance willingness.

3. Methods

Through three experimental studies that explored the attribute framework, the goal framework, and the risk framework, respectively, this paper explored the influence of different security notice formats on user compliance willingness. To analyse of the various information system situations, the E-prime program was used to present a simulated security notice. The program is designed to carry out behavioral experiments, and it is able to record and measure the system users' compliance decisions and reaction times within the specific attribute, goal, and risk frameworks.

3.1. Participants

Kühberger (1998) found no appreciable difference between the findings of framing effect research that used a student group as the experimental sample compared to a sample comprised of adults with job experience [42]. Therefore, we chose a student group as the experimental sample.

A laboratory study was conducted in which undergraduate and graduate students from general colleges and universities in China participated in the experiment. Empirical studies have shown that the number of participants in E-prime behavioral experiments should generally be within the range of 80 to 200, and the number of participants in framing effect experiment should generally be above 100. For our formal experiment, 180 subjects were recruited and the sample size passed the effect size test, and each subject was required to complete three E-prime experimental procedures, comprising either three positive framework procedures (i.e., positive attribute framework, goal framework, and risk framework) or three negative framework procedures (i.e., negative attribute framework, goal framework, and risk framework). All participants were between the ages of 20 and 30 years. All were familiar with enterprise information systems and had experience in using them. According to the empirical criteria, the experimental subjects all had experience using or hearing information system information prompts. The participants were all in good physical condition, had normal vision, and were right-handed. The experiment of the study was approved by the IRB of university organization.

This study adopted a between-groups design, with participants divided into two groups of 30 each, in accordance with the classification of frameworks. In the attribute framework experiment, the first group completed the positive attribute framework experimental task while the second group completed the negative attribute framework experimental task. In the goal framework experiment, the first group completed the positive goal framework experimental task while the second group completed the negative-goal framework experimental task. In the risk framework experiment, the first group completed the positive risk framework experimental task and the second group completed the negative risk framework experimental task. A pre-experiment had been conducted for all three frameworks to ensure that validity was maintained both internally and externally, leading to an adjustment in the order in which the framework stimulus materials and security notice messages were presented. All participants in the study met the following criteria:

(1) To ensure that visual fatigue did not occur during the experiment, participants were given regular pauses and rest breaks.
(2) Participants had not taken part in similar framework effect experiments prior to participating in the attribute framework experiment, the goal framework experiment, and the risk framework experiment.

3.2. Experimental Procedure

The overall experimental procedure of the framing effect situational experiment is shown in Figure 3.

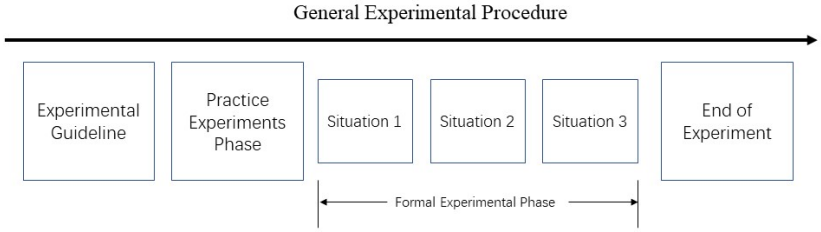

Figure 3. General Experimental Procedure.

(1) *Attribute Framework Experiment Process*

The attribute framework experiment used a 2framework properties (positive frame, negative frame) × 3situations (setting strong passwords, regularly updating security patches, using security protection software) three-factor mixed design, where the information presentation framework and its corresponding frame properties were between-group variables and the security notice situation was a within-group variable. There were three situations: Situation I was to set a strong password, Situation II was to regularly update security patches, and Situation III was for using security protection software. The framework properties of the two security notice situations of the attribute framework were presented randomly, and each experimental subject participated in only one condition (i.e., either positive or negative attribute framework). The attribute framework experiment was divided into a practice experiment phase followed by a formal experiment phase. The content of the experimental stimulus materials for the attribute framework of the setting strong passwords situation is described in detail as an example, and the content of the stimulus materials for the using security protection software situation and the regularly updated security patches situation are detailed in the Appendix A. Situational experiment practice session stage flow and steps are detailed in the Appendix B.

(1) Attribute Framework: (The strong and weak properties of the password-the level of complexity)

【Positivity】When you first register your account for password setting, the confidentiality of your system account depends on the strength of your password, so be sure to set a strong password with high complexity when designing your password. In this case you will set a strong password of your choice.

【Negativity】When you first register your account for password setting, the confidentiality of your system account depends on the strength of the password, so do not set a weak password with low complexity when designing your password. In this case you will set a strong password of your choice.

(2) Formal Phase: The formal experiment was a keystroke response experiment. Before seeing the security notice design, the situational instructions appeared on the screen:

"Suppose you are an information system user and you and the following security notice pops up onscreen while you are at work, how likely would you be to comply? Rate your compliance willingness by choosing a number from 1 to 7 for the given situation, with 1 representing "definitely would not" and 7 representing "definitely yes". The larger the number, the stronger your willingness to comply with the security notices. Please reply honestly." After this screen, the situational experiment began.

In the situational experimental phase, each participant was asked to browse through the attribute formats of the three security notice situations and make a decision about their compliance willingness, regardless of whether the respondent was in the positive or negative attribute framework experiment. Participants were first presented with the attribute framework for Situation 1 (i.e., setting strong passwords), after which they responded to the four measures of compliance willingness using keystroke responses. Once their answers were recorded, the experiment continued following the same procedure for Situation 2 (i.e., regularly updating security patches) and Situation 3 (i.e., using security protection software). The compliance questions used in all three security notice situations were identical in presentation style and wording. The experiment was concluded after the scoring was completed. Participants were then required to complete a post-test questionnaire regarding their information security cognition. The experimental procedure of the attribute framework for the positive–negative framework is shown in Figure 4.

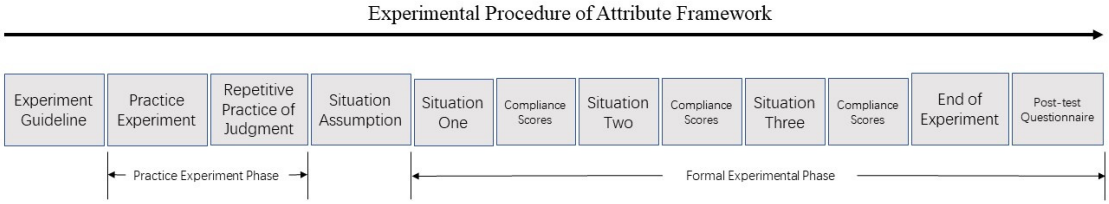

Figure 4. Experimental Procedure for Attribute Framework Effects.

(2) *Goal Framework Experiment Process*

The goal framework experiment used a 2framework properties (positive frame, negative frame) × 3situations (setting strong passwords, regularly updating security patches, using security protection software) three-factor mixed design, where the information presentation framework and its corresponding frame properties were between-group variables and the security notice situation was a within-group variable. The three situations were the same as in the previous part of the experiment, with Situation 1 addressing setting strong passwords, Situation 2 asking the user to regularly update security patches, and Situation 3 for using security protection software. The framework nature of the two security notice situations (i.e., positive or negative goal framework) was presented randomly, and each experimental subject participated in only one goal framework condition. The experiment was divided into a practice experiment phase, followed by a formal experiment phase. The content of the experimental stimulus materials for the goal framework of the setting strong passwords situation is described in detail as an example, and the content of the stimulus materials for the using security protection software situation and the regularly updated security patches situation are detailed in the Appendix A.

(1) Goal Framework: (The degree of security of strong passwords for system accounts)

【Positivity】When you first register your account to log in, you will need to set your password, at which point you will be prompted to pay attention to how strong or weak your password is. If you set a strong password, there is an 80% chance that the system account you are using for work will be secured. At this point you will set a strong password of your choice.

