MIS Quarterly

RESEARCH ARTICLE

WHAT USERS DO BESIDES PROBLEM-FOCUSED COPING WHEN FACING IT SECURITY THREATS: AN EMOTION-FOCUSED COPING PERSPECTIVE

Huigang Liang and Yajiong Xue
College of Business, East Carolina University,
Greenville, NC 27858 U.S.A. {huigang.liang@gmail.com} {xuey@ecu.edu}

Alain Pinsonneault
Desautels Faculty of Management, McGill University, 1001 Sherbrooke Street West,
Montréal, QC CANADA H3A 1G5 {alain.pinsonneault@mcgill.ca}

Yu "Andy" Wu
College of Business, University of North Texas,
Denton, TX 76203 U.S.A. {andy.wu@unt.edu}

Appendix A

Summary of Past IT Security Research on PFC and EFC

There is a large body of IS research on individuals' IT security behavior. In the paper, we attempted to understand how individuals cope with IT security threats when such behavior is volitional. In this appendix, we briefly review the past studies in this domain. The current literature on individuals' volitional security behaviors has focused primarily on the cognitive reasoning process that motivates individuals to take protective actions against IT security threats. As shown in Table A1, this literature has extensively studied individuals' security behavior in a variety of threat contexts including malware, spyware, hacking, email spam, phishing, identity theft, and device theft. Major theories applied include the protection motivation theory (PMT), the technology threat avoidance theory (TTAT), the health belief model (HBM) , and the theory of planned behavior (TPB). Based on the major theory applied, we grouped the studies in Table A1. Regardless of the theory applied, these studies share a clear commonality – the focal dependent variable is either the security behavior or intention to perform such behavior. From the coping perspective, the action or intention to take protective measures to counter threats is essentially a PFC approach. Therefore, it is conspicuous that the existing research has predominantly investigated PFC. As to EFC, none of the studies that applied PMT, HBM and TPB has mentioned this concept. We have only found one article (Liang and Xue 2009) that discussed EFC in depth and developed formal propositions to explain EFC's relationship with other coping constructs. However, it is a pure theory building paper that offers no empirical evidence to back up the propositions. Several empirical studies based on TTAT (Arachchilage and Love 2014; Herath et al. 2014; Lai et al. 2012; Liang and Xue 2010) allude to EFC, but it is limited to a brief mention in the literature review. Neither is EFC theoretically elaborated, nor empirically tested in these studies. To date, in the IT security literature, we still know little about EFC. Questions such as "what EFC strategies are relevant in the IT security context," "why do people perform EFC when facing IT security threats," and "what are the consequences of EFC" have never been answered.

It should be noted that there is another stream of IT security research focused on employees' compliance with IS security policies mandated by organizations. We have conducted a comprehensive search within this stream by using the keyword "emotion-focused coping" and found one article by D'Arcy et al. (2014) that examines how employees use EFC to cope with security-related stress. This is the only study that explicitly used the term of EFC in this research stream. However, in this study, the research context is mandatory compliance with information

security policies. D'Arcy et al. explain that, in this context, stress is aroused by the overload, complexity, and uncertainty of security policy compliance. This is in sharp contrast with the volitional context in which users' stress is aroused by IT security threats. In addition, D'Arcy et al. did not study EFC directly; instead, they used moral disengagement as a surrogate of EFC. While moral disengagement makes sense when mandatory compliance is the target behavior, it is not as relevant when volitional security behavior is of interest, because individuals are unlikely to think their lack of security behavior to be immoral. Therefore, D'Arcy et al.'s study cannot be readily extended to the context of volitional security behavior. The role of EFC in the volitional context remains unknown.

Table A1. Summary of IS Research on Volitional IT Security Behaviors

Study	Threat Context	Theory Applied	Dependent Variable	Sample	Research Design	Major Findings	EFC	PFC
Chen and Zahedi (2016)	Internet security attacks	PMT	Protective action, knowledge seeking, avoidance	480 U.S. home users and 235 Chinese home users	Survey	Security concern, response efficacy, and self-efficacy influence protective action, and their effects are moderated by espoused culture.	No	Yes
Tsai et al. (2016)	Online security threat	PMT	Security intention	988 MTurk users	Survey	Coping appraisals increase security intention, but threat appraisals have no effect.	No	Yes
Boss et al. (2015)	Data backup, Malware	PMT	Security behavior	Study 1: 104 MBA students Study 2: 327 college students	1: Survey 2: Experiment	Besides traditional threat and coping appraisal variables, fear and maladaptive rewards influence behavioral intention, which leads to security behavior.	No	Yes
Tu et al. (2015)	Mobile device theft	PMT	Coping intention	339 mobile device users	Survey	Response efficacy, self-efficacy, perceived threat, and social influence increase coping intention.	No	Yes
Boehmer et al. (2015)	Online security breach	PMT	Safe online behavior	1: 565 college students 2: 206 college students	1: Survey 2: Experiment	Personal responsibility, self-efficacy and response efficacy are found to enhance behavioral intention.	No	Yes
Crossler and Bélanger (2014)	General IT security threats	PMT	Unified security behaviors	279 employees	Survey	Perceived severity, vulnerability, response efficacy, and self-efficacy increases unified security behavior.	No	Yes
Herath et al. (2014)	Email spam	PMT, TTAT	Intention to adopt email authentication	134 college students	Survey	Risk perception, email screening self-efficacy, and overall appraisal of coping mechanisms increase users' coping motivation.	No	Yes
Jenkins et al. (2014)	Hacking	PMT	Creation of unique passwords	135 college students	Experiment	Just-in-time fear appeals decrease password reuse.	No	Yes
Anderson and Agarwal (2010)	Internet security breaches	PMT, goal framing	Intention to perform security behavior	Study 1: 594 home users Study 2: 101 college students	1: survey 2: experiment	Behavioral intention is influenced by a combination of cognitive, social, and psychological components. Message framing influences the drivers of intention.	No	Yes
Gurung et al. (2008)	Spyware	PMT	Use of anti-spyware tool	232 college students	Survey	All threat and coping appraisal variables significantly affect adoption decision.	No	Yes
Johnston and Warkentin (2010)	Spyware	PMT	Intention to adopt anti-spyware software	275 college faculty, staff, and students	Experiment	Response efficacy, self-efficacy, and social influence increase adoption intention.	No	Yes

