Positively Fearful: Activating an Individual's HERO within to Explain Volitional Security Technology Adoption

Abstract

Regardless of what security professionals do to motivate personal users to adopt security technologies volitionally, the end-result seems to be the same – low adoption rates. To increase these rates, we propose activating their positive psychological capital (PsyCap), which consists of hope, self-efficacy, resilience, and optimism (i.e., their HERO within). We argue that greater PsyCap towards the security technology will be associated with greater adoption rates (and intentions thereof) because positivity increases motivation. We further posit that PsyCap will be both a moderator and be moderated by other constructs. We propose a personal user's conditioned fear from the security threat will moderate the effect of PsyCap on adoption intentions because some fear is necessary to activate their positive PsyCap to form their behavioral intentions to adopt security technologies. We further hypothesize that PsyCap will moderate the effect of adoption intentions on actual adoption rates because activating an individual's HERO within encourages individuals to exert the effort necessary to translate their intentions into actual adoption. Finally, we theorize that enhancing fear-appeal messages with appeals to an individual's HERO within will have a greater effect on volitional adoption rates relative to messages without these PsyCap-related appeals. To support our hypotheses, we conducted two experiments using the volitional adoption of a password manager application and a two-factor authentication (2FA) service. We found differential support for our hypotheses across the two security technologies, which suggests technology characteristics might mitigate the impact of PsyCap on volitional adoption decisions.

Keywords: Behavioral information security, psychological capital, conditioned fear, fear-appeals, positive psychology, volitional security actions, password manager applications, and 2FA services

1. INTRODUCTION

Motivating personal users to adopt a security technology volitionally often feels like an impossible task, especially if it requires any amount of implementation effort (Anderson & Agarwal, 2010; Liang, Xue, Pinsonneault, & Wu, 2019). Google recently reported that only 10% of their email accounts used two-factor authentication (Iyer, 2018). Given that this free and easy to activate security feature had such low adoption rates, security technologies that cost money and take effort to implement will likely see even less adoption. To increase adoption rates, security professionals have tried many tactics such as awareness campaigns and different fear-appeal messages (Dincelli & Chengalur-Smith, 2020; Herath et al., 2012; Johnston & Warkentin, 2010).

Seemingly, however, the end result of these different tactics is inevitably the same – low volitional adoption rates (Bélanger & Crossler, 2019; Chenoweth, Gattiker, & Corral, 2019). The literature has proposed many possible explanations for these low adoption rates such as a lack of awareness of the problem or potential solutions, low self-confidence, high perceived implementation costs relative to benefits, minimal trust in the security defense mechanisms, and low perceived likelihood of the threat materializing (Chen & Zahedi, 2016; Herath et al., 2012; Liang & Xue, 2010; Ng, Kankanhalli, & Xu, 2009; Tsai et al., 2016; Tu, Turel, Yuan, & Archer, 2015). On paper, these explanations make logical sense. In practice, however, the application of many of these variables has not translated into any meaningful increase in the volitional adoption rates of security technologies (Bélanger & Crossler, 2019; Seo & Park, 2019).

Even when personal users are aware of the threat landscape, they are still generally apathetic about implementing a security technology today to potentially reduce losses in the future (Y. Lee & Kozar, 2005; Stafford & Poston, 2010). We suggest incorporating more positive psychology in fear-appeal messages might reduce this user indifference towards security technologies. Focusing on, say, hope and resilience in addition to fear and vulnerability may be helpful because hope and resilience are a part of a positive appraisal of the circumstances, which has been demonstrated to motivate individuals to perform many behaviors (Luthans, Avolio, Avey, & Norman, 2007). The behavioral security literature, however, has yet to investigate these tactics in the personal computing context. As such, we investigate the following research question:

> **RQ**: Do positive constructs or positive stimuli increase, decrease or have no impact on the volitional adoption of security technologies for personal users?

To address this research question, we use psychological capital (PsyCap), which is a higher order construct comprised of hope, self-efficacy, resilience, and optimism (i.e., an individual's HERO within) (Luthans, Vogelgesang, & Lester, 2006). Activating an individual's HERO within regarding an action promotes positive thought patterns towards the behavior, which may increase an individual's control over an action (Culbertson, Fullagar, & Mills, 2010; Luthans, Youssef, & Rawski, 2011). Therefore, PsyCap may encourage individuals to persevere under challenging circumstances (Luthans & Broad, 2022).

We specifically propose that greater PsyCap regarding the security technology will be associated with greater volitional adoption rates (and intentions thereof) because hopeful, efficacious, resilient, and optimistic personal users are more likely to persist through mindful security adoptions. We further posit that PsyCap will be both a moderator and be moderated by other constructs. We propose a personal user's conditioned fear from the security threat will moderate the effect of PsyCap on behavioral intentions because some conditioned fear is necessary to activate their positive PsyCap to form their behavioral intentions to adopt security technologies. Without a conditioned fear of the threat, personal users have minimal need to activate their HERO within to form their intentions to adopt a security technology to defend against a threat that they are not scared of. We also theorize that PsyCap will moderate the effect of adoption intentions on actual adoption rates because activating an individual's HERO within encourages personal users to exert the effort necessary to translate their intentions into actual adoption. Higher levels of PsyCap give individuals a sense of agency over actions (Culbertson, Fullagar, & Mills, 2010), which may make up for low adoption intentions or amplify the likelihood of following through on their high adoption intentions.

As a result of these proposed PsyCap effects, we hypothesize that enhancing fear-appeal messages with appeals to a personal user's HERO within toward the action will have a greater effect on increasing volitional adoption rates (and intentions thereof) relative to messages without PsyCap enhancements. To test our research conjectures empirically, we conducted two experiments using two volitional security actions: 1) password manager applications (i.e., applications that administer passwords across multiple websites) and 2) two-factor authentication (2FA) services (i.e., service requiring users to enter two pieces of information for verification). Across both experiments, we found that our high PsyCap experimental groups had greater adoption rates (and intentions thereof) relative to our control groups. We also found that our participants' level of conditioned fear moderated the impact of PsyCap on 2FA adoption intentions. Finally, we found that PsyCap moderated the effect of adoption intentions on actual adoption rates for the 2FA study only.

We make several notable contributions to the behavioral information security literature. First, without the positive motivator (PsyCap in our case), a personal user might not adopt a security technology to defend against a threat that they are sufficiently afraid of (i.e., “I am scared of a data breach but I fail to defend myself because I am pessimistic, not hopeful, not efficacious, and not resilient concerning the adoption of the technical defense mechanism”). The behavioral security literature has typically used self-efficacy in this manner but PsyCap is a richer positive construct that includes three additional positive resources that work in tandem with one another. Second, the prior literature has reported mixed results for the impact of fear on many security behaviors (Boss, Galletta, Lowry, Moody, & Polak, 2015; Chen et al., 2021; Posey, Roberts, & Lowry, 2015). We first suggest that the fear construct used in the behavioral security literature is primarily conditioned fear, which is different from the fear construct used in the health literature. We then argue and demonstrate empirically that conditioned fear might be contingent on a personal user’s level of PsyCap. Third, we contribute to the recent literature on the design of fear-appeal messages. Our results reveal that a fear-appeal message that appeals to an individual’s HERO within in addition to including specific threats and coping mechanisms that are personally relevant can positively increase adoption rates (and intentions thereof). Finally, we contribute to the fear-appeal model (FAM) literature by introducing the PsyCap construct as a potential replacement for self-efficacy and the moderating effect of conditioned fear. We further demonstrate that PsyCap could be a construct that helps explain the path between adoption intentions and actual behaviors in the FAM. Our results also suggest that our PsyCap effects in the FAM might be contingent upon the type of security technology being adopted.

2. LITERATURE REVIEW

Unlike employees in organizations, personal users do not have formal training programs, employer mandates, and social pressures from coworkers to encourage security actions (Aurigemma & Mattson, 2019; Liang & Xue, 2009; Thompson, McGill, & Wang, 2017). Therefore, personal users must decide what security actions to take completely volitionally. To explain personal user’s volitional security decisions, behavioral security researchers have used protection motivation theory (Boss et al., 2015; Tsai et al., 2016; Tu et al., 2015), the theory of planned behavior (Y. Lee & Kozar, 2005), technology threat avoidance theory (Lai, Li, & Hsieh, 2012; Liang & Xue, 2010), the fear appeals model (Johnston & Warkentin, 2010), and the health belief model (Ng et al., 2009). From these theories (and extensions thereof), we have learned that a lack of awareness of threat landscape along with available coping mechanisms, minimal efficacy, high perceived implementation costs relative to benefits, low perceived threat-related attributes, and the design of fear-appeal messages impact a personal user’s decisions to adopt security technologies (Anderson & Agarwal, 2010; Chen & Zahedi, 2016; Herath et al., 2012; Liang & Xue, 2010; Ng et al., 2009; Schuetz, Lowry, Pienta, & Thatcher, 2020; Tsai et al., 2016; Tu et al., 2015).

Liang et al. (2019) note that much of the literature takes a problem-solving approach to explain personal user’s security decisions. However, personal users also act based on their emotional responses to threats (Liang & Xue, 2009; Liang et al., 2019). Individuals may be more or less susceptible to a security threat depending on their emotional coping strategies (Arachchilage & Love, 2014; Liang et al., 2019, Xin, Siponen & Chen, 2021). The challenge with emotions is their instability (i.e., individuals may go from happy to sad in moments) (Luthans & Youssef-Morgan, 2017). Therefore, designing fear-appeal messages to only stimulate emotions might be problematic. Instead, appealing to an individual's trait-like or state-like characteristics that are more stable (but still moldable) might be a better (albeit untested) approach.

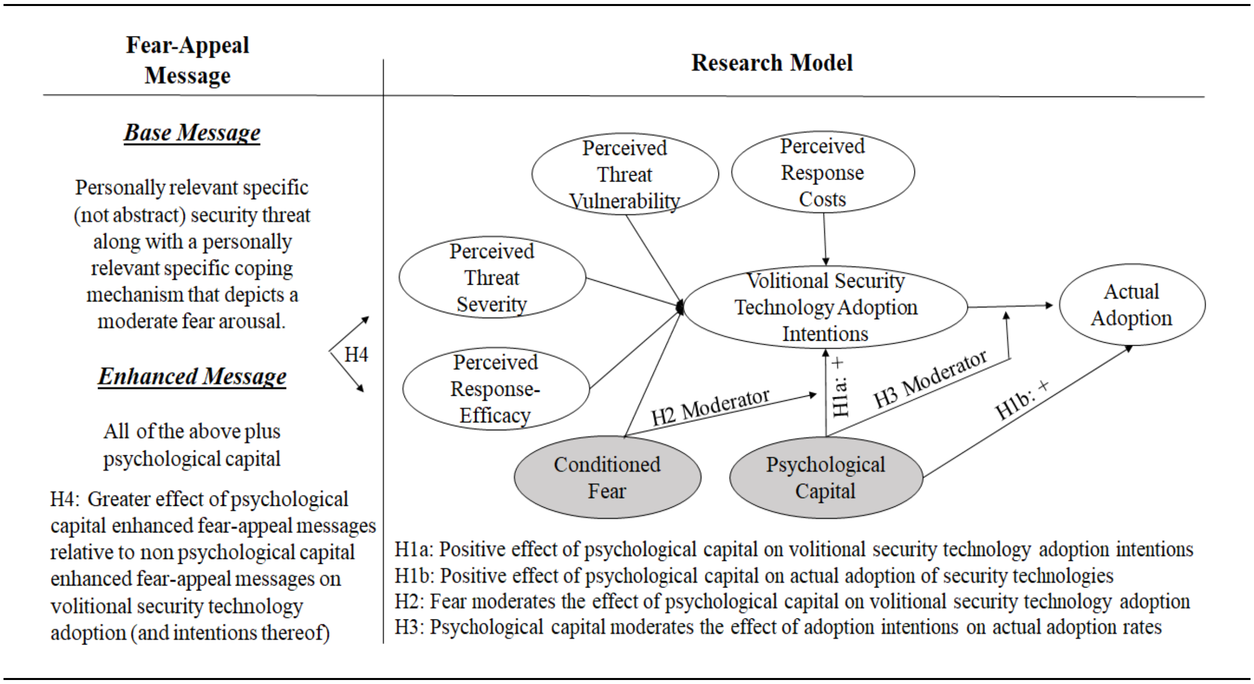
Prior security literature reports that arousing fear in personal users increases security actions (or intentions thereof) (Boss et al., 2015; Jenkins, Grimes, Proudfoot, & Lowry, 2014). Jenkins et al. (2014), for instance, found that high depicted fear in fear-appeal messages reduced the propensity to reuse passwords. Boss et al. (2015) also found that high fear arousals increased the volitional adoption of data backups and anti-malware. These results suggest that inducing a fear response concerning the adverse impact of a threat may increase a personal user's tendency to perform security actions. Fear is also fleeting (Beaudry & Pinsonneault, 2010). For instance, an individual may be fearful of identity theft today but significantly less fearful tomorrow, which might hinder their propensity to take precautionary actions to guard against identity theft.

Self-efficacy (i.e., an individual's belief that they are capable of performing an action) is a strong antecedent of personal users' volitional security behaviors (Chen & Zahedi, 2016; Herath et al., 2012; Tu et al., 2015). Self-efficacy is a positive construct that is related to an individual's self-confidence and perceived control over an action (Luthans & Youssef-Morgan, 2017). If a single positive construct (self-efficacy) is so strongly associated with security actions, then other positive constructs might also have strong effects. One additional positive construct is PsyCap, which is a logical extension to this literature because self-efficacy is a core PsyCap component. PsyCap has been used in the behavioral compliance literature (Burns, Posey, Roberts, & Lowry, 2017; Burns, Roberts, Posey, & Lowry, 2019), but it has yet to be investigated in the context of volitional technology adoption decisions for personal users.

3. RESEARCH HYPOTHESES

PsyCap is our primary construct of interest. We hypothesize about the following: 1) the main effect of PsyCap on volitional adoption rates (and intentions thereof), 2) how conditioned fear of the threat moderates the effect between PsyCap and adoption intentions, 3) how PsyCap moderates the effect of adoption intentions and actual adoption, and 4) how PsyCap enhanced fear-appeal messages impact a personal user's volitional adoption of security technologies (and intentions thereof). PsyCap may be evaluated independently as a stand-alone construct. Our last hypothesis, however, theorizes about the effect of a PsyCap enhanced fear-appeal message. Therefore, the most appropriate nomological net for our hypotheses is a fear-appeals model (FAM) (Johnston et al., 2015, 2019; Warkentin et al., 2016).

The FAM includes five perceptions that individuals form in response to a fear-appeal message. That is, if an individual engages with the content of and the arguments presented in a fear-appeal message, they will form perceptions related to the threat (susceptibility and vulnerability), response costs, and efficacy (response and self) based on the quality of the fear-appeal message. In turn, those perceptions are hypothesized to influence behavioral intentions to take security actions. Finally, those behavioral intentions are proposed to positively impact actual adoption rates (i.e., individuals first form intentions to act and then they act primarily based on those intentions). Several proposed mediating effects among these FAM constructs have been proposed in the literature but the empirical evidence and theoretical development of those effects are still emerging (Orazi, Warkentin, & Johnston, 2019; Johnston et al., 2019). Therefore, we use a main-effects only FAM model as the nomological net for our proposed relationships (see Figure 1).



Personally relevant specific (not abstract) security threat along with a personally relevant specific coping mechanism that depicts a moderate fear arousal.

All of the above plus psychological capital

H4: Greater effect of psychological capital enhanced fear-appeal messages relative to non psychological capital enhanced fear-appeal messages on volitional security technology adoption (and intentions thereof)

H1a: Positive effect of psychological capital on volitional security technology adoption intentions
H1b: Positive effect of psychological capital on actual adoption of security technologies
H2: Fear moderates the effect of psychological capital on volitional security technology adoption
H3: Psychological capital moderates the effect of adoption intentions on actual adoption rates

Figure 1. *Research Hypotheses & Fear-Appeals Model Nomological Network*

We propose replacing self-efficacy with PsyCap in the FAM because PsyCap is a higher-order construct that includes self-efficacy as a lower order resource. Depending on the security technology being adopted, the relative importance of the different PsyCap resources may vary. For instance, certain security technologies might rely on a personal user's hope and resilience more heavily whereas others may rely more deeply on their self-efficacy and optimism towards the action to explain their volitional adoption decisions. Therefore, including just self-efficacy in the FAM may not capture the contextual differences between security technologies well enough. That is, PsyCap provides more theoretical flexibility to explain a wider variety of security technology adoption decisions.

Additionally, self-efficacy by itself may not be a rich enough construct to tease out the differential effect of conditioned fear on security adoption intentions. Chen et al. (2021) argue that different levels of self-efficacy determine the impact of fear arousals on security compliance and non-compliance inside of organizations. Outside of organizations, however, self-efficacy alone may not be enough because personal users have no organizational policies to follow or mandated training programs to take. Without these organizational factors, the inter-play or the synergistic effects of the four HERO PsyCap resources might be necessary to explicate how conditioned fear impacts security technology adoption.

