Article

Mindless Response or Mindful Interpretation: Examining the Effect of Message Influence on Phishing Susceptibility

Frank Kun-Yueh Chou [1,*], Abbott Po-Shun Chen [2] and Vincent Cheng-Lung Lo [3]

[1] Department of Accounting, College of Management, Fu Jen Catholic University, New Taipei 242062, Taiwan
[2] Department of Marketing and Logistics Management, College of Management, Chaoyang University of Technology, Taichung 413310, Taiwan; chprosen@gm.cyut.edu.tw
[3] Department of Information Management, School of Management, National Central University, Taoyuan 320317, Taiwan; s100483007@ncu.edu.tw
* Correspondence: 149224@mail.fju.edu.tw

Abstract: Influence-based deceptive messages constantly play a critical role in email phishing attacks. However, the literature lacks adequate understanding about how phishing messages with attractive and coercive influence result in the receivers' adverse consequences. We therefore take the perspective of mindless response and mindful interpretation to address this issue by examining comprehensive relationships among message influence, cognitive processing, and phishing susceptibility. To accomplish this, a survey approach was adopted after a simulated phishing attack was conducted in campuses. Our empirical evidence shows that both message influence and cognitive processing can lead to people being phished, and a combination of different influences can also trigger cognitive processing. This research makes contributions to the literature of information security, persuading influence, and cognitive psychology.

Keywords: phishing susceptibility; message influence; cognitive processing; smart power; mindlessness; mindfulness

Citation: Chou, F.K.-Y.; Chen, A.P.-S.; Lo, V.C.-L. Mindless Response or Mindful Interpretation: Examining the Effect of Message Influence on Phishing Susceptibility. *Sustainability* **2021**, *13*, 1651. https://doi.org/10.3390/su13041651

Academic Editor: Manuela Tvaronaviciene

Received: 7 November 2020
Accepted: 29 January 2021
Published: 4 February 2021

1. Introduction

People gradually rely on electronically mediated messages instead of paper-based ones as a daily information source. They receive notifications, advertisements, and event messages from emails and mobile phones everyday. However, these messages are easily forged and can be fraudulent. Unlike traditional messages, which are edited by an authoritative organization or a reliable media, the authenticity of online content is debatable. When people mistakenly believe in untrue content and take further actions, the consequences can be serious. In addition, COVID-19 escalates the threat from all three sides of the famed fraud triangle: pressure, opportunity, and rationalization [1]. It creates ideal conditions for fraud risk. Given the global pandemic of COVID-19, this disease continues to affect people's environments in countless ways, including travel bans, employees working remotely, and economic uncertainty [2]. In 2020, the Association of Certified Fraud Examiners (ACFE) polled more than 1800 anti-fraud professionals about ten types of fraud and found cyber fraud leading the way with 81% of respondents seeing an increase. When phishers combine two well-known cyber-fraud techniques, phishing emails and ransomware, to make people to mistakenly hit hyperlinks or open attachments in the phishing emails, ransomware can kidnap the computers that people rely on for important work, and both individuals and organizations may pay a painful price. Unfortunately, fraudulent emails can be found everyday in everyone's mailboxes. What makes the situation worse is that people have no idea whether those messages are genuine. As such widespread electronic fraud continues to create real crises, cyber governance acquires serious academic attentions.

Recently, fraudulent email phishing has been estimated to bring losses close to a half billion dollars in the USA [3]. A study indicates that 19% of individuals clicked phishing links in email messages, while 3% admitted to giving up financial or personal information [4]. In the meantime, Gartner Group reports that 3.3% of phishing-email receivers might lose money as a result [4]. Along with these pervasive phishing consequences, phishing attacks are frequently viewed as crimes ranging from identity and intellectual property theft to financial fraud, cyber espionage, and hacktivism [5]. Since 2007, phishing attacks have accounted for a third of cyber crimes [5]. A few evidences also augment people's fear about the phenomenon of cyber attacks. For example, the Pentagon receives 10 million cyber attacks each day, and most major banks, financial institutions, and media organizations report 50,000 cyber intrusions each day [6]. In addition, PhishTank, a phishing-tracing organization, also verified 31,850 unique phishing attacks during July 2012 [7]. Even in the highly regulated financial environment, Internal Revenue Service (IRS) likewise reported a 66% increase in attacks on U.S. taxpayers in one year, resulting in thousands of cases of identity theft [8]. In addition, Google reported that 9,500 websites are blacklisted daily because of phishing concerns [9]. These pessimistic figures would not even be the worst cases because phishing attacks constantly increase their sophistication with new techniques and strategies. This circumstance discourages information-security specialists as it makes anti-phishing work more difficult to be effective. When a phishing email can be sent to thousands of people at the same time, a 2–3% success rate of phishing can be financially costly [4]. A study by Gartner group reported that losses caused by phishing email have reached $1.2 billion in 2003 [4]. Apparently, evolutionary phishing attacks frequently defeat established cyber defenses and erode anti-phishing efforts. In sum, phishing attacks generate inevitable challenges to all three pillars of sustainability: social, economic, and environmental—also known as "people, profit, and planet" or the "triple bottom line" [10]. If the intent of sustainability is to pursue social harmony, economic development, and environmental protection, then the efforts to address phishing attacks can definitely increase people's mutual trust in society and encourage positive economic behaviors. At the same time, reliable information and communication technologies such as email systems can promote substantial social progress [11].

Given that phishing attacks are commonplace, many organizations rely on technical means of intervention, such as filtering out phishing messages, automating detection of fake websites, and deploying anti-phishing warning systems to combat phishing activities [8]. However, technical interventions cannot entirely remove the threat of phishing attacks [12]. A major reason is that phishers usually operate in legitimate communication channels, and it is difficult to distinguish their messages from genuine ones [13]. A prior study has shown that even with the effects of modern anti-phishing efforts, more than 11% of the users will read a spoofed message, click the link it contains, and enter their login information [14]. Therefore, some research streams instead focus more on central questions to address phishing issues, such as "what causes people to be deceived by phishing messages?" and "what motivates them to click on phishing links?" Extant research on phishing attack has suggested the cognitive effort made by message recipients as a key reason for individual victimization [4]. This is because phishing attacks tend to exploit human cognitive biases instead of technology loopholes [7]. In other words, people are the weakest link in the information-security system, and it is no longer sufficient to ensure the information security in organizations by merely using technical measures [15]. Given this circumstance, recent phishing studies pay greater attention to individuals' mindless and mindful cognitive behaviors. For the mindless cognitive behavior, some studies argue that communication media has the potential to convey deceptive messages and influence the outcomes. In this view, each influence technique has its ability to make an automatic, mindless compliance from people's long-established cognitions [8,16]. For the mindful cognitive behavior, a prior study also suggests that the most vigorous phishing messages would be those that can exploit individuals' mindful behaviors, especially referring to heuristic and systematic cognitive processing [7]. When heuristic cognitive processing relies on simple cues for judging fraudulent messages, systematic cognitive processing instead put an emphasis on individual deliberation to prevent phishing victimization.

Apart from the behaviors of cognition, other research streams have various foci to understand why people get phished. An early stream emphasizes message characteristics such as the source of the email, grammar, spelling, and email title. A later research stream considers the importance of individual characteristics like involvement, knowledge, and self-efficacy [4]. The rest of the research streams have diverse foci on antecedents of phishing victimization, such as experiential and dispositional factors [16], demographic differences [4], the severity of the phishing attack [17], and the pragmatic preparedness of practitioners [18]. In particular, interpersonal familiarity [8,19], event urgency [4,7,19–21], and personal relevance [4,19,22] are also frequently emphasized. Among various research streams, the cognitive concept of mindlessness and mindfulness has a more solid theoretical basis for illustrating the process by which people respond to or interpret received messages. People's cognitive behavior therefore plays a salient role in dealing with phishing issues. However, mindful cognitive behavior is merely one component about "interpretation" in the stimulus-interpretation-response (S-I-R) logic in comparison to the mindless cognitive behavior which serves as the underlying concept in the stimulus-response (S-R) logic. The very relevant antecedent of stimulus, i.e., message influence, still lacks adequate investigations in literature.

In the line of exploring antecedents of email phishing activity, Wright and Marett [16] ever-convincingly emphasize messages' potentials to deceive email receivers, but their study somehow lowers its priority and focuses on the exploration of experiential and dispositional factors. However, Wright et al. [8] have experimentally investigated whether six taxonomic message influences can increase the likelihood of receivers' vulnerability. Even so, the extant body of knowledge still does not know whether both attractive and coercive messages result in phishing susceptibility or invoke people's cognitive processing and associated consequences. This knowledge gap can undermine the belief for the logic of stimulus-response (S-R) and stimulus-interpretation-response (S-I-R). In addition, taxonomy is a less rigid classification because mutual exclusion and collective exhaustion are not guaranteed. A few taxonomic influence techniques may partially overlap each other. Instead, a typological classification of message influences, such as attractive and coercive influences, can effectively increase the credibility of research examination. In addition, some studies have long been curious about whether different types of influence interactions will produce useful effects [23,24]. Moreover, there are studies claiming that different types of cognitive-processing interactions can magnify the consequences of victimization [7,21]. Therefore, the lack of finer classification of message influences and the desire to bridge these knowledge gaps motivated this study to examine the comprehensive relationships among message influences, cognitive processing, and phishing susceptibility.

Specifically, this research attempts to answer the following questions: (1) whether distinct message influences can lead to phishing susceptibility, (2) whether both message influences and their interaction can invoke individuals' heuristic and systematic cognitive processing, and (3) whether distinct cognitive processing and their interaction can result in phishing susceptibility. Accordingly, our research will contribute the following to the literature: (1) a more theoretical conceptualization of message influence to provide a better basis for investigating phishing susceptibility, (2) a better illustration of how the stimulus-response (S-R) and stimulus-interpretation-response (S-I-R) logic deal with phishing issues, in terms of mindless/mindful cognitive behavior, and (3) unveiling the long-guessed interactive effects of typological concepts such as message influence and cognitive processing.

The remainder of this paper is arranged as follows: first, we illustrate the research framework, discuss the theoretical foundations, and develop associated hypotheses. Next, we introduce the methods for collecting and analyzing the data. After discussing the results and their implications, we conclude with the limitations of the research and suggest directions for future research.