Table A1. Summary of IS Research on Volitional IT Security Behaviors (Continued)

Study	Threat Context	Theory Applied	Dependent Variable	Sample	Research Design	Major Findings	EFC	PFC
Lee and Larsen (2009)	Malware	PMT	Adoption intention	239 SMB executives	Survey	All threat and coping appraisal variables significantly affect adoption decision.	No	Yes
Workman et al. (2008)	System breaches	PMT, social cognitive theory	Omissive behavior	588 employees	Survey	Threat and coping assessment, self-efficacy, and locus of control affect omissive behaviors.	No	Yes
Arachchilage and Love (2014)	Phishing	TTAT	Avoidance motivation and behavior	161 college students	Survey	Procedural and conceptual knowledge jointly influence elf-efficacy which in turn increases avoidance motivation and behavior.	No	Yes
Lai et al. (2012)	Identity theft	TTAT	Protective behavior	117 college students	Survey	Both technological and conventional coping are effective in reducing identity theft.	No	Yes
Liang and Xue (2010)	Spyware	TTAT	Use of anti-spyware software	152 college students	Survey	Threat appraisal variables affect perceived threat. All coping variables affect avoidance motivation, which in turn influence behavior.	No	Yes
Liang and Xue (2009)	General IT security threats	TTAT	PFC and EFC	n/a	Theory building	Individuals engage in both PFC and EFC. Perceived threat and avoidability interactively determine PFC and EFC.	**Yes**	Yes
Ng et al. (2009)	Email virus	HBM	Precaution in reading emails	134 part-time college students	Survey	Perceived susceptibility, perceived benefits, and self-efficacy are determinants of computer security behavior.	No	Yes
Lee and Kozar (2005)	Spyware	TPB, innovation diffusion theory	Intention to adopt anti-spyware software	212 Internet users	Survey	Attitude (relative advantage and moral compatibility), social influence (visibility of others' use and image) and perceived behavioral control (computing capacity and trialability) influence behavioral intention.	No	Yes

Appendix B

Coping Factors from WCQ and COPE

Coping Type	Coping Factor	Definition	Source	Include	Justification for Inclusion/Exclusion
EFC	Distancing	Efforts to detach oneself or create a positive outlook.	WCQ	Yes	Most users we interviewed reported that they tried to forget the existence of the threat.
	Self-control	Efforts to regulate one's own feelings and actions.	WCQ	Yes	Security threats can provoke emotions and users need to regulate these emotions. Merged with venting.
	Seeking social support	Efforts to seek informational support, tangible support, and emotional support	WCQ	Yes	Social support is widely used by people to cope with stress. In our research, we are only interested in emotional support. Merged with emotional support seeking.
	Accepting responsibility	Acknowledging one's own role in the problem with a concomitant theme of trying to put things right.	WCQ	No	Conceptually it is more in line with problem-focused coping because when a user accepts his/her responsibility when facing IT security threats, he/she would take security behaviors.
	Escape-avoidance	Wishful thinking and behavioral efforts to escape or avoid.	WCQ	Yes	Users are often unrealistically optimistic and wishfully believe they are safer than others. Merged with wishful thinking.
	Positive reappraisal	Efforts to create positive meaning by focusing on personal growth.	WCQ	No	It is rare for users to positively reappraise the IT security threat.
	Seeking social support for emotional reasons	Getting moral support, sympathy, or understanding.	COPE	Yes	Merged with emotional support seeking.
	Focusing on and venting of emotions	The tendency to focus on whatever distress or upset one is experiencing and to ventilate those feelings.	COPE	Yes	Many users we interviewed reported that they expressed their emotions when they felt the pressure of security threats.
	Behavioral disengagement	Reducing one's effort to deal with the stressor.	COPE	No	It is an EFC strategy when the behavior causes stress. For example, when a child is stressed out by practicing piano, she can disengage herself from piano playing to reduce stress. In the IT security context, this cannot be considered as a type of EFC, because the disengagement of security behaviors does not help to regulate emotions.
	Mental disengagement	Distracting the person from thinking about the behavioral dimension or goal with which the stressor is interfering.	COPE	Yes	The rationale is the same as for distancing.
	Positive reinterpretation	Construing a stressful transaction in positive terms.	COPE	No	Same as positive reappraisal. Irrelevant for the IT security context.
	Denial	Denying the reality of the event.	COPE	Yes	Users deny that they are under the threat of security breaches in order to mitigate stress.
	Acceptance	Acceptance of a stressor as real.	COPE	Yes	Users develop a perception that IT security threats cannot be completely eliminated and their existence have to be accepted. This is conceptually the opposite of denial.
	Turning to religion	The tendency to turn to religion in times of stress.	COPE	No	It is very rare for users to turn to religion when facing IT security threats. It is usually used when facing major disasters or life events. IT security threats are not severe enough to drive people to pray for God's help.