3.1. Main Effect of Psychological Capital (PsyCap)

PsyCap was developed in the positive organizational behavior and positive psychology literature streams (Fredrickson, 1998; Gable & Haidt, 2005; Seligman & Csikszentmihalyi, 2000). These scholarly disciplines focus on the role of positivity in human functioning (Newman et al., 2014; Seligman & Csikszentmihalyi, 2000). Positive thought processes make employees more productive while also maximizing their job satisfaction (Avey et al., 2009; Culbertson et al., 2010; Luthans et al., 2011). Furthermore, employees with positive as opposed to negative thought patterns tend to demonstrate stronger citizenship behaviors inside and outside of their work environments (Avey, Reichard, Luthans, & Mhatre, 2011; Larson & Luthans, 2006).

Figure 2 displays the PsyCap construct. It is a higher-order construct containing the following resources: 1) hope, 2) self-efficacy, 3) resilience, and 4) optimism (i.e., an individual's HERO within) (Luthans, Vogelgesang, et al., 2006). These four first order components constitute a resource reservoir or caravan of resources that work synergistically to promote individual well-being (Hobfoll, 2011; Luthans & Youssef-Morgan, 2017). Removing one of these resources changes PsyCap's definition (Luthans, Vogelgesang, et al., 2006). PsyCap has proactive and reactive components that are inwardly and externally oriented (Luthans, Norman, Avolio, & Avey, 2008), which makes it relevant to security actions. Personal users, for instance, may take security actions after they have been compromised (reactive) but they may also install security technologies before they are adversely impacted by a cyberattack (proactive).

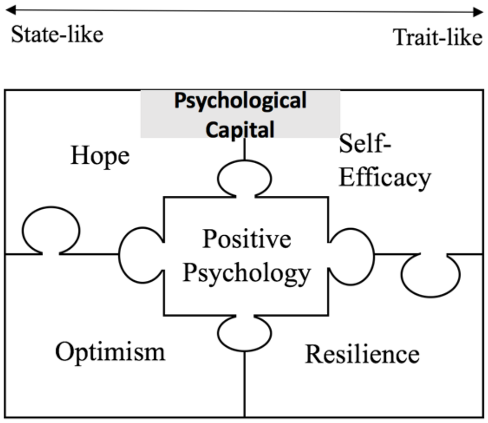


Figure 2. *First Order Components of Psychological Capital*

Hope is a positive motivational state based on goals and plans to meet those goals (Luthans et al., 2007; Luthans et al., 2011). In the context of volitional security actions, a goal for a personal user might be to not become the victim of a cyberattack that compromises one or more of their online accounts. The plan to meet that goal may be to create strong passwords that are not reused across multiple websites along with practicing safe internet surfing habits. In general, hope increases an individual's perception that they have the ability to implement a security technology because hope implies an expectation that a positive event will happen after a goal and pathway (or multiple pathways) have been identified (Snyder & Rand, 2003).

Self-efficacy represents an individual's belief that they are capable of performing a specific behavior (Bandura, 1986). It requires a strong belief in one's abilities, cognitive strengths, and capacities to persevere to complete specific tasks (Luthans, Vogelgesang, et al., 2006). Self-efficacy has been applied to many contexts with the general idea being that more self-efficacy is better than less (Luthans & Youssef-Morgan, 2017). Behavioral security researchers have used self-efficacy extensively to explain the variance in security behavioral intentions inside and outside of organizations because forming intentions to act securely often requires a strong belief in one's ability to persist through obstacles (Rhee, Kim, & Ryu, 2009).

Resilience is the capacity to bounce back from negative events and to grow from positive events (Luthans, 2002a, 2002b). Resilient individuals are generally unphased by failure and often use negative events to become stronger (Linnenluecke, 2017; Shin, Taylor, & Seo, 2012). Resilience involves deploying positive adaptation patterns to overcome adversities (Masten, 2001). In our security context, a resilient personal user is one who does not get discouraged when their machine gets infected with a virus or when one of their accounts gets compromised. This resilient user would learn from these negative events to prevent these issues from happening again. Resilience is a state that can be primed via effective communications (Linnenluecke, 2017; Masten, 2001).

Optimism is an explanatory style that explains outcomes in terms of positive variables (Peterson, 2000). An individual with an optimistic explanatory style explains positive events as a function of their actions and negative events as context-specific (Luthans et al., 2007; Luthans & Youssef-Morgan, 2017; Peterson, 2000). Optimistic reasoning considers positive events as permanent and negative events as temporary, which is the opposite for pessimistic reasoning (Li, Fay, & Frese 2019; Peterson, 2000). In our security context, a personal user with an optimistic explanatory style would consider getting a virus on their personal device (negative event) as an external, temporary, or situation-specific factor. This same optimistic personal user would explain why their accounts have remained secure in terms of their personal decisions regarding proper password management. An individual with an optimistic explanatory style expects good things to happen as a result of their choices (Luthans, Vogelgesang, et al., 2006; Peterson, 2000). Security professionals generally want individuals who have an optimistic explanatory style because optimistic individuals can be convinced to act securely by promoting the importance of their individual choices.

PsyCap is a psychological state that contains trait-like and state-like resources (Luthans, Vogelgesang, et al., 2006). In this manner, PsyCap is "malleable and open to development but relatively more stable than, for example, emotions" (Luthans & Youssef-Morgan, 2017, p. 344). Psychological states are not characteristics such as the Big 5 personality traits (which are relatively fixed once developed) or emotions (which can change from moment-to-moment) (Luthans & Youssef-Morgan, 2017; Luthans et al., 2011). In essence, psychological states fall between stable characteristics and volatile emotions if those are plotted on opposite ends of a continuum. Individuals, however, may "become more positive, and sustain positivity over time, which is consistent with the state-like conceptualization of PsyCap" (Luthans & Youssef-Morgan, 2017, p. 345). Hope, for instance, may be developed whereas emotions cannot be developed (only stimulated) (Masten, 2001; Schneider, 2001).

Managing a personal user's PsyCap in our security context is similar to managing players on a sports team. Most sports teams along with the players on those teams go through a series of highs (successes) and lows (failures). An effective coach focuses on the positives to help the individual players and the team succeed, especially during turbulent times. Focusing on the positive means communicating reasons to be optimistic and hopeful while teaching resilience and instilling self-confidence (self-efficacy). Fixating exclusively or mostly on the negatives (i.e., the team's current losing streak or a player's current performance slump) may be a self-fulfilling prophecy that leads to even worse results. In the security context, individuals also have a series of successes (e.g., anti-virus software stopped a virus from being installed) and failures (e.g., fell victim to a phishing scam). Unfortunately, the failures are significantly more memorable than the successes. That is, individuals tend to remember the time when their system was infected with a virus more vividly than the time when their anti-virus software prevented a virus from infecting their system.

We suggest that security professionals who focus mostly on the negatives (i.e., the inevitability that one's personal information will be compromised) promote inaction and low behavioral intentions to adopt security technologies proactively. This strategy encourages a pessimistic explanatory style with no hope that a personal user's choices will do anything to protect themselves from the current cybersecurity threats. Conversely, security professionals who focus more on the positives (i.e., providing individuals with reasons to be hopeful about the current protective technologies available) promote an action-oriented environment for personal users. In this more positive and optimistic framing, we argue that personal users may develop a sense of control and agency over protecting themselves, which increases both intentions to adopt security technologies volitionally and actual adoptions. We posit that focusing on infectious positivity ("you can do this") will promote more secure behaviors (and intentions thereof) relative to focusing on infectious negativity ("you are doomed regardless what you do"). That idea is one of the central ideas of PsyCap (Luthans, Avey, Avolio, Norman, & Combs, 2006; Luthans & Youssef-Morgan, 2017). As such, we hypothesize the following main effect of PsyCap:

H1a: Greater PsyCap will be associated with greater volitional adoption intentions of security technologies.

H1b: Greater PsyCap will be associated with greater actual volitional adoption of security technologies.

3.2. Moderating Effect of Conditioned Fear

Fear is a "negatively-valanced emotion, accompanied by a high arousal, and is elicited by a threat that is perceived to be significant and personally relevant" (Witte, 1992, p. 331). Rogers (1975, p. 96) similarly proffers that fear is "aroused in response to a situation that is judged as dangerous." These fear definitions pose an interesting question: how can fear be conceptualized as a negatively-valanced emotion but also involve perceptions and judgments that are cognitively based? Many information systems scholars argue that emotions and cognitions have different mechanisms and processes thereby making them distinct (Beaudry & Pinsonneault, 2010; Liang et al., 2019; Xu, Luo, & Hsu, 2020). That is, the general viewpoint in the information systems literature is that individuals act based on either their emotions or their cognitions.

To resolve this apparent contradiction with these fear definitions, we consider Scherer's (2005) model of emotions. In this model, he argues that there are five elements of emotions that happen sequentially: 1) cognitive appraisals of events and situations, 2) bodily symptoms or the physiological components, 3) action response tendencies, 4) physical expressions, and 5) subjective feelings. Notably, his first proposed process is a cognitive appraisal, which strongly suggests that emotions and cognitions are not distinctly different processes as has been argued in the information systems literature. Conceptualizing fear through Scherer's (2005) model means that fear contains a cognitive component (i.e., at least some overlap in the processes between cognitions and emotions). This theoretical insight may help explain why a subset of behavioral security scholars have included fear in traditionally cognitive-based theories to explain non-avoidance security actions (c.f., Boss et al, 2015; Chen et al., 2021; Posey et al., 2015).

Fear drives individuals toward a set of behaviors to cope with their fear arousals, which may disrupt rational decision making and promote risk-averse behaviors (Beaudry & Pinsonneault, 2010; C. J. Lee & Andrade, 2011; de Hoog, Stroebe, & de Wit, 2007). In general, individuals act to reduce their fear to restore their emotional balance (de Hoog et al., 2007; Hebb, 1946). In the behavioral information security literature, scholars propose that individuals resolve their fear arousals from security threats with either fear control or danger control processes (Johnston & Warkentin, 2010; Liang & Xue, 2010). A fear control process is a type of maladaptive coping whereby individuals mitigate their fear by avoiding the threat that caused their fear arousal (Witte, Cameron, Mckeon, & Berkowitz, 1996). Contrarily, a danger control process is a type of adaptive coping whereby individuals take remedial actions to reduce (not avoid) the threat that caused their fear arousal (Witte et al., 1996). In the behavioral security context, whether individuals employ a fear control or a danger control process depends on their appraisal of the threat and their perceived ability to cope with the threat that caused their fear (Johnston & Warkentin, 2010; Johnston et al., 2015). It is difficult to avoid online threats in everyday technology use, which makes fear control processes unproductive. Danger control processes, however, might lead to more productive outcomes such as adopting security technologies proactively (Johnston & Warkentin, 2010).

Too much fear from a security threat might trigger a fear control process, which may result in users questioning the signals that caused their fear arousals and taking no security actions (Chen et al., 2021; Moody et al., 2018). That is one of the primary reasons why early research on fear suggested an inverted U-shaped relationship between fear and precautionary actions (Witte & Allen, 2000). Advocates of this school of thought argued that fear could have both facilitating and inhibiting effects on precautionary actions, which suggested that moderate levels of fear might have the greatest effect on attitudes and precaution taking (Janis & Feshbach, 1953; Witte & Allen, 2000). Despite the logical nature of this argument, there has been minimal empirical evidence supporting this curvilinear relationship (Witte & Allen, 2000).

The lack of empirical support for this inverted U-shaped relationship across many actions could stem from the source or context of the fear arousal. It is possible that not all fear arousing events are the same. We argue that fear as used in the behavioral information security literature has similarities but also differences from fear as used in other disciplines. For example, individuals cannot learn how to respond to or prepare themselves for a fear arousing event such as being told that they have a deadly illness or encountering an armed criminal late at night. Those types of fear arousing events involve immediate physical danger or even death. We cannot imagine any type of adverse information security event that could arouse fear in that manner. However, that does not mean fear (in some form) is unimportant for personal user's security technology decisions.

We proffer that fear in a security context is learned over time similar to a generalized fear of crime (Houts & Kassab, 1997; Mears & Stewart, 2010) or a generalized fear of death (Mitchell & Schulman, 1981). Societies, educational systems, families, and other factors condition individuals to be scared of such phenomena as death and crime (Houts & Kassab, 1997). Moreover, a fear arousal from a generalized fear of crime does not elicit the same type of physiological fear arousal as almost getting into a car accident but both involve fear. Similarly, security professionals and news organizations condition mindful personal users to be afraid of and how to respond to fear arousals from threats such as malware, ransomware, and identity theft. It is fear in line with the aforementioned definitions by Witte (1992) and Rogers (1975) but it is different from fear in health or physically dangerous situations. As a result, we refer to fear in the information security context as conditioned fear. We define conditioned fear as a generalized fear arousal originating from information security threats. It may be triggered or stimulated by a specific event or communication message but it does not elicit an arousal as sharp as a stimulus that poses an immediate physical danger.

We posit that personal users must have some level of hope, efficacy, resilience, and optimism concerning their ability to implement a security technology to mitigate their conditioned fear of security threats. As a result, PsyCap and conditioned fear emanating from security threats do not work in isolation from one another. We consider four possibilities: 1) high PsyCap and high conditioned fear, 2) high PsyCap and low conditioned fear, 3) low PsyCap and low conditioned fear, and 4) low PsyCap and high conditioned fear.

If a personal user has high PsyCap about adopting a password manager application but has no conditioned fear from the compromised accounts threat, then they will have a relatively low behavioral intentions to adopt a password manager application. Without some fear from the adverse effects of the threat, a personal user may logically have no need to activate their high PsyCap to adopt a security technology for a threat that induces a low fear arousal. Logically, this combination would result in a relatively low behavioral intention to adopt the security technology. Conversely, if the threat elicits a strong conditioned fear response, then we posit that the impact of high PsyCap will be amplified because these individuals are hopeful, efficacious, resilient, and optimistic concerning their ability to mitigate a threat that they are sufficiently afraid of with a security technology. This strong fear arousal will activate a high PsyCap personal user's HERO within toward the mitigating action to adopt the security technology (or at least to form strong behavioral intentions to do so).

A personal user with low PsyCap and minimal conditioned fear originating from the threat is arguably the worst combination. In this case, neither their conditioned fear nor PsyCap is strong enough to drive the personal user to develop high behavioral intentions to adopt the security technology volitionally. This combination is one where the personal user is not efficacious, hopeful, resilient or optimistic regarding their ability to mitigate a threat that they are not scared of. Not surprisingly, we theorize that such a combination would result in minimal behavioral intentions to adopt a security technology volitionally. However, a strong fear arousal coupled with low PsyCap is also problematic. In this case, the personal user might engage in a fear control instead of a danger control process partially due to their low PsyCap. Said differently, these personal users might be so overcome with their conditioned fear but not have enough HERO within to mitigate the threat causing their strong fear arousal that they develop minimal intentions to take any preventative actions. Consequently, these personal users might be subject to a fear control process instead of a danger control process to restore their emotional equilibrium. Therefore, we hypothesize the following moderating effect of conditioned fear on PsyCap:

H2: Conditioned fear moderates the effect of PsyCap on the volitional adoption intentions of security technologies.

3.3. Moderating Effect of PsyCap on Actual Adoption

Hypothesizing about increasing a personal user's volitional adoption intentions is important but increasing actual adoption rates is the ultimate goal. Therefore, we now consider the potential effect of PsyCap on the structural path between adoption intentions and actual adoption rates. From the cross-disciplinary literature investigating the path between intentions and actual behaviors, we know that individual-level characteristics (e.g., Big 5 personalities, attitudes, and general cognitive beliefs), attributes of the intention (e.g., general versus specific), the type of behavior (e.g., single action versus multiple action behaviors), and behavioral control over the outcome impact the propensity of individuals following through on their adoption intentions (Gollwitzer & Sheeran, 2006; Sheeran, 2002; Sheeran & Webb, 2016). PsyCap is an individual-level construct. Higher levels of PsyCap are associated with positive attitudes, perseverance, perceived control, and agency over actual behaviors (Luthans & Youssef-Morgan, 2017; Luthans et al., 2007; Luthans et al., 2011), which suggests that higher PsyCap levels might facilitate the translation of intentions into actual security actions such as volitionally adopting security technologies.

The relationship between intentions and actual behaviors has not received much attention in the behavioral security literature. This lack of attention may be the result of the theories used in this stream of research. Many of the theories used by behavioral security scholars specifically explain the variability in behavioral intentions or motivation intentions, which are then theorized to be positively associated with actual actions with a single unmoderated and unmediated path (Johnston & Warkentin, 2010; Y. Lee & Kozar, 2005; Ng et al., 2009; Tsai et al., 2016). Two notable exceptions that we found are Crossler et al. (2014) and Jenkins et al. (2021) who both found that the effort associated with the security-related action moderated the path between intentions and security actions. PsyCap is related to effort because greater PsyCap promotes perseverance during tasks that require effort to complete (Luthans & Youssef-Morgan, 2017; Luthans et al., 2011).