2. Theoretical Foundations

The stimulus-response theory assumes that the intuitive response comes from repeated learning of experiencing stimulus. However, cognitive psychology believes that there is cognitive processing between stimulation and response. In other words, the individual's interpretation of the stimulated message could affect the behavioral response. People's behavioral response to a phishing email was originally seen as a stimulus-response process, but researchers have started to explore other possible processes, including whether different types of cognitive processing can raise or resist intuitive response of message stimulus, in order to better combat phishing attacks.

In general, special messages may bring new opportunities or threats to people. Such a situation means that the message has an ability to influence people. Thus, this ability has been conceptualized as message influence as playing the role of stimulus. In addition to both favorable and unfavorable messages having abilities to cause people's behavioral outcomes, they may invoke people's disparate cognitive processing in different ways, and in turn result in compliant behavior or a refused response. In order to adequately investigate whether different types of message influences produce idiosyncratic behavioral responses through disparate cognitive processing, this study proposes that both attractive and coercive influences can invoke cognitive interpretations, represented by heuristic cognitive processing and systematic cognitive processing, and therefore result in behavioral response. In other words, in addition to the stimulus-response (S-R) logic, the message stimulus, logically, can indirectly lead to behavioral responses through cognitive interpretations. To be in juxtaposition with this rival proposition in reality, we examine the S-I-R logic at the same time.

Though the S-R and S-I-R logic are remarkable, they can be understood by the salient concept of mindlessness and mindfulness because the above-mentioned logic is all about people's cognitive efforts. Langer [25] (p. 37) thought that people cling to constructed rules and categories in a mindless manner that psychologists call premature cognitive commitment. Such a cognitive commitment is a mindset formed before people have much of a reaction. A classic example of this is the story of the ugly duckling. When the ugly duckling came out of its egg, it made the first premature cognitive commitment: the largest and nearest duck was its mother. When it saw that it was different from its brothers and sisters, it made the second premature cognitive commitment: it was ugly. Likewise, people tend to rely on long-established cognitions and habitually make mindless behaviors. In other words, when people accept a single-minded explanation, they typically do not pay attention to information that runs counter to it [25] (p. 53). Truly, we can see this sort of "mindless response" everywhere in our daily life. Specifically, highly specific instructions or requests usually encourage mindlessness. By contrast, scholars recognize mindfulness as a process orientation. In the mindful process, we might pay more attention to our surroundings and openness to new information [25,26] in order to span our cognitive boundary or exert considerable cognitive efforts to search for meaning behind surface messages. In other words, that is the "mindful interpretation" process. Such a process may help us resist mental inertia and be alert to familiar language structure. For a better understanding about how people are phished, we used the mindlessness/mindfulness labels to clarify our study. We summarized our research idea and above-explanation into Figure 1 as our research framework.

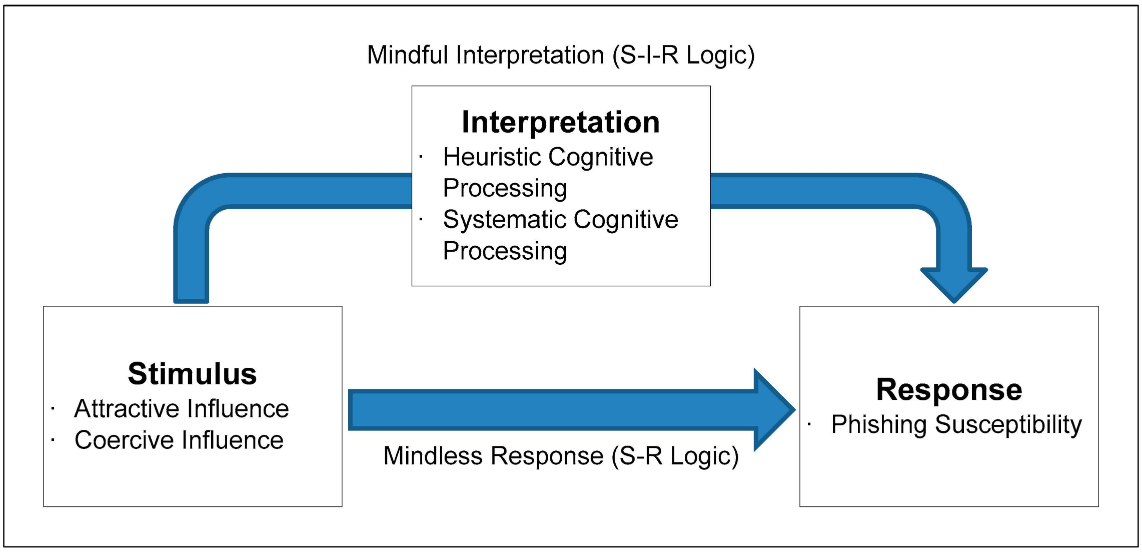
Mindful Interpretation (S-I-R Logic)
Interpretation
· Heuristic Cognitive Processing
· Systematic Cognitive Processing
Stimulus
· Attractive Influence
· Coercive Influence
Mindless Response (S-R Logic)
Response
· Phishing Susceptibility

Figure 1. Research framework.

2.1. Message Influence

Phishing email is all about messages. In fact, messages play the role of bait in the "phishing" metaphor. In general, phishing victimization cannot happen if they lack deceptive messages. Such messages usually mix true and false information to exert influence on targeted people. While message influence can be a better conceptualization in question, it is still required to analyze its types in order for anti-phishing efforts to be effective. Prior literature has clearly recognized coercive influence and non-coercive influence [27]. Coercive influence is the way to exert direct pressure through communicating adverse consequences of non-compliance. By contrast, non-coercive influence somehow makes people do something willingly. Aside from the above classifications, Frazier and Summers [28] also dichotomize it into perception influence and behavior influence. However, some researchers argue that perception influence perhaps is effective only if two parties have shared goals.

In addition to concise categories of influence, many studies instead focus on the taxonomy of six influences: information exchange, recommendation, request, promise, threat, and legalistic plea [29–31]. According to the studies of Lai [29] and Gelderman et al. [30], information-exchange influence means that someone may discuss general business issues and broad operating philosophies with the other, without making specific statements about what they want the other to do. Recommendation influence means that someone can predict greater profitability if the other follows the suggestions. Request influence is understood to be when someone simply states the actions they want the other to take, without any explanation. Promise influence is understood to be when someone promises to provide rewards if the other complies with these requests. Threat influence is considered to be when someone threatens a future penalty if there is no compliance with the request. Legalistic plea influence refers to when someone informs the other that the consequence of certain action is not permitted according to contracts or agreements. Based on the above understandings, coercive influence may include threats and promises [31] or contain threats and legalistic pleas [29]. Meanwhile, threats, promises, and legalistic pleas are also viewed as the kinds of behavior influence. Instead, non-coercive influence may include information exchange, recommendation, and request, while all or some of these influences can also be a kind of perception influence [29,31]. However, classifying these six strategies into more concise coercive and non-coercive influences, as well as behavior and perception influences, raises strong debate in the literature. For example, although a recommendation influence is generally viewed as a non-coercive influence, it is likely to experience a level of tension [29]. In addition, a request influence may plausibly influence both perceptions and behaviors. Moreover, a promise can play either a coercive or a non-coercive role, depending on its contingent nature.

Another set of taxonomic influences is proposed as liking, reciprocity, social proof, consistency, authority, and scarcity. According to Wright et al. [8], liking influence means that people always say yes to individuals they know and like [32]. In order to generate liking influence, a message sender must win the recipient's goodwill, trust, and friendship. A sender may do so through compliments [33] or similarities [34]. In addition, reciprocity influence takes advantage of people's tendency to repay an earlier favor. Social proof influence uses people's tendency to determine what is correct by finding out what other people think is correct [35]. Consistency influence takes advantage of individuals' desires to appear consistent in their words, beliefs, and actions [32]. For example, a phisher may send "reminders" to encourage individuals to perform a fake scheduled update of login information. Authority influence uses power such as job titles [36], appearance [37], and demeanor [38] to influence others. Scarcity influence takes advantage of individuals' tendency to feel that an object, event, or experience is more valuable when they perceive it as rare, inimitable, or available for a limited time.

Obviously, the above-mentioned two sets of taxonomic influences indeed increase academic understanding of influence. However, they are neither mutually exclusive nor exhaustive, and they may raise some problems on measurement. Instead, Nye [23] starts up from definition and terms the ability to influence others as power. Nye [24] distinguishes two types of power. He recognizes that soft-side power is the kind that exerts attractive influence to shape others' desires and hard-side power is the kind that exerts coercive influence to change others' behaviors. Therefore, this study adapts Nye's [24] concepts to design two constructs of message influence for illustrating the email phishing phenomena. First, attractive influence is the extent by which the email conveys information about the favorable consequences of taking the required actions. Instead, coercive influence is the extent by which the email conveys information about the unfavorable consequences of not taking the required actions. This study thinks these two constructs are adequate to represent message influences in phishing emails.

2.2. Cognitive Processing

Extant literature has attributed phishing susceptibility to human cognitive limitations and psychological manipulation of victims [21]. Regarding human cognitive issues, Kahneman [39] distinguishes a quick mode of cognitive processing from a slower mode of cognitive processing. The quick mode is rather automatic to detect simple relationships and to integrate information to maintain perceptions of our world. The slower mode is quite deliberate and associated with the subjective experiences. The first is like a machine using limited clues to jump to conclusions. The second instead allocates attention to mental activities and compares objects according to several attributes, follows complicated rules, and makes multiple choices.

Similarly, Petty and Cacciopo [40] also proposed the elaboration likelihood model (ELM) of persuasion. Elaboration is the process through which individuals make conscious connections between the cues they observe and their prior knowledge [41]. ELM identifies two cognitive-processing routes in persuasion: a peripheral path and a central path. The peripheral path is characterized by limited conscious attention that relies on cues and mental shortcuts that bypass counter-argumentation. Instead, the central path relies on rational analysis that involves elaborating on information and arguments. When people process information peripherally, they do not think carefully about the content of the message, but they are influenced by superficial factors surrounding the communication. Phishers often attempt to exploit peripheral paths to provoke action without deliberation.

