Blurring Safety Between Online and Offline Worlds:

Archival, Correlational, and Experimental Evidence of

Generalized Threat in the Digital Age

by

Jessica E. Bodford

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved April 2017 by the
Graduate Supervisory Committee:

Virginia S. Y. Kwan, Chair
Bradley Adame
Douglas Kenrick
Paulo Shakarian

ARIZONA STATE UNIVERSITY

May 2017

ABSTRACT

Decades of research in cyberpsychology and human-computer interaction has pointed to a strong distinction between the online and offline worlds, suggesting that attitudes and behaviors in one domain do not necessarily generalize to the other. However, as humans spend increasing amounts of time in the digital world, psychological understandings of safety may begin to influence human perceptions of threat while online. This dissertation therefore examines whether perceived threat generalizes between domains across archival, correlational, and experimental research methods. Four studies offer insight into the relationship between objective indicators of physical and online safety on the levels of nation and state; the relationship between perceptions of these forms of safety on the individual level; and whether experimental manipulations of one form of threat influence perceptions of threat in the opposite domain. In addition, this work explores the impact of threat perception-related personal and situational factors, as well as the impact of threat type (i.e., self-protection, resource), on this hypothesized relationship.

Collectively, these studies evince a positive relationship between physical and online safety in macro-level actuality and individual-level perception. Among individuals, objective indicators of community safety—as measured by zip code crime data—were a positive reflection of perceptions of physical safety; these perceptions, in turn, mapped onto perceived online safety. The generalization between perceived physical threat and online threat was stronger after being exposed to self-protection threat manipulations, possibly underscoring the more dire nature of threats to bodily safety than those to valuable resources. Most notably, experimental findings suggest that it is not the physical that informs the digital, but rather the opposite: Online threats blur more readily into physical domains, possibly speaking to the concern that dangers specific to the digital world will bleed into the physical one. This generalization of threat may function as a strategy to prepare oneself for future dangers wherever they might appear; and indeed, perceived threat in either world positively influenced desires to act on recommended safety practices. Taken together, this research suggests that in the realm of threat perception, the boundaries between physical and digital are less rigid than may have been previously believed.

To Virginia, who gave me a chance when
cyberpsychology was still in its infancy;

and to my favorite beard and co-pilot, for harboring
an identical optimism that this digitally connected
world will solve more problems than it creates.

ACKNOWLEDGMENTS

I gratefully acknowledge the National Science Foundation for funding early iterations of this research through the Graduate Research Fellowship Program (Grant No. 12-061). I would also like to express my sincerest gratitude to Facebook, Inc. for funding this dissertation, for approaching this area of work with enthusiasm, and for teaching me to never mistake motion for progress.

TABLE OF CONTENTS

Page

Page

APPENDIX

LIST OF TABLES

Table Page

Table Page

Table Page

LIST OF FIGURES

Figure Page

For millions of years, humans have been faced with external threats to safety. In recent decades, however, *safety* has increasingly incorporated two key environments: the historically physical milieu and the ever-growing reach of the digital world. The present paper concerns the translation of physical safety into safety while online—a dynamically evolving environment in which the average American adult spends 11 hours each day (Nielsen, 2016). The online world now presents new threats that do not appear in our traditional representations; predators, gunshots, and tell-tale signs of toxic substances do not necessarily translate into a disembodied world. However, the threats encountered in the digital age are not to be disregarded: In 2015 alone, a third of Americans were victims of healthcare data breaches (Bitglass, 2016) and on average, victims of phishing scams lost a median amount of $560 (Internet Crime Complaint Center, 2015). Social media sharing of geotagged locations contribute to the ease and prevalence of cyberstalking, and approximately one person becomes a victim of identity fraud every two seconds (Pascual, 2014). Collectively, although online threats do not appear to closely approximate threats in the physical world, they may pose as much danger to human lives.

As our physical world becomes increasingly intertwined with the digital one, we might expect a generalized—or blurring—effect in which physical social cues that guide attitudes and behaviors in day-to-day life must extend into digital navigation and conversation (e.g., Bodford, in press; Bodford, Kwan, & Sobota, in press; Kwan & Bodford, 2015). It is possible that because the digital world has existed for a comparably short time, actual and perceived safety in the online world stems, in part, from the factors predicting safety in the physical world.

Overview of the Present Research

To examine this question, we conducted four studies across archival, correlational, and experimental methodologies, and on the levels of nation, state, and individual. By adopting this multi-method, multi-level approach, we sought to establish a holistic understanding of the relationship between physical and online safety.

Studies 1 and 2. We first examine the relationship between physical and online safety as it exists in reality—that is, while observing objective, empirical indices of safety and threat in online and offline environments around the world. While holding constant macro-level factors that may influence online and offline safety (i.e., national- and state-level wealth), we explore whether a relationship between physical and online safety exists across countries and U.S. states.

Study 3. Second, we seek to investigate whether this relationship exists at the individual, and perceptual, level. We will first assess whether actual measures of physical safety (i.e., indicated by zip code-level census data) map onto perceptions of physical safety to establish whether we can assume that actual threats translate into individual-level perceptions. We will next examine whether the relationship between self-reported perceptions of physical safety are positively related to perceptions of safety while online. Just as we hypothesize a positive correlation between *actual* physical and online safety in Studies 1 and 2, we predict a positive tie between their perceptual counterparts. As a secondary aim, we will examine the role that person-specific factors (i.e., individual difference variables relevant to threat perception) may play in this relationship.

Study 4. Using experimental methods, we will further examine whether manipulations of physical threat guide or inform perceptions of online threat—and whether the opposite also holds true, in which manipulations of online threat predict perceptions of safety in the offline world. As was the case in Study 3, we will explore the impact of person- and situation-specific factors on this causal relationship.

Taken together, these questions add to our previously limited understanding of the nature of online safety and its relationship with the physical world.

Physical and Online Safety

Safety, in its broadest sense, refers to the condition of being protected from danger, risk, or injury. From an early age, humans form a basic and deep-rooted understanding of how to remain safe in their physical environments. We typically think of safety as a construct stemming from physical barriers separating the self from a potential threat (locked doors, walls, fences), from knowledge of threat in the immediate environment, or from our own ability to defend ourselves (physical size, self-defense expertise).

When we translate our physical understanding of safety into the online world, we commonly use the term *security*, which entails protection against deliberate and planned acts (Idsø & Jakobsen, 2000; Pearsall & Hanks, 2001). For purposes of simplicity, however, we will refer to physical and online security as *safety* throughout this document to highlight the connection between historic senses of safety (e.g., in our ancestral environment) and our modern-day sense of security.[1] In this paper, we distinguish

[1] *Safety* and *privacy*, on the other hand, are notably disparate concepts. Whereas *privacy* implies an ability to close a metaphorical door, *safety* or *security* implies being able to lock the door. Whereas the latter implies keeping unwanted others from breaking into—or stealing personal belongings from—a private space (be it a home or online account), the former implies keeping those belongings in the hands of their proper owner. Although companies may promise that they will keep users' information private from third parties,

between two forms of safety: safety in the physical environment, which carries cues of immediate threat, and safety in the online world, in which cues may be subtle or even unseen. To better understand online safety, it is important to first explore what we know about safety in the physical world, as well as the universal human motivation to detect and avoid threats in day-to-day life.

Self-protection motive. Abraham Maslow (1943) theorized a hierarchy of human needs, in which the basest of needs (i.e., physiological needs: water, food, metabolic requirements for survival) must supersede any needs that follow (e.g., love, belonging). Immediately following physiological needs, however, are safety needs—a drive for physical safety and security that has served as a fundamental human motive for millions of years (Kenrick et al., 2010). Evolutionary social psychology supports the idea that human thoughts and behaviors are often guided and regulated by these basic underlying motives. Just as mate acquisition and care of offspring speak to recurring ancestral problems, the *self-protection motive* speaks to a universal drive to detect, and protect oneself from, physical threat (Neuberg, Kenrick, & Schaller, 2011). Past research suggests that individuals' judgment and decision-making processes change when placed under a self-protection motivation, regardless of gender (Griskevicius et al., 2006; Griskevicius et al., 2009; Li et al., 2012). From angry faces to ambient darkness, both men and women consistently show increased sensitivity to potential threat when under a self-protection mindset (Becker et al., 2007; Schaller, Park, & Mueller, 2003).

malicious players (e.g., hackers, disgruntled employees) may find ways to obtain that information anyway—which does not imply a breach of privacy, but rather a breach of security.

Of course, “threat” does not refer exclusively to bodily harm. Victims of burglary may never come into physical contact with the perpetrator, and therefore never experience a threat to their life;[2] however, just as a stolen credit card might spur feelings of violation, the loss of resources (i.e., items of monetary or sentimental value) may certainly induce a sense of threat. Burglary, in this sense, stands as a less physically involved form of threat that may still pose severe impacts on a person’s ability to function in society. This form of threat, called *resource threat*, may challenge self-protection, but it may also endanger other fundamental motives. For example, the status (or esteem) motive describes the universal drive to protect resources—monetary or otherwise—to preserve one’s status in society, possibly by lessening one’s lifestyle in outward-facing ways (i.e., conspicuous consumption; Kenrick et al., 2010; Veblen, 1994). Although this universal drive entails protection against threat, it revolves exclusively around the loss of property, rather than potential loss of life. Of course, it could argued that resource threat may pose a much more significant threat than the ability to outwardly consume luxurious or status-related resources. Depending on one’s socioeconomic status, or on the magnitude of the resource threat itself, the loss of money or valuable items could pose a direct threat to one’s ability to pay for food, water, shelter, and other means of survival—that is, threats to physiological needs, which are paramount to human survival. Taken together, these two forms of threat—namely, self-protection

[2] Here, we distinguish between the legal definitions of (1) burglary, entailing breaking and entering (e.g., into a person’s home) to steal, but without the added component of bodily threat; (2) larceny, or theft without necessarily trespassing onto a person’s property; and (3) robbery, meaning larceny with the added component of physical force or intimidation.

threat and resource threat—will serve as important constituents of our approach to safety in the present research, both on- and offline.

Physical safety. Most broadly, we might imagine the physical world as a series of concentric circles surrounding the self, encompassing one's neighborhood, society, country, and immediate international context. If we were to consider these concentric circles in terms of physical safety, we might consider a person's ability to combat threat in the physical world as one's (1) personal ability to protect oneself, (2) societal ability (e.g., neighborhood or municipality safety), and (3) national ability (military expenditures). For the present work, we define physical safety more broadly than freedom from bodily harm. Not only can safety imply protection of an individual's monetary resources, but it can also be captured on a societal or national scale—for instance, through indices of military presence, homicide rates, federal bank robberies, and government infrastructure for basic protection.

Online safety. In information and computer science, *online safety* is often conceptualized as the act of maximizing the user's personal safety by recognizing and protecting against risks of data breaches (e.g., of personal information) while online. Such risks are usually posed by external actors that actively work against the user to undermine their safety; and just as an individual can lock his or her home to ensure physical security, so too can they take measures to increase their safety in cyberspace. Research in human-computer interaction suggests that factors such as visual design and website quality largely determine website trustworthiness (Grabner-Kräuter & Kaluscha, 2003; Ou & Sia, 2009; Yu & Singh, 2002);[3] but although this body of past empirical work highlights the importance of the *aesthetic* of the digital world on perceptions of online safety, little is known about the roles—if any—played by threats in the physical world. Most broadly, and for the purposes of this research, we could conceptualize a safe online environment as a counterpart to a safe physical milieu: a cyberspace without concern of data breaches, or armed with heavy encryption to protect its users.

Actual and perceived safety. The present work seeks to establish a connection between physical and online safety as they exist on a perceptual, psychological level. As such, it is important to first establish whether this connection exists in actuality, as will be investigated in Studies 1 and 2. After examining this relationship, we seek to extend this focus to the perceptual level in Studies 3 and 4.

Safety is, by its very nature, an abstract concept: because it is advantageous to human survival for actual, objective physical threats to translate into conscious perceptions of those threats, it would follow that actual and perceived safety are positively related in the offline world. Humans have adapted over time to detect and avoid threat, and it has historically been imperative to survival that actual threats translate into perceived, mentally acknowledged risks to be avoided. This translation, however, might be less clear while online. When a user takes a pro-security measure in cyberspace (e.g., enabling a protective tool or security layer), there is rarely a visible threat, nor is

[3] For example, when a website's visual design is cluttered, difficult to navigate, or wrought with grammatical or spelling errors, users are more likely to view that website as a scam, and therefore more likely to engage in safety-seeking behaviors—for example, withholding personal (e.g., name, e-mail, phone number) and financial information (Banks, 2014; Fogg, 2003; Neff, 2003; Sillence et al., 2004).

there an immediate positive outcome. As such, we might predict that for a user to take such precautionary measures, they must first perceive a threat while online (West, 2008). The reward for acting upon online safety behaviors is only the lack of a detrimental outcome, and when there are few cues of threat online (as opposed to nearby theft or the sound of gunshots), this profitless pursuit may not seem worthwhile (West, 2008). As such, online safety is intricately tied with threat detection in the online world, which may come less naturally to human users than more historic cues of threat in our ancestral environments.

Whereas much of past research has gauged individual-level judgments of physical safety along Likert-type scales indicating fear of "getting murdered" or "being robbed" (Chong et al., 2012), online safety is often operationalized through actual indicators of online threat (e.g., prevalence of phishing and spam attacks, availability of secure Internet servers). Perceived online safety remains a conceptually distinct variable about which we know little. There is, therefore, a need to empirically study perceptions of online safety and the factors that may underlie it.

The physical-online relationship. Although we can postulate a correlation between physical and online safety, such a relationship has not yet been demonstrated, and nor—if causal—has its potential directionality. Because the digital world has existed for a comparably short period of time relative to the physical world, one might speculate that cues of online threats stem from what humans have gathered across offline experiences, creating a causal relationship from the physical to the digital.

However, we could just as readily imagine a situation in which the two are inversely related. For example, the seemingly innocuous act of sharing geotagged photos during a weekend vacation indicates to other users—both friends and foes—lowered defenses and a vacant home. Just as personally identifiable information can be used to pinpoint a user's identity, so too can geotagged or location-specific information uniquely track a user's physical location, thereby endangering their physical safety or property. In this example, it is online safety that determines offline safety—the digital bleeds into the physical.

We have thus far presented possible situations in which physical and online safety might be related, both in actuality and in individual-level perception. But regardless of its directionality, we cannot assume that an increase in one form of safety will predict an equivalent increase in the other; we do not contend that this hypothesized tie is a one-to-one correlation. Not only should we expect all people to perceive threats in the same way, but it is unlikely that all threats will be perceived equally as threatening. Some people may tend to feel more or less threatened than others due to person-specific factors, or even aspects of their past or ongoing situation (i.e., context- or situation-specific factors). Similarly, there may be qualities of the threat itself that may uniquely threaten one individual, but not another. As such, we seek to explore whether there are person- and situation-specific factors relevant to threat perception that may alter the strength (or mere presence) of this relationship.

Person- and Situation-Specific Factors

The Extended Parallel Process Model. In the realm of communications, the Extended Parallel Process Model (EPPM; Witte, 1998; 1994) breaks down the process of threat perception and evaluation as a product of both person- and situation-specific (i.e., threat-specific) factors: (1) perceived severity of the threat, in which the type of threat itself (e.g., self-protection or resource) may differ in the extent to which others view it as foreboding, or in which a threat might seem more or less probable; (2) an individual's perceived susceptibility to that threat, which may, for the purposes of this research, be influenced by past experiences with physical or online threats (i.e., past victimization); and (3) his or her perceived efficacy in avoiding the threat, which may stem from physical size or knowledge of safety precautions—self-defense experience or even digital literacy (Hullett & Witte, 2001). We further break down these constituents by whether they can be attributed to the person encountering the threat (person-specific factor) or the threat itself (situation-specific factor).

Person-specific factors. Following this breakdown of threat perception, we might state that both threat susceptibility (e.g., past victimization, wealth) and efficacy in avoiding the threat (physical size, self-defense, digital literacy) comprise factors that are specific to the person. Even with all else held equal, individuals may respond to the same threats very differently if certain qualities alter their perceived susceptibility to falling victim to, or their efficacy in avoiding or controlling, the threat. Indeed, a wealth of past research in communications, psychology, and criminology suggests that physical safety—both in perception and in actuality—largely stems from: (1) demographic characteristics (i.e., sex, age, and socioeconomic status), (2) past victimization experiences, and (3) ability to defend oneself against threat.

Demographic characteristics. Past research suggests that sex and age play large roles in both actual and perceived physical safety. Although women and older adults perceive higher threat in their day-to-day lives, men—especially from younger age groups—actually experience higher violence and victimization rates (Donnelly, 1989;

Janson & Ryder, 1983; Perkins, Brown, & Taylor, 1996; Skogan & Maxfield, 1981; Toseland, 1982). In addition, individual- and community-level socioeconomic status has been found to be negatively related to physical risk perception (Austin, Furr, & Spine, 2002; Simsek et al., 2014), as well as a sense of control over physical threats (Feldman & Steptoe, 2004). Research contends that this loss of perceived control is related to an increased sense of vulnerability and, therefore, susceptibility to the threat at hand (Simsek et al., 2014). As such, we might postulate that participants who are older, female, or hail from a lower socioeconomic background might chronically perceive a higher level of physical threat than actually exists. Research has yet to examine whether these factors predict lasting differences in perceived threat while online.

Past victimization. Crime researchers have found that past victims of physical violence (e.g., robbery, assault) demonstrate markedly higher levels of perceived risk that remain stagnant long after victimization (Connor-Smith et al., 2010; Foster & Hagedorn, 2014; Garofalo, 1979; Wolff & Shi, 2009). On the one hand, it is possible that such experiences might generalize from physical threat to perceived digital threat: A victim of burglary in the physical world may experience heightened fear of identity theft or credit card fraud online. However, we might just as readily imagine that victims of crime in one domain might turn to the other as a markedly disparate environment. Someone who has been robbed at gunpoint while walking home might avoid certain physical situations (e.g., running errands at night, going to unfamiliar places alone), all the while maintaining, or even increasing, their use of the online world—a milieu in which physical attacks are impossible. As such, their sense of online safety might remain relatively unchanged in the face of physical threats. Similarly, past victims of online crime—

identity fraud, cyberstalking—might respond to the contextual cues that stem from these past online experiences by turning to the physical, disconnected world, such that their sense of physical safety remains independent of their sense of threat online. In either situation, we might speculate that past victimization is an important person-specific factor to explore.

On- and offline self-efficacy. As might seem intuitive, individuals feel more efficacious in controlling or avoiding a physical threat if they are of a larger physical size than others of their gender or age group (Bailey, Caffrey, & Hartnett, 1976; Sell et al., 2009). This means that on average, larger men are less likely to feel threatened than smaller women. However, research has found that increased knowledge of self-defense tactics improves fear response and perceived self-efficacy in avoiding threats for both males (Phillips & Rudestam, 1995) and females (McDaniel, 1993).

We might also consider one's ability to protect oneself online (e.g., digital literacy) as a similar form of self-efficacy. Stated differently, just as physical size may reinforce physical safety, so too might digital literacy act as a buffer for online safety. Researchers in information and computer science have attributed perceptions of online safety to differences in perceived self-efficacy (i.e., *Could I protect myself if I wanted to?*; Shillair et al., 2015). Indeed, efficacy beliefs—which largely stem from exposure to technology—are paramount in instilling a sense of control over perceived online threats (Lallmahamood, 2007; Lee, LaRose, & Rifon, 2008; O'Cass & Fenech, 2003; Witte et al., 1995). As such, if an individual is physically small and typically vulnerable to physical attack, this sense of physical threat may not necessarily translate into perceived online threat if that same person is well-equipped to avoid danger while navigating the digital world.

Taken together, research defends the role that certain individual differences (i.e., person-specific factors) play in physical safety, with a particular emphasis on gender, past victimization, physical size, and ability to defend oneself (here, either on- or offline).

Situation-specific factors. We also believe it important to consider situation- or context-specific factors that might play a role in the relationship between perceived physical and online safety. These factors may alter an individual's subjective evaluation of the threat at hand, possibly through reinforcing a sense of resilience to the threat (e.g., judging a threat's severity to be low) or the belief that a certain threat is unlikely to occur.

Type of threat. For the purposes of the present research, we might consider the importance of *type* of threat on perceptions of threat severity. In particular, we have discussed two key forms of threats—self-protection threats and resource threats—and have postulated that because the former may pose a more direct threat to one's survival (than, say, loss of money or valuable resources), self-protection threats may be seen as more severe, and more threatening, than resource threats. Although Studies 1, 2, and 3 examine safety on a broader level—that is, across both types of threat—Study 4 examines this distinction more closely.

Probability of threat. A second situation-specific factor worth considering is the probability that a threat will occur. For example, although Internet-facilitated crimes against children can be deemed highly severe and impactful threats, they occur very rarely compared with identity theft and phishing scams (IC3, 2015). Past research has substantiated the important role that threat probability plays in threat perception across a variety of situations. For one, Fuller (1984) found that self-reported safe driving behaviors are largely based on the perceived probability that a crash will occur; similarly, Rogers and Mewborn (1976) found that people are more likely to avoid smoking and other unhealthy behaviors if cancer likelihood appears more probable.

In one study by Rapee (1997), participants were shown a series of threat situations that were either physical (walking down a dark alley at night) or social in nature (being interviewed on live television). For each, they rated the probability and consequences of the threat, as well as the control they believed they would have in such a situation. Although fear of social threat stemmed from consequences of—and personal control over—the threat itself, the only predictor of fear in *physical* situations was the probability that the threat would occur at all. Furthermore, threat probability may, in some cases, be deemed even more important than threat severity, even in situations involving resource (rather than self-protection) threat: A social psychological study on threat avoidance illustrated that the most effective deterrent of tax evasion was considering the probability that an audit would occur, rather than the severity of the fines (Friedland, 1982). Even vague, potentially inaccurate information about audit probability was more powerful than exact (but low) probability information coupled with small fines.

In summary, the EPPM outlines important qualities that guide human perceptions, or evaluations, of threats. We have differentiated these qualities by their specificity to the person or the situation, and speculate that—even with all else held equal—both sets of factors may alter the relationship between physical and online safety. We aim to explore the role that these qualities play in our individual-level, perception-based studies (i.e., Studies 3 and 4).

Taken together, the key focus of this work is to examine the relationship between physical and online safety, both in actuality (on the national and state levels; Studies 1 and 2) and in individual-level perception (Studies 3 and 4). In our first three studies, we examine a combination of threats to both self-protection and resources; in Study 4, we tease apart these types of threat to study the unique impacts of each in isolation. Lastly, and for exploratory purposes, we will also examine person- and situation-specific factors that may moderate or break down this relationship—namely, demographic characteristics, past victimization, self-efficacy, and probability of threat.

Research Questions and Hypotheses

We can thus break down our primary research questions by level of analysis, method of study, and distinction between actual and perceived safety.

1. National and State, Correlational, Actual (Studies 1 and 2)

To examine the perceptual nature of the relationship between physical and online safety, we must first assess whether such a relationship exists in actuality. Thus, our first question regards the nature of the relationship between actual physical and actual online safety as they exist on the macro-level. Furthermore, we have previously discussed the importance of wealth on *perceived* susceptibility to a given threat; however, across nations and even U.S. states, one could conceptualize the role that wealth (e.g., gross domestic product) might play on a country's ability to combat physical (e.g., military presence, homicide rate) and online threat (secure Internet servers): Wealthier countries can afford to invest monetary resources into militarization and homeland protection, just as they can invest in secure cyberinfrastructure. We are therefore interested in whether a relationship exists between quantifiable indicators of physical and online safety on the macro-level, above and beyond the potential role that wealth might play. This first research question can be broken down into the following hypothesis:

H1: We predict that, when controlling for macro-level indicators of wealth, actual physical safety will be positively related to actual online safety across both nations (H1A) and U.S. states (H1B).

2. Individual, Correlational, Actual and Perceived (Study 3)

After establishing whether a relationship exists between actual, macro-level indicators of physical and online safety, we are interested in examining whether this link exists at the level of individual perceptions. As such, we first examine whether actual and perceived safety map on to one another by gauging the correlation between participant zip code safety and perceived safety of one's neighborhood. Assuming a positive relationship between actuality and perception, we next assess whether a correlation between perceived physical safety (e.g., neighborhood safety) and perceived online safety exists. And third, we explore whether the relationship between physical and online safety depends on individual difference measures that have demonstrated relevance to threat perception in past research (i.e., physical size, past victimization experiences, self-efficacy). This third research aim will primarily serve exploratory goals, and may help account for outliers in responses to our perceived safety measures. In sum, Study 3 will investigate the following hypotheses:

H2: We predict that actual physical safety, as quantified by participant zip code, will demonstrate a positive correlation with perceived physical safety.

H3: We predict that perceived physical safety will be positively related to perceived online safety.

H4: For exploratory purposes, we predict that person-specific factors related to threat perception will moderate or buffer the relationship between perceived physical and perceived online safety.

3. Individual, Experimental, Perceived (Study 4)

For our fourth and final study, we are interested in expanding our understanding of the relationship between perceived physical and online safety by examining whether manipulations of one type of threat affect the other. More specifically, if we experimentally alter physical safety, does it impact perceived online safety? And does the opposite hold true, in which manipulations of online threat predict perceived physical safety? We conducted a 3 × 2 between-subjects test of this question, in which type of threat (self-protection threat vs. resource threat vs. control condition) and domain of threat (physical vs. online) are manipulated via random assignment to condition.

Manipulating physical vs. online threat. The goal of our experimental manipulations is to prime perceptions of threat in the physical or online world by increasing the salience of real-world crime or cybercrime. Past empirical work has primed perceived threat using guided visualization stories, also referred to as guided imagery. This technique was first empirically used in clinical psychology in the mid-1980s to reduce anxiety and enhance work performance by imagining oneself in a situation that is less physically or psychologically threatening (Ayres & Hopf, 1985; 1990; 1992). In the decades since, other areas of psychology have adopted guided visualization as a strategy to increase the vividness and clarity of participants' mental imagery through text-based prompts.

In the realm of physical safety, extant work in evolutionary social psychology has primed self-protection motives through similar techniques (White et al., 2013; White, Kenrick, & Neuberg, 2013). One text-based scenario guides participants through a dark, windy evening spent alone at home. The story ends as the second-person subject (supposedly the participant) hears someone force open the front door and, just as the power goes out, hears footsteps slowly approach their bedroom. This story has been shown to activate motives of self-protection, which is precisely the aim of our physical threat manipulation. Other empirical works have primed self-protection motives through threat-related movie clips detailing murder, stalking, or robbery (e.g., *Silence of the Lambs*; Maner et al., 2005; White, 2014; Young, Slepian, & Sacco, 2015).

Because Studies 1 and 2 examine *actual* safety through the prevalence of true crimes (e.g., intentional homicide, prevalence of identity theft), we manipulated physical threat through examples of what seem to be actual crimes in the community or online world. As such, we showed participants altered news stories detailing concrete, dangerous events that have purportedly happened in their close neighborhood. Rather than presenting them with guided visualization scenarios, these doctored news stories should prime decreased perceptions of physical safety in participants' immediate environments, a prime that would be based on supposed actuality rather than imagination. Similarly, we manipulated online threat by presenting participants with altered news stories detailing examples of cybercrime that may put Internet users at risk.

Manipulating type of threat. Although Studies 1, 2, and 3 conceptualize safety more broadly—namely, incorporating facets of safety that stem from both bodily threats (e.g., homicide rate, assault) and threats to valuable possessions (bank robberies, burglary)—we cannot assume that all threats are held equal on the individual, perceptual level. One situation-specific factor relevant to the present work is type of threat, distinguishing between self-protection threats and resource threats. In the hierarchy of fundamental motives, self-protection motives are more paramount to ensuring human survival than motives that fall higher in the pyramid. Although resource threats could endanger status motives through threatening one's ability to outwardly display a particular lifestyle, these threats could also pose a threat to base physiological needs such as obtaining food and shelter—that is, needs that are even more paramount to survival than self-protection. As such, we would expect that these two types of threat will not generalize between physical and online domains in the same way; one type of threat may generalize more strongly, yielding a more positive physical-online relationship. Therefore:

H5: We predict that type of threat (either self-protection or resource) will impact the physical-online relationship to differing degrees.

We used two news stories as experimental manipulations: One article primed self-protection threat by presenting participants with an alarming event that should induce a desire to protect oneself from bodily harm; the other primed resource threat by detailing the loss of monetary resources. We then altered—as minimally as possible, to maintain comparability between the two—each of these stories to apply to both the online and offline worlds. For example, a physical self-protection threat prime might discuss a voyeur who spends many hours each day watching individuals from outside their homes; an online self-protection threat prime, however, might discuss a webcam hacker who spends the same number of hours each day watching individuals through their laptop cameras. Similarly, a physical resource threat prime could describe a series of burglaries where valuable possessions were stolen from multiple cars shortly after their owners had left; an online resource threat could outline a series of online bank account thefts.

For each of these primes, we aimed to manipulate only one type of threat at a time; our self-protection threat primes do not implicate monetary or valuable resources, and our resource threat primes do not pose direct physical harm. However, it is important to consider a key difference between physical and online threats in each of these situations. If a voyeur is watching a person's every move in the physical world, the threat ends there. It may instill a sense of fear and alarm, and the person may feel that their survival is in danger, but the actual threat posed remains purely physical (even if a person were to generalize or "blur" that threat to the online world). The same can be said for physical resource threat: If a burglar were to break into a person's house while they were away, the threat ends with the loss of valuable—but solely physical—resources. Online assets remain untouched and unthreatened.

If we were to consider online threats, however, this isolation of domain breaks down. A hacker who may be watching a person's every move online could conceivably track his or her victim down in the physical world; the online threat could transform into a physical one. Similarly, an online resource threat such as credit card fraud or stealing from an online bank account yields a loss of resources that trickles into the physical world. The resources are, after all, monetary; they can be spent both online and offline.

Taken together, we might expect that threat domain will impact the degree to which perceived threat generalizes to the opposite domain.

H6: We predict that threat domain—either physical or online—will impact the generalized relationship between perceived physical and online safety to differing degrees.

And finally, we presented participants in control conditions (for either physical or online modalities) with a straightforward news story detailing either generic neighborhood news or basic news surrounding online developments (e.g., non-safety-related app releases). Because these control conditions did not reference crime or prime threat, we have no reason to expect that reading a neutral news story will impact perceived safety in either modality, regardless of threat type; therefore, we do not predict an effect among participants in control conditions.

Downstream safety behaviors. Beyond capturing perceptions of online and offline safety, we are also interested in the impacts of perceived threat on downstream safety behaviors—more specifically, whether a person is more likely to follow recommended safety practices after being made to feel threatened either online or offline. Our primary goal in examining intentionality to follow safety practices is to assess whether safer on- and offline behaviors can be encouraged immediately following reports of an attack. We might predict that participants assigned to a threat condition should experience heightened self-protection or status motives (i.e., compared with participants in control conditions), and will therefore show higher intentionality to act on safety practices. We might also expect that participants primed with online threat will be more likely to act on online safety practice recommendations due to the relevance between primed threat and possible solution or defense, whereas those primed with physical threat will be more likely to act on physical safety practice recommendations.