Let's consider the potential effect of PsyCap for personal users who have low and high adoption intentions for a security technology. If intentions are a necessary precondition for actual behaviors (Ajzen, 1991), then personal users with low adoption intentions should have a low likelihood of actually adopting the security technology. In this situation, there is not much that can be done to change their minds about adopting the security technology volitionally (i.e., their low intentions mean they probably have already decided to not act). However, activating their HERO within regarding the action may help increase adoption rates for these low intention individuals. We still expect low overall adoption rates for those personal users who have low adoption intentions, but we expect higher PsyCap to be better than lower PsyCap due to the positive benefits associated with hope, efficacy, resilience, and optimism.

On the opposite end of the continuum, personal users may have high adoption intentions. In a perfect world, individuals will not need any added encouragement to act on their high adoption intentions (Ajzen, 1991). However, the reality is that most individuals fail to actually act on their high intentions across all types of actions (Jenkins et al., 2021; Sheeran & Webb, 2016). Sheeran (2002) notes that most of the explained variance in actual behaviors across a variety of behaviors is not explained by adoption intentions. The literature demonstrates that self-efficacy alone does not always moderate the effect of adoption intentions on actual adoption rates but a few studies have demonstrated positive effects of self-efficacy (Sheeran, 2002; Sheeran & Webb, 2016). We proffer that the different reported evidence for self-efficacy might be due to needing a richer positive construct to explain the variability associated with different actions in the security context.

As such, we propose that PsyCap has the potential to moderate this path for high intentioned personal users because it includes additional positive resources beyond just efficacy. That is, activating a personal user's HERO within regarding the action has the potential to convince them to actually act on their high intentions because a positive mindset about the technology might help individuals put forth the necessary effort to act on their high adoption intentions. Contrarily, personal users with low PsyCap have more negative attitudes, which reduces the likelihood of following through on their high adoption intentions (Luthans & Youssef-Morgan, 2017, Sheeran & Webb, 2016). Therefore, we hypothesize the following moderating effect of PsyCap:

> H3: PsyCap moderates the effect of volitional adoption intentions of security technologies on actual adoption rates.

3.4. Effect of PsyCap Enhanced Fear-Appeal Messages

A fear-appeal message is "a persuasive communication that attempts to arouse fear in order to promote a precautionary motivation and self-protective action" (Ruiter, Kessels, Peters, & Kok, 2014, p. 65). There is no singe theory responsible for the design of fear-appeal messages. Instead, a collection of theories across multiple disciplines have contributed to the body of knowledge related to the development of effective fear-appeal messages (Johnston et al., 2019; Williams, 2012). Therefore, we cite a variety of literature and theoretical perspectives to develop our hypothesis related to PsyCap enhanced fear-appeal messages.

Effective fear-appeals should stimulate two processes: 1) a threat appraisal and 2) a coping response. The threat appraisal is an individual's assessment of the personal vulnerability and severity of a threat while the coping response is their assessment of the perceived effectiveness of the potential responses along with their ability to undertake those responses (Johnston & Warkentin, 2010; Johnston et al., 2015). If a fear-appeal has a well-articulated description of the threat without an associated recommended coping mechanism (and vice versa), then that fear-appeal will probably be unsuccessful (Johnston et al., 2019; Witte, 1998). Successful fear-appeal messages can activate precautionary actions even with small levels of depicted fear in the message (Gore & Bracken, 2005; Ruiter et al., 2014). However, fear-appeals with excessively high scare tactics even when coupled with recommended coping mechanisms generally do not result in the desired behaviors (Gore & Bracken, 2005; Witte, Meyer, & Martell, 2001).

In an information security context, an effective fear-appeal message that engages individuals and convinces them to perform the security behavior outlined in the message must make a few key arguments (Johnston et al., 2019; Johnston et al., 2015; Johnston & Warkentin, 2010; Schuetz et al., 2020). First, the message must effectively argue that the threat outlined in the message is severe enough to warrant action. If a personal user is not convinced that the threat is severe enough to act upon, then they will have a low likelihood of complying with the recommended security actions. Second, the message must convince the audience that the threat is personally relevant. Without personal relevancy, it is difficult to convince an individual to take the prescribed security action (i.e., "threat is not related to me so I do not have to act"). Third, the fear-appeal message must effectively argue that the prescribed coping mechanism to counteract the threat is both effective and low cost. If a security-action requires too much effort to implement (i.e., high cost) and is only partially effective at mitigating the threat, then it is going to be challenging to convince individuals to take the recommended security action. Finally, an effective security fear-appeal message must convince individuals that they are capable of performing the coping mechanism. This part of the message has historically focused on appeals to an individual's self-efficacy but we propose broadening this to include appeals to all four PsyCap resources.

Schuetz et al. (2020) note that the behavioral information security literature has reported inconsistent results for similarly designed fear-appeal messages. There are several plausible explanations for these inconsistent findings. First, fear-appeal messages have been tested with both employees in organizational contexts and personal users. Employees and personal users may have different interest levels in information-security, which could impact whether they pay attention and engage with similar fear-appeal messages (Johnston et al., 2016; 2019; Schuetz et al., 2020). Second, it could be that a (conditioned) fear-response from the depicted fear in a fear-appeal message is idiosyncratic resulting in different levels of (conditioned) fear and adaptive (or maladaptive) responses (LaTour & Rotfeld, 1997). Therefore, matching messages to the characteristics (e.g., disposition, situational, and personality characteristics) of each individual might be necessary (albeit challenging to implement) to maximize the effectiveness of the fear-appeal messages (Johnston et al., 2019; Johnston et al., 2016). Third, fear-appeal messages may need to be developed for specific (e.g., "you need to implement a password manager") as opposed to general ("you need to practice sound identity management practices") security actions (Schuetz et al., 2020). Overly generic fear-appeal messages may not draw the attention of different audiences in a consistent manner.

Given the prior literature on the design of fear-appeal messages, we argue that an effective fear-appeal for personal users to adopt a security technology volitionally should include the following: 1) personally relevant specific (as opposed to general) threat with moderate depicted conditioned fear, 2) personally relevant specific (as opposed to general) coping mechanism, and 3) PsyCap motivational components related to the specific coping mechanism. Personal relevancy has been identified as one of the most important characteristics of successful fear-appeal messages because the target audience must find the threat and coping mechanism to be personally relevant to elicit the security action (Johnston et al., 2019; Johnston et al., 2016; Schuetz et al., 2020). We suggest that an effective fear appeal message for personal users is one that provokes enough conditioned fear to stimulate a danger control response but not too much fear to risk pushing the personal users into an unproductive fear control response (Johnston & Warkentin, 2010; Witte & Allen, 2000).

However, fear-appeals are only effective if they are coupled with efficacy statements (Witte & Allen, 2000). Efficacy statements include words of encouragement to assure the recipients that they have the ability to perform the recommended coping mechanism (self-efficacy) and that performing the recommended action will have the desired outcome (response-efficacy) (de Hoog et al., 2007; Witte & Allen, 2000). Ruiter et al. (2014) found that both self-efficacy and response-efficacy were two of the most important elements of effective fear-appeal messages. Effective fear-appeal messages should communicate greater (stronger) statements of efficacy than statements of fear (Witte & Allen, 2000). Fear-appeals without these efficacy statements (or weak efficacy statements) typically result in one of the following: 1) negative results or 2) weaker results.

Therefore, we propose enhancing the efficacy or positive components further to include the other three first-order components of PsyCap for two primary reasons. First, individuals often need a reason to be optimistic given the plethora of negativity that is published in the popular press surrounding cyberthreats. It is easy for personal users to conclude that there is no hope or reason to be optimistic concerning their ability to protect themselves online. In other words, threats emerge too quickly for ordinary personal users to protect themselves effectively. Therefore, when personal users watch a fear-appeal message in this security context, they are not necessarily 50-50 on whether to take the action or not when first watching the appeal. They might already be overly pessimistic and are leaning toward taking no action (even before watching the fear-appeal) given what they see in their everyday lives concerning data breaches and compromised accounts. To combat this issue, we propose including additional positive statements of hope, optimism, resilience, and even more self-efficacy to counter-balance all of the reasons to be pessimistic concerning a personal user's ability (or lack thereof) to protect themselves online.

Second, individuals typically require immediate gratification for their actions (Ray & Najman, 1986). However, most volitional security actions do not involve any type of instant or visible gratification. Personal users, for instance, do not see their anti-malware software working while they surf the internet. Security technologies typically work in the shadows or behind the scenes. As a result, we propose that individuals need additional encouragement (by appealing to their HERO within) to adopt security technologies volitionally. We assert that constructing a fear-appeal message that appeals to a personal user's core PsyCap resources in addition to including a moderate amount of fear, a specific (personally relevant) threat appraisal, and a specific (personally relevant) coping mechanism has the potential to increase their exerted effort towards adopting a security technology volitionally. Therefore, we hypothesize the following:

> H4: PsyCap enhanced fear-appeal messages will result in greater adoption rates (and intentions thereof).

4. RESEARCH DESIGN AND METHODS

4.1. Research Design

To test our hypotheses, we conducted two randomized experiments using two security technologies related to online identity management: 1) password manager applications (Study 1) and 2) 2FA services (Study 2). We chose online identity management because personal users have generally not adopted technologies to improve upon their poor identity management practices (Kaleta, Lee, & Yoo, 2019). For the password manager study, we used LastPass as the recommended coping mechanism. At the time of our study, LastPass was a freemium dedicated password management application that used industry accepted encryption techniques. For the 2FA study, we used a 2FA service linked to our participants university email accounts. In both studies, we manipulated PsyCap and not the amount of depicted (conditioned) fear in the fear-appeal messages. We delivered the base-fear appeal messages and PsyCap enhanced fear-appeal messages in video form. Figure 3 displays our research design.

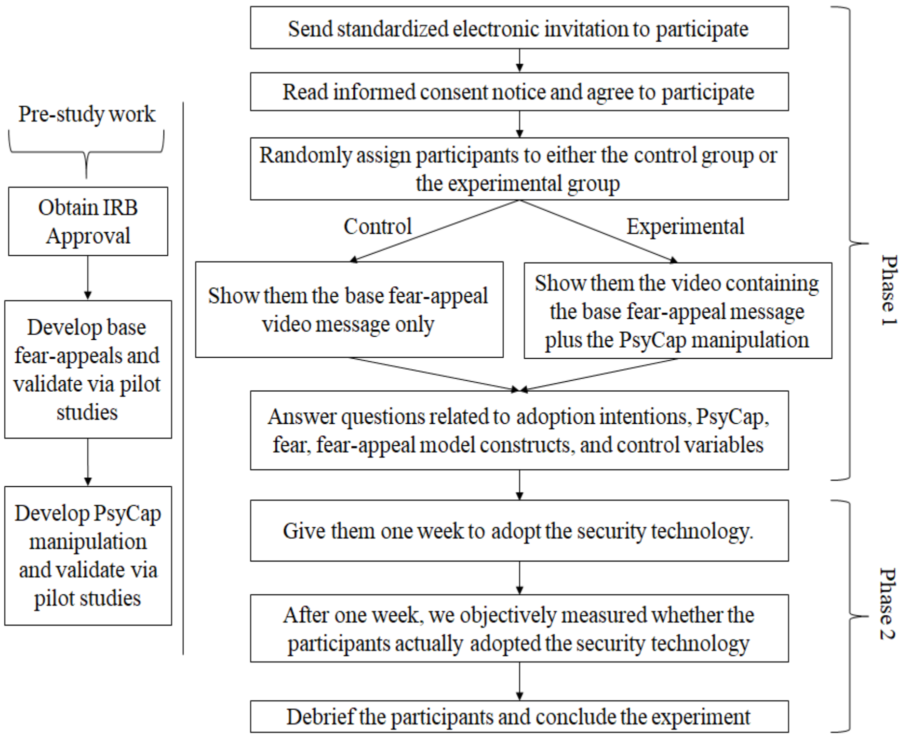

Pre-study work
Obtain IRB Approval
Develop base fear-appeals and validate via pilot studies
Develop PsyCap manipulation and validate via pilot studies
Send standardized electronic invitation to participate
Read informed consent notice and agree to participate
Randomly assign participants to either the control group or the experimental group
Control
Experimental
Show them the base fear-appeal video message only
Show them the video containing the base fear-appeal message plus the PsyCap manipulation
Answer questions related to adoption intentions, PsyCap, fear, fear-appeal model constructs, and control variables
Give them one week to adopt the security technology.
After one week, we objectively measured whether the participants actually adopted the security technology
Debrief the participants and conclude the experiment
Phase 1
Phase 2

Figure 3. *Research Design Across Both Studies*

In both studies, we used the same two-phased (between-subjects) experimental design. In the first phase, we randomly assigned each participant to either the control group or the PsyCap experimental group. For the control group, we gave those participants a base fear-appeal video message related to password manager applications (Study 1) or 2FA services (Study 2) to watch. For the experimental group, we gave them a video that included the same base fear-appeal message that the control group viewed plus our PsyCap manipulation to watch. After watching the randomly assigned videos, we instructed each participant to answer a series of Likert-scale questions concerning their intention to adopt the specified technology, their level of fear of the threat, the four PsyCap resources, and the other FAM constructs. Next, we gave them one week to adopt the technology. After one week, we conducted the second phase of each of our studies where we captured whether the participants actually adopted the technology or not.

To measure actual adoption, we did not rely on self-reported measures, which have social desirability problems. For the password manager study, we asked several questions that could be answered only by using the “Security Challenge” tool built in LastPass. If the participants did not actually adopt the tool, then they could not answer those questions. These items included the relative strength of their master password, total security score for all their accounts from the password managers vault, and total number of accounts in their password manager application after initial use. The research team then converted the participants’ responses to these security challenge questions to either a yes (adopted) or no (did not adopt). We saw no evidence that our participants attempted to put non-sensical answers to these questions. These questions were either filled out fully or left completely blank. For the 2FA study, we obtained confirmation from the

University's technology department as to whether the participants actually adopted the email 2FA service after the conclusion of our study.

With any experimental design, a demand effect (i.e., participants are cued implicitly or explicitly about their expected behaviors related to our hypotheses) is a potential problem (Lonati, Quiroga, Zehnder, & Antonakis, 2018; Zizzo, 2010). One potential method to combat this problem is to objectively establish a baseline for the participants before the start of the study and test the experimental effects above or below those baselines (Lonati et al., 2018). This technique, however, only works if researchers have an objective way to establish such baselines. Unfortunately, we did not have an objective way to measure our participant's PsyCap without Likert style questions so this was not a viable design option. The electronic nature of our studies helped reduce the possibility that the researcher might cue the participants as to the nature of our studies because all participants received the same email inviting them to participate. Our between-subjects research design as opposed to a within-subjects research design also helped us minimize a potential demand effect (Eckerd, DuHadway, Bendoly, Carter, & Kaufmann, 2021).

To further evaluate the potential for demand effects, we executed a pilot study using our PsyCap-enhanced fear-appeal messages. We showed 30 participants our PsyCap manipulation videos, had them answer our Likert-scale questions, and then asked them an open-ended question about the purpose of our manipulation. In these open-ended responses, 10 out of 30 identified fear or a similar fear-related mood adjective, but we were not manipulating fear. None of these 30 participants guessed that we were investigating anything related to the higher order PsyCap construct or any of the four first-order PsyCap resources. These results suggest that there is nothing in the video manipulations or our invitation to participate email message that cued them that we were investigating PsyCap.[1]

The design of our instrument included questions for our independent variables and our behavioral intention dependent variable. Therefore, to minimize potential issues related to common method bias (variance) in both of our studies, we did the following as advocated by Podsakoff and colleagues (2012): 1) presented the measurement items in a jumbled manner and 2) carefully worded all items based on existing scales (and adjusted accordingly based on pilot study feedback). After we collected our data in both of our studies, we ran the unmodeled latent construct (UMLC) test for common method bias (Richardson, Simmering, & Sturman, 2009). Like all other post-hoc tests for common method bias, the UMLC test has limitations (Richardson et al., 2009). Ultimately, there may be no way to detect method variance issues without the use of marker variables and even that method has limitations (Spector et al., 2019). However, this UMLC test is often recommended as the best practice (Podsakoff et al., 2012), so we used it as a matter of convention. Our results do not provide evidence of a major common method bias in our data, but this does not guarantee that such problems would not exist because of the limitations of the UMLC technique. Table A3 in Appendix A shows the results of our UMLC test.

[1] We could have done additional work during each study's debrief sessions instead of just relying on this pilot study to evaluate a potential demand effect. Therefore, we can't 100% rule out the possibility that some of our results are driven by demand characteristics due to our original design decisions. However, this pilot study provides at least some evidence refuting a potential demand effect associated with our procedures, videos, and instruments.

4.1.1. Base Fear-Appeal Design

To design, develop, and validate our base fear-appeal messages, we used the following process: 1) identified attributes of the fear-appeal messages to focus on in the fear-appeal messages, 2) incorporated those attributes into a video fear-appeal message, 3) tested those videos in group settings with students and academics, and 4) repeated the first three steps as necessary.