These two types of cognitive processing may occur simultaneously, and some successful phishing attempts capitalize on both of them [21], termed as heuristic systematic-processing model (HSM) [42,43]. Heuristic cognitive processing refers to relying on judgmental rules and cognitive shortcuts. It is associated with rapid decisions that individuals often base on immediate judgment and are subject to cognitive biases. Instead, systematic cognitive processing involves carefully scrutinizing information and refers to analytically and comprehensively dealing with messages [21]. With heuristic cognitive processing, individuals use simple decision rules or cognitive heuristics triggered by adjunct cues in the context to reach judgments. With systematic cognitive processing, individuals make judgments by carefully examining the quality of arguments within the persuasive context [5]. A study has found that heuristic cognitive processing results in lower burdens on risk evaluations [44], and an emerging study has also connected such cognitive processing to the increased likelihood of deception on social media [45]. By contrast, systematic cognitive processing, due to its high scrutiny toward the content and need for comprehension, results in more reasoned and optimal decisions [5]. Luo et al. [7] suggest that the most effective phishing messages would be those that can operate on both the heuristic and systematic cognitive-processing activities. However, overwhelming research evidence points to individuals acting like cognitive misers, preferring economical over effortful information evaluation [46,47]. Consequently, heuristic processing tends to dominate cognitive information processing [5].

2.3. Phishing Susceptibility

When the focus of phishing research shifts from technical means to human factors, the impact of phishing activities is usually at the core of research questions. Most studies select relevant constructs surrounding the concept of “whether people get phished” as dependent variables, such as phishing vulnerability [4,8,21,48], phishing victimization [7,20,49], and phishing susceptibility [3,5]. Vulnerability may refer to the quality of being easily hurt or attacked. While victimization means the process of being victimized or becoming a victim, victimization can also be understood to be causing someone to be treated unfairly or in a bad position. Susceptibility can be considered to be the lack of ability to resist some extraneous agent. Whatever the phishing consequences are named, extant literature frequently locks itself in the myth of measurement with apparatus, resulting in designing dichotomous variables to count the numbers of phishing success or failure as their dependent variables.

If we look back at the earlier progress in information system (IS) discipline, the information system success (ISS) model can be enlightening in determining dependent variables. The salient work of DeLone and McLean [50] appeals to the quest for the dependent variable of IS success. No matter what kind of quality serves as the antecedents of information systems success, success itself can be the impact of individual or organizational use. The meaningful dependent variables are not limited to actual use or objective measurement through hardware monitors or counters. Instead, empirical, subjective measurements are suitable for research comparability. In a similar vein, the counts of phishing success can be translated into an equally meaningful continuous variable in terms of vulnerability, victimization, or susceptibility. Besides, there is no convincing rationale to support that phishing studies have to stick to experimental methodology to be viewed as legitimate. Thus, the less restricted concept “susceptibility” was chosen, and a continuous scale was designed to represent the behavioral consequence or individual impact of phishing activities in the cross-sectional investigation. Extant phishing studies still need well-designed measurements, as this research proposed, to provide trustworthy research validity in the process of investigating phishing issues.

Based on the above-explanation and conceptual discussion, we summarized the definitions of research constructs in Table 1 for clarity.

Table 1. Construct Definitions.

Research Construct	Definition
Attractive influence	The extent to which the email conveys information about the favorable consequences of taking the required actions.
Coercive influence	The extent to which the email conveys information about the unfavorable consequences of not taking the required actions.
Heuristic cognitive processing	The extent to which the individual uses simple rules to decide whether the email is credible.
Systematic cognitive processing	The extent to which the individual carefully thinks about or analyzes the email content to decide whether the email is credible.
Phishing susceptibility	The extent to which the individual believes deceptive emails.

3. Hypothesis Development

3.1. Message Influence and Phishing Susceptibility

When individuals keep their habitual patterns of email use, it can increase the possibility to be phished [19]. As we know, many individuals ritualistically check emails when they get up in the morning, when they end the day at night, or whenever they are able to conveniently use their email-readable devices [5]. Habits are automatic, non-conscious actions. They are also automatic patterns of response that follow fixed cognitive schemas, are triggered by environmental stimuli, and are performed without active consideration [4]. Habitual email use is particularly dangerous because habits once established persist with little further cognitive involvement [4]. Habits are also similar to routines. They are embedded within individuals' values and norms. Routines can easily entrap individuals into a fixed cognition trajectory that is inconsistent with a changing environment. Therefore, we argue that the email messages which individuals received, whether they contain attractive or coercive influences, are subject to individuals' long-established habits or routines, demonstrating the stimulus-response logic. Under such logic, individuals assume that the emails are normal as usual, problem-free, and secured. Therefore, they believe in the emails, follow their instructions, and suffer as a result. Consequently, this study proposes the following hypotheses:

Hypothesis 1 (H1). *Attractive influence is positively associated with phishing susceptibility.*

Hypothesis 2 (H2). *Coercive influence is positively associated with phishing susceptibility.*

3.2. Attractive Influence and Heuristic Cognitive Processing

Phishers can influence email recipients by providing attractive information, offers, or programs. For example, phishers may provide lottery information, prizes, job opportunities, relationship channels, etc., to attract email recipients to accept requests or click on links. They may also gain the willingness, trust, and friendship of email recipients by emphasizing personal similarities or by giving compliments [8]. For example, they may emphasize similarity in having a favorite basketball team to make email recipients like their persuasions [51]. Another example in commercial contexts is that potential customers may be more willing to buy insurance from salespeople who are similar in age, religion, politics, and smoking habits [51]. In addition to the use of similarity, praise can also intoxicate and disarm persons. In other words, positive remarks about a person's traits, attitude, or performance can generate a liking in return. However, the attraction in the message allows the recipients to allocate excessive attention to appreciate the people and things they like and to immerse themselves in the pleasant imagination and enjoy the feeling. This can make the message recipients tend to ignore things around themselves, refuse to interrupt the feeling of happiness, and devalue other negative clues. In the worst cases, this can also lead to affective intoxication or cognitive blindness. In general, a happy feeling can lower a person's alertness or decrease cognitive-processing intention. Thus, attractive messages make the recipients tend to use simpler rules or less cognitive resources, i.e., using heuristic cognitive processing, to judge the credibility of the messages. Thus, this study proposes the following hypothesis:

Hypothesis 3 (H3). *Attractive influence is positively associated with heuristic cognitive processing.*

3.3. Attractive Influence and Systematic Cognitive Processing

Attraction is not always good, and many times, it is fatal. Very attractive things can give people an unreal feeling, and people may even suspect whether traps exist, leading people to think about whether these things are credible. Perhaps it is the animal's instinct to be aware of the existence of traps. For wild animals, the hardest part in life is to get food. If too-easy-to-get foods show up in their living space, it will increase their alertness of trap. Humans are much the same case, too. Things that are strongly needed or desired but hard to get become very attractive. In this case, attractiveness is likely to contain traps. As the saying goes, "too good to be true" suggests that traps are not impossible. Something requiring no cost or anything charging too little usually suggests a trap. At an organizational level, discussions of various traps are also common in the literature. For example, the most favorable option for operational performance is to maximize the exploitation of organizational capability, but excessive exploitation may turn internal competences into core rigidities and create competence traps. Similarly, manufacturers' over-focus on the exploitation of core competence may also fall into the failure trap of weaker innovation capability or poorer adaptability for environmental change. Ahuja and Lampert [52] have observed that companies may fall into three traps: familiarity, maturity, and similarity. The familiarity trap overemphasizes existing knowledge without exploring new knowledge; the maturity trap comes from the need to rely on reliable and predictable outputs, but limits the exploration of new knowledge; and the proximity trap reflects the company's exploration of the closest areas to its expertise. Organizational literature often discusses companies that are unconsciously falling into a trap, but in the cyber world, people are often aware of the existence of certain traps. Thus, if an attractive message triggers people's alertness about traps, individuals often use their knowledge and experience to carefully analyze the content of the message. In other words, they use systematic cognitive processing to assess the credibility of the message. Thus, this study proposes the following hypothesis:

Hypothesis 4 (H4). *Attractive influence is positively associated with systematic cognitive processing.*

3.4. Coercive Influence and Heuristic Cognitive Processing

Coercive influence is to put pressure on the message recipients. When a person feels that the power of coercion is strong, they may feel threatened and quickly turn it into fear and may be overwhelmed by this feeling. With this fear, people cannot concentrate and cannot think carefully, so they use simple rules to make judgments. The 60 years of fear-appeal research [53] tells us that fear-arousing content could be persuasive for specific circumstances. When people are threatened, fear often dominates people's reactions. For example, it is common for people to receive an email notifying that an incorrect password will prevent them from accessing their own mailbox. The severity of this consequence could trigger message recipients' fear and make them ignore other opposite clues. Another example is that the US auto industry was devastated by the financial crisis in 2008, forming a recession caused by fear [54]. Perceived fear has been defined as an expectation of psychological, physical, or social harms on an individual or other people [48]. Therefore, the fear-arousing content is to make people feel fear by describing terrible things will happen to them if the suggested actions are not taken [55]. Workman [56] also argues that the phishers always create messages to reduce the amount of cognitive processing. In other words, coercive messages can cause fear, which shrinks our cognitive-processing ability. Thus, people use heuristic cognitive processing with less cognitive effort to judge the authenticity of emails. Thus, this study proposes the following hypothesis:

Hypothesis 5 (H5). *Coercive influence is positively associated with heuristic cognitive processing.*

3.5. Coercive Influence and Systematic Cognitive Processing

People do not like being coerced. Instead, they like to do something voluntarily. When people feel coerced, they recognize that the reality is highly inconsistent with their own assumptions and raise sentiments and resistance. Such a resistance is usually manifested by avoiding harm to their interest. Thus, people tend to deal with coercive messages by analyzing the content and finding out the possibility to avoid or reduce damage. Once the messages begin to be analyzed, the recipient of the messages thinks carefully about the source of this coercion, including the message senders' motivation, purpose, and the authenticity of the messages to justify their own assumptions about the real world. In other words, they activate systematic cognitive processing. In addition to self-interest logic, people sometimes believe that they have no need to change their behaviors as they are coerced. Workman [48] mentioned that if a threat is not believed, or is not serious, people will resist. Furthermore, individuals with higher perceived risk are more likely to have risk-averse behaviors [16]. Messages with coercive influence could increase these individuals' risk awareness, causing them generate excessive risk aversion. Therefore, they will try the most effective way to reduce the risk, i.e., carefully evaluate the credibility of messages. Consequently, this study proposes the following hypothesis:

Hypothesis 6 (H6). *Coercive influence is positively associated with systematic cognitive processing.*

3.6. Interactive Influence and Cognitive Processing

Although attraction or coercion have the chance to trigger individuals' cognitive processing, a single form of influence sometimes may not be strong enough to do this. Instead, when coercion is coupled with attraction, it acts with chemistry and thereby forms a particular influence that is more difficult to identify and reject. This weaved influence is as if one hand was guiding you and another hand was pushing you in an invisible way. As individuals are immersed in this atmosphere, they feel that the whole world is calling for them to take the proposed action. Therefore, individuals would have little concern about merely using simple rules in judging the credibility of the email message. Of course, when attraction and coercion are proceeded in an interactive way, blindly liking and irrational fear could also be amplified. In this situation, individuals are overwhelmed by these affects, so the simple rule is used to judge whether the email message is credible. This special form of influence is quite like the so-called "smart power" [23], referring to the integration of enticement and threat to achieve one's purpose. Thus, this study proposes the following hypothesis:

Hypothesis 7 (H7). *The interaction of attractive influence and coercive influence is positively associated with heuristic cognitive processing.*

Even though the combination of attraction and coercion can urge individuals to perform heuristic cognitive processing in order to save cognitive effort, it can also drive individuals to conduct systematic cognitive processing. Specifically speaking, when trap alertness that is rooted in strong attraction couples with a resistance that is caused by heavy coercion, it is likely to allow individuals to analyze the content of the message more carefully and to consider possible clues more thoroughly. That is to avoid catastrophic, irreparable consequences. An understandable example is a commercial advertisement that promotes a health supplement or slimming medicine to lose weight and to shape the body. It makes individuals who are unable to maintain their ideal body shape feel attracted but also forced, because they may have a high degree of trap alert and may be very resistant to take the risk of side effects. In other words, if the supplement or medicine is not effective, they might lose considerable money and have unpredictable harm to their bodies. Therefore, the proposals or options will be considered with deliberation when they combine attraction and coercion. Consequently, this study proposes the following hypothesis:

Hypothesis 8 (H8). *The interaction of attractive influence and coercive influence is positively associated with systematic cognitive processing.*

3.7. Heuristic Cognitive Processing and Phishing Susceptibility

Overwhelming research evidence points to individuals acting as cognitive misers, and thus heuristics tends to dominate cognitive processing [5]. In order to save mental resources, people prefer to make quick decisions based on learned rules and heuristics [22]. Some studies have found heuristic cognitive processing can result in lower risk evaluations and increase likelihood of deception [5]. Heuristic cognitive processing takes advantage of the factors embedded within or surrounding a message, called heuristic cues, such as message source, format, length, and subject matter for a quick assessment of message validity [7]. When decisions are thought to be complex or personal information processing is overloaded, some heuristics may make the decision process more manageable [19]. Williams et al. [19] identified three heuristics. The availability heuristic refers to previous exposure to a particular situation that makes the judgment biased. For example, lottery scams exploit recent media reports of lottery winners so that winning a lottery is perceived as more likely. The representativeness heuristic focuses on activating previous stereotypes, such as online romance scams that take advantage of special features and communication styles. The affect heuristic is the judgment based on emotional response rather than systematic consideration of various risks and benefits. However, using simple rules to determine whether the content of message is true or not will bring a higher risk of misjudgment, especially in a more open and uncertain electronic communication environment. When the risk of misjudgment becomes higher, people are more likely to be harmed by believing fake messages. In other words, when the message is deliberately forged, the risk of misjudgment becomes a real danger. Therefore, using simple rules to determine the credibility of a message increases the likelihood of being phished. Thus, this study proposes the following hypothesis:

Hypothesis 9 (H9). *Heuristic cognitive processing is positively associated with phishing susceptibility.*

3.8. Systematic Cognitive Processing and Phishing Susceptibility

It is widely believed that careful analysis and interpretation of the message can improve problem detection capabilities and discover the problems that are intentionally hidden. When people think that the content of message has concerns, they are consequently less likely to believe it in order to avoid being harmed. In other words, if messages are purposefully forged, people who try very hard to detect the hidden problem are less likely to be phished by these messages. Phishing messages are fraudulent communications that attempt to obtain sensitive information. Despite an older and low-technological type of cybercrime, phishing messages are still highly effective [49]. Phishing is also called social engineering, and it refers to manipulating or tricking individuals into certain actions [3]. To reduce the risk of individuals being deceived by phishing, individuals should improve their ability to detect problematic messages. Karumbaiah et al. [57] suggested two methods for this. First, people can set appropriate thresholds for known features in order to identify both suspicious links and clues of urgency. Second, they can carefully add new diagnostic features to improve detection. Systematic cognitive processing puts more effort, time, and cognitive resources on the establishment of diagnostic criteria and clue identification, which is expected to reduce the situation of individuals being deceived. Thus, this study proposes the following hypothesis:

Hypothesis 10 (H10). *Systematic cognitive processing is negatively associated with phishing susceptibility.*

3.9. Interactive Cognitive Processing and Phishing Susceptibility

The most dangerous phishing messages can be those weaving heuristic and systematic cognitive processing. Luo et al. [7] concur with this viewpoint by pointing out that such a weaved cognitive processing is the most effective phishing attack. Specifically speaking, successful phishing emails may allow the recipient to carefully examine the message, so that the two different types of cognitive processing get the same conclusion. In other words, heuristic cognitive processing can produce a preliminary impression first, and then systematic cognitive processing confirms it [21]. Because systematic cognitive processing is a careful analysis and deliberation of the message, the message recipient with this cognitive processing will think of the email as credible and be more convinced that his preliminary, simple judgment was correct. In this circumstance, if the message is fraudulent, the individual is easy to be phished. However, such a situation may also require some kind of supportive condition. On the one hand, individuals may have confirmation biases [39], and thereby phishing messages that combine heuristic and systematic cognitive processing tend to succeed. On the other hand, well-designed phishing messages which operate on both heuristic and systematic cognitive processing may also deceive individuals who are specifically targeted, such as CEOs and individuals with high net worth, even if they do not have confirmation biases. Thus, this study proposes following hypothesis:

Hypothesis 11 (H11). *The interaction of heuristic cognitive processing and systematic cognitive processing is positively associated with phishing susceptibility.*

4. Research Methodology

4.1. Research Design

This research was designed as a post-simulated survey. Specifically speaking, questionnaires were issued after simulated phishing attacks. The research targets were university students, and the research procedure was as follows: first, the researchers prepared the phishing emails (i.e., the stimulus material) to simulate phishing attacks and target student groups. The phishing email with attractive and coercive information is shown in Appendix A.

Next, the teachers who assisted the research sent the phishing emails to the students that took the teachers' courses. University students were chosen because they are particularly vulnerable to phishing attacks, as research evidence has pointed out. The subject of the phishing email is informing students to confirm their membership in the alumni association to help them find a job. The phishing email contained a fake hyperlink and a fake attachment about membership. Even if students clicked on the hyperlink or open the attachment, neither caused a real attack. Instead, they opened an anti-phishing educational document, which provided tips to avoid phishing traps and suggested actions that should be taken after being phished, and then invited the students to participate in a short survey in the next few days, in which the students would be asked about their perceptions of the phishing message. The anti-phishing educational document is shown in Appendix B.

Finally, the questionnaire was distributed accordingly. The distributing principle was consistent with the random method of statistical sampling, and cluster sampling was adopted. That is, a teaching course acts as a sampling cluster, as recommended by Cooper and Schindler [58]. The main reason for adopting this sampling method is that it is not easy to simulate phishing attacks in a real environment. If the simulation lacks proper arrangements, many controversies could occur after the simulated attacks conducted. Therefore, simulated attacks must be practically feasible. Therefore, the researchers in this study first looked for teachers who were willing to assist in distributing phishing emails and questionnaires. Then, the teachers treated all students who took their courses as survey targets, so that the chosen chance of each student was not zero.

4.2. Survey Administration

The post-simulated survey was administered after students had completed all assessment associated with the simulated phishing email. A total of 350 surveys were issued to students in 7 courses across two universities by four teachers during mid-April, 2018. Subsequently, 274 surveys were returned. Of which, 273 completed surveys were adequate for analysis, yielding an effective response rate of 78%. The survey given to each respondent included a cover letter explaining the purpose of the study. In order to make it easy for students to recall the recent simulated phishing attack, the original content of phishing email was listed again in the questionnaire, and the students were prompted to answer based on the actual situation when they read the letter in the first place. The characteristics of the respondent are depicted in Table 2. Among these characteristics, the percentage of female respondents is relatively high (male: 41%; female: 59%), and most of the respondents generally belong to the age of college students (18–21 years old: 76%). The year of web experience for most of the respondents is more than 3 years (90%), which shows that most people have sufficient web experience.

Table 2. Demographic characteristics of the respondents (n = 273).

Sample Statistics	Frequency	Percent
Gender		
Male	112	0.41
Female	161	0.59
Missing value	0	0.00
Age		
18–19	98	0.36
20–21	108	0.40
22–30	31	0.11
31–50	21	0.08
Above 50	2	0.01
Missing value	13	0.05
Year of web experience		
0–1	4	0.01
1–2	2	0.01
2–3	18	0.07
3–4	80	0.29
4–5	28	0.10
5–10	102	0.37
Above 10	37	0.14
Missing value	2	0.01
Total	273	1.00

For more useful insights into emphasizing risk management strategy [59], we tried to identify high-risk groups by combining these sample characteristics with specific research variable. Since the research variable “phishing susceptibility” belongs to five-point Likert scale, we viewed those samples with phishing susceptibility having an average score of 4 or higher as high-risk individuals. These samples aggregate 102 people in total and share an average score of 4.29. Next, we used these high-risk individuals as a basis and then analyzed each characteristic and their combinations to observe whether high-risk groups appear. The analysis results show that there are 43 high-risk males with an average score of 4.39 and 58 high-risk females with an average score of 4.21. Therefore, males are more inclined to believe in fraudulent messages than females and could be a higher-risk group. On the other hand, because the rest of the sample characteristics and various combinations of each characteristic divide the high-risk individuals into much smaller groups and the number of individuals in each group varies greatly, the average scores of these groups may be less meaningful for comparison, and it is not easy to assert which groups are high-risk ones.

