Journal of the Association for Information Systems (2020) **21**(2), 428-459
doi: 10.17705/1jais.00607

RESEARCH ARTICLE

ISSN 1536-9323

Can Secure Behaviors Be Contagious? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions

Ali Vedadi[1], **Merrill Warkentin**[2]

[1]Middle Tennessee State University, ali.vedadi@mtsu.edu
[2]Mississippi State University, m.warkentin@msstate.edu

Abstract

IT users often make information security-related decisions in complex and multidimensional environments, which could lead to phenomena like behavioral anomalies. For instance, under uncertain circumstances, users may discount their own limited information about a security technology and make their adoption decisions based on what the majority of users' decisions are in this regard. In this context, imitation can become a legitimate and rational strategy for making security-related decisions. Current behavioral security theories generally assume that users possess sufficient information about security technologies before making security-related decisions. This theory assumption limits our understanding of how security decisions are made in various real-world circumstances. Our research is focused on security behaviors under *uncertain circumstances*. We investigate how providing popularity information can trigger herd behavior and can subsequently influence security behaviors. We also provide insights into security-related decisions that are influenced by herd mentality and investigate whether they persist over time. Additionally, we conceptualize and operationalize two constructs that can be used in future research to better examine post-adoption security behaviors. The findings of this multistage experiment show that in uncertain circumstances, when users are aware of the widespread use of a certain security technology, they develop a significantly higher intention to engage in protection-motivated behaviors. Furthermore, the results show that at the post-adoption stage, users rely more heavily on their own information about their continuous use of security technologies and put less emphasis on herd-related factors.

Keywords: Herd Behavior, Uncertainty, Bounded Rationality, Imitation, Information Security, Protection Motivation, Continuance Intention.

Richard Baskerville was the accepting senior editor. This research article was submitted on May 20, 2018, and underwent three revisions.

1 Introduction

Information system (IS) security incidents and issues, such as insider threats, insidious malware, and system penetration, are increasingly prevalent every year (Ponemon, 2017). According to the Online Trust Alliance's (OTA) latest report (2018), cyber incidents targeting businesses nearly doubled from 82,000 in 2016 to nearly 160,000 in 2017, thus making 2017 the worst year yet for data breaches and cybersecurity attacks. Similarly, individuals face threats to the security of their personal information in the form of hard-drive failure, malware, social engineering, etc. How do these individuals determine the best approach to protect their information assets?

The IS security literature suggests that to engage users in secure behavior, threats that inspire protection motivation must outweigh the maladaptive rewards earned by not engaging in protection motivation (Boss, et al., 2015, p. 843). Second, in the coping-appraisal stage, the users' response efficacy (the perception that a security technology/action can be useful in protecting

against security threats) must outweigh the response costs in order for them to engage in secure behavior and evaluate whether they can successfully use the technology for protection (Johnston & Warkentin, 2010; Johnston, Warkentin & Siponen, 2015). One of the most prevalent assumptions in prior IS security studies has been the certainty and vigilance of users regarding security technologies. For example, Johnston & Warkentin (2010) state that: "in an end user's contemplation of whether or not he or she will adopt [a security solution], he or she will consider the capabilities of the … solution and form a disposition … based on this appraisal" (p. 553). This appraisal is informed by perceptions of the technology's efficacy and usability. But what if a user's fear of a security threat is significantly high but there is also a high level of uncertainty about the capabilities and usability of the protective response? In uncertain circumstances, do users base their information security-related decisions on their limited personal assessments? In such circumstances, the sole reliance on the assumptions of current IS security theories may yield insufficient insight. We argue that to truly explain security decisions, one must seek a more nuanced theoretical understanding and empirical analysis than extant research has provided heretofore.

Imperfect information, which can lead to uncertainty, is a major phenomenon that can "bound" an individual's rationality (Simon, 1976). The term "bounded rationality" refers to situations in which the rationality of individuals in decision-making is usually limited by imperfect information, cognitive restrictions, and the amount of time available. Subsequently, the existence of uncertainty prevents the rational quantification of the probabilities of future events (Baddeley, 2011). In uncertain circumstances, herd mentality plays a highly influential role in predicting human behavior. According to herd theory, without a clear course to follow, it could be rational for an individual to observe the behavior of others, imitate what they do, and learn from the signals of others (Acemoglu, 1993; Wang, 2009; Wang, Li, & Rao, 2017). This phenomenon is particularly important and influential in the age of the internet. Because of the popularity of IT-related innovations, it has become easy to observe other users' decisions about technology acceptance or rejection.

In the context of security behavior, users may have to make security-related decisions in a complex and multidimensional environment. Thus, the reliance on behavioral security theories grounded in deliberative rational decision processes that do not consider phenomena such as decision-making in uncertain circumstances could limit our understanding and lead to conflicting results in the literature. In fact, it is reasonable to argue that the precision of the predictions and explanation of users' secure behavior could be improved if the circumstances under which they are likely to process potentially threatening information and make resulting decisions are carefully identified and controlled. Thus, our first research question is as follows:

RQ1: In uncertain circumstances, to what extent are users more likely to cope with security threats by engaging in herd behavior?

Furthermore, users must continue to engage in secure behaviors to maintain the security of their information (Warkentin, Johnston, et al., 2016). Users' beliefs, attitudes, and appraisals are not static because when users experience (directly or vicariously) a security threat (e.g., data loss, computer virus, etc.), they tend to engage in improved security hygiene, but often only for a limited time (Vedadi & Warkentin, 2018; Mutchler & Warkentin, 2020). Therefore, understanding the impact of imitation on secure behavior over time is crucial. Thus, our second research question is:

RQ2: To what extent does herd mentality influence users' post-adoption security behaviors?

This study contributes to the IS security literature by examining how obtaining popularity information about a security technology in uncertain circumstances can trigger herd mentality and subsequently affect security behaviors. We show that in such circumstances, users who receive popularity information may develop a higher level of protection motivation than those who do not. Another contribution of this study is that it provides insights into how security-related decisions that are influenced by herd mentality persist over time. Specifically, we examine whether and to what extent herd mentality and personal assessments influence users' continuance intention at the post-adoption stage.

In this regard, we also conceptualized and operationalized two constructs that could be used in future research to more accurately measure the antecedents of continuance intention at the post-adoption stage. We show that users may modify their beliefs about security technologies at the post-adoption stage (based on new information and actual experience with a security technology) and that the influence of these modified beliefs on continuance behavior may be different from their influence on initial security behaviors. Our findings show support for most of our hypotheses. In addition, our findings enhance our understanding of the contextual circumstances in which users make security-related decisions.

The rest of this paper is organized as follows. First, we briefly review the issue of bounded rationality in the IS security context and the role of high uncertainty in security-related decision-making. Next, we review the limited amount of literature on secure behavior continuance and the dynamics of herd behavior over

time. Based on these theoretical foundations, we develop our hypotheses and research model. Next, we describe our multistage experimental methods and their application to test the hypotheses. We then present our results. We conclude by discussing our findings and their theoretical and practical implications and then provide suggestions for future research.

2 Bounded Rationality in Security Behaviors

Bounded rationality occurs when the rationality of individual decision makers is limited by incomplete information, cognitive constraints, and/or time pressure. If individuals are boundedly rational, then the logical application of clear mathematical rules (e.g., utility maximization) is not possible because the existence of incalculable uncertainty prevents the quantification of the probabilities of future events (Simon, 1976). Conventional economic theories assume that individuals act as independent agents, but contemporary economic theories recognize that learning processes (e.g., social learning) are highly important when individuals are inclined to seek additional information before making decisions. Economics theorists have also proposed belief learning models that are focused on the processes through which individuals learn about the beliefs of their opponents (Baddeley, 2011).

Herd behavior, which is also known as observational learning, has received growing attention in the IS literature (Li & Hitt, 2008; Tucker & Zhang, 2011; Yoo, Jeon, & Han, 2016; Dewan, Ho, & Ramaprasad, 2017; Liu, Feng, & Liao, 2017; Wang, Zhang, & Hann, 2018). Without a clear path to follow, which leads to high uncertainty, it could be rational to follow the crowd, that is, engage in imitation-based behavior and learn from the signals in the behavior of others (Acemoglu, 1993). Similarly, it could be argued that when information is sparse, individuals will do what others are doing because they assume that it is the rational choice. Accordingly, rational agents may be incentivized to follow the herd based on perceptions of their own lack of knowledge. Therefore, herd behavior is rational when individuals have reason to believe that other people's judgments are based on better, more complete information than their own. Consequently, such individuals incorporate the behavior of others into their own set of prior information (Keynes, 1937).

The primary implication of these arguments for security behaviors is that if users' security-related behaviors are observed and identified, then other users will be highly likely to follow their lead. If the information about the adoption of the most effective IT safeguards by others is preeminent in the information provided, then this influence will encourage users to do what other users are doing, which could lead to the evolution of new social norms in making security-related decisions. Because decisions about security behaviors are made in complex and multidimensional environments, they could be based on contradictory goals (e.g., choosing a facile but ineffective safeguard versus a complex, yet highly effective safeguard). Therefore, relying solely on behavioral security theories that do not account for insightful phenomena, such as decision-making in highly uncertain circumstances, herd behavior and any other factor that bounds users' rationality can seriously limit the understanding of secure behaviors. The fact that the findings from many IS security behavior studies have not yielded consistent results is evidence of this shortcoming (Crossler et al., 2014). Hence, secure behavior could be better predicted and explained if the circumstances in which users were likely to process potentially threatening information and the potential responses were carefully identified and controlled. Furthermore, it is important to investigate the influence of the circumstances in which decisions are made (e.g., high uncertainty and herd behavior) on secure behavior over time. As mentioned earlier, the initial security-related reactions of IT users to security threats and secure behavior are important, but the real value of these behaviors is dependent upon their continuous and sustained practice. Therefore, in the following section, we review the fundamentals of herd behavior and its influence on decision-making over time.

3 Herd Behavior: Fundamentals and Dynamics

In a wide range of social situations, people base their decisions on the behavior of the people around them. For instance, we usually decide to try a new restaurant based on its apparent popularity (Banerjee, 1992). Keynes (1937) suggested that investors in asset markets often make decisions based on observational learning. Similarly, in a study on fertility choices, it was found that such decisions (e.g., how many children to have) were substantially influenced by observing what other people do in the same geographic area (Baddeley, 2011). This phenomenon, known as herd behavior, also occurs in other contexts, such as citizens' voting patterns, "hot" topics that researchers choose to investigate, online ratings, and crowdfunding (Bretschneider & Leimeister, 2017; Muchnik, Aral, & Taylor, 2013).

In Banerjee's (1992) model of herd behavior, agents capture all the returns generated by their choice so that there is no considerable distortion in incentives (Scharfstein & Stein, 1990). Herd behavior involves both one's own information and one's observations of the actions of others. In some cases, all people make the same choice, which is unrealistic because not everyone completely disregards their own information in imitating others. People tend to depend on a combination of their own information and their

observations of the behavior of others. Thus, herd behavior is "observed but is somewhat less widespread than is predicted by the respective theories, with agents following their own signals more than the theory predicts" (Hey & Morone, 2004, p. 639). It has also been shown that financial agents often trade on the differences between their own information and that which is publicly available (Avery & Zemsky, 1998).

At first glance, herd behavior may seem similar to the concept of social norms. Despite having some conceptual overlap, herd behavior is inherently different from subjective norms in several important ways.[1] First, these two concepts differ in terms of the source of information leading to the focal individual's actions, as pointed out by Sun (2013) and others. Subjective norms emanate from someone's reference group, consisting of those important to them—"important others," who are often a small group of known individuals, such as family members, co-workers, or close friends, whereas the herd (popularity information) are typically unknown strangers. People in one's reference group do not necessarily use the technology themselves, but they may express an opinion that reflects the social norm.