As previously discussed, we focused on the following attributes to include in our base fear appeal messages: 1) personal relevancy, 2) moderate level of depicted (conditioned) fear from a specific (as opposed to a general) threat, and 3) a specific (as opposed to a general) coping mechanism. To establish personal relevancy, we focused on two aspects of each base fear-appeal message. First, we used the "you" pronoun as frequently as possible to link the examples, threats, and coping mechanisms to each individual personal user who watched the videos. Second, we used social media, online entertainment, and online shopping examples to make the fear-appeal messages relevant to tasks that individuals in this age group regularly perform online (at the time of our data collection).

Next, we made our threats and coping mechanisms in the base fear-appeals video messages specific rather than general (abstract). To do this, we focused on lower level details about the threats and coping mechanisms similar to Schuetz et al. (2020). For Study 1, we focused the message as much as possible on the LastPass password manager (specific) instead of password managers more broadly (general). For Study 2, we similarly focused on the 2FA service linked to their email system (specific) instead of discussing 2FA services abstractly (general).

Finally, we developed our base fear appeal messages in both studies with a moderate level of depicted (conditioned) fear (i.e., a greater than neutral amount of conditioned fear). We wanted viewing the message to elicit enough fear to prompt a danger control remediation process but not risk stimulating too much fear as to prompt a fear control process. Importantly, a fear-appeal message designed to arouse a moderate amount of fear does not mean that all participants will have the same moderate fear arousal because no stimuli evokes the same fear response from all individuals (LaTour & Rotfeld, 1997). For instance, an anti-smoking fear-appeal message designed to have moderate depicted fear might induce minimal fear in certain individuals but strong fear responses in others. Therefore, a moderate level of depicted fear may still have a wide variance of fear arousals but we would expect an average individual to have a moderate level of aroused (conditioned) fear with our fear-appeal messages.

For both studies, we conducted two pilot studies to validate the base fear-appeal messages after we developed them. After the second pilot test for both studies, we were qualitatively and quantitatively confident that our base fear-appeal messages were performing as expected. The final study 1 base fear-appeal video may be found at https://youtu.be/ru3JXo7YoVc and the final study 2 base fear-appeal video may be found at https://youtu.be/ftowWzKqec8.

4.1.2. PsyCap Manipulation Design

PsyCap is not as easily manipulated as emotions because it contains both trait-state and state-like resources (Luthans, Avey, et al., 2006). In the organizational behavior literature, an employee's PsyCap psychological state is typically developed via a series of in-person trainings (Luthans et al., 2006). This approach was not feasible for us, so we developed a video manipulation where we focused on different elements of hope, efficacy, resilience, and optimism. To determine these elements, we first had group discussions with students and academics to discuss the PsyCap construct. In these discussion sessions, we brainstormed about what rhetorical language might move each of them to the positive side of the continuum for each PsyCap resource related to the implementation of the proposed coping mechanisms. As a result of these discussions and the suggested micro-interventions suggested by Luthans et al. (2006), we focused on goal-setting (i.e., “goal of more secure accounts”) and different pathways to meet those goals, which is a common theme across all four PsyCap resources.

In our manipulations, we provided them with reasons to be hopeful and optimistic along with encouraging them to believe in their abilities and to be resilient even if their first adoption attempts were not successful (e.g., “it is easy”, “even someone as busy as you”, “reward for adopting”, and “superior account protection”). We also provided support resources as a part of the manipulation to activate all four first order PsyCap components because having a support system provides individuals with a specific reason for them to be hopeful, efficacious, resilient, and optimistic about their ability to perform the action successfully. Finally, the positive and encouraging tone (e.g., “you can do this” tone) of the video manipulations was just as important (if not more important) to activate their HERO within as the specific language contained in our PsyCap manipulations.[2]

After creating drafts of our PsyCap manipulation videos, we piloted each of those drafts once, obtained feedback, modified the manipulation videos, and piloted the modified manipulations again. For each pilot study, we measured each subject’s PsyCap scores before and after the manipulation to determine if our PsyCap manipulations increased their overall PsyCap across all of the first order components. After the second pilot test in both studies, we were confident that our PsyCap manipulations were working effectively to increase each of PsyCap’s first order constructs. The final Study 1 PsyCap enhanced fear-appeal message that includes appeals to the four first order PsyCap constructs may be found at https://youtu.be/RnIJQtd9sZw and the final study 2 PsyCap enhanced fear-appeal manipulation may be found at https://youtu.be/ItSGEdnXlqk.

4.2. Measurement Items

For both of our studies, we adapted all construct measurement items from pre-existing scales. We modified the wording of the PsyCap measurement items from their original organizational context to each of our volitional security actions because the pre-existing PsyCap scales were developed in organizational settings (Luthans et al., 2007). We also measured response efficacy, perceived threat vulnerability, perceived threat severity, and response costs using adapted measurement items from pre-existing scales.[3] Tables A1 and A2 in Appendix A display all of our measurement items and their respective sources. Modifying a few of the measurement items from their original contexts to our security technologies required a fair bit of adaptation, specifically in terms of the length and complexity of the items. Although we pilot tested our adaptations, we want to note that

[2] Given that PsyCap is usually developed via multiple in-person trainings and team building exercises, we were not expecting excessively large increases in each PsyCap resource as we might expect if we were manipulating an emotion via a short video. Our goal was to have small but statistically significant increases along each PsyCap resource.

[3] We also measured maladaptive rewards (i.e., rewards for not adopting the security technologies). However, this construct is not a component of the FAM so it was not used in the analyses.

our items weren't single word adaptations from the original items. Therefore, the original validity tests that were published during the development of these scales are only partially relevant to our specific items. Furthermore, additional scale development might be necessary to better refine our items to personal computing contexts. We measured all of these items using 7-point scales.

Fear cannot be measured directly because there are a multitude of different processes and elements associated with fear (Rogers, 1983; Scherer, 2005; Witte, 1992). Therefore, all measures of fear whether physiological or self-reported are indirect proxies. The cognitive element of emotions in Scherer (2005)'s model is one of the main justifications scholars have used to measure fear via Likert-items. Based on this model, individuals have the cognitive capacity to remember their fear arousals (Rogers, 1983; Witte, 1992). As a result, self-reported fear has long history across a variety of disciplines (c.f. Block & Keller, 1995; Gleicher & Petty, 1992; Mewborn & Rogers, 1979; Posey et al., 2015). Rogers (1983, p. 164) states that an individual's "self-rated fear is more global in nature and more adequately reflects an overall emotional state, while physiological arousal fluctuates substantially during the presentation of a fear appeal."[4] Therefore, we adapted an existing set of fear measurement items for both of our studies.

4.3. Study Participants

Across both studies, we used business school students from the same private University in the Midwest portion of United States. Many of the complaints about student samples are related to attempting to generalize from students to employees in organizations. For our study related to personal users, students are acceptable (even preferred) because they are not subjected to any organizational level policies that might spillover into their decision-making in their personal computing environments. To obtain our participants, we first approached faculty teaching classes in the business school and then students in the classes taught by the faculty who agreed to participate. We randomly assigned our research subjects to either our control or experimental groups. Next, we sent the respective link (either control or experimental) to the participants. The participants were unaware whether they were in the experimental or control groups. We removed all personal information (which was collected for the course extra credit and to verify actual adoption in the 2FA study) prior to performing any of our data analyses.

As a participation incentive, the students were given a small amount of course extra credit for participating in each of our studies. None of the students who initially agreed to participate opted

[4] Scholars have previously used physiological arousals as proxies for fear (Mewborn & Rogers, 1979). These physiological arousals are most related to fear arousing events in health contexts (e.g., getting informed about a terrible health condition) as opposed to conditioned fear arising from generalized security threats or a generalized fear of crime. However, we still expect Scherer's (2005) model of emotions to apply, which means there should be some physiological arousal when stimulating our conditioned fear of compromised accounts. Therefore, we ran a validation study to determine if there was a correlation between the self-reported fear Likert-scale measures and physiological arousals. We used heart-rate as our physiological arousal in this validation study. We then have to make the theoretical leap that this heart-rate arousal is from fear and not some other construct (in part or in full), but it is a reasonable physiological proxy for fear for our validation study. We recruited 25 participants for this measurement validation study. We showed each participant our videos and measured their heart rates throughout their participation using a heart-rate monitoring device. During this validation study, we also captured our Likert-scale measures of fear (along with other FAM constructs). We found a 0.87 correlation between changes in heart-rate after watching our video manipulations and our Likert-scale fear measures. This result suggests that our Likert-scale measures are just as plausible proxies for fear as heart-rate physiological proxies for fear.

out after reading the informed consent agreement. The only participation exclusion criterion was if the student had already adopted a password manager application (Study 1) or the 2FA system linked to their university email account (Study 2). No participant in either experiment met these conditions to be excluded.[5] Table 1 displays the descriptive statistics for both studies. The participants in the control and experimental groups for both studies had similar general computer knowledge, ages, grade point averages, and gender distributions.

Table 1. *Study Demographics*

	Study 1		**Study 2**	
	Control	Experimental	Control	Experimental
Sample Size	116	117	90	90
Age Groups				
18-20	77	55	38	60
21-24	24	59	48	28
>25	5	3	4	2
Gender				
Female	58	62	47	46
Male	58	55	43	44
Grade Point Average				
<3.0	37	38	25	26
3-3.5	37	38	33	34
>3.5	42	41	32	30
General Computer Knowledge (7-point scale)	3.155	3.199	3.122	3.133

Following the guidance of Aguinis, Gottfredson, and Joo (2013), we assessed the impact of potential outliers by creating a series of box plots and scatter plots along with calculating a generalized Cook's D statistic. For Study 1, we found 12 potential univariate outliers (single construct), 11 potential bivariate outliers (construct pairs), and 6 observations with higher than expected generalized Cook's D values.[6] For Study 2, we found 3 potential univariate outliers, 9 potential bivariate outliers, and 3 observations with higher than expected generalized Cook's D values. For both studies, we ran all of our models with and without the potential outliers. When

[5] At the time of our data collections, many web-browsers had built-in password managers. As such, it is interesting that none of the participants identified that they were using these built-in tools when asked if they were using a password manager application. It is possible that a few of the participants in Study 1 did not conceptualize those browser-based tools as substitutes for the LastPass dedicated password manager application. We did not re-ask the question during the study's debrief sessions to see if by doing the study they realized that they were already using one of these browser-based password manager applications.

[6] These categories of outliers are not mutually exclusive. That is, an observation may be flagged as a potential univariate outlier and contain a high generalized Cook's D statistic.

we removed different combinations of these potential outliers in both studies, we found negligible differences in factor loads, path coefficients, path directionality (no differences), and significance (no differences) compared to the full data sets. We further followed up by creating index plots, which did not reveal any noticeable issues. Therefore, we report the models with the full data sets only in the remaining sections.

5. DATA ANALYSES & RESULTS

In our two studies, we had two outcome variables: 1) behavioral intentions to adopt the security technologies (Likert 1 to 7 continuum) and 2) actual adoption (binary 0 or 1). For both outcome variables, we used CBSEM because it is generally considered the most appropriate method for theory testing with a well-established theory (FAM) while allowing us to determine model fit when adding or substituting constructs to our FAM models (Gefen, Rigdon, & Straub, 2011).

5.1. Manipulation Checks

Table 2 contains the manipulation checks across both studies. Given that PsyCap contains both trait-like and state-like resources, we were not expecting our video manipulation to increase each lower-order resource equally. However, we were expecting to see statistically significant increases for the experimental group over the control group for each lower-order resource, which we did except for resilience in Study 2. The higher-order PsyCap construct was also statistically different for both studies. Our PsyCap manipulations (which only stimulated the four HERO constructs) should not have resulted in different conditioned fear arousals across the control and experimental groups because the PsyCap manipulation did not have any statements designed to increase or decrease our subjects' conditioned fear of the threat. Therefore, the experimental and control groups should not have statistically different levels of conditioned fear, which was the case in both of our studies. Our PsyCap manipulation did reduce perceived response costs associated with the coping mechanisms in both studies. These lower values are somewhat expected due to the added self-control and individual agency associated with greater PsyCap. However, our multi-group analyses (explained later) revealed that the path differences for response costs in our structural models were not statistically different between the two groups in both studies.

Table 2. *Manipulation Checks*

	Study 1					Study 2				
Variables	Control		Experimental		ANOVAs	Control		Experimental		ANOVAs
	Mean[1]	Stdev[1]	Mean[1]	Stdev[1]		Mean[1]	Stdev[1]	Mean[1]	Stdev[1]	
Psychological Capital[2]	55.35	7.10	59.91	8.09	15.22***	54.69	7.47	59.13	7.63	15.44**
Hope	4.23	1.05	4.58	0.98	4.66*	4.14	1.29	4.60	1.31	5.49*
Self-Efficacy	5.04	0.98	5.47	0.93	11.95***	5.12	1.09	5.66	0.94	12.35***
Resilience	4.59	0.88	5.00	0.87	12.77***	4.49	0.83	4.61	0.93	0.86
Optimism	4.59	0.88	4.92	0.93	7.6**	4.48	1.05	4.84	1.10	5.06*
Conditioned Fear	4.76	1.24	4.80	1.27	0.01	4.64	1.19	4.66	1.31	0.01
Threat Severity	5.89	0.91	6.11	0.74	4.12*	5.64	1.08	5.67	1.20	0.02
Perceived Threat Vulnerability	4.59	1.01	4.76	1.12	1.51	4.50	1.05	4.61	1.22	0.46
Response Efficacy	5.64	0.97	5.87	0.84	3.66	5.75	0.97	5.96	0.98	2.03
Response Costs	4.20	1.23	3.26	1.24	33.45***	3.79	1.03	3.16	1.37	12.42***

*p<0.05, **p<0.01, ***p<0.001

[1] To calculate these means and standard deviations, we averaged all measurement items for each construct equally.

[2] The values for psychological capital are the averages of the summed lower-order resources across all observations.

5.2. Behavioral Intentions

We see higher behavioral intentions to adopt the security technologies for the experimental groups relative to the control groups in both studies. In Study 1, the experimental group had average behavioral intentions scores of 4.45 (standard deviation of 1.52) relative to the control group who had average behavioral intentions scores of 3.89 (standard deviation of 1.39). That difference was statistically significant (t=2.93, standard error=0.19, p=0.004). In Study 2, the experimental group had average behavioral intentions scores of 4.95 (standard deviation of 1.35) relative to the control group who had average behavioral intentions scores of 4.30 (standard deviation of 1.32). That difference was also statistically significant (t=3.28, standard error=0.20, p=0.001).

We followed the Anderson and Gerbing (1988) two-step process for our CBSEM analyses for assessing our measurement (step 1) and structural (step 2) models for both studies. To perform our CBSEM analyses, we used MPlus v8. We first conducted a confirmatory factor analysis (CFA) with all measured constructs to assess our measurement models. For both studies, we used bootstrapping with 1000 samples to account for our mild deviations from normality.[7] Tables A4 (Study 1) and A5 (Study 2) in Appendix A display the CFA results, which includes the factor loadings, composite reliabilities, inter-construct correlations, and construct correlation confidence intervals. In both studies, all of our measurement items had composite reliabilities above 0.7. Both

[7] The kurtosis values for our measures ranged from -1.02 to 4.188 for Study 1 and from -0.901 to 2.508 for Study 2.

Study 1 (χ^2=450.7, df = 360, p = .212) and Study 2 (χ^2=515.13, df = 360, p = .083) pass the inferential χ^2 test for our CFA models. To assess discriminant validity, we used the CI_{CFA} (sys) method described in Rönkkö and Cho (2022). To estimate these correlation confidence intervals, we freed the first item loading for each measured construct and constrained each factor's variance to 1. Based on these correlation confidence intervals, we see no evidence of a problem (i.e., the upper limits are less than 0.80) between all constructs with the exception of the PsyCap lower order constructs, which is expected based on the definitions of the lower order PsyCap components.