In addition, non-response bias was assessed through the procedure recommended by Armstrong and Overton [60]. In this procedure, because the last group of respondents is considered to be the most likely to be similar to non-respondents, a comparison of the first and last quartile of respondents provided a test of response bias. No significant differences between the first and last quartile of all respondents were found in regards to key study variables (attractive influence, t = −1.450; coercive influence, t = −0.580; phishing susceptibility, t = −0.346). Accordingly, non-response bias may not be a serious concern in this study.

4.3. Measurement Development

All measures of this study were adapted from existing measures in the literature to match the research context. In this study, a five-point Likert scale was adopted, with anchors ranging from strongly disagree (1) to strongly agree (5), and all measurement items were reflective indicators of the research constructs. After compiling an English-language version of the questionnaire, the original questionnaire was translated into Chinese. The measurement items then were verified and refined for translation accuracy by two MIS professors and a senior doctoral student. The measurement items are provided in Appendix C.

4.4. Data Analysis

The data analysis utilized the two-step approach recommended by Anderson and Gerbing [61]. The first step involved the analysis of the measurement model, while the second step tested the structural relationships among the latent constructs. The aim of the two-step approach is to establish the reliability and validity of the measurements before assessing the structural relationships of the model. SmartPLS 2.0 M3 was used to assess both the measurement model and the structural model, because PLS places minimal restrictions on measurement scales, sample size, and residual distribution [62].

4.4.1. Measurement Model

The adequacy of the measurement model was evaluated on the principles of reliability, convergent validity, and discriminant validity. Reliability was examined via the composite reliability values. Table 3 shows that all such values are above 0.7, satisfying the commonly accepted threshold. The convergent validity of the scales was assessed via two criteria [63]: (1) all indicator loadings are significant and exceed 0.7, and (2) the average variance extracted (AVE) of each construct exceeds the variance caused by measurement error for that construct (i.e., AVE should exceed 0.5). As shown in Appendix D, all items exhibit a loading higher than 0.7 on their respective construct, and as shown in Table 3, all the AVEs range from 0.83 to 0.92, thus satisfying both criteria for convergent validity.

Table 3. Reliabilities and average variance extracted.

Constructs	Items	Composite Reliability	Mean (STD)	AVE	Adapted Scales
Attractive influence (AI)	4	0.95	2.60 (1.07)	0.92	Hausman and Johnston [31]
Coercive influence (CI)	4	0.93	2.26 (1.00)	0.89	Hausman and Johnston [31]
Heuristic cognitive processing (HCP)	3	0.87	3.55 (0.97)	0.83	Vishwanath et al. [5]
Systematic cognitive processing (SCP)	3	0.90	3.52 (0.95)	0.86	Vishwanath et al. [5]
Phishing susceptibility (PS)	5	0.93	2.81 (1.13)	0.85	Moody et al. [3]; Vishwanath et al. [5]

Discriminant validity was assessed using two criteria. First, the loading of each measurement item on its assigned construct needed to be larger than its loadings on all other constructs [64]. Second, the square root of the AVE of a construct must have been greater than the correlations between the construct and other constructs in the model [63]. As shown in Appendix D (cross loadings of measurement items) and Table 4, both criteria were clearly met, demonstrating sufficient discriminant validity of the scales.

Table 4. Correlation among constructs and the square root of the average variance extracted (AVE).

	AI	CI	HCP	SCP	PS
AI	0.92	0	0	0	0
CI	0.67	0.89	0	0	0
HCP	0.07	−0.03	0.83	0	0
SCP	0.15	0.07	0.55	0.86	0
PS	0.49	0.43	0.17	0.19	0.85

Common method variance (CMV) was addressed by following the guidelines of Podsakoff et al. [65] in order to accommodate for the single survey method. At the design stage, two professors from different universities reviewed the survey. Based on their comments, revisions were made, and common method variance was reduced by addressing item complexity and ambiguity. At the reporting stage, we told the respondents that the survey was anonymous and that no individual data would be disclosed at any time. We also subtly changed the display sequence of the constructs in the survey. Doing so has been shown to alleviate method effects substantially. In addition, we applied statistical techniques to address common method variance. We ran the Harman's single-factor test. In the test, an exploratory factor analysis (EFA) of all indicators generated four distinct unrotated factors with eigenvalues greater than 1.0, which accounted for 72.5% of the total variance. The first extracted factor explained 37.9% of the total variance, less than the 50% criterion. No one general factor accounted for the majority of the variance among the measures [65]. The statistical results suggested that common method variance was not a concern in our research design.

4.4.2. Structural Model

Based on our theoretical foundations and related arguments, we developed a model with linear and interactive effects. We examined the significant paths in the model to assess the explanatory capability for our research questions via PLS analysis. Figure 2 shows the results of structural path analysis (solid-line relationship: significant; dotted-line relationship: insignificant), and Table 5 summarizes the results of the hypotheses. Interactive terms were created with mean-centering disposition to ease the concern of multicollinearity. This model focused on our research propositions as well as looked for the largest possibility to get relevant explanations and therefore gave up exploring the relationships between some constructs that shared similar concepts but with different types. A number of paths, ranging from weak significance ($p < 0.1$) to extreme significance ($p < 0.001$), demonstrated the linear and interactive effects to fit our research questions adequately.

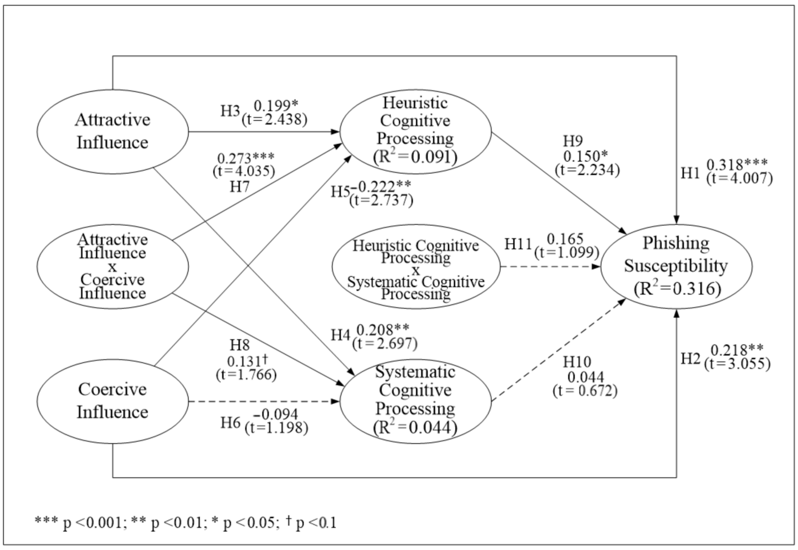
Attractive Influence
H3 0.199* (t=2.438)
Heuristic Cognitive Processing (R^2=0.091)
H9 0.150* (t=2.234)
H1 0.318*** (t=4.007)
0.273*** (t=4.035) H7
H5 −0.222** (t=2.737)
Attractive Influence x Coercive Influence
Heuristic Cognitive Processing x Systematic Cognitive Processing
H11 0.165 (t=1.099)
Phishing Susceptibility (R^2=0.316)
H4 0.208** (t=2.697)
H8 0.131† (t=1.766)
H10 0.044 (t= 0.672)
H2 0.218** (t=3.055)
Coercive Influence
Systematic Cognitive Processing (R^2=0.044)
H6 −0.094 (t=1.198)
*** p <0.001; ** p <0.01; * p < 0.05; † p <0.1

Figure 2. Results of PLS Analysis.

Table 5. Summary of Hypotheses and Results.

Hypotheses	Results
Hypothesis 1. *Attractive influence is positively associated with phishing susceptibility.*	Significant
Hypothesis 2. *Coercive influence is positively associated with phishing susceptibility.*	Significant
Hypothesis 3. *Attractive influence is positively associated with heuristic cognitive processing.*	Significant
Hypothesis 4. *Attractive influence is positively associated with systematic cognitive processing.*	Significant
Hypothesis 5. *Coercive influence is positively associated with heuristic cognitive processing.*	Significant (negative correlation)
Hypothesis 6. *Coercive influence is positively associated with systematic cognitive processing.*	Insignificant
Hypothesis 7. *The interaction of attractive influence and coercive influence is positively associated with heuristic cognitive processing.*	Significant
Hypothesis 8. *The interaction of attractive influence and coercive influence is positively associated with systematic cognitive processing.*	Significant
Hypothesis 9. *Heuristic cognitive processing is positively associated with phishing susceptibility.*	Significant
Hypothesis 10. *Systematic cognitive processing is negatively associated with phishing susceptibility.*	Insignificant
Hypothesis 11. *The interaction of heuristic cognitive processing and systematic cognitive processing is positively associated with phishing susceptibility.*	Insignificant

5. Discussion and Implication

5.1. Discussion of Results

We would like to center on the research questions to discuss the results of analysis. More specifically, we want to know (1) whether distinct message influences can lead to phishing susceptibility, (2) whether both message influences and their interaction can invoke individuals' heuristic and systematic cognitive processing, and (3) whether distinct types of cognitive processing and their interaction can result in phishing susceptibility. The results of the analysis show that the answers to these questions can be positive, as detailed below. First, all of the direct relationships between message influence and phishing susceptibility are fully supported by this study. The results of the analysis show that message influences have strong positive effects on phishing susceptibility (i.e., H1 and H2). This means that influential messages may result in people's acceptance of phishing messages with little cognitive effort by people's rigid cognitive schemas and long-established habitual behaviors. If researchers further wonder whether the interaction of the two influences would lead to phishing susceptibility, it is not supported with our extra test. In addition, if researchers are curious about whether heuristic cognitive processing impacts systematic cognitive processing as a few prior studies posited, the extra-tested relationship is positively significant but with a side effect of rendering the relationship between attractive influence and systematic cognitive processing insignificant. We did not show these relationships in the results in order to avoid the path diagram being overcomplicated.