On the other hand, herd behavior usually has a much more extensive information source, often comprising many prior users or a large user base of strangers. In addition, in the herd behavior context, an individual follows those predecessors who have already adopted the behavior or technology (Sun, 2013). When it comes to subjective norms, individuals expect that their adoption decision may later be judged by the reference group. They care how the use of a certain technology will influence their image in their personal social circle (Moore & Benbasat, 1991). But in the case of herd behavior, an individual receives popularity information about the value of a technology and tries to avoid costs or blame related to a bad choice. Such individuals do not care about how the people they follow judge them for using a certain technology. In fact, the members of the large anonymous herd will not know about their choices. In addition, herd behavior and subjective norms are different in terms of how information is acquired. Herd behavior relies on "observation" of other people's behavior, whereas subjective norm usually hinges on messages received from significant others. (Triandis, 1980; Thompson, Higgins, & Howell, 1991).

In the IS context, herd behavior can be described as the phenomenon of users following other users in adopting a technology, even when their private information suggests doing something different. According to Rao, Greve, and Davis (2001), studies on herd behavior have focused on discrete decisions, such as whether to invest or not invest in a certain project or whether to adopt or to reject a technology. However, the decision to adopt or reject a technology typifies a situation that can lead to herd behavior. Duan, Gu, and Whinston (2009) found that internet users' choices of software significantly fluctuated when the total number of downloads changed, indicating that users were likely to follow the previous adopters' choices. They also found that users' reliance on the total of number downloads may lead to choosing inferior technologies. According to Sun (2013), users may consider including both the observations of others and their own perceptions in making a decision to adopt a technology. First, the actions of other people may be considered less relevant. The behavior of other users usually conveys information that could differ from one's own information. That many users have adopted a certain technology may signify that the technology is popular and useful. Furthermore, the user's own information specifies how this technology meets his or her own needs. Second, the current users of a technology may send mixed signals (e.g., adoption or rejection signals), indicating their contrasting perspectives regarding the technology, which may cause users to question the value of the technology and use their own information.

In this regard, to explain herd behavior in the context of technology adoption, Sun (2013) conceptualized and operationalized two new concepts: *discounting [one's] own information* (DOI) (i.e., the degree to which one disregards his or her own beliefs about a technology in making an adoption decision) and *imitation* (i.e., the degree to which one follows the previous adopters of a certain technology). Sun also elaborated the conditions under which herd behavior occurs in the context of technology adoption, the ways in which such behavior influences decisions to adopt a technology, and its effects on its post-adoption usage. The findings of his longitudinal study suggested that discounting personal beliefs and imitating others when adopting a new technology are triggered mainly through observing prior adoptions and perceptions of high uncertainty regarding the adoption of new technology. Inconsistent with the herd literature in finance and economics, Sun (2013) found that imitation decreased post-adoption regret and therefore was a legitimate strategy for choosing a satisficing technology that might not necessarily be optimal. In exhibiting adherence to herd behavior, users are inclined to adjust their personal beliefs, and they might readjust their originally discounted beliefs at the post-adoption stage (Sun, 2013).

[1] Contrast these two situations: In one case, your friends urge you to switch to a mapping app they like. In another case, you see ratings (popularity information) of mapping apps on a website.

In another study that focused on understanding herd behavior in the early adoption of novel technologies and the dynamics of this phenomenon, Walden and Browne (2009) examined a model of observational learning to explain decisions to adopt a technology by simulating users' behavior based on both their own information and the signals inferred by observing the behavior of others. One of their key findings was that IT herds that collectively select an effective technology are robust in the face of contrary information. Specifically, imitation does not necessarily help in adopting a technology that best fits the user's needs and exceeds his or her expectations. Therefore, when the users in a herd receive a signal that indicates the existence of a better technology, the herd itself may not necessarily collapse. This phenomenon is inconsistent with the finance and economics literature, which claims that herds are fragile and extremely sensitive to contrary information.

4 Research Model and Hypothesis Development

Based on the previous discussion of bounded rationality in behavioral security and the relevant theoretical foundations, we propose the research model depicted in Figure 1. Consistent with the IS security literature (Liang & Xue, 2010), it is expected that beliefs regarding the protective capability of a certain security technology will increase in strength because the user perceives that a related IT security threat is more probable. In other words, when users admit that they are susceptible to an IT security threat, they are likely to engage in using a protective technology that is deemed effective. Furthermore, because a security threat is perceived to be severe and avoidable, a user will be more likely to adopt this IT security solution to address the threat. Finally, moderate to high levels of perceived response efficacy increase protection motivation with regard to the threat against which a security technology is targeted. Users will evaluate the capabilities of such a technology and form a disposition toward it (Boss et al., 2015; Johnston & Warkentin, 2010; Johnston, Warkentin & Siponen, 2015; Liang & Xue, 2010). Based on these arguments, we argue that:

H1: Perceptions of threat susceptibility positively influence perceptions of response efficacy.

H2: Perceptions of threat severity positively influence perceptions of response efficacy.

H3: Response efficacy positively influences the intention to use the information security solution.

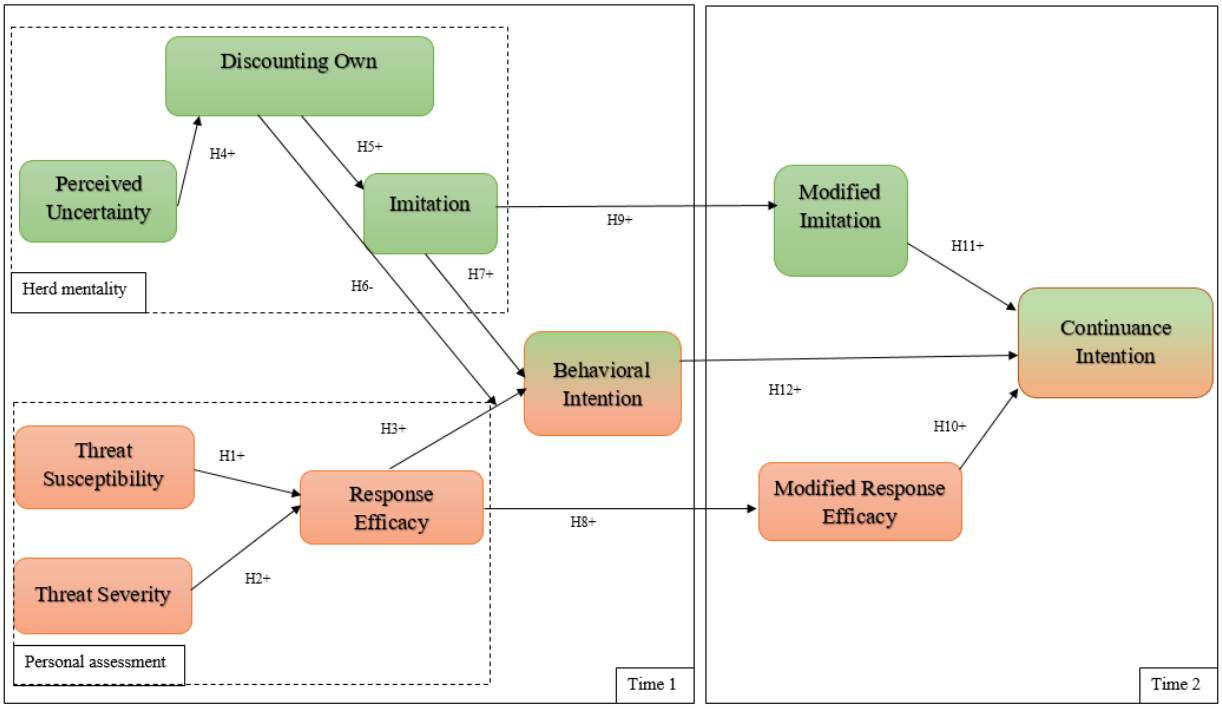


Figure 1. The Proposed Research Model

In highly uncertain circumstances, users are less likely to adequately assess and understand the relationship between their adoption and the outcomes of that adoption. This response inhibits the accurate evaluation of the efficacy of a potential security software. Therefore, it is a legitimate strategy for users to follow other users' decisions and, subsequently, to discount their limited information and beliefs, which they deem inadequate in making an effective adoption decision (Banerjee, 1992).

Furthermore, when users discount their own information, they rely less on their initial information and beliefs than on the insights obtained from their observations of others' behavior. Logically, the more a user discounts his or her own information, the more likely he or she will be to imitate the behavior of others (Banerjee, 1992). Discounting one's own information can increase the likelihood of users' imitating the actions of others instead of making a decision based solely on their own information/beliefs because as one reduces the use of one's own information and opinions, where else is there to turn except to the actions of others? In circumstances in which a user discounts his or her own opinion, a reasonable strategy is to imitate the actions of others (Au & Kaufmann, 2003; Thies et al. 2016). We argue that uncertainty alone does not necessarily lead to imitation because in some cases, the level of uncertainty can be too high, thereby paralyzing the decision-making process. Additionally, being uncertain, without being aware of the herd direction (i.e., receiving no popularity information), users might simply prefer the status quo, regardless of their strong perceptions of an information security threat. The nonsignificant relationship between perceived uncertainty and imitation, as empirically demonstrated by Sun (2013), confirms this claim. Therefore, we argue that in uncertain circumstances, imitation becomes an authentic alternative strategy based on discounting one's own information because users may believe that others have better and more complete information regarding that security technology. Thus, we propose the following hypotheses:

H4: Uncertainty about using a security technology is positively associated with users' discounting their own information.

H5: Discounting one's own information increases the tendency of users to imitate the behavior of other users.

According to herd theory, discounting one's own information means that users rely less on their own beliefs in making technology adoption decisions. Thus, it is reasonable to argue that the more that users discount their own information, the less important that personal beliefs are in making decisions, demonstrating a weak anchoring effect of beliefs (Sun, 2013). Therefore, discounting one's own information can negatively moderate the relationship between perceived response efficacy and adoption of a security technology. Therefore, we hypothesize that:

H6: Discounting one's own information negatively moderates the relationship between response efficacy and behavioral intention to engage in protection-motivated behaviors.

In the finance and economics literature, there is sufficient evidence that many investors mimic the investment decisions of other investment managers to avoid being considered incompetent in the case of a poor return on investment (Scharfstein & Stein, 1990). Generally, individuals may prefer the odds of being wrong along with everybody else to the risk of providing an atypical prediction that is the only incorrect forecast (Graham, 1999). Similarly, in the information security context, the act of imitation indicates that even when a security technology that is adopted by a herd is inefficient, this situation is more acceptable than the circumstance in which a user is the only one who makes the wrong decision not to adopt an efficient IT security technology and then suffers reputational damage. Additionally, the issues of information asymmetry and information imperfection are pervasive in the IS context (Liu et al., 2017). Decision makers might make judgments about the value of an emerging technology based on their own information. For example, it has been found that a large number of positive reviews for an app encourages further adoption (Keith et al., 2016). Therefore, we hypothesize the following:

H7: Imitating others is positively associated with a user's intention to use an information security solution to protect against a security threat.