Coping Type	Coping Factor	Definition	Source	Include	Justification for Inclusion/Exclusion
PFC	Planful problem solving	Deliberate problem-focused efforts to alter the situation coupled with an analytical approach to solving the problem	WCQ	Yes	Users undertake specific actions to solve IT security problems. Some of the actions require appropriate planning and scheduling such as update of security software, hard disc scan, system backup, and security patching. In the research, the concept of PFC behavior overlaps with planful problem solving.
	Confrontive coping	Aggressive efforts to alter the situation.	WCQ	No	It is an "aggressive form of problem-focused coping that is largely interpersonal" (Folkman et al 1986a, p. 995). An example item is "I tried to get the person responsible to change his or her mind." It is not relevant when dealing with IT security threats because IT security threat is intangible.
	Active coping	Taking active steps to try to remove or circumvent the stressor or to ameliorate its effects.	COPE	Yes	Users often actively take protective measures to reduce IT security threats. We included it as PFC behavior.
	Planning	Thinking about how to cope with a stressor.	COPE	Yes	It indicates users' intention to cope with threats. Consistent with PFC intention, which is considered in our robustness test.
	Suppression of competing activities	Putting other projects aside, trying to avoid becoming distracted by other events, even letting other things slide, if necessary, in order to deal with the stressor.	COPE	No	This form of coping is most appropriate when the activity to deal with the stressor is complicated and time consuming. For example, a Ph.D. candidate preparing for her thesis defense would suppress all other competing activities and focus only on her presentation. In the IT security context, security action is not highly complicated and doesn't need a lot of time to complete. Hence, it is farfetched to claim that one has to suppress other activities to engage in security action.
	Restraint coping	Waiting until an appropriate opportunity to act presents itself, holding oneself back, and not acting prematurely.	COPE	No	Makes little sense in the IT security context. When facing IT security threats, it is necessary to act immediately rather than wait.
	Seeking social support for instrumental reasons	Seeking advice, assistance, or information.	COPE	No	It is an auxiliary PFC behavior because it does not resolve security threats directly. It reduces the threat by influencing PFC behavior.

Note: WCQ = Ways of Coping Questionnaire (Folkman et al. 1986a); COPE = COPE inventory (Carver et al. 1989). The inclusion/exclusion justifications are based on our deductive reasoning and interviews with 40 IT users.

Appendix C

Definitions of EFC Concepts

Concept	Definition/Description	Source
Emotion-focused coping (EFC)	A type of coping in which individuals try to pacify or control the emotions aroused by the stressful situation or to dismiss the emotional discomforts. It includes inward and outward EFC.	Carver et al. 1989; Folkman and Lazarus 1985; Liang and Xue 2009
Inward EFC	A type of EFC that deals with attention and appraisal of the emotion-arousing situation. It relies on attentional deployment and cognitive change to achieve emotional stability. Three specific inward EFC are selected in our research context: denial, distancing, and wishful thinking.	Folkman et al. 1986a; Gross and Thompson 2007
Distancing	Psychological distancing, also known as "mental disengagement," refers to efforts to psychologically detach oneself from the stressor.	Carver et al. 1989; Folkman et al. 1986b
Denial	Denial is defined as refusal to admit the reality of the stressful situation.	Carver et al. 1989; Liang and Xue 2009
Wishful thinking	Wishful thinking refers to a person's escaping from the stressful situation by fantasizing that some intervening act or forth will turn things around in a desirable direction.	Folkman et al. 1986a
Outward EFC	It refers to individuals' direct modulation of emotional responses or outcome of the emotion-generating process. Two specific outward EFC are selected in our research context: emotional support seeking and venting.	Gross and Thompson 2007
Emotional support seeking	Emotional support seeking means that a person reaches out to his or her social network to obtain moral support, sympathy, or understanding, in the presence of a stressor.	et al. 1989; Folkman and Lazarus 1985
Venting	Venting is the engagement in actions that ventilate whatever the distress that a person is experiencing so that emotional stability is achieved.	Beaudry and Pinsonneault 2010; Carver et al. 1989

Appendix D

Measurements

For each question, please indicate the extent to which you agree with the statement: 1 = strongly disagree, 2 = disagree, 3 = slightly disagree, 4 = neutral, 5 = slightly agree, 6 = agree, 7 = strongly agree.

Perceived Threat

Please describe how you thought about the IT security threat after you noticed it?

1. The malicious nature of the problem threatened me
2. The threat was fearful
3. The threat made me anxious

Perceived Avoidability

Taking everything into consideration (e.g., effectiveness of countermeasures, costs, and my confidence in employing countermeasures), I thought …

1. The threat could be prevented
2. I could protect my computer from the threat
3. The threat was avoidable

Please answer the following questions based on what you have done after you noticed the IT security threat.

Emotional Support Seeking

1. I talked to someone about how I feel
2. I tried to get emotional support from friends or relatives.
3. I discussed my feelings with someone.
4. I got sympathy and understanding from someone.

Emotional Venting

1. I got upset and let my emotions out.
2. I let my feelings out.
3. I felt a lot of emotional distress and I found myself expressing those feelings a lot.
4. I got upset, and was really aware of it.

Denial

1. I refused to believe that it could happen.
2. I persuaded myself that it wouldn't really happen.
3. I acted as though it wouldn't really happen.
4. I said to myself, "This isn't real."

Psychological Distancing

1. I tried not to get too serious about it.
2. I went on as if it has nothing to do with me.
3. I tried not to think about it too much.
4. I tried to forget it as much as I can.

Wishful Thinking

1. I fantasized that it would go away or somehow be over with.
2. I fantasized that I would somehow come across a magical solution for it.
3. I fantasized that all of a sudden it disappears by itself.
4. I fantasized that everything turns out just fine as if nothing happened.

PFC Intention (for Robustness Test)

1. I intended to take safeguarding actions to counter the threat immediately.
2. I predicted I would take safeguarding actions to counter the threat immediately.
3. I planned to take safeguarding actions to counter the threat immediately.