We cannot assume that likelihood of following recommended safety practices will be equally appealing or even possible for all participants. For some, perceived self-efficacy in following these behaviors may act as a barrier; for example, a participant with low digital literacy or comfort with technology might consider a recommendation to enable two-factor authentication on their e-mail account to be too technical to follow, which would limit that individual from carrying out this recommendation. Similarly, some participants may feel that particular types of safety recommendations are not efficacious in controlling or avoiding the threat at hand—not as a fault of the individual, but of the recommendation itself (i.e., *response efficacy*; Witte et al., 1995). As such, and for exploratory purposes, we will examine perceptions of response efficacy and self-efficacy as they relate to these recommended safety practices.

Person- and situation-specific factors. As was the case in Study 3, we collected person- and situation-specific measures that may play a role in the physical-online relationship. In the realm of person-specific factors, we again examined demographic characteristics such as physical size, past victimization experiences, and self-efficacy in on- and offline self-defense. Because we are manipulating one of our two situation-specific factors of interest (namely, type of threat: self-protection or resource), we examined another potentially important situational factor: participants' estimated probability that the threat will occur to the individual him- or herself. These estimations could highlight threat-specific qualities that could impact perceived safety (e.g., credit card fraud might be seen as more probable than burglary, particularly among those who live in physically safe neighborhoods). Finally, we presented participants with two subscales from Witte and colleagues' (1995) Risk Behavior Diagnosis Scale that operationalize perceived susceptibility to the threat at hand (i.e., as a person-specific factor) as well as perceived threat severity (as a situation-specific, or threat-specific, factor). The inclusion of these two factors speaks directly to our interest in the EPPM as a building block for the factors that may alter or moderate the physical-online relationship. As was the case in Study 3, our broader interest in these person- and situation-specific factors is purely exploratory in nature, and may help explain any outliers in responses to our dependent variables; however, we could repeat Hypothesis 4 from our third study, which predicts that:

H4: Person- and situation-specific factors related to threat perception may moderate or buffer the hypothesized physical-online relationship.

Outcome variables. To answer our primary research question, we observe whether those primed with physical threat demonstrate a higher sense of online threat, and whether the reverse holds true—in which those primed with online threats demonstrate higher perceived physical threat. In addition to examining perceived safety as an outcome variable, we also examined intentionality to act upon, or increase the use of, safety behaviors both on- and offline. We are interested in the behaviors people might demonstrate after being made to feel threatened, and whether these threats increase intentionality to protect oneself.

Table 1 summarizes our four studies by design, independent and dependent variables, and hypotheses.

Table 1

Summary of all studies: Design, variables, hypotheses

Study		Details
1.	Design:	Correlational, using national-level archival data
	IV:	Actual physical safety
	DV:	Actual online safety
	H1A:	Actual physical safety is positively related to actual online safety on the national level, even when controlling for wealth
2.	Design:	Correlational, using state-level archival data
	IV:	Actual physical safety
	DV:	Actual online safety
	H1B:	Actual physical safety is positively related to actual online safety on the state level, even when controlling for wealth
3.	Design:	Correlational, self-report inventories
	IV:	Actual physical safety, perceived physical safety
	DV:	Perceived online safety
	H2:	Actual physical safety will be positively related to perceived physical safety
	H3:	Perceived physical safety will be positively related to perceived online safety
	H4:	Person- and situation-specific variables related to threat perception will moderate or buffer the physical-online relationship (*exploratory*)
4.	Design:	Experiment, 3 × 2 between-subjects
	IV:	Self-protection threat vs. resource threat vs. control (3 levels), physical vs. online (2 levels)
	DV:	Perceived safety (in the opposite domain of assigned condition), safety behavior intentionality
	H5:	Physical and online safety are more positively related in self-protection threat conditions
	H6:	Physical and online safety are more positively related in online threat conditions
	H4:	(*See Study 3*)

Theoretical Contributions

The aim of this research is to better understand the relationship between safety in the physical world and perceptions of safety online. Taken together, these four studies seek to establish:

(1) whether a connection exists between measures of physical and online safety in actuality, and on a global scale;

(2) whether an individual’s actual physical safety, as measured by zip code, is a positive reflection of his or her perception of physical safety;

(3) whether perceptions of physical and online safety are positively correlated at a given point in time;

(4) whether manipulations of physical or online threat predict perceptions of threat in the opposite modality;

(5) the role that personal and situational factors relevant to threat perception play in the relationship between perceived physical and perceived online safety; and

(6) the impact of physical or online threats on an individual’s intention to act upon, or educate themselves about, downstream safety practices.

To expound upon this sixth and more applied aim, we are interested in using these findings to encourage safer online behaviors, or to increase awareness of potential threats when navigating the online world. When made to feel threatened, does a person’s intentionality to learn more about, and act upon, online safety practices increase? And if so, could organizations (e.g., IC3) immediately follow up on reported cyberattacks with suggested safety practices to increase attention to, and proactive steps toward, securing a safer cyberspace?

And finally, how might we predict differences in the willingness to adopt these downstream behaviors as a function of physical situation? With respect to social networking sites, for example, these findings may guide the creation of new segmentation strategies to deliver catered lists of security settings to their users. Just as users of certain demographic profiles may change their password more frequently (e.g., by gender, age, employment status; Bryant & Campbell, 2006), so too might users from certain physical settings (e.g., as judged by safety of zip code, city) benefit from a tailored security experience online. If a user's zip code is associated with physical threat, and if we observe a connection with perceptions of online threat, they may be more likely to proactively avoid those threats in cyberspace, and more likely to seek out—and act upon—customized safety controls on their account. As such, we hope that our findings might help streamline this user process of discovering and carrying out online safety practices through segmenting users based on relevant demographic characteristics.

In summary, we wish to update our social psychological understanding of the relationship between physical safety and online safety in an age when the average American adult spends most waking hours interacting with the digital world. More specifically, we are interested in whether, and when, the boundary between physical and digital breaks down in this highly digitally connected world.

Study 1

Our first study seeks to examine the relationship between actual physical and actual online safety on the national level, using archival variables and a correlational design.

Method

Materials

Actual physical safety. We operationalized physical safety through an objective composite measure called the Global Peace Index, first developed by the Institute for Economics and Peace in 2006 and updated annually. This index, which ranges from 1.148 (most physically safe; Iceland) to 3.645 (most physically dangerous; Syria), ranks 163 countries and 99.6 percent of the world's population. It takes three key areas into consideration: (1) Ongoing domestic and international conflicts (including deaths from internal conflict and impacts of terrorism), (2) militarization and internal suppression of a country's citizens, and—weighted most heavily—(3) societal safety and security, including measures of homicide rate and likelihood of violent demonstrations.

Actual online safety. We considered five operational markers of actual online safety on the national level: (1) the HE Index (HostExploit), a composite measure reflecting the extent of malware, spam, and botnet reported per country; (2) the number of secure Internet servers per 1 million people (The World Bank, 2015); (3) the number of attacks on a country's specific domain (e.g., .au as an Australian domain); (4) the number of unique phishing domains detected per country (Antiphishing.org), and (5) the number of phishing attacks—separate from general attacks—on a country's specific domain (Antiphishing.org). However, four of these five measures reflect potentially external attacks on a country's internal online safety, rather than a country's internal initiative to secure a safe online environment for its citizens. The countries highest in these four measures correlate strongly with political and governmental strife (e.g., the highest countries in the HE Index include Russia and the Ukraine) or government-sponsored online corruption (the highest in phishing domains and domain attacks include the Central African Republic, Nigeria, and Libya). Unique phishing domains and raw number of phishing attacks are, understandably, highly indicative of national population, with Brazil and China scoring as the highest countries for both ($r[184] = .442$, $p < .001$).[4]

[4] We tested these five indicators within Estonia, regarded as a global leader in cybersecurity (Hattem, 2014; Ilves, 2013; Kinstler, 2015) and within the 95th percentile worldwide of government commitment to cybersecurity (ITU, 2015). As might be expected, the HE Index did not provide a satisfactory illustration of Estonia's online

We therefore operationalized actual online safety through Secure Internet Servers, which reflects "an important element in investment decisions for both domestic and foreign investors," namely, "how many companies conduct encrypted transactions over the Internet […], the use of encrypted transactions through extensive automated exploration, tallying the number of Web sites using a secure socket layer (SSL)" (Netcraft, 2015).

Table 2

Study 1: Partial correlations of country demographics and online safety

	HE Index	Domain Attacks	Unique Phishing Domains	Phishing Attacks	Secure Internet Servers
Land Mass	.142	-.058	.628***	.617***	-.129
Land Mass per Capita	-.182†	.030	.068	.052	.140
Population	.275**	-.116	.483***	.485***	-.025
Population Density	.086	.144	-.013	-.012	.094
Urban Population	-.025	-.132	.169	.176†	-.089
Rate of Urbanization	-.131	.222*	.029	.006	.150
GINI[5]	-.177†	.134	.188†	.180†	-.181†
Unemployment Rate	-.143	-.004	-.129	-.124	.015

*** *p* < .001, ** *p* < .01, * *p* < .05, † *p* < .10; *n* = 90

safety: Their score of 66.3 was above average, and almost twice the median score of 35.05 (*n* = 198), which may reflect recent and ongoing political strife in its immediate surroundings. They scored in the bottom quartile of domain attacks with a score of 3.6 against a mean of 19.36 (*n* = 141), and their 24 unique phishing domains brings them to less than a fifth of the mean of 125.69 (*n* = 199). Lastly, Estonia placed within the top 85th percentile in secure Internet servers with a score of 927.0, more than 25 times the median score of 36.0 (*n* = 199). Although Estonia's placement along the HE Index may be a less valid indicator of online safety, it appears that secure Internet servers may be a close proxy.

[5] The GINI is a country-level indicator of income inequality across citizens, with high values indicating high inequality.

As is reflected in Table 2, which shows partial correlations of our five possible online safety variables (while holding GDP per capita constant), this measure was notably independent of country-specific demographics (e.g., land mass, population and population density, rate of urbanization) that may confound our hypothesized model.

Overview of analysis

The present paper concerns the relationship between physical and online safety above and beyond the impact of country-level wealth. Indeed, it is conceivable that both physical and online safety could be correlated with national wealth: wealthy nations can afford to provide highly trained police, military forces, and cyber-protection agencies to protect their citizens from harm. As such, all analyses described henceforth control for gross domestic product (GDP) per capita to better observe the unique impact of actual physical safety alone. This particular index, which is reported by the CIA World Factbook, compares GDP on a purchasing power parity basis, divided by population as of the beginning of the fiscal year (i.e., July 1) of 2015.

Results and Discussion

To assess whether actual physical safety and actual online safety were related, we examined the bivariate correlation between the two variables. As predicted in Hypothesis 1A, Global Peace Index and Secure Internet Servers were strongly negatively related (r[156] = -.513, p < .001), evincing a strong *positive* relationship between physical and online safety—again, higher scores on the Global Peace Index indicate more physical *danger*, not safety. This relationship remained significant when controlling for GDP per capita, r(155) = -.308, p < .001. Table 3 depicts both bivariate and partial (controlling for GDP per capita) correlation coefficients for our three variables of interest.

Table 3

Study 1: Bivariate and partial (controlling for GDP) correlations

	Bivariate		Partial
	1.	2.	2.
1. GDP per Capita	—	—	—
2. Global Peace Index	-.499***	—	—
3. Secure Internet Servers	.602***	-.513***	-.308***

*** *p* < .001, ** *p* < .01, * *p* < .05

Summarizing the findings from our macro-level Study 1, our primary hypothesis—namely, that physical safety would predict online safety—held true, even when controlling for GDP per capita.

Study 2

Our second study seeks to replicate the design and hypotheses of Study 1, but on the state level; it examines whether a positive relationship existed between indices of actual physical and actual online safety, even when holding state-level wealth constant.

Method

Materials

Actual physical safety. We assessed actual physical safety along three federally published indices that captured various forms of safety in day-to-day life within the United States; more specifically, these three indices spoke to violence against people, against property, and against federal entities (e.g., banks). The FBI (Federal Bureau of Investigation, 2015; 2016; Uniform Crime Reporting Statistics, 2017) has published (1) an index of violent crime (rate per 100,000), which takes into account offenses of murder, rape, robbery, and aggravated assault per state (*M* = 379.86, *SD* = 186.69); (2) an index of property crime, including burglary, larceny-theft, and motor vehicle theft (again, rate per 100,000; *M* = 2,854.33, *SD* = 606.76); and (3) a count of bank robberies (*M* = 78.84, *SD* = 90.23), including theft from any national or state member bank of the Federal Reserve.

Actual online safety. Similarly, the FBI's Internet Crime Complaint Center (IC3, 2015) releases an annual report of filed complaints for 35 different types of cybercrime (e.g., phishing, malware, personal data breach, government impersonation), separated by the state where each victim and—if known—perpetrator lives. We collected indices detailing (1) the number of victims of cybercrime per state (divided by population to create a victim *rate*; *M* = 0.0007, *SD* = 0.00024), (2) the number of perpetrators of cybercrime per state (again, controlling for population; *M* = 0.0004, *SD* = 0.00037), (3) an overall index of identity theft complaint rate per 100,000 (*M* = 79.59, *SD* = 28.78), and (4) a credit card fraud complaint rate (*M* = 12.20, *SD* = 5.00). We saw it prudent to more specifically examine identity theft and credit card fraud because they comprise two major forms of cybercrime in the United States and, furthermore, are highly nondiscriminatory in nature (i.e., anyone with a credit card and/or a legal identity can become a victim).[6]

Overview of analysis

As was the case in Study 1, we are interested in the relationship between macro-level indicators of actual physical and actual online safety, above and beyond the effects that wealth might play on these constructs. As such, we controlled for Gross State Product (GSP) as published by the U.S. Department of Commerce Bureau of Economic Analysis (2015).

[6] Although credit card fraud has existed long before public access to the World Wide Web (e.g., through ATM tampering or through phishing scams facilitated through phone conversations), its prevalence has grown exponentially with the aid of digital connection and malware (Holmes, 2015).

Results and Discussion

Tables 4 and 5 illustrate the bivariate and partial (i.e., controlling for GSP) correlation matrices, respectively, of our variables of interest.

Table 4

Study 2: Bivariate correlations of variables of interest

	1.	2.	3.	4.	5.	6.	7.
1. Violent crime	—	—	—	—	—	—	—
2. Property crime	.660***	—	—	—	—	—	—
3. Bank robberies	.011	-.059	—	—	—	—	—
4. Victims of cybercrime	.571***	.235†	.107	—	—	—	—
5. Perpetrators of cybercrime	.659***	.469***	-.054	.445***	—	—	—
6. Identity theft	.426**	.498***	.456***	.415**	.348*	—	—
7. Credit card fraud	.442***	.281*	.657***	.470***	.446***	.804***	—
8. Gross state product	.020	-.037	.939***	.061	-.048	.367**	.591***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; *n* = 49

Table 5 evinces few significant relationships between GSP and our physical safety variables, with the exception of bank robberies (*r*[49] = .939, *p* < .001); however, we see a strong positive relationship between wealth and both identity theft rates (*r*[49] = .367, *p* = .008) and credit card fraud rates (*r*[49] = .591, *p* < .001).

Table 5

Study 2: Partial correlations (controlling for GSP)

	1.	2.	3.	4.	5.	6.
1. Violent crime	—	—	—	—	—	—
2. Property crime	.661***	—	—	—	—	—
3. Bank robberies	-.023	-.068	—	—	—	—
4. Victims of cybercrime	.571***	.238†	.145	—	—	—
5. Perpetrators of cybercrime	.661***	.468***	-.026	.450***	—	—
6. Identity theft	.451***	.551***	.348*	.422**	.394**	—
7. Credit card fraud	.533***	.376**	.367**	.538***	.588***	.783***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; *n* = 48

Of interest to our central hypothesis, we observed consistently strong, positive correlations between our physical safety variables and our online safety variables, with only two nonsignificant exceptions (i.e., bank robberies and victims of cybercrime, *r*[49]

= .107, *p* > .05, *ns*; bank robberies and perpetrators of cybercrime, *r*[49] = -.054, *p* > .05, *ns*). The average correlation coefficient across these 12 relationships was *r*(49) = .405 (*p* = .004). These trends were mirrored after controlling for GSP: the two nonsignificant relationships remained nonsignificant, but otherwise, all correlations between physical and online safety measures remained highly positive (mean *r*[48] = .395, *p* = .005). In support of Hypothesis 1B, we observed a positive relationship between indicators of actual physical safety and actual online safety across U.S. states, even after controlling for state-level wealth.

Study 3

Study 3 seeks to extend the focus of Studies 1 and 2 to the individual, perceptual level by examining whether (1) actual physical safety maps onto perceived physical safety, whether (2) perceived physical safety is positively related to perceived online safety, and—for exploratory purposes—whether (3) person- and situation-specific factors related to threat perception will moderate or buffer the physical-online relationship.

Method

Participants

Our sample comprised 1,687 undergraduate students enrolled in an introductory psychology course at a large, public institution. Survey items were presented as part of a larger prescreening battery, which students could complete for partial research credit. Of this sample, 48.8 percent were female with a mean age of 19.43 (*SD* = 2.67); 56.3 percent were White, 16.3 percent Hispanic/Latino, and 8.2 percent East Asian. 81.4 percent self-reported that they hailed from at least a middle-class background.

Materials

Actual physical safety. To measure actual physical safety of participants' physical surroundings, we asked participants to report the zip code of their permanent home at the end of the survey. Trained research assistants coded each zip code for three measures of actual safety, released by the FBI across local police departments and municipalities and standardized by Move, Inc. (2017). Move, Inc. releases city profiles separated by zip code, which include standardized indices of total crime risk, personal crime risk, and property crime risk; for each, a score of 100 reflects the national average, whereas a score of 50 indicates half the national crime risk, 200 indicates twice the national risk, and so forth. Scores were based on seven years' worth of demographic and geographic analyses of zip code-specific crime.

Total crime risk represents the combined risks of rape, murder, assault, robbery, burglary, larceny, and vehicle theft—that is, an amalgamation of both self-protection threats and resource threats. The various types of crime were given equal weight in this publicly available measure, so murder—for example—was not weighted more or less heavily than vehicle theft. Personal crime risk represented the combined risks of rape, murder, assault, and robbery; property crime risk reflected the combined risks of burglary, larceny, and motor vehicle theft.

After data entry, these index scores were randomly spot-checked for accuracy and reverse-coded to indicate physical *safety* (total, personal, property), rather than risk, by computing ((max+1)–x) for each value where x indicates the raw score, subtracted from one point more than the maximum possible value.

Perceived physical safety. We gauged perceptions of physical safety through Austin, Furr, and Spine's (2002) four-item index of "perception of safety in one's neighborhood" (p. 420). Participants were asked to indicate the degree to which they agreed or disagreed with each statement (e.g., *People in my neighborhood can leave their personal property outside and unattended without fearing that it will be damaged or stolen*) along a 7-point Likert-type scale. Furthermore, participants were instructed to think of their permanent home (i.e., the home corresponding to their provided zip code) while answering these items. Because these items demonstrated acceptable reliability within our sample (α = .76; DeVellis, 2012), we formed a single averaged composite across these four items, the descriptive statistics for which are portrayed in Table 7.

Perceived online safety. To capture perceptions of online safety, it was important that we confine our definition of safety to one form of online interaction. Whereas our indices of actual and perceived physical safety tapped into safety in participants' own neighborhoods, we ran the risk that online safety—measured most broadly—could be interpreted to mean safety while texting, using third-party applications, surfing the Internet, performing online banking transactions, sending e-mails, or participating in multiplayer online games. Each of these examples may certainly pertain to perceptions of safety and threat in cyberspace; however, it would be impossible to tease apart variations in participant responses if we lacked specificity surrounding the nature of the online interaction. As such, and given the increasing universality of social networking use,[7] we assessed perceptions of online safety while using social networking sites (SNSs).

[7] As of November, 2016, approximately 80 percent of online adults actively used Facebook (Greenwood, Perrin, & Duggan, 2016), with as many as a third of adults using

We therefore asked participants to report which SNSs they used or visited at least once a month out of Facebook, Google+, Instagram, LinkedIn, and Snapchat.[8] On the next screen, we displayed Flavián and Guinalíu's (2006) index of perceived website security, which builds off O'Cass and Fenech (2003) and measures participants' agreement with statements such as *This website has enough security measures to protect my personal information*. For each statement, which we altered to refer to "these websites" (i.e., in plural form), we asked participants to answer based on the website(s) they had selected on the previous page. Responses to these six items showed high internal consistency (α = .88), and we formed a single composite variable averaging across all items.

Past victimization. We used Thompson, Bankston, and St. Pierre's (1992) index of property victimization (*Have you or a household member ever been a victim of theft or burglary (either when you were at home or away from home?*) and personal victimization (*Have you or a household member ever been a victim of assault/battery, robbery, or murder?*). Responses to these two binary items were summed so that a score of 1

Instagram, LinkedIn, or other major social networking sites. Whereas even basic Internet surfing cannot be standardized across individuals (no two users visit the same websites or conduct the same online transactions), interactions with these major SNSs form a more uniform set of interactions. Finally, although e-mail could arguably be more universal than SNS use, we cannot assume that perceived online safety is comparable between Gmail, Apple iCloud, AOL, and city-specific, Internet Service Provider-given email clients.

[8] We specified a timeframe of one month to control for situations including, for example, Google+'s 2.5 billion-user platform on which more than 90 percent of users have never posted a single piece of content. We chose these SNSs based on popularity (Moreau, 2016), excluding social media—rather than social networking—sites (e.g., Twitter, YouTube, Pinterest).

indicated that the participant (or a household member) had never been a victim of either crime; 2 indicated victimization of at least one type of crime; and 3 indicated victimization of both types of crime. We further adapted these items to pertain to online victimization, in which theft/burglary was adapted to *Have you … victim of identity theft?* and assault/battery was adapted to *Have you … victim of cyberbullying or cyberstalking?* Frequencies of responses to these items are displayed in Table 6.

Table 6
Study 3: Frequencies of physical and online victimization

Frequency of victimization	Neither	One	Both
Physical victimization	57.1%, *n* = 719	33.4%, *n* = 421	9.5%, *n* = 120
Online victimization	69.1%, *n* = 871	25.5%, *n* = 25.5	5.4%, *n* = 68

Demographic variables. At the end of the survey, we asked a series of demographic items (including participant zip code) that addressed our individual difference variables of interest. Participants reported their physical size as a comparison against "the average person of your sex (male/female)" on a 7-point scale from *Much smaller than average* to *Much larger than average*; their height; their self-defense expertise (e.g., taekwondo, karate) on a 5-point scale from *None at all* to *A great deal*; and a two-item index of web-oriented digital literacy from Hargittai (2005). Both digital literacy items were tailored to address skill surrounding online security, distinguished by whether the skill was concentrated around the Internet (*In terms of your Internet skills (e.g., changing privacy or security settings in your browser), do you consider yourself to be…*) or the computer more broadly (*In terms of your computer skills (e.g., securing your computer against viruses or safety threats), do you consider yourself to be…*).

Participants responded along 5-point Likert-type scales that ranged from *Not at all skilled* to *Expert*.

Table 7

Study 3: Descriptive statistics for variables of interest

Variable	Mean	*SD*	*N*
Total safety (inverse of total crime risk)	426.63	72.27	1196
Personal safety (inverse of personal crime risk)	423.96	59.71	1196
Property safety (inverse of property crime risk)	512.47	81.92	1196
Perceived physical safety	5.43	2.07	1262
Perceived online safety	4.49	1.89	1251
Physical size; 7-point scale	4.07	1.13	1255
Height; inches	67.70	4.47	1254
Self-defense expertise; 5-point scale	1.90	1.02	1259
Digital literacy: Internet; 5-point scale	3.46	0.84	1261
Digital literacy: Computer; 5-point scale	2.89	0.94	1262

Table 7 displays basic descriptive statistics for our variables of interest in Study 3, including mean, standard deviation, and sample size values. All study materials, including all scales and indices, are displayed in Appendix A. IRB approval for this study is displayed in Appendix B.[9]

Results and Discussion

Table 8 depicts a bivariate correlation matrix of our key variables of interest. We saw a positive relationship between actual safety and perceived physical safety ($r[1194] = .187, p < .001$) but not between actual safety and perceived online safety ($r[1184] = .008, p > .05$, *ns*); in addition, we saw a positive relationship between perceived physical and perceived online safety, $r(1249) = .130, p < .001$. Past victimization experiences (in both online and offline settings) were negatively related to perceived physical and perceived online safety ($-.195 \leq r[1247\text{-}1258] \leq .070$, $.001 \leq p \leq .013$). Taller individuals tended to

[9] Because Studies 1 and 2 necessitated the use of publicly available archival data, IRB approval was not required.

feel more safe (*r*[1252] = .113, *p* < .001), although self-reported physical size did not appear to play a role in perceived physical or online safety. Those who self-reported that they were more digitally literate tended to feel more safe both online (*r*[1248] = .102, *p* < .001) and offline (*r*[1259] = .091, *p* = .001).

Table 8

Study 3: Correlation matrix of variables of interest

	1.	2.	3.	4.	5.	6.	7.	8.
1. Actual safety	—	—	—	—	—	—	—	—
2. Phys safety	.187***	—	—	—	—	—	—	—
3. Online safety	.008	.130***	—	—	—	—	—	—
4. Victim: phys	-.051	-.195***	-.075**	—	—	—	—	—
5. Victim: online	-.012	-.082**	-.070**	.220***	—	—	—	—
6. Height	.060*	.113***	-.016	-.015	-.074**	—	—	—
7. Physical size	-.036	-.029	-.010	.023	.030	.509***	—	—
8. Self-defense	.023	-.022	-.070**	.053†	.001	.190***	.136***	—
9. Digital lit.	-.021	.091***	.102***	-.037	-.012	.166***	.091***	.154***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 1186 ≤ *n* ≤ 1261

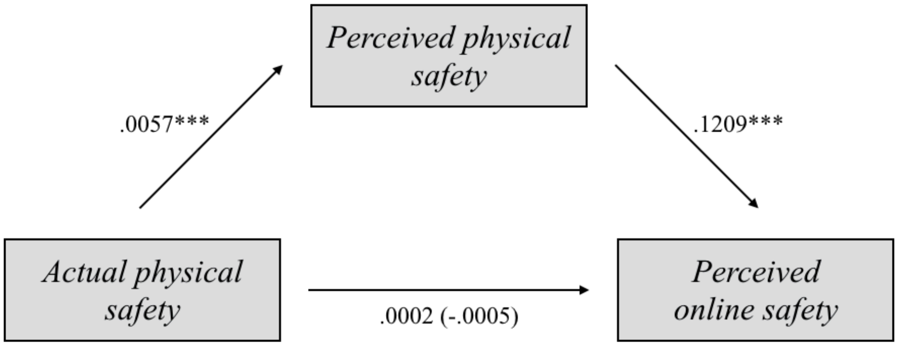
Actual physical safety. As is evident in Table 8, our second hypothesis held that actual physical safety would be a positive reflection of perceived physical safety, in which people who live in safer neighborhoods should report feeling safer in their day-to-day lives. We found that this was indeed the case, even when controlling for self-reported wealth (i.e., annual household income; *r*[1192] = .154, *p* < .001). As such, we found support for Hypothesis 2.

The physical-online relationship. Hypothesis 3 further extended our findings from Studies 1 and 2 by predicting a positive physical-online relationship on the level of individual perception. Supporting this hypothesis, we saw not only a positive bivariate correlation between these perceptions, but also a significant partial correlation when holding wealth constant, *r*(1247) = .126, *p* < .001. Of secondary interest is the website, or websites, of which participants were thinking when they responded to our perceived online safety scale. A majority of participants reported that they used Snapchat, Facebook, and Instagram at least once a month (62.8%, 61.3%, and 61.1%, respectively), with significantly fewer using Google+ (26.6%) and LinkedIn (15.5%). As such, responses to our online safety measure are more likely to pertain to perceptions of safety when using Snapchat, Facebook, and Instagram; and indeed, approximately half (48.9%) of all participants used all three major services. Only 4.7 percent of participants used all five in a typical month.

It is noteworthy that although actual physical safety was related to perceived physical safety, and perceived physical safety was related to perceived online safety, we did not observe a direct relationship between actual physical safety and perceived online safety. Indeed, a test of the mediating impact of perceived physical safety on the relationship between actual physical safety and perceived online safety yields a significant mediation model (Sobel = 3.74, *p* < .001) with highly significant paths from predictor to mediator and mediator to outcome; however, no direct relationship appears between offline actuality and online perception. This mediation model is depicted in Figure 1.

Figure 1

Study 3: Mediation of actual and perceived physical safety and perceived online safety



Person- and situation-specific factors. Hypothesis 4 sought to explore the possibility that person- and situation-specific factors related to threat perception might moderate or buffer this positive relationship between perceived physical and perceived online safety. We used Hayes and Matthes's (2009) computational procedure for probing interactions in ordinary least squares (OLS) regression, displayed in equation form in Equation 1 below. Here, $\hat{Y}$ stands for our dependent variable, perceived online safety; X represents our key predictor of interest, perceived physical safety; and M represents any given person- or situation-specific factor that may act as a moderator variable. Our interaction term is reflected as a product terms (e.g., the interaction of X and M takes the form of XM), and b_0 represents the intercept of each regression line, where $b_{1\text{-}3}$ represents the slope of each respective term.

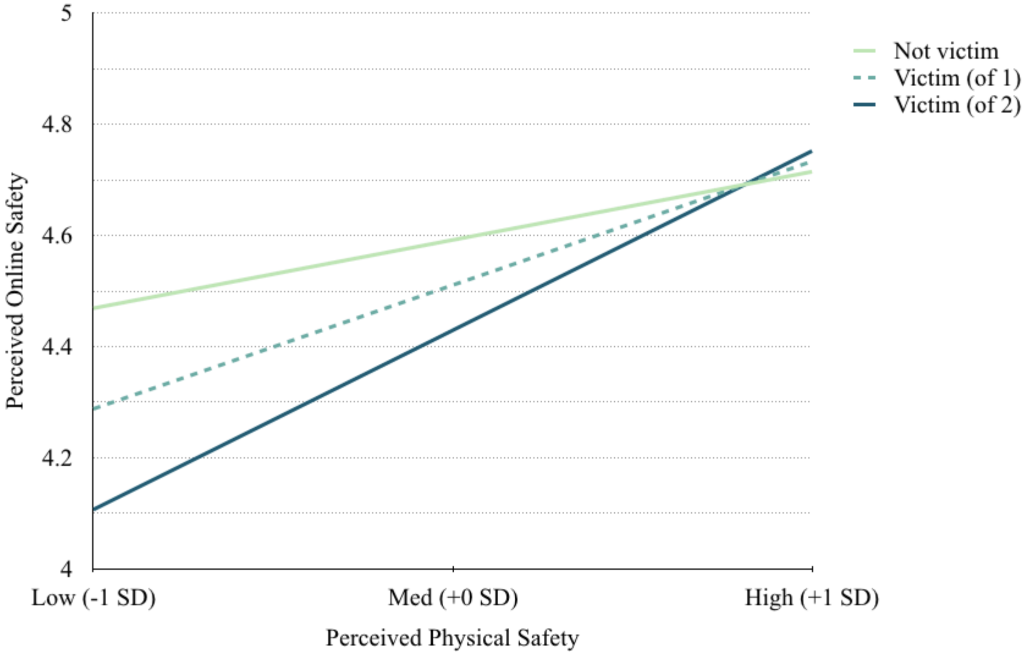
$$\hat{Y} = b_1X + b_2M + b_3XM + b_0 \qquad (1)$$

Through this procedure, we observed a significant interaction of past victimization experiences of physical crime (e.g., burglary, robbery) whereby past victim status played no role in perceived online safety among those who felt highly safe in their physical environments ($b_{\text{not victim}} = .059$, $p > .05$, *ns*). It was only among those who felt very unsafe in day-to-day life where past victim status made a difference ($R^2 = .023$, $F[3,1245] = 9.658$, $p < .001$; $b_{\text{victim1}} = .108$, $p < .001$; $b_{\text{victim2}} = .156$, $p < .001$).[10] For past victims in unsafe physical environments, perceived offline safety was significantly lower; we observed a much sharper decline in perceived online safety with decreases in physical safety.