Drawing on expectation-disconfirmation theory (EDT) (Bhattacherjee, 2001) and the cognition change model (CCM) (Bhattacherjee & Premkumar, 2004), we argue that post-adoptive modified beliefs—that is, the degree to which one perceives that a security technology is useful at the post-adoption stage—are formed based on the initial beliefs at the adoptive stage. Through a belief-updating mechanism, a user updates personal beliefs based on both old beliefs and new information about a security technology (Kim & Malhotra, 2005). Early beliefs can be selectively stored in long-term memory and thus can also have distal effects on modified beliefs (Kim, 2009). Therefore, it is reasonable to argue that users update their perceptions of response efficacy at the post-adoption stage when they have gained experience in using a specific security technology. Imitation-based mentality can also be modified at the post-adoption stage. Based on evidence in the IS literature (Edelen, Ince, & Kadlec, 2016; Sun, 2013), this mentality can positively influence users' continuance intention, as the literature

shows that IT herds tend to be robust over time (Walden & Browne, 2009). Thus, we hypothesize that:

H8: Response efficacy beliefs at the pre-adoption stage are positively associated with modified response efficacy beliefs at the post-adoption stage.

H9: Imitation at the pre-adoption stage is positively associated with modified imitation at the post-adoption stage.

Moderate to high levels of perceived response efficacy may lead to increased protection motivation. Users tend to evaluate the efficacy of a technology and form perceptions about it. In the CCM, users' perceptions change over time as they gain firsthand experience with an IT, which may cause them to change their subsequent IT usage behavior (Bhattacherjee & Premkumar, 2004). Therefore, it is likely that users' perceptions of response efficacy will significantly influence their continuance intention. Hence,

H10: Modified response efficacy is positively associated with continuance intention.

As previously discussed, in the IS context, the tendency to imitate other users in uncertain circumstances can influence users' adoption of security technologies. Herd theory posits that one of the primary drivers of herd behavior in uncertain circumstances is that a user (manager) follows the decisions of others because she or he does not want to be blamed for being the only one who did not adopt a certain innovation. Therefore, blame sharing could be a major reason for herd behavior (Scharfstein & Stein, 1990). Conversely, users may imitate each other's decisions in adopting so-called "best practices" for information security management because they think others have superior information about the alternatives or because they want to maintain competitive parity and limit rivalry (Von Solms & Von Solms, 2004; Lieberman & Asaba, 2006).

Building on the existing literature on herd behavior in the IS context (Sun, 2013; Walden & Browne, 2009), which suggests that IT herds are usually robust and resilient to contrary information, we can argue that herd mentality may positively influence the continuance intention at the post-adoption stage. Therefore, we hypothesize that:

H11: Modified imitation is positively related to continuance intention.

The findings of previous IS research support the direct relationship between intention to use in the adoption stage and continuance intention at the post-adoption stage (Kim, 2009; Kim & Malhotra, 2005). This relationship is based on the sequential updating mechanism in which users form subsequent intentions with respect to the previous intentions that are stored in their long-term memories. These intentions can be recalled to serve as the input for subsequent intentions (Kim, 2009). Thus, it is reasonable to assume that the intention to use in the initial adoption stage can be a distal influence on the continuance intention at the post-adoption stage. Therefore, we hypothesize that:

H12: Intention to use an information security solution at the pre-adoption stage is positively associated with post-adoption continuance intention.

5 Research Method

We used a two-group experimental design by randomly assigning each participant to either the control group or the treatment group. The participants were recruited from two professional survey panels. A password manager was chosen as the security technology because there is a high degree of uncertainty among IT users about these technologies in terms of response efficacy. Previously, we had asked more than 100 business undergraduate and graduate students at a public university in the US whether they had ever used a password manager. Fewer than 2% said they had previously used or experienced using a password manager. In addition, a survey published by *PC Magazine* (Rubenking, 2015) showed that few people had used a password manager and that most users still employed traditional password management techniques. Therefore, we determined this IT artifact to be a good fit in the context our study. To ensure that each study subject had high uncertainty about the target security technology, only internet users with no or limited familiarity with password managers were qualified to participate in the first stage of the experiment.

During the first stage, after reading a narrative, the participants answered items related to herd behavior and intention to engage in protection-motivated behaviors. After the completion of this phase, we invited our participants to use the password manager, Dashlane, for one week and tell us their opinions about this technology. Subsequently, the subjects in both groups who used Dashlane were qualified to participate in the second stage of the experiment. Our invitation language was designed to reduce the bias toward using Dashlane for a reward. Specifically, we asked the participants (who successfully completed the first phase) to come back and tell us what they thought about using this password manager. For the second phase, we used recruitment language that basically revolved around the participants' "opinions" about Dashlane, rather than on the confounding factor that they could only participate in the second phase if they intended to continue using Dashlane. Later in our study, we found enough variance in the continuance intention construct to indicate that the monetary reward did not influence participants in expressing their true continuance intentions.

Table 1. The Experimental Design

Condition	Stage 1			Stage 2 (1 week later) (both groups)
	Pre-treatment measures (both groups)	**Treatment**	**Post-treatment measures (both groups)**	
Control group	1. Qualifying question (no prior experience with password managers) 2. Demographic information	No	1. Manipulation check 2. Behavioral intention 3. Herd behavior items 4. PMT items	1. Modified beliefs 2. Modified imitation 3. Continuance intention
Treatment group	1. Qualifying question (no prior experience with password managers) 2. Demographic information	Yes (providing facts about the widespread use and popularity of Dashlane, to trigger herd mentality).		

The responses collected from subjects who did not participate in the second stage of the experiment were discarded. The constructs were measured using a 7-point Likert scale and semantic differential scales (see Appendix A). Table 1 describes the experimental design used in the pilot and primary investigations, which are discussed below.

5.1 The Treatment

The following is the structure of the narrative that the treatment group received (see Appendix B):

- The first paragraph discussed the threats of traditional password management to capture the subjects' threat appraisal.
- The second paragraph briefly discussed the need for a password management tool and presented Dashlane as an example to capture the subjects' coping appraisal.
- The third section included a list of herd-related factors (also known as popularity information) regarding the widespread use of Dashlane. Prior research has used this treatment to trigger herd mentality in users (e.g., Tucker & Zhang, 2011; Dewan et al. 2017; Wang et al. 2018).

The subjects in the control group received only the first two paragraphs but received no information about the popularity and widespread use of the password manager Dashlane.

The narrative was discussed and refined in consultation with an expert panel team. The panel was convened to provide additional ideas and insights that would allow for the refinement of the narrative and the experimental instrument. The panel included six faculty members and IS doctoral students who were knowledgeable about research instrument design and the protection motivation literature, having conducted several similar experimental studies involving the measures used in this research. Subsequently, the full narrative was reviewed by several potential (nonacademic) subjects to ensure its clarity and cohesiveness.

5.2 Manipulation Checks

We also used two manipulation checks in this study. The first manipulation check was provided to our subjects immediately after they read the narrative to ensure that they had paid attention to the content (*What was the name of the password manager that was discussed in the previous page*?). Only subjects who chose Dashlane among other options were allowed to participate in the rest of the experiment. The second manipulation check was used to determine whether the subjects' perceptions of the independent variable in each group were manipulated in the intended manner and to ensure that the experimental treatment was indeed effective. In other words, this manipulation check was conducted to determine whether the experimental manipulation was effective in providing strong evidence for inferring causality, thus proving that the level of the treatment was sufficiently different across groups (Marett, 2015). The second manipulation check we used was: *Dashlane seems to be a widely used password manager* (7-point Likert scale, agree/disagree).

5.3 Software Usage Validation

Because we had no affiliation with the Dashlane Corporation, we were not able to directly observe our subjects' use of the Dashlane password manager. Therefore, we took several measures to increase the likelihood of obtaining truthful responses from the subjects by ascertaining that they had used Dashlane in the one-week interval between the Stage 1 instrument and the Stage 2 instrument. First, at the beginning of the survey conducted in Stage 2, we provided the subjects with the names of nine password managers. We then asked the subjects to choose the one that they were asked to use during the one-week interval. (See Appendix C.) Any subject who chose the wrong answer or chose Dashlane in their second or third

attempt was automatically disqualified to participate in the rest of the survey. In the next step in the screening process, we asked subjects to "certify" whether they had used Dashlane during the week. Those who chose "no" were disqualified from participating in the rest of the survey. Fortunately, only a few subjects failed these two validation checks. Although this method of validating the subjects' use of the software was not perfect, the results ensured our confidence in the quality of the data.

6 Initial Analysis

Prior to the main data collection, we conducted a pilot study to test item reliability, factor loadings, and the manipulation check by using SPSS v23. In the pilot study, in Stage 1, we collected 103 usable responses from Amazon Mechanical Turk (mTurk) workers (53 in the control group; 50 in the treatment group; average age 34 years; 43 female and 60 male respondents). We ran three tests before collecting the data for Stage 2. First, we tested the manipulation check item. The results of the independent *t*-test showed a significant difference between the two groups in terms of their understanding of the popularity of Dashlane ($t(101) = -2.831$, $p < 0.01$). Next, we conducted Cronbach's reliability test. The results showed that all values were greater than 0.8, which indicated high item reliability. We also ran a principal component analysis (varimax rotation). The results showed that items significantly loaded on their corresponding factors with minimal cross-loading (see Appendix D). After one week, we managed to collect only 37 usable responses for use in Stage 2. High attrition rate is one of the most common challenges in multistage data collections. The sample size was too small to conduct a principal component analysis of Stage 2 constructs, so we ran a Cronbach's reliability analysis. All values were above 0.9, indicating high reliability (see Appendix D). The manipulation was effective, the item loadings were significant, and reliability was confirmed. Therefore, we proceeded to the main study.

7 Main Analysis

In the main stage of the data collection, we first collected 158 usable responses from mTurk Masters who had demonstrated excellence across a wide range of studies in which they had participated. They had been awarded the Masters qualification based on the high reliability of their responses. A usable response refers to data obtained from a respondent who successfully participated in both phases of the study and passed all the data quality checks (e.g., attention check, speed-check). Because the sample size was insufficient to conduct a robust confirmatory factor analysis and a structural analysis, we collected 56 usable responses from a Qualtrics professional panel and obtained a total of 214 usable responses (107 in the control group and 107 in the treatment group; average age 39 years; 89 female and 125 male respondents). Because we collected data from two different sources (Amazon Mechanical Turk Masters and the Qualtrics panel), we needed to conduct measurement invariance tests before pooling the data obtained from these sources. Therefore, we conducted configural and metric invariance tests. Configural invariance is established when the unconstrained model has good fit (Ellis et al., 2008). The model showed a good fit: χ^2/df was under 3 (1.63), CFI and IFI were equal or greater than 0.90, and RMSEA was less than 0.07 (0.05). Additionally, metric invariance is established when the measurement weights χ^2 statistic is not significant (Steenkamp & Baumgartner, 1998). The results of a chi-square difference test indicated metric invariance between the groups ($df = 30$; $\chi^2 = 38.47$; $p = 0.138$). Thus, we pooled the data from both sources and proceeded with the analysis. The descriptive statistics, such as average means and standard deviations, are provided in Appendix E.

7.1 Measurement Reliability and Validity

We conducted a confirmatory factor analysis using AMOS v24. This analysis included the assessment of factor loadings, model fit, construct reliability, convergent validity, discriminant validity, and the test for common method bias. The factor loadings were significant (above 0.7), and the model fit statistics were above the minimum acceptable levels (Chin & Todd, 1995), which indicated that the model fit the data ($\chi^2/df = 1.66$, CFI = 0.95, IFI = 0.95, RMSEA = 0.05). Table 2 shows the factor loadings.