PFC Behavior

1. I installed/updated anti-virus software.
2. I installed/updated anti-spyware software.
3. I updated my operating system with the latest security patch.
4. I turned on the Internet firewall.

Appendix E

Q-Sort Procedures and Results

We validated the items with the Q-sort method, largely following the practices by Moore and Benbasat (1991). We performed four rounds of sorting. In each round, we recruited five judges: two business faculty members, two doctoral students, and an information security professional who worked in the local area. When selecting the judges, we paid particular attention to their gender, nationality, and educational and professional background, so that a variety of perspectives could be offered.

We printed each of the candidate items on one 3 × 5 inch index card. In addition, we created 10 test cards for a test run with the judges. These cards contained 10 statements about automobiles. Some of them were ambiguously worded so that they might appear equally good for two or more categories to the judges. Before the sorting started, a set of standard instructions were read to the judges and we answered their questions about the sorting process. Then the judges sorted the 10 test cards by following the instructions. Afterward, we discussed with the judges the sorting results and resolved problems caused by ambiguous statements. After the judges familiarized themselves with the sorting method through this test run, we asked them to sort the emotion-focused coping items.

In Round 1, we did not provide the labels or definitions of the constructs to the judges. Each judge was asked to group the items into any number of categories and to label and define each category with their own language. As a result, two judges came up with seven categories and the other three came up with eight. A judge might not come up with an equivalent for every construct in our study. Similarly, some of the categories they identified did not have equivalents in our set of constructs. A judge might also determine that a particular item did not belong to any constructs. The inter-judge raw agreement scores averaged 0.588 and the Kappa scores averaged 0.532 (Table E1). The overall placement ratio was 66.72% (Table E2). We examined the off-diagonal entries and found cross-loading between Denial and Psychological Distancing. Based on this observation as well as comments from the judges, we revised the wording in two items for Denial and two items for Wishful Thinking. We also added a new item into Wishful Thinking.

In Round 2, the revised items were sorted by another group of five judges. This time, we provided the judges with the labels and definitions for the constructs. Other than this, the entire process, including the test run, was identical to that of Round 1. As shown in Table E1, the average inter-judge raw agreement increased to 0.836 and the inter-judge Kappa was 0.813. All Kappa coefficients were above the recommend threshold of 0.65 (Moore and Benbasat 1991). The overall placement ratio improved to 91.00% (Table E2).

In Round 3, we asked another five judges to participate. To test whether the improvement in inter-judge agreement and placement ratios in Round 2 were due to the fact that Round 2 judges had the construct labels and definitions, we used the exact same items from Round 2. However, this time the judges were told to decide by themselves how many categories should be created, how they were to be labeled, and what their definitions would be. Four judges identified eight constructs and the remaining one found seven. All the identified constructs matched well with the constructs in this study. Despite not having construct labels and definitions, the placement ratio continued to rise to 91.83% (Table E2). The average inter-judge raw agreement and Kappa also showed improvement to 0.882 and 0.865, respectively (Table E1). This assured us that the items had desirable construct validity and that the improvement from the first to the second round was not due to the judges having construct labels and definitions. In addition, based on comments from the Round 3 judges, we modified the wording of one item for Psychological Distancing. We also made slight changes to two items for Wishful Thinking. Each of the five constructs had four items. Overall, we had a set of 20 items.

In Round 4, the 20 items were sorted by another five judges. Similar to Round 2, the judges had the construct labels and definitions when they started. The sorting results showed further improvement. The average inter-judge raw agreement, average inter-judge Kappa, and the placement ratio increased to 0.921, 0.933, and 95.83%, respectively.

Table E1. Inter-Judge Raw Agreement and Inter-Judge Kappa

	Raw Agreement				Kappa			
	Round 1	**Round 2**	**Round 3**	**Round 4**	**Round 1**	**Round 2**	**Round 3**	**Round 4**
J1-J2	0.594	0.879	0.909	0.909	0.537	0.862	0.896	0.933
J1-J3	0.656	0.697	0.818	0.939	0.605	0.653	0.793	0.966
J1-J4	0.500	0.909	0.939	0.909	0.427	0.896	0.931	0.933
J1-J5	0.625	0.909	0.939	1.000	0.565	0.896	0.931	1.000
J2-J3	0.719	0.727	0.818	0.909	0.682	0.688	0.793	0.899
J2-J4	0.438	0.909	0.909	0.879	0.386	0.896	0.896	0.866
J2-J5	0.562	0.909	0.909	0.909	0.508	0.896	0.896	0.933
J3-J4	0.625	0.727	0.818	0.909	0.576	0.692	0.793	0.899
J3-J5	0.656	0.758	0.818	0.939	0.608	0.723	0.793	0.966
J4-J5	0.500	0.939	0.939	0.909	0.422	0.930	0.931	0.933
Average	**0.588**	**0.836**	**0.882**	**0.921**	**0.532**	**0.813**	**0.865**	**0.933**

Table E2. Placement Ratio Summary

	Round 1	**Round 2**	**Round 3**	**Round 4**
Emotional support seeking	100.00%	100.00%	95.00%	100.00%
Venting	80.00%	100.00%	90.00%	95.00%
Denial	55.00%	85.00%	90.00%	100.00%
Psychological distancing	60.00%	70.00%	90.00%	80.00%
Wishful thinking	33.33%	95.00%	90.00%	100.00%
Average	**66.72%**	**91.00%**	**91.83%**	**95.83%**