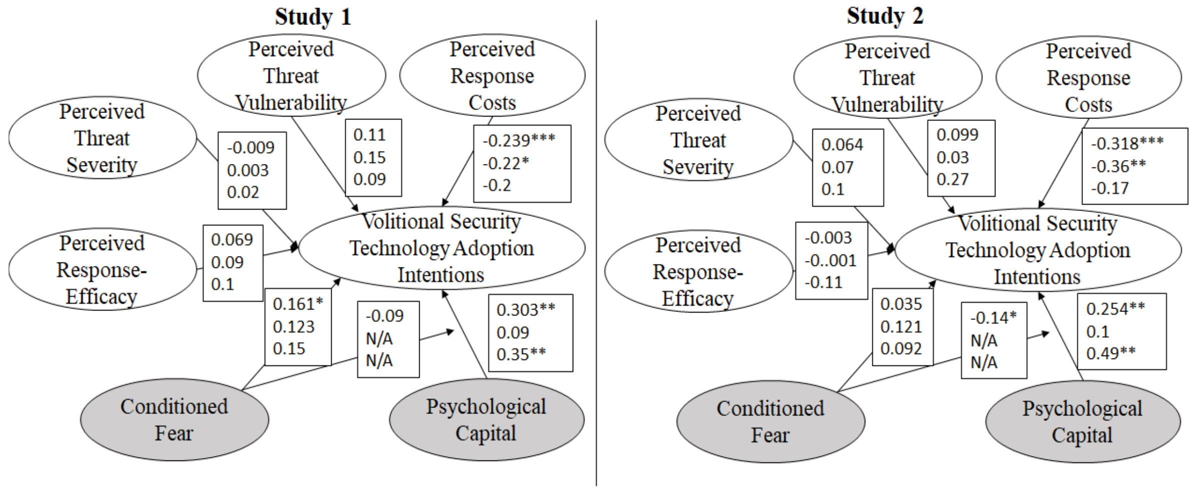
Consistent with PsyCap's theoretical development (Luthans et al., 2006, 2007), we modeled PsyCap as a reflective-reflective higher-order construct. This operationalization means that the lower order constructs are all measured reflectively and there is a reflective relationship between the lower order constructs and the higher order construct (Jarvis, MacKenzie, & Podsakoff, 2003). Comparing the upper limit of the correlation (see Tables A4 and A5 in Appendix A) for hope and resilience in both studies, the correlation upper limit (Study 1 = 0.874, Study 2 = 0.841) is between 0.8 and 0.9, which indicates marginal discriminant validity issues (Rönkkö & Cho, 2022, p. 20). We believe this high correlation is evidence of some conceptual overlap between the hope and resilience constructs. By including hope and resilience in our PsyCap higher order construct (instead of separately directly into behavioral intentions), we believe that we will avoid any potential discriminant validity issues with these constructs in our structural path model results.

Next, we fit a series of structural path models using the FAM and PsyCap for both studies based on our research model displayed in Figure 1. Our initial inferential χ^2 tests failed for both Study 1 (χ^2=603.018, df=381, p=.005) and Study 2 (χ^2=617.63, df = 381, p=.007). Moving forward with structural path analysis in the presence of a failed χ^2 test is not recommended until diagnostics are conducted to identify the most likely causes of model misfit and reasoned justification is given to proceed (Ropovik, 2015). Therefore, we followed Kline (2016, p. 268-269)'s general guidance and conducted local fit testing to identify the possible source of our model misfit. We started by evaluating our model with our dependent variable (behavioral intentions) and added one antecedent construct and relationship at a time in a systematic manner. We examined the normalized correlation residuals after each incremental model run. As a result of this process, we identified large residuals between self-efficacy and behavioral intentions when self-efficacy was included as a lower-order construct in the higher-order PsyCap construct. When we removed self-efficacy from the PsyCap higher-order construct and modeled it directly into behavioral intentions (along with the other constructs and relationships in Figure 1), the inferential χ^2 test passes for both Study 1 (χ^2=506.163, df=375, p=.07) and Study 2 (χ^2=532.597, df = 375, p = .09). This result indicates that self-efficacy loads more strongly directly on behavioral intentions as opposed to indirectly through the PsyCap higher-order construct in the data for both of our studies. We also see this in the lower factor loadings from self-efficacy relative to the other sub-constructs on PsyCap for both studies. Unfortunately, previous PsyCap studies do not report their χ^2 test results (p values in particular) or any diagnostics. Therefore, we do not know if our data are unique or if this problem is a persistent problem in the PsyCap literature.

In order to decide how to proceed with self-efficacy's placement in the structural model, we evaluated our hypotheses with self-efficacy as both a component of and external to PsyCap. We found that the χ^2 test results were better with self-efficacy when it was modeled externally (Study

1: $\Delta\chi^2$=96.855, Δdf=6; Study 2: $\Delta\chi^2$=85.033, Δdf=6). However, the path coefficients between PsyCap and the other exogenous constructs going into behavioral intentions do not substantially change in terms of magnitude, direction (no change), and significance (no change). Given the general similarity of the structural path model results, we decided to continue our analyses with self-efficacy as a lower-order construct component of PsyCap in order to keep with the theoretical foundation of PsyCap.

Figure 4 displays our structural path model results for both studies. Tables A6 to A7 in Appendix A provide more detailed statistics related to each of our models. In the experimental group, we see a statistically significant effect for PsyCap in both studies. That is, the greater the PsyCap, the more likely a personal user is to have greater intentions to adopt the dedicated password manager (Study 1) or the 2FA system attached to their email accounts (Study 2). We see a statistically significant interaction effect with PsyCap and conditioned fear for the 2FA study (Study 2). The interaction effect of conditioned fear and PsyCap on adoption intentions of password manager applications (Study 1) was not significant. Therefore, we have evidence for our conditioned moderating effect in Study 2 but not in Study 1.



Total Sample Frame = upper values; Control Group = middle values; Experimental Group = lower values; *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$

Figure 4. *CBSEM Structural Path Model Results*[8]

Next, we tested whether the path coefficients between the control and experimental groups were significantly different via a Wald $\chi2$ test in a multi-group analysis (MGA) (Muthen & Muthen, 2017, p. 711). Before conducting our MGAs in both studies, we first established metric invariance (weak factorial invariance), which enabled us to effectively interpret the MGA results. Tables A8 and A9 in Appendix A display the results from our measurement invariance tests. Figure 4 shows the path coefficients and statistical significance for the total sample frame (all participants in each respective study), the control group, and the experimental group. Our MGA analyses in both studies show statistically significant differences along the PsyCap paths between the control and

[8] We could not test the interaction effect separately for the control and experimental group because we needed the full range of PsyCap values from low (control) to high (experimental). Testing the interaction effect with just the experimental group would be testing a differential effect from high to higher (or low to lower for the control group), which was not our hypothesized effect.

experimental groups; PsyCap has a statistically significantly stronger effect on behavioral intentions for the experimental group relative to the control group.

We also analyzed the effect of each lower order PsyCap construct separately to investigate the impact of each individual component on behavioral intentions. These analyses allowed us to determine which sub-constructs were driving the PsyCap results for our two studies. They further allowed us to investigate whether the individual sub-constructs significantly interacted with conditioned fear. Tables A6 and A7 in Appendix A show these results. Interestingly, the interaction effect between self-efficacy and conditioned fear is not significant in either study. Therefore, had we just used self-efficacy instead of the higher-order PsyCap construct as typically done in the behavioral security literature, we would not have found evidence for our proposed moderating effect of conditioned fear. From the lower-order PsyCap construct analyses, we also see that adoption intentions for each security technology are driven by a different set of PsyCap's sub-constructs. Hope and optimism were the driving factors for PsyCap in Study 1. For Study 2, however, hope, resilience, and self-efficacy were the most important factors for PsyCap. PsyCap, as a higher order construct, has greater theoretical flexibility than any of its individual sub-constructs investigated in isolation. Obviously, the theoretical flexibility associated with the higher-order PsyCap construct comes at a cost of parsimony. However, it is a richer construct that contains a reservoir of resources that can explain a wide variety of personal users' security technology adoption decisions given the contextual differences associated with the different security technologies that are available.

5.3. Actual Adoption

In Study 1, 35 out of 117 (30%) participants in the experimental group actually adopted LastPass whereas only 14 out of 116 (12%) participants in the control group actually adopted it. That difference was significantly different (t=3.41, standard error=0.05, p=0.0008). In Study 2, 30 out of 90 (33%) participants in the experimental group actually adopted the 2FA email service whereas only 18 out of 90 (20%) participants in the control group actually adopted the 2FA email service. That difference was significantly different (t=2.03, standard error=0.07, p=0.04). Therefore, the PsyCap enhanced fear-appeal message resulted in greater actual rates across both security technologies.

To test our hypotheses regarding the structural paths between behavioral intentions, PsyCap, and actual adoption rates, we used CBSEM following the same procedures we used to test our behavioral intentions hypotheses. Figure 5 displays these results. For Study 1 (password managers), we see a strong positive main effect of PsyCap on actual adoption rates. Higher PsyCap is associated with higher actual rates for the entire sampling frame (control plus experimental) and for just the experimental group. However, the interaction effect of behavioral intentions and PsyCap is not significant for the actual adoption of LastPass. Therefore, the effect of PsyCap is not different for varying levels of adoption intentions for the password manager technology.

For Study 2 (2FA), however, we find a different pattern of results. With this security technology, we find no support for the main effect of PsyCap. However, we find a significant interaction effect between adoption intentions and PsyCap so PsyCap still matters for explaining the variance in actual adoption rates. With this interaction effect, the effect of PsyCap on actual adoption is greatest (positive) for those personal users who have high 2FA adoption intentions. The effect of PsyCap on actual adoption for those personal users who have low adoption intentions is slightly negative but relatively flat, which means higher PsyCap cannot overcome their low adoption intentions for the 2FA service.

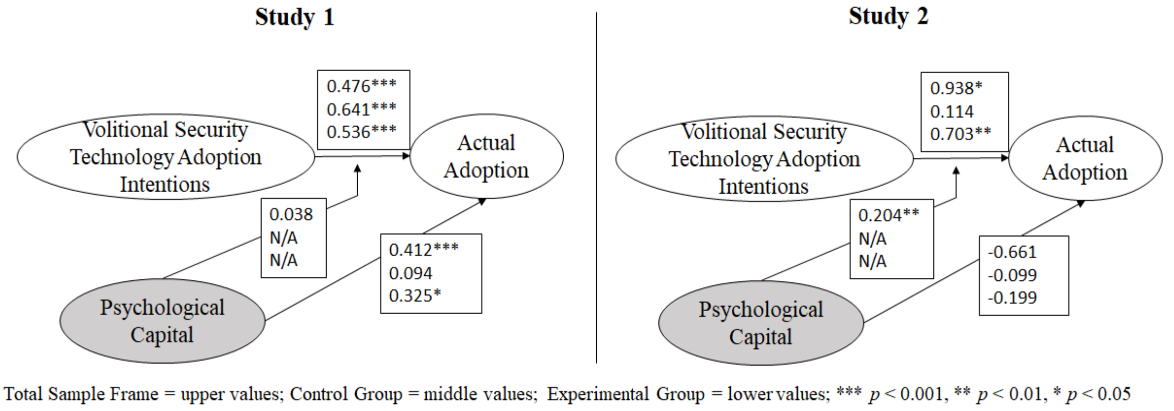

Study 1
Volitional Security Technology Adoption Intentions
Actual Adoption
Psychological Capital
0.476***
0.641***
0.536***
0.038
N/A
N/A
0.412***
0.094
0.325*
Study 2
Volitional Security Technology Adoption Intentions
Actual Adoption
Psychological Capital
0.938*
0.114
0.703**
0.204**
N/A
N/A
-0.661
-0.099
-0.199
Total Sample Frame = upper values; Control Group = middle values; Experimental Group = lower values; *** p < 0.001, ** p < 0.01, * p < 0.05

Figure 5. *CBSEM Results for Actual Adoption*

6. DISCUSSION AND CONCLUSION

In this paper, we investigated the impact of PsyCap on the volitional adoption of security technologies, specifically for personal users. Table 3 displays a summary of our conclusions relative to our hypotheses. In both studies, we saw increased adoption rates (and intentions thereof) for our PsyCap experimental groups relative to our control groups. Our overall results, however, were different across both security technologies. Although password managers and 2FA services are both identity management solutions, there are at least two noticeable differences between the security technologies. First, most of our participants had previously configured a 2FA service with a different system prior to participating in our study. Almost none of our Study 1 participants had prior experience with password managers prior to participating in our study. Second, the 2FA service is less black-box than the password manager application. Personal users might be hesitant to adopt a password manager application because they are unsure how the application manages and secures passwords across multiple websites. Contrarily, the 2FA service using text messaging is easier for many personal users to understand. Individuals tend to be less likely to adopt technologies that they do not understand (Rai, 2020), which might logically impact the relative importance of a personal user's HERO within regarding the technology.

Table 3. *Summary of Conclusions*

	Study 1: **Password Managers**	**Study 2:** **2FA**
Greater PsyCap is associated with greater intentions (H1a) and greater actual adoption (H1b) (main effects)	Supported for adoption intentions and for actual adoption	Supported for adoption intentions but not supported in the actual adoption CBSEMs.
Conditioned fear moderates the effect of PsyCap on intentions (H2)	Not Supported	Supported
PsyCap moderates the effect of intentions on actual adoption (H3)	Not Supported	Supported
PsyCap enhanced fear-appeal messages is associated with greater volitional adoption rates (and intentions thereof) (H4)	Supported for adoption intentions and actual adoption	Supported for adoption intentions and actual adoption

It is important to consider the possibility that having too much PsyCap might be problematic for security actions. For instance, personal users might be less diligent about scanning emails for phishing attempts if they are overly optimistic, hopeful, efficacious, and resilient regarding how much protection their anti-phishing application provides. We posit that excessive PsyCap might be troubling post-adoption but not for initial adoption rates (and intentions thereof). Given equal conditions, having too much HERO within about installing (adopting) a security technology would not logically result in a lower propensity to adopt the tool. Post-adoption, however, personal users must be careful to not let their high PsyCap about the usefulness of the security technology result in careless behaviors because they have the security technology as their safety net (Chen, Turel, & Yuan, 2022; Rhee, Ryu, & Kim, 2012). The focus of our paper was on initial adoption so our proposed positive linear effect of PsyCap is reasonable. However, future research may extend our research by testing the effect of PsyCap post-adoption, which would help further understand the role of PsyCap in other security contexts.

6.1. Theoretical Contributions

We make several notable contributions to the literature. First, we are the first (to the best of our knowledge) to introduce the PsyCap construct to the volitional adoption of security technology literature. Prior to our study, PsyCap has been primarily used in organizational settings (Burns et al., 2017; Burns et al., 2019; Luthans & Youssef-Morgan, 2017; Newman et al., 2014). For our personal computing context, we investigated PsyCap using the FAM, but PsyCap is a construct that may be used in many different theories. Any theory that uses a single positive construct such as resilience or self-efficacy may benefit from using the higher-order PsyCap construct. Obviously, the higher-order PsyCap construct comes at a cost of parsimony and testing complexity, but PsyCap offers more theoretical flexibility relative to a single positively valanced construct. For instance, certain security technologies may require PsyCap's trait-like characteristics whereas others may require PsyCap's state-like characteristics to explain personal users' security technology decisions. Across both studies, we see different lower-order PsyCap resources impacting our personal users' adoption decisions.

Second, we contribute to the FAM literature (Johnston et al., 2015, 2019; Orazi et al., 2019; Warkentin et al., 2016) by introducing the PsyCap construct as having a main effect and both moderating and moderator effects. We are also the first to argue and demonstrate empirically that conditioned fear has a moderating role in the FAM. Including the higher-order PsyCap construct in the FAM allowed us to see a few interaction effects (for the 2FA service) that would not have been evident had we just investigated them using self-efficacy or the other three first-order constructs in isolation. In our 2FA data, for instance, the interaction effect of conditioned fear and self-efficacy was not significant. We have argued and demonstrated empirically that PsyCap is a rich addition to the FAM.

Third, the use of the fear construct in traditionally cognitively based theories has sparked considerable debate in the behavioral security literature (Boss et al., 2015; Chen et al., 2021; Johnston & Warkentin, 2010; Posey et al., 2015). We suggest that the fear construct as used in the security literature has similarities but also differences from the fear construct used in the health literature. Individuals cannot learn how to respond to a fear arousing event such as being told that they have a deadly illness. We cannot imagine any type of adverse information security event that could arouse fear in that manner. However, that does not mean fear is unimportant for personal user's security technology decisions. We proffer that fear in a security context is learned over time via news stories, public service announcements, and general awareness campaigns similar to a generalized fear of crime (Houts & Kassab, 1997; Mears & Stewart, 2010) or a generalized fear of death (Mitchell & Schulman, 1981). Mindful personal users are conditioned to be afraid of and how to respond to security threats such as malware, ransomware, and identity theft. In this manner, we argue that fear in the information security context follows Scherer (2005)'s model of emotions, particularly not by-passing the first step in the process related to a cognitive appraisal.

Fourth, we contribute to the recent behavioral security literature on the design of fear-appeal messages (Johnston et al., 2015, 2019; Schuetz et al., 2020). Our results reveal that a fear-appeal message that appeals to an individual's HERO within in addition to including specific threats and coping mechanisms that are personally relevant can positively increase adoption rates (and intentions thereof). Across both of our studies, we see that our participants who watched the PsyCap enhanced fear-appeal messages had greater adoption intentions and actual adoption rates. We demonstrate that a psychological state such as PsyCap may be stimulated in a fear-appeal message. In organizational contexts, PsyCap is typically developed via in-person training and team-building sessions (either single day or multiple day) (Luthans, Avey, et al., 2006; Luthans, Avey, & Patera, 2008; Luthans & Youssef-Morgan, 2017). Across both our experiments, we showed that we were able to increase an individual's PsyCap as it related to a specific coping mechanism in a roughly 2- to 3-minute video manipulation. This is an important first-step in stimulating more stable psychological states, which can be integrated in fear-appeal messages.