Second, most of the direct relationships between distinct message influences and cognitive processing are very idiosyncratic and supported by this study. Specifically speaking, the relationship between attractive influence and heuristic cognitive processing, the relationship between attractive influence and systematic cognitive processing, and the relationship between coercive influence and heuristic cognitive processing are significant (i.e., H3, H4, and H5). The significant relationships between attractive influence and heuristic cognitive processing means that attractive influence can make people immerse themselves in good feelings and reduce cognitive efforts, causing them to use simple rules to judge the credibility of a message. In addition, the significant relationship between attractive influence and systematic cognitive processing means that attractive influence can also trigger people's alertness of traps and allow people to carefully analyze the content of message according to their knowledge and experience. Though attractive influence shows positive, significant relationships on both heuristic cognitive processing and systematic cognitive processing, coercive influence indicates a negative, significant relationship on heuristic cognitive processing, disobeying our original view. A reasonable explanation is that highly coercive message could bring a strong sense of immediate crisis and make people to give up using simple rules in judgment. Apart from the direct relationships, it is worth noting that the interaction of both influences has a very significant relationship on heuristic cognitive processing (i.e., H7) and a weak significant relationship on systematic cognitive processing (i.e., H8). This interaction means that the combined form of two influences can produce a quite special power, enabling people to not only use simple rules but also carefully analyze the content of message according to their knowledge and experience to judge the credibility of a message. When attractive influence shows all significant relationships on both types of cognitive processing, unlike coercive influence, we reasonably think that attractive influence is more likely to invoke both types of individuals' cognitive processing. Overall, the relationship between message influence and cognitive processing is not always as significant as expected but depends on the type of influence, the type of cognitive processing, and whether different influences are combined.

Third, the relationships between cognitive processing and phishing susceptibility are partially supported by this study. In these relationships, we can see that only heuristic cognitive processing has a significant effect on phishing susceptibility (i.e., H9). This effect means that people are more likely to be deceived when they use simple rules to judge the credibility of a message. However, systematic cognitive processing has no significant effect on phishing susceptibility, which shows that systematic cognitive processing may not be an effective approach to resist phishing attacks, thus requiring more future research. In addition, the results show no evidence to support the argument that the combination of heuristic and systematic cognitive processing is the most dangerous way to be phished, while past studies advocated it.

Lastly, let us discuss the results at a theoretical level. Given that the results fully support the viewpoint that message influence being able to directly result in phishing susceptibility, mindless response is supposed to always exist in phishing activities (i.e., H1 and H2). In addition, because the results only partially support the viewpoint that the message influence is able to result in phishing susceptibility through the receiver's cognitive processing (i.e., H3, H5, H7, and H9), mindful interpretation is speculated to not always appear in phishing activities. Since mindless responses seem to more easily result in phishing susceptibility than mindful interpretation, researchers should pay the most vigilant attention to mindless behaviors in order to minimize adverse consequences of phishing attacks.

5.2. Implications for Theory

This research is the first to devise the construct of message influence and to investigate its relationship with phishing susceptibility. In other words, our empirical evidence distinguishes the current research from previous descriptive or prescribing studies that were just inferred from some cases. In addition, because this research adopts the survey method incorporating continuous variables and causal hypotheses, in comparison to the paradigmatic experimental method with nominal variables and comparative hypotheses, it is more advantageous in improving scientific validity. Our research also contributes the following to the literature: (1) a more theoretical conceptualization of message influence to provide a better basis for investigating phishing susceptibility, (2) a better illustration of how the stimulus-response (S-R) and stimulus-interpretation-response (S-I-R) logic deal with phishing issues, in terms of mindless/mindful cognitive behavior, and (3) unveiling the guessed interactive effects of typological message influence. Apart from the above contributions, this research has following implications for theory. First, phishing is a semantic attack rather than a syntactic attack, which means that reading the embedded influence inside the message is at the core of addressing the phishing issues. Nevertheless, the understanding about influence in prior study is limited to taxonomy [8], known as a classification of data-driven form, with less help for theoretical building and theoretical testing [66]. Instead, this research uses typology, which belongs to a classification of theory-driven form, and can test theory by its very nature.

Second, this research confirms that message influence can be very powerful because it significantly causes unfavorable consequences, including directly and indirectly resulting in phishing susceptibility, as well as invokes heuristic cognitive processing with a special form of combining two influences. The result is consistent with decades of research that emphasize influential content being able to be effective in persuasion [8,53]. In addition, prior literature also debates which kind of influence is more effective, i.e., attractive [8] or coercive ones [3]. Our results show that attractive influence can be more effective in an email-phishing context. In addition, while the effect of combining different forms of influence is not clear in prior literature, we provide empirical evidence to confirm the effect of smart combination of different influences [23,24].

Third, this research confirms that people's cognitive processing can result in their responsive action. However, this confirmation includes an interesting part. That is, although prior studies consider that heuristic cognitive processing can promote unfavorable consequences and systematic cognitive processing can instead resist them [3,5,7,21,45], our results concur with the effect of heuristic cognitive processing but refute the effect of systematic cognitive processing. Thus, taking systematic cognitive processing to be a weapon in combating phishing attacks still needs more supportive evidence. In addition, this research also extends the understanding about mindlessness and mindfulness [25]. When this research takes cognitive processing as a mindful behavior and habitual response as a mindless behavior, we can see mindlessness is more powerful than mindfulness, because the desired mindful effects are not always significant, but adverse mindless effects are constant and strong. Thus, researchers should be more vigilant to mindless actions rather than purely looking forward to mindful effects.

Fourth, the meaning of success can be understood flexibly, including the success of phishing attacks. Success itself is not limited to the conception of "all or nothing." Any kind of success in nature can be understood to be "how successful it is." Thus, this research views the success of phishing attacks as an individual's phishing susceptibility and correspondingly defines it as the extent to which the individual believes deceptive emails, rather than the dichotomy of "being deceived or not being deceived." In this way, the consequence of phishing attacks can be flexibly measured and thereby advance future phishing researches. Researchers can learn similar concepts from information system (IS) success [50], enterprise resource planning (ERP) implementation success [67], or project success [68].

5.3. Implications for Practice

This research provides several implications for practice as follows: first, anti-phishing education and training should refocus on identifying the influence inside messages rather than the syntactic structure. Because current means of message detection cannot fully resist semantic attacks, information security practitioners should develop capability in addressing message influence and transfer knowledge about how to identify and deal with influential messages. Specifically speaking, it is insufficient to merely identify the technical characteristics of messages, such as source of email, grammar, spelling, email title, and so on. The education and training for combating phishing attacks still requires identifying complementary social characteristics. Among the social characteristics, human factors such as carelessness, optimism, and experiential reliance may be noteworthy because poor human factor design can contribute to many of the top computer security risks. In this research, we used the gender of the respondents as a basic social characteristic to identify males as a high-risk group for phishing susceptibility. That is, in a phishing setting with providing job opportunities, males are more inclined to believe in fraudulent messages than females. Such an insight could be useful for organizational information security managers and policy-makers.

Second, individuals should not rely too much on cognitive processing to deal with suspicious email messages. This is because cognitive processing still has its own biases. For example, the use of heuristic rules to judge suspicious messages for saving cognitive efforts can lead to adverse consequences, as confirmed by this research and past studies. In addition to using heuristic rules, individuals using deliberate methods to judge the authenticity of messages may also be affected by subjective confirmation biases; that is, they may use only their own subjective logic for cognitive processing and may also merely screen for interesting clues in the process of analyzing messages. Whether heuristic or thoughtful, people still have the chance to ignore well-established knowledge in the external environment or evidence that has been confirmed by objective third-party reports. Individuals should first use the more objective mechanisms available, such as calling the anti-fraud hotline, or using search engines such as Google to investigate whether the various people and things stated in the email messages really exist. If these more objective mechanisms are not available, then individuals can rely cautiously on cognitive processing. In this research, we provide similar recommendations in the anti-phishing educational document. That is, anyone who suspects that he/she has encountered cyber fraud can also report to the police station or credit/ATM card issuer. Information security managers can assist organizational members by providing anti-phishing guidelines and tips in classroom training or on hallway posters to prevent human's cognitive weakness.

Third, IT managers should not overemphasize absolute information security. Their attention should be shifted to information governance and individual's incentive alignment. That is, they should consider the individual's tradeoff for different types of value, such as the tradeoff between privacy and convenience. Many times, an individual will give up some privacy for convenience, which will have a sizable erosion on security. For example, an individual may voluntarily surrender some personal privacy in order to use a convenient mobile application. In addition, IT managers can strengthen environmental control rather than behavioral control. Environmental control refers to the overall technical architecture, such as the implementation of a digitally signed email. The reason for not recommending behavioral control is that the individuals' intuitive, habitual responses to incoming messages are too powerful to control. Thus, IT managers can collaborate with information security companies in trying to integrate the email server with the digital signature. In this way, the true identity of the email sender can be confirmed through the nature of non-repudiation in asymmetric encryption algorithm, and the email recipient will not mistakenly believe in the fraudulent emails.

5.4. Conclusions

The results of this research show that both mindless response and mindful interpretation can happen simultaneously in phishing context. Namely, the process between influence and consequence is not merely a proposition of alternative route. The influences of phishing messages not only cause the receivers' mindless responses but also conditionally trigger their mindful interpretations. In the case of mindless response, both attractive and coercive influence can result in phishing susceptibility. In the case of mindful interpretation, the attractive and coercive influence and their interaction can trigger heuristic cognitive processing, which in turn result in phishing susceptibility. While attractive influence is able to trigger systematic cognitive processing, systematic cognitive processing fails to result in phishing susceptibility. Thus, there is a special answer for the "mindless response or mindful interpretation" question. That is, both mindless response and mindful interpretation can illustrate how people get phished.