All constructs had acceptable levels of reliability (≥ 0.70) (MacKenzie, Podsakoff, & Podsakoff, 2011). The initial reliability scores were obtained through reliability analysis in which composite reliability (CR) was computed. Next, the convergent and discriminant validity of the measures were assessed by a confirmatory factor analysis using AMOS v24. Convergent validity is demonstrated when the items in the same construct are significantly correlated. Furthermore, item loadings greater than 0.70 and an average variance extracted (AVE) above 0.50 indicate convergent validity (Straub, Boudreau, & Gefen, 2004). All items were loaded significantly on their corresponding construct (> 0.70). Additionally, all constructs had an AVE greater than 0.50. Therefore, the results indicate convergent validity. Discriminant validity is present when the items in a construct do not significantly correlate with the items in another construct. Discriminant validity is confirmed by calculating the square root of AVEs and comparing them against the correlation measures of other constructs. The square root of AVEs was greater than interconstruct correlations; therefore, the results indicated discriminant validity (Straub et al. 2004). Table 3 shows the composite reliabilities and AVEs, as well as the square roots of AVEs (in bold) and their correlations:

Table 2. Factor Loadings

Construct	Item	Loading
Threat susceptibility (TSUS)	TSUS1	.72
	TSUS2	.75
	TSUS3	.86
Threat severity (TSEV)	TSEV1	.88
	TSEV2	.79
	TSEV3	.93
Response efficacy (RE)	RE1	.87
	RE2	.89
	RE3	.76
Perceived uncertainty (UNC)	UNC1	.80
	UNC2	.76
	UNC3	.83
	UNC4	.77
Discounting own information (DOI)	DOI1	.86
	DOI2	.85
	DOI3	.69
Imitation (IMI)	IMI1	.90
	IMI2	.91
	IMI3	.89
Switching costs (SW)	SW1	.76
	SW2	.85
	SW3	.86
Modified response efficacy (ModRE)	ModRE1	.94
	ModRE2	.89
	ModRE3	.91
Continuance intention (CONT)	CONT1	.95
	CONT2	.95
	CONT3	.98
Modified imitation (ModIMI)	ModIMI1	.87
	ModIMI2	.93
	ModIMI3	.92
Behavioral intention (BI) to engage in protection-motivated behaviors	B1	.93
	B2	.93
	B3	.96
	B4	.96

Table 3. Reliability, Validity, the Square Roots of AVEs (in Bold), and Correlations

Construct (CR; AVE)	BI	TSUS	TSEV	RE	UNC	DOI	IMI	SW	Mod RE	CONT	Mod IMI
BI (0.97;0.90)	**.95**										
TSUS (.82;.61)	.38	**.78**									
TSEV (.90;.76)	.18	.49	**.87**								
RE (.88;.71)	.61	.45	.39	**.84**							
UNC (.87;.62)	-.31	-.00	.02	-.36	**.79**						
DOI (.85;.65)	.03	.11	-.09	-.23	.62	**.81**					
IMI (.93;.81)	.68	.38	.15	.56	-.18	.21	**.90**				
SW (.86;.68)	.11	.21	.04	.06	.21	.22	.22	**.82**			
ModRE (.93;.83)	.46	.16	.11	.33	-.11	.10	.39	.15	**.91**		
CONT (.97;.92)	.41	.18	.11	.31	-.02	.14	.41	.25	.85	**.96**	
ModIMI (.93;.83)	.48	.25	.10	.23	.09	.33	.53	.36	.62	.67	**.91**

Table 4. The Chi-Square Difference Test

Prior to dropping items				After dropping items			
Without CLF		With CLF		Without CLF		With CLF	
χ^2	df	χ^2	df	χ^2	df	χ^2	df
1260	782	1230	781	857.4	587	853.8	586

7.2 Common Method Bias

We tried to reduce the common method bias using procedural and statistical methods (Podsakoff et al., 2003). Specifically, we used several procedural remedies, such as the temporal separation of construct measurement, ensuring the anonymity of the participants, item randomization, and attention checks. Additionally, before testing the structural model and hypotheses, we used the common latent factor (CLF) method as a post hoc statistical procedure, which is highly effective in detecting common method bias (Schwarz et al., 2017). If a systematic bias due to the method is present, the CLF will be found to have a relationship with every scale item. The variance of the unmeasured latent method factor is set to 1 and the regression weights for all relationships to this variable are constrained equally. In this study, a confirmatory factor analysis was performed with and without a common method factor to determine the presence of common method bias. The results of the chi-square analysis showed a significant difference (> 3.84). To determine the items that caused the significant bias, we ran the measurement model 43 times, which was the number of items in the model. We compared the chi-square differences between the models with and without the CLF. Five items (TSEV2, DOI3, BI3, SAT4, and UNC2) accounted for the significant difference between the chi-square values. After these items were eliminated in order to reduce the common method bias, the chi-square difference between the two models was insignificant (χ^2 difference = 3.6, df difference = 1), which is shown in Table 4.

Table 5. Path Estimates

Relationship	Control group			Treatment group		
	Std. estimate	*t*-value	*p*-value	Std. estimate	*t*-value	*p*-value
H1: TSUS → RE	.35	2.93	.003**	.31	2.58	.01*
H2: TSEV → RE	.21	1.91	.056 (n.s)	.29	2.51	.01*
H3: RE → BI	.37	4.18	***	.38	4.53	***
H4: UNC → DOI	.77	8.25	***	.34	3.14	.002**
H5: DOI → IMI	.09	.90	.36 (n.s)	.26	2.22	.02*
H6: DOI moderating effect	-.20	-2.82	.005**	-.32	-6.37	***
H7: IMI → BI	.51	5.77	***	.63	8.01	***
H8: RE → ModRE	.37	3.69	***	.32	3.04	002**
H9: IMI → ModIMI	.59	6.56	***	.51	5.28	***
H10: ModRE → CONT	.77	12.65	***	.78	10.97	***
H11: ModIMI → CONT	.36	5.91	***	.24	3.50	***
H12: BI → CONT	-.01	-.17	.85 (n.s)	-.02	-.39	.69 (n.s)
Control: Age → CONT	.10	1.67	.093(n.s)	.10	.21	.833(n.s)
Control: Gender → CONT	.06	1.07	.283(n.s)	.05	.20	.376(n.s)
Control: SW → CONT	.06	1.49	.13 (n.s)	.11	1.77	.07 (n.s)

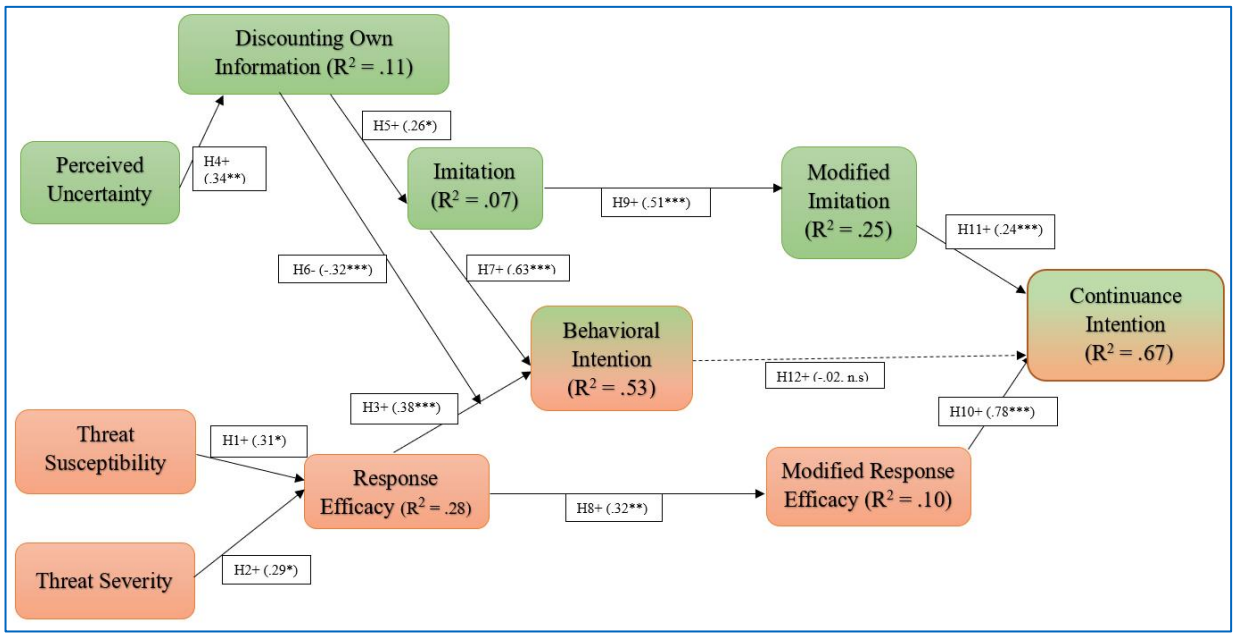
Notes: n.s = nonsignificant, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

Table 6. Hypotheses Testing Results

Hypothesis	Supported?
H1: Perceptions of threat susceptibility positively influence perceptions of response efficacy.	Yes
H2: Perceptions of threat severity positively influence perceptions of response efficacy.	Yes
H3: Response efficacy positively influences the intention to use the information security solution.	Yes
H4: Uncertainty about using a security technology is positively associated with users' discounting their own information.	Yes
H5: Discounting one's own information increases the tendency of users to imitate the behavior of other users.	Yes
H6: Discounting one's own information negatively moderates the relationship between response efficacy and behavioral intention to engage in protection-motivated behaviors.	Yes
H7: Imitating others is positively associated with a user's intention to use the information security solution to protect against a security threat.	Yes
H8: Response efficacy beliefs at the pre-adoption stage are positively associated with modified response efficacy beliefs at the post-adoption stage.	Yes
H9: Imitation at the pre-adoption stage is positively associated with modified imitation at the post-adoption stage.	Yes
H10. Modified response efficacy is positively associated with continuance intention.	Yes
H11: Modified imitation is positively related to continuance intention.	Yes
H12: Intention to use an information security solution at the pre-adoption stage is positively associated with post-adoption continuance intention.	No

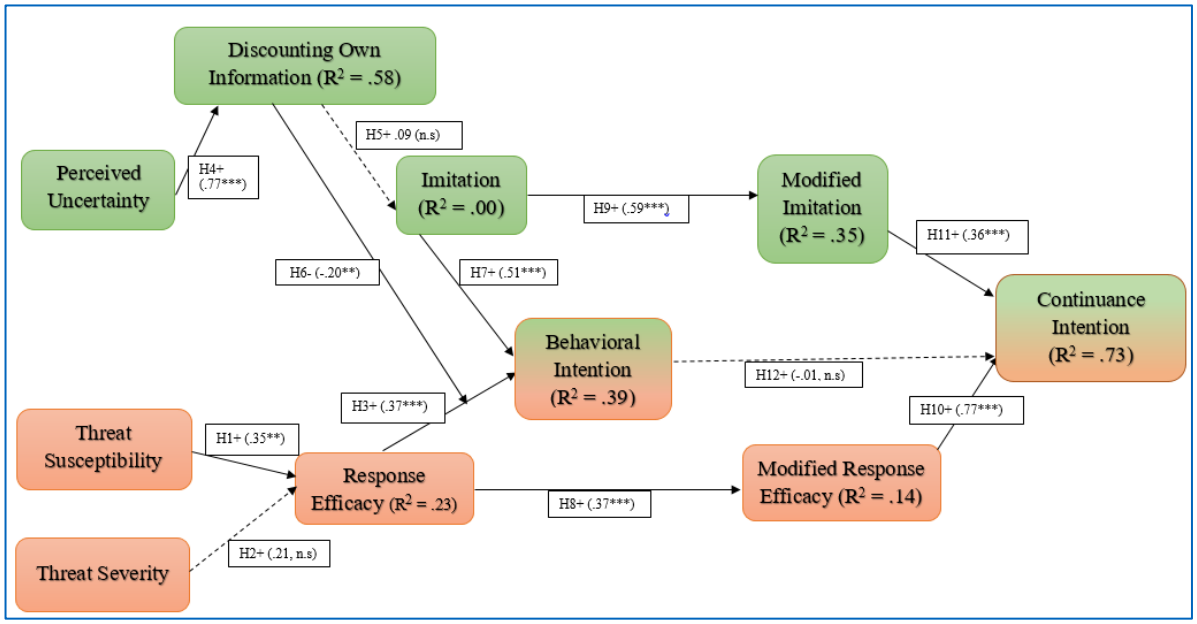
Table 7. Model Comparison

Model	Control group	Treatment group
PMT constructs only	.35	.39
Full model	.39	.53



Notes: n.s = nonsignificant, * p <0.05, ** p <0.01, *** p < 0.001, dotted lines = unsupported paths.