Appendix F

Cross Loadings Generated by the Pilot Study

	DIS	DNY	WT	ESS	V	THR	PA	INT	ACT
Chronbach's alpha	0.92	0.97	0.96	0.99	0.99	0.88	0.89	0.94	0.91
DIS1	**0.80**	0.09	0.14	0.08	0.09	-0.16	-0.06	-0.17	-0.001
DIS2	**0.80**	0.29	0.30	0.06	0.13	-0.01	-0.07	-0.28	-0.05
DIS3	**0.82**	-0.01	-0.05	-0.02	-0.14	-0.15	-0.18	-0.07	-0.04
DIS4	**0.82**	0.23	0.24	0.10	0.10	0.02	-0.07	-0.07	0.003
DNY1	0.18	**0.91**	0.15	0.14	0.06	-0.03	-0.07	-0.06	0.09
DNY2	0.15	**0.92**	0.05	0.17	0.07	0.02	-0.09	-0.13	0.15
DNY3	0.17	**0.91**	0.09	0.17	0.08	0.00	-0.16	-0.09	-0.17
DNY4	0.12	**0.87**	0.13	0.22	0.16	0.01	-0.09	-0.20	0.09
WT1	0.28	0.17	**0.83**	0.18	0.06	0.07	-0.14	-0.05	0.03
WT2	0.16	0.10	**0.90**	0.08	0.04	0.05	0.00	-0.12	-0.13
WT3	0.22	0.05	**0.89**	0.08	0.12	-0.05	-0.05	-0.02	0.03
WT4	0.08	0.12	**0.88**	0.07	0.12	0.03	0.11	-0.14	-0.10
ESS1	0.10	0.21	0.15	**0.81**	0.33	0.01	-0.04	-0.06	0.03
ESS2	0.06	0.21	0.13	**0.83**	0.33	0.01	-0.03	-0.04	0.05
ESS3	0.15	0.22	0.08	**0.85**	0.23	0.09	-0.04	-0.09	0.06
ESS4	0.12	0.23	0.13	**0.88**	0.20	0.03	-0.08	-0.12	0.001
V1	0.08	0.11	0.08	0.23	**0.89**	0.07	-0.03	-0.10	-0.02
V2	0.08	0.06	0.08	0.21	**0.91**	0.06	-0.08	-0.09	-0.002
V3	0.12	0.14	0.14	0.23	**0.86**	-0.01	-0.05	-0.15	-0.06
V4	0.07	0.06	0.07	0.21	**0.91**	0.07	-0.10	-0.08	-0.02
THR1	-0.04	-0.01	0.09	-0.04	-0.13	**0.74**	-0.16	0.05	0.18
THR2	-0.07	-0.03	-0.04	-0.02	0.14	**0.91**	-0.05	0.07	0.23
THR3	0.01	0.04	0.06	0.15	0.10	**0.86**	0.01	0.10	0.10
PA1	-0.03	-0.12	0.01	-0.10	0.01	-0.04	**0.90**	0.12	0.09
PA2	-0.18	-0.07	-0.06	-0.09	-0.20	-0.05	**0.83**	0.15	-0.01
PA3	-0.12	-0.15	0.00	0.05	-0.04	-0.06	**0.85**	0.25	-0.03
INT1	-0.16	-0.09	-0.15	-0.06	-0.15	0.14	0.23	**0.87**	0.18
INT2	-0.17	-0.13	-0.18	-0.07	-0.13	0.02	0.20	**0.88**	0.13
INT3	-0.18	-0.26	0.01	-0.16	-0.11	0.01	0.19	**0.80**	0.06
ACT1	-0.30	-0.05	-0.06	0.37	0.03	0.02	0.03	0.37	**0.88**
ACT2	-0.48	-0.03	-0.14	0.10	-0.11	-0.01	0.25	0.23	**0.88**
ACT3	-0.08	-0.03	-0.002	0.22	0.04	-0.07	-0.01	0.43	**0.77**
ACT4	0.05	-0.07	-0.05	-0.08	-0.04	0.09	0.01	0.08	**0.60**

Note: DNY = denial; DIS = psychological distancing; WT = wishful thinking; ESS = emotional support seeking; V = venting; THR = perceived threat; PA = perceived avoidability; INT = PFC intention; ACT = PFC behavior.

Appendix G

Experiment Scenarios

Scenario 1 (High threat, high avoidability):
After you downloaded a free movie from a website that you have never visited before, you suspected that malware could be downloaded onto your computer along with the movie. The malware could steal your personal information and make you a victim of identity theft and suffer from serious losses. This is a serious threat. You know that you have firewall and anti-virus and anti-spyware software running on your computer. You trust these protective tools and believe that they can effectively protect your computer from security breaches. You are confident that you can easily run a scan to find and remove the malware.

Scenario 2 (High threat, low avoidability):
After you downloaded a free movie from a website that you have never visited before, you suspected that malware could be downloaded onto your computer along with the movie. The malware could steal your personal information and make you a victim of identity theft and suffer from serious losses. This is a serious threat. You know that you have firewall and anti-virus and anti-spyware software running on your computer. But you are not sure these tools can protect your computer from the malware, because hackers keep finding new ways to outsmart the security tools. You feel that there is not much you can do about the malware.

Scenario 3 (Low threat and high avoidability):
After you downloaded a free movie from a website that you have never visited before, you suspected that adware could be downloaded onto your computer along with the movie. The adware creates pop-up ads whenever you open a new page in the browser. It can be annoying, but nothing threatening. You know that you have firewall and anti-virus and anti-spyware software running on your computer. You trust these protective tools and believe that they can effectively protect your computer from security breaches. You are confident that you can easily run a scan to find and remove the adware.

Scenario 4 (Low threat and low avoidability):
After you downloaded a free movie from a website that you have never visited before, you suspected that adware could be downloaded onto your computer along with the movie. The adware creates pop-up ads whenever you open a new page in the browser. It can be annoying, but nothing threatening. You know that you have firewall and anti-virus and anti-spyware software running on your computer to protect your computer from security breaches. But you are not sure these tools can protect your computer from the adware, because hackers keep finding new ways to outsmart the security tools. You feel that there is not much you can do about the adware.