Although this research shows a large number of significant effects and supports our research idea, there are limitations. First, deceptive emails are not easy to simulate on a large scale because most environments are either discouraged or do not allow simulated deception. Second, measuring the subjective perception of the message receivers is subject to individual cognitive bias. Third, this research is conducted in a campus environment, so the external validity of the general working environment is limited. Fourth, this research did not investigate many other variables, such as risk alertness, self-efficacy, and experience, so it does not mean that various antecedents of cognitive processing and phishing susceptibility have been understood fully.

In addition, based on our research insights and both the academic and practical importance of phishing issues, we suggest the following directions for future research: first, the classification of influence is not limited to attractiveness and coerciveness. Researchers can explore more typologies. Second, influential communication media is not limited to email. Researchers can investigate the content of social media, online news, or messaging software. Third, it is interesting to cleverly combine different types of influence. Scholars have long been curious about whether the combination will be effective. Fourth, the idea of cognitive processing needs more research to support its positive and negative effects.

Author Contributions: Conceptualization, F.K.-Y.C., A.P.-S.C. and V.C.-L.L.; data curation, F.K.-Y.C., A.P.-S.C. and V.C.-L.L.; formal analysis, F.K.-Y.C.; funding acquisition, V.C.-L.L.; investigation, F.K.-Y.C., A.P.-S.C. and V.C.-L.L.; methodology, F.K.-Y.C., A.P.-S.C. and V.C.-L.L.; project administration, V.C.-L.L.; resources, V.C.-L.L.; software, V.C.-L.L.; supervision, V.C.-L.L.; validation, F.K.-Y.C., A.P.-S.C.; writing—original draft, F.K.-Y.C.; writing—review & editing, F.K.-Y.C., A.P.-S.C. and V.C.-L.L. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by the Ministry of Science and Technology (Taiwan), under the Grant No. MOST108-2410-H-030-089-MY2.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data will be available on request from corresponding author.

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

Appendix A

Box A1. Simulated Phishing Email.

Subject: Confirm membership in Alumni Association
Dear student,
Don't become a person without friends. Act now to confirm your membership in the Alumni Association.
The Alumni Association has created an account for you on its wide interpersonal network. This network offers internships in all areas, part-time jobs, and high-paying full-time jobs. Relying on your alumni network, your career development will be more advantageous.
You must confirm your account as soon as possible, otherwise your account will be deleted and you will regret in your future life.
Please click on the link below to confirm your personal information and retain your membership.
http://www.google.com.tw/AlumniAssociation/membership.htm
May you excellent at your studies, and good luck in everything.
System Administrator
Alumni Association Member Management Team

PDF
Alumni Association Membership.pdf

Appendix B

Box A2. Anti-Phishing Educational Document.

Dear student:
This is an email to test if you click on a phishing link (or open an attachment). This is a research test and does not harm your computer. But if this is a real phishing email, you may have been suffered. Our goal is simply to disclose the dangers of phishing email and remind you to avoid being the victims of identity thieves.
This research is completely anonymous, and we don't know your true identity. **We will invite you to participate in a short survey in which you will be asked about your perception of this phishing message.** First of all, we want to give you some tips to avoid being phished. Even if you decide not to participate in our survey, please pay attention to these tips:
1. Normal organizations (company) will not ask for your account number, password, verification method of security problems, or other sensitive information.
2. Even if the sender of the email looks like a normal organizations (company) with which you have transactions, the email may still be a phishing email in disguise. If you are suspicious of such an email, please do not reply and remember to ask the agency's customer service center first.
3. Be careful with the emails' warnings that mention about security loophole or account intrusion. If these emails ask you to provide detailed account information, they are phishing emails.
4. Please pay extra attention to the misspelled name in the email, such as "google" spelled "gogle", or "pchome" spelled "pch0me". This is a common feature of phishing emails.
However, if you get phished, phishers may be conducting credit/ATM card fraud, bank fraud, or identity theft. For such cases, you need to take the following steps:
1. About credit card/ATM card fraud
A. Report the stolen information to the credit/ATM card issuer and disable your current credit/ATM card.
B. Check your credit/ATM card account to see if there are any transactions you don't recognize.
C. Report to the credit/ATM card issuer that those transactions have not been authorized by you.
2. About bank fraud
A. Immediately inquire the financial institution and report your loss.
B. Disable your account and apply for a new account.
3. About identity theft
Apply for a credit report from the financial institution and see if anyone has applied for any false account by your name. If such a malicious activity is found, please take the following actions:
A. Call the anti-fraud hotline (direct dial 165) for help.
B. Report to the police station.
C. Ask the passport issuer if someone has applied for a passport by your name.
In order to help us improve the information security on campus, we kindly ask you to fill out a short anonymous questionnaire in the next few days to be the basis for our investigation of the perception about phishing risk. Thank you.

Appendix C Measurement Items

Attractive Influence (AI)

The email mentions that . . .

AI01 if I take the specific action, good things would happen to me.
AI02 if I value its suggestion for action, it brings extra favors.
AI03 if I pay serious attentions to its request, I will get an excellent opportunity.
AI04 if I comply with its instruction, I will get a privilege.

Coercive Influence (CI)

The email mentions that . . .

CI01 if I reject its suggestion, I will have a loss.
CI02 if I ignore its suggestion, it brings unfavorable consequence.
CI03 if I disregard its reminder, the prospection in my life will not be very good.
CI04 if I don't follow its instruction, I will lose some rights.

Heuristic Cognitive Processing (HCP)

HCP01 I rely on easy-to-judge clues in the email to consider my action.
HCP02 I use simple methods to judge whether the email is credible.
HCP03 I use the rule of thumb to evaluate the email's request.

Systematic Cognitive Processing (SCP)

SCP01 I connect the email's request with my knowledge about it to consider my action.
SCP02 Before I make my decision, I spent some time thinking about the email's request.
SCP03 I think about the action I will take by analyzing the email content.

Phishing Susceptibility (PS)

PS01 I click hyperlinks or open attachments in the email with little doubts.
PS02 When I read the email, I believe its source is reliable.
PS03 When I read the email, I believe its content is not a fake.
PS04 When I read the email, I believe it has no difference with normal emails.
PS05 When I read the email, I believe it would not bring unfavorable consequences with clicking hyperlinks or opening attachments.

Appendix D

Table A1. Cross Loadings of Measurement Items.

	AI	CI	HCP	SCP	ES
AI01	0.9043	0.5817	0.0912	0.1638	0.4213
AI02	0.9406	0.6143	0.0810	0.1354	0.4755
AI03	0.9254	0.6281	0.0890	0.1691	0.4677
AI04	0.9116	0.6705	0.0272	0.1180	0.4674
CI01	0.5553	0.8794	−0.0381	0.0982	0.3556
CI02	0.6087	0.8982	−0.0671	0.0270	0.3578
CI03	0.6395	0.9103	−0.0162	0.0634	0.4145
CI04	0.6083	0.8780	0.0002	0.0720	0.4021
HCP01	0.0732	−0.0560	0.8095	0.4682	0.1849
HCP02	0.0338	−0.0471	0.8544	0.4375	0.0933
HCP03	0.0875	0.0259	0.8334	0.4817	0.1560
SCP01	0.0613	−0.0010	0.5406	0.7923	0.0729
SCP02	0.1952	0.1145	0.4402	0.9077	0.2050
SCP03	0.1248	0.0477	0.5131	0.8985	0.1852
ES01	0.4238	0.3613	0.1546	0.1720	0.8745
ES02	0.4257	0.3825	0.1765	0.1951	0.9021
ES03	0.4397	0.3834	0.1957	0.2154	0.8669
ES04	0.3869	0.3164	0.1139	0.1305	0.8175
ES05	0.4533	0.3956	0.1075	0.1018	0.8198