[10] The subscripts accompanying our *b* coefficients indicate whether the participant has been a victim of one type of physical crime (victim1) or both in the scale (victim2).

Figure 2

Study 3: Moderation of past victim status, physical

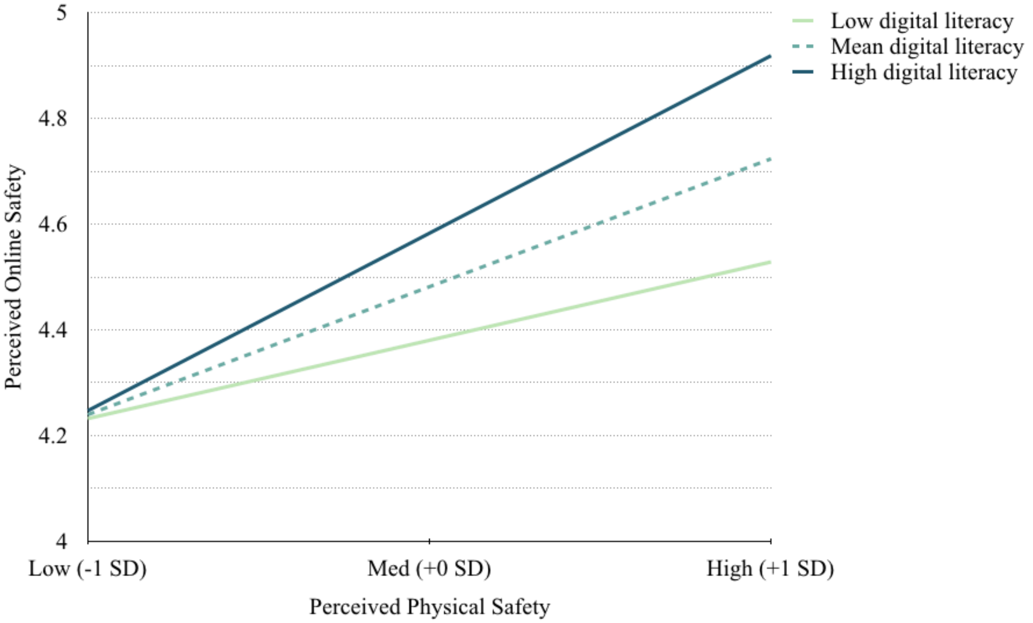


This moderation model ($b_{\text{interaction}}$ = .073, p = .05), which is displayed in Figure 2, may suggest that individuals who have been victimized in the past more readily “blur” or generalize a sense of threat in one domain to the other, possibly to prepare for future attack. If so, this strategy may prove useful in allocating precautionary attention to other domains in which a threat might appear.

We also found a marginally significant moderation effect of digital literacy skills surrounding computer security—namely, securing one’s computer against viruses or safety threats ($b_{\text{interaction}}$ = .048, p = .065, *marginal*). More specifically, and as is shown in Figure 3, digital literacy did not affect perceived online safety among those who felt physically unsafe. But as perceived physical safety increased, those who reported that they were highly digitally literate were those who felt significantly safer online (R^2 =

.023, $F[3,1247] = 9.738$, $p < .001$; $b_{\text{high}} = .162$, $p < .001$); the physical-online relationship grew increasingly positive among these individuals.

Figure 3
Study 3: Moderation of digital literacy, computer security

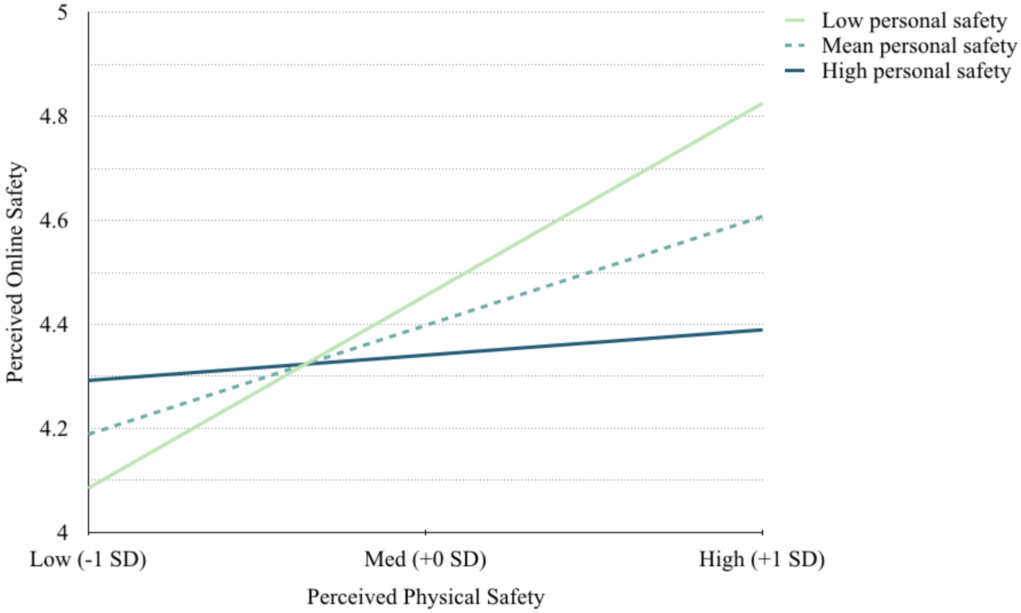


Lastly, we observed a marginal interaction of our actual physical safety composite on the physical-online relationship ($R^2 = .020$, $F[3,1182] = 7.998$, $p < .001$; $b_{\text{interaction}} = -.001$, $p = .084$, *marginal*); probing further, we found that the moderating impact of personal safety—determined by participant zip code—was responsible for this interaction. Indeed, whereas total safety and property safety held no moderating role on the physical-online relationship ($b_{\text{interaction}} = .164$ and .277, respectively; $p > .05$, *ns*), personal safety yielded a significant disordinal (i.e., crossover) interaction, $b_{\text{interaction}} = -.001$, $p = .004$.

Figure 4 illustrates this moderation effect, in which increases in perceived physical safety yielded no impact on perceived online safety among participants who lived in zip codes devoid of rape, murder, assault, and robbery ($R^2 = .025$, $F[3,1182] =$

10.000, $p < .001$; $b_{\text{high}} = .047$, $p > .05$, *ns*). Among participants in mean- or low-safety neighborhoods, however, we saw our predicted positive relationship between physical and online safety: Increases in actual physical safety yielded an increasingly positive relationship between the two ($b_{\text{mean}} = .122$ and $b_{\text{low}} = .197$, respectively; $p < .001$).

Figure 4
Study 3: Moderation of actual physical safety, personal



We observed no additional moderation effects of our person- or situation-specific factors of interest on the relationship between perceived physical and perceived online safety. We therefore found partial support for Hypothesis 4, in which past victim status (namely, of physical crime), digital literacy surrounding computer security, and actual physical safety of one’s neighborhood moderated the physical-online relationship.

Study 4

Our fourth and final study sought to examine the directionality of the tie between physical and online safety by examining whether manipulations of physical safety impacting perceived online safety, as well as the opposite, in which manipulations of online safety informed perceptions of physical safety. We also sought to test the differing roles that type of threat played on the physical-online relationship: Whereas Studies 1, 2, and 3 operationalize threat in self-protection (i.e., bodily harm: assault, murder) and resource domains (burglary, bank robbery), Study 4 separates these two types of threat to assess the unique role that each plays on the generalized nature of threat between physical and online domains.

We therefore conducted an experiment with a 3 × 2 between-subjects design, in which type of threat (3 levels: self-protection threat, resource threat, control) and threat domain (physical, online) were manipulated. Furthermore, and for exploratory purposes, we again examine the role that certain person- and situation-specific factors play on this relationship. Finally, we explore the impact of perceptions of threat on inclination to act upon recommended safety practices both on- and offline.

Method

Participants

Whereas our third study utilized a sample of undergraduate students, our fourth study comprised individuals ("Turkers") who participate in online studies through Amazon's Mechanical Turk (Mturk) in exchange for monetary compensation. To avoid potential confounds of national culture, we required that participants currently reside in the United States and be at least 18 years of age. After running a small pilot study (N = 30) to ensure correctly programmed randomization, display logic, and skip logic within our Qualtrics study, we calculated that the a priori sample size needed for Study 4 should be N = 650 to obtain desired statistical power ($1–\beta = 0.80$) across six conditions with an expected effect size of Cohen's d = .150.

Our final sample on Mturk comprised 656 individuals (52.1% female) with the modal age range between 25 and 34 years old. (84.1% of our sample was younger than 55 years of age.) 75.2 percent were White, 9.1 percent Asian, and 7.2 percent Black or African American; and 46.2 percent self-reported an annual household income between $20,000 and $60,000. It took Turkers an average of 7.59 minutes (*SD* = 4.62) to complete the study. Participants were randomly assigned more or less evenly across the six conditions (15.7-17.2% per condition).[11]

Procedure

To avoid introducing demand characteristics to the study—namely, subtle cues that hint to participants what the experimenter is hoping to find—each participant saw a single prompt at the beginning of the study that read, *We're interested in the impact of information processing on decision-making strategies. Please read the following article carefully. When you've finished reading, we will ask comprehension questions about the article*. This purported focus on information processing and decision-making was meant to mislead participants' expectations as to the nature of the experiment. Upon moving forward, participants were randomly assigned to one of our six conditions with equal presentation (i.e., the randomization was programmed to allot 16.67% of participants into each condition, rather than a purely random assignment). Those assigned to a physical condition were asked to *Imagine that the following article describes events happening in*

[11] More specifically, 16.0% (*n* = 105) were randomly assigned to the physical self-protection threat condition, 17.5% (*n* = 115) to the physical resource threat condition, and 15.7% (*n* = 103) to the physical control condition. 17.1% (*n* = 112) were randomly assigned to the online self-protection threat condition, 16.5% (*n* = 108) to the online resource threat condition, and 17.2% (*n* = 113) to the online control condition.

your community; those in online conditions were asked to *Imagine that the following article describes events that actually happened*. The threat manipulation that followed was altered to look like a news article participants might encounter online, following the style elements of USAToday.com but with the fictitious name *The Courier Sun*.[12]

On the next page, participants answered a single attention check item that asked, *Which of the following best describes the article you just read?* The six answer choices each described our six manipulations in 9-15 words. Of our sample, 96.8 percent correctly answered this attention check item; because we might expect that the remaining 3.2 percent (n = 22) did not read the manipulation (and indeed, these individuals spent an average of 48.06 fewer seconds on the manipulation screen)[13], they were excluded from all further analysis.[14]

Participants then answered all outcome variables pertaining to perceptions of safety,[15] intention to act upon safety practices, person- and situation-specific factors, and demographic characteristics. Table 9 depicts a breakdown of this survey flow, where

[12] When this paper was written, no news source existed under the name *The Courier Sun*; one fictional exception is the community newspaper in *Leave it to Beaver*.

[13] In two of the five conditions for which at least one participant provided an inaccurate answer, we saw a significant difference in time spent on each manipulation, $2.186 \leq t(112) = \leq 2.956$, $.004 \leq p \leq .031$.

[14] All sample descriptive statistics reported above (e.g., mean age, ethnicity frequencies) pertain to only those participants who passed the attention check item (total N = 703, with 53 partial cases).

[15] Participants will view the batteries of perceived safety (physical, online, financial) in their assigned—or “matched”—domain; for example, participants assigned to a physical threat condition will first respond to items gauging perceived *physical* safety, followed by their perceived *online* safety (unmatched domain). Items pertaining to financial safety always appeared last.

columns represent order of presentation for each section of the study (from top to bottom).

Table 9
Study 4: Survey flow

Random Assignment	**Physical**			**Online**		
	Self-protection	**Resource**	**Control**	**Self-protection**	**Resource**	**Control**
News Story Prime	In-person voyeur	Series of car burglaries	Neighborhood development news	Webcam hacker voyeur	Series of bank account burglaries	App development news
Attention Check: Single-item "quiz" to ensure participant attention						
Outcome: Matched Safety	Perceived physical safety			Perceived online safety		
Outcome: Unmatched Safety	Perceived online safety			Perceived physical safety		
Safety practice intentionality (online and offline)						
Person- and situation-specific factors: e.g., past victimization, self-efficacy, threat probability						
Demographic characteristics						

Materials

Threat primes. Our threat primes were modeled very closely after existing news articles published in *USA Today*, *Q13 Fox* (Seattle), and *WeLiveSecurity* priming control conditions, resource threat, and self-protection threat, respectively (Cluley, 2015; Daykin, 2017; Romero, 2017). These three articles were altered to pertain to either the online or offline world, using the same language, sentence structure, and topic flow between both stories to maintain the highest possible comparability between physical and online conditions. For example, *Webcam hacker spent up to 12 hours a day watching his victims* (online, self-protection) was altered to pertain to *Neighborhood voyeur spent up to 12* *hours a day watching his victims* (physical, self-protection). The six articles comprised an average of 211.17 words (*SD* = 7.03), and all proper nouns—names, companies, locations—were altered to fictitious equivalents. It took participants an average of 79.87 seconds (*SD* = 81.77 seconds) to read these primes.[16]

Perceived threat. In Study 3, we operationalized perceived physical safety and perceived online safety more generally: For neighborhoods, we examined the extent to which a person's neighborhood was perceived to feel safe (e.g., belief of safety from bodily harm or stolen property); for the online world, we examined perceptions of safety while navigating major social media sites (e.g., belief that personal information was safe from data breaches). However, in Study 4, our aim was to capture perceptions of safety as they resulted from a recently encountered manipulation, rather than safety more generally; that is, we wanted to tap into immediate senses of threat, risk, and worry rather than stagnant perceptions of safety in one's permanent neighborhood or general Facebook experiences. As such, we used the Financial Threat Scale (FTS) from Marjanovic and colleagues (2013), which was developed to cover a wide breadth of perceived threats, uncertainties, and preoccupations, rather than just financial concerns.

This five-item measure was mirrored across topics of physical threat, online threat, and financial threat by altering the target language in each item. For example, the prompt asked participants to *indicate how you feel at this moment about your personal safety (i.e., in your day-to-day life)* (physical), *...about your online safety (i.e., while*

[16] Our notably high standard deviation stemmed from one participant who took 35.38 minutes to proceed to the next page. This participant passed our attention check and did not score as an outlier on any variable of interest, so was thus kept for all further analyses.

using technology) (online), or *...about your financial safety (i.e., from someone stealing from you)*. Subsequent items were phrased to refer to the original target (safety type): *How much does your (personal/online/financial) safety feel at risk?* or *How much does your (personal/online/financial) safety feel threatened?*. All answer choices fell along a five-point Likert-type scale from *Not at all* to *A great deal*.

Because our physical threat (*M* = 2.22, *SD* = 0.92), online threat (*M* = 2.67, *SD* = 0.88), and financial threat (*M* = 2.74, *SD* = 1.10) scales demonstrated very strong reliability for five-item scales (α = .94, .92, and .95, respectively), we formed averaged composites for each.

Safety practice intentionality. After reporting perceptions of safety, participants viewed a page titled *Tips to Stay Safe*. This first page contained three recommended practices, written in an educational format, with links to webpages or applications that assist in online safety (e.g., preventing identity theft and phishing, adding two-factor authentication to e-mail or social networking accounts) and physical safety (avoiding physical altercations or other physical threats), alternating between the two safety domains. These tips were, on average, 63.43 words in length (*SD* = 13.31 words). For each tip, there was a question asking participants' likelihood of following the recommendation along a 6-point Likert-type scale. At the end of the page, participants had the option to view more tips; if they selected *Yes*, they viewed up to three more pages of an identical format, alternating between online and offline safety tips. If they selected *No*, they were redirected to the next section of the study. For each page of safety practices, we collected length of time spent on this instructional page, actual clicking behaviors following the embedded links, and the number of pages they read (between 1 and 4).

Regardless of the number of pages participants chose to visit, the section ended with the response efficacy and self-efficacy subscales of Witte and colleagues' (1995) Risk Behavior Diagnosis (RBD) Scale. These items gauged the extent to which participants felt that the tips would be effective in avoiding personal or online harm (e.g., *If I follow these tips, I am less likely to be attacked*; α = .86)—that is, response efficacy—as well as the extent to which participants felt that they had the ability or resources to act on the tips (*I have the skills to follow these tips to stay safe*; α = .89)—that is, their self-efficacy.

Table 10 displays basic descriptive statistics concerning participants' consumption of these safety practices, including the percentage of participants who viewed each page; the amount of time spent on each page; the total number of times participants clicked on a link on the page; and the average likelihood that participants reported they would follow the tips on that page (on a 6-point Likert-type scale).

Table 10

Study 4: Descriptive statistics for safety practice consumption

	Viewers (%)[17]	Time spent (sec)	Click count	Likelihood of following
Page 1 (3 tips)	70.9	71.79 (55.86)	6.33 (4.79)	4.51 (1.35)
Page 2 (3 tips)	13.5	51.02 (29.02)	6.05 (4.15)	4.94 (1.20)
Page 3 (4 tips)	6.9	53.56 (36.54)	7.13 (4.91)	5.26 (0.99)
Page 4 (4 tips)	8.7	45.48 (42.05)	5.25 (3.32)	5.09 (1.14)

Time spent, Click count, and Likelihood of following are displayed as M(SD).

[17] This column indicates the percentage of participants who viewed only up until the end of that page; for example, 13.5% of participants viewed pages one and two, whereas 8.7% viewed all four pages.

We created two composite variables for likelihood of acting on these safety practices, separated by whether the tips concerned online (α = .76; *M* = 5.00, *SD* = 1.00) or physical safety (α = .83; *M* = 3.70, *SD* = 1.60). On the whole, reported likelihoods were positively correlated with a mean inter-item correlation of .327 across all online tips, and .453 for all physical tips.

Situation-specific factors. We operationalized perceived threat probability through a single-item measure prompting participants to think of the threat described in the article from the beginning of the study. They were then asked to indicate *How often do you think an event like this occurs?* on a 7-point Likert-type scale ranging from *Never* to *All the time*. Participants then responded to the three-item threat severity subscale from Witte and colleagues' (1995) RBD Scale (e.g., *I believe that the threat described in this article is severe*), which we combined into a single composite index (α = .88).

Person-specific factors. To measure perceived susceptibility to the threat, we presented participants with the RBD susceptibility subscale (e.g., *I am at risk for a threat like this*; Witte et al., 1995).[18] Given the high degree of inter-item agreement for a three-item scale (α = .87), we created a single composite of perceived susceptibility. We then gauged physical size, height, self-defense expertise, security-specific digital literacy, and permanent zip code through the same indices described in Study 3. The study concluded with a suite of standard demographic items gauging sex, age group, race/ethnicity, annual household income, and education.

[18] Because Control participants did not read about a threat in their assigned news article, we used Display Logic to ensure they did not see threat severity, susceptibility, or probability items.

All study materials, including all scales, indices, and threat primes, are displayed in Appendix C. IRB approval for this study is displayed in Appendix D. Table 11 displays basic descriptive statistics for all variables of interest, including our person- and situation-specific factors. These descriptive statistics are separated by condition in Tables 12-17 in Appendix E.

Table 11
Study 4: Descriptive statistics for all variables of interest

Variable Type	Variable	Range	Mean	*SD*	*N*
Perceived threat	Perceived physical threat	1-5	2.22	0.92	656
	Perceived online threat	1-5	2.67	0.88	656
	Perceived financial threat	1-5	2.74	1.10	654
Safety practice intentionality	Safety practice intentionality: Online	1-6	5.00	1.00	654
	Safety practice intentionality: Physical	1-6	3.70	1.60	653
	Safety practices pages viewed	1-4	1.53	0.95	654
	Response efficacy (safety practices)	1-6	4.56	0.91	650
	Self-efficacy (safety practices)	1-6	4.96	0.76	650
Victimization	Victim: Physical crime	0-2	0.59	0.73	649
	Victim: Cybercrime	0-2	0.36	0.58	650
Situation-specific	Perceived threat severity	1-6	4.67	0.94	435*
	Perceived threat probability	1-7	4.49	1.35	435*
Person-specific	Perceived threat susceptibility	1-6	3.71	1.13	435*
	Physical size	1-7	4.19	1.30	648
	Height (inches)	56-83	67.19	4.03	645
	Self-defense expertise	1-5	1.82	0.97	648
	Security-related digital literacy	1-5	3.25	0.75	648

* *Smaller sample size reflects that only participants in non-control conditions viewed and answered these items*

Results and Discussion

Tables 18, 19, and 20 display correlation matrices of our key variables of interest. Table 18 depicts the relationships between our key dependent variables, including perceived safety and intentionality to act on safety practices; Table 19 depicts the relationships between our person- and situation-specific factors; and Table 20 depicts the relationships between these two sets of variables (i.e., with our outcome variables as rows and exploratory factors as columns).

Table 18

Study 4: Correlations of dependent variables of interest

	1.	2.	3.	4.	5.	6.	7.
1. Physical threat	—	—	—	—	—	—	—
2. Online threat	.538***	—	—	—	—	—	—
3. Financial threat	.457***	.482***	—	—	—	—	—
4. Online tip intent	.076†	.186***	.089*	—	—	—	—
5. Physical tip intent	.240***	.234***	.148***	.357***	—	—	—
6. Tip pages viewed	.132***	.149***	.096**	.154***	.376***	—	—
7. Response efficacy	.088*	.116**	-.017	.369***	.388***	.181***	—
8. Self-efficacy	.026	.032	.010	.317***	.317***	.164***	.634***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 649 ≤ *n* ≤ 656

Table 19

Study 4: Correlations of person- and situation-specific factors

	9.	10.	11.	12.	13.	14.	15.	16.
9. Victim: phys	—	—	—	—	—	—	—	—
10. Victim: online	.234***	—	—	—	—	—	—	—
11. Severity	-.002	-.001	—	—	—	—	—	—
12. Probability	.156***	.104*	.254***	—	—	—	—	—
13. Susceptibility	.116*	.120*	.219***	.574***	—	—	—	—
14. Physical size	.071†	-.002	.054	.153***	.085†	—	—	—
15. Height	.001	-.026	-.097*	-.045	-.022	.502***	—	—
16. Self-defense	.054	.150***	-.015	.130**	.044	.100**	.196***	—
17. Digital literacy	.016	.027	-.126**	.005	-.003	.085*	.138***	.237***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 434 ≤ *n* ≤ 649

Table 20

Study 4: Correlations of dependent and exploratory factors

	9.	10.	11.	12.	13.	14.	15.	16.	17.
1.	.088*	.057	.122*	.242***	.271***	.002	-.101**	.084*	-.038
2.	.052	.102**	.237***	.240***	.267***	.049	<.001	.126***	-.127***
3.	.116***	.106**	.140**	.225***	.281***	.042	-.040	.044	.034
4.	-.017	-.017	.253***	.122**	.061	-.017	-.113**	-.059	.023
5.	.009	.064	.179***	.253***	.213***	-.020	-.153***	.149***	.017
6.	.143***	.061	.049	.110*	.068	-.001	-.042	.160***	.020
7.	-.026	.006	.285***	.150**	.144***	-.041	-.120**	.033	-.018
8.	.038	.010	.290***	.187***	.115*	-.023	-.146***	.027	.111**

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 435 ≤ *n* ≤ 650

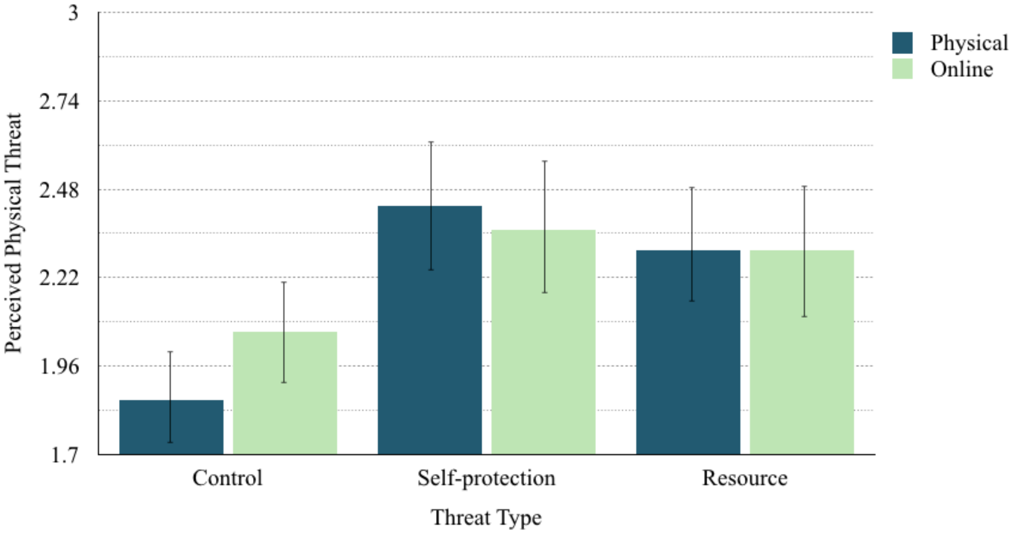
Tables 21-38—which can be found in Appendix E—depict these correlations in the same order, separated by condition.

Analyses of variance

We first examined whether our manipulations were effective at priming threat in their respective domains. We ran a series of analyses of variance (ANOVA) in which threat domain condition (2-level: physical, online) and threat type condition (3-level: self-protection, resource, control) were entered as random factors predicting perceived physical threat, perceived online threat, and perceived financial threat. There were no two-way interactions of threat domain and threat type on perceived physical threat (*F*[2,650] = 1.224, p > .05, *ns*, η_p^2 = .004), perceived online threat (*F*[2,650] = 1.305, p > .05, *ns*, η_p^2 = .004), or perceived financial threat (*F*[2,648] = .002, p > .05, *ns*, η_p^2 < .001). However, we did observe a significant main effect of condition on perceived physical safety (*F*[5,650] = 5.892, p < .001, η_p^2 = .043) and perceived online safety (*F*[5,650] = 4.047, p = .001, η_p^2 = .030), which we probe further in the following section. There was no main effect of condition on perceived financial safety, *F*(5,648) = .186, p > .05, *ns*, η_p^2 = .001. Figures 5, 6, and 7 illustrate mean values of perceived physical, online, and financial threat (respectively) across each of our six conditions. Interestingly, these graphs—as well as the descriptive statistics displayed in Table 11—suggest that overall, participants report feeling less physical threat than online or financial threat, regardless of condition.

Perceived physical threat. Figure 5 illustrates a clear between-group difference on perceived physical safety (*F*[5,650] = 5.892, p < .001, η_p^2 = .043) in which overall (and as should be expected), participants assigned to our control conditions reported significantly lower perceptions of physical threat, $F(1,650) = 26.22$, $t(650) = 5.12$, $p < .001$, $\eta_p^2 = .039$.

Figure 5
Study 4: Mean perceived physical threat scores across conditions



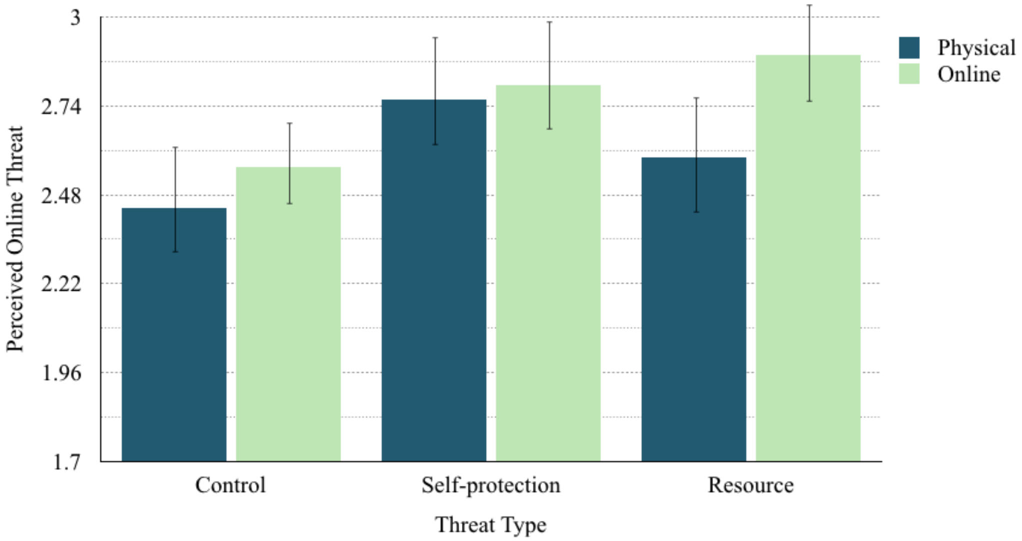
When contrasting participants in any of our physical conditions against those in our online conditions, we again see significantly higher perceptions of threat, $F(1,650) = 8.54$, $t(650) = 2.93$, $p = .004$, $\eta_p^2 = .013$. However, when we contrasted only physical threat conditions against online threat conditions (that is, excluding control conditions from analysis), this difference vanished ($t[438] = .339$, $p > .05$, *ns*), possibly suggesting that both physical and online threat primes may generalize or "blur" to impact perceptions of physical safety.

When contrasting participants by type of threat, we found that perceived physical threat was significantly higher among self-protection groups (both physical and online) compared with all other groups, $F(1,650) = 12.282$, $t(650) = 3.51$, $p < .001$, $\eta_p^2 = .019$; however, this difference vanished when excluding control groups from analysis ($t[438] =

1.002, $p > .05$, *ns*). We found no such distinction among resource threat groups, $F(1,650) = 2.672$, $t(650) = 1.64$, $p > .05$, *ns*, $\eta_p^2 = .004$.

Perceived online threat. Figure 6 illustrates clear differences between our six conditions on perceptions of online threat, $F(5,650) = 4.047$, $p = .001$, $\eta_p^2 = .030$; and indeed, participants assigned to our control conditions reported notably lower perceived online threat than those in our threat conditions, $F(1,650) = 12.836$, $t(650) = 3.58$, $p < .001$, $\eta_p^2 = .019$.