Appendix H

Measurement Validation for Study Tw

Before validating the measurements, we assessed two potential biases associated with survey data: nonresponse bias and common method bias (CMB). Following Armstrong and Overton (1977), we compared the demographic variables between the first 100 and last 100 respondents. T-tests show that the two groups do not differ in age ($p = .06$), computer experience ($p = .86$), number of security problems experienced ($p = .59$) and Internet hours per day ($p = .85$). Chi-square tests show that the two groups do not differ in gender ($p = .49$) and education ($p = .41$). These results suggest that nonresponse bias is not likely to exist.

In addition to procedural remedies to reduce CMB, we conducted three statistical tests to evaluate CMB. First, we carried out the Harmon's one factor test by following Podsakoff et al. (2003). The items of the 10 first-order theoretical constructs were entered into a principal component analysis. Nine factors were identified and the first factor of the unrotated solution explains only 23.63% of the total variance, showing no indication of the existence of CMB. Second, we employed the correlational marker variable technique to assess CMB. Following Lindell and Whitney (2001), the second smallest positive correlation amongst measurement items ($r = .002$) was selected as a conservative estimate of CMB. All of the between-item correlations were adjusted by partialling out the CMB estimate. Results revealed that the correlations only changed slightly in magnitude and remained unchanged in significance, suggesting that CMB is unlikely a concern. Third, following Podsakoff et al., we took the single latent method factor approach to testing CMB. A confirmatory factor analysis model including the 10 first-order constructs was created in AMOS. A latent method factor was added which took all of the construct items as its indicators.

Thus, each item was determined by both its theoretical construct and the latent method factor. The results show that the method factor only explains on average 0.56% variance in the items whereas the theoretical constructs explain on average 64.57% (see Table H1). Variances explain by common method only accounts for 1.03% of theoretically explained variances, indicating that CMB has no significant influence on our data.

Table H1. Latent Common Factor Test for Common Method Bias

Item	Factor Loading (R1)	$R1^2$	Method Loading (R2)	R^2	$R2^2 / R1^2$
DNY1	0.78	60.06%	0.07	0.46%	0.77%
DNY2	0.87	76.21%	0.05	0.29%	0.38%
DNY3	0.86	73.62%	0.06	0.32%	0.44%
DNY4	0.69	48.02%	0.08	0.58%	1.20%
DIS1	0.78	61.00%	0.05	0.27%	0.44%
DIS2	0.86	73.27%	0.05	0.23%	0.31%
DIS3	0.88	77.26%	0.05	0.28%	0.36%
DIS4	0.79	63.04%	0.06	0.38%	0.61%
WT1	0.84	70.39%	0.06	0.30%	0.43%
WT2	0.85	72.08%	0.05	0.25%	0.35%
WT3	0.90	81.18%	0.04	0.18%	0.22%
WT4	0.87	76.39%	0.05	0.21%	0.28%
ESS1	0.77	58.98%	0.05	0.28%	0.48%
ESS2	0.78	61.00%	0.06	0.37%	0.61%
ESS3	0.90	80.82%	0.04	0.17%	0.21%
ESS4	0.79	62.88%	0.05	0.27%	0.43%
V1	0.87	76.39%	0.05	0.25%	0.33%
V2	0.88	77.62%	0.05	0.28%	0.36%
V3	0.82	67.08%	0.06	0.32%	0.48%
V4	0.79	62.57%	0.05	0.28%	0.45%
THR1	0.74	54.61%	0.08	0.61%	1.11%
THR2	0.86	74.48%	0.07	0.50%	0.68%
THR3	0.81	65.12%	0.06	0.37%	0.57%
PA1	0.72	51.27%	0.16	2.56%	4.99%
PA2	0.80	64.00%	0.15	2.25%	3.52%
PA3	0.52	26.73%	0.13	1.72%	6.42%
INT1	0.82	67.40%	0.09	0.88%	1.31%
INT2	0.72	51.98%	0.11	1.23%	2.37%
INT3	0.78	60.53%	0.11	1.25%	2.07%
BEH1	0.87	80.10%	0.04	0.15%	0.39%
BEH2	0.85	83.36%	0.06	0.35%	0.42%
BEH3	0.79	73.27%	0.08	0.66%	0.48%
BEH4	0.72	63.68%	0.07	0.50%	0.64%
Average	**0.81**	**66.56%**	**0.07**	**0.58%**	**1.03%**

We then validated the measurement model with confirmatory factor analysis (CFA) using AMOS 22. For both inward EFC and outward EFC, we respectively estimated three models: (1) the first-order model, (2) the second-order reflective model, and (3) the second-order formative model. In covariance-based SEM, it is necessary for a formative construct to have two emitting paths to achieve model identification (Diamantopoulos 2011; Jarvis et al. 2003). The emitting paths point to two reflective indicators of the formative construct or two other endogenous constructs (the so-called MIMIC model). Because we did not have any reflective indicators for inward EFC and outward EFC, we included PFC intention and PFC behavior in the CFA model.