【Negativity】When you first register for an account to log in, you will need to set your password, and you will be prompted to pay attention to how strong or weak your password is. If you set a strong password, there is a 20% chance that the system account you are using for work will be stolen. At this point you will set a strong password of your choice.

(2) Formal Phase: The formal experiment was a keystroke response experiment which followed the same procedure and instructions of the previous part of the experiment.

In the situational experimental phase, regardless of whether the respondents were placed in the positive or the negative goal framework experiment, each participant was asked to look at the goal formats of the three security notice situations and report their willingness to comply with the request. Respondents were first exposed to the goal framework for Situation 1 (i.e., strong password setting) and then asked to rate their responses to this situation using the four measures of compliance willingness according to situation 1. They then followed the same instructions and procedure for Situation 2 (i.e., regularly updating security patches) and Situation 3 (i.e., using security protection software). The compliance questions used in all three security notice situations used the same wording and presentation style, and the experiment was concluded after scoring was complete. Afterwards, participants completed a post-test questionnaire regarding their information security cognition.

(3) *Risk Framework Experiment Process*

The risk framework experiment used a 2framework properties (positive frame, negative frame) × 3situations (setting strong passwords, regularly updating security patches,

using security protection software) three-factor mixed design, where the information presentation framework and its corresponding framework properties were between-group variables and the security notice situation was a within-group variable. The three situations were the same as in the previous two parts of the experiment, with Situation 1 regarding setting strong passwords, Situation 2 addressing regularly updating security patches, and Situation 3 for using security protection software. The framework properties of the two security notice situations of the risk framework were presented randomly, and each participant responded to only one goal framework condition (i.e., positive or negative risk framework). The risk framework experiment was divided into a practice experiment phase and a formal experiment phase. The content of the experimental stimulus materials for the risk framework of the setting strong passwords situation is described in detail as an example, and the content of the stimulus materials for the using security protection software situation and the regularly updated security patches situation are detailed in the Appendix A.

(1) Risk Framework: (The probability of strong passwords to protect system accounts)

【Positivity】The account password of the information system may encounter 600 hacking attacks in a year, and it is necessary to reset the account password to ensure the security of the system account. Below are two options for you to choose from, please select the one you are most likely to comply with.

Option A: Setting a strong password can protect the system account from 400 attacks.

Option B: Setting a strong password has a 2/3 probability of protecting the system account from attacks and a 1/3 probability of not protecting the system account from 600 attacks.

【Negativity】The account password of the information system may encounter 600 hacking attacks in a year, and it is necessary to reset the account password to ensure the security of the system account. Below are two options for you to choose from, please select the one you are most likely to comply with.

Option C: Setting a strong password will expose the system account to 200 attacks.

Option D: Setting a strong password has a 2/3 probability of keeping the system account safe from attacks and a 1/3 probability that the system account will be attacked 600 times.

(2) Formal Phase:

The formal experiment was a keystroke response experiment. Before being shown the security notice, the situation instructions appeared on the screen: "Suppose you are an information system user and you and the following security notice pops up onscreen while you are at work, which choice would you make? Two possible choices are presented for each situation in response to the information system security notices. There is no advantage nor disadvantage between Option A and Option B for each situation. The letters are used only to distinguish between the situations. Please reply honestly." The situational experiment then began.

Respondents were placed in either the positive or negative risk framework condition, and each participant was asked to look at the risk formats of the three security notice situations and to choose a response to the risk situation. Respondents were first presented with the risk format of Situation 1 (i.e., setting strong passwords) and, after seeing it, they chose between two risky situations by choosing the appropriate key. Situation 2 (i.e., regularly updating security patches) and 3 (i.e., using security protection software) were then presented, both following the same presentation style and procedure. The experiment was concluded after the final choice was made. Participants then completed a post-test questionnaire regarding their information security cognition.

3.3. Variable Measurement

The study's independent variables were the three framework formats (i.e., attribute, goal, and risk) that corresponded to the security notice situations. There were six subcat-

egories, as each of the three formats had its own content of positive and negative frameworks.

The users' compliance willingness was set as the dependent variable and was determined by the E-prime program's keystroke response value, which was a score between 1 and 7; higher scores indicated a stronger compliance willingness with the security notifications. There were six subcategories of compliance willingness as well, due to the positive and negative conditions of each of the three frameworks.

The moderating variables in this study were the security notice situation and the information security cognition. Information security cognition can also be understood as security information cognition and refers to the process of individuals receiving and processing system security information and generating relevant cognitive information [43]. Information security cognition is described in the realm of information security as the user's total cognition and judgment of the importance of security notice compliance decisions when making decisions regarding information system operations.

In relation to the security notice situation, Chen (2016) noted the following three examples of information system security policy compliance behavior: utilizing security protection software, setting strong passwords, and keeping up with security patch updates [44]. In this experiment, these three examples were used as the moderating variables. In terms of experimental stimulus materials, following the results of existing studies examining framework effects, we chose to translate and use the "Different beef components purchase willingness problem" and the "Asian disease problem". This experiment controlled the word count of the security notice situation of the attribute framework at 75 $\pm$ 10 words, the word count of the security notice situation of the goal framework at 85 $\pm$ 10 words, and the word count of the security notice situation of the risk framework at 155 $\pm$ 20 words to ensure relative consistency in the reading difficulty across the positive and negative conditions and to control the length of the experiment. No substantial differences existed between the sample groups participating in the different experimental groups.

4. Results

4.1. Testing the Relationship between Attribute Framework and Compliance Willingness

The scale items of the attribute framework situation experiment all passed the reliability and validity tests, as shown in Table 2.

Table 2. Reliability and Validity Analysis Results.

Notice Format	Variants	Item Number	KMO	Approximate Cardinality	df	*p*	Cronbach's α Coefficient
Attribute Framework	Information security cognition	11	0.838	921.675	55	0	0.884
	User compliance	4	0.839	546.509	6	0	0.917

(1) *Hypothetical Test*

A two-way analysis of variance was used to test the influence of the situation and framework nature on participants' compliance willingness (see Table 3). The results show that the situation did not show a significant relationship with compliance willingness (F = 1.276, p = 0.282 > 0.05), indicating that the situation had no differential effect on compliance willingness. The framework properties were significant (F = 11.746, p = 0.001 < 0.05), indicating a main effect and that the different framework properties had differing relationships with compliance willingness. Neither situation nor framework properties showed a significant correlation (F = 0.050, p = 0.951 > 0.05), indicating that there was no second-order relationship between the two variables. Comparison of means for situation and framework properties shown in Table 4.

Table 3. Two-Way ANOVA Results.

Source of Difference	Sum of Squares	*df*	Mean Square	*F*	*p*
Intercept	5740.401	1	5740.401	4403.445	0.000 ***
Situation	3.326	2	1.663	1.276	0.282
Framework nature	15.313	1	15.313	11.746	0.001 ***
Situation × framework nature	0.131	2	0.066	0.050	0.951
Residual	226.829	174	1.304		

Note: *** $p < 0.001$.

Table 4. Comparison of Means for Situation and Framework Properties (Mean ± *SD*).

Situation	Positivity ($n = 90$)	Negativity ($n = 90$)
Using security protection software	5.18 ± 1.19	5.84 ± 1.06
Regularly updating security patches	5.32 ± 1.16	5.88 ± 1.10
Setting strong passwords	5.57 ± 1.31	6.10 ± 0.99

As shown in Table 5, the positive format compliance willingness score of the attribute framework was significantly lower than the negative condition compliance willingness score ($p < 0.05$) in the security protection software situation, thus supporting Hypothesis H1-3. A lower positive condition compliance willingness score was found for the attribute framework while a lower negative condition compliance willingness score was found for the security patch update situation; however, these were statistically not significant ($p > 0.05$). Our Hypothesis H1-2 was not validated. The positive compliance willingness score of the attribute framework was lower than the negative compliance willingness score, but the difference was not statistically significant ($p > 0.05$), indicating that Hypothesis H1-1 was invalid. Mean comparisons of framework properties and situations shown in Figure 5.