Figure 6
Study 4: Mean perceived online threat scores across conditions



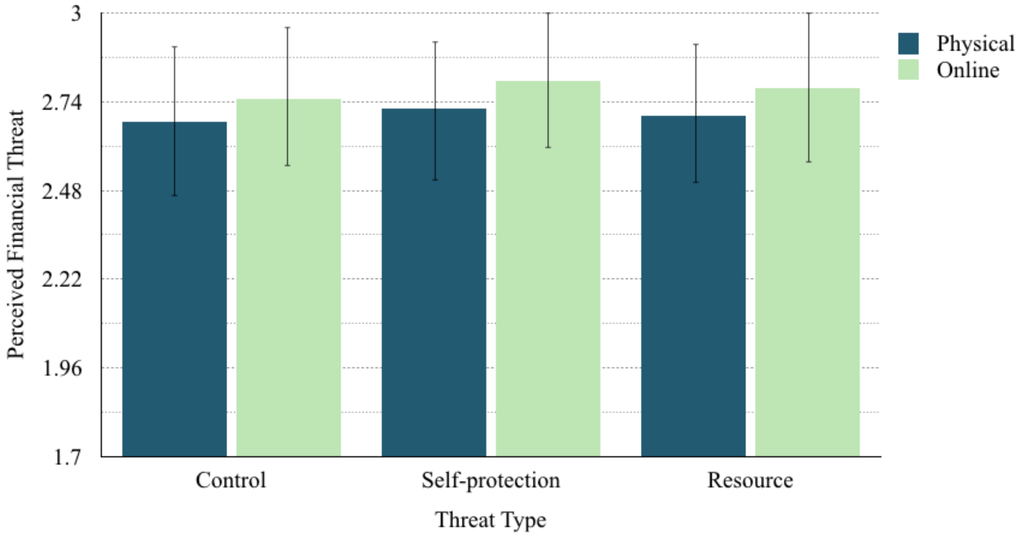
As we would expect to see, participants reported higher perceptions of online threat if they were randomly assigned to one of our online threat conditions compared with the remaining four conditions ($F[1,650] = 12.53$, $t(650) = 3.54$, $p < .001$, $\eta_p^2 = .019$), and this difference remained significant when contrasting our online threat groups against only our physical threat groups (i.e., excluding control groups from analysis), $t(438) = 1.976$, $p = .049$.

Again, and as was the case with perceived physical threat, perceived online threat was significantly higher among self-protection groups than our four remaining groups, $F(1{,}650) = 4.960$, $t(650) = 2.22$, $p = .03$, $\eta_p^2 = .008$; however, when we excluded our control groups from analysis, this difference vanished ($t[438] = .544$, $p > .05$, *ns*). There were no significant differences when contrasting resource threat groups against other conditions, $F(1{,}650) = 1.877$, $t(650) = 1.37$, $p > .05$, *ns*, $\eta_p^2 = .003$.

Perceived financial threat. Figure 7 depicts markedly similar levels of perceived financial threat across our six conditions, none of which are significantly different from one another ($F[5{,}648] = .186$, $p > .05$, *ns*, $\eta_p^2 = .001$). No differences emerged when contrasting conditions by threat domain ($t[437] = -.754$, $p > .05$, *ns*) or type of threat ($F[1{,}648] = .001$, $t[648] = .03$, $p > .05$, *ns*, $\eta_p^2 < .001$).

Figure 7

Study 4: Mean perceived financial threat scores across conditions



That we found no difference in perceived financial threat among participants assigned to our resource threat conditions is noteworthy; logically, these threat primes should have yielded increased perceptions of financial threat. However, it is possible that among the demographic of our present sample, the loss of car parts or valuables kept inside participants' cars did not pose as grave a financial threat as we might have anticipated; regarding our online resource threat prime, participants may have (possibly correctly) expected that if they were to fall victim to bank account fraud through a mobile payment app such as Venmo or Paypal—that is, the target of a string of burglaries in our news article prime—these apps would reimburse them for their losses, as is customary for many financial institutions.

Taken together, our ANOVA results indicate that our threat manipulations seem to have achieved their purpose: Physical threat primes yielded higher perceptions of physical threat, and online threat primes led to higher perceptions of online threat. As we would expect, participants assigned to control conditions reported the lowest perceived threat in either domain. On average, participants in self-protection conditions reported higher levels of threat compared with other groups, and there were no between-group differences in perceptions of financial threat. Finally, it appears that when participants were primed with either physical or online threats, their perceptions of physical threat increased to similar levels, suggesting a generalized or blurred effect from even online threats to perceptions of physical threats.

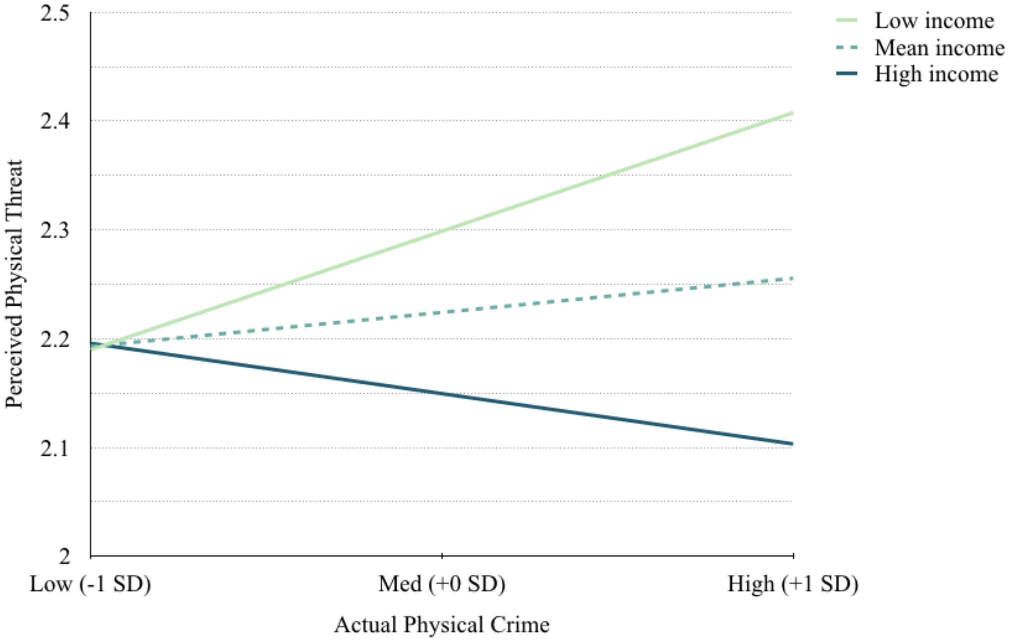
Relationship between physical and online safety

Actual physical safety. After examining these between-group differences on our threat outcome variables, we compared the strength of the relationship between perceptions of physical and online safety by condition, which constitutes our fifth and sixth hypotheses. Although only an exploratory aim for our fourth study, we first examined the relationship between actual physical safety and perceived physical safety, replicating our methods of participant zip code safety coding described in Study 3. Because our indices in Study 4 reflect perceived threat, rather than perceived safety, we did not reverse-code these safety scores; rather, we left them in their original form as total crime, personal crime, and property crime indices ($\alpha = .95$), creating a final composite of actual crime ($M = 100.60$, $SD = 84.83$).

Contrary to Study 3, actual crime was not related to perceived physical threat ($r[615] = .045$, $p > .05$, *ns*), online threat ($r[615] = .005$, $p > .05$, *ns*), or financial threat ($r[615] = -.001$, $p > .05$, *ns*). When contrasting participants who viewed a threat prime against those assigned to a control condition, these correlations remained nonsignificant for both groups (physical: $z = .128$, $p > .05$, *ns*; online: $z = -.360$, $p > .05$, *ns*; financial: $z = 1.058$, $p > .05$, *ns*). Because Studies 1, 2, and 3 underscore the importance of wealth on threat perception and perceived safety, we examined whether income moderated the impact of actual physical safety on perceived physical safety, and found a significant interaction effect ($R^2 = .016$, $F[3,610] = 3.28$, $p = .02$; $b_{\text{interaction}} = -.0003$, $p = .043$) whereby participants (across all six conditions) from low-crime zip codes perceive approximately similar levels of physical threat; however, as crime increases, threat increases most rapidly among participants from low-income households, possibly reflecting a decreased ability to counter or avoid the threat through safety tools (e.g., alarm systems) and similar security resources. Alternatively, due to neighborhood variation within zip codes, it is likely that low-income households are more cognizant of crime if they are located in lower-income, and higher-crime, neighborhoods; wealthy households may exist within the same zip code, but in safer communities. As such, these wealthier individuals may not perceive physical threat because they are rarely privy to actual crimes in their own immediate surroundings. This interaction effect is depicted in Figure 8.

Figure 8

Study 4: Impact of wealth on the actual-perceived physical safety relationship



Correlations between actual crime, its constituents, and our key threat variables of interest are displayed in Table 39.

Table 39

Study 4: Correlations of actual physical crime and perceived threat variables

	1.	2.	3.	4.	5.	6.	7.
1. Actual crime	—	—	—	—	—	—	—
2. Total crime	.992***	—	—	—	—	—	—
3. Personal crime	.935***	.893***	—	—	—	—	—
4. Property crime	.945***	.957***	.770***	—	—	—	—
5. Physical threat	.045	.049	.064	.025	—	—	—
6. Online threat	.005	.012	.012	-.001	.538***	—	—
7. Financial threat	-.001	-.010	.013	-.010	.457***	.482***	—
8. Annual income	-.098*	-.115**	-.073†	-.106**	-.103**	-.024	-.118***

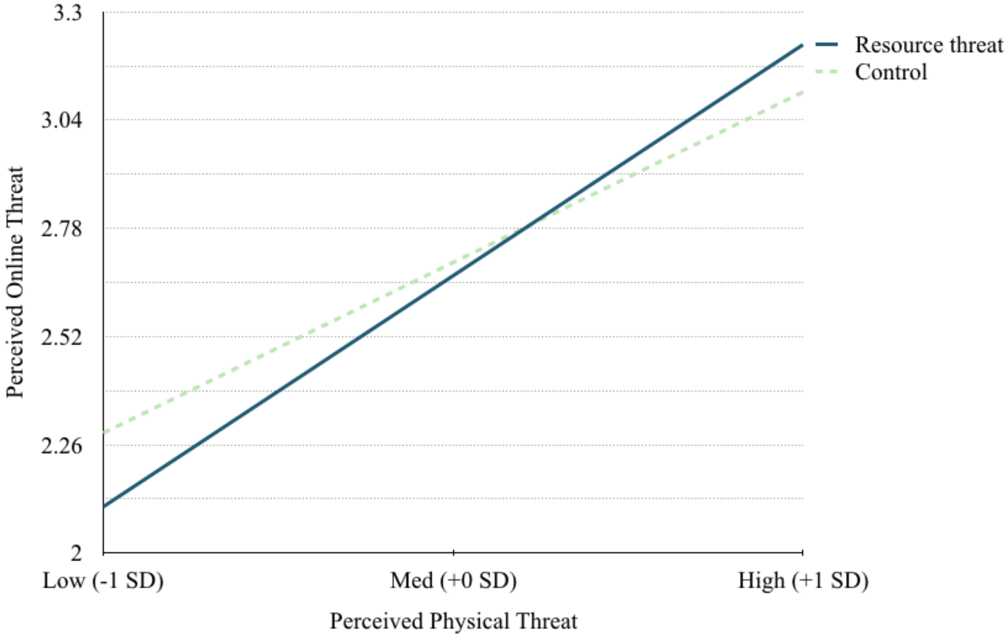
† $p < .10$, * $p < .05$, ** $p < .01$, *** $p < .001$; $597 \leq n \leq 654$

Self-protection vs. resource threat. The core research question that Study 4 sought to answer was whether manipulations of physical threat would predict perceptions of online threat, as well as the reverse, in which manipulations of online threat would predict perceived physical threat. We first examined the former of these directional ties using Equation 1 from Study 3, in which we regressed (1) perceived physical threat (b_1X), (2) type of threat (dummy-coded as either [A] self-protection threat or control or [B] resource threat or control; b_2M), and (3) the interaction of these two predictors (b_3XM) on our outcome variable ($\hat{Y}$), perceived online threat. We found no significant interaction effect when examining self-protection threat groups against control conditions (β = .037, $t[652] = 1.109$, $p > .05$, *ns*); instead, both groups of participants displayed consistently positive relationships between physical and online safety. Similarly, no interaction effect emerged when only examining participants assigned to a physical threat condition ($R^2 = .237$, $F[3,319] = 32.993$, $p < .001$; $b_{\text{interaction}} = -.048$, $p > .05$, *ns*).

However, when examining resource threat groups against control conditions, we found a significant interaction (β = -.078, $t[652] = -2.324$, $p = .02$; $R^2 = .296$, $F[3,652] = 91.551$, $p < .001$) in which participants assigned to resource threat conditions showed a much stronger positive relationship between perceived physical and online safety compared with control participants ($b_{\text{interaction}} = -.096$, $p = .02$). Stated differently, among those who perceive very little physical threat, resource threat participants perceive less online threat than participants who viewed no threat prime at all. Among those who felt highly physically threatened, however, control participants reported lower levels of online threat than their resource threat counterparts. This means that control participants showed less blurring between perceptions of physical and online threat—that is, a lesser degree of generalized threat—compared with participants who saw a resource threat prime. This interaction effect is illustrated in Figure 9.

Figure 9

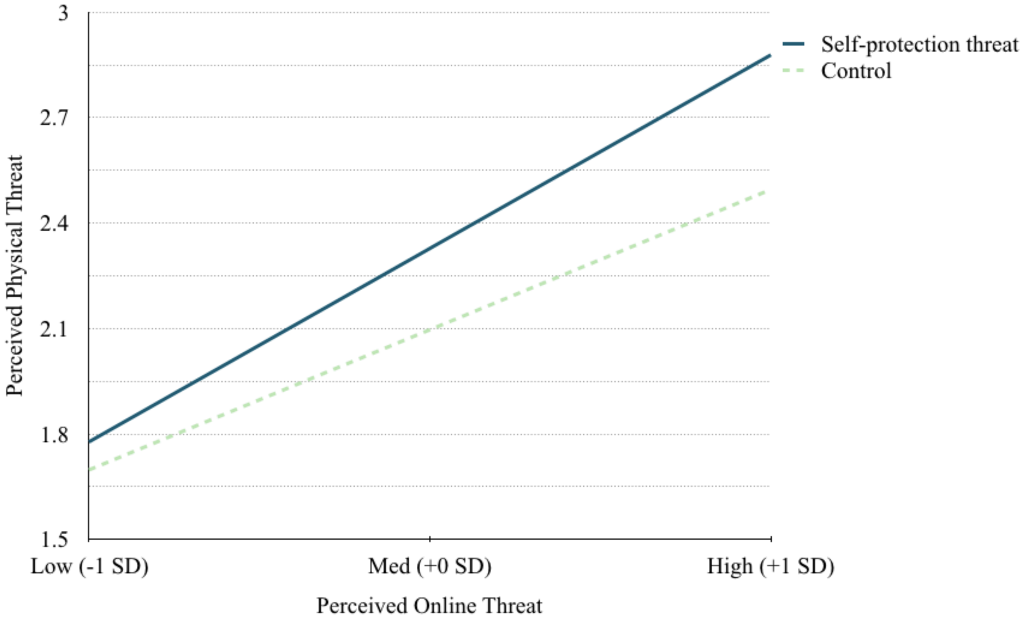
Study 4: Impact of resource threat vs. control on the physical-online relationship



We next examined this contrast between threat type in the reverse direction, in which perceived online threat predicts perceptions of physical threat. We found a significant interaction when contrasting self-protection threat against control group participants, β = .081, $t(652) = 2.472$, $p = .014$; $R^2 = .311$, $F(3,652) = 97.953$, $p < .001$. This interaction, which is portrayed in Figure 10 ($b_{\text{interaction}} = .106$, $p = .014$), depicts a stronger positive relationship between perceived online threat and perceived physical threat among participants in self-protection conditions, as opposed to control conditions. When participants perceive very low levels of online threat, perceptions of physical threat remain relatively similar regardless of condition; however, among those who felt highly physically threatened, participants who viewed a self-protection threat prime (either online or offline) reported significantly higher levels of perceived physical threat.

Figure 10

Study 4: Impact of self-protection threat vs. control on the online-physical relationship



When contrasting control groups against resource threat groups, however, we found no such interaction effect (β = -.020, $t[652] = -.601$, $p > .05$, *ns*); instead, we found approximately similar slopes of positive relationships between online and physical safety. This remained the case when only examining participants assigned to online threat conditions ($R^2 = .352$, $F[3,329] = 59.437$, $p < .001$; $b_{\text{interaction}} = .037$, $p > .05$, *ns*. We found no gender effects when examining self-protection threat primes against control conditions ($R^2 = .291$, $F[4,639] = 65.653$, $p < .001$; $b_{\text{gender}} = -.020$, $p > .05$, *ns*), nor did we observe a difference when examining resource threats against control conditions ($R^2 = .296$, $F[4,639] = 67.040$, $p < .001$; $b_{\text{gender}} = -.014$, $p > .05$, *ns*. Stated differently, we found consistently positive relationships between physical and online threat among participants in self-protection threat conditions (β = .643, $t[215] = 12.313$, $p < .001$; $R^2 = .414$, $F[1,215] = 151.599$, $p < .001$) and resource threat conditions (β = .421, $t[221] = 6.899$, $p < .001$; $R^2 = .177$, $F[1,221] = 47.596$, $p < .001$).

To test Hypothesis 5, which explored the possibility that threat type would pose differing impacts on the physical-online tie, we examined the strength of the relationships between perceived physical (*X*) and online safety ($\hat{Y}$) within the individual groups of our moderator variable *Z*, the dummy-coded measure of threat type (self-protection vs. resource). To accomplish this, we separated data by group before estimating individual regression equations, deemed our simple slopes—quite literally, the magnitude of the slopes of each regression line of *X* on $\hat{Y}$. Equations 2 and 3 depict our simple slopes equations for self-protection threat participants (Equation 2) and resource threat participants (Equation 3).

$$\hat{Y} = b_{1,Z=1}X + b_{0,Z=1} \tag{2}$$

$$\hat{Y} = b_{1,Z=2}X + b_{0,Z=2} \tag{3}$$

Next, we tested the difference between our obtained simple slopes using the method elucidated in Robinson, Tomek, and Schumacker (2013), whereby:

$$t = \frac{b_{\text{diff}}}{SE_{\text{pooled}}} \tag{4}$$

where b_{diff} is the difference between out obtained *b* values stemming from our regression equation, and SE_{pooled}—that is, pooled standard error—is equal to:

$$SE_{\text{pooled}} = \sqrt{\frac{n_1 SE_1^2 + n_2 SE_2^2}{n_1 + n_2 - 2}} \tag{4}$$

We computed the significance of our obtained *t* statistic, or the value indicating the degree of difference between both simple slopes, by using a degrees of freedom of ($n_1 + n_2 - 2$) in our calculations.

In support of Hypothesis 5, we observed a main effect of threat type on the relationship between perceived physical and online safety; namely, this relationship was stronger in self-protection threat conditions than in resource threat conditions (*t*[438] = 4.145, *p* < .001). This difference was also significant when examining the impact of perceived online threat on perceived physical threat, *t*(438) = 3.659, *p* < .001.

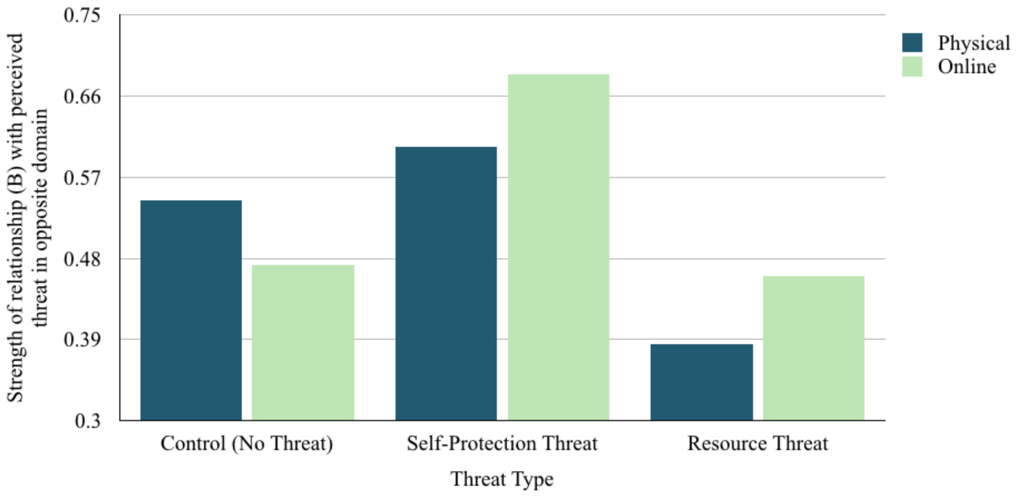
Physical vs. online threat. When comparing participants assigned to physical and online threat manipulations, we again found positive relationships between physical and online safety for both groups (physical: β = .447, *t*[218] = 7.379, *p* < .001; R^2 = .200, *F*[1,218] = 54.455, *p* < .001; online: β = .623, *t*[218] = 11.768, *p* < .001; R^2 = .388, *F*[1,218] = 138.475, *p* < .001). We regressed perceived physical threat, assignment to threat domain (dummy-coded to indicate physical or online conditions), and the interaction of these two predictors on perceptions of online threat while aggregating across threat type. Although there was a significant relationship between physical and online safety in both groups, the relationship was not significantly stronger among online threat participants as per a simple slope difference analysis (*t*[654] = .805, *p* > .05, *ns*). However, when we regressed perceived online threat on perceived physical threat in the same fashion, we found a significant difference between these simple slopes; more specifically, participants in online threat conditions displayed a significantly stronger relationship (that is, more blurring) between perceived online and perceived physical threat, *t*(654) = 3.806, *p* < .001.

As such, we found partial support for Hypothesis 6: We observed a main effect of threat domain in which participants in online threat conditions showed a stronger positive relationship between perceived online safety and perceived physical safety. However, this effect vanished when predicting perceived online safety from perceived physical safety. This finding suggests that when primed with online threats, perceptions of those online threats will readily, and strongly, generalize to perceptions of physical threats—more so than the reverse, in which perceived physical threat guides or informs perceived online threat.

Comparing relationship strength across conditions. Across all six conditions, we observed positive relationships between perceived physical and perceived online threat. Figure 11 plots the strength of these six relationships, which are indicated through obtained *B* coefficients for each regression equation.

Figure 11

Study 4: Comparing indices of relationship strength across conditions



Each coefficient, which measures the change in our dependent variable with every one-unit increase in our predictor variable, reflects the predictive power of the manipulated threat type on perceived threat in the opposite domain: For participants assigned to a physical threat condition, we regressed physical threat on perceived online threat, and performed the reverse regression equation for those assigned to online threat conditions.

The strength of the relationships observed among participants in self-protection (physical: B = .604; online: B = .685) and resource threat conditions (physical: B = .385; online: B = .460) very closely approximates our original conjectures—namely, that (1) self-protection threats may be more dire to survival and therefore generalize more readily; and that (2) online threats may generalize more readily than physical threats because they may trickle into the physical world. However, we see a much stronger relationship between perceived physical (B = .545) and perceived online safety (B = .473) among participants assigned to our control conditions than we might have expected to find, considering participants in these conditions were not primed with threat at all. On average, these individuals showed a significantly positive relationship between perceived physical and online threat (β = .508, t[214] = 8.629, p < .001; R^2 = .258, F[1,214] = 74.465, p < .001), possibly reflecting generalized perceptions of *safety* between the two domains, even in the absence of primed threat: As was the case in Studies 1, 2, and 3, there appears to be a tie between perceptions of safety between the two spheres. For control participants in this study, who reported consistently lower perceptions of threat, we see that those who tend to feel safer in one domain also feel safer in the other.

Also worthy of note is the difference between physical and online threat domains in each threat type condition: Whereas participants in self-protection and resource threat conditions displayed a stronger positive relationship between perceived physical and online safety if they were assigned to an online threat prime, participants in the online control condition showed a weaker relationship between the two. It is possible that when people are not primed with overt examples of cybercrime, they do not readily generalize perceptions of threat into other domains. As such, it may be that people still require clear examples of threats in the online world to perceive it as dangerous, and to generalize that threat into the physical world.

Table 40 displays these *B* coefficients alongside their respective standard errors, as well as the conditions from which each condition is significantly different. For example, our physical self-protection threat condition is significantly different from the obtained slopes for the online control, physical resource threat, and online resource threat conditions ($|2.443| \leq t[433] \leq |4.149|$, $<.001 \leq p \leq .01$).

Table 40

Study 4: Standardized differences between B *coefficients per condition*

	Control	**Self-Protection**	**Resource**
Physical	.545 (.063) $_{a}$	.604 (.049) $_{a, c}$	.385 (.056) $_{b}$
Online	.473 (.055) $_{a, b}$	.685 (.056) $_{c}$	.460 (.067) $_{a, b}$

B coefficients (paired with standard errors) with unmatched subscripts are significantly different, $p < .05$

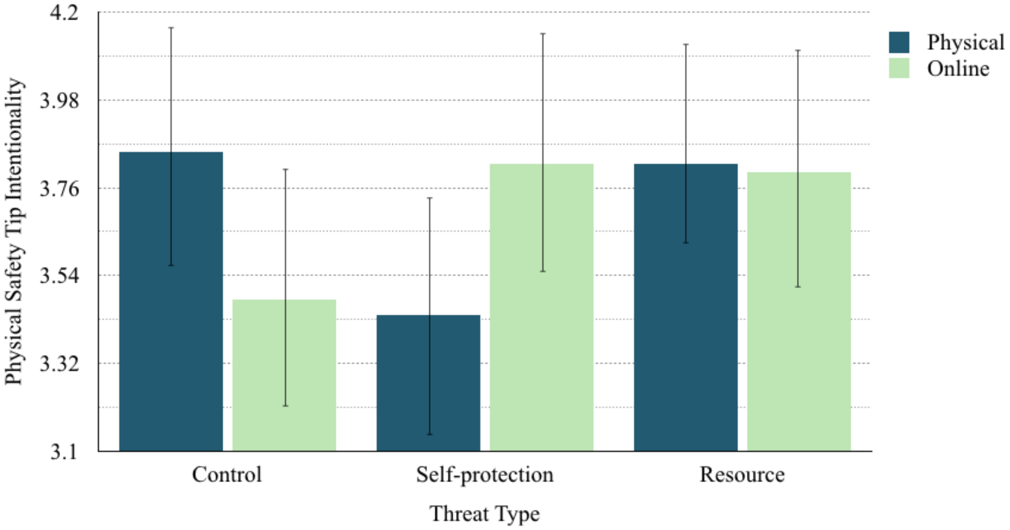
Downstream safety behaviors

After establishing that (1) our manipulations had our intended effect on perceptions of threat and (2) physical and online threat are positively related across conditions, we sought to examine whether these heightened perceptions of threat impacted intentionality to follow recommended safety practices both on- and offline.

A one-way ANOVA revealed no significant differences across our six conditions in intentionality to follow safety practices either online ($F[5,648] = .811$, $p > .05$, *ns*, $\eta_p^2 = .006$) or offline ($F[5,647] = 1.464$, $p > .05$, *ns*, $\eta_p^2 = .011$). There was a marginal difference in the number of safety tip pages viewed by condition, $F[5,648] = 1.864$, $p = .10$, $\eta_p^2 = .014$, *marginal*. Although we found no two-way interaction on online safety practice intentionality ($F[2,648] = .956$, $p > .05$, *ns*, $\eta_p^2 = .003$), we observed a marginal two-way interaction on its physical safety counterpart ($F[2,647] = 2.912$, $p = .055$, $\eta_p^2 = .009$, *marginal*) whereby participants in the resource condition reported relatively stagnant likelihoods of following safety practices between physical and online conditions, whereas control participants were more likely to follow these physical safety-related tips only if they were assigned to the physical control condition. Interestingly, participants in self-protection conditions were more likely to follow these tips only if they read the online self-protection prime, but not the physical self-protection prime. This indicates that participants who read about an online voyeur who had used widely propagated malware to hack others' webcams reported that they were more likely to follow physical safety recommendations than those who read about a neighborhood voyeur who posed a physical safety threat. This interaction may evince our previously hypothesized fears that online threats such as being watched by a webcam hacker may trickle into physical threats (e.g., s/he could track me down and hurt me), which may increase intentionality to act on physical safety recommendations. Furthermore, individuals who read about a neighborhood voyeur may have responded with lower intentionality to act on physical safety tips than even control participants due to a sense of removal from the neighborhood-specific threat at hand. For one, participants may have considered such an event as unlikely in their own neighborhood or living situation (e.g., if they live in a high-rise apartment safe from prying eyes); for another, participants may have discounted the possible bodily harm a voyeur could pose to his or her victims if always separated by a windowed wall. As such, physical safety tips may have seemed irrelevant to the previously primed threat. This interaction is displayed in Figure 12.

Figure 12

Study 4: Interaction of threat type on physical safety tip intentionality



When contrasting participants in any of the four threat conditions against those in control conditions, we found no significant difference in likelihood of following online safety practices, $F(1,648) = 2.113$, $t(648) = 1.452$, $p > .05$, *ns*, $\eta_p^2 = .003$; similarly, we found no difference in likelihood of following physical safety practices, $F(1,647) = .149$, $t(647) = .385$, $p > .05$, *ns*, $\eta_p^2 < .001$. However, participants assigned to a threat condition were significantly more likely to view more pages of recommended safety practices than control participants, $F(1,648) = 6.108$, $t(648) = 2.470$, $p = .014$, $\eta_p^2 = .009$ ($M_{\text{diff}} = 0.199$, $t[503.83] = 2.684$, $p = .008$).[19]

When contrasting physical threat and online threat groups (i.e., excluding control groups from analysis), we saw no significant difference in intentionality to follow either physical ($t[437] = -1.093$, $p > .05$, *ns*) or online safety tips ($t[437] = .459$, $p > .05$, *ns*), nor

[19] Partial *df* indicates a statistical correction for unequal observed variances in this analysis.

did we see a difference in the number of safety tip pages viewed (t[437] = .209, $p > .05$, *ns*). Participants' self-reported likelihood of following physical safety tip recommendations positively predicted the number of tip pages viewed (β = .368, t[650] = 9.474, $p < .001$), but likelihood of following online safety recommendations did not (β = .023, t[650] = .583, $p > .05$, *ns*; $R^2 = .142$, F[2,650] = 53.864, $p < .001$).

We ran a regression model in which perceived physical, online, and financial threat predicted likelihood of following online safety tips and found a significant overall model ($R^2 = .036$, F[3,650] = 7.995, $p < .001$); however, only perceived online threat was a significant (positive) predictor (β = .202, t[650] = 4.190, $p < .001$). Perceived physical threat and perceived financial threat had no impact on participants' reported intentionality to follow recommended online safety practices. Stated differently, when people felt threatened online, they were more interested in protecting themselves from online dangers. When we ran the same model predicting physical safety tip intentionality (R^2 = .073, F[3,649] = 17.029, $p < .001$), we found that both perceived physical threat and perceived online threat positively predicted likelihood of following physical safety tips (physical threat: β = .159, t[649] = 3.420, $p = .001$; online threat: β = .145, t[649] = 3.076, $p = .002$). This is noteworthy, and again speaks to the possibility that online threats will more readily "bleed into" the physical world: Not only will physical threats increase a person's willingness to protect themselves in the physical world, but online threats will yield the same effect. After removing all variance explained by perceptions of physical threat, perceived online threat still accounted for a significant amount of observed variance, $R^2_{\text{change}} = .016$, $F_{\text{change}}(1,672) = 11.560$, $p = .001$. Perceived financial threat had no impact on physical safety tip intentionality (β = .005, *t*[649] = .116, *p* > .05, *ns*).

Response efficacy and self-efficacy. When examining the impact of response efficacy and self-efficacy on likelihood of following these safety practices, we found that although both positively predicted intentionality for online safety practices, self-efficacy was a stronger predictor (self-efficacy: β = .320, *t*[647] = 7.019, *p* < .001; response efficacy: β = .166, *t*[647] = 3.650, *p* < .001; R^2 = .197, *F*[2,647] = 79.404, *p* < .001). This was not the case with physical safety practice intentionality, for which response efficacy (β = .312, *t*[646] = 6.687, *p* < .001) was a stronger predictor than self-efficacy (β = .120, *t*[646] = 2.564, *p* = .011; R^2 = .159, *F*[2,646] = 61.010, *p* < .001).