Table H2. Confirmatory Factor Analysis for Measurement Models

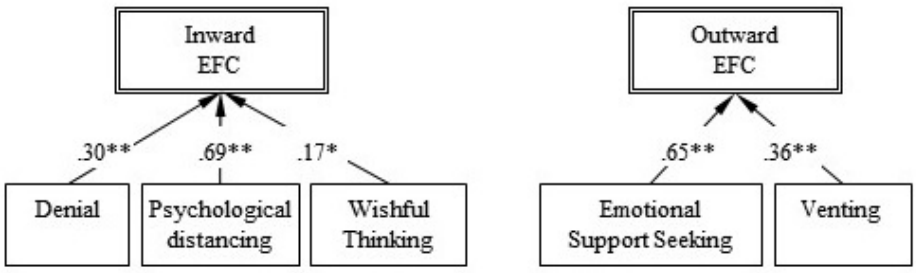
		Inward EFC			Outward EFC		
Fit Index	Cutoff	First-Order	Second-Order Reflective	Second-Order Formative	First-Order	Second-Order Reflective	Second-Order Formative
χ^2/df	< 3	3.013	2.995	2.677	3.13	2.581	2.581
CFIs	> 0.90	0.982	0.982	0.985	0.984	0.988	0.988
TLI	> 0.90	0.975	0.975	0.979	0.976	0.982	0.982
RMSEA	< 0.08	0.046	0.046	0.042	0.048	0.041	0.041

Note: The cutoffs are based on Hu and Bentler (1999) and Gefen et al. (2011). Gefen et al. noted that the the χ^2/df ratio can only be used as a simplifying heuristic and should not be relied on to affirm acceptable model fit. GFI and AGFI are biased by sample size and degrees of freedom and there is consensus against using these indexes to assess model fit (Sharma et al. 2005). Therefore, we focus on using CFI, TLI, and RMSEA.

As Table H2 shows, for inward EFC, the second-order formative model fits better than the first-order model and the second-order reflective model, and for outward EFC, the second-order formative and second-order reflective models have identical fit indices and both are better than the first-order model. However, the differences are marginal, suggesting that all three models could be valid. We selected the second-order formative model over the first-order model because (1) it is theoretically parsimonious (Cenfetelli and Bassellier 2009; Gerbing and Anderson 1984; Law et al. 1999), and (2) it avoids the muliticollinearity issue if the first-order constructs are used as independent variables (Koufterosa et al. 2009). We preferred the second-order formative model to the second-order reflective model because the subconstructs conceptually differ from each other, are not exchangeable, and do not necessarily covary (Jarvis et al. 2003; Petter et al. 2007). Therefore, the formative model is more theoretically justifiable than the reflective model.

Following Petter et al. (2007), construct validity and reliability of the second-order formative measures were assessed by examining path weights and the VIF (variance inflation factor) statistics. As Figure H1 shows, each first-order subconstruct has a significant path pointing to inward or outward EFC, suggesting satisfactory construct validity. The VIF values of the five first-order subconstruct are under the recommended threshold, 3.3 (see Table H2), indicating acceptable reliability (Diamantopoulos and Siguaw 2006).

Finally, following Gefen et al. (2000), validity of all of the first-order construct measures was tested using two procedures. First, the square root of each construct's average variance extracted (AVE) is much greater than the construct's correlations with all other constructs, suggesting sufficient discriminant validity (Table H3). Second, factor loadings and cross loadings (Table H4) were generated by conducting a principal component analysis. All factor loadings on the substantive constructs are over 0.70, suggesting sufficient convergent validity. In addition, each item's factor loading is much higher than its cross-loadings on other constructs, confirming the sufficiency of discriminant validity (Hair et al. 1998). We assessed the internal consistency of each construct by examining Cronbach's alpha and AVE. As Table 3 shows, all alpha coefficients exceed Nunnally's (1978) recommended .70, indicating acceptable internal consistency, and all AVEs are above the .50 level (Fornell and Larcker 1981).



**p < .01
*p < .05

Figure H1. Second-Order Formative Models for Inward and Outward Emotion-Focused Coping

Table H3. Construct Reliability, Variance, and Correlations

	Mean (SD)	VIF	alpha	AVE	DN	DIS	WT	ESS	V	THR	PA	PFC
DN	2.95 (1.64)	2.09	0.93	0.59	**0.77**							
DIS	2.77 (1.66)	1.39	0.96	0.74	0.52**	**0.86**						
WT	3.34 (1.87)	1.80	0.95	0.69	0.67**	0.39**	**0.83**					
ESS	3.67 (1.76)	1.61	0.92	0.68	0.22**	0.17**	0.19**	**0.82**				
V	3.85 (1.74)	1.65	0.94	0.70	0.26**	0.13**	0.25**	0.62**	**0.83**			
THR	4.82 (1.21)	–	0.89	0.74	0.06	0.11*	0.11*	0.29**	0.34**	**0.86**		
PA	5.38 (1.10)	–	0.86	0.65	-0.09*	-0.22**	-0.04	0.05	0.02	0.18**	**0.81**	
PFC	5.45 (1.15)	–	0.90	0.67	-0.20*	-0.27**	-0.20**	0.18**	0.12**	0.29**	0.41**	**0.82**

Note: alpha = Cronbach's alpha, DN = denial; DIS = psychological distancing; WT = wishful thinking; ESS = emotional support seeking; V = venting; THR = perceived threat; PA = perceived avoidability; PFC = PFC behavior. Square roots of AVE are on diagonal.

Table H4. Loadings and Cross-Loadings of the Formal Study (N = 934)