Table 5. Simple Effects (Situation and Framework Nature).

Situation	Framework Nature	Mean Difference	*SE*	*t*	*p*
Using security protection software	positivity–negativity	−0.658	0.295	−2.233	0.027
Regularly updating security patches	positivity–negativity	−0.558	0.295	−1.894	0.060
Setting strong passwords	positivity–negativity	−0.533	0.295	−1.809	0.072

A two-way analysis of variance was used to test the relationship between information security cognition and framework nature on compliance willingness (see Table 6). According to the data analysis results, information security cognition showed significant results ($F = 13.373$, $p = 0.000 < 0.05$), indicating that information security cognition showed an association with compliance willingness in a differential manner. The framework properties were significant ($F = 11.986$, $p = 0.001 < 0.05$), suggesting that a main effect was present and that framework properties would influence compliance differently. No significant association was found between information security cognition and framework properties ($F = 0.998$, $p = 0.319 > 0.05$), indicating that there was no second-order effect. Mean comparison of information security cognition and nature shown in Table 7.

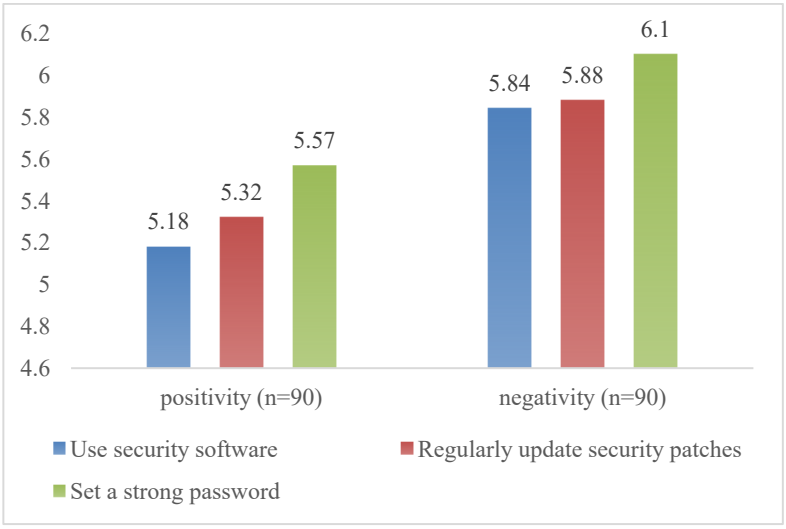

Figure 5. Mean Comparisons of Framework Properties and Situations.

Table 6. Results of Two-Way ANOVA.

Source of Difference	Sum of Squares	*df*	Mean Square	*F*	*p*
Intercept	5479.638	1	5479.638	4531.888	0.000 ***
Information security cognition	16.169	1	16.169	13.373	0.000 ***
Framework nature	14.492	1	14.492	11.986	0.001 ***
Information security cognition × framework nature	1.207	1	1.207	0.998	0.319
Residual	212.807	176	1.209		

Note: *** $p < 0.001$.

Table 7. Mean Comparison of Information Security Cognition and Nature (Mean ± Standard Deviation).

Information Security Cognition	Positivity (n = 90)	Negativity (n = 90)
Low information security cognition	5.09 ± 1.02	5.50 ± 1.08
High information security cognition	5.53 ± 1.32	6.27 ± 0.90

Table 8 shows that the positive condition compliance willingness score of attribute framework did not differ significantly from the negative condition compliance willingness score in the low information security cognition group ($p > 0.05$). Thus, Hypothesis H4-2 is not valid. As expected, however, the high information security cognition group had a significantly lower score for the positive condition compliance willingness within the attribute framework compared to the score for negative condition compliance willingness for the same framework ($p < 0.05$), confirming Hypothesis H4-1. Comparison of the mean value of the nature of the framework and the information security cognition shown in Figure 6.

Table 8. Simple Effects (Information Security Cognition and Framework Properties).

Information Security Cognition	Nature	Mean Difference	*SE*	*t*	*p*
Low information security cognition	positivity–negativity	−0.410	0.254	−1.612	0.109
High information security cognition	positivity–negativity	−0.742	0.215	−3.456	0.001

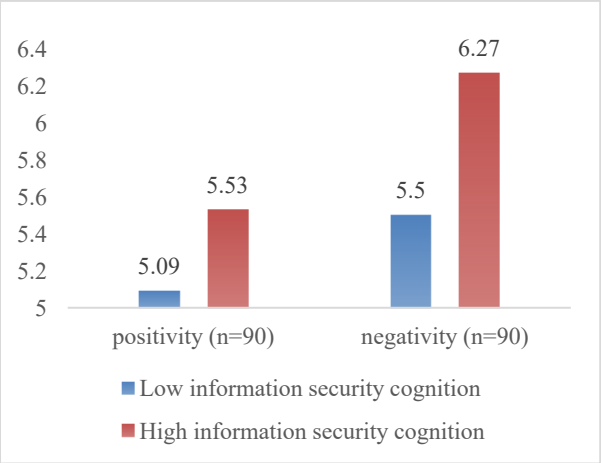

Figure 6. Comparison of the Mean Value of the Nature of the Framework and the Information Security Cognition.

4.2. Testing of the Relationship between Goal Framework and Compliance Willingness

The scale items of the goal framework situation experiment all passed the reliability and validity tests, as shown in Table 9.

Table 9. Reliability and Validity Analysis Results.

Notice Format	Variants	Item Number	KMO	Approximate Cardinality	df	*p*	Cronbach's α Coefficient
Goal Framework	Information security cognition	11	0.838	921.675	55	0	0.884
	User compliance	4	0.843	622.443	6	0	0.935

(1) *Hypothetical Test*

The impact of situation and framework nature on willingness compliance was tested using a two-way analysis of variance, with the results presented in Table 10. These results showed significant differences between the situations (F = 8.055, p = 0.000 < 0.05), indicating that the main effect existed and that the situation affected willingness compliance. A significant difference was not found according to the nature of the framework (F = 0.035, p = 0.851 > 0.05), suggesting that the nature of the framework did not affect compliance willingness. Neither situation nor framework properties were significantly correlated (F = 0.197, p = 0.821 > 0.05), indicating no second-order effect. Comparison of Means for Situation and Framework Properties shown in Table 11.

Table 10. Two-Way ANOVA Results.

Source of Difference	Sum of Squares	*df*	Mean Square	*F*	*p*
Intercept	5811.209	1	5811.209	4883.654	0.000 ***
Situation	19.169	2	9.585	8.055	0.000 ***
Framework nature	0.042	1	0.042	0.035	0.851
Situation × framework nature	0.469	2	0.235	0.197	0.821
Residual	207.048	174	1.190		

Note: *** p < 0.001.

Table 11. Comparison of Means for Situation and Framework Properties (Mean ± Standard Deviation).

Situation	Positivity (n = 90)	Negativity (n = 90)
Using security protection software	5.13 ± 1.10	5.31 ± 1.29
Regularly updating security patches	5.92 ± 0.85	5.88 ± 1.08
Setting strong passwords	5.95 ± 0.83	5.91 ± 1.30

No significant difference was found between the positive condition compliance willingness score in the goal framework and the negative condition compliance willingness score when security protection software is used ($p > 0.05$; see Table 12). Hypothesis H2-3 was thus not supported. In accordance with Hypothesis 2-2, no significant difference was found between positive and negative condition compliance willingness in the goal framework ($p > 0.05$) when it came to regularly updating security patches. However, no significant difference was found between the positive and negative condition compliance willingness scores in the goal framework when it comes to setting strong passwords ($p > 0.05$), so Hypothesis H2-1 could not be verified. Mean comparison plot of framework nature and situation shown in Figure 7.