Fifth, we contribute to the PsyCap literature via our model fit diagnostics in our CBSEM analyses. We uncovered potential issues related to the modelling of the higher-order PsyCap construct that have not been previously reported in the literature. Based on the theoretical formulation of the PsyCap construct, we expect that the lower-order constructs will be correlated. However, we demonstrate in our data that this is not always the case. For instance, certain individuals had high efficacy and optimism but low resilience and average hope. We would logically expect different individuals to have varying levels of hope, efficacy, resilience, and optimism regarding the security technology. In our experimental manipulation, we also did not expect to manipulate all of the trait-like and state-like PsyCap resources equally because certain lower-order resources are more malleable than others (Luthans et al., 2006). In our data, we saw that self-efficacy was not as highly correlated with the other three HERO constructs. This is not to say that self-efficacy will always be less correlated in other contexts with other security technologies. It might be any of the lower-order constructs depending on the research context and study participants. However, we believe that our fit testing analyses identified an important area for future PsyCap research. Instead of just assuming that each of the sub-constructs might behave in a similar manner to prior empirical PsyCap research, scholars should do their own validation of the construct. This will help tease out contextual differences and possibly identify areas where the construct's definition might need refinement.

6.2. Practical Implications

Unfortunately, there is a plethora of negative news related to cyberthreats that personal users are exposed to each day. Therefore, it is easy for a personal user to conclude that there is no hope for them to do anything to defend themselves. To combat this problem, we suggest that security professionals focus on the positives by giving them reasons to be optimistic or resilient in the face of these dangerous online threats. That is, security professionals should appeal to a personal user's HERO within that their computing environments, identities, and accounts can be secure by implementing appropriate security technologies and by following other secure computing recommendations. Even relatively small increases in PsyCap (as our two studies demonstrated) can have meaningful increases in both behavioral intentions and actual adoption rates of security technologies. As such, PsyCap is a powerful construct that security professionals can leverage to motivate personal users to use technologies to help them be more secure.

One of the benefits of the PsyCap construct is its practical usefulness (Newman et al., 2014). The HERO constructs are not theoretically abstract, which makes them relatively easy for security professionals to understand, manage, and manipulate. PsyCap emphasizes positivity, which has been linked to many positive outcomes inside and outside of organizations (Avey, Reichard, Luthans, & Mhatre, 2011; Larson & Luthans, 2006). In our PsyCap enhanced fear-appeals the positive "you can do this!" tone engaged our participants more than our non-PsyCap enhanced fear-appeals. We did this with a single 2- to 3-minute video manipulation. Security professionals may be able to motivate personal users even more than we did via repeated exposures to appeals to their HERO within regarding the security technology. Instead of hearing that they have the necessary hope, efficacy, resilience and optimism to adequately defend themselves a single time, security professionals have the benefit of being able to expose them repeatedly via a variety of different channels.

Across both of our studies, PsyCap was more consistently associated with adoption intentions than conditioned fear. PsyCap was a significant positive contributor in both studies whereas fear was only a positive contributor in the password manager study. Therefore, security professionals have to be careful about just relying on (conditioned) fear to motivate personal users to adopt their security technologies. We further found that conditioned fear moderated the effect of PsyCap in the 2FA study. This moderating effect showed that the effect of conditioned fear was not always positive. That is, conditioned fear and PsyCap do not work in isolation from one another. Therefore, marketers and security organizations need to understand (and stimulate) the positive PsyCap of their potential consumers (personal users) to maximize the effect of conditioned fear in their communication messages.

Practitioners probably care more about actual adoption rates than adoption intentions. Our insight that PsyCap can help translate adoption intentions to actual adoption in the 2FA context is useful for security professionals. Specifically, for those personal users who have high adoption intentions, they can focus on the four PsyCap resources to get them to follow-through on their adoption intentions. We show that the combination of high adoption intentions and high PsyCap is the most beneficial for explaining the variance in actual adoption rates. We have to provide a slight bit of caution to this practical recommendation because we only found this effect with the 2FA service and not for the password manager application.

6.3. Limitations and Future Research

Like all research, our paper has limitations. First, we only studied volitional adoption decisions related to security technologies designed to mitigate the poor identity management threat. Volitional adoption of technologies in other security contexts such as anti-virus or anti-spyware might have a different pattern of results because those security technologies require a different amount of implementation effort and they are related to a different set of cyberthreats. We saw differences with password manager and 2FA service adoption rates (and intentions thereof) that can plausibly be explained by technology related differences even though both technologies helped solve the same identity management threat. Future research may investigate different volitional security technologies to investigate whether the same effects are present in their volitional technology decisions.

Second, there is clearly a difference between initial adoption and post-adoption (continued) use of a security technology. We investigated initial adoption rates (and intentions thereof) in both of our empirical studies. In the Warkentin et al. (2016) study, for instance, they captured participant data over time for initial installation and continued use of a simulated anti-malware program. In their study, participants volitionally installed a security program, which repeatedly reminded them to keep using the security software over time. We did not investigate this type of behavior in either one of our studies. PsyCap may have the same or different effects if it is stimulated and developed repeatedly post-adoption. Therefore, future research can build from our study by investigating post-adoption use of a volitional security technology to test our proposed PsyCap effects over time.

Third, we controlled for gender and general computer knowledge in both studies. Neither were significant in any of our models. However, other factors such as security knowledge and security fatigue might impact a personal user's volitional adoption decisions. For instance, the more fatigued a personal user is regarding information security, the less likely they may be to adopt any type of security technology. Our general computer knowledge control variable did not specifically capture information security knowledge. It would seem reasonable that personal users with differing levels of security knowledge might have different adoption propensities. Future research can investigate our model with these additional control variables or investigate how security knowledge or fatigue might have a moderating or a mediating effect on PsyCap. It would seem plausible that PsyCap may have a differential effect depending on specific knowledge related to security more generally or the specific threat. These additional studies would further help explicate the effects of PsyCap for personal user's adoption decisions.

Finally, the scope of our paper was personal users. Employees have significant organizational inhibitors, facilitators, and constraints related to their security actions that personal users do not have (Burns et al., 2017; Dhillon, Syed, & Pedron, 2016; Kam et al., 2020; Pérez-González, Presiado, & Solana-Gonzalez, 2019). Therefore, employees may experience a different effect from a similar PsyCap enhanced fear-appeal message depending on industry, organizational culture, the specific policies and procedures in their organizations, or the security related training programs in their organizations. Having said that, the organizational behavioral literature and the initial reported PsyCap findings related to behavioral security actions in organizations suggest that PsyCap might have similar effects. However, the number of confounding variables in an organizational setting is much greater than for personal users. Therefore, a fruitful area of future research could investigate the effects of PsyCap in different organizational environments.

6.4. Concluding Remarks

Our paper demonstrated the positive effects of PsyCap in a sample of younger personal users. We are cautiously optimistic that our PsyCap experimental effects will generalize to other populations of personal users and other security technologies. Obviously, however, more research with more diverse samples of personal users and different security technologies are needed to validate these claims but our results provide some initial evidence. Our data and analyses suggest that PsyCap has a place in the FAM and possibly other theories that include a single positive construct such as hope or self-efficacy.

REFERENCES

Aguinis, H., Gottfredson, R. K., & Joo, H. (2013). Best-Practice Recommendations for Defining, Identifying, and Handling Outliers. *Organizational Research Methods*, *16*(2), 270-301.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: a Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly, 34*(3), 613-643.

Anderson, J. C., & Gerbing, D. W. (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-step Approach. *Psychological Bulletin*, *103*(3), 411.

Arachchilage, N. A. G., & Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. *Computers in Human Behavior, 38*, 304-312.

Aurigemma, S. & Mattson, T. (2019). Generally Speaking, Context Matters: Making the Case for Increased Emphasis on Specific Threat Contexts in Information Security Behavior Research. *Journal of the Association for Information Systems, 20*(12), 1700-1742

Avey, J. B., Luthans, F., & Jensen, S. M. (2009). Psychological Capital: A Positive Resource for Combating Employee Stress and Turnover. *Human Resource Management, 48*(5), 677-693.

Avey, J. B., Reichard, R. J., Luthans, F., & Mhatre, K. H. (2011). Meta-Analysis of the Impact of Positive Psychological Capital on Employee Attitudes, Behaviors, and Performance. *Human Resource Development Quarterly, 22*(2), 127-152.

Bandura, A. (1986). The Explanatory and Predictive Scope of Self-Efficacy Theory. *Journal of Social and Clinical Psychology, 4*(3), 359-373.

Beaudry, A., & Pinsonneault, A. (2010). The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use. *MIS Quarterly, 34*(4), 689-710.

Bélanger, F., & Crossler, R. E. (2019). Dealing with Digital Traces: Understanding Protective Behaviors on Mobile Devices. *Journal of Strategic Information Systems, 28*(1), 34-49.

Block, L. G., & Keller, P. A. (1995). When to Accentuate the Negative: The Effects of Perceived Efficacy and Message Framing on Intentions to Perform a Health-related Behavior. *Journal of Marketing Research*, *32*(2), 192-203.

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.

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the Relationship of Organizational Insiders' Psychological Capital with Information Security Threat and Coping Appraisals. *Computers in Human Behavior, 68*, 190-209.

Burns, A. J., Roberts, T. L., Posey, C., & Lowry, P. B. (2019). The Adaptive Roles of Positive and Negative Emotions in Organizational Insiders' Engagement in Security-Based Precaution Taking. *Information Systems Research, 30*(4), 1228–1247.

Chen, Y., Galletta, D., Lowry, P. B., Luo, X., Moody, G. D., Willison, R. L. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research, 32*(3), 1043-1065.

Chen, H., Turel, O. and Yuan, Y. (2022). E-waste information security protection motivation: the role of optimism bias. *Information Technology & People, 35*(2), 600-620

Chen, Y., & Zahedi, F. M. (2016). Individual's Internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China. *MIS Quarterly, 40*(1), 205-222.

Chenoweth, T., Gattiker, T., & Corral, K. (2019). Adaptive and Maladaptive Coping with an IT Threat. *Information Systems Management, 36*(1), 24-39.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding Compliance with Bring Your Own Device Polcies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems, 28*(1), 209-226.

Culbertson, S. S., Fullagar, C. J., & Mills, M. (2010). Feeling Good and Doing Great: The Relationship Between Psychological Capital and Well-Being. *Journal of Occupational Health Psychology, 15*(4), 421-433.

de Hoog, N., Stroebe, W., & de Wit, J. B. F. (2007). The Impact of Vulnerability to and Severity of a Health Risk on Processing and Acceptance of Fear-Arousing Communications: A Meta-Analysis. *Review of General Psychology, 11*(3), 258-285.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting Information Security Culture: An Organizational Transformation Case Study. *Computers & Security, 56*, 63-69.

Dincelli, E., & Chengalur-Smith, I. (2020). Choose Your Own Training Adventure: Designing a Gamified SETA Artefact for Improving Information Security and Privacy Through Interactive Storytelling. *European Journal of Information Systems*, *29*(6): 669-687

Eckerd, S., DuHadway, S., Bendoly, E., Carter, C. R., & Kaufmann, L. (2021). On Making Experimental Design Choices: Discussions on the Use and Challenges of Demand

Effects, Incentives, Deception, Samples, and Vignettes. *Journal of Operations Management, 67*(2), 261-275.

Fredrickson, B. L. (1998). What Good Are Positive Emotions? *Review of General Psychology, 2*(3), 300-319.

Gable, S. L., & Haidt, J. (2005). What (and Why) Is Positive Psychology? *Review of General Psychology, 9*(2), 103-110.

Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's Comments: An Update and Extension to SEM Guidelines for Administrative and Social Science Research. *MIS Quarterly*, *35*(2), 3-14.

Gleicher, F., & Petty, R. E. (1992), Expectations of Re-assurance Influence the Nature of Fear-Stimulated Attitude Change. *Journal of Experimental Social Psychology*, *28*(1), 86-100.

Gollwitzer, P. M., & Sheeran, P. (2006). Implementation Intentions and Goal Achievement: A Meta-Analysis of Effects and Processes. *Advances in Experimental Social Psychology*, *38*, 69-119.

Gore, T. D., & Bracken, C. C. (2005). Testing the Theoretical Design of a Health Risk Message: Reexamining the Major Tenets of the Extended Parallel Process Model. *Health Education & Behavior, 32*(1), 27-41.

Hebb, D. O. (1946). On the Nature of Fear. *Psychological Review, 53*(5), 259-276.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2012). Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service. *Information Systems Journal, 24*(1), 61-84.

Hobfoll, S. E. (2011). Conservation of Resource Caravans and Engaged Settings. *Journal of Occupational and Organizational Psychology, 84*(1), 116-122.

Houts, S., & Kassab, C. (1997). Rotter's Social Learning Theory and Fear of Crime: Differences by Race and Ethnicity. *Social Science Quarterly*, *78*(1), 122-136.

Iyer, K. (2018). Less than 10% of Gmail Users Have Enabled Two-Factor Authentication: Google. Downloaded from https://beebom.com/less-than-10-of-gmail-users-have-enabled-two-factor-authentication-google/ on 11/21/2020.

Janis, I. L., & Feshbach, S. (1953). Effects of Fear-Arousing Communications. *Journal of Abnormal and Social Psychology, 48*(1), 78-92.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research, 30*(2), 199-218.

Jenkins, J. L., Durcikova, A., & Nunamaker Jr., J. F. (2021). Mitigating the Security Intention-Behavior Gap: The Moderating Role of Required Effort on the Intention-Behavior Relationship. *Journal of the Association for Information Systems*, 22(1), 246-272.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving Password Cybersecurity through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse through Keystroke-Dynamics Monitoring and Just-In-Time Fear Appeals. *Information Technology for Development, 20*(2), 196-213.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(3), 549-566.

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak Their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making. *Decision Sciences, 50*(2), 245-284.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and Situational Factors: Influences on Information Security Policy Violations. *European Journal of Information Systems, 25*(3), 231-251.

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.

Kaleta, J. P., Lee, J. S., & Yoo, S. (2019). Nudging with Construel Level Theory to Improve Online Password Use and Intended Password Choice: A Security-Usability Tradeoff Perspective. *Information Technology & People, 32*(4), 993-1020.

Kam, H. J., Mattson, T., & Goel, S. (2020). A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness. *Information Systems Frontiers, 22*(5), 1241-1264.

Kline, R. B. (2016). *Principles and Practice of Structural Equation Modeling, Fourth Edition*. New York: Guilford Publications.

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting Identity Theft: The Coping Perspective. *Decision Support Systems, 52*(2), 353-363.

Larson, M., & Luthans, F. (2006). Potential Added Value of Psychological Capital in Predicting Work Attitudes. *Journal of Leadership and Organizational Studies, 13*(2), 75-92.

LaTour, M. S., & Rotfeld, H. J. (1997). There Are Threats and (Maybe) Fear-Caused Arousal: Theory and Confusions of Appeals to Fear and Fear Arousal Itself. *Journal of Advertising, 26*(3), 45-59.

Lee, C. J., & Andrade, E. B. (2011). Fear, Social Projection, and Financial Decision Making. *Journal of Marketing Research, 48*(SPL), 121-129.

Lee, Y., & Kozar, K. A. (2005). Investigating Factors Affecting the Adoption of Anti-Spyware Systems. *Communications of the ACM, 48*(8), 72-77.

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly, 33*(1), 71-90.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. A. (2019). What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective. *MIS Quarterly, 43*(2), 373-394.

Linnenluecke, M. K. (2017). Resilience in Business and Management Research: A Review of Influential Publications and a Research Agenda. *International Journal of Management Reviews, 19*(1), 4-30.

Lonati, S., Quiroga, B. F., Zehnder, C., & Antonakis, J. (2018). On Doing Relevant and Rigorous Experiments: Review and Recommendations. *Journal of Operations Management*, *64*, 19-40.

Luthans, F. (2002a). The Need For and Meaning of Positive Organizational Behavior. *Journal of Organizational Behavior, 23*(6), 695-706.

Luthans, F. (2002b). Positive Organizational Behavior: Developing and Managing Psychological Strengths. *Academy of Management Perspectives, 16*(1), 57-72.

Luthans, F., Avey, J. B., Avolio, B. J., Norman, S. M., & Combs, G. M. (2006). Psychological Capital Development: Toward a Micro-Intervention. *Journal of Organizational Behavior, 27*(3), 387-393.

Luthans, F., Avey, J. B., & Patera, J. L. (2008). Experimental Analysis of a Web-based Training Intervention to Develop Positive Psychological Capital. *Academy of Management Learning & Education, 7*(2), 209-221.

Luthans, F., Avolio, B. J., Avey, J. B., & Norman, S. M. (2007). Positive Psychological Capital: Measurement and Relationship with Performance and Satisfaction. *Personnel Psychology, 60*(3), 541-572.