The importance of self-efficacy in defending oneself against digital security threats is clear: digital literacy and other learned abilities are paramount in detecting, and protecting oneself from, cybercrime. But it is possible that self-efficacy is considered less relevant to following recommended physical safety practices for those who feel that their ability to counter physical attacks is out of their control, particularly if they do not feel that they are biologically equipped to avoid or address the threat. Stated differently, physical size, height, and even self-defense expertise may be considered important factors in self-efficacy when considering physical threats, but should be less relevant to online threats. Indeed, although physical size (β = .025, *t*[639] = .618, *p* > .05, *ns*), height (β = -.047, *t*[639] = -1.135, *p* > .05, *ns*), and self-defense expertise (β = -.057, *t*[639] = -1.577, *p* > .05, *ns*) were nonsignificant predictors of intentionality to follow online safety practices, both height (β = -.167, *t*[638] = -3.955, *p* < .001) and self-defense expertise (β = .165, *t*[638] = 4.545, *p* < .001) were significant predictors of physical safety practice intentionality, and physical size was a trending predictor (β = .063, *t*[638] = 1.536, *p* = .125, *trending*).

Interestingly, men were less likely to consider following both online (*t*[642] = 4.279, *p* < .001) and physical safety tips (*t*[594.376] = 5.417, *p* < .001), possibly because they feel less need to invest in their physical safety in day-to-day life; although men experience more physical violence than women, women report higher fears for their safety, and tend to perceive threat more readily than their male counterparts (Bailey, Caffrey, & Hartnett, 1976; Sell et al., 2009).[20] Finally, digital literacy—which we might suppose could also serve as a form of self-efficacy in defending oneself against threat—had no impact on either online (β = .023, *t*[646] = .582, *p* > .05, *ns*) or physical safety practice intentionality (β = .017, *t*[645] = .422, *p* > .05, *ns*).

Personal and situational factors

Our final exploratory aim for this fourth and final study was to examine whether, as was the case with Hypothesis 4 in Study 3, certain personal and situational factors moderate the physical-online relationship.

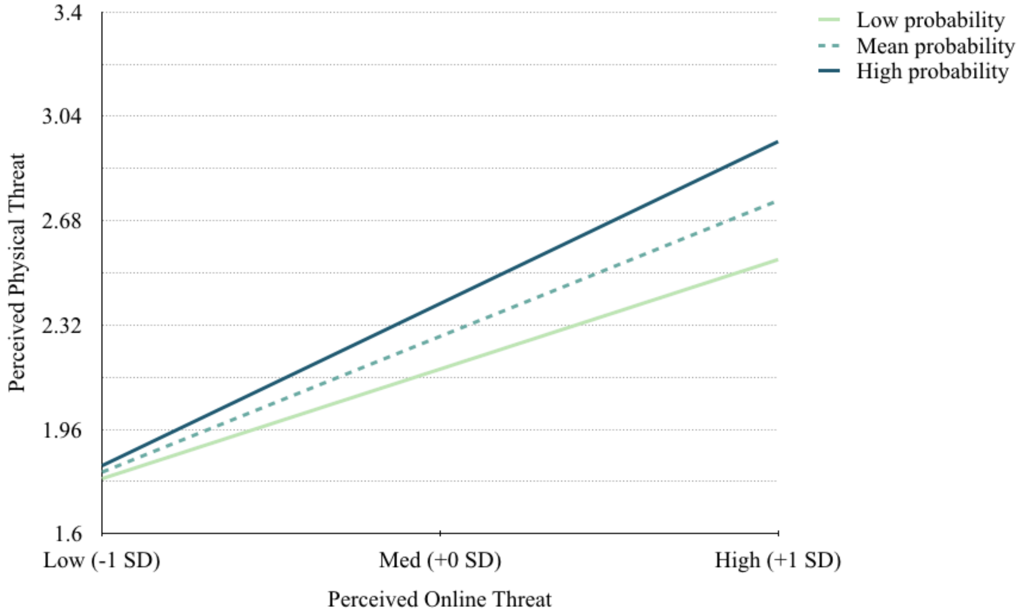
Situation-specific factors. One of our key situation-specific factors of interest was the type of threat (i.e., self-protection threat vs. resource threat), which we experimentally manipulated in Study 4. As we have reported, participants primed with resource threats displayed a stronger blurring or generalizing effect between the physical and the digital than did control participants; we did not, however, see the same pattern

[20] Although it appears that taller individuals report lower intentionality to follow online (*r*[643] = -.113, *p* = .004) or physical safety recommendations (*r*[642] = -.153, *p* < .001), this finding is confounded by gender; when holding gender constant, these relationships vanish (online: *r*[638] = .008, *p* > .05, *ns*; physical: *r*[638] = -.014, *p* > .05, *ns*).

among those assigned to self-protection threat conditions. Of our remaining situational factors—namely, perceived threat probability and perceived threat severity—only perceived threat probability played a role in the relationship between perceived physical safety and perceived online safety (R^2 = .312, F[3,431] = 65.090, p < .001).

Figure 13

Study 4: Impact of threat probability on the online-physical relationship



This interaction effect, which is displayed in Figure 13, illustrates a trend in which the relationship between perceived online threat and perceived physical threat is highest among those who perceive the threat prime at hand to be highly probable ($b_{\text{interaction}}$ = .077, t[431] = 2.435, p = .015). This speaks to an assumption that for those who consider a threat to be highly probable to occur in their lives, the need to generalize a sense of threat from one domain—here, online safety—to the other (namely, physical safety) is paramount. This moderation effect did not exist in the reverse, in which perceived physical threat predicted perceived online threat ($b_{\text{interaction}}$ = .018, t[431] =

.681, $p > .05$, *ns*). Perceived threat severity did not significantly moderate the relationship between perceived physical and online threat, $b_{\text{interaction}} = .041$, $t(431) = .873$, $p > .05$, *ns*.

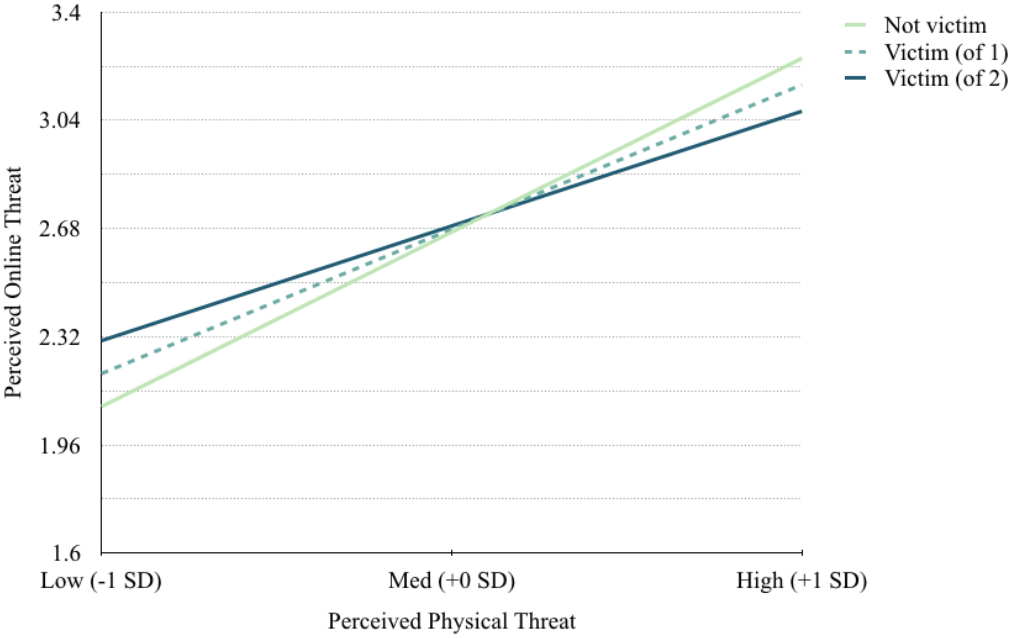
Person-specific factors. Of our person-specific factors, perceived threat susceptibility ($b_{\text{interaction}} = .021$, $t[431] = .608$, $p > .05$, *ns*),[21] past victimization experiences with cybercrime ($b_{\text{interaction}} = -.082$, $t[646] = -1.348$, $p > .05$, *ns*), physical size ($b_{\text{interaction}} = -.024$, $t[644] = -.916$, $p > .05$, *ns*), self-defense expertise ($b_{\text{interaction}} = .035$, $t[644] = 1.063$, $p > .05$, *ns*), and digital literacy ($b_{\text{interaction}} = -.060$, $t[644] = -1.382$, $p > .05$, *ns*) did not play a role on the relationship between perceived physical and perceived online safety. Instead, only past victimization experiences with physical crime, as well as participants' height, significantly moderated this relationship.

More specifically, and as is depicted in Figure 14, we observed that participants who had never been a victim of physical crime showed the strongest positive relationship between perceived physical and perceived online threat ($R^2 = .302$, $F[3,645] = 92.949$, $p < .001$; $b_{\text{interaction}} = -.147$, $t[645] = -3.528$, $p < .001$). This finding opposes the moderation effect found in Study 3, in which the reverse held true: Victims of physical crime showed the strongest relationship between perceived physical and online safety, whereas non-victims displayed a positive, but weaker, relationship.

[21] Because past victimization experiences were originally captured as an index of perceived susceptibility following the EPPM, we examined whether these measures were indeed correlated. We observed a positive relationship between perceived susceptibility and past victimization experiences with physical crime ($r[446] = .122$, $p = .01$) and cybercrime ($r[447] = .125$, $p = .008$).

Figure 14

Study 4: Impact of physical crime victimization on the physical-online relationship

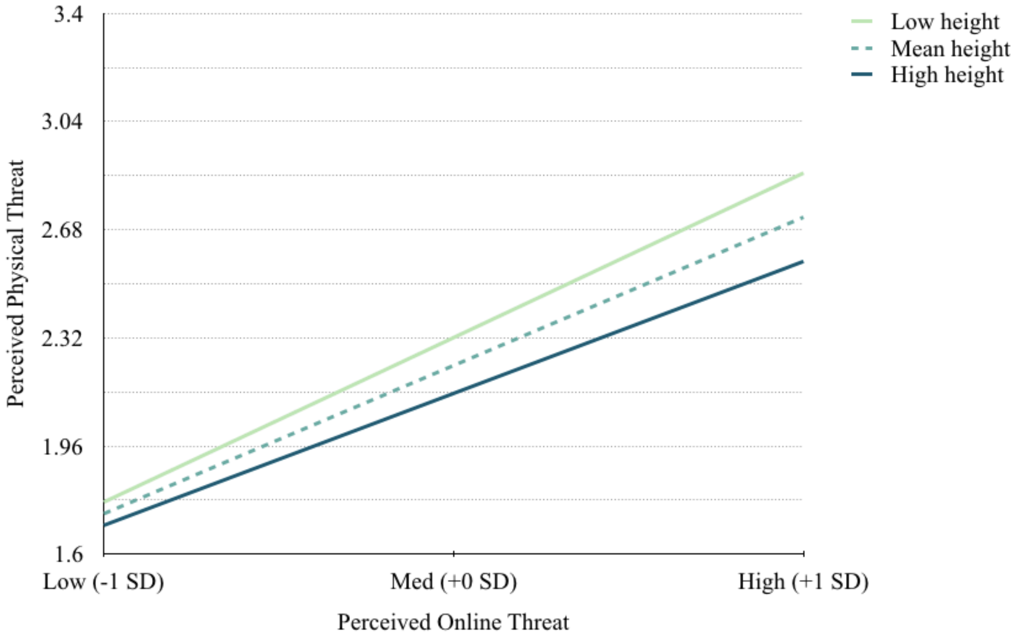


Stated differently, our Study 4 findings point to a trend whereby victims of past physical crimes perceive the lowest online threat when they perceive that they are in highly threatening physical situations (b_{high} = .413, p < .001). However, those who find themselves in safer physical conditions perceive higher levels of online threat. It is possible that victims of past physical crimes who maintain a higher sense of physical threat view the online world as a refuge or escape, or create a mental separation between the two worlds to establish a sense of safety in at least one domain in which they have not been victimized. We will discuss this possibility in more depth in the general discussion section.

We also found a marginal moderation effect of height on the online-physical relationship, in which taller participants displayed a weaker positive relationship between perceived online threat and perceived physical threat (R^2 = .301, F[3,641] = 92.164, p < .001; $b_{\text{interaction}}$ = -.015, t[641] = -1.788, p = .074, *marginal*). Just as it may be more dire for high-probability threats to generalize between the two domains (i.e., to act upon these threats, regardless of where they might appear), it is possible that participants of a shorter height feel less able to defend themselves against threats, and therefore more readily generalize or blur their perceptions of threat between domains. This interaction effect, which is illustrated in Figure 15, grows even more significant when controlling for gender in the same model ($b_{\text{interaction}}$ = -.016, t[637] = -1.852, p = .064, *marginal*; R^2_{change} = .015, F_{change}[1,640] = 9.984, p = .002).

Figure 15

Study 4: Impact of height on the online-physical relationship



Lastly, we observed a gender effect on perceptions of physical threat whereby female participants perceived higher threat than their male counterparts, regardless of assigned condition, t(642) = -3.119, p = .002. When pairing gender and height as predictors of perceived physical threat (R^2 = .023, F[3,660] = 5.071, p = .002; $b_{\text{interaction}}$ = .057, p = .022), we found that women reported higher perceptions of physical threat than their male counterparts, regardless of height (b_{female} = .021, *t*[660] = 1.227, *p* > .05, *ns*); among male participants, taller men reported lower perceptions of physical safety than their shorter counterparts (b_{male} = -.036, *t*[660] = -2.019, *p* = .04). There were no differences between male and female participants on perceived online threat (*t*[642] = -.1434, *p* > .05, *ns*) or perceived financial threat (*t*[642] = -1.178, *p* > .05, *ns*).

In summary, we found partial support for Hypothesis 4, in which several person- (i.e., physical victimization experiences, height) and situation-specific factors (i.e., threat probability) moderated the relationship between perceptions of safety in the physical and online worlds.

Summary of findings. Taken together, findings from Study 4 evince a generalization effect in which manipulations of threat in one domain "blur" into perceived threat in the opposite domain. We again establish a positive relationship between perceptions of physical and online safety regardless of randomly assigned condition, replicating our key findings from Studies 1, 2, and 3. It appears that online threats blur more readily into physical domains, possibly speaking to the concern that online dangers (such as webcam hackers and bank account fraud) will trickle into the physical world. Similarly, online threat primes are even more effective at increasing the likelihood of following recommended safety practices in the *physical* world than are physical threat primes, possibly speaking to the concern that the ramifications of online dangers (such as webcam hacking) will trickle into the physical world. And finally, the generalization between perceptions of physical threat into perceptions of online threat was stronger after being exposed to a self-protection threat prime compared with a resource threat prime, possibly underscoring the more dire nature of threats to bodily safety than those to valuable resources. Although resource threats could certainly pose danger to survival (i.e., due to a lack of monetary resources to afford food and shelter), self-protection threats should—by their very nature—pose a threat that is more direct and therefore more costly. As such, it is possible that self-protection threats encourage the generalization of perceived danger between domains to better prepare the target to act on, or avoid, the threats at hand.

This distinction between type of threat should be replicated in additional research, and potential moderators should be more closely examined. First, although self-protection threats and resource threats comprise our operationalization of crime, safety, and threat across all four studies in the present research, there are many forms of threat in the physical and online worlds; threats to information loss and reputation damage are two examples that may interact with threat domain (physical or online). Second, decades worth of FBI data defends the gendered nature of physical crime: perpetrators are more likely to be male, and—with the exception of violent crime—victims of assault and robbery are more likely to be female (FBI, 2016; Skogan & Maxfield, 1981). As such, women often perceive higher self-protection threat both on- and offline (Donnelly, 1989; Toseland, 1982). Furthermore, a wealth of evolutionary psychological research indicates that males place heavy emphasis on status to improve mating opportunities (Li & Kenrick, 2006; Li et al., 2013), which may increase males' sensitivity to resource threats compared with female participants. Future research may wish to introduce a mating prime to this study design with the intention of exploring whether mating motives underlie gender differences in the impact of status-threatening resource threat on perceptions of physical and online threat.

Finally, and as we will discuss in depth in our final discussion, our sample—although not solely comprised of college students—remained relatively homogeneous compared with the general population in the U.S. Given the high percentage of White, working class participants, we might expect differences in perceptions of safety given fundamental differences in lifestyle, location, and day-to-day experiences in the physical world. We might also expect that individuals earning money through an online survey-taking platform may be higher in digital literacy than the average U.S. citizen; indeed, even compared with predominately White, middle- and upper-class college students from Study 3, we observe a significant increase in self-reported digital literacy between the two samples, $t(1907) = 2.06$, $p = .04$. Future research should seek to replicate these findings with a more diverse sample in ethnicity, age, and socioeconomic status.

General Discussion

Summary of Findings

Studies 1 and 2. Across four studies, we found a positive relationship between physical and online safety in macro-level actuality and in individual-level perception. At the national level, objective indices of physical safety were positively related to objective measures of online safety, even when holding the confounding effects of wealth constant. We replicated these findings at the state level using measures of personal (violent crime) and resource crime (property crime, bank robberies) while controlling for state-level wealth.

Study 3. Among individuals, actual safety—as measured by zip code crime data—was a positive reflection of perceptions of physical safety; these perceptions, in turn, mapped onto perceived online safety, even when holding annual household income constant. We examined whether certain person-specific factors related to threat perception altered the strength of this positive tie between the physical and the digital, and found that past victimization of physical crime, computer security-related digital literacy, and actual physical safety from personal crime were significant moderators.

More specifically, past victims of burglary, robbery, and similar physical crimes who also perceived that they lived in highly unsafe physical environments also reported significantly lower perceptions of online safety compared with non-victims. As such, past victims displayed a higher degree of "blurring" between the online and the offline, possibly as a way to generalize perceived threat into any potentially related domain in case of attack. Individuals who perceived that they lived in physically safe environments reported significantly higher perceptions of online safety if they felt that they were digitally literate in areas of computer security (e.g., protecting their machines from viruses). This indicates that we observed the highest degree of blurring among those high in digital literacy—that is, those who would be best equipped to handle perceived threats in the online world. Just as threat appears to generalize between domains among past victims, perceived *safety* seems to generalize among those who feel particularly safe in a given domain; the moderation models of these two interactions are opposites (see Figures 2 and 3), in that past victimization differed among threatened individuals, and digital literacy differed among individuals who feel particularly safe. Finally, participants who lived in unsafe areas—specifically, zip codes high in assault, murder, and robbery—displayed our predicted positive relationship between perceived physical and online safety, whereas those in safe zip codes displayed no change in perceived online safety across two standard deviations of variation in perceived physical safety. This interaction effect fits closely with our findings from past victims, in which generalization of perceived threats may be more dire for those who expect to be threatened in the physical world.

Study 4. In our final study, a series of ANOVA suggested that our experimental manipulations of threat seem to have achieved their purpose: Physical threat primes yielded higher perceptions of physical threat, and online threat primes led to higher perceptions of online threat. As we would expect, participants assigned to control conditions reported the lowest perceived threat in physical and online domains. Although we did not find a direct impact of resource threat primes on perceived financial threat, it is possible that neither resource threat prime—namely, a series of car break-ins and fraudulent bank account transactions—instilled the same degree of threat that we might have expected. Participants in our online resource threat condition may have expected the companies implicated in these fraudulent transactions (e.g., Venmo, Paypal) to reimburse them for their losses; similarly, although we chose to prime car break-ins rather than house burglaries to remove any bodily harm component from the article, individuals in our sample may not have kept valuable items in their cars, and may have had comprehensive insurance to cover theft of car parts. On average, participants in self-protection conditions reported higher levels of threat, possibly underscoring the more dire nature of threats to bodily safety than those to valuable resources. Interestingly, it appears that when participants were primed with either physical or online threats, their perceptions of physical threat increased to similar levels, suggesting a generalized or blurred effect from online threats to perceptions of physical threats.

Actual and perceived physical safety. Contrary to findings from Study 3, we observed no direct relationship between actual physical safety and perceived physical safety; however, because our third study comprised a geographically homogeneous sample from the same university, we examined whether increased heterogeneity of geographic location might also entail increased variation in wealth. Indeed, annual household income significantly moderated the relationship between actual and perceived physical safety, such that low-income households may be more cognizant of crime if they are located in lower-income—and higher-crime—neighborhoods. Even if wealthy households exist within the same zip code, they may live in safer communities where actual crime is not apparent and cannot guide or inform perceptions of physical danger.

Threat domain and type of threat. We predicted that type of threat (self-protection vs. resource) and threat domain (physical vs. online) would play a role in the positive relationship between perceived physical and perceived online safety. First, we found that this relationship was stronger in self-protection threat conditions than in resource threat conditions, possibly because self-protection threats may be seen to pose a more direct threat to bodily safety than threats to valuable or monetary resources. Second, we found that although the physical-online relationship was consistently positive (i.e., not significantly different) between both physical and online threat conditions, this was not the case when regressing perceived online safety on perceived physical safety: Instead, we observed a significantly stronger relationship among participants in online threat conditions. This finding suggests that when online dangers are made salient, perceptions of those online threats will readily, and strongly, generalize to perceptions of physical threats, possibly speaking to the concern that online dangers will trickle into the physical world.

Downstream safety behaviors. Contrary to expectations, we found no significant differences between our six conditions in self-reported intention to follow physical or online safety practices; however, participants assigned to any of our four threat conditions were more likely to read more pages of safety practice recommendations than control participants. Again supporting the possibility that online threats may generalize more readily to physical domains, we found that participants who read about an online webcam hacker voyeur were more likely than participants who read about an in-person neighborhood voyeur to act upon physical safety recommendations, possibly out of the fear that a webcam hacker could track down victims in the physical world.

Although we found no impact of threat prime on safety practice intentionality, we did observe that perceived online threat positively predicted likelihood of following online safety tips. Interestingly, perceived online threat and perceived physical threat jointly predicted likelihood of following physical safety tips, again offering credence to our hypothesis that online threats will bleed more readily into the physical world. Furthermore, perceived online threat remained a significant predictor even after removing from the regression equation all variance explained by perceived physical threat.

We may have found no between-group differences in safety practice intentionality due to demand characteristics, in which participants form predictions about the experiment’s purpose and alter their responses to fit those interpretations. Even participants in control conditions may have formed the opinion that, after responding to batteries of perceived threat scales, they were meant to respond to safety practice recommendations in a certain way. If this is the case, future research may wish to investigate the impact of type of threat and threat domain on safety tip intentionality with distractor scales between manipulations, threat indices, and safety tips to mislead participants' interpretations about the experiment. Alternatively, future research may wish to employ a two-part study whereby participants receive a follow-up survey several days after encountering the threat prime and answering related threat scales, allowing for enough time for participants to read recommended safety practices without feeling pressured to respond a particular way. Finally, our sample comprised Turkers, who are compensated on a study-by-study basis; time spent completing one study could be spent earning more money on a following opportunity, which encourages Turkers to finish each study as quickly as possible. Because almost three-quarters of participants skipped ahead after viewing only one page of recommended safety tips, we might guess that participants chose to rush through this optional section, making at least one of our dependent variables (i.e., number of tip pages viewed) less indicative of actual likelihood of acting on these recommendations.

Personal and situational factors. As was the case in Study 3, we found that several person- and situation-specific factors related to threat perception moderated the positive relationship between perceived physical and online safety. We observed a more positive relationship—possibly indicating more blurring between the physical and the digital—when participants perceived that the threat to which they were exposed was more probable to occur in their lives. As was the case with past victimization and actual personal safety in Study 3, this interaction effect may speak to the more dire need for highly probable threats to generalize readily into any potentially relevant domain, regardless of the domain in which that threat first appeared (i.e., when collapsing across physical and online conditions). Similarly, we found that shorter participants displayed a stronger relationship between perceived online threat and perceived physical threat, again speaking to the possibility that individuals who feel more defenseless against physical crimes should more readily generalize senses of threat across domains. The directionality of this particular interaction—namely, that perceived online threat predicts perceived physical threat—is noteworthy: Shorter participants who might consider a webcam hacker a direct and physical threat to bodily safety (e.g., *he or she will track me down*) seemed more likely to generalize that threat to the physical world than their taller counterparts, regardless of gender. More broadly, female participants perceived higher physical threat than their male counterparts, even when taking height into consideration; perceived online and financial threat, on the other hand, did not differ by gender.

Contrary to findings from Study 3, we found that past victims of physical crime displayed a *weaker* relationship between perceived physical and online threat than non-victims. Following our original hypotheses, we might have expected past victims to show stronger generalizations from the physical to the digital when made to feel threatened; but instead, we found that when in a physically safe environment, past victims feel much more threatened online than do non-victims. When highly threatened offline, however, their sense of online safety remains relatively higher than their non-victim counterparts. It is possible that victims who maintain a higher sense of physical threat may view the online world as refuge or an escape; without a sense of physical safety as a buffer from fear of future victimization, these individuals may create a mental separation between the two worlds to establish a false perception of safety in at least one domain in which they have not been victimized. If this were the case, it would be possible that past victims are engaging in motivated cognition to accomplish a self-deceiving end goal: Those who fear unsafe environments based on their past experiences are motivated to construe their surroundings in a safer light, even if such construals are deceptive (Balcetis, 2008; Dunning, 2015). Without further context surrounding this particular analysis, we are left with only this conjecture, which future research may wish to explore more deeply.

Limitations and Future Directions

As has been discussed, our samples from Studies 3 and 4 comprised relatively homogeneous groups within the U.S. Study 3 investigated correlational ties between actual and perceived physical safety and perceived online safety among a predominately White, upper-middle-class group of college students living in a safe, university-dominated city. Although more geographically diverse, Study 4 examined the causal effects of threat on perceived safety among a majority young, White, working-class sample that earned money on a digitally mediated platform. We must therefore bring into question the external validity of our samples on the individual level, and along two key spectrums: First, it remains to be investigated whether older generations demonstrate the same spillover effect from perceived online threats into perceived threats in day-to-day life, particularly considering differences in amounts of time spent online and levels of comfort with cyberspace (Thomas, 2011). Second, and beyond the U.S., we must also question whether our findings generalize to societies with lower infrastructure for technology; if the cornerstone of our empirical investigation regards the blurring or overlap between the physical and the digital, this argument may break down in countries where most households lack computer access; where online banking is not only rare, but impossible; or where online identities are only half-formed for purposes of amusement, rather than necessity.

In the present research, we investigated two types of threat commonly encountered in modern-day life: threats to self-protection and threats to valuable or monetary resources. However, we know that not only are there other forms of dangers—say, to reputation or social belonging—but that the range of self-protection and resource threats extends far beyond the manipulations presented in our fourth study. Unlike cyberstalking or overt threats of bodily harm communicated through online channels, we chose to prime a form of online self-protection threat that is not directly connected to the physical world—namely, being watched through a webcam, just as someone may be watched by a voyeur outside his or her window. But even without this logical connection to physical safety, it is possible that our participants felt just as unsettled by the idea of an online perpetrator whose geographic location remained unknown: The ubiquitous nature of this threat may have underscored the sensation that there are no metaphorical doors to lock against a threat with unknown origins. As such, it remains unclear whether all online threats generalize equally readily to the physical world as did those primed in the present research. Future work may wish to explore a wider array of such threats to examine differential impacts on the generalization of threat perception between domains.

Although our individual-level indices of threat and person- and situation-specific factors demonstrated high reliability and validity in past research, we must note that our measure of digital literacy was subjective in nature, and therefore not an objective illustration of participants' actual ability to defend themselves from online threats. Research suggests that millennials, who comprise a majority of our samples for Studies 3 and 4, believe themselves to be higher in digital literacy than they actually are (Considine, Horton, & Moorman, 2009); in fact, their digital literacy skills are scarcely higher than those of the generation before them—it is only their comfort with technology that has increased.[22] As such, it remains to be seen whether actual computer security skills play a role in this generalization of threat between domains.

Although we have examined the causal nature of the tie between manipulated threat and perceived safety, we know little of the impact of time on this relationship. A two-part study examining lingering perceptions of threat and safety tip intentionality days—or even weeks—after prime exposure would add to our understanding of the longevity of these effects. Given the ubiquity of online threats such as data breaches (e.g., one third of Americans were victims of healthcare data breaches in 2015 alone; Bitglass, 2016), a large-scale longitudinal study could capture ongoing perceptions of physical and online safety and how they relate to crime-related events in mainstream news and participants' immediate communities. This same study could then serve as a time-series analysis after (a portion of) participants personally experience a physical crime- or cybercrime-related event: How does the onset of this event impact perceptions of threat, and in which domains? Does safety tip intentionality increase over time when perceptions of threats continue to linger? Is the longevity of these perceptions partially dependent on personality factors (e.g., neurotic individuals may perceive threats for a comparably

[22] Supporting this finding, a recent Pew Internet study found that only 10% of American Internet users recognize two-factor authentication, a leading security measure, when they see it—a number far lower than our observed estimates of self-reported digital literacy surrounding security methods (Collins, 2017).

longer period of time due to a heightened tendency to ruminate over negative events; McCullough et al., 2001)?

And finally, a core assumption underlying our theoretical argument is that we have observed this generalization between the physical and the digital due to unprecedented levels of interaction with the digital world. We surmise that as human "screen time" continues to increase, the blurring between threats in either domain will grow even stronger to protect oneself in any related domain. The digital world has become an added layer of existence that is growing increasingly integrated into our day-to-day, and previously unconnected, lives; as such, we might expect that people who spend more time online show stronger blurring effects, or a more positive relationship between perceptions of physical and online safety. To investigate this possibility, future research would need to sample from a wider array of human users; we might expect that college students and young Turkers show inordinately high levels of digital engagement compared with older generations, individuals from rural communities, or citizens of countries lacking in cyberinfrastructure.

This research is the first to our knowledge to expand our social psychological understanding of the relationship between physical safety and online safety in this highly digitally connected world; however, many questions remain to be answered to provide a more comprehensive illustration of this relationship across more heterogeneous samples and cultures, as it relates to objective measures of factors related to threat perception, over time following the onset of a real-life threat, and as it applies to time spent in the online world.

Contributions and Implications

Taken together, these four studies established (1) a connection between objective measures of physical and online safety on the level of nation and state; (2) the relationship between community safety and perceptions of physical safety on the individual level; and (3) the nature of this tie on the level of individual perception, both at any point in time and as a result of experimental manipulation. In addition, we established (4) the roles that personal and situational factors relevant to threat perception play in this relationship, and (5) the impact of threat perception on downstream safety practices.

Downstream safety behaviors. Regarding this fifth and more applied contribution, we found that perceptions of physical and online threat positively predict a person's intentionality to learn more about, and act upon, online safety practices. These findings were not dependent upon randomly assigned threat condition, but rather on self-reported perceptions of threat following prime exposure. Interestingly, when people feel threatened in the online world, they report higher intentionality to follow recommended safety practices both online and offline, again hinting at heightened blurring from the digital to the physical. As such, organizations such as IC3 may consider immediately following up on reported cyberattacks with suggested safety practices to increase attention to, and proactive steps toward, securing a safer cyberspace; in addition, this government-supported site may serve as an optimal platform for communicating ways to stay safe offline following cybercrime incidents with a possibly physical component (e.g., cyberstalking).