Table 12. Simple Effects (Situation and Framework Nature).

Situation	Framework Nature	Mean Difference	*SE*	*t*	*p*
Using security protection software	positivity–negativity	−0.175	0.282	−0.621	0.535
Regularly updating security patches	positivity–negativity	0.042	0.282	0.148	0.883
Setting strong passwords	positivity–negativity	0.042	0.282	0.148	0.883

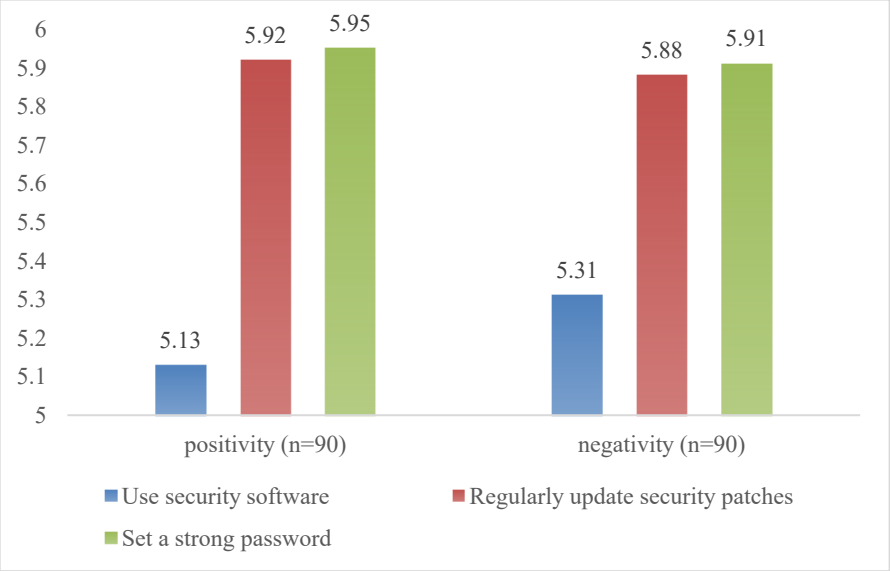

Figure 7. Mean Comparison Plot of Framework Nature and Situation.

This table(Table 13) presents the results of the two-way analysis of variance used to test the influence of information security cognition and nature on willingness compliance. Information security cognition did not appear to have a significant linear relationship with willingness compliance ($F = 2.263$, $p = 0.134 > 0.05$). As a result, there was no significant difference was found between the frameworks ($F = 0.074$, $p = 0.785 > 0.05$), indicating no relevant relationship between the frameworks and compliance willingness. A significant relationship was also not found between information security cognition and framework properties ($F = 0.068$, $p = 0.795 > 0.05$), suggesting that there was no second-order effect

between them. Mean comparison of information security cognition and nature shown in Table 14.

Table 13. Results of Two-Way ANOVA.

Source of Difference	Sum of Squares	*df*	Mean Square	*F*	*p*
Intercept	5598.737	1	5598.737	4404.222	0.000 ***
Information security cognition	2.877	1	2.877	2.263	0.134
Framework nature	0.094	1	0.094	0.074	0.785
Information security cognition × framework nature	0.086	1	0.086	0.068	0.795
Residual	223.735	176	1.271		

Note: *** $p < 0.001$.

Table 14. Mean Comparison of Information Security Cognition and Nature. (Mean ± Standard Deviation).

Information Security Cognition	Positivity ($n = 90$)	Negativity ($n = 90$)
Low information security cognition	5.49 ± 0.99	5.58 ± 1.02
High information security cognition	5.79 ± 0.99	5.79 ± 1.39

As shown in Table 15, there was no significant difference between the positive condition compliance willingness scores of the goal framework and the negative condition compliance willingness scores in the low information security cognition group ($p > 0.05$), so Hypothesis H5-2 was validated. In the high information security cognition group, there was no significant difference between the positive condition compliance willingness scores of the goal framework and the negative condition compliance willingness scores ($p > 0.05$), so Hypothesis H5-1 was also not validated. Comparison of the mean values of the nature of the framework and information security cognition shown in Figure 8.

Table 15. Simple Effects (Information Security Cognition and Framework Properties).

Information Security Cognition	Nature	Mean Difference	*SE*	*t*	*p*
Low information security cognition	positivity–negativity	−0.091	0.261	−0.348	0.728
High information security cognition	positivity–negativity	−0.002	0.220	−0.010	0.992

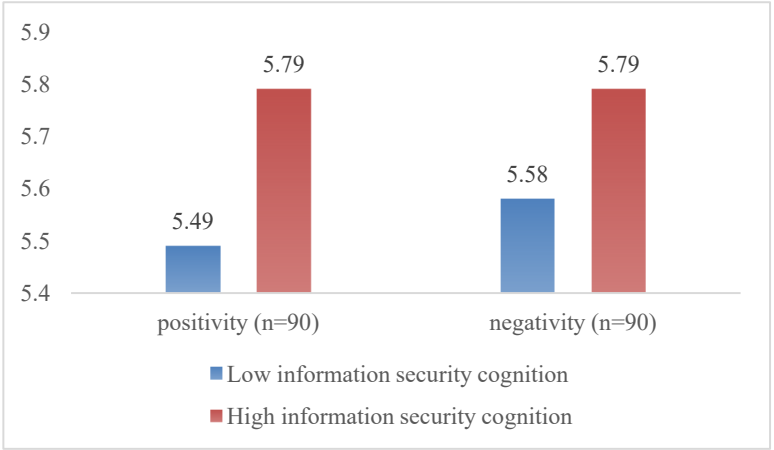

Figure 8. Comparison of the Mean Values of the Nature of the Framework and Information Security Cognition.

4.3. Testing the Relationship between Risk Framework and Compliance Willingness

The scale items of the risk framework situation experiment all passed the reliability and validity tests, as shown in Table 16.

Table 16. Reliability and Validity Analysis Results.

Notice Format	Variants	Item Number	KMO	Approximate Cardinality	df	*p*	Cronbach's α Coefficient
Risk Framework	Information security cognition	11	0.838	921.675	55	0	0.884

(1) Hypothetical Test

Table 17 shows that the nature of the framework showed a 0.05 level of significance (chi = 5.554, $p = 0.018 < 0.05$) for the risky scenario selection in the security protection software situation. Meanwhile, 73.33% of users selected uncertainty scenarios in the negative condition, which is significantly higher than the percentage of uncertainty scenarios selected in the positive condition (43.33%). There was a significant increase in the percentage of users selecting the deterministic scenario in the positive condition, with 56.67% compared to 26.67% in the negative condition.

Table 17. Results of Cross-Tabulation (Chi-Square) Analysis.

Situation	Program Nature	Framework Nature (%)		Grand Total	χ^2	*p*
		Positivity	Negativity			
Using security protection software	Uncertainty scenarios	13 (43.33)	22 (73.33)	35 (58.33)	5.554	0.018 *
	Deterministic scenarios	17 (56.67)	8 (26.67)	25 (41.67)		
Regularly updating security patches	Uncertainty scenarios	7 (23.33)	20 (66.67)	27 (45.00)	11.38	0.001 ***
	Deterministic scenarios	23 (76.67)	10 (33.33)	33 (55.00)		
Setting strong passwords	Uncertainty scenarios	11 (36.67)	19 (63.33)	30 (50.00)	4.267	0.039 *
	Deterministic scenarios	19 (63.33)	11 (36.67)	30 (50.00)		

* $p < 0.05$, *** $p < 0.001$.