References

1. Kelly, M. Fighting the New Fraud Risks of COVID-19. 2020. Available online: https://www.wegalvanize.com/fraud/fighting-new-fraud-risks-of-covid-19/ (accessed on 28 September 2020).
2. Association of Certified Fraud Examiners. Fraud in the Wake of COVID-19: Benchmarking Report. 2020. Available online: https://www.acfe.com/covidreport.aspx (accessed on 28 September 2020).
3. Moody, G.D.; Galletta, D.F.; Dunn, B.K. Which phish get caught? An exploratory study of individuals' susceptibility to phishing. *Eur. J. Inf. Syst.* **2017**, *26*, 564–584. [CrossRef]
4. Vishwanath, A.; Herath, T.; Chen, R.; Wang, J.; Rao, H.R. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decis. Support Syst.* **2011**, *51*, 576–586. [CrossRef]
5. Vishwanath, A.; Harrison, B.; Ng, Y.J. Suspicion, cognition, and automaticity model of phishing susceptibility. *Commun. Res.* **2018**, *45*, 1146–1166. [CrossRef]
6. Fung, J. How Many Cyber Attacks Hit the United States Last Year. 2013. Available online: http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-lastyear/ (accessed on 31 December 2017).
7. Luo, X.; Zhang, W.; Burd, S.; Seazzu, A. Investigating phishing victimization with the heuristic-systematic model: A theoretical framework and an exploration. *Comput. Secur.* **2013**, *38*, 28–38. [CrossRef]
8. Wright, R.T.; Matthew, L.J.; Thatcher, J.B.; Dinger, M.; Marett, K. Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Inf. Syst. Res.* **2014**, *25*, 385–400. [CrossRef]
9. Arachchilage, N.A.G.; Love, S. Security awareness of computer users: A phishing threat avoidance perspective. *Comput. Hum. Behav.* **2014**, *38*, 304–312. [CrossRef]
10. Kuhlman, T.; Farrington, J. What is sustainability. *Sustainability* **2010**, *2*, 3436–3448. [CrossRef]
11. De la Hoz-Rosales, B.; Camacho, J.; Tamayo, I. Effects of innovative entrepreneurship and the information society on social progress: An international analysis. *Entrep. Sustain. Issues* **2019**, *7*, 782–813. [CrossRef]
12. Abbasi, A.; Zahedi, F.; Chen, Y. Impact of anti-phishing tool performance on attack success rates. In Proceedings of the 2012 IEEE International Conference on Intelligence and Security Informatics, Arlington, VA, USA, 11–14 June 2012; pp. 12–17.
13. Dhamija, R.; Tygar, J.D.; Hearst, M. Why phishing works. In Proceedings of the Conference on Human Factors in Computing Systems, Montréal, QC, Canada, 22–27 April 2006; pp. 581–590.
14. Purkait, S. Phishing counter measures and their effectiveness—literature review. *Inf. Manag. Comput. Secur.* **2012**, *20*, 382–420. [CrossRef]
15. Stefaniuk, T. Training in shaping employee information security awareness. *Entrep. Sustain. Issues* **2020**, *7*, 1832–1846. [CrossRef]
16. Wright, R.T.; Marett, K. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *J. Manag. Inf. Syst.* **2010**, *27*, 273–303. [CrossRef]
17. Chen, X.; Bose, I.; Leung, A.C.M.; Guo, C. Assessing the severity of phishing attacks: A hybrid data mining approach. *Decis. Support Syst.* **2011**, *50*, 662–672. [CrossRef]
18. Bose, I.; Leung, A.C.M. Assessing anti-phishing preparedness: A study of online banks in Hong Kong. *Decis. Support Syst.* **2008**, *45*, 897–912. [CrossRef]
19. Williams, E.J.; Beardmore, A.; Joinson, A.N. Individual differences in susceptibility to online influence: A theoretical review. *Comput. Hum. Behav.* **2017**, *72*, 412–421. [CrossRef]
20. Harrison, B.; Svetieva, E.; Vishwanath, A. Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Inf. Rev.* **2016**, *40*, 265–281. [CrossRef]
21. Goel, S.; Williams, K.; Dincelli, E. Got phished? Internet security and human vulnerability. *J. Assoc. Inf. Syst.* **2017**, *18*, 22–44. [CrossRef]
22. West, R.; Mayhorn, C.; Hardee, J.; Mendel, J. The weakest link: A psychological perspective on why users make poor security decisions. In *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*; Gupta, M., Sharman, R., Eds.; Information Science Reference: Hershey, PA, USA, 2008; pp. 43–60.
23. Nye, J. *Soft Power: The Means to Success in World Politics*; PublicAffairs: New York, NY, USA, 2004.
24. Nye, J. Soft power. *Leadersh. Excell. Essent.* **2009**, *25*, 10. [CrossRef]
25. Langer, E.J. *Mindfulness*; Perseus Publishing: Cambridge, MA, USA, 1989.
26. Levinthal, D.; Rerup, C. Crossing an Apparent Chasm: Bridging Mindful and Less-Mindful Perspectives on Organizational Learning. *Organ. Sci.* **2006**, *17*, 502–513. [CrossRef]
27. Frazier, G.L.; Summers, J.O. Perceptions of interfirm power and its use within a franchise channel of distribution. *J. Mark. Res.* **1986**, *23*, 169–176. [CrossRef]
28. Frazier, G.L.; Summers, J.O. Inter-firm influence strategies and their application within distribution channels. *J. Mark.* **1984**, *48*, 43–55. [CrossRef]
29. Lai, C.S. The effects of influence strategies on dealer satisfaction and performance in Taiwan's motor industry. *Ind. Mark. Manag.* **2007**, *36*, 518–527. [CrossRef]
30. Gelderman, C.J.; Semeijn, J.; Zoete, R.D. The use of coercive influence strategies by dominant suppliers. *J. Purch. Supply Manag.* **2008**, *14*, 220–229. [CrossRef]
31. Hausman, A.; Johnston, W.J. The impact of coercive and non-coercive forms of influence on trust, commitment, and compliance in supply chains. *Ind. Mark. Manag.* **2010**, *39*, 519–526. [CrossRef]

32. Cialdini, R.B. *Influence: Science and Practice*, 5th ed.; Scott-Foresman: Glenview, IL, USA, 2009.
33. Howard, D.J.; Gengler, C.; Jain, A. What's in a name? A complimentary means of persuasion. *J. Consum. Res.* **1995**, *22*, 200–211. [CrossRef]
34. Burger, J.M.; Messian, N.; Patel, S.; Prado, A.D.; Anderson, C. What a coincidence! The effects of incidental similarity on compliance. *Personal. Soc. Psychol. Bull.* **2004**, *30*, 35–43. [CrossRef] [PubMed]
35. Cialdini, R.B.; Goldstein, N.J. Social influence: Compliance and conformity. *Annu. Rev. Psychol.* **2004**, *55*, 591–621. [CrossRef] [PubMed]
36. Castilla, E.J. Managerial influence in workplace inequality. *Am. Sociol. Rev.* **2011**, *76*, 667–694. [CrossRef]
37. Bushman, B. Perceived symbols of authority and their influence on compliance. *J. Appl. Soc. Psychol.* **1984**, *14*, 501–508. [CrossRef]
38. Ward, A.; Brenner, L. Accentuate the negative: The positive effects of negative acknowledgment. *Psychol. Sci.* **2006**, *17*, 959–965. [CrossRef]
39. Kahneman, D. *Thinking, Fast and Slow*; Farrar, Straus and Giroux: New York, NY, USA, 2011.
40. Petty, R.E.; Cacioppo, J.T. The elaboration likelihood model of persuasion. In *Advances in Experimental Social Psychology*; Berkowitz, L., Ed.; Academic Press: San Diego, CA, USA, 1986; Volume 19, pp. 123–205.
41. Perse, E.M. Audience selectivity and involvement in the newer media environment. *Commun. Res.* **1990**, *17*, 675–697. [CrossRef]
42. Chaiken, S. The heuristic model of persuasion. In *Social Influence: The Ontario Symposium*; Zanna, M.P., Olson, J.M., Herman, C.P., Eds.; Lawrance Erlbaum Associates: Hillsdale, NJ, USA, 1987; Volume 5, pp. 3–39.
43. Chen, S.; Chaiken, S. The heuristic-systematic model in its broader context. In *Dual-Process Theories in Social and Cognitive Psychology*; Chaiken, S., Trope, Y., Eds.; Guilford: New York, NY, USA, 1999; pp. 73–96.
44. Trumbo, C.W. Information processing and risk perception: An adaptation of the Heuristic-Systematic model. *J. Commun.* **2002**, *52*, 367–382. [CrossRef]
45. Vishwanath, A. Diffusion of deception in social media: Social contagion effects and its antecedents. *Inf. Syst. Front.* **2014**, *17*, 1353–1367. [CrossRef]
46. Sundar, S.S.; Knobloch-Westerwick, S.; Hastall, M.R. News cues: Information scent and cognitive heuristics. *J. Am. Soc. Inf. Sci. Technol.* **2007**, *58*, 366–378. [CrossRef]
47. Sundar, S.S. The MAIN model: A heuristic approach to understanding technology effects on credibility. In *Digital Media, Youth, and Credibility*; Metzger, M.J., Flanagin, A.J., Eds.; MIT Press: Boston, MA, USA, 2008; pp. 73–100.
48. Workman, M. Gaining access with social engineering: An empirical study of the threat. *Inf. Syst. Secur.* **2007**, *16*, 315–331. [CrossRef]
49. Graham, R.; Triplett, R. Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behav.* **2016**, *38*, 1371–1382. [CrossRef]
50. DeLone, W.H.; McLean, E.R. Information systems success: The quest for the dependent variable. *Inf. Syst. Success* **1992**, *3*, 60–95. [CrossRef]
51. Cialdini, R.B. Harnessing the science of persuasion. *Harv. Bus. Rev.* **2001**, *79*, 72–79.
52. Ahuja, G.; Lampert, C.M. Entrepreneurship in the large corporation: A longitudinal study of how established firms create breakthrough inventions. *Strateg. Manag. J.* **2001**, *22*, 521–544. [CrossRef]
53. Ruiter, R.A.C.; Kessels, L.T.E.; Peters, G.Y.; Kok, G. Sixty years of fear appeal research: Current state of the evidence. *Int. J. Psychol.* **2014**, *49*, 63–70. [CrossRef]
54. Ersek, B.; Keller, E.W.; Mullins, J. Break your industry's bottlenecks. *Harv. Bus. Rev.* **2015**, *93*, 98–105.
55. Johnston, A.C.; Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS Q.* **2010**, *34*, 549–566. [CrossRef]
56. Workman, M. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *J. Am. Soc. Inf. Sci. Technol.* **2008**, *59*, 662–674. [CrossRef]
57. Karumbaiah, S.; Wright, R.T.; Durcikova, A.; Jensen, M.L. Phishing Training: A Preliminary Look at the Effects of Different Types of Training. In Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy, Dublin, Ireland, 10 December 2016; Volume 11, pp. 1–10.
58. Cooper, D.R.; Schindler, P.S. *Business Research Methods*, 10th ed.; McGraw-Hill: New York, NY, USA, 2008.
59. Javaria, K.; Masood, O.; Garcia, F. Strategies to manage the risks faced by consumers in developing e-commerce. *Insights Reg. Dev.* **2020**, *2*, 774–783. [CrossRef]
60. Armstrong, J.S.; Overton, T.S. Estimating non-response bias in mail surveys. *J. Mark. Res.* **1997**, *14*, 396–402. [CrossRef]
61. Anderson, J.C.; Gerbing, D. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **1988**, *103*, 411–423. [CrossRef]
62. Chin, W.W.; Newsted, P.R. Structural equation modeling analysis with small samples using partial least squares. *Stat. Strateg. Small Sample Res.* **1999**, *2*, 307–342.
63. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
64. Chin, W.W. The partial least squares approach to structural equation modelling. In *Modern Methods for Business Research*; Marcoulides, W., Ed.; Lawrence Erlbaum: Mahway, NJ, USA, 1998.

65. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psychol.* **2003**, *88*, 879–903. [CrossRef]
66. Colquitt, J.A.; Zapata-Phelan, C.P. Trends in theory building and theory testing: A five-decade study of the Academy of Management Journal. *Acad. Manag. J.* **2007**, *50*, 1281–1303. [CrossRef]
67. Hong, K.K.; Kim, Y.G. The critical success factors for ERP implementation: An organizational fit perspective. *Inf. Manag.* **2002**, *40*, 25–40. [CrossRef]
68. Shao, J.; Muller, R.; Turner, J.R. Measure program success. *Proj. Manag. J.* **2012**, *43*, 37–49. [CrossRef]