Furthermore, we observed that participants who live in dangerous zip codes (Study 3)—or, alternatively, low-income households in dangerous zip codes (Study 4)—perceive higher levels of physical threat, and that these perceptions positively inform perceived online threat. E-mail clients and social networking sites with access to users' physical locations should consider new segmentation strategies to increase awareness—and use—of settings that will increase account security. If a user's zip code is associated with physical threat, and because these findings suggest that these threats generalize into the online domain, we might expect users to want to proactively avoid those threats in cyberspace, making them more likely to seek out—and act upon—customized safety controls on their account. As such, users from particular physical settings may benefit from a tailored security experience while online, including uniquely sorted lists of proffered security controls, walkthroughs of new safety measures, and periodic "check-ups" of the security of users' accounts.

The digital informs the physical. Most notably, the present research has established that perceptions of online threat generalize more strongly into perceived threat in the physical world than is the reverse, in which physical threat informs perceived online safety. First, when participants were primed with either physical or online threats, their perceptions of physical threat increased to similar—that is, not statistically different—levels. Second, we observed a significantly stronger relationship between perceived online threat and perceived physical threat among participants in online threat conditions. Third, participants who read about an online webcam hacker voyeur were more likely than participants who read about a physical, neighborhood voyeur to act upon physical safety recommendations; and fourth, even after removing all variance explained by perceived physical threat, perceptions of online threat significantly predicted physical safety tip intentionality.

This finding is noteworthy because, taken together, this research establishes a connection between the physical and the digital in an era of unprecedented engagement with the online world. Every day, the average American adult spends more time gazing at a screen into an intangible world than they do interacting with the physical milieu around them (Nielsen, 2016). It would be imprudent to assume that our basic human instincts cannot, and should not, change to meet the new environments in which we find ourselves: Our sense of safety and security that has historically stemmed from the creation of barriers between self and danger must now incorporate new methods of self-protection against still-evolving threats that can occur anywhere, at any time. Although we have demonstrated that—even beyond the confounding effects of wealth—societies that are physically safe also tend to be safe in the online world (i.e., implying a relationship from the physical to the digital), our findings suggest that among individual-level perceptions, it is the online that informs the offline—the digital that guides the physical.

These fears of an unknown, unseen threat in cyberspace appear to permeate our sense of security in day-to-day life, leading to a blurring effect between perceived threats in the online and offline worlds. But most importantly, it would seem that we—as human users—are quite aware of the potential for online threats to pose downstream physical consequences to bodily or resource-related safety; furthermore, this awareness is only heightened among individuals who may perceive chronically higher levels of threat due to personal and situational factors such as community safety, physical size, past victimization experiences, ability to defend oneself online, and the probability that the threat will occur at all. In the absence of a metaphorical lock and key, this generalization of threat between domains may function as a strategy to prepare oneself for future dangers wherever they might appear; and indeed, perceived threat in either world appears to positively influence a person's drive to act on recommended safety practices.

Decades of past research in cyberpsychology and human-computer interaction has supported a strong distinction between the online and offline worlds in self-presentation, interpersonal perception, and control over the time and pace of interaction with external stimuli (Bodford, in press; Bodford & Kwan, in press; McKenna & Bargh, 2000). As such, human attitudes and behaviors have been shown to differ substantially between the two spheres. In the offline world, we are bound to physical forms and geographic situations that remain relatively stagnant. But online, we can assume whatever identities we wish without consideration of temporal or spatial bounds; to adopt two entirely separate personas is not only possible, but easy. As such, empirical work has conceptualized cyberspace as a separate dimension—a layer of interaction that can be added to the physical world, but that can just as easily be removed from it.

However, the present work suggests that these two worlds are not as distinct as past literature—and indeed, popular culture—would have us believe: Instead, it appears that our perceptions of the world around us are shared between domains, and that when made to feel frightened, our psychological processes bleed from one world to the other. Across four studies, we observed consistently positive ties between safety in the physical and online worlds across countries ($|r[155]| = .308$, $p < .001$) and U.S. states ($r[48] = .395$, $p = .005$) after controlling for the confounding effects of wealth to afford reliable infrastructures for societal safety. We observed a smaller correlation ($r[1249] = .130$, $p <$

.001) when gauging this correlational tie on the level of individual perceptions, signaling that even when measured in the absence of manipulation, psychological processes are not independent between the two domains. But most notably, the dividing line between these perceptions becomes least rigid—that is, most blurred—in the face of threat (*r*[654] = .538, $p < .001$), pointing to a collapsing of the boundary between the physical and digital when threat is made salient through experimental manipulation. Stated differently, when we are made to feel afraid, these two worlds seem to collapse even further.

In social domains where self-presentation, interpersonal perception, and mediated communication are concerned, it is certainly possible that we take for granted the physically removed nature of the digital world, seeking ways to hide in the shadows of this new medium. But in the domain of fear, our work seems to point to a feeling that there is nowhere to hide—that a threat in one world will bleed into the other. These findings beg the question of the exact nature of the consequences of this perceived collapsing between the two worlds. If this generalization of threat is an adaptive strategy, one might hope to see an increase in online safety precautions, wariness of novel sites or contacts, and withholding of personal information from unknown entities; whether this is indeed the case, however, is another matter entirely. It also remains to be seen if a person's extent of online engagement—the time spent in cyberspace, the resources invested in an intangible world—heightens this generalization of threat, and to what end. As younger generations invest more time and energy into a space accompanied by unknown and ever-advancing dangers, we must work to champion awareness of cybercrime and safety practices while emphasizing the blurred boundaries between the online and the offline. On this note, we close with a quote from Lucas's (2015, pp. xxi-xxiii) *Cyberphobia*:

> Our sense of security in the wider world outside our homes and workplaces is instinctive. We know that some neighborhoods are safer than others, that some times of day require special precautions. Like many generations before us, our security in real life depends on locks and keys. Once we venture online, all that vanishes. Our real-world senses are constrained. It is a simulacrum of the real world, but a deceptive one.

REFERENCES

Austin, D. M., Furr, L. A., & Spine, M. (2002). The effects of neighborhood conditions on perceptions of safety. *Journal of Criminal Justice*, *30*(5), 417-427.

Ayres, J., & Hopf, T. (1992). Visualization: Reducing speech anxiety and enhancing performance. *Communication Reports*, *5*(1), 1-10.

Ayres, J., & Hopf, T. S. (1990). The long-term effect of visualization in the classroom: A brief research report. *Communication Education*, *39*(1), 75-78.

Ayres, J., & Hopf, T. S. (1985). Visualization: A means of reducing speech anxiety. *Communication Education*, *34*(4), 318-323.

Baba, Y. & Austin, D. M. (1989). Neighborhood environmental satisfaction, victimization, and social participation as determinants of perceived neighborhood safety. *Environment and Behavior*, *21*(6), 763-780.

Balcetis, E. (2008). Where the motivation resides and self-deception hides: How motivated cognition accomplishes self-deception. *Social and Personality Psychology Compass*, *2*(1), 361-381.

Bailey, K. G., Caffrey, J. V., & Hartnett, J. J. (1976). Body size as implied threat: Effects on personal space and person perception. *Perceptual & Motor Skills*, *43*(1), 223-230.

Banks, R. (2014). Dialogues: Trust in Design. In Harper, R. H. R. (Ed.), *Trust, Computing, and Society* (pp. 250-271). New York, NY: Cambridge University Press.

Becker, D. V., Kenrick, D. T., Neuberg, S. L., Blackwell, K. C., & Smith, D. M. (2007). The confounded nature of angry men and happy women. *Journal of Personality and Social Psychology*, *92*, 179-190.

Bitglass (2016, January 27). One in three Americans affected by healthcare breaches. *Bitglass: Total Data Protection*. Retrieved from http://www.bitglass.com/press-releases/bitglass-report-one-in-three-americans-affected-by-healthcare-breaches-in-2015

Bodford, J. E. (2017, in press). Loneliness in modern life. In T. K. Shackelford & V. A. Weekes-Shackelford (Eds.) *The Encyclopedia of Evolutionary Psychological Science*. New York, NY: Springer Publishing.

Bodford, J. E. & Kwan, V. S. Y. (2017, in press). A Game Theoretical Approach to Hacktivism: Is Attack Likelihood a Product of Risks and Payoffs?

Cyberpsychology, Behavior, and Social Networking: Special Issue on Cybercrime.

Bodford, J. E., Kwan, V. S. Y., & Sobota, D. S. (2017, in press). Fatal attractions: Attachment to smartphones predicts anthropomorphic beliefs and dangerous behaviors. *Cyberpsychology, Behavior, and Social Networking*.

Bryant, K., & Campbell, J. (2006). User behaviours associated with password security and management. *Australasian Journal of Information Systems*, *14*(1).

Chong, Y. M. G., Teng, K. Z. S., Siew, S. C. A., & Skoric, M. M. (2012). Cultivation effects of video games: a longer-term experimental test of first-and second-order effects. *Journal of Social and Clinical Psychology*, *31*(9), 952.

Cluley, G. (2015, October). Webcam hacker spends up to 12 hours a day watching his victims. *WeLiveSecurity*. Retrieved from http://www.welivesecurity.com/2015/10/09/webcam-hacker/

Collins, K. (2017, March). Most American internet users have no idea how to protect their accounts. *Quartz*. Retrieved from https://qz.com/938621/pew-survey-finds-that-most-american-adults-cant-identify-two-factor-authentication/

Connor-Smith, J. K., Henning, K., Moore, S., & Holdford, R. (2011). Risk assessments by female victims of intimate partner violence: Predictors of risk perceptions and comparison to an actuarial measure. *Journal of Interpersonal Violence*, *26*(12), 2517-2550.

Considine, D., Horton, J., & Moorman, G. (2009). Teaching and reaching the millennial generation through media literacy. *Journal of Adolescent & Adult Literacy*, *52*(6), 471-481.

Daykin, T. (2017, January). Supermarket coming to near south side. *USA Today*. Retrieved from http://www.usatoday.com/story/money/real-estate/commercial/2017/01/23/supermarket-coming-near-south-side/96960426/

DeVellis, R. F. (2012). *Scale development: Theory and applications* (pp. 109-110). Los Angeles: Sage Publications.

Donnelly, P. G. (1989). Individual and neighborhood influences on fear of crime. *Sociological Focus*, 69-85.

Dunning, D. (2015). Motivated cognition in self and social thought. In M. Mikulincer & P. R. Shaver (Eds.) *APA Handbook of Personality and Social Psychology: Vol 1. Attitudes and Social Cognition* (pp. 777-803). Washington, DC: American Psychological Association.

Federal Bureau of Investigation (2016). *Crime in the United States, Table 4*. Retrieved from https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/tables/table-4

Federal Bureau of Investigation (2015). *Bank Crime Statistics*. Retrieved from https://www.fbi.gov/file-repository/stats-services-publications-bank-crime-statistics-2015-bank-crime-statistics-2015/view

Feldman, P. J. & Steptoe, A. (2004). How neighborhoods and physical functioning are related: the roles of neighborhood socioeconomic status, perceived neighborhood strain, and individual health risk factors. *Annals of Behavioral Medicine*, *27*(2), 91-99.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Industrial Management & Data Systems*, *106*(5), 601-620.

Fogg, B. J. (2003, April). Prominence-interpretation theory: Explaining how people assess credibility online. In *CHI'03 extended abstracts on human factors in computing systems* (pp. 722-723). ACM.

Foster, J. M. & Hagedorn, W. B. (2014). A Qualitative exploration of fear and safety with child victims of sexual abuse. *Journal of Mental Health Counseling*, *36*(3), 243-262.

Friedland, N. (1982). A Note on tax evasion as a function of the quality of information about the magnitude and credibility of threatened fines: Some preliminary research. *Journal of Applied Social Psychology*, *12*(1), 54-59.

Fuller, R. (1984). A Conceptualization of driving behavior as threat avoidance. *Ergonomics*, *27*(11), 1139-1155.

Garofalo, J. (1979). Victimization and the fear of crime. *Journal of Research in Crime and Delinquency*, *16*(1), 80-97.

Gerrold, D. (1972). *When HARLIE was One*. New York, NY: Bantam Spectra.

Gottfredson, G. (1984). *The effective school battery*. Odessa, FL: Psychological Assessment Resources.

Grabner-Kräuter, S. & Kaluscha, E. A. (2003). Empirical research in on-line trust: A Review and critical assessment. *International Journal of Human-Computer Studies*, *58*(6), 783-812.

Greenwood, S., Perrin, A., & Duggan, M. (2016, November). Social media update 2016. *Pew Research Center: Internet, Science, & Tech*. Retrieved from http://www.pewinternet.org/2016/11/11/social-media-update-2016/

Griffin, M. A., & Neal, A. (2000). Perceptions of safety at work: a framework for linking safety climate to safety performance, knowledge, and motivation. *Journal of Occupational Health Psychology*, *5*(3), 347.

Griskevicius, V., Goldstein, N. J., Mortensen, C. R., Cialdini, R. B., & Kenrick, D. T. (2006). Going along versus going alone: When fundamental motives facilitate strategic (non)conformity. *Journal of Personality and Social Psychology*, *91*, 281-294.

Griskevicius, V., Goldstein, N. J., Mortensen, C. R., Sundie, J. M., Cialdini, R. B., & Kenrick, D. T. (2009). Fear and loving in Las Vegas: Evolution, emotion, and persuasion. *Journal of Marketing Research*, *46*, 384-395.

Hargittai, E. (2009). An update on survey measures of web-oriented digital literacy. *Social Science Computer Review*, *27*(1), 130-137.

Hattem, J. (2014, May). Is Estonia leading the way for cybersecurity? *The Hill*. Retrieved from http://thehill.com/policy/technology/207406-is-estonia-leading-the-way-for-cybersecuirty

Hayes, A. F., & Matthes, J. (2009). Computational procedures for probing interactions in OLS and logistic regression: SPSS and SAS implementations. *Behavior Research Methods*, *41*(3), 924-936.

Hayes, B. E., Perander, J., Smecko, T., & Trask, J. (1998). Measuring perceptions of workplace safety: Development and validation of the work safety scale. *Journal of Safety Research*, *29*(3), 145-161.

Holmes, T. E. (2015, September). Credit card fraud and ID theft statistics. *NASDAQ*. Retrieved from http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388

Hullett, C. R., & Witte, K. (2001). Predicting intercultural adaptation and isolation: Using the extended parallel process model to test anxiety/uncertainty management theory. *International Journal of Intercultural Relations*, *25*(2), 125-139.

Idsø, E. S. & Jakobsen, M. Ø. (2000). *Objekt- og informasjonssikkerhet: Metode for risiko- og sårbarhetsanalyse*. Norwegian University of Technology & Science (NTNU): Institutt for produksjons- og kvalitetsteknikk.

Ilves, T. H. (2013, April). Cybersecurity: A view from the front. *The New York Times: Global Opinion*. Retrieved from https://nyti.ms/2jBGMSh

International Telecommunication Union (2015). Global cybersecurity index & cyberwellness profiles [White paper]. Retrieved from http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

Internet Crime Complaint Center (2015). 2015 Internet crime report [White paper]. *Federal Bureau of Investigation Internet Crime Complaint Center (IC3)*. Retrieved from https://pdf.ic3.gov/2015_IC3Report.pdf

Janson, P. & Ryder, L. K. (1983). Crime and the elderly: The relationship between risk and fear. *The Gerontologist*, *23*(2), 207-212.

Juvonen, J., Nishina, A., & Graham, S. (2006). Ethnic diversity and perceptions of safety in urban middle schools. *Psychological Science*, *17*(5), 393-400.

Kenrick, D. T., Griskevicius, V., Neuberg, S. L., & Schaller, M. (2010). Renovating the pyramid of needs: Contemporary extensions built upon ancient foundations. *Perspectives on Psychological Science*, *5*(3), 292-314.

Kinstler, L. (2015, January). Here's what the us could learn from Estonia about cybersecurity. *Nextgov*. Retrieved from http://www.nextgov.com/cybersecurity/2015/01/heres-what-us-could-learn-estonia-about-cybersecurity/103959/

Kwan, V. S. Y. & Bodford, J. E. (2015). The Psychological impacts of cyberlife engagement. In R. A. Scott & S. M. Kosslyn (Eds.) *Emerging Trends in the Social and Behavioral Sciences*. Thousand Oaks, CA: Wiley Publications.

Lallmahamood, M. (2007). An Examination of individual's perceived security and privacy of the Internet in Malaysia and the influence of this on their intention to use e-commerce: Using an extension of the Technology Acceptance Model. *The Journal of Internet Banking and Commerce*, *12*(3), 1-26.

Li, J. Y., Kenrick, D. T., Griskevicius, V., & Neuberg, S. L. (2012). Economic decision biases and fundamental motivations: How mating and self-protection alter loss aversion. *Journal of Personality and Social Psychology*, *102*(3), 550-561.

Li, N. P., & Kenrick, D. T. (2006). Sex similarities and differences in preferences for short-term mates: What, whether, and why. *Journal of Personality and Social Psychology*, *90*(3), 468-489.

Li, N. P., Yong, J. C., Tov, W., Sng, O., Fletcher, G. J. O., Valentine, K. A., . . . Balliet, D. (2013). Mate preferences do predict attraction and choices in the early stages of mate selection. *Journal of Personality and Social Psychology*, *105*(5), 757-776.

Lucas, E. (2015). *Cyberphobia: Identity, trust, security and the Internet*. London: Bloomsbury Publishing.

Maner, J. K., Kenrick, D. T., Neuberg, S. L., Becker, D. V., Robertson, T., Hofer, B., Delton, A. W., Butner, J., & Schaller, M. (2005). Functional projection: How fundamental social motives can bias interpersonal perception. *Journal of Personality and Social Psychology*, *88*, 63–78.

Marjanovic, Z., Greenglass, E. R., Fiksenbaum, L., & Bell, C. M. (2013). Psychometric evaluation of the Financial Threat Scale (FTS) in the context of the great recession. *Journal of Economic Psychology*, *36*, 1-10.

Maslow, A. H. (1943). A Theory of human motivation. *Psychological Review*, *50*(4), 370-396.

McCullough, M. E., Bellah, C. G., Kilpatrick, S. D., & Johnson, J. L. (2001). Vengefulness: Relationships with forgiveness, rumination, well-being, and the Big Five. *Personality and Social Psychology Bulletin*, *27*(5), 601-610.

McDaniel, P. (1993). Self-defense training and women's fear of crime. *Women's Studies International Forum*, *16*(1), 37-45.

McKenna, K. Y. A. & Bargh, J. A. (2000). Plan 9 from cyberspace: The Implications of the internet for personality and social psychology. *Personality and Social Psychology Review*, *4*(1), 57-75.

Moreau, E. (2016, October). The Top 25 social networking sites people are using: All the places people are sharing and consuming information online. *Lifewire*. Retrieved from https://www.lifewire.com/top-social-networking-sites-people-are-using-3486554

Move, Inc. (2017). *City Profiles: Research City Data*. Retrieved from http://www.moving.com/real-estate/city-profile/

Neff, J. (2003). Spam research reveals disgust with pop-up ads. *Advertising Age*, *74*(44).

Neuberg, S. L., Kenrick, D. T., & Schaller, M. (2011). Human threat management systems: Self-protection and disease-avoidance. *Neuroscience & Biobehavioral Reviews*, *35*, 1042–1051.

Nielsen (2016). The Total audience report: Q1 2016. *The Nielsen Company*. Retrieved from http://www.nielsen.com/us/en/insights/reports/2016/the-total-audience-report-q1-2016.html

O'Cass, A., & Fenech, T. (2003). Web retailing adoption: exploring the nature of Internet users Web retailing behaviour. *Journal of Retailing and Consumer Services*, *10*(2), 81-94.

Ou, C. X. & Sia, C. L. (2009). To trust or to distrust, that is the question: Investigating the trust-distrust paradox. *Communications of the ACM*, *52*(5), 135-139.

Pascual, A. (2014). 2014 Identity fraud report: Card data breaches and inadequate consumer password habits fuel disturbing fraud trends. *Javelin*. Retrieved from https://www.javelinstrategy.com/coverage-area/2014-identity-fraud-report-card-data-breaches-and-inadequate-consumer-password-habits

Pearsall, J. & Hanks, P. (Eds.) (2001). *The New Oxford Dictionary of English*. Oxford, England: Oxford University Press.

Perkins, D. D., Brown, B. B., & Taylor, R. B. (1996). The ecology of empowerment: Predicting participation in community organizations. *Journal of Social Issues*, *52*(1), 85-110.

Phillips, D. & Rudestam, K. E. (1995). Effect of nonviolent self-defense training on male psychiatric staff members' aggression and fear. *Psychiatric Services*, *46*(2), 164-168.

Rapee, R. M. (1997). Perceived threat and perceived control as predictors of the degree of fear in physical and social situations. *Journal of Anxiety Disorders*, *11*(5), 455-461.

Robinson, C. D., Tomek, S., & Schumacker, R. E. (2013). Tests of moderation effects: Difference in simple slopes versus the interaction term. *Multiple Linear Regression Viewpoints*, *39*(1), 16-24.

Rogers, R. W. & Mewborn, R. C. (1976). Fear appeals and attitude change: Effects of a threat's noxiousness, probability of occurrence, and the efficacy of coping responses. *Journal of Personality and Social Psychology*, *34*(1), 54-61.

Romero, N. (2017, February). Shoreline neighbors vigilant after 6 burglaries in two days. *Q13 Fox*. Retrieved from http://q13fox.com/2017/02/10/neighbors-vigilant-after-six-shoreline-burglaries-in-two-days/

Schaller, M., Park, J. H., & Mueller, A. (2003). Fear of the dark: Interactive effects of beliefs about danger and ambient darkness on ethnic stereotypes. *Personality and Social Psychology Bulletin*, *29*, 637-649.

Sell, A., Cosmides, L., Tooby, J., Sznycer, D., von Rueden, C., & Gurven, M. (2009). Human adaptations for the visual assessment of strength and fighting ability from the body and face. *Proceedings of the Royal Society B: Biological Sciences*, *276*(1656), 575-584.

Sillence, E., Briggs, P., Fishwick, L., & Harris, P. (2004, April). Trust and mistrust of online health sites. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 663-670). ACM.

Simsek, H., Doganay, S., Budak, R., & Ucku, R. (2014). Relationship of socioeconomic status with health behaviors and self-perceived health in the elderly: A community-based study, turkey. *Geriatrics & Gerontology International*, *14*(4), 960-968.

Skogan, W. G., & Maxfield, M. G. (1981). *Coping with crime: Individual and neighborhood reactions* (Report No. NCJ 078899). National Criminal Justice Reference Service. Washington, D.C.: National Institute of Justice.

Thomas, M. (Ed.). (2011). *Deconstructing digital natives: Young people, technology, and the new literacies*. Milton Park, UK: Taylor & Francis.

Thompson, C. Y., Bankston, W. B., & St. Pierre, R. L. (1992). Parity and disparity among three measures of fear of crime: A research note. *Deviant Behavior*, *13*(4), 373-389.

Toseland, R. W. (1982). Fear of crime: Who is most vulnerable? *Journal of Criminal Justice*, *10*(3), 199-209.

U.S. Department of Commerce Bureau of Economic Analysis (2015). *National Income and Product Accounts: Gross Domestic Product*. Retrieved from https://www.bea.gov/newsreleases/national/gdp/gdpnewsrelease.htm

Uniform Crime Reporting Statistics (2017). *Reported crime by locality (city, county), state, and nation*. Division of the U.S. Department of Justice, Federal Bureau of Investigation. Retrieved from https://www.ucrdatatool.gov/Search/Crime/Crime.cfm

Veblen, T. (1994). *The Theory of the leisure class* [Reprint edition]. Mineola, NY: Dover Publications.

West, R. (2008). The Psychology of Security. *Communications of the ACM*, *51*(4), 34–41.

White, A. E. (2014). *The Effectiveness of reciprocity appeals in economic booms and busts* (Order No. 3619602). Available from Dissertations & Theses at Arizona State University; ProQuest Dissertations & Theses Global. (1535787291).

White, A. E., Kenrick, D. T., Neel, R., & Neuberg, S. L. (2013). From the bedroom to the budget deficit: Mate competition changes men's attitudes toward economic redistribution. *Journal of Personality and Social Psychology*, *105*(6), 924-940.

White, A. E., Kenrick, D. T., & Neuberg, S. L. (2013). Beauty at the ballot box: Disease threats predict preferences for physically attractive leaders. *Psychological Science*, *24*(12), 2429-2436.

Witte, K. (1998). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. (1998). In P. A. Andersen & L. K. Guerrero (Eds.) *Handbook of communication and emotion: Research, theory, applications, and contexts* (pp. 423-450). San Diego, CA: Academic Press.

Witte, K., McKeon, J., Cameron, K., & Berkowitz, J. (1995). *The Risk behavior diagnosis scale: A Health educator's tool* [Manual]. Michigan State University. East Lansing, MI.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs*, *61*(2), 113-134.

Wolff, N. & Shi, J. (2009). Feelings of safety inside prison among male inmates with different victimization experiences. *Violence and Victims*, *24*(6), 800-816.

Young, S. G., Slepian, M. L., & Sacco, D. F. (2015). Sensitivity to perceived facial trustworthiness is increased by activating self-protection motives. *Social Psychological and Personality Science*, *6*(6), 607-613.

Yu, B. & Singh, M. P. (2002). Distributed reputation management for electronic commerce. *Computational Intelligence*, *18*(4), 1-16.

APPENDIX A

STUDY 3 MATERIALS

The questions below ask about the neighborhood where your *permanent home* is located. Please indicate how much you agree or disagree with each statement.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
In the neighborhood where I live, people really do not need to lock their doors when they leave their homes for a short period of time.							
People who live in my neighborhood have to worry about someone breaking into their home to steal things.							
People in my neighborhood can walk around at night without fear of being attacked or bothered by strangers.							
People in my neighborhood can leave their personal property outside and unattended without fearing that it will be damaged or stolen.							

Is there any area within two blocks of your home where you would be worried about walking alone at night?

❍ Yes
❍ No

If there any area within two blocks of your home where you would be worried about walking at night, even if someone else were with you?

❍ Yes
❍ No

Have you or a household member ever been a victim of **theft or burglary** (either when you were at home or away from home)?

❍ Yes
❍ No

Have you or a household member ever been a victim of **assault/battery, robbery, or murder**?

❍ Yes
❍ No

Have you or a household member ever been the victim of **identity theft**?

❍ Yes
❍ No

Have you or a household member ever been the victim of **cyberbullying or cyberstalking**?

○ Yes
○ No

Which of the following websites do you use or visit *at least once a month*? (Select all that apply.)

□ Facebook
□ Google+
□ Instagram
□ LinkedIn
□ Snapchat

Thinking *only of the websites you indicated above*, please indicate how much you agree or disagree with each of the following statements.

If you only used *one* of the above websites, please answer these questions with only that website in mind.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
These websites have enough security measures to protect my personal information.							
When I post information on these websites, I am sure that it will not be intercepted or obtained by unauthorized third parties.							
I am confident that the private information I provide these websites will be secured.							
I think these websites are very concerned about the security of any transactions.							
I feel secure using these websites.							
I feel safe when I provide personal information to these websites.							

In terms of your Internet skills (e.g., changing privacy or security settings in your browser), do you consider yourself to be...

○ Not at all skilled
○ Not very skilled
○ Fairly skilled
○ Very skilled
○ Expert

In terms of your computer skills (e.g., securing your computer against viruses or safety threats), do you consider yourself to be...

○ Not at all skilled
○ Not very skilled
○ Fairly skilled
○ Very skilled
○ Expert

Compared with the average person of your sex (male/female), how would you describe your physical size?

○ Much smaller than average
○ Smaller than average
○ A little smaller than average
○ About average
○ A little larger than average
○ Larger than average
○ Much larger than average

What is your height?

___ feet
___ inches

How much experience do you have with self-defense (e.g., taekwondo, karate, aikido)?

○ None at all
○ A little
○ A moderate amount
○ A lot
○ A great deal

What is your sex?

○ Male
○ Female
○ Other: _______

What is your age?

____

Which best describes your race or ethnicity?

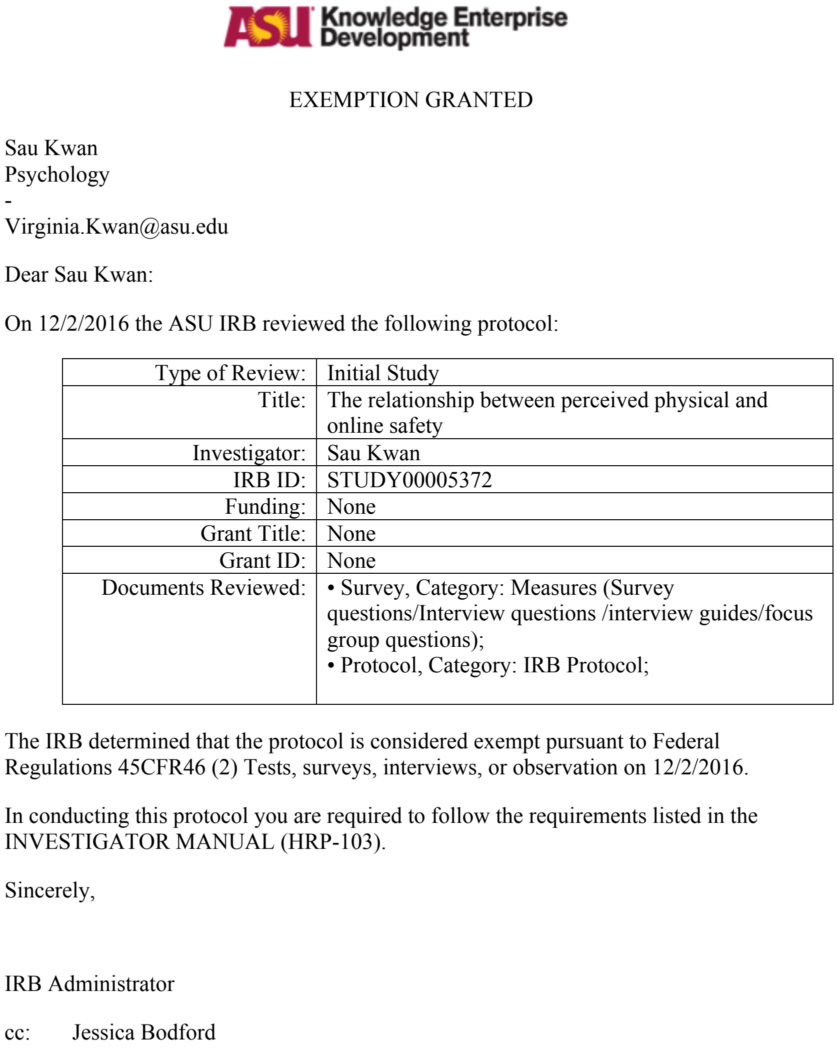
❍ White/Caucasian
❍ Black/African-American
❍ Hispanic/Latino
❍ Native American
❍ East Asian (e.g., China, Japan)
❍ South Asian (e.g., India)
❍ Southeast Asian (e.g., Indonesia)
❍ Asian-American
❍ Middle Eastern
❍ Arab/Arab-American
❍ Other: _______

In terms of income, how would you describe your family's socio-economic status?
❍ Upper class
❍ Upper-middle class
❍ Middle class
❍ Lower-middle class
❍ Working class
❍ Other: _______

What is the 5-digit zip code of your permanent home?
____

APPENDIX B

STUDY 3 IRB APPROVAL



ASU Knowledge Enterprise Development

EXEMPTION GRANTED

Sau Kwan
Psychology
-
Virginia.Kwan@asu.edu

Dear Sau Kwan:

On 12/2/2016 the ASU IRB reviewed the following protocol:

Type of Review:	Initial Study
Title:	The relationship between perceived physical and online safety
Investigator:	Sau Kwan
IRB ID:	STUDY00005372
Funding:	None
Grant Title:	None
Grant ID:	None
Documents Reviewed:	• Survey, Category: Measures (Survey questions/Interview questions /interview guides/focus group questions); • Protocol, Category: IRB Protocol;

The IRB determined that the protocol is considered exempt pursuant to Federal Regulations 45CFR46 (2) Tests, surveys, interviews, or observation on 12/2/2016.