In the security patch update situation, the nature of the framework showed a 0.001 level of significance (chi = 11.380, $p = 0.001 < 0.01$) for the risky solution selection, with 66.67% of users choosing the uncertainty scenarios in the negative condition, which was significantly higher than the percentage of users who chose the uncertainty scenarios for the positive condition (23.33%). The percentage of users who chose the deterministic scenarios in the positive condition was 76.67%, which was significantly higher than the percentage of those who chose the deterministic scenarios in the negative condition (33.33%).

In the strong password situation, the nature of the framework showed a 0.05 level of significance (chi = 4.267, $p = 0.039 < 0.05$) for the risky solution selection. There was a significant difference between the percentages of users who chose uncertainty scenarios under the negative format (63.33%) and those who chose uncertainty scenarios under the positive condition (50.00%). It is noteworthy that the percentage of users who chose the deterministic scenarios in the positive condition was 63.33%, which is significantly higher than that of the users who chose the deterministic scenarios in the negative condition, which was 36.67%. Thus, hypotheses H3-3, H3-2, and H3-1 are all valid.

Table 18 shows that, in the low information security cognition group, the nature of the framework presents a 0.01 level of significance for the risky solution selection (chi = 7.090, $p = 0.008 < 0.01$), and the percentage of users who chose the uncertainty scenarios in the negative condition was 64.10%, which is significantly higher than the percentage of users who chose the uncertainty scenarios in the positive condition, which was 33.33%. It was found that 66.67% of users chose the deterministic scenarios in the positive condition, which was significantly higher than the 34.90% who chose them in the negative condition.

Table 18. Results of Cross-Sectional (Chi-Square) Analysis.

Classification Items	Program Nature	Framework Nature (%)		Grand Total	χ^2	p
		Positivity	Negativity			
Low information security cognition	Uncertainty scenarios	12 (33.33)	25 (64.10)	37 (49.33)	7.09	0.008 **
	Deterministic scenarios	24 (66.67)	14 (35.90)	38 (50.67)		
High information security cognition	Uncertainty scenarios	19 (35.19)	36 (70.59)	55 (52.38)	13.18	0.000 ***
	Deterministic scenarios	35 (64.81)	15 (29.41)	50 (47.62)		

** $p < 0.01$, *** $p < 0.001$.

In the high information security cognition group, the nature of the framework showed a 0.001 level of significance (chi = 13.180, $p = 0.000 < 0.001$) for the choice of risky scenarios, and a percentage comparison of the differences showed a 70.59% percent choice of uncertainty scenarios in the negative condition compared with the 35.19% who choose the uncertainty scenarios in the positive condition. It is significant that 64.81% of users chose the deterministic scenario in the positive condition, which was significantly higher than the 29.41% who chose it in the negative condition. As such, Hypotheses H6-2 and H6-1 are supported.

5. Discussion

5.1. Discussion on the Experimental Results of the Attribute Framework

A user's compliance willingness was shown to be stronger in the negative format of the attribute framework, regardless of which security notice situation they were in. The situations of regularly updating security patches and setting strong passwords had no significance in terms of users' compliance in the attribute framework; that is, the p-value is not significant, although the use of security protection software showed an indistinctive effect. Despite the fact that users may make different compliance decisions when it comes to setting strong passwords and updating security patches, the situational effects of these two situations may be less apparent than those associated with using security protection software, which can lead to the problems described by the other two situations. We would propose that an insufficient amount of attention has been put on the specific situation when developing security notices, and strong situational cognition has not been developed in users, resulting in no significant changes made in users' decision-making process regarding compliance.

5.2. Discussion on the Experimental Results of the Goal Framework

Users' compliance willingness in the positive condition in the goal framework was more than in the negative condition when it came to updating security patches and creating strong passwords. In situations where security protection software is used, compliance willingness with the negative condition was significantly higher than in the positive condition. There was a greater compliance willingness with this framework than there was in the positive condition. Therefore, the p value was not significant in any of the above three situations, which indicates that there was no significant user compliance willingness. As a result, while users tended to make various compliance judgments in response to the various situations in the positive and negative conditions, the goal framework itself may accentuate the positive or negative effects of a particular action, creating further encouragement for users to act a certain way. Additionally, in the attribute framework situation, it is possible for cognitive dissonance to have arisen in relation to situational factors, for example, thinking that the goal framework situation may result in irreversible commitments that may ultimately result in insignificant differences in compliance decision-making.

5.3. Discussion on the Experimental Results of the Risk Framework

In the risk framework experiment, significant differences were found between users' choices of deterministic and uncertain solutions in both the positive and negative condition

in all three situations (i.e., setting strong passwords, regularly updating security patches, and using security protection software). Meanwhile, in both the high and low information security cognition groups, differences were found in users' compliance willingness with security notices when faced with different risk framework nature.

In the risk framework, regardless of the security notice situation, users preferred the uncertain risk option in the negative condition while they preferred the deterministic risk option in the positive condition. This result is consistent with those of Tversky and Kahneman (1981) in response to their Asian disease problem study, finding that individuals tended to be risk-averse (i.e., choosing deterministic options) when faced with a benefit framework and risk-seeking (i.e., choosing uncertain options) when faced with a loss framework. This is also similar to the results of other existing studies on risk frameworks. Meanwhile, the results of the data analysis showed that there were significant differences, that is, significant p-values in users' risky scenario decisions in all three security notice situations. This shows that the individual risk preference phenomenon also exists in the information security domain.

Generally speaking, users showed strong compliance willingness or risk preference in the negative conditions of all three frameworks (i.e., attribute, goal, and risk frameworks) while their compliance willingness and risk preference in the positive conditions of all three frameworks were not strong. The intensity of users' compliance willingness or risk preference in both the positive and negative conditions was limited by their own information security cognition; that is, users showed similar compliance willingness and risk appetite in all positive or all negative conditions, regardless of the framework. The performance indicates that users' compliance willingness is the result of the interaction between the individual and the situational factors.

5.4. Practical Inspiration

With regard to security notices in information systems, no new frameworks were explored in this study, only the three frameworks mentioned in this study. This study proposes recommendations for the design and management of security notices for system users and information system platforms, respectively, in order to improve the degree of users' compliance willingness with security notices and reduce the possibility of system information security problems. For system users, the following aspects should be emphasized in terms of compliance willingness.

(1) In terms of behavioral will, users should regulate their own information security behavior. Users should pay attention to the decision of compliance with information system security warnings, set strong passwords for system accounts, update security patches regularly, and use security protection software according to the recommended operation settings of security warnings, so as to comply with the prompt requirements of security notices. Users also need to develop a good awareness of information system security notice compliance to avoid risks such as information leakage due to violation of the norms of security warnings. At the same time, users should pay attention to the security notices presented by the information system in a timely manner, especially the security notice situations involving the security of users' property, and should not ignore the security notices presented by the information system but should always pay attention to them to ensure the security of personal and system information.

(2) In information security cognition, users should strengthen their personal information security awareness. Users need to pay attention to various forms and types of information security training and education to enhance their own information security cognition. Only by realizing the importance of information security at the cognitive level can we control the occurrence of security threats such as information leakage from the root. Users can actively participate in the information security lectures or education training organized by their own organizations to enrich the theoretical knowledge of relevant information security, enrich the knowledge accumulation of

personal information security, and avoid unnecessary losses due to certain fake and deceptive nature of security notice links.