Figure 2. Treatment Group Path Estimates



Notes: n.s = nonsignificant, * p < 0.05, ** p < 0.01, *** p < 0.001, dotted lines = unsupported paths.

Figure 3. Control Group Path Estimates

To ensure that the elimination of these items did not negatively influence the reliability and validity of the constructs, we also ran these tests using the remaining items. The results showed that the factor loadings, CR, and convergent and discriminant validity were acceptable. The tables showing the results of these analyses are provided in Appendix F.

7.3 Structural Analysis

In the next step, we analyzed the structural model. The model fit statistics were equal to or greater than the recommended values (χ^2/df = 1.76, CFI = 0.91, IFI = 0.91, RMSEA = 0.06). We tested the hypotheses through covariance-based structural equation modeling (SEM) using AMOS v24). To test for the moderating effects, we used the product-of-sums approach recommended by Goodhue, Lewis, and Thompson (2007). Specifically, the moderating factor (discounting one's own information) and the independent variable (response efficacy) were multiplied to generate an interaction factor (DOI × RE), which was then linked to the intention to engage in protection-motivated behaviors (the dependent variable). We also measured the influence of the control variables (age, gender, and switching costs) on continuance intention (the ultimate dependent variable). As previously described, this study used a control group and a treatment group. We conducted an analysis to compare the statistical differences between these two groups. For this purpose, we used a dummy-coded variable to split the dataset into two groups. Table 5 shows the path estimates in both groups. Table 6 provides a summary of the results of testing the hypotheses. Figure 2 and Figure 3 depict the structural model analysis of the treatment and control groups.

Finally, in the post hoc analysis, we compared the explained variance of protection motivation (behavioral intention) across groups. To conduct this analysis, we compared two models, "PMT constructs only" and "full model," which included both PMT constructs and herd behavior constructs. Table 7 summarizes the results of this comparison.

The results show that for the control group, adding the herd behavior constructs to the PMT constructs (which forms the full model) only explains 4% more of the variance in behavioral intention. However, for the treatment group (i.e., the participants who received the popularity information about Dashlane), the full model (which included both PMT constructs and herd behavior constructs) explained 14% more variance in behavioral intention than the PMT constructs-only model. These findings indicate that the treatment made a significant difference in the participants' intentions to use the password manager, which was the popular security technology in the narrative. See Appendix G for the effect sizes related to this analysis.

8 Discussion

This research contributes to the literature by examining whether obtaining popularity information about a security technology can trigger herd mentality and increase protection motivation. We hypothesized that discounting one's own information can lead to the tendency to imitate the behavior of others. By discounting one's own information in uncertain circumstances, the user relies less on limited information and beliefs and tends to rely heavily on the insights gained from observations of others' behavior. Logically, the more that users discount their own limited information, the more likely they will tend to imitate the behavior of others. In contrast, if users do not discount their own beliefs, their protection motivation is determined by their personal perceptions of response efficacy. Consistent with this line of reasoning, we found that the effect on imitation of discounting one's own information was nonsignificant for the control group, which did not receive the popularity information (the treatment) about Dashlane. Conversely, discounting one's own information significantly and positively influenced imitation in the treatment group. Discounting their own information drove subjects to become less responsive to their own information; instead, these subjects favored other users' decisions, believing that others were better informed. Therefore, they tended to imitate others even if their own information might have led them to different conclusions.

Furthermore, the findings show that the subjects in the treatment group developed a higher level of protection motivation compared to those in the control group. In terms of explained variance (R^2), the treatment group model explained more variance in the ultimate dependent variable at the pre-adoption stage (behavioral intention) compared to the control group (54% and 39%, respectively). This difference could be the result of a stronger tendency to imitate among the subjects in the treatment group compared to the subjects in the control group. Response efficacy, as the other direct antecedent of behavioral intention, similarly influenced the motivation of the treatment and control group. The standardized path coefficients equaled 0.38 and 0.37, respectively, suggesting that the tendency to imitate caused the difference between the two groups. Additionally, we found that discounting one's own information negatively moderates the relationship between response efficacy (i.e., personal assessment) and behavioral intention. According to herd theory, discounting one's own information means that users rely less on their own beliefs in making technology adoption decisions. Thus, the more discounting, the less important personal beliefs are in making such decisions, demonstrating a weak anchoring effect of these beliefs (Sun 2013). As we expected, this moderating effect was stronger for the

treatment group (-0.32*** versus -0.20**). In addition, the cognitive process of discounting one's own information leading to imitation was only significant for the treatment group. Originally, we hypothesized that when users discount their own information, they rely less on their initial information and beliefs than on the insights obtained from their observations of others' behavior. Logically, the more a user discounts his or her own information, the more likely he or she will be to imitate the behavior of others. Our findings show that this only happened for the treatment group, which received the popularity information about Dashlane.

Drawing on these findings, we argue that in the IS security context, the tendency to imitate other users in highly uncertain circumstances influences users' protection motivation (i.e., the adoption of security technologies). It is reasonable to argue that at the post-adoption stage, users may continue to imitate others. In other words, users may continue to use the same security technology because it is used by a large number of people. Consistently, we hypothesized that modified perceptions of response efficacy and imitation are positively related to users' continuance intentions. The results show that herd mentality is not as influential as personal assessments (i.e., response efficacy) at the post-adoption stage. Modified response efficacy, which can be a proxy for the personal assessment of a security technology at the post-adoption stage, influenced continuance intention with a beta-coefficient (0.78) more than three times as strong as that of the modified imitation (0.24), suggesting that at the post-adoption stage, personal assessment becomes the dominant factor in determining continuance intention.

In contrast, at the pre-adoption stage, the influence of herd mentality on adoption intention (i.e., protection motivation) was twice as strong as that of personal assessment (0.63 versus 0.38) in the treatment group. This finding indicates that at the post-adoption stage, when users have less uncertainty about the security technology because of their experience, they rely heavily on their own assessments and put less emphasis on the popularity information about a security technology. A possible explanation for this finding could be the sensitivity and delicacy of security-related decisions. The consequences of making a poor adoption decision in the security context could be far more catastrophic than the consequences of a decision regarding a technology in another context (e.g., hedonic). Therefore, users are likely to put less emphasis on its popularity and exert greater efforts into making personal evaluations of the security technology efficacy.

An unexpected finding of this research is that behavioral intention at Stage 1 did not influence continuance intention at the post-adoption stage (H12). Similar to our findings, the findings of Kim & Malhotra (2005) also show that the relationship between behavioral intention at the pre-adoption and post-adoption stage is not significant. A reason explaining this result could be the role of experience with security technologies. It is reasonable to argue that prior experience with security technologies is a crucial factor in determining continuous behavior because users who have directly experienced using such technologies are likely to have a significant level of expectation disconfirmation (positive or negative); thus, the anticipation of a direct relationship between intention to engage in protection-motivated behaviors (at the pre-adoption stage) and continuous secure behavior (at the post-adoption stage) may be unwarranted. In a post hoc analysis of possible mediating effects of modified imitation and modified response efficacy on the relationship between pre-adoption behavioral intention and later continuance intention, we ran two mediation analyses (using bootstrapping) and found that both modified imitation and modified response efficacy fully mediate the relationship between behavioral intention and continuance intention (p = 0.004 and p = 0.01, respectively).

9 Contributions to Research

Consistent with the recent call for understanding the roots of behavioral security (Chatterjee, Sarker & Valacich, 2015), this study contributes to the literature by examining the effects of herd mentality on security behaviors. IT users often make decisions related to information security decisions in complex and multidimensional environments, which could lead to phenomena like behavioral anomalies. Current behavioral security theories generally assume that users possess sufficient information about security technologies before making security-related decisions. This theory assumption limits our understanding of how security decisions are made in various real-world circumstances. We further improved our understanding of secure behavior by examining herd mentality as one of the most important boundary conditions in this area. In this regard, our findings show that when individuals make decisions in highly uncertain circumstances, they may observe the behavior of others, discount their own limited information, and imitate others. According to our empirical analysis, the "discounting own information → imitation" and the "imitation → behavioral intention" relationships were stronger in the treatment group because the subjects received information about the behavior of others, that is, the widespread use of the password manager.

This study also contributes to the literature by providing insights into the continuity of security behaviors over time when such behaviors are influenced by a herd mentality. Based on the few relevant studies in the IS

context, we hypothesized that at the post-adoption stage, herd mentality can still influence continuance intentions because IT herds have been shown to be robust and they tend to survive even when contrary signals and information are received (Edelen et al., 2016; Sun, 2013). Surprisingly, the findings of our study show that herd mentality (conceptualized as modified imitation), as compared to updated personal perceptions (conceptualized as modified response efficacy), becomes weaker at the post-adoption stage. Instead, the personal assessment of the focal security technology used in this study significantly influenced users' continuance intentions.

Our findings indicate that at the post-adoption stage, after the users had gained experience with the security technology, they relied heavily on their own assessments. These findings indicate that the awareness of the popularity and widespread use of the security response were not as important as they were at the pre-adoption stage. In addition, the results of the post hoc analysis showed that dropping "modified imitation" from the Time 2 model did not reduce the R-squared of continuance intention in either group, indicating that while imitation is an important factor at the post-adoption stage, it is not as influential as it is in the pre-adoption stage. The findings of this study indicate that a deep understanding of secure behavior requires nuanced and fine-grained analyses of this phenomenon for several reasons. For example, different boundary conditions could affect IS security behaviors differently. Furthermore, the effects of boundary conditions on secure behaviors could differ in other contexts. Moreover, based on the findings of this study, these effects could differ in the different stages of security technology use.

As mentioned earlier, users' perceptions of response efficacy (i.e., the effectiveness of a specific security solution) and other perceptions (e.g., imitation tendency) should be measured at both the post-adoption stage and at the adoption stage in order to capture the dynamic nature of the continuous behavior phenomenon, thus allowing for understanding the distal effects of the underlying cognitive process that influences continuous behavior (Kim & Malhotra, 2005; Vedadi & Warkentin, 2018). Regarding the multistage design of this study, which includes pre-adoption and post-adoption perceptions of the security software, we used rigorous scale development guidelines (MacKenzie et al., 2011) to develop and validate two constructs—modified response efficacy and modified imitation—in order to measure these perceptions at the post-adoption stage. This method was especially important because users generally undergo a belief-updating process after gaining direct experience with a technology. Therefore, the conceptualization and operationalization of these concepts were crucial. In future research on behavioral security and herd behavior in the IS context, these validated measurement scales can be used to measure the longitudinal nature of security behavior and decision-making in highly uncertain circumstances (see Appendix H).