In conducting this protocol you are required to follow the requirements listed in the INVESTIGATOR MANUAL (HRP-103).

Sincerely,

IRB Administrator

cc: Jessica Bodford

APPENDIX C

STUDY 4 MATERIALS

We're interested in the impact of information processing on decision-making strategies. **PLEASE READ THE FOLLOWING ARTICLE CAREFULLY.** When you've finished reading, ***we will ask comprehension questions about the article***. We will observe the amount of time you spend on the page.

{CONDITION = PHYSICAL}

Imagine that the following article describes events happening **in your community**.

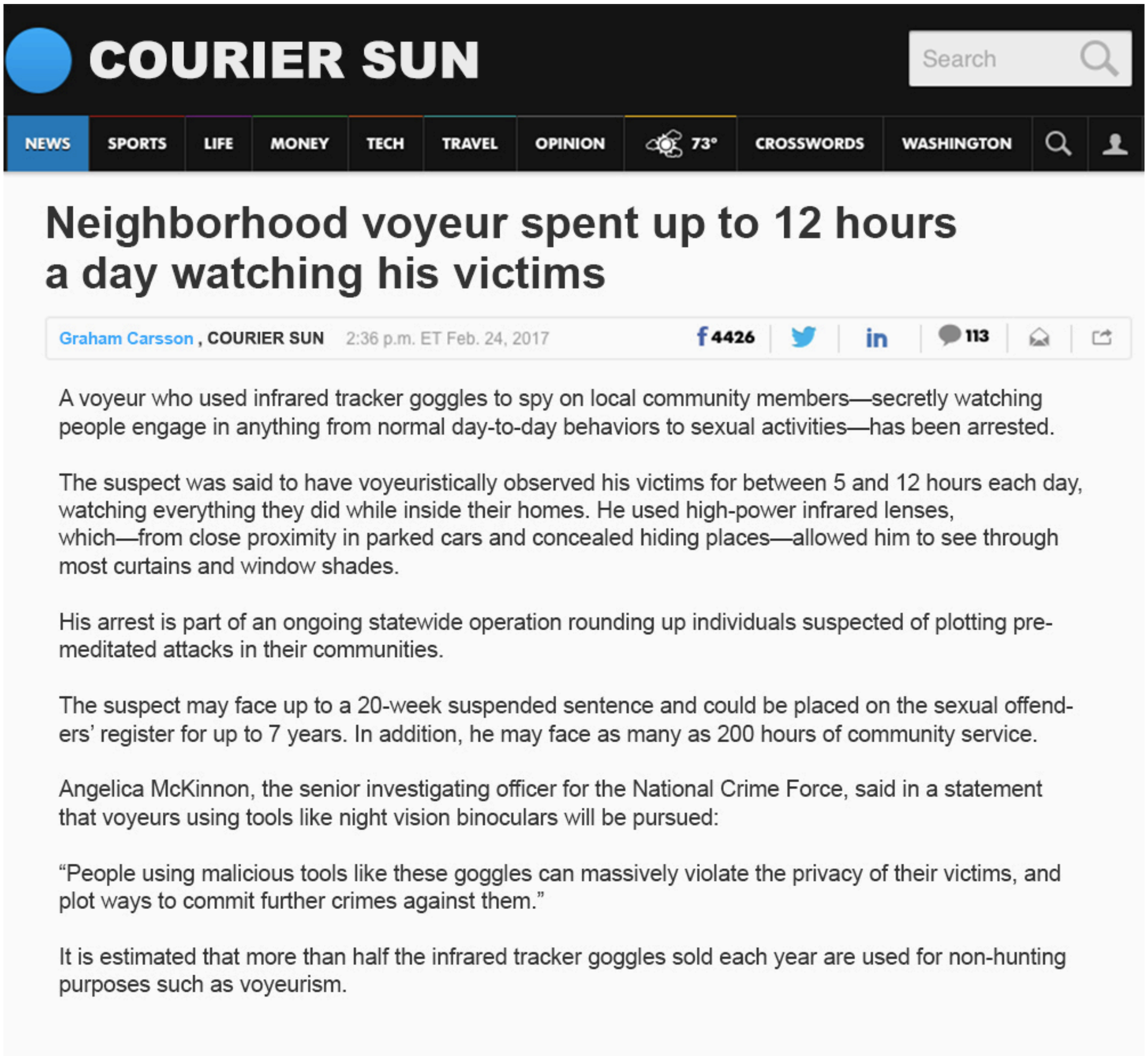
{*Timing data: First Click, Last Click, Page Submit, Click Count*}

{CONDITION = ONLINE}

Imagine that the following article describes events that actually happened.

{*Timing data: First Click, Last Click, Page Submit, Click Count*}

{Physical, Self-Protection Threat}



Neighborhood voyeur spent up to 12 hours a day watching his victims

Graham Carsson , COURIER SUN 2:36 p.m. ET Feb. 24, 2017

A voyeur who used infrared tracker goggles to spy on local community members—secretly watching people engage in anything from normal day-to-day behaviors to sexual activities—has been arrested.

The suspect was said to have voyeuristically observed his victims for between 5 and 12 hours each day, watching everything they did while inside their homes. He used high-power infrared lenses, which—from close proximity in parked cars and concealed hiding places—allowed him to see through most curtains and window shades.

His arrest is part of an ongoing statewide operation rounding up individuals suspected of plotting pre-meditated attacks in their communities.

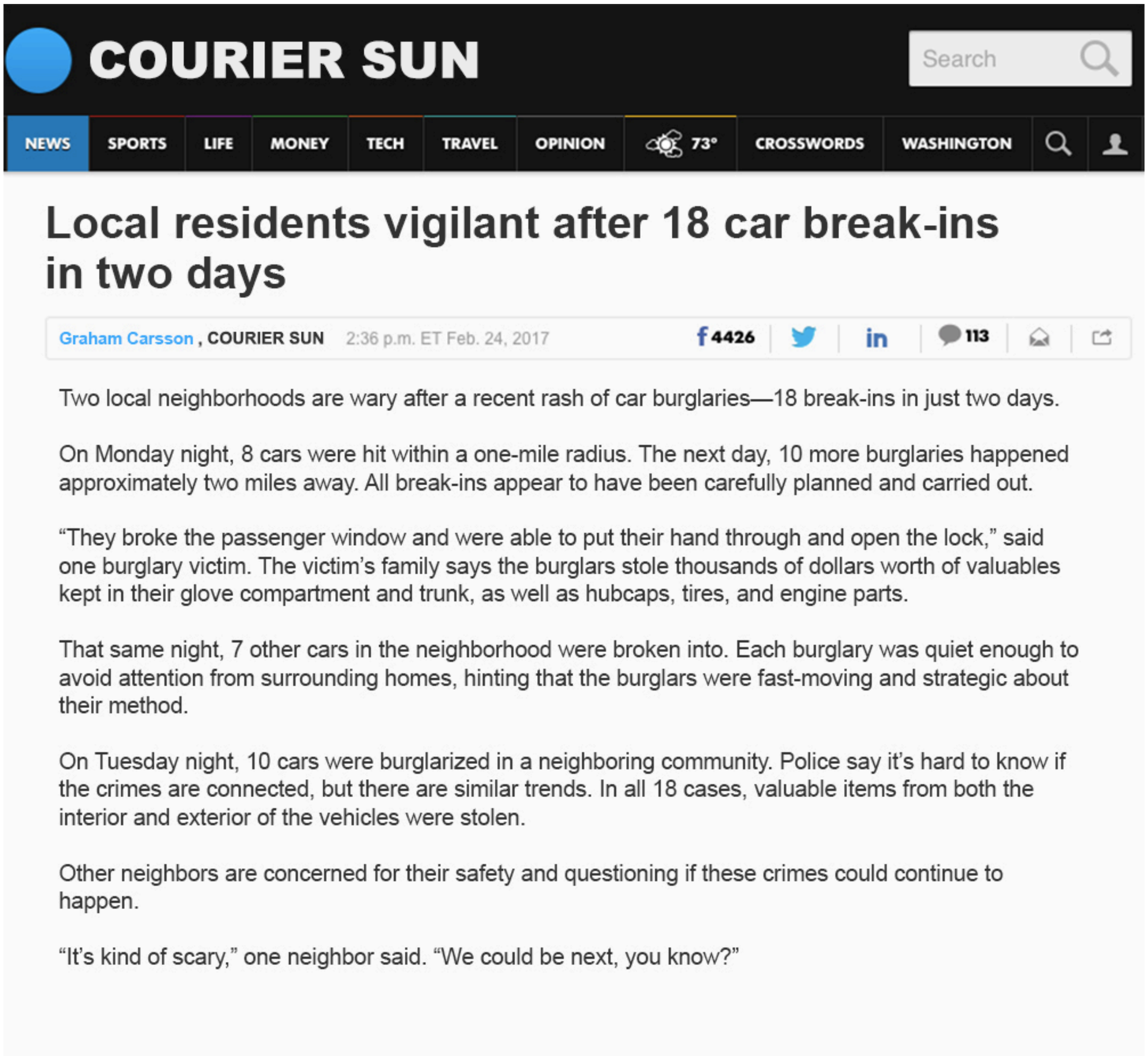
The suspect may face up to a 20-week suspended sentence and could be placed on the sexual offenders' register for up to 7 years. In addition, he may face as many as 200 hours of community service.

Angelica McKinnon, the senior investigating officer for the National Crime Force, said in a statement that voyeurs using tools like night vision binoculars will be pursued:

"People using malicious tools like these goggles can massively violate the privacy of their victims, and plot ways to commit further crimes against them."

It is estimated that more than half the infrared tracker goggles sold each year are used for non-hunting purposes such as voyeurism.

{Physical, Resource Threat}



Local residents vigilant after 18 car break-ins in two days

Graham Carsson , COURIER SUN 2:36 p.m. ET Feb. 24, 2017

Two local neighborhoods are wary after a recent rash of car burglaries—18 break-ins in just two days.

On Monday night, 8 cars were hit within a one-mile radius. The next day, 10 more burglaries happened approximately two miles away. All break-ins appear to have been carefully planned and carried out.

“They broke the passenger window and were able to put their hand through and open the lock,” said one burglary victim. The victim’s family says the burglars stole thousands of dollars worth of valuables kept in their glove compartment and trunk, as well as hubcaps, tires, and engine parts.

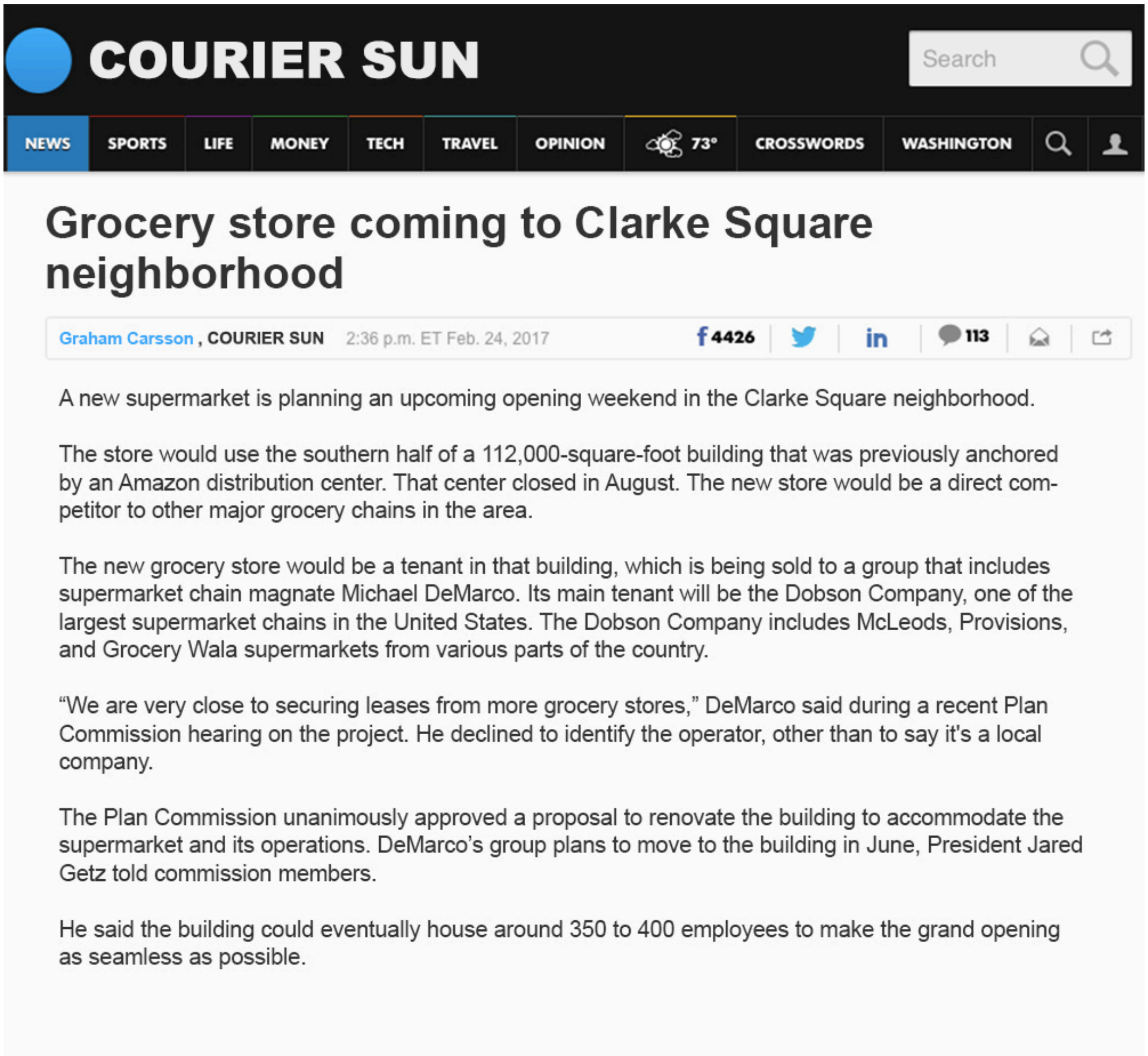
That same night, 7 other cars in the neighborhood were broken into. Each burglary was quiet enough to avoid attention from surrounding homes, hinting that the burglars were fast-moving and strategic about their method.

On Tuesday night, 10 cars were burglarized in a neighboring community. Police say it’s hard to know if the crimes are connected, but there are similar trends. In all 18 cases, valuable items from both the interior and exterior of the vehicles were stolen.

Other neighbors are concerned for their safety and questioning if these crimes could continue to happen.

“It’s kind of scary,” one neighbor said. “We could be next, you know?”

{Physical, Control}



Grocery store coming to Clarke Square neighborhood

Graham Carsson , COURIER SUN 2:36 p.m. ET Feb. 24, 2017

A new supermarket is planning an upcoming opening weekend in the Clarke Square neighborhood.

The store would use the southern half of a 112,000-square-foot building that was previously anchored by an Amazon distribution center. That center closed in August. The new store would be a direct competitor to other major grocery chains in the area.

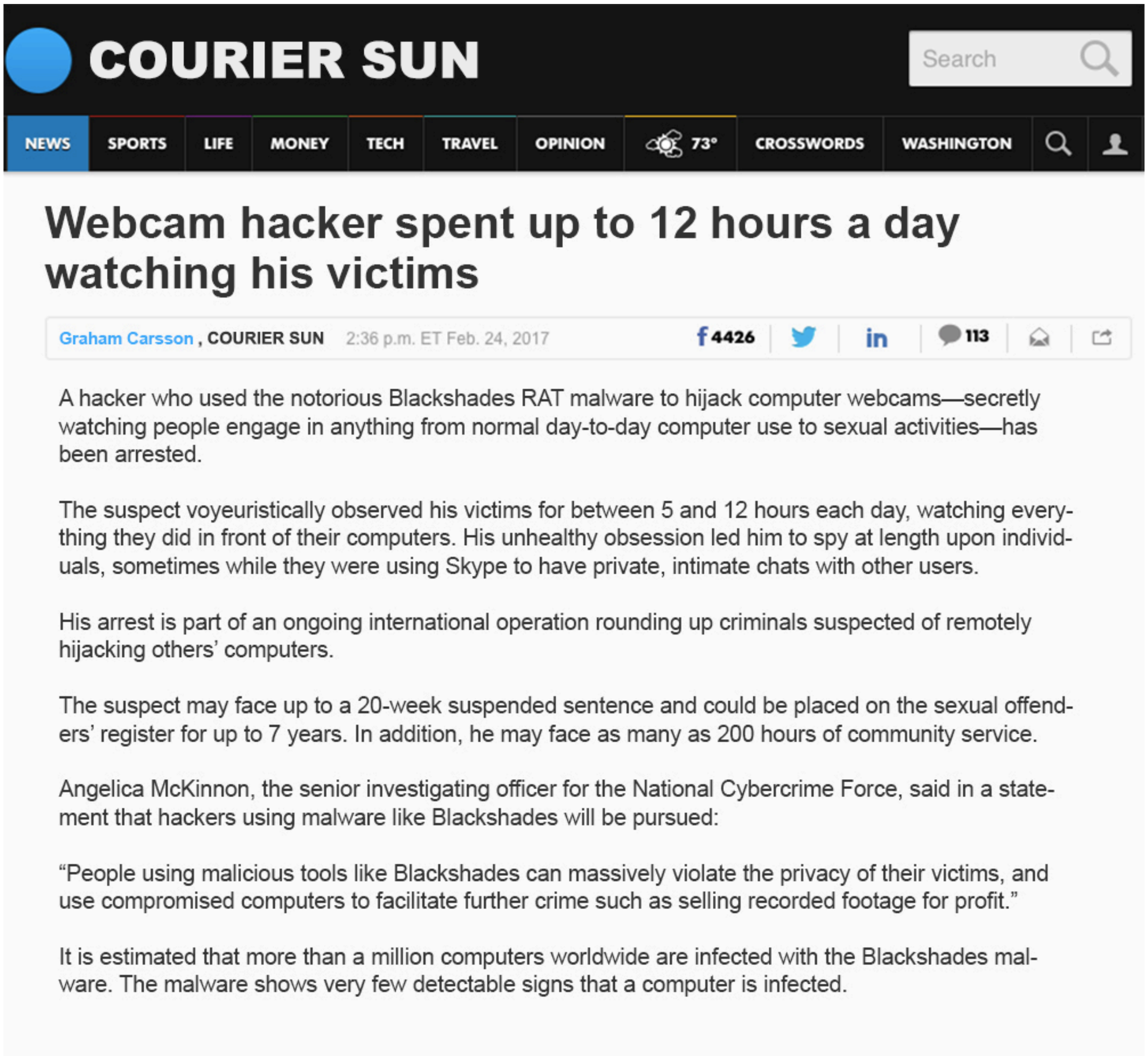
The new grocery store would be a tenant in that building, which is being sold to a group that includes supermarket chain magnate Michael DeMarco. Its main tenant will be the Dobson Company, one of the largest supermarket chains in the United States. The Dobson Company includes McLeods, Provisions, and Grocery Wala supermarkets from various parts of the country.

“We are very close to securing leases from more grocery stores,” DeMarco said during a recent Plan Commission hearing on the project. He declined to identify the operator, other than to say it's a local company.

The Plan Commission unanimously approved a proposal to renovate the building to accommodate the supermarket and its operations. DeMarco’s group plans to move to the building in June, President Jared Getz told commission members.

He said the building could eventually house around 350 to 400 employees to make the grand opening as seamless as possible.

{Online, Self-Protection Threat}



Webcam hacker spent up to 12 hours a day watching his victims

Graham Carsson, COURIER SUN 2:36 p.m. ET Feb. 24, 2017

A hacker who used the notorious Blackshades RAT malware to hijack computer webcams—secretly watching people engage in anything from normal day-to-day computer use to sexual activities—has been arrested.

The suspect voyeuristically observed his victims for between 5 and 12 hours each day, watching everything they did in front of their computers. His unhealthy obsession led him to spy at length upon individuals, sometimes while they were using Skype to have private, intimate chats with other users.

His arrest is part of an ongoing international operation rounding up criminals suspected of remotely hijacking others' computers.

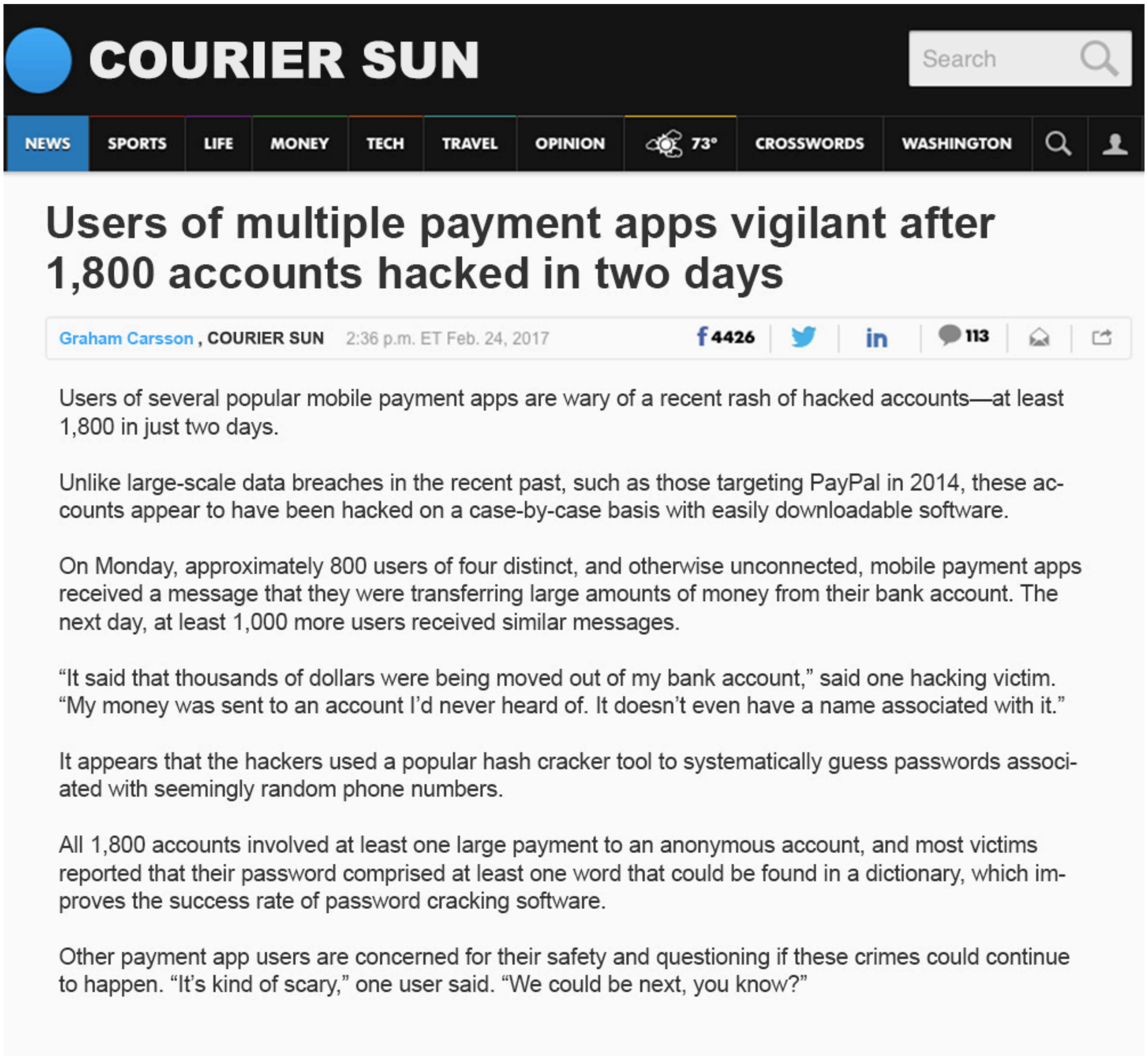
The suspect may face up to a 20-week suspended sentence and could be placed on the sexual offenders' register for up to 7 years. In addition, he may face as many as 200 hours of community service.

Angelica McKinnon, the senior investigating officer for the National Cybercrime Force, said in a statement that hackers using malware like Blackshades will be pursued:

"People using malicious tools like Blackshades can massively violate the privacy of their victims, and use compromised computers to facilitate further crime such as selling recorded footage for profit."

It is estimated that more than a million computers worldwide are infected with the Blackshades malware. The malware shows very few detectable signs that a computer is infected.

{Online, Resource Threat}



Users of multiple payment apps vigilant after 1,800 accounts hacked in two days

Graham Carsson, COURIER SUN 2:36 p.m. ET Feb. 24, 2017

Users of several popular mobile payment apps are wary of a recent rash of hacked accounts—at least 1,800 in just two days.

Unlike large-scale data breaches in the recent past, such as those targeting PayPal in 2014, these accounts appear to have been hacked on a case-by-case basis with easily downloadable software.

On Monday, approximately 800 users of four distinct, and otherwise unconnected, mobile payment apps received a message that they were transferring large amounts of money from their bank account. The next day, at least 1,000 more users received similar messages.

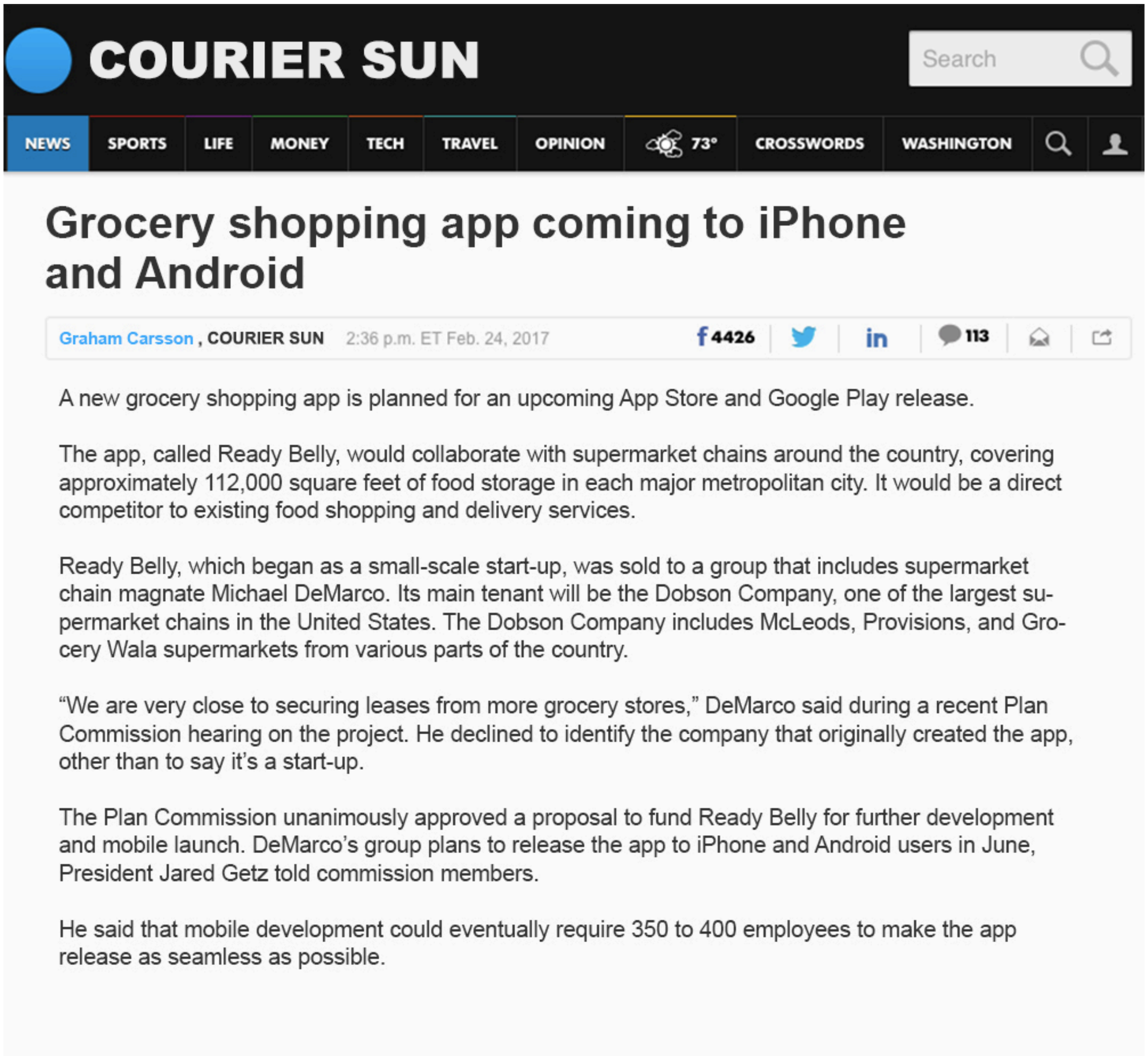
“It said that thousands of dollars were being moved out of my bank account,” said one hacking victim. “My money was sent to an account I’d never heard of. It doesn’t even have a name associated with it.”

It appears that the hackers used a popular hash cracker tool to systematically guess passwords associated with seemingly random phone numbers.

All 1,800 accounts involved at least one large payment to an anonymous account, and most victims reported that their password comprised at least one word that could be found in a dictionary, which improves the success rate of password cracking software.

Other payment app users are concerned for their safety and questioning if these crimes could continue to happen. “It’s kind of scary,” one user said. “We could be next, you know?”

{Online, Control}



Grocery shopping app coming to iPhone and Android

Graham Carsson, COURIER SUN 2:36 p.m. ET Feb. 24, 2017

A new grocery shopping app is planned for an upcoming App Store and Google Play release.

The app, called Ready Belly, would collaborate with supermarket chains around the country, covering approximately 112,000 square feet of food storage in each major metropolitan city. It would be a direct competitor to existing food shopping and delivery services.

Ready Belly, which began as a small-scale start-up, was sold to a group that includes supermarket chain magnate Michael DeMarco. Its main tenant will be the Dobson Company, one of the largest supermarket chains in the United States. The Dobson Company includes McLeods, Provisions, and Grocery Wala supermarkets from various parts of the country.

“We are very close to securing leases from more grocery stores,” DeMarco said during a recent Plan Commission hearing on the project. He declined to identify the company that originally created the app, other than to say it’s a start-up.

The Plan Commission unanimously approved a proposal to fund Ready Belly for further development and mobile launch. DeMarco’s group plans to release the app to iPhone and Android users in June, President Jared Getz told commission members.

He said that mobile development could eventually require 350 to 400 employees to make the app release as seamless as possible.

{CONDITION = ALL}

Which of the following best describes the article you just read?