The findings of this paper can also provide organizations or enterprises with theoretical support in information security management, which can be used to guide users to protect system information security more reasonably and effectively, and it can also help system developers to adopt effective, appropriate, and reasonable security notice design plans and measures. Specific aspects can be carried out as follows:

(1) Design and use a framework for presenting security notice information that facilitates user compliance. Guiding users' information security behavior and making users' compliance with security notices a normal behavior. Security notices are an important part of information system development and design; system developers should avoid complicating the design of security notices and should not abuse security notices. It is better to come from and go to the actual situations of information systems, design suitable security notices according to different situations, and pay attention to the design of the information presentation framework of security notices while complying with different design specifications and summarize the personalized information presentation framework suitable for each situation. The personalized information presentation framework for each situation is summarized, and if necessary, "one situation, one design" is achieved.

(2) Optimize the visual design of security notices. While focusing on the information presentation framework of security notices, attention should also be paid to the graphical design of security notices. Studies have pointed out that window size, button order change, window inverse color, window background color, text background color, and font color are the style design elements of the graphical design of the warning pop-up window. System developers can optimize one or all of these elements according to the specific information system and the characteristics of the information presentation framework of security notices.

(3) It has been shown that, compared to "security tips", "security warnings" are more attractive to users' attention when they appear, causing them to devote more cognitive resources to read the warnings carefully, and they are more likely to act in compliance with the text message of the security warning. They are also more likely to comply with the text message.

It can be seen that, as a type of warning that brings new stimuli to users and arouses their awareness, security warnings can achieve better warning effects and promote stronger compliance behaviors. In view of this, system developers should design more warning-type security notices in information systems, especially in interfaces involving the confirmation of important information, such as the entry of critical personal information, property amount entry, or payment, because users will rely more on the content of security notices in these interfaces to indicate cautious decision making. In other information system interfaces of relatively minor importance, security warnings can be replaced by security tips to reduce the cognitive load of users. In addition, in the process of designing security warnings, attention should be paid to the customary expression of textual information (i.e., to achieve the expression of warning alerts while conforming to the reading habits of the warning language).

6. Conclusions and Limitations

6.1. Limitations

Our findings shed new light on users' compliance willingness in an information security situation with consideration of framing effect theory. However, it should be noted that there are some limitations to the current study. First, the E-prime platform was used to collect behavioral experimental data in this study. This platform provides simulated security notices and provides users with a fair amount of control over their design and presentation; however, due to the limitations of the platform, specific notice content and

the content related to the real environment can still be vague or unspecific. In the future, better experimental tools should be adopted to develop improved schemes for selecting risk frameworks for the three security notice situations that would better reflect real-world situations.

Second, all three experiments in the current study used the seven numeric keys of the E-prime keyboard to indicate users' degree of compliance willingness. In real-life situations, the user may also be required to use touch screens, electronic pens, or other devices in addition to a keypad. Simultaneous needs to respond to notices, perform repeated operations, or face task operation decisions in addition to making a decision regarding a given security notice may result in further uncertainty due to social facilitation effects in real-life situations, which alters users' actual decision-making environment in comparison to the simulated decision-making situation.

6.2. Conclusions

Using framing effect theory as its foundation, this study examined the impact of information formats (in terms of positive or negative presentations) on users' compliance willingness when making decisions instigated by information system security notices. Our findings verified that users will respond differently to different types of security notices. Furthermore, system users with varying information security cognition levels demonstrated different compliance willingness. However, different formats of security notices are associated with different security notice situations. In turn, they can have an effect on one's level of information security cognition and, subsequently, on their level of compliance. Our findings suggest the following conclusions:

(1) Within the attribute framework experiment, a significant difference was found between users' compliance willingness with the positive condition compared to the negative condition in the security protection software situation. However, when faced with security notice situations with different attribute framework properties, users with high information security cognition exhibited different compliance willingness. Compliance willingness was not affected by the situation or nor information security cognition in the remaining situations.
(2) In the goal framework experiment, neither the positive nor the negative conditions were associated with significant differences in user compliance willingness in any of the three situations (i.e., strong passwords, security patches, and security protection software). Furthermore, no difference was seen in users' compliance willingness across the various security notice situations with different goal framework properties in either the high or low information security cognition groups.
(3) In the risk framework experiment, users showed significant differences in their choices of deterministic or uncertain schemes across the various tested situations (i.e., setting strong passwords, updating security patches, and using security protection software). Furthermore, differences were seen in users' compliance willingness in the high and low information security cognition groups in response to the security notices with different risk framework properties.
(4) Compliance willingness varied according to the framework in which information security cognition was applied.

6.3. Prospects and Future Work

The current study focused on the independent element design of the information system security notice in order to explore user compliance willingness. Three common security notice situations, which corresponded with the experimental design requirements, were used to assess design frameworks, specifically the attribute framework, the goal framework, and the risk framework. Future research should consider and test more security notice situations, and a format for presenting information should be designed to provide users with a better understanding regarding the impacts of their security notice compliance decisions.

Future research should also consider combining the graphic framing effect with graphic representation to determine whether graphic representations influence users' compliance willingness under the same conditions as when the security notice expression information remains the same, as well as to better understand the mechanisms involved in users' judgment and decision-making.

Author Contributions: Project administration, L.S. and J.G.; Supervision, F.C.; Writing–original draft, review & editing, X.L. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by the National Key R&D Program Project: "Open Ecological Cloud ERP Platform" (Project No.: 2019YFB1704103).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All relevant data used in the evaluation is displayed in the graphs contained within this article. Values for the raw data points are available upon request.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Situational stimulus materials on information system security notices.

1. Strong Password Setting
Attribute Framework: (The strong and weak properties of the password-the level of complexity) 【Positivity】When you first register your account for password setting, the confidentiality of your system account depends on the strength of your password, so be sure to set a strong password with high complexity when designing your password. In this case you will set a strong password of your choice. 【Negativity】When you first register your account for password setting, the confidentiality of your system account depends on the strength of the password, so do not set a weak password with low complexity when designing your password. In this case you will set a strong password of your choice.
Goal Framework: (The degree of security of strong passwords for system accounts) 【Positivity】When you first register your account to log in, you will need to set your password, at which point you will be prompted to pay attention to how strong or weak your password is. If you set a strong password, there is an 80% chance that the system account you are using for work will be secured. At this point you will set a strong password of your choice. 【Negativity】When you first register for an account to log in, you will need to set your password, and you will be prompted to pay attention to how strong or weak your password is. If you set a strong password, there is a 20% chance that the system account you are using for work will be stolen. At this point you will set a strong password of your choice.
Risk Framework: (The probability of strong passwords to protect system accounts) 【Positivity】The account password of the information system may encounter 600 hacking attacks in a year, and it is necessary to reset the account password to ensure the security of the system account. Below are two options for you to choose from, please select the one you are most likely to comply with. Option A: Setting a strong password can protect the system account from 400 attacks. Option B: Setting a strong password has a 2/3 probability of protecting the system account from attacks and a 1/3 probability of not protecting the system account from 600 attacks. 【Negativity】The account password of the information system may encounter 600 hacking attacks in a year, and it is necessary to reset the account password to ensure the security of the system account. Below are two options for you to choose from, please select the one you are most likely to comply with. Option C: Setting a strong password will expose the system account to 200 attacks. Option D: Setting a strong password has a 2/3 probability of keeping the system account safe from attacks and a 1/3 probability that the system account will be attacked 600 times.