Luthans, F., & Broad, J. D. (2022). Positive Psychological Capital to Help Combat the Mental Health Fallout from the Pandemic and VUCA Environment. *Organizational Dynamics, 51*(2), 100817.

Luthans, F., Norman, S. M., Avolio, B. J., & Avey, J. B. (2008). The Mediating Role of Psychological Capital in the Supportive Organizational Climate: Employee Performance Relationship. *Journal of Organizational Behavior, 29*(2), 219-238.

Luthans, F., Vogelgesang, G. R., & Lester, P. B. (2006). Developing the Psychological Capital of Resiliency. *Human Resource Development Review, 5*(1), 25-44.

Luthans, F., & Youssef-Morgan, C. M. (2017). Psychological Capital: An Evidenced-Based Positive Approach. *Annual Review of Organizational Psychology and Organizational Behavior, 4*(1), 339-366.

Luthans, F., Youssef, C. M., & Rawski, S. L. (2011). A Tale of Two Paradigms: The Impact of Psychological Capital and Reinforcing Feedback on Problem Solving and Innovation. *Journal of Organizational Behavior Management, 31*(4), 333-350.

Masten, A. S. (2001). Ordinary Magic: Resilience Processes in Development. *American Psychologist, 56*(3), 227-238.

Mears, D. P., & Stewart, E. A. (2010). Interracial Contact and Fear of Crime. *Journal of Criminal Justice and Popular Culture*, *38*(1), 34-41.

Mewborn, C. R., & Rogers, R. W. (1979). Effects of Threatening and Reassuring Components of Fear Appeals on Physiological and Verbal Measures of Emotion and Attitudes. *Journal of Experimental Social Psychology*, *15*(3), 242-253.

Mitchell, N. L., & Schulman, K. R. (1981). The Child and the Fear of Death*. Journal of the National Medical Association*, *73*(10), 963.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Security Policy Compliance. *MIS Quarterly, 42*(1), 285-A22.

Muthén, L.K. & Muthén, B.O. (2017). *Mplus User's Guide, Eighth Edition*. Los Angeles, CA: Muthén & Muthén.

Newman, A., Ucbasaran, D., Zhu, F., & Hirst, G. (2014). Psychological Capital: A Review and Synthesis, *Journal of Organizational Behavior*, *35*(1), 120-138.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems, 46*(4), 815-825.

Orazi, D. C., Warkentin, M., & Johnston, A. C. (2019). Integrating Construal-level Theory in Designing Fear Appeals in IS Security Research. *Communications of the Association for Information Systems*, *45*(1), 397-410.

Pérez-González, D., Preciado, S. T., & Solana-Gonzalez, P. (2019). Organizational Practices as Antecedents of the Information Security Management Performance: An Empirical Investigation. *Information Technology & People, 32(*5), 1262-1275

Peterson, C. (2000). The Future of Optimism. *American Psychologist, 55*(1), 44-55.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of Method Bias in Social Science Research and Recommendations on How to Control It. *Annual Review of Psychology, 63*(1), 539-569.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Rai, A. (2020). Explainable AI: From Black Box to Glass Box. *Journal of the Academy of Marketing Science*, *48*(1), 137–141.

Ray, J. J., & Najman, J. M. (1986). The Generalizability of Deferment of Gratification. *Journal of Social Psychology, 126*(1), 117-119.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior. *Computers & Security, 28*(8), 816-826.

Rhee, H-S., Ryu, Y. U., Kim, C. (2012). Unrealistic Optimism on Information Security Management. *Computers & Security*, *31*(2), 221-232.

Richardson, H., Simmering, M., & Sturman, M. (2009). A Tale of Three Perspectives: Examining Post Hoc Statistical Techniques for Detection and Correction of Common Method Variance. *Organizational Research Methods, 12*(4), 762–800.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. in J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153-176). Guilford.

Rönkkö, M., & Cho, E. (2022). An updated guideline for assessing discriminant validity. *Organizational Research Methods*, *25*(1), 6-14.

Ropovik, I. (2015). A Cautionary Note on Testing Latent Variable Models. *Frontiers in Psycholog*y, *6,* 1715.

Ruiter, R. A. C., Kessels, L. T. E., Peters, G.-J. Y., & Kok, G. (2014). Sixty Years of Fear Appeal Research: Current State of the Evidence. *International Journal of Psychology, 49*(2), 63-70.

Schneider, S. L. (2001). In Search of Realistic Optimism: Meaning, Knowledge, and Warm Fuzziness. *American Psychologist, 56*(3), 250-263.

Schuetz, S. W., Lowry, P. B., Pienta, D., & Thatcher, J. B. (2020). Effectiveness of Abstract versus Concrete Fear Appeals in Information Security. *Journal of Management Information Systems, 37*(3), 723-757.

Seligman, M. E. P., & Csikszentmihalyi, M. (2000). Positive Psychology: An Introduction. *American Psychologist, 55*(1), 5-14.

Seo, B.-G., & Park, D.-H. (2019). The Effect of Message Framing on Security Behavior in Online Services: Focusing on the Shift of Time Orientation via Psychological Ownership. *Computers in Human Behavior, 93*, 357-369.

Scherer, K. R. (2005) What are emotions? And how can they be measured? *Social Science Information, 44*(4), 693-727.

Sheeran, P. (2002). Intention-Behavior Relations: A Conceptual and Empirical Review. *European Review of Social Psychology*, 12(1), 1-36.

Sheeran, P., & Webb, T. L. (2016). The Intention-Behavior Gap. *Social and Personality Psychology Compass*, *10*(9), 503-518.

Shin, J., Taylor, M. S., & Seo, M.-G. (2012). Resources for Change: The Relationships of Organizational Inducements and Psychological Resilience to Employees' Attitudes and Behaviors Toward Organizational Change. *Academy of Management Journal, 55*(3), 727-748.

Snyder, C. R., & Rand, K. L. (2003). The Case Against False Hope. *American Psychologist, 58*(10), 820-822.

Spector, P. E., Rosen, C. C., Richardson, H. A., Williams, L. J., & Johnson, R. E. (2019). A new perspective on method variance: A measure-centric approach. *Journal of Management, 45*(3), 855–880.

Stafford, T. F., & Poston, R. (2010). Online Security Threats and Computer User Intentions. *Computer, 43*(1), 58-64.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security Begins at Home": Determinants of Home Computer and Mobile Device Security Behavior. *Computers & Security, 70*, 376-391.

Tsai, H.-y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security, 59*, 138-150.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to Cope with Information Security Risks Regarding Mobile Device Loss or Theft: An Empirical Examination. *Information & Management, 52*(4), 506-517.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of Protective Security Behavior: A Longitudinal Study. *Decision Support Systems, 92*(1), 25-35.

Williams, K. C. (2012). Fear Appeal Theory. *Research in Business Economics Journal, 5*(1), 1-21.

Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs, 59*(4), 329-349.

Witte, K., Cameron, K. A., Mckeon, J. K., & Berkowitz, J. M. (1996). Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. *Journal of Health Communication, 1*(4), 317-342.

Witte, K. (1998). Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Process Model to Explain Fear Appeal Successes and Failures. In P. A. Anderson & L. K. Guerrero (Eds.), *Handbook of Communication and Emotion: Research, Theory, Application, and Contexts* (pp. 423-450). San Diego, CA: Academic Press.

Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. *Health Education & Behavior, 27*(5), 591-615.

Witte, K., Meyer, G., & Martell, D. (2001). *Effective Health Risk Messages: A Step-By-Step Guide*. Thousand Oaks: Sage Publications.

Xin, T., Siponen, M., Chen, S. (2021). Understanding the Inward Emotion-Focused Coping Strategies of Individual Users in Response to Mobile Malware Threats. *Behaviour & Information Technology*, 1-25.

Xu, F., Luo, X. R., Hsu, C. (2020). Anger or Fear? Effects of Discrete Emotions on Employee's Computer-related Deviant Behavior. *Information & Management, 57*(3), 103180

Zizzo, D. J. (2010). Experimenter Demand Effects in Economics Experiments. *Experimental Economics, 13*(1), 75-98.

Appendix A

Table A1. *Psychological Capital Construct Definitions and Measurement Items*

Construct	Conceptual Definition	Original Measurement Items in Behavioral Security Context	Our Survey Question/Measurement Item	Item
Hope	Hope is a positive motivational state based on goal directed behaviors with specific plans to meet those goals (Luthans et al., 2007a; Luthans et al., 2011)	At the present time, I am energetically pursuing my work goals (Luthans et al., 2007b).	At the present time, I am energetically pursuing my goals to protect my online accounts from being accessed by cyber-criminals by using password manager applications [2FA services].	HOP1
		Right now, I see myself as being pretty successful at work (Luthans et al., 2007b).	Right now, I see myself as being pretty successful at protecting my online accounts from being accessed by cyber-criminals by using password manager applications [2FA services].	HOP2
		At this time, I am meeting the work goals that I set for myself (Luthans et al., 2007b).	At this time, I am meeting the goals I set for myself regarding protecting my online accounts from being accessed by cyber-criminals by using password manager applications [2FA services].	HOP3
Optimism	Optimism is an explanatory style that explains outcomes in terms of positive variables (Peterson, 2000)	When things are uncertain for me at work, I usually expect the best (Luthans et al., 2007b).	I usually expect the best when things are uncertain for me regarding protecting my online accounts from being accessed by cyber-criminals by using password manager applications [2FA services].	OPT1
		I always look on the bright side of things regarding my job (Luthans et al., 2007b).	I always look on the bright side of things regarding protecting my online accounts from being accessed by cyber-criminals by using password manager applications [2FA services].	OPT2
		I'm optimistic about what will happen to me in the future as it pertains to work (Luthans et al., 2007b).	I'm optimistic about what will happen to me in the future as it pertains to protecting my online accounts from being accessed by cyber-criminals by using password manager applications [2FA services].	OPT3
Resilience	Resilience is the capacity to bounce back from negative events and to grow further	I usually manage difficulties one way or another at work (Luthans et al., 2007b).	One way or the other, I usually manage difficulties regarding the use of password manager applications [2FA services] to protect my online accounts from being accessed by cyber-criminals.	RES1

	from positive events (Luthans, 2002a, 2002b)	I usually take stressful things at work in stride (Luthans et al., 2007b).	I usually take stressful things associated with using password manager applications [2FA services] to protect my online accounts from being accessed by cyber-criminals in stride.	RES2
		I feel I can handle many things at a time at this job (Luthans et al., 2007b).	I feel I can handle many things at a time while using password manager applications [2FA services] to protect my online accounts from being accessed by cyber-criminals.	RES3
Self-efficacy	Self-efficacy represents an individual's belief that they are capable of performing a specific behavior (Bandura, 1986)	Anti-spyware software is easy to use (Johnston & Warkentin 2010).	Password manager applications [2FA services] are easy to use.	SE1
		Anti-spyware software is convenient to use (Johnston & Warkentin 2010).	Password manager applications [2FA services] are convenient to use.	SE2
		I am able to use anti-spyware software without much effort. (Johnston & Warkentin 2010).	I am able to use password manager applications [2FA services] without much effort.	SE3

Note: Study 1 focused on the use of password manager applications. Study 2 focused on the use of 2FA services. The measurement items were the same for both studies except we changed the []s to the appropriate security technology.

Table A2. *Fear Appeals Model and Conditioned Fear Construct Definitions and Measurement Items*

Construct	Conceptual Definition	Original Measurement Items in Behavioral Security Context	Our Survey Question/Measurement Item	Item
Perceived Threat Vulnerability	"How personally susceptible an individual feels to the communicated threat" (Milne, Sheeran, & Orebell, 2000, p. 108)	My computer is at risk for becoming infected with spyware (Johnston & Warkentin 2010).	My online account passwords are at risk of being stolen and abused by cyber-criminals	PVUL1
		It is likely that my computer will become infected with spyware (Johnston & Warkentin 2010).	It is likely that my online account passwords will be stolen and abused by cyber-criminals.	PVUL2
		It is possible that my computer will become infected with spyware (Johnston & Warkentin 2010).	It is possible that my online account passwords will be stolen and abused by cyber-criminals.	PVUL3
Perceived Threat Severity	"How serious the individual believes that the threat would be" to him- or herself (Milne et al., 2000, p. 108)	If my computer were infected by spyware, it would be severe (Johnston & Warkentin 2010).	If my online account passwords were stolen and abused by cyber-criminals, it would be severe.	TSEV1
		If my computer were infected by spyware, it would be serious (Johnston & Warkentin 2010).	If my online account passwords were stolen and abused by cyber-criminals, it would be serious.	TSEV2
		If my computer were infected by spyware, it would be significant (Johnston & Warkentin 2010).	If my online account passwords were stolen and abused by cyber-criminals, it would be significant.	TSEV3
Response Efficacy	"The belief that the adaptive [coping] response will work, that taking the protective action will be effective in protecting the self or others" (Floyd, Prentice-Dunn, & Rogers, 2000, p. 411; Maddux & Rogers, 1983)	Anti-spyware software works for protection (Johnston & Warkentin 2010).	Password manager applications [2FA services] work to protect my online account passwords from being stolen and abused by cyber-criminals.	REFF1
		Anti-spyware software is effective for protection (Johnston & Warkentin 2010).	Password manager applications [2FA services] are an effective solution to protect my online account passwords from being stolen and abused by cyber-criminals.	REFF2
		When using anti-spyware software, a computer is more likely to be protected (Johnston & Warkentin 2010).	When using a password manager application [2FA services], online passwords are more likely to be protected from being stolen and abused by cyber-criminals.	REFF3
Behavioral Intentions		I intend to use anti-spyware software in the next 3 months (Johnston & Warkentin 2010).	I intend to use a password manager [2FA services] in the next week.	BINT1

	Self-reported intention to perform the security behavior.	I predict I will use anti-spyware software in the next 3 months (Johnston & Warkentin 2010).	I predict I will use a password manager [2FA services] in the next week.	BINT2
		I plan to use anti-spyware e software in the next 3 months (Johnston & Warkentin 2010).	I plan to use a password manager [2FA services] in the next week.	BINT3
Conditioned Fear	A negatively valenced emotion representing a response that arises from recognizing danger. This response may include any combination of apprehension, fright, arousal, concern, worry, discomfort, or a general negative mood, and it manifests itself emotionally, cognitively, and physically (Witte, 1992, 1996)	When thinking about the security threats to your organization's information and information systems, to what extent do you feel nervous (Posey et al., 2015)?	I am worried about the prospect of having my online accounts accessed and abused by cybercriminals.	FEAR1
		When thinking about the security threats to your organization's information and information systems, to what extent do you feel frightened (Posey et al., 2015)?	I am frightened about the prospect of having my online accounts accessed and abused by cybercriminals.	FEAR2
		When thinking about the security threats to your organization's information and information systems, to what extent do you feel anxious (Posey et al., 2015)?	I am anxious about the prospect of having my online accounts accessed and abused by cybercriminals.	FEAR3
Self-efficacy[1]	Self-efficacy represents an individual's belief that they are capable of performing a specific behavior (Bandura, 1986)	Anti-spyware software is easy to use (Johnston & Warkentin 2010).	Password manager software [2FA services] is easy to use.	SE1
		Anti-spyware software is convenient to use (Johnston & Warkentin 2010).	Password manager software [2FA services] is convenient to use.	SE2
		I am able to use anti-spyware software without much effort (Johnston & Warkentin 2010).	I am able to use password software [2FA services] without much effort.	SE3
Response Costs	"Any costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response" (Floyd et al., 2000, p. 411)	There are too many overheads associated with trying to enable security measures on a home wireless network (Woon et al., 2005).	There is too much work associated with trying to increase the security of my online account. passwords through the use of a password manager application [2FA services].	COST1
		Enabling security features on my wireless router would require considerable investment of effort other than time (Woon et al., 2005).	Using a password manager application [2FA services] on my computer would require considerable investment of effort other than time.	COST2

	Enabling security features on a wireless router would be time consuming (Woon et al., 2005).	Using a password manager application [2FA services] would be time consuming.	COST3

Note: Study 1 focused on the use of password manager applications. Study 2 focused on the use of 2FA services. The measurement items were the same for both studies except we changed the []s to the appropriate security technology.

[1] Self-efficacy has the same theoretical origins and conceptual definition in both the Fear Appeal Model and Psychological Capital literature.