Finally, though our contributions, especially informed by Sun (2013), contextualize herd theory within the security behavior continuance domain, this study is distinguished from other IT herd behavior studies, especially Sun's (2013), in several ways. Our primary focus in the pre-adoption stage is the participants' level of protection motivation and how providing popularity information (the experimental treatment) can increase the level of these intentions to engage in protection-motivated behaviors. We found that the treatment was successful in increasing the level of protection motivation and that such herd mentality can exert an even stronger influence than users' personal perceptions (i.e., perceived response efficacy). Furthermore, Sun (2013) measured users' perceptions vicariously by using constructs such as disconfirmation and satisfaction. We, however, conceptualized and operationalized two new constructs (modified response and modified imitation) in order to more accurately and directly measure these perceptions. Specifically, Sun (2013) did not measure herd mentality at the post-adoption stage and limited his measurement of this important phenomenon by finding a positive relationship between imitation (at the pre-adoption stage) and disconfirmation (at the post-adoption). Using these two new constructs, we directly measured our participants' perceptions and our findings were consistent with theory.

10 Contributions to Practice

Because users' decision-making can be strongly influenced by the behavior of others, both managers and software security vendors should consider framing their communications (e.g., advertising and security training, respectively) to publicize positive information (e.g., performing a popular security procedure that is widely used by other employees). Our empirical findings support this argument because the size of the effect of herd-related factors on protection motivation was found to be medium (0.29) for the treatment group, whereas it was small for the control group (0.04), thus indicating that the experimental treatment (providing popularity information) made a significant difference in the participants' intention to use the password manager. In other words, managers can expect to increase the overall security of their organization by providing information about the security behavior of others. For example, Barlow et al. (2018) found that a message providing information about the compliance of others increased the likelihood that users would comply with security policies. Specifically, their normative influence manipulation, a

form of psychological nudge, informed the message recipient that "a recent survey of our employees concerning this policy showed that over 85 percent would not share their password, even with another employee, regardless of the circumstances." (pp. 709-710)

Furthermore, fostering herd mentality in security behavior could significantly enhance and accelerate the process of securing information assets. Nevertheless, herding users toward or away from a certain behavior should be done with extreme care. It is possible that users may find that the advertised organizational adopters (i.e., the herd leaders) do not resemble them in terms of organizational tasks, sophistication, and so on. Therefore, the successful promotion of herd mentality to ensure certain secure behaviors that comply with IT security policies in organizations would require managers to highlight the similarities between the prior adopters and potential adopters to increase the likelihood of imitation.

Managers should also recognize that in a voluntary context, IT security herds may not last because a high number of users might lose interest in using a security technology, thus leading to the collapse of the current user base and the herd itself. Specifically, users may ultimately evaluate their own needs and contexts of local use (Sun, 2013). Consequently, they may cease to incorporate herd mentality in their decision-making and may rely strictly on their own perceptions of and experiences in using a security technology. Similarly, companies sometimes imitate each other to emulate their competitors or they believe that their competitors' choices of technology and systems are based on better information (Lieberman & Asaba, 2006). This approach to decision-making can occasionally increase the likelihood of errors for first movers and it can lead to sending the wrong signal to late movers. Therefore, imitation-based IT strategies may lead to negative consequences for companies if they decide to use the wrong security technologies. Hence, it is important for IT managers and policy makers to predict the IT security phenomena that are highly likely to become popular, thoroughly identify their disadvantageous implications, and consider the possible opportunities for leveraging such phenomena in a positive way while diminishing potential negative consequences.

11 Limitations and Future Research

This research has the following limitations. First, a distinction between correct and incorrect herds in the security context should be made in future studies. In uncertain circumstances, a user may join and remain in an IT herd, thus adopting a superior security technology when there is a positive and strong enough signal about it (Walden & Brown, 2009). Conversely, incorrect herds are characterized by users who develop unrealistic expectations based on observation of actions of predecessors and, consequently, become more susceptible to contrary information at the post-adoption stage; therefore, these herds are generally more fragile than correct herds. In our study, we only tested the positive effects of popularity information, but we question whether negative information about few adoptions at the post-adoption stage also has an influence. This limitation provides an interesting opportunity for future research to examine how contrary information about a security technology over time may reverse herd direction.

Future research should also account for relevant individual differences. In the herd behavior context, some users may intentionally avoid joining a security technology herd because they want to stand out from the crowd. In other words, some users may feel that adopting popular technology may make them seem average. This attitude has also been observed at the organizational level; some organizations persist in differentiating themselves from their competitors, and they avoid using a security technology because it is "too popular" in the industry (Abrahamson & Rosenkopf, 1993). Future studies should investigate the cognitive styles and personality traits that make users more or less likely to follow an IT herd.

In addition to individual differences in personality traits, cultural differences might influence herd behavior in the IT security context. The subjects of this study were in the US, which limits the generalizability of the findings to users in other cultures. Ethnic groups may have significantly different espoused cultural values, which may or may not be reflected in individual behavior (Srite & Karahanna, 2006; Crossler, et al., 2013). The finance literature indicates that cultural differences can have a significant influence on herd behavior (Hong et al., 2016). For instance, Chang and Lin's (2015) study on the effects of national culture on investors' decision-making in international stock markets provide evidence that herd behavior occurs more often in Confucian equity markets. Their findings also show that certain national cultural indices closely correlate with herding behavior. Therefore, cross-cultural research should be conducted to reveal the importance of additional factors that could influence herd mentality in the behavioral security context.

To ensure that our research model was as parsimonious as possible, we decided not to include all behavioral security constructs and to focus on the most established constructs of threat and coping appraisal. Future research could evaluate the effects of various fear appeals and other constructs on herd behavior, such as response cost, maladaptive reward, and self-efficacy. Response cost, which is any perceived cost (e.g., monetary, personal, time, and effort) associated with the adaptive coping response, may substantially affect users' tendency to join or avoid a herd. Response

efficacy and self-efficacy may elevate the probability of adopting a security technology, whereas the perception of high response costs could decrease this probability (Floyd, Prentice-Dunn, & Rogers, 2000).

Regarding the use of password managers, one of the most important concerns of potential users is the issue of trust. In line with the conventional wisdom, "do not put all your eggs in one basket," using a *single* password manager could invite hackers to attack and steal a user's passwords if that single control were compromised. However, some users might risk using a single password manager if it provided more security than their own passwords. Therefore, investigating the influence of different types and levels of trust (McKnight, Choudhury, & Kacmar, 2002) and how it can affect users' herd mentality is an interesting and important topic for future research. Baddeley (2011) emphasized the important role of trust in herd behavior, noting that in human behavior regarding security, decisions are made in a multidimensional space that reflects contradictory goals. Therefore, trust is a vital influence in this area because effective security software allows transparent communication between trusted parties, which is closed to the "bad guys" (p. 13).

Because there is often a high risk of drop-out (attrition) with multistage data collection projects, we opted for a one-week time frame between the data collection stages to reduce this threat. In addition, because password managers are typically simple technologies that, unlike some utilitarian technologies with numerous features and complexities, are fairly easy to use and mostly automated, we considered our time frame to be adequate. However, this short time frame might be insufficient for comprehensively reflecting the continuance intention of users; thus, future studies could define multistage data collection projects with longer time frames in order to more realistically examine the continuance intention phenomenon in the herd behavior context.

Future research could examine this security-related phenomenon using objective data collection methods, as recommended by Crossler, et al (2013) and Warkentin, Straub, and Malimage (2012), such as examining neurophysiological indicators of cognitive functions evident during this decision process (e.g., Warkentin, Walden et al., 2016). Another interesting future research avenue would be to analyze the difference between organizational and home users' behavior in this context, given that norms and popularity information may be more established in the workplace than in homes because of the larger cohort of peers at work. Differential organizational cultures may also impact herd mentality in ways that could be explored in future research. Much like national culture, some organizational cultures may convey a greater implicit signal regarding conformity or individuality, thus moderating the impact of popularity information and the resulting herd behavior.

12 Conclusion

IT users often make information security-related decisions in complex and multidimensional environments, which could lead to phenomena like behavioral anomalies. For instance, under uncertain circumstances, users may discount their own limited information about a security technology and make their adoption decisions based on what the majority of users' decisions are in this regard. Current behavioral security theories generally assume that users possess sufficient information about security technologies before making security-related decisions. This theory assumption limits our understanding of how security decisions are made in various real-world circumstances. We investigated how providing popularity information can trigger herd behavior and can subsequently influence security behaviors. We also provide insights into security-related decisions that are influenced by herd mentality and whether they persist over time. We found that in uncertain circumstances, when users become aware of the widespread use of a certain security technology, they develop a significantly higher protection motivation. Furthermore, we found that at the post-adoption stage, users rely more heavily on their own information about their continuous use of security technologies and place less emphasis on herd-related factors.

References

Abrahamson, E., & Rosenkopf, L. (1993). Institutional and competitive bandwagons: Using mathematical modeling as a tool to explore innovation diffusion. *Academy of Management Review*, *18*(3), 487-517.

Acemoglu, D. (1993). Learning about others' actions and the investment accelerator. *Economic Journal*, *103*(417), 318-328.

Au, Y.A., & Kauffman, R. (2003). What do you know? Rational expectations in information technology adoption and investment. *Journal of Management Information Systems*, *20*(2), 49-76.

Avery, C., & Zemsky, P. (1998). Multidimensional uncertainty and herd behavior in financial markets. *American Economic Review*, *88*(4), 724-748.

Baddeley, M. (2011). Information security: Lessons from behavioural economics. Workshop on the Economics of Information Security, http://www.heinz.cmu.edu/~acquisti/SHB/SHB11BaddeleyFinal.pdf

Banerjee, A. V. (1992). A simple model of herd behavior. *The Quarterly Journal of Economics*, *107*(3), 797-817.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 689-715.

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, *25*(3), 351-370.

Bhattacherjee, & Premkumar. (2004). Understanding changes in belief and attitude toward information technology usage: A theoretical model and longitudinal test. *MIS Quarterly*, *28*(2), 229-254.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837-864.

Bretschneider, U., & Leimeister, J. M. (2017). Not just an ego-trip: Exploring backers' motivation for funding in incentive-based crowdfunding. *Journal of Strategic Information Systems*, *26*(4), 246-260.

Chang, C. H., & Lin, S. J. (2015). The effects of national culture and behavioral pitfalls on investors' decision-making: Herding behavior in international stock markets. *International Review of Economics and Finance*, *37*, 380-392.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49-87.

Chin, W. W., & Todd, P. A. (1995). On the use, usefulness, and ease of use of structural equation modeling in MIS research: A note of caution. *MIS Quarterly*, *19*(2), 237-246.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences.* Erlbaum.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209-226.

Dewan, S., Ho, Y. J., & Ramaprasad, J. (2017). Popularity or proximity: Characterizing the nature of social influence in an online music community. *Information Systems Research*, *28*(1), 117-136.

Duan, W., Gu, B., & Whinston, A. B. (2009). Informational cascades and software adoption on the internet: An empirical investigation. *MIS Quarterly*, *33*(1), 23-48

Edelen, R. M., Ince, O. S., & Kadlec, G. B. (2016). Institutional investors and stock return anomalies. *Journal of Financial Economics*, *119*(3), 472-488.

Ellis, M. E., Aguirre-Urreta, M. I., Sun, W. N., & Marakas, G. M. (2008). Establishing the need for measurement invariance in information systems research: A step-by-step example using technology acceptance research. *Proceedings of the Decision Science Institute*.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429.