Table A1. *Cont.*

2. Regularly Updating Security Patches
Attribute Framework: (Timeliness and relevance of patch installation) 【Positivity】In the process of using the system, the system prompts you to update the patch, because the security patch in the system is time-sensitive and targeted, be sure to install the patch package in time, and select all the security patch content. At this time you will update the security patch will choose. 【Negativity】In the process of using the system, the system prompts you to update the patch, because the security patch in the system is time-sensitive and targeted, do not install the patch package out of date, do not miss the security patch content. At this time, you will update the security patch will choose.
Goal Framework: (The extent of patching on system data recovery) 【Positivity】In the process of using the system, the system prompts you to update the patch, because the security patch in the system is time-sensitive and targeted, if the patch package is installed in time, there is an 80% possibility to get restored in case of information loss. At this time you will update the security patch will choose. 【Negativity】In the process of using the system, the system prompts you to update the patch, because the security patch in the system is time-sensitive and targeted, if the patch package is installed in time, there is a 20% chance of permanent loss in the event of information loss. At this time you will update the security patch will choose.
Risk Framework: (Probability of success/failure of software updates) 【Positivity】During the period of using the information system, the system prompts you that there are 20 security patches for your device software that need to be updated in a timely manner. Below are two options for you to choose from, please select the one you are most likely to comply with. Option A: This update will have 15 patches updated successfully. Option B: There is a 3/4 chance that 20 patches will be updated successfully with this update, and a 1/4 chance that no patches will be updated successfully. 【Negativity】During the period of using the information system, the system prompts you that there are 20 security patches for your device software that need to be updated in a timely manner. Below are two options for you to choose from, please select the one you are most likely to comply with. Option C: This update will have 5 patch updates fail. Option D: There is a 3/4 chance that this update will fail without a patch, and a 1/4 chance that the 20-patch update will fail.
3. Using Security Protection Software
Attribute Framework: (Versions of Software-Genuine and Pirated) 【Positivity】For security maintenance needs, the system prompts you to use security protection software to ensure the stable operation of the system, as the protection function on the software depends on the system's data services, it is important to apply genuine security protection software. At this time you will use the security protection software will choose. 【Negativity】For security maintenance needs, the system prompts you to use security protection software to ensure the stable operation of the system, as the protection function on the software depends on the system's data services, do not use pirated security protection software. At this time you will use the security protection software will choose.
Goal Framework: (Software prevention against hacking and theft) 【Positivity】For security maintenance purposes, you are prompted to use security protection software to ensure stable system operation. If you use security protection software, you have a 60% chance of being protected from hacker attacks and theft. At this time you will use the security protection software will choose. 【Negativity】For security maintenance purposes, you are prompted to use security protection software to ensure stable system operation. If you use security protection software, there is a 40% possibility of hacking and theft. At this time you will use the security protection software will choose.
Risk Framework: (The probability of protection of the system by protection software 【Positivity】The security protection software of the information system may encounter 600 attacks in a year. To ensure the stable operation of the system, it is necessary to download and install the security protection software. The download and installation of the security protection software needs to be done on the system website. There are two options for you to choose from, please select the one you are most likely to follow. Option A: The security protection software protects the system from 400 attacks. Option B: The security protection software has a 2/3 probability of protecting the information system from attacks and a 1/3 probability of not protecting the information system from 600 attacks. 【Negativity】The security protection software of the information system may encounter 600 attacks in a year. To ensure the stable operation of the system, it is necessary to download and install the security protection software. The download and installation of the security protection software needs to be done on the system website. There are two options for you to choose from, please select the one you are most likely to follow. Option C: The security protection software will make the information system suffer from 200 attacks. Option D: There is a 2/3 probability that the security protection software will protect the information system from attacks and a 1/3 probability that the information system will be attacked 600 times.

Appendix B

Table A2. Situational experiment practice session stage flow and steps.

Attribute Framework Situational Experimentation Practice Session Flow
The exercise phase: The stimulus material for the exercise phase of the attribute framing experiment was Levin and Gaeth's (1998) purchase decision problem for different compositions of beef. In the positive attribute framework experimental exercise phase, the situation was described as follows: "Suppose you go to the supermarket to buy beef and the label indicates that 70% of this beef is lean meat. How willing are you to buy this beef?" Respondents responded by pressing a numbered key, ranging from 1 to 7 to indicate their willingness to purchase the meat, with 1 representing "definitely not" and 7 representing "definitely yes". The larger the number, the stronger the respondent's willingness to make the purchase. In the negative attribute framework experimental exercise phase, the situation was described as follows: "Suppose you go to the supermarket to buy beef and the label indicates that 30% of this beef is fatty meat. How willing are you to buy this beef?" Respondents responded by pressing a numbered key ranging from 1 to 7 to indicate their willingness to purchase the meat, with 1 representing "definitely not" and 7 representing "definitely yes". The larger the number, the stronger the respondent's willingness to make the purchase.
Goal Framework Situational Experimentation Practice Session Flow
The exercise phase: The purchase decision problem regarding beef of various compositions, as developed by Levin and Gaeth (1998), again served as the stimulus material for the goal framework experiment's exercise phase. The positive goal framework experimental exercise phase was described as follows: "Suppose you go to the supermarket to buy beef and the label indicates that 70% of this beef is lean meat. How likely would you be to buy this beef?" In the negative condition, the material was described as follows: "Suppose you go to the supermarket to buy beef and the label indicates that 30% of this beef is fatty meat. How likely would you be to buy this beef?" Subjects responded by pressing a key corresponding a number from 1 to 7 to indicate how likely they would be to purchase the meat, where 1 represents "definitely not" and 7 represents "definitely yes". The larger the number, the stronger the respondent's willingness to purchase the meat.
Risk Framework Situational Experimentation Practice Session Flow
The exercise phase: The stimulus material for the risk framework experiment exercise phase was Tversky and Kahneman's (1981) "Asian Disease" problem, regarding disease treatment options. The manner in which the material for the positive–negative risk framework experiment exercise phase was described varied depending on the specific nature of the problem. The material in the positive risk framework condition was described as follows: "Suppose a country is preparing to face a rare epidemic, the onset of which is expected to result in 600 possible deaths. Two responses are possible: Scenario Q, in which 200 people will survive, or Scenario P, in which there is a one in three chance that everyone will survive, but a two in three chance that no one will survive". The negative condition of the exercise phase is worded as follows: "Suppose a country is preparing to face a rare epidemic, the onset of which is expected to result in 600 possible deaths. Two responses options are possible: Scenario W, in which 400 people will die, or Scenario O, in which there is a one in three chance that no one will die, but a two in three chance that everyone will die."

References

1. Ali, R.F.; Dominic, P.; Ali, S.E.A.; Rehman, M.; Sohail, A. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Appl. Sci.* **2021**, *11*, 3383. [CrossRef]
2. Bornschein, R.; Schmidt, L.; Maier, E. The effect of consumers' perceived power and risk in digital information privacy: The example of cookie notices. *J. Public Policy Mark.* **2020**, *39*, 135–154. [CrossRef]
3. Tversky, A.; Kahneman, D. The framing of decisions and the psychology of choice. *Science* **1981**, *211*, 453–458. [CrossRef] [PubMed]
4. Levin, I.P.; Schneider, S.L.; Gaeth, G.J. All frames are not created equal: A typology and critical analysis of framing effects. *Organ. Behav. Hum. Decis. Process.* **1998**, *76*, 149–188. [CrossRef]
5. Wang, X.T. Self-framing of risky choice. *J. Behav. Decis. Mak.* **2004**, *17*, 1–16. [CrossRef]
6. Wang, X.T. Framing effects: Dynamics and task domains. *Organ. Behav. Hum. Decis. Process.* **1996**, *68*, 145–157. [CrossRef] [PubMed]
7. Levy, D.S.; Frethey-Bentham, C.; Cheung, W.K.S. Asymmetric framing effects and market familiarity: Experimental evidence from the real estate market. *J. Prop. Res.* **2020**, *37*, 85–104. [CrossRef]
8. Shan, L.; Diao, H.; Wu, L. Influence of the framing effect, anchoring effect, and knowledge on consumers' attitude and purchase intention of organic food. *Front. Psychol.* **2020**, *11*, 02022. [CrossRef]
9. Qu, H.; Daniel, J.L. Is "overhead" a tainted word? A survey experiment exploring framing effects of nonprofit overhead on donor decision. *Nonprofit Volunt. Sect. Q.* **2021**, *50*, 397–419. [CrossRef]
10. Zhang, B.; Ritchie, B.; Mair, J.; Driml, S. Can message framings influence air passengers' perceived credibility of aviation voluntary carbon offsetting messages? *J. Sustain. Tour.* **2019**, *27*, 1416–1437. [CrossRef]