○ A voyeur used infrared tracker goggles to spy on people in their homes
○ Burglars stole thousands of dollars worth of goods and car parts from parked cars
○ A new grocery store is opening in the neighborhood
○ A voyeur used malware to hack into people's webcams and spy on them
○ Hackers stole thousands of dollars from mobile payment app users
○ A new grocery shopping app is being released on the App Store and Google Play

In the following questions, please indicate how you feel *at this moment* about **your personal safety (i.e., in your day-to-day life)**.

How uncertain do you feel about your personal safety?
❍ Not at all uncertain
❍ A little uncertain
❍ Moderately uncertain
❍ Very uncertain
❍ Extremely uncertain

How much does your personal safety feel at risk?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

How much does your personal safety feel threatened?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

How much do you worry about your personal safety?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

How much do you think about your personal safety?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

In the following questions, please indicate how you feel *at this moment* about **your online safety (i.e., while using technology)**.

How uncertain do you feel about your online safety?
❍ Not at all uncertain
❍ A little uncertain
❍ Moderately uncertain
❍ Very uncertain
❍ Extremely uncertain

How much does your online safety feel at risk?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

How much does your online safety feel threatened?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

How much do you worry about your online safety?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

How much do you think about your online safety?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

In the following questions, please indicate how you feel *at this moment* about **your financial safety (i.e., from someone stealing from you)**.

How uncertain do you feel about your financial safety?
❍ Not at all uncertain
❍ A little uncertain
❍ Moderately uncertain
❍ Very uncertain
❍ Extremely uncertain

How much does your financial safety feel at risk?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

How much does your financial safety feel threatened?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

How much do you worry about your financial safety?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

How much do you think about your financial safety?
❍ Not at all
❍ A little
❍ A moderate amount
❍ A lot
❍ A great deal

Tips to Stay Safe

Please read the safety tips below and answer the questions that follow.

{*Timing data: First Click, Last Click, Page Submit, Click Count*}

{*Each tip followed by the following item:*
How likely are you to follow this recommendation?
○ Extremely unlikely
○ Moderately unlikely
○ Slightly unlikely
○ Slightly likely
○ Moderately likely
○ Extremely likely}

Guard basic personal information carefully
When an unknown site or app requests a piece of information about you (e.g., camera access, zip code), think carefully before providing it. With just your date of birth, zip code, and gender, a hacker has a 63% likelihood of correctly identifying who you are and where you live (Golle, 2006). Steer clear of providing your birthday or year of birth in usernames.

Use an app to share your whereabouts if you're attacked
The mobile app LiveSafe sends location-tagged text, calls, photos, and video clips if you are attacked. Users can set up scalable mass notifications, access safety resources, and ask peers to remotely keep an eye on them when walking alone. For more information, **click here**.

Refrain from sharing your location
Do not share geotagged posts of places you visit on a regular basis. Stalkers may use this information to predict your habits, which could leave you vulnerable to physical attack. Disable location-tracking services on apps that do not require this information (for instructions, **click here**. If you are away from home for an extended period of time, refrain from publicly sharing this information on social media; criminals may monitor public posts to better plan home break-ins.

Would you like to see more tips?
○ No
○ Yes

Condition: No Is Selected.
Skip To: End of Safety Tips (Response Efficacy, Self-Efficacy)

Pay attention to your surroundings
If you are walking to your car alone, and particularly at night, keep an eye out for anything that looks suspicious. If you feel unsafe, throw off potential predators by walking in circles, talking to yourself, or entering your car through the passenger side door. If you are parked near a mall or shopping center, do not hesitate to ask for an escort from security personnel. If someone threatens you, throw your keys as far as possible and run in the opposite direction. For similar tips, **click here**.

Turn on sign-in notifications
Sign-in notifications alert you via e-mail or text when one of your accounts is accessed. If a hacker tries to log into to your account from another location, you can act more quickly to protect your account. **Click here** to activate these notifications for Gmail accounts, and **here** for Facebook accounts.

Be prepared for home invasions
Sleep with your car keys by your bed. In case of a home invasion, the Panic button should startle the attacker and alert neighbors that something is wrong. Consider keeping pepper spray close to your bed, just in case. For similar tips, **click here**.

Would you like to see more tips?
○ No
○ Yes

Condition: No Is Selected.
Skip To: End of Safety Tips (Response Efficacy, Self-Efficacy)

Be wary of e-mail attachments
When you receive an e-mail, even from a friend, consider the possibility that it is infected. If anything seems suspicious about the message or attachment, check with the friend to make sure he or she actually sent it. **Click here** for more information about scanning attachments for viruses or malware.

Always carry the essentials for self-protection
Keep a cell phone battery charged and ready to use in case you find yourself stranded without a method of communication. In case your wallet is stolen, keep cash in another pocket or section of your bag. Consider carrying a whistle or pepper spray to ward off attackers and alert passersby that you need help. For a longer list of safety essentials, **click here**.

Keep your content private
Check all social media settings to ensure that only friends and family can view your content. By hiding your Friends list on Facebook (**click here** for instructions), you can better prevent impersonation attempts while also protecting the privacy of your social contacts.

Walk with confidence
Always look around you when walking, even during the day. Instead of looking at a cell phone or at the ground, carry yourself with a sense of confidence to discourage potential attackers. Make eye contact with people you pass, and especially if anyone seems to be following you; predators are wary of victims who might recognize them later. For more ways to appear confident when traveling alone, **click here**.

Would you like to see more tips?
○ No
○ Yes

Condition: No Is Selected.
Skip To: End of Safety Tips (Response Efficacy, Self-Efficacy)

Set a reminder to change your passwords at least every 6 months
Periodically changing passwords helps prevent identity theft and sensitive data breaches. Use internal (e.g., Keychain Access for Mac users) or reputable third-party apps to store unique passwords, and refrain from using the same password across multiple accounts. **Click here** for a list of trusted (and free) password managers.

Know the signs that an ATM that has been tampered with
Use only ATMs located in well-lit, highly trafficked areas, and cover your fingers while entering PIN numbers and other sensitive information. Furthermore, learn the symptoms of an ATM that has been "skimmed" or tampered with, which allows thieves to store card data, zip codes, and PIN numbers for future use. **Click here** for these warning signs.

Install an anti-virus program, and keep it updated
Anti-virus software can protect against malicious programs or other attempts to compromise your computer. These programs can often detect far more than just viruses, including browser hijackers, spyware, online banking attacks, and phishing attempts. **Click here** for a list of the most highly rated anti-virus software packages.

Look for the emergency exits
Scan any public place (particularly crowded areas) for emergency exits. If anything happens, have an escape plan at the ready. If you enter an unfamiliar place with a group of people, establish a location where the group can meet again if anyone gets separated.

Thinking of the safety tips you just read, please indicate how much you agree or disagree with each of the following statements.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
These tips are effective in keeping me safe from harm.							
These tips work in preventing attack.							
If I follow these tips, I am less likely to be attacked.							
I am able to follow these tips to stay safe.							
I have the skills to follow these tips to stay safe.							
I have the time to follow these tips to stay safe.							
I can easily follow these tips to stay safe.							

Display This Question:
{Physical, Control} **Is Not Displayed**
And
{Online, Control} **Is Not Displayed**

At the beginning of this study, you read an article that described a dangerous or alarming event. How often do you think an event like this occurs?

❍ Never
❍ Very rarely
❍ Rarely
❍ Occasionally
❍ Often
❍ Very often
❍ All the time

Keeping this particular event in mind, please indicate how much you agree or disagree with the following statements.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I believe that the threat described in this article is severe.							
I believe that the threat described in this article has serious negative consequences.							
I believe that the threat described in this article is extremely harmful.							
If you are reading this, select Somewhat Agree							
It is likely that I will face this threat in my lifetime.							
I am at risk for a threat like this.							
It is possible that I will experience this threat one day.							

Have you or a household member ever been a victim of **theft or burglary** (either when you were at home or away from home)?

❍ No
❍ Yes

Have you or a household member ever been the victim of **assault/battery, robbery, or murder**?

❍ No
❍ Yes

Have you or a household member ever been the victim of **identity theft**?

❍ No
❍ Yes

Have you or a household member ever been the victim of **cyberbullying or cyberstalking**?
○ No
○ Yes

Compared with the average person of your sex (male/female), how would you describe your physical size? (This may refer to body frame, height, etc.)
○ Much smaller than average
○ Smaller than average
○ A little smaller than average
○ About average
○ A little larger than average
○ Larger than average
○ Much larger than average

What is your height?
___ feet
___ inches

How much experience do you have with self-defense (e.g., taekwondo, karate, aikido)?
○ None at all
○ A little
○ A moderate amount
○ A lot
○ A great deal

In terms of your Internet skills (i.e., changing privacy or security settings in your browser), do you consider yourself to be...
○ Not at all skilled
○ Not very skilled
○ Fairly skilled
○ Very skilled
○ Expert

In terms of your computer skills (i.e., securing your computer against viruses or safety threats), do you consider yourself to be...
○ Not at all skilled
○ Not very skilled
○ Fairly skilled
○ Very skilled
○ Expert

What is your sex?
❍ Male
❍ Female

What age group do you belong to?
❍ Under 18
❍ 18 - 24
❍ 25 - 34
❍ 35 - 44
❍ 45 - 54
❍ 55 - 64
❍ 65 - 74
❍ 75 - 84
❍ 85 or older

What is your race/ethnicity?
❍ White
❍ Black or African American
❍ Latino/a
❍ American Indian or Alaska Native
❍ Asian
❍ Native Hawaiian or Pacific Islander
❍ Two or more ethnicities
❍ Other

Which of the following best describes your annual household income?
❍ Less than $10,000
❍ $10,000 - $19,999
❍ $20,000 - $29,999
❍ $30,000 - $39,999
❍ $40,000 - $49,999
❍ $50,000 - $59,999
❍ $60,000 - $69,999
❍ $70,000 - $79,999
❍ $80,000 - $89,999
❍ $90,000 - $99,999
❍ $100,000 - $149,999
❍ More than $150,000

What is the highest level of education you've attained?
❍ Less than high school
❍ High school graduate
❍ Some college
❍ 2-year degree
❍ 4-year degree
❍ Professional degree
❍ Doctorate

What is the 5-digit zip code of your permanent home?

____

APPENDIX D

STUDY 4 IRB APPROVAL

EXEMPTION GRANTED

Sau Kwan
Psychology
-
Virginia.Kwan@asu.edu

Dear Sau Kwan:

On 3/2/2017 the ASU IRB reviewed the following protocol:

Type of Review:	Initial Study
Title:	The Relationship between Physical and Online Safety
Investigator:	Sau Kwan
IRB ID:	STUDY00005848
Funding:	None
Grant Title:	None
Grant ID:	None
Documents Reviewed:	• Recruiting, Category: Recruitment Materials; • Qualtrics Survey, Category: Measures (Survey questions/Interview questions /interview guides/focus group questions); • Consent, Category: Consent Form; • Protocol, Category: IRB Protocol; • Debriefing, Category: Other (to reflect anything not captured above);

The IRB determined that the protocol is considered exempt pursuant to Federal Regulations 45CFR46 (2) Tests, surveys, interviews, or observation on 3/2/2017.

In conducting this protocol you are required to follow the requirements listed in the INVESTIGATOR MANUAL (HRP-103).

Sincerely,

APPENDIX E

ADDITIONAL TABLES

Table 12

Study 4: Descriptive statistics for all variables, physical self-protection threat

Variable Type	Variable	Mean	*SD*	*N*
Perceived threat	Perceived physical threat	2.43	0.95	105
	Perceived online threat	2.76	0.90	105
	Perceived financial threat	2.72	1.06	105
Safety practice intentionality	Safety practice intentionality: Online	5.01	0.87	105
	Safety practice intentionality: Physical	3.44	1.55	105
	Safety practices pages viewed	1.60	0.99	105
	Response efficacy (safety practices)	4.46	0.85	104
	Self-efficacy (safety practices)	4.88	0.73	104
Victimization	Victim: Physical crime	0.51	0.67	103
	Victim: Cybercrime	0.31	0.56	104
Situation-specific	Perceived threat severity	4.45	1.03	104
	Perceived threat probability	3.71	1.30	104
Person-specific	Perceived threat susceptibility	3.07	1.09	104
	Physical size	3.95	1.29	104
	Height (inches)	67.11	4.17	104
	Self-defense expertise	1.88	1.02	104
	Security-related digital literacy	3.37	0.75	104

Table 13

Study 4: Descriptive statistics for all variables, physical resource threat

Variable Type	Variable	Mean	*SD*	*N*
Perceived threat	Perceived physical threat	2.30	0.92	115
	Perceived online threat	2.59	0.91	115
	Perceived financial threat	2.70	1.11	115
Safety practice intentionality	Safety practice intentionality: Online	5.10	0.94	115
	Safety practice intentionality: Physical	3.82	1.58	115
	Safety practices pages viewed	1.62	1.01	115
	Response efficacy (safety practices)	4.49	0.90	115
	Self-efficacy (safety practices)	4.98	0.80	115
Victimization	Victim: Physical crime	0.71	0.75	115
	Victim: Cybercrime	0.43	0.64	115
Situation-specific	Perceived threat severity	4.41	0.85	114
	Perceived threat probability	4.79	1.35	115
Person-specific	Perceived threat susceptibility	4.13	1.02	114
	Physical size	4.20	1.33	115
	Height (inches)	67.63	3.81	115
	Self-defense expertise	1.71	0.90	115
	Security-related digital literacy	3.27	0.85	115

Table 14

Study 4: Descriptive statistics for all variables, physical control

Variable Type	Variable	Mean	*SD*	*N*
Perceived threat	Perceived physical threat	1.86	0.68	103
	Perceived online threat	2.44	0.88	103
	Perceived financial threat	2.68	1.12	103
Safety practice intentionality	Safety practice intentionality: Online	4.85	1.20	103
	Safety practice intentionality: Physical	3.85	1.60	103
	Safety practices pages viewed	1.45	0.87	103
	Response efficacy (safety practices)	4.46	0.93	103
	Self-efficacy (safety practices)	4.92	0.75	103
Victimization	Victim: Physical crime	0.45	0.70	103
	Victim: Cybercrime	0.33	0.55	103
Person-specific	Physical size	4.25	1.37	102
	Height (inches)	67.08	3.92	102
	Self-defense expertise	1.81	0.94	102
	Security-related digital literacy	3.26	0.73	102

Table 15

Study 4: Descriptive statistics for all variables, online self-protection threat

Variable Type	Variable	Mean	*SD*	*N*
Perceived threat	Perceived physical threat	2.36	1.03	112
	Perceived online threat	2.80	0.96	112
	Perceived financial threat	2.80	1.09	112
Safety practice intentionality	Safety practice intentionality: Online	5.05	0.94	112
	Safety practice intentionality: Physical	3.82	1.65	112
	Safety practices pages viewed	1.69	1.12	112
	Response efficacy (safety practices)	4.59	0.96	112
	Self-efficacy (safety practices)	4.99	0.76	112
Victimization	Victim: Physical crime	0.66	0.74	112
	Victim: Cybercrime	0.40	0.58	112
Situation-specific	Perceived threat severity	4.77	0.96	112
	Perceived threat probability	4.42	1.30	112
Person-specific	Perceived threat susceptibility	3.41	1.10	112
	Physical size	4.14	1.13	111
	Height (inches)	66.94	3.96	111
	Self-defense expertise	1.85	1.01	111
	Security-related digital literacy	3.23	0.68	111

Table 16

Study 4: Descriptive statistics for all variables, online resource threat

Variable Type	Variable	Mean	*SD*	*N*
Perceived threat	Perceived physical threat	2.30	1.02	108
	Perceived online threat	2.89	0.84	108
	Perceived financial threat	2.78	1.13	107
Safety practice intentionality	Safety practice intentionality: Online	4.98	1.03	107
	Safety practice intentionality: Physical	3.80	1.63	107
	Safety practices pages viewed	1.49	0.87	107
	Response efficacy (safety practices)	4.77	1.00	105
	Self-efficacy (safety practices)	5.01	0.72	105
Victimization	Victim: Physical crime	0.60	0.74	105
	Victim: Cybercrime	0.35	0.60	105
Situation-specific	Perceived threat severity	5.08	0.77	105
	Perceived threat probability	5.01	1.07	104
Person-specific	Perceived threat susceptibility	4.22	0.85	105
	Physical size	4.16	1.37	105
	Height (inches)	67.16	4.06	103
	Self-defense expertise	1.95	1.05	105
	Security-related digital literacy	3.23	0.75	105

Table 17

Study 4: Descriptive statistics for all variables, online control

Variable Type	Variable	Mean	*SD*	*N*
Perceived threat	Perceived physical threat	2.06	0.79	113
	Perceived online threat	2.56	0.72	113
	Perceived financial threat	2.75	1.09	112
Safety practice intentionality	Safety practice intentionality: Online	4.99	1.01	112
	Safety practice intentionality: Physical	3.48	1.60	111
	Safety practices pages viewed	1.36	0.79	112
	Response efficacy (safety practices)	4.60	0.80	111
	Self-efficacy (safety practices)	4.98	0.79	111
Victimization	Victim: Physical crime	0.59	0.76	111
	Victim: Cybercrime	0.34	0.56	111
Person-specific	Physical size	4.41	1.28	111
	Height (inches)	67.17	4.29	110
	Self-defense expertise	1.74	0.91	111
	Security-related digital literacy	3.17	0.75	111

Table 21

Study 4: Correlations of dependent variables, physical self-protection threat

	1.	2.	3.	4.	5.	6.	7.
1. Physical threat	—	—	—	—	—	—	—
2. Online threat	.551***	—	—	—	—	—	—
3. Financial threat	.580***	.605***	—	—	—	—	—
4. Online tip intent	.114	.244**	.192*	—	—	—	—
5. Physical tip intent	.298**	.300**	.326***	.288**	—	—	—
6. Tip pages viewed	.167†	.213*	.183†	.146	.452***	—	—
7. Response efficacy	.050	.188†	.072	.259**	.450***	.193*	—
8. Self-efficacy	.065	.139	.094	.370***	.389***	.270**	.653***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 104 ≤ *n* ≤ 105

Table 22

Study 4: Correlations of exploratory factors, physical self-protection threat

	9.	10.	11.	12.	13.	14.	15.	16.
9. Victim: phys	—	—	—	—	—	—	—	—
10. Victim: online	.092	—	—	—	—	—	—	—
11. Severity	.116	-.057	—	—	—	—	—	—
12. Probability	.191†	.097	.324***	—	—	—	—	—
13. Susceptibility	.087	.097	.305***	.583***	—	—	—	—
14. Physical size	.121	.075	.141	.178†	.009	—	—	—
15. Height	.076	.082	-.042	-.036	-.127	.529***	—	—
16. Self-defense	.038	.051	-.106	.097	.069	.158	.261**	—
17. Digital literacy	.038	.054	-.083	.055	-.004	.084	.154	.168†

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 103 ≤ *n* ≤ 104

Table 23

Study 4: Correlations of dependent and exploratory factors, physical self-protection threat

	9.	10.	11.	12.	13.	14.	15.	16.	17.
1.	.177†	.041	.181†	.386***	.423***	-.122	-.248**	.144	-.025
2.	.038	.157	.330***	.336***	.292**	-.023	-.016	.087	-.051
3.	.138	.180†	.185†	.345***	.415***	.002	-.117	.076	.011
4.	.004	.099	.277**	.199*	.161	.091	.093	-.035	.109
5.	.025	.030	.239**	.376***	.415***	-.132	-.237*	.154	.014
6.	.158	.081	.144	.206*	.173†	-.061	-.009	.258**	.052
7.	-.074	-.135	.369***	.127	.139	.059	-.024	.052	.016
8.	-.014	-.071	.298**	.209*	.157	.033	-.012	-.069	.263**

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 103 ≤ *n* ≤ 104

Table 24

Study 4: Correlations of dependent variables, physical resource threat

	1.	2.	3.	4.	5.	6.	7.
1. Physical threat	—	—	—	—	—	—	—
2. Online threat	.345***	—	—	—	—	—	—
3. Financial threat	.281**	.322***	—	—	—	—	—
4. Online tip intent	.034	.167†	.178†	—	—	—	—
5. Physical tip intent	.348***	.287**	-.042	.323***	—	—	—
6. Tip pages viewed	.149	.157†	.040	.144	.418***	—	—
7. Response efficacy	.074	.112	-.109	.162†	.326***	.182*	—
8. Self-efficacy	.087	.073	-.052	.363***	.304***	.207*	.525***

† p < .10, * p < .05, ** p < .01, *** p < .001; n = 115

Table 25

Study 4: Correlations of exploratory factors, physical resource threat

	9.	10.	11.	12.	13.	14.	15.	16.
9. Victim: phys	—	—	—	—	—	—	—	—
10. Victim: online	.334***	—	—	—	—	—	—	—
11. Severity	-.011	-.020	—	—	—	—	—	—
12. Probability	.193*	.156†	.145	—	—	—	—	—
13. Susceptibility	.238**	.094	.038	.586***	—	—	—	—
14. Physical size	.041	-.008	.080	.176†	.110	—	—	—
15. Height	.015	-.105	-.213*	-.075	-.018	.519***	—	—
16. Self-defense	.059	.232**	-.039	.226*	.082	.174†	.252**	—
17. Digital literacy	.080	-.033	-.211*	.076	.199*	.152	.218*	.246**

† p < .10, * p < .05, ** p < .01, *** p < .001; 114 ≤ n ≤ 115

Table 26

Study 4: Correlations of dependent and exploratory factors, physical resource threat

	9.	10.	11.	12.	13.	14.	15.	16.	17.
1.	.077	.052	.261**	.250**	.334***	.187*	-.066	.143	.080
2.	.085	.067	.099	.173†	.182*	.187*	-.084	.172†	-.170†
3.	.176†	.195*	.116	.237**	.257**	.093	-.061	.051	.058
4.	-.074	-.026	.144	.151	.072	.110	-.157†	-.015	.012
5.	-.124	-.001	.157†	.273**	.274**	.149	-.147	.238**	.045
6.	-.007	.105	.042	.198*	.200*	.051	-.048	.091	-.008
7.	-.001	.145	.183*	.318***	.225*	.054	-.135	.050	.013
8.	.153	.080	.171†	.290**	.173†	.180*	-.024	.091	.215*

† p < .10, * p < .05, ** p < .01, *** p < .001; 114 ≤ n ≤ 115

Table 27

Study 4: Correlations of dependent variables, physical control

	1.	2.	3.	4.	5.	6.	7.
1. Physical threat	—	—	—	—	—	—	—
2. Online threat	.568***	—	—	—	—	—	—
3. Financial threat	.519***	.470***	—	—	—	—	—
4. Online tip intent	-.038	.156	-.033	—	—	—	—
5. Physical tip intent	.139	.292**	.103	.390***	—	—	—
6. Tip pages viewed	.087	.132	.117	.191*	.316***	—	—
7. Response efficacy	-.050	.068	-.061	.439***	.360***	.221*	—
8. Self-efficacy	-.066	-.018	.097	.465***	.321***	.186†	.612***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; *n* = 103

Table 28

Study 4: Correlations of exploratory factors, physical control

	9.	10.	11.	12.	13.	14.	15.	16.
9. Victim: phys	—	—	—	—	—	—	—	—
10. Victim: online	.123	—	—	—	—	—	—	—
11. Severity	—	—	—	—	—	—	—	—
12. Probability	—	—	—	—	—	—	—	—
13. Susceptibility	—	—	—	—	—	—	—	—
14. Physical size	.200*	-.061	—	—	—	—	—	—
15. Height	.041	-.081	—	—	—	.548***	—	—
16. Self-defense	.099	.140	—	—	—	.076	.203*	—
17. Digital literacy	-.042	.124	—	—	—	.091	.109	.109

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; *n* = 102

Table 29

Study 4: Correlations of dependent and exploratory factors, physical control

	9.	10.	11.	12.	13.	14.	15.	16.	17.
1.	.162	.001	—	—	—	-.024	-.083	.055	-.152
2.	.222*	.049	—	—	—	.201*	.004	-.028	-.133
3.	.219*	.220*	—	—	—	.076	-.164†	-.043	-.003
4.	-.029	-.031	—	—	—	.074	-.124	-.181†	.023
5.	.041	.063	—	—	—	.145	-.097	.033	-.151
6.	.298**	.017	—	—	—	.095	-.030	.197*	.064
7.	-.022	.007	—	—	—	.013	-.057	-.033	-.019
8.	.051	.138	—	—	—	-.010	-.193*	.011	-.035

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 102 ≤ *n* ≤ 103

Table 30

Study 4: Correlations of dependent variables, online self-protection threat

	1.	2.	3.	4.	5.	6.	7.
1. Physical threat	—	—	—	—	—	—	—
2. Online threat	.719***	—	—	—	—	—	—
3. Financial threat	.506***	.587***	—	—	—	—	—
4. Online tip intent	.253**	.362***	.314***	—	—	—	—
5. Physical tip intent	.354***	.266**	.436***	.383***	—	—	—
6. Tip pages viewed	.191*	.156†	.120	.144	.392***	—	—
7. Response efficacy	.259**	.201*	.195*	.522***	.459***	.216*	—
8. Self-efficacy	.221*	.225*	.136	.593***	.354***	.147	.697***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; *n* = 112

Table 31

Study 4: Correlations of exploratory factors, online self-protection threat

	9.	10.	11.	12.	13.	14.	15.	16.
9. Victim: phys	—	—	—	—	—	—	—	—
10. Victim: online	.237**	—	—	—	—	—	—	—
11. Severity	-.057	.029	—	—	—	—	—	—
12. Probability	.205*	.170†	.246**	—	—	—	—	—
13. Susceptibility	.013	.212*	.212*	.458***	—	—	—	—
14. Physical size	.097	-.001	-.022	.072	.112	—	—	—
15. Height	-.032	.075	-.081	-.012	.029	.540***	—	—
16. Self-defense	.065	.247**	-.024	.139	.114	.169†	.157†	—
17. Digital literacy	-.093	.032	-.220*	-.078	-.209*	.326***	.311***	.295**

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 111 ≤ *n* ≤ 112

Table 32

Study 4: Correlations of dependent and exploratory factors, online self-protection threat

	9.	10.	11.	12.	13.	14.	15.	16.	17.
1.	.016	.103	.130	.298***	.341***	-.075	-.096	.087	-.143
2.	.003	.133	.277**	.291**	.521***	-.065	.042	.214*	-.184*
3.	-.035	-.018	.214*	.203*	.363***	-.131	.021	.220*	.034
4.	.062	.059	.364***	.112	.124	-.098	-.051	.058	-.137
5.	.003	.118	.140	.142	.137	-.169†	-.173†	.099	-.110
6.	.066	.070	.074	.115	.065	.026	-.068	.126	-.093
7.	-.032	.082	.242**	-.054	.111	-.076	-.116	.077	-.084
8.	.001	.046	.393***	.092	.080	-.082	-.162†	.011	-.118

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 111 ≤ *n* ≤ 112

Table 33

Study 4: Correlations of dependent variables, online resource threat

	1.	2.	3.	4.	5.	6.	7.
1. Physical threat	—	—	—	—	—	—	—
2. Online threat	.517***	—	—	—	—	—	—
3. Financial threat	.603***	.601***	—	—	—	—	—
4. Online tip intent	.051	.130	-.042	—	—	—	—
5. Physical tip intent	.177†	.188*	.062	.405***	—	—	—
6. Tip pages viewed	.100	.119	.019	.198*	.367***	—	—
7. Response efficacy	.057	.078	-.099	.529***	.353***	.168†	—
8. Self-efficacy	-.013	-.037	-.085	.414***	.285**	.171†	.710***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 105 ≤ *n* ≤ 108

Table 34

Study 4: Correlations of exploratory factors, online resource threat

	9.	10.	11.	12.	13.	14.	15.	16.
9. Victim: phys	—	—	—	—	—	—	—	—
10. Victim: online	.210*	—	—	—	—	—	—	—
11. Severity	-.043	.068	—	—	—	—	—	—
12. Probability	-.057	-.096	.144	—	—	—	—	—
13. Susceptibility	.059	.035	.236*	.341***	—	—	—	—
14. Physical size	-.106	-.023	-.021	.118	.021	—	—	—
15. Height	.022	-.030	-.038	-.130	-.061	.437***	—	—
16. Self-defense	.123	.284**	.038	.104	-.060	.072	.098	—
17. Digital literacy	.100	.018	.076	.052	.057	.094	.141	.397***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 102 ≤ *n* ≤ 105

Table 35

Study 4: Correlations of dependent and exploratory factors, online resource threat

	9.	10.	11.	12.	13.	14.	15.	16.	17.
1.	-.052	-.004	-.045	.186†	.190*	.165†	-.045	.011	-.048
2.	-.037	.128	.131	.234*	.147	.044	-.093	.080	-.011
3.	.073	-.031	.008	.164†	.199*	.136	.066	.070	.112
4.	-.035	-.135	.311***	.052	-.119	-.145	-.180†	-.093	.041
5.	.085	.087	.157	.162†	-.055	-.067	-.080	.325***	.223*
6.	.227*	.109	-.047	-.057	-.122	-.026	-.115	.119	-.028
7.	-.025	-.009	.267**	.126	.023	-.202*	-.236*	.060	-.024
8.	-.029	-.041	.308***	.088	-.024	-.189*	-.302**	.225*	.122

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 103 ≤ *n* ≤ 105

Table 36

Study 4: Correlations of dependent variables, online control

	1.	2.	3.	4.	5.	6.	7.
1. Physical threat	—	—	—	—	—	—	—
2. Online threat	.458***	—	—	—	—	—	—
3. Financial threat	.313***	.327***	—	—	—	—	—
4. Online tip intent	-.056	.033	-.053	—	—	—	—
5. Physical tip intent	.139	.077	.026	.362***	—	—	—
6. Tip pages viewed	-.087	.034	.103	.084	.310***	—	—
7. Response efficacy	.054	-.074	-.122	.256**	.402***	.136	—
8. Self-efficacy	-.217*	-.283**	-.118	.357***	.255**	.011	.633***

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 111 ≤ *n* ≤ 113

Table 37

Study 4: Correlations of exploratory factors, online control

	9.	10.	11.	12.	13.	14.	15.	16.
9. Victim: phys	—	—	—	—	—	—	—	—
10. Victim: online	.314***	—	—	—	—	—	—	—
11. Severity	—	—	—	—	—	—	—	—
12. Probability	—	—	—	—	—	—	—	—
13. Susceptibility	—	—	—	—	—	—	—	—
14. Physical size	.100	.007	—	—	—	—	—	—
15. Height	-.110	-.100	—	—	—	.471***	—	—
16. Self-defense	-.040	-.072	—	—	—	-.010	.234*	—
17. Digital literacy	.006	.011	—	—	—	-.153	-.078	.193*

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 110 ≤ *n* ≤ 111

Table 38

Study 4: Correlations of dependent and exploratory factors, online control

	9.	10.	11.	12.	13.	14.	15.	16.	17.
1.	.147	.125	—	—	—	-.077	-.092	.035	-.046
2.	-.034	.085	—	—	—	-.006	.179†	.164†	-.245**
3.	.133	.103	—	—	—	.042	.004	-.141	-.008
4.	-.073	-.060	—	—	—	-.130	-.243**	-.062	.089
5.	.015	.068	—	—	—	-.085	-.194*	.030	.070
6.	.175†	-.075	—	—	—	-.047	.014	.194*	.147
7.	-.039	-.120	—	—	—	-.102	-.139	-.064	.023
8.	.017	-.118	—	—	—	-.117	-.204*	-.113	.192*

† *p* < .10, * *p* < .05, ** *p* < .01, *** *p* < .001; 110 ≤ *n* ≤ 111