Goodhue, D., Lewis, W., & Thompson, R. (2007). Statistical power in analyzing interaction effects: Questioning the advantage of PLS with

product indicators. *Information Systems Research*, *18*(2), 211-227.

Graham, J. R. (1999). Herding among investment newsletters: Theory and evidence. *Journal of Finance*, *54*(1), 237-268.

Hey, J. D., & Morone, A. (2004). Do markets drive out lemmings or vice versa? *Economica*, *71*(284), 637-659.

Hong, Y., Huang, N., Burtch, G., & Li, C. (2016). Culture, conformity and emotional suppression in online reviews. *Journal of Association of Information Systems*, *17*(11), 737-758.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-134.

Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. B. (2016). Limited information and quick decisions: Consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction 8*(3), 88-130.

Keynes, J. M. (1937). The general theory of employment. *The Quarterly Journal of Economics*, *51*(2), 209.

Kim, S. S. (2009). The integrative framework of technology use: An extension and test. *MIS Quarterly*, *33*(3), 513-537.

Kim, S. S., & Malhotra, N. K. (2005). A Longitudinal model of continued is use: An Integrative view of four mechanisms underlying postadoption phenomena. *Management Science*, *51*(5), 741-755.

Kim, S. S., & Son, J. (2009). Out of dedication or constraint? A dual model of post-adoption phenomena and its empirical test in the context of online services. *MIS Quarterly*, *33*(1), 49-70.

Li, X., & Hitt, L. M. (2008). Self-selection and information role of online product reviews. *Information Systems Research*, 19(4), 456-474.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(07), 394-413.

Lieberman, M. B., & Asaba, S. (2006). Why do firms imitate each other? *Academy of Management Review*, *31*(2), 366-385.

Liu, Y., Feng, J., & Liao, X. (2017). When online reviews meet sales volume information: Is more or accurate information always better? *Information Systems Research*, *28*(4), 723-743.

MacKenzie, Podsakoff, & Podsakoff. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293-334.

Marett, K. (2015). Checking the manipulation checks in information security research. *Information and Computer Security*, *23*(1), 20-30.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334-359.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192-222.

Muchnik, L., Aral, S., & Taylor, S. J. (2013). Social influence bias: A randomized experiment. *Science*, *341*(6146), 647-651.

Mutchler, L.A. & Warkentin, M. (2020). Experience matters: The role of vicarious experience in secure actions. *Journal of Database Management*, *31*(2), Article 1.

Online Trust Alliance (2018). Online trust alliance reports doubling of cyber incidents in 2017. https://otalliance.org/news-events/press releases/online-trust-alliance-reports-doubling-cyber-incidents-2017-0.

Ponemon. (2017). Cost of data breach study. https://www.ibm.com/security/data-breach/

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879-903.

Rao, H., Greve, H. R., & Davis, G. F. (2001). Fool's gold: Social proof in the initiation and abandonment of coverage by wall street analysts. *Administrative Science Quarterly*, *46*(3), 502-526.

Rubenking, N.J. (2015). Survey: Hardly anybody uses a password manager, *PC Magazine*. https://securitywatch.pcmag. com/security-software/332517-survey-hardly-anybody-uses-a-password-manager.

Scharfstein, D. S., & Stein, J. C. (1990). Herd behavior

and investment. *American Economic Review*. *80*(3), 465-479.

Schwarz, A., Rizzuto, T., Carraher-Wolverton, C., Roldán, J. L., & Barrera-Barrera, R. (2017). Examining the impact and detection of the "urban legend" of common method bias. *The DATA BASE for Advances in Information Systems*, *48*(1), 93-119.

Simon, H. A. (1976). From substantive to procedural rationality. In T. J. Kastelein, S. K. Kuipers, W. A. Nijenhuis, & G. R. Wagenaar (Eds.) *25 Years of Economic Theory* (pp. 65-86). Springer.

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*(1), 380-427.

Srite, & Karahanna. (2006). The role of espoused national cultural values in technology acceptance. *MIS Quarterly*, *30*(3), 679-704.

Steenkamp, J. E. M., & Baumgartner, H. (1998). Assessing measurement invariance in cross-national consumer research. *Journal of Consumer Research*, *25*(1), 78-107.

Sun, H. (2013). A longitudinal study of herd behavior in the adoption and continued use of technology. *MIS Quarterly*, *37*(4), 1013-1041.

Thies, F., Wessel, M., & Benlian, A. (2016). Effects of social interaction dynamics on platforms. *Journal of Management Information Systems*, *33*(3), 843-873.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization, *MIS Quarterly*, *15*(1), 125-143.

Triandis, H. C. (1980). Values, attitudes, and interpersonal behavior. *Nebraska Symposium on Motivation, Beliefs, Attitudes, and Values* (pp. 195-259). University of Nebraska Press.

Tucker, C., & Zhang, J. (2011). How does popularity information affect choices? A field experiment. *Management Science*, *57*(5), 828-842.

Vedadi, A., & Warkentin, M. (2018). Secure behavior over time: Perspectives from the Theory of Process Memory. *ACM SIGMIS Database: The DATA BASE for Advances in Information Systems*, *49*(1), 39-48.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376.

Walden, E., & Browne, G. J. (2009). Sequential adoption theory: A theory for understanding herding behavior in early adoption of novel technologies. *Journal of the Association for Information Systems*, *10*(1), 31-62.

Wang, P. (2009). Popular concepts beyond organizations: Exploring new dimensions of information technology innovations. *Journal of the Association for Information Systems*, 10(1), 1-30.

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378-396.

Wang, C., Zhang, X., & Hann, I. H. (2018). Socially nudged: A quasi-experimental study of friends' social influence in online product ratings. *Information Systems Research*, *29*(3), 641-655.

Warkentin, M., D. Straub, and K. Malimage (2011). *Measuring the dependent variable for research into secure behaviors*. Presented at the Decision Sciences Institute Annual National Conference.

Warkentin, M., Johnston, A.C., Shropshire, J. & Barnett, W.D. (2016) Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*, 25-35.

Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3), 194-215.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education and Behavior*, *27*(5), 591-615.

Yoo, B., Jeon, S., & Han, T. (2016). An analysis of popularity information effects: Field experiments in an online marketplace. *Electronic Commerce Research and Applications*, *17*, 87-98.

Appendix A. Construct Definitions and Measurement Scales

Perceived uncertainty (UNC)

Definition: the degree to which one is unable to accurately predict the issues related to the adoption of a technology due to imperfect information (Sun, 2013).

Measurement scale (7-point *agree/disagree* Likert scale):
1. I am NOT sure what Dashlane is about and what it can do for me.
2. I feel uncertain whether my needs when logging onto websites securely could be met by using Dashlane.
3. I feel uncertain whether I would be able to respond appropriately to any changes/upgrades of Dashlane.
4. I feel that using Dashlane involves a high degree of uncertainty.

Imitation (IMI)

Definition: the degree to which one follows previous adopters to adopt a certain form of technology (Sun, 2013).

Measurement scale (7-point *agree/disagree* Likert scale):
1. It seems that Dashlane is a widely-used password manager, therefore I would like to use it too.
2. I follow others in deciding to use Dashlane.
3. I would choose to use Dashlane because many others are already using it.

Discounting one's own information (DOI)

Definition: the degree to which one disregards his/her own beliefs about a technology when making an adoption decision (Sun, 2013).

Measurement scale (7-point *agree/disagree* Likert scale):
1. I don't fully trust my own thinking about how Dashlane could work for me.
2. I would not necessarily follow my own thoughts about Dashlane's features.
3. I would not rely only on my own information about how Dashlane works.

Behavioral intention (protection motivation) (BI)

Definition: Users' intention to use a particular security solution (Johnston & Warkentin, 2010).

Measurement scale (7-point *agree/disagree* Likert scale):
1. I intend to use Dashlane in future.
2. I plan to use Dashlane soon.
3. I predict I will use Dashlane soon.
4. I expect to adopt Dashlane soon.

Threat severity (TSEV)

Definition: the degree to which a user believes a security threat could have severe consequences (Johnston & Warkentin, 2010).

Measurement scale (7-point *agree/disagree* Likert scale):
1. If my passwords were stolen, lost, or forgotten, the consequences would be severe.
2. If my passwords were stolen, lost, or forgotten, the consequences would be serious.
3. If my passwords were stolen, lost, or forgotten, the consequences would be significant.

Threat susceptibility (TSUS)

Definition: refers to users' perception about the probability of suffering from an IT security threat (Johnston & Warkentin, 2010).

Measurement scale (7-point *agree/disagree* Likert scale):
1. My passwords are at risk of being stolen, lost, or forgotten.
2. It is likely that my passwords will be stolen, lost, or forgotten.

3. It is possible that my passwords will be stolen, lost, or forgotten.

Response efficacy (RE)

Definition: the degree to which an individual believes the response to be effective in alleviating a threat (Johnston & Warkentin, 2010).

Measurement Scale (7-point *agree/disagree* Likert scale):
1. Using Dashlane works for password protection.
2. Using Dashlane is effective for password protection.
3. By using Dashlane, my passwords are more likely to be protected.

Continuance intention (CONT)

Definition: Users intention to continue using a technology (Bhattacherjee, 2001).

Measurement Scale (7-point *agree/disagree* Likert scale):
1. I intend to continue using Dashlane rather than discontinue its use.
2. My intentions are to continue using Dashlane rather than use any alternative means.
3. I would like to continue my use of Dashlane.

Modified response efficacy (ModRE)

Definition: as the degree to which one perceives that a security technology is useful at the post-adoption stage (self-developed).

Measurement Scale (7-point *agree/disagree* Likert scale):
1. Using Dashlane improves my performance in managing my passwords.
2. Using Dashlane increases my productivity in managing my passwords.
3. Using Dashlane enhances my effectiveness in managing my passwords.

Modified imitation (ModIMI)

Definition: as the degree to which one perceives that imitation is a good strategy for continuous use of a technology (self-developed).

Measurement Scale (7-point *agree/disagree* Likert scale):
1. It seems that Dashlane is a widely-used password manager, therefore I would like to continue using it.
2. I follow others to continue to use Dashlane.
3. I would choose to continue to use Dashlane because many others are already using it.

Switching costs (SW)

Definition: The extent to which a customer feels dependent on a service because of economic, social or psychological investments that would become useless in other services (Kim & Son, 2009).

Measurement Scale (7-point *agree/disagree* Likert scale):
1. Switching to a new password manager would involve some hassle.
2. Some problems may occur if I switch to another password manager.
3. It would be complex to change my password manager.

Appendix B. Treatment Narrative

Using strong passwords has always been one of the most important issues of data security. Many users create security problems by using passwords that are too simple to ensure security or too complex to remember. Other users reuse the same password for different websites, which also creates security problems, or make themselves vulnerable to password theft by saving their passwords on their browsers.