11. Liu, P.; Fei, Q.; Liu, J.; Wang, J. Naming is framing: The framing effect of technology name on public attitude toward automated vehicles. *Public Underst. Sci.* **2021**, *30*, 691–707. [CrossRef] [PubMed]
12. Nuria, R.; van Bavel, R.; José, V.; Briggs, P. Framing effects on online security behavior. *Front. Psychol.* **2020**, *11*, 527886.
13. Wen, T.; Xi, Y.L.; Li, B.; Hu, L. Examining framing effect in travel package purchase: An application of double-entry mental accounting theory. *Ann. Tour. Res.* **2021**, *90*, 103265. [CrossRef]
14. Dixit, A.; Hall, K.D.; Dutta, S. Psychological influences on customer willingness to pay and choice in automated retail settings: Context effects, attribute framing, and perceptions of fairness. *Am. J. Bus.* **2014**, *29*, 237–260. [CrossRef]
15. Gasteiger, C.; Jones, A.S.; Kleinstäuber, M.; Lobo, M.; Horne, R.; Dalbeth, N.; Petrie, K.J. Effects of message framing on patients' perceptions and willingness to change to a biosimilar in a hypothetical drug switch. *Arthritis Care Res.* **2020**, *72*, 1323–1330. [CrossRef]
16. Meyerowitz, B.E.; Chaiken, S. The effect of message framing on breast self-examination attitudes, intentions, and behavior. *J. Personal. Soc. Psychol.* **1987**, *52*, 500–510. [CrossRef]
17. Yang, X.; Chen, S.C.; Zhang, L. Promoting sustainable development: A research on residents' green purchasing behavior from a perspective of the goal-framing theory. *Sustain. Dev.* **2020**, *28*, 1208–1219. [CrossRef]
18. Wang, L.; Guo, Z.; Zhang, G. Effective destination user-generated advertising: Matching effect between goal framing and self-esteem. *Tour. Manag.* **2022**, *92*, 104557. [CrossRef]
19. Tanford, S.; Choi, C.; Joe, S.J. The influence of pricing strategies on willingness to pay for accommodations: Anchoring, framing, and metric compatibility. *J. Travel Res.* **2019**, *58*, 932–944. [CrossRef]
20. Ceylan, M.; Hayran, C. Message framing effects on individuals' social distancing and helping behavior during the COVID-19 pandemic. *Front. Psychol.* **2021**, *12*, 579164. [CrossRef]
21. Degolia, A.H.; Hiroyasu, E.; Anderson, S.E. Economic losses or environmental gains? Framing effects on public support for environmental management. *PLoS ONE* **2019**, *14*, e0220320. [CrossRef] [PubMed]
22. Altay, S.; Mercier, H. Framing messages for vaccination supporters. *J. Exp. Psychol. Appl.* **2020**, *26*, 567. [CrossRef] [PubMed]
23. Fehrenbacher, D.D.; Wiener, M. The dual role of penalty: The effects of IT outsourcing contract framing on knowledge-sharing willingness and commitment. *Decis. Support Syst.* **2019**, *121*, 62–71. [CrossRef]
24. Channa, H.; Ricker Gilbert, J.; De Groote, H.; Bauchet, J. Willingness to pay for a new farm technology given risk preferences: Evidence from an experimental auction in Kenya. *Agric. Econ.* **2021**, *52*, 733–748. [CrossRef]
25. Li, M.; Wang, J.; Zhao, P.; Chen, K.; Wu, L. Factors affecting the willingness of agricultural green production from the perspective of farmers' perceptions. *Sci. Total Environ.* **2020**, *738*, 140289. [CrossRef] [PubMed]
26. Xu, S.; Wang, M.; Liu, Q.; Wang, C.; Zhang, C. Exploring the valence-framing effect: Gain frame enhances behavioral and brain sensitivity to the failure of decision-making under uncertainty. *Int. J. Psychophysiol.* **2020**, *153*, 166–172. [CrossRef]
27. Zhou, W.; Ning, N.; Zhou, Y.; Qiao, J.; Su, Y.; Zhang, X. Influence of framing effect on risk decision-making behavior of medical students in a university in Harbin under the emergency situation. *Med. Soc.* **2022**, *35*, 23–26.
28. Xu, H.; Li, M.; Peng, H. The influence of eye gaze cues on risk decision-making in the economic field: Based on the framing effect paradigm. *Psychol. Behav. Res.* **2022**, *20*, 37–44.
29. Chang, S.; Sun, Y. Influence of cognitive load and emotion on the risk decision frame effect of basketball players. *J. Tianjin Inst. Phys. Educ.* **2021**, *36*, 569–573.
30. Lin, J.; Chen, Y. The frame effect of college students' risk decision-making in different task areas. *J. Guizhou Norm. Univ.* **2019**, *35*, 44–51.
31. Zheng, M.; Chen, Y.; Chi, X. The influence of college students' disposable income on risk decision-making under the framework effect. *Bus. Econ.* **2018**, *36*, 175–179.
32. Ki-Aries, D.; Faily, S. Persona-centred information security awareness. *Comput. Secur.* **2017**, *70*, 663–674. [CrossRef]
33. Hadlington, L.; Popavac, M.; Janicke, H.; Yevseyeva, I.; Jones, K. Exploring the role of work identity and work locus of control in information security awareness. *Comput. Secur.* **2019**, *81*, 41–48. [CrossRef]
34. Hadlington, L.; Binder, J.; Stanulewicz, N. Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Comput. Hum. Behav.* **2021**, *114*, 106557. [CrossRef]
35. Jaeger, L.; Eckhardt, A. Eyes wide open: The role of situational information security awareness for security-related behaviour. *Inf. Syst. J.* **2020**, *3*, 429–472. [CrossRef]
36. Khando, K.; Shang, G.; Islam, S.M.; Salman, A. Enhancing employees information security awareness in private and public organisations: A systematic literature review-ScienceDirect. *Comput. Secur.* **2021**, *106*, 102267. [CrossRef]
37. van der Schyff, K.; Flowerday, S. Mediating effects of information security awareness. *Comput. Secur.* **2021**, *106*, 102313. [CrossRef]
38. Song, G. The new theory of conformity. *Psychol. Sci.* **2005**, *41*, 1174–1178.
39. Gurses, A.P.; Rosen, M.A.; Pronovost, P.J. Improving guideline compliance and healthcare safety using human factors engineering: The case of Ebola. *J. Patient Saf. Risk Manag.* **2018**, *23*, 251604351876283. [CrossRef]
40. Enwereuzor, I.K.; Adeyemi, B.A.; Onyishi, I.E. Trust in leader as a pathway between ethical leadership and safety compliance. *Leadersh. Health Serv.* **2020**, *33*, 201–219. [CrossRef]
41. Kilbane, H.; Oxtoby, C.; Tivers, M.S. Staff attitudes to and compliance with the use of a surgical safety checklist. *J. Small Anim. Pract.* **2020**, *61*, 332–337. [CrossRef] [PubMed]

42. Kühberger, A. The influence of framing on risky decisions: A meta-analysis. *Organ. Behav. Hum. Deci. Process* **1998**, *75*, 23–55. [CrossRef] [PubMed]
43. Chen, Y.; Wang, Y.; Feng, W. The discipline construction of security information cognition. *Sci. Technol. Manag. Res.* **2021**, *41*, 204–210.
44. Chen, H.; Li, W.; Ke, Y. Research progress on security behavior of organizational employee information system. *J. Inf. Syst.* **2016**, *9*, 118–134.