Table A3. *Unmodeled Latent Construct (UMLC) Test for Common Method Bias*

		Study 1 (Password Manager)					Study 2 (2 Factor Authentication)				
		CFA		CFA with UMLC			CFA		CFA with UMLC		
		χ2	df	χ2	df		χ2	df	χ2	df	
		450.7	360	407.339	330		515.13	360	472.338	330	
Construct	**Item**	**β**	**s.e.**	**β**	**s.e.**	**Δβ**	**β**	**s.e.**	**β**	**s.e.**	**Δβ**
Hope	HOP1	0.67	0.048	0.638	0.06	0.032	0.61	0.056	0.656	0.048	-0.046
	HOP2	0.756	0.042	0.732	0.081	0.024	0.76	0.043	0.744	0.06	0.016
	HOP3	0.697	0.046	0.651	0.056	0.046	0.833	0.039	0.794	0.05	0.039
Self-efficacy	SE1	0.766	0.033	0.759	0.038	0.007	0.922	0.022	0.923	0.025	-0.001
	SE2	0.891	0.024	0.886	0.025	0.005	0.801	0.031	0.825	0.036	-0.024
	SE3	0.825	0.028	0.831	0.028	-0.006	0.846	0.029	0.838	0.026	0.008
Resilience	RES1	0.703	0.048	0.699	0.057	0.004	0.634	0.057	0.613	0.054	0.021
	RES2	0.72	0.046	0.716	0.046	0.004	0.665	0.052	0.694	0.059	-0.029
	RES3	0.597	0.054	0.596	0.053	0.001	0.829	0.043	0.82	0.049	0.009
Optimism	OPT1	0.783	0.038	0.777	0.039	0.006	0.653	0.058	0.592	0.064	0.061
	OPT2	0.742	0.04	0.741	0.04	0.001	0.771	0.053	0.719	0.078	0.052
	OPT3	0.78	0.038	0.771	0.045	0.009	0.639	0.059	0.701	0.081	-0.062
Behavioral Intentions	BINT1	0.932	0.01	0.899	0.031	0.033	0.904	0.016	0.849	0.04	0.055
	BINT2	0.989	0.006	0.936	0.035	0.053	0.993	0.009	0.935	0.045	0.058
	BINT3	0.91	0.013	0.854	0.038	0.056	0.888	0.018	0.845	0.046	0.043
	FEAR1	0.783	0.029	0.786	0.033	-0.003	0.878	0.023	0.85	0.034	0.028

Conditioned Fear	FEAR2	0.9	0.02	0.858	0.033	0.042	0.879	0.022	0.866	0.041	0.013
	FEAR3	0.913	0.02	0.872	0.033	0.041	0.908	0.02	0.88	0.038	0.028
Perceived Threat Severity	TSEV1	0.734	0.036	0.714	0.04	0.02	0.828	0.03	0.825	0.04	0.003
	TSEV2	0.982	0.028	0.963	0.033	0.019	0.91	0.024	0.903	0.034	0.007
	TSEV3	0.723	0.037	0.701	0.042	0.022	0.805	0.032	0.808	0.046	-0.003
Perceived Threat Vulnerability	PVUL1	0.793	0.045	0.791	0.045	0.002	0.771	0.047	0.757	0.051	0.014
	PVUL2	0.867	0.045	0.886	0.041	-0.019	0.757	0.05	0.754	0.051	0.003
	PVUL3	0.564	0.053	0.555	0.053	0.009	0.72	0.049	0.763	0.051	-0.043
Response Efficacy	REFF1	0.773	0.036	0.724	0.047	0.049	0.723	0.041	0.668	0.071	0.055
	REFF2	0.901	0.029	0.891	0.035	0.01	0.902	0.026	0.838	0.057	0.064
	REFF3	0.698	0.04	0.678	0.044	0.02	0.843	0.03	0.775	0.065	0.068
Response Cost	COST1	0.883	0.023	0.882	0.023	0.001	0.807	0.037	0.804	0.039	0.003
	COST2	0.783	0.03	0.786	0.034	-0.003	0.812	0.036	0.766	0.057	0.046
	COST3	0.884	0.023	0.882	0.023	0.002	0.792	0.038	0.772	0.041	0.02

Table A4. *Confirmatory Factor Analysis (CFA) for Study 1*

Construct	Item	Factor Load	CR	HOPE	SE	RES	OPT	BINT	FEAR	TSEV	PVUL	REFF	COST	PSYCAP
Hope	HOP1	0.67	0.751	1.00	[.180, .517]	[.658, .874]	[.441, .677]	[.200, .475]	[-.135, .175]	[-.016, .281]	[-.128, .200]	[.004, .318]	[-.414, -.120]	-
	HOP2	0.756												
	HOP3	0.697												
Self-efficacy	SE1	0.766	0.868	0.172	1.00	[.155, .469]	[.100, .431]	[.255, .495]	[.026, .306]	[.033, .305]	[.035, .326]	[.441, .659]	[-.612, -.385]	-
	SE2	0.891												
	SE3	0.825												
Resilience	RES1	0.703	0.714	0.766	0.169	1.00	[.548, .788]	[.061, .356]	[-.107, .209]	[-.097, .211]	[-.119, .222]	[.055, .371]	[-.280, .043]	-
	RES2	0.72												
	RES3	0.597												
Optimism	OPT1	0.783	0.812	0.489	0.16	0.527	1.00	[.217, .474]	[-.121, .178]	[-.063, .225]	[-.139, .173]	[.022, .321]	[-340, -.048]	-
	OPT2	0.742												
	OPT3	0.78												
Behavioral Intentions	BINT1	0.932	0.96	0.338	0.375	0.208	0.346	1.00	[.080, .340]	[-.019, .242]	[.068, .344]	[.134, .394]	[-.460, -.215]	[.258, .535]
	BINT2	0.989												
	BINT3	0.91												
Conditioned Fear	FEAR1	0.783	0.901	0.02	0.166	0.051	0.028	0.21	1.00	[.035, .305]	[.215, .480]	[-.074, .214]	[-.087, .198]	[-.102, .213]
	FEAR2	0.9												
	FEAR3	0.913												
Perceived Threat Severity	TSEV1	0.734	0.792	0.132	0.169	0.057	0.081	0.112	0.17	1.00	[-.063, .227]	[.104, .373	[-.255, .018]	[-.016, .288]
	TSEV2	0.982												
	TSEV3	0.723												
	PVUL1	0.793	0.842	0.036	0.181	0.052	0.017	0.206	0.348	0.082	1.00	[.090,	[-.186,	[-.103,

Perceived Threat Vulnerability	PVUL2	0.867										.378]	.111]	.266]
	PVUL3	0.564												
Response Efficacy	REFF1	0.773	0.836	0.161	0.55	0.213	0.172	0.264	0.07	0.238	0.234	1.00	[-.417,	[.131,
	REFF2	0.901											-.147]	.451]
	REFF3	0.698												
Response Cost	COST1	0.883	0.887	-0.267	-0.499	-0.119	-0.194	-0.338	0.056	-0.119	-0.038	-0.282	1.00	[-.457,
	COST2	0.783												-.149]
	COST3	0.884												
Psychological Capital	HOP	0.844	0.754	-	-	-	-	0.397	0.056	0.136	0.061	0.291	-0.303	1.00
	SE	0.204												
	RES	0.903												
	OPT	0.583												

Note: Composite Reliability (CR), Perceived Vulnerability to Threat (PVUL), Perceived Threat Severity (TSEV), Response Efficacy (REFF), Response Costs (COST), Resilience (RES), Optimism (OPT), Hope (HOP), Behavioral Intentions (BINT), Self-efficacy (SE), Psychological Capital (PSYCAP), and Conditioned Fear (FEAR).

Diagonal numbers are same-construct correlations (value = 1). Off diagonal numbers below the diagonal are inter-construct correlations. Off diagonal numbers above the diagonal are construct correlation confidence intervals (lower 2.5%, upper 2.5%).

Table A5. *Confirmatory Factor Analysis (CFA) for Study 2*

Construct	Item	Factor Load	CR	HOPE	SE	RES	OPT	BINT	FEAR	TSEV	PVUL	REFF	COST	PSYCAP
Hope	HOP1	0.61	0.782	1.00	[.036, .430]	[.607, .841]	[.412, .710]	[.054, .373]	[-.26, .075]	[-.122, .224]	[-.259, .105]	[.012, .348]	[-.339, .008]	-
	HOP2	0.76												
	HOP3	0.833												
Self-efficacy	SE1	0.922	0.893	0.194	1.00	[-.074, .328]	[.028, .404]	[.335, .588]	[-.013, .302]	[-.002, .315]	[-.005, .333]	[.408, .653]	[-.672, -.42]	-
	SE2	0.801												
	SE3	0.846												
Resilience	RES1	0.634	0.755	0.724	0.052	1.00	[.386, .698]	[.125, .435]	[-.267, .076]	[-.076, .27]	[-.273, .096]	[-.088, .262]	[-.292, .069]	-
	RES2	0.665												
	RES3	0.829												
Optimism	OPT1	0.653	0.73	0.561	0.176	0.542	1.00	[-.09, .251]	[-.205, .149]	[-.208, .15]	[-.327, .05]	[.015, .366]	[-.243, .129]	-
	OPT2	0.771												
	OPT3	0.639												
Behavioral Intentions	BINT1	0.904	0.95	0.214	0.461	0.28	0.08	1.00	[.033, .33]	[.127, .416]	[.05, .392]	[.146, .434]	[-.558, -.285]	[.084, .454]
	BINT2	0.993												
	BINT3	0.888												
Conditioned Fear	FEAR1	0.878	0.917	-0.093	0.144	-0.096	-0.028	0.181	1.00	[.271, .545]	[.347, .624]	[.01, .326]	[-.23, .101]	[-.261, .088]
	FEAR2	0.879												
	FEAR3	0.908												
Perceived Threat Severity	TSEV1	0.828	0.885	0.051	0.156	0.097	-0.029	0.271	0.408	1.00	[.309, .600]	[.325, .593]	[-.413, -.094]	[-.101, .252]
	TSEV2	0.91												
	TSEV3	0.805												
	PVUL1	0.771	0.794	-0.077	0.164	-0.089	-0.138	0.226	0.486	0.454	1.00	[.17,	[-.323,	[-.288,

Perceived Threat Vulnerability	PVUL2	0.757										.493]	.028]	.087]
	PVUL3	0.72												
Response Efficacy	REFF1	0.723	0.865	0.18	0.5312	0.087	0.191	0.29	0.168	0.459	0.332	1.00	[-.605,	[.042,
	REFF2	0.902											-.33]	.392]
	REFF3	0.843												
Response Cost	COST1	0.807	0.845	-0.165	-0.546	-0.111	-0.057	-0.422	-0.064	-0.254	-0.148	-0.468	1.00	[-.373, -.012]
	COST2	0.812												
	COST3	0.792												
Psychological Capital	HOP	0.89	0.755	-	-	-	-	0.178	-0.048	0.039	-0.051	0.087	-0.011	1.00
	SE	0.173												
	RES	0.82												
	OPT	0.651												

Note: Composite Reliability (CR), Perceived Vulnerability to Threat (PVUL), Perceived Threat Severity (TSEV), Response Efficacy (REFF), Response Costs (COST), Resilience (RES), Optimism (OPT), Hope (HOP), Behavioral Intentions (BINT), Self-efficacy (SE), Psychological Capital (PSYCAP), and Conditioned Fear (FEAR).

Diagonal numbers are same-construct correlations (value = 1). Off diagonal numbers below the diagonal are inter-construct correlations. Off diagonal numbers above the diagonal are construct correlation confidence intervals (lower 2.5%, upper 2.5%).

Table A6. *CBSEM Model Fit and Structural Path Results for Study 1*

Model	**FAM with PsyCap (Figure 1)**	**FAM with HOP**	**FAM with SE**	**FAM with RES**	**FAM with OPT**
χ2	564.29	192.753	194.933	191.843	158.724
df	380	168	168	168	168
p	0.014	0.454	0.526	0.461	0.857
RMSEA	0.046	0.025	0.026	0.025	0
CFI	0.952	0.991	0.991	0.991	1
SRMR	0.083	0.04	0.038	0.041	0.035
R^2	0.29	0.253	0.216	0.216	0.268
	β	**β**	**β**	**β**	**β**
PVUL → BINT	0.112	0.105	0.094	0.102	0.12
TSEV → BINT	-0.009	-0.017	0.006	0.005	0.0001
REFF → BINT	0.069	0.114	0.066	0.113	0.098
COST → BINT	-0.239**	-0.257***	-0.235**	-0.296***	-0.269***
FEAR → BINT	0.164*	0.182**	0.154*	0.175*	.0.165*
PSYCAP → BINT	0.303**				
PSYCAP * Fear → BINT	-0.09				
HOP → BINT		0.246**			
HOP * Fear → BINT		-0.085			
SEFF → BINT			0.178 (p=0.089)		
SEFF * Fear → BINT			-0.015		
RES → BINT				0.134 (p=.088)	
RES * Fear → BINT				-0.026	

OPT → BINT	0.27***
OPT * Fear → BINT	-0.08

Note: Fear Appeals Model (FAM), Perceived Vulnerability to Threat (PVUL), Perceived Threat Severity (TSEV), Response Efficacy (REFF), Response Costs (COST), Resilience (RES), Optimism (OPT), Hope (HOP), Behavioral Intentions (BINT), Self-efficacy (SE), Psychological Capital (PSYCAP), and Conditioned Fear (FEAR)
* = $p < 0.05$ ** = $p < 0.001$ *** = $p < 0.001$

Table A7. *CBSEM Model Fit and Structural Path Results for Study 2*

Model	**FAM with PsyCap (Figure 1)**	**FAM with HOP**	**FAM with SE**	**FAM with RES**	**FAM with OPT**
χ2	616.45	256.275	261.633	239.349	231.007
df	380	168	168	168	168
p	0.008	0.035	0.045	0.089	0.117
RMSEA	0.059	0.054	0.056	0.049	0.046
CFI	0.925	0.962	0.963	0.969	0.972
SRMR	0.101	0.049	0.049	0.049	0.049
R^2	0.297	0.242	0.298	0.278	0.221
	β	**β**	**β**	**β**	**β**
PVUL → BINT	0.099	0.084	0.079	0.084	0.099
TSEV → BINT	0.064	0.075	0.163	0.038	0.103
REFF → BINT	-0.003	0.012	-0.12	0.047	0.018
COST → BINT	-0.318**	-0.333**	-0.21*	-0.321**	0.358***
FEAR → BINT	0.151	0.151	0.067	0.144	0.064
PSYCAP → BINT	0.254**				
PSYCAP * Fear → BINT	-0.141*				
HOP → BINT		0.182*			
HOP * Fear → BINT		-0.146 (p=.056)			
SEFF → BINT			0.377**		
SEFF * Fear → BINT			-0.119		
RES → BINT				0.261**	
RES * Fear → BINT				-0.138 (p=.059)	
OPT → BINT					0.06

OPT * Fear → BINT	0.042

Note: Fear Appeals Model (FAM), Perceived Vulnerability to Threat (PVUL), Perceived Threat Severity (TSEV), Response Efficacy (REFF), Response Costs (COST), Resilience (RES), Optimism (OPT), Hope (HOP), Behavioral Intentions (BINT), Self-efficacy (SE), Psychological Capital (PSYCAP), and Conditioned Fear (FEAR)
* = $p < 0.05$ ** = $p < 0.001$ *** = $p < 0.001$

Table A8. *Measurement Invariance Test for Study 1*

Model	**Parameters**	**χ2**	**df**	**p**	**CFI**	**RMSEA**	**SRMR**
Configural	270	1013.13	720	<0.05	0.904	0.067	0.075
Metric	250	1036.79	740	<0.05	0.903	0.067	0.081
Models Compared			**Δdf**	**p**			
Metric against Configural		23.66	20	0.257			

Configural model has no constraints; Metric model has constrained factor loads

Table A9. *Measurement Invariance Test for Study 2*

Model	Parameters	χ2	df	p	CFI	RMSEA	SRMR
Configural	270	933.59	720	<0.05	0.946	0.05	0.064
Metric	250	954.55	740	<0.05	0.945	0.05	0.068
Models Compared			**Δdf**	**p**			
Metric against Configural		20.96	20	0.399			

Configural model has no constraints; Metric model has constrained factor loads.

References

Bandura, A. (1986). The Explanatory and Predictive Scope of Self-Efficacy Theory. *Journal of Social and Clinical Psychology, 4*(3), 359-373.

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.

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

Luthans, F. (2002a). The Need For and Meaning of Positive Organizational Behavior. *Journal of Organizational Behavior, 23*(6), 695-706.

Luthans, F. (2002b). Positive Organizational Behavior: Developing and Managing Psychological Strengths. *Academy of Management Perspectives, 16*(1), 57-72.

Luthans, F., Avolio, B. J., Avey, J. B., & Norman, S. M. (2007a). Positive Psychological Capital: Measurement and Relationship with Performance and Satisfaction. *Personnel Psychology, 60*(3), 541-572.

Luthans, F., Youssef, C. M., & Avolio, B. J. (2007b). Psychological Capital: Developing the Human Competitive Edge.

Luthans, F., Youssef, C. M., & Rawski, S. L. (2011). A Tale of Two Paradigms: The Impact of Psychological Capital and Reinforcing Feedback on Problem Solving and Innovation. *Journal of Organizational Behavior Management, 31*(4), 333-350.

Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

Milne, S., Sheeran, P., & Orebell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

Peterson, C. (2000). The Future of Optimism. *American Psychologist, 55*(1), 44-55.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs, 59*(4), 329-349.

Witte, K. (1996). Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. *Journal of Health Communication, 1*(4), 317-342.

Woon, I., Tan, G. W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *ICIS 2005 Proceedings.* 31.