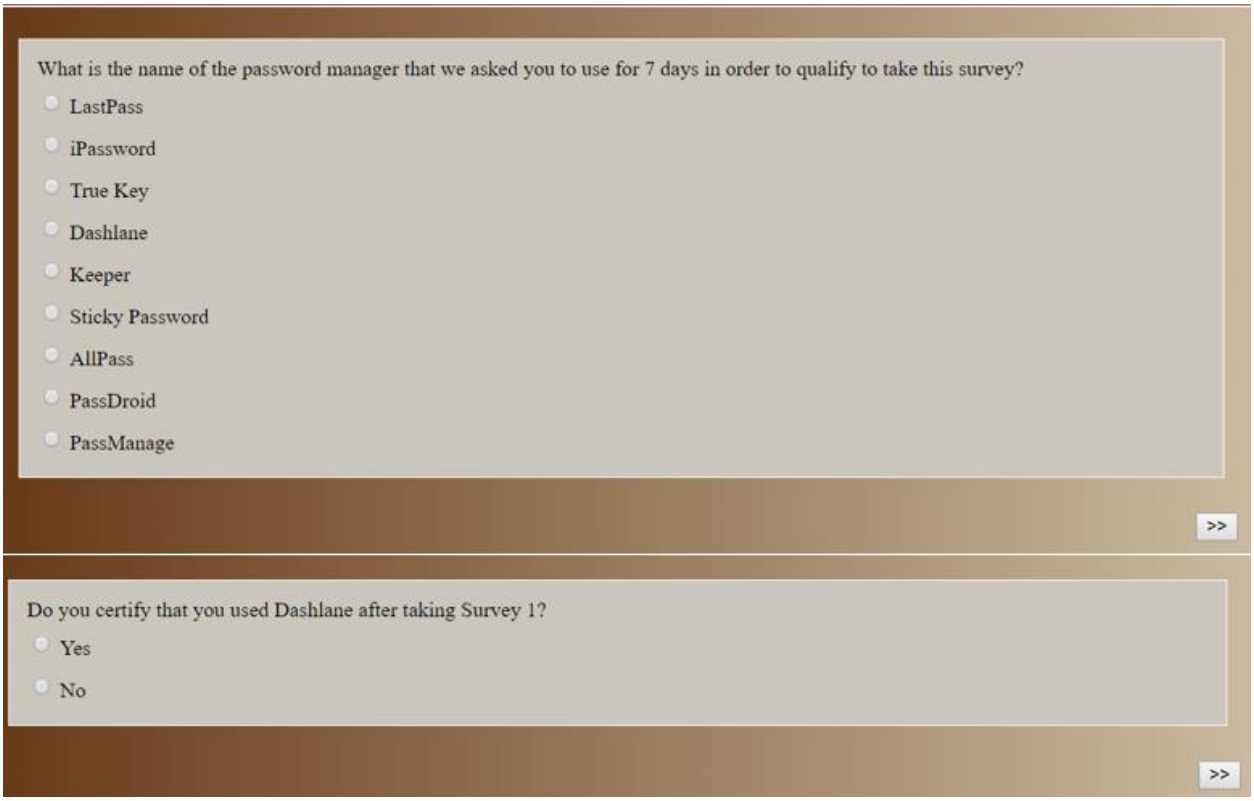
A password manager is a software that helps you effectively and conveniently store and organize passwords. A good example is Dashlane, which is a free, efficient and easy-to-use password manager that can be comfortably integrated with most web browsers and smartphones.

Here is the list of facts about Dashlane:

- The number of internet users who are using password managers is rapidly growing.
- According to Download.com, Dashlane is one of the most downloaded password managers.
- The password manager market is expected to increase from $311 million in 2014 to $710 million by 2019.
- 1 out of 3 internet users is actively using password manager tools.
- Other reports show that the vast majority of internet users are planning to adopt password managers in near future.
- Leading analyst firms have predicted that the number of companies throughout the world that are planning to invest in password managers, and especially in Dashlane, will exponentially grow in near future.

Appendix C. Software Usage Validity Checks

Figure C1. Usage Validity Checks



Appendix D. Pilot Study Statistics

Table D1. Stage 1: Cronbach's Alpha Reliability Test

Construct	Alpha
Protection motivation	.96
Threat severity	.91
Threat susceptibility	.83
Response efficacy	.88
Perceived uncertainty	.85
Discounting own information	.83
Imitation	.91
Modified response efficacy	.91
Switching cost	.83
Modified imitation	.95
Continuance intention	.95

Table D2. Stage 1: Principal Component Analysis

	1	2	3	4	5	6	7
BI1	.85						
BI2	.89						
BI3	.89						

BI4	.92						
UNC1		.79					
UNC2		.81					
UNC3		.77					
UNC4		.81					
DOI1		.40		.72			
DOI2				.79			
DOI3				.81			
IMI1					.79		
IMI2	.44				.73		
IMI3					.86		
RE1						.74	
RE2						.78	
RE3						.83	
TSUS1							.83
TSUS2							.79
TSUS3							.83
TSEV1			.89				
TSEV2			.87				
TSEV3			.89				
Notes: The values are suppressed to 0.4. Varimax rotation.							

Appendix E. Item Descriptive Statistics

Table E1. Item Average Means and Standard Deviations

	Control		Treatment	
Item	**Average**	**Std. deviation**	**Average**	**Std. deviation**
TSUS1	5.07	1.5	5.10	1.3
TSUS2	4.36	1.5	4.30	1.4
TSUS3	4.93	1.4	4.71	1.4
TSEV1	5.43	1.5	5.42	1.4
TSEV2	5.34	1.4	5.59	1.3
TSEV3	5.22	1.4	5.24	1.4
RE1	5.37	1.3	5.21	1.4
RE2	5.32	1.3	5.17	1.2
RE3	5.31	1.4	5.37	1.1
UNC1	3.10	1.7	3.47	1.7
UNC2	3.07	1.6	3.11	1.6
UNC3	3.40	1.7	3.86	1.6
UNC4	2.91	1.7	3.14	1.7
DOI1	3.05	1.8	3.06	1.5
DOI2	3.04	1.5	3.42	1.5
DOI3	3.76	1.7	4.01	1.6
IMI1	4.32	1.6	4.28	1.8
IMI2	4.58	1.6	4.54	1.6
IMI3	4.06	1.7	4.03	1.6
SW1	4.44	1.6	5.00	1.3
SW2	4.01	1.5	4.48	1.4
SW3	3.87	1.6	4.33	1.4
ModRE1	5.19	1.4	5.35	1.3
ModRE2	5.13	1.4	5.11	1.4
ModRE3	5.19	1.4	5.35	1.4
CONT1	4.50	1.8	4.82	1.7
CONT2	4.65	1.8	4.91	1.6
CONT3	4.64	1.8	4.83	1.7
ModIMI1	3.64	1.8	3.73	1.7
ModIMI2	3.92	1.7	3.89	1.7
ModIMI3	3.86	1.7	3.80	1.7
B1	4.67	1.6	4.29	1.5
B2	4.62	1.6	4.19	1.6
B3	4.44	1.5	4.27	1.6
B4	4.64	1.6	4.13	1.7

Appendix F. Validity Measures after Dropping Items

Table F1. Reliability, Validity, the Square Roots of AVEs (in Bold) and Correlations

Construct (CR; AVE)	BI	TSUS	TSEV	RE	UNC	DOI	IMI	SW	Mod RE	CONT	Mod IMI
BI (0.96; 0.89)	**.94**										
TSUS (0.82; 0.61)	.38	**.78**									
TSEV (0.90; 0.82)	.18	.47	**.90**								
RE (0.88; 0.71)	.61	.45	.40	**.84**							
UNC (0.84; 0.64)	-.37	-.03	.00	-.42	**.80**						
DOI (0.84; 0.73)	.04	.12	-.13	-.25	.59	**.86**					
IMI (0.93; 0.81)	.68	.37	.13	.56	-.24	.19	**.90**				
SW (.86;.68)	.10	.21	.04	.06	.16	.20	.22	**.82**			
ModRE (0.93; 0.83)	.46	.16	.10	.33	-.15	.08	.39	.15	**.91**		
CONT (0.97; 0.92)	.41	.18	.10	.31	-.07	.11	.41	.24	.85	**.96**	
ModIMI (0.93; 0.83)	.48	.25	.08	.23	.02	.32	.53	.36	.62	.67	**.91**

Table F2. Factor Loadings after Dropping Items

Construct	Item	Loading
Threat susceptibility	TSUS1	.72
	TSUS2	.75
	TSUS3	.86
Threat severity	TSEV1	.89
	TSEV3	.92
Response efficacy	RE1	.87
	RE2	.89
	RE3	.76
Perceived uncertainty	UNC1	.80
	UNC3	.85
	UNC4	.74
Discounting one's own information	DOI1	.90
	DOI2	.81
Imitation	IMI1	.90
	IMI2	.91
	IMI3	.89
Switching costs	SW1	.76
	SW2	.85
	SW3	.86
Modified response efficacy	ModRE1	.94
	ModRE2	.88
	ModRE3	.91
Continuance intention	CONT1	.95
	CONT2	.95
	CONT3	.98
Modified imitation	ModIMI1	.87
	ModIMI2	.93
	ModIMI3	.92
Protection motivation	B1	.94
	B2	.94
	B4	.95

Appendix G. Effect Sizes for the Herd-Related Factors

To calculate the effect sizes for the herd-related factors, we ran a partial model without these factors (only PMT constructs) and compared it with the full model (including both PMT and herd-related constructs) to assess the effect sizes, using Cohen's f^2 formula. As shown in Table G-1, the size of the effect of herd-related factors on protection motivation is medium (.29) for the treatment group, whereas it is small for the control group (0.04). Effect size (f^2) is calculated by the formula (R^2 *full* – R^2 *partial*) / (*1* – R^2 *full*). An effect size of 0.02, 0.15, and 0.35 as are defined as small, medium and large effect sizes respectively (Cohen 1988).

Table G1. Effect Sizes

Control group			Treatment group		
Partial model R^2	**Full model R^2**	**Effect size**	**Partial model R^2**	**Full model R^2**	**Effect size**
.35	.39	.04	.39	.54	.32

Appendix H. Construct Development and Validation Results

Table H1. Reliability Analysis

Construct	Alpha	Square multiple correlation	
Modified response efficacy	.93	ModRE1	.79
		ModRE2	.73
		ModRE3	.76
Modified imitation	.93	ModIMI1	.70
		ModIMI2	.78
		ModIMI3	.78

Table H2. Response Efficacy vs. Modified Response Efficacy (PCA)

Item	Factor 1	Factor 2
RE1		.88
RE2		.91
RE3		.85
ModRE1	.94	
ModRE2	.92	
ModRE3	.93	
Notes: Values less than 0.4 are suppressed. Varimax rotation		

Table H3. Imitation vs. Modified Imitation (PCA)

Item	Factor 1	Factor 2
IMI1		.90
IMI2		.90
IMI3		.91
ModIMI1	.90	
ModIMI2	.91	
ModIMI3	.91	
Notes: Values less than 0.4 are suppressed. Varimax rotation		

About the Authors

Ali Vedadi is an assistant professor of information systems and analytics at Middle Tennessee State University. His research is focused on behavioral IS security, IS post-adoption, and social influence. His research has appeared in the *DATA BASE for Advances in Information Systems*, *Computers & Security*, *AIS Transactions on Replication Research*, *International Journal of Process Management and Benchmarking*, and multiple international and national conference proceedings such ICIS and HICSS. He teaches information security and assurance courses at the undergraduate and graduate levels. He completed his doctoral studies at Mississippi State University.

Merrill Warkentin is a William L. Giles Distinguished Professor at Mississippi State University, where he serves as the James J. Rouse Endowed Professor of Information Systems in the College of Business. His research, primarily on the impacts of organizational, contextual, and dispositional influences on individual behaviors in the contexts of information security, privacy, and social media, has appeared in *MIS Quarterly*, *Journal of MIS*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Information Systems Journal*, *Decision Sciences*, *Information & Management*, and other journals. He is the author of 100 peer-reviewed journal articles and the author or editor of seven books. He has served in editorial roles for *MIS Quarterly*, *Information Systems Research*, *Journal of the Association for Information Systems*, *Decision Sciences*, *European Journal of Information Systems*, *Information & Management*, and other journals. His work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM, and other institutions.