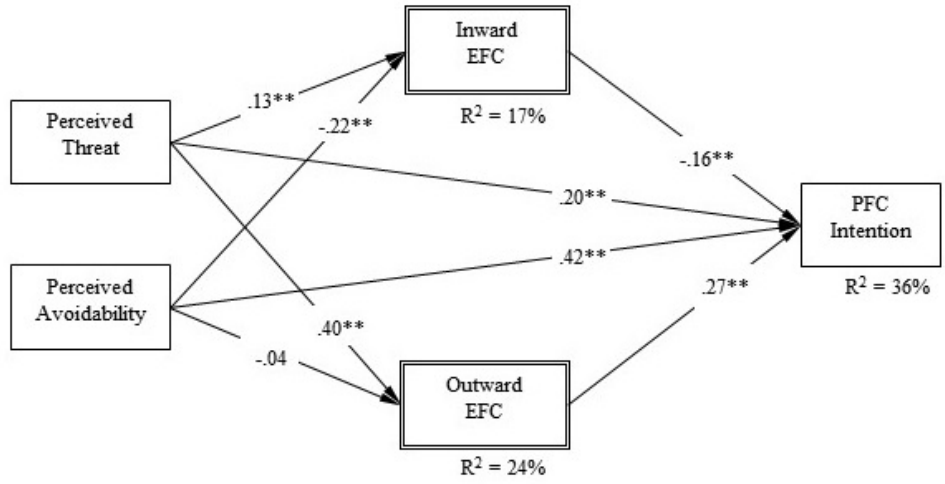
	Mean	SD	DNY	DIS	WT	ESS	V	THR	PA	INT	BEH
DNY1	2.79	1.79	**.771**	.271	.291	.105	.102	.056	-.058	-.043	-.101
DNY2	2.92	1.78	**.790**	.365	.267	.074	.082	.057	-.084	-.033	-.092
DNY3	3.05	1.85	**.769**	.375	.295	.044	.080	.064	-.021	-.033	-.134
DNY4	3.08	1.92	**.738**	.196	.299	.106	.147	.156	-.002	-.005	-.043
DIS1	3.50	1.93	.123	**.761**	.124	.032	-.091	-.104	-.012	-.038	-.184
DIS2	3.05	1.91	.222	**.817**	.213	-.027	-.006	-.087	-.043	-.066	-.128
DIS3	3.54	1.94	.164	**.876**	.178	-.046	-.048	-.048	-.015	-.053	-.097
DIS4	3.38	1.93	.207	**.874**	.178	-.013	-.023	-.002	-.015	-.034	-.107
WT1	3.19	1.96	.301	.338	**.781**	.057	.113	.103	-.048	-.017	-.106
WT2	3.34	2.03	.251	.222	**.840**	.118	.129	.092	.002	-.049	-.067
WT3	3.37	2.08	.250	.277	**.856**	.077	.120	.086	-.013	-.012	-.062
WT4	3.52	2.09	.254	.315	**.832**	.042	.057	.092	.018	.003	-.094
ESS1	4.06	2.09	-.031	-.075	.091	**.809**	.234	.157	.016	.113	.141
ESS2	3.20	1.89	.200	.061	.088	**.818**	.198	.142	-.003	.091	-.036
ESS3	3.85	2.02	.048	.010	.037	**.865**	.306	.131	.007	.047	.062
ESS4	3.65	1.98	.056	.048	.041	**.817**	.298	.123	.030	.021	.030
V1	3.86	1.95	.093	-.021	.092	.280	**.862**	.186	.011	.060	-.001
V2	4.02	1.90	.042	-.018	.056	.309	**.866**	.178	.019	.070	.029
V3	3.61	1.90	.152	-.005	.139	.319	**.803**	.199	-.050	.080	-.001
V4	4.13	1.96	.088	-.091	.111	.233	**.824**	.239	-.002	.065	.065
THR1	4.97	1.65	-.048	-.074	.063	.073	.061	**.832**	.049	.088	.111
THR2	4.76	1.72	.078	-.064	.090	.085	.091	**.898**	.065	.058	.067
THR3	4.30	1.76	.158	-.018	.057	.192	.152	**.843**	.028	.080	-.016
PA1	5.66	1.17	-.113	-.054	.010	.024	-.028	.154	**.799**	.137	.188
PA2	5.72	1.16	-.145	-.070	.038	-.002	-.015	.111	**.816**	.141	.224
PA3	5.33	1.44	-.061	-.018	.079	-.008	-.002	.044	**.804**	-.014	.121
INT1	5.46	1.41	-.078	-.106	-.042	.098	.091	.135	.251	**.818**	.260
INT2	5.19	1.42	.036	-.029	-.002	.074	.094	.055	.196	**.866**	.194
INT3	5.46	1.38	-.066	-.096	-.024	.111	.071	.120	.281	**.814**	.251
BEH1	5.74	1.48	-.062	-.177	-.052	.070	.001	.102	.153	.210	**.859**
BEH2	5.68	1.49	-.041	-.180	-.073	.072	.007	.097	.153	.230	**.869**
BEH3	5.57	1.50	.006	-.186	-.111	.021	-.001	.049	.229	.152	**.793**
BEH4	5.87	1.37	-.183	-.069	-.053	.027	.071	.044	.164	.080	**.744**

Note: DNY = denial; DIS = psychological distancing; WT = wishful thinking; ESS = emotional support seeking; V = venting; THR = perceived threat; PA = perceived avoidability; INT = PFC intention; BEH = PFC behavior.

Appendix I

Robustness Test

While PFC behavior is the most central to improve security because it directly counters IT threats, behavioral intention has been widely used by IT security researchers to infer users' future security behavior (e.g., Anderson and Agarwal 2010; Johnston and Warkentin 2010). To relate this research to the broad IT security literature, we estimated an alternative research model in which PFC behavior was replaced by PFC intention while all the other parts remained unchanged. As Figure I1 shows, the model fit is satisfactory. The left side of the model remains virtually the same. On the right side of the model, PFC intention is reduced by inward EFC decreases ($\beta = -.23$, $p < .01$), but increased by outward EFC ($\beta = .27$, $p < .01$), perceived threat ($\beta = .20$, $p < .01$), and perceived avoidability ($\beta = .42$, $p < .01$). Therefore, it is confirmed that the effects of EFC are consistent, despite some changes in magnitude, on both PFC behavior and PFC intention.



Notes: $^{**}p < .01$; $^{*}p < .05$
$\chi^2 = 662.48$; *df* = 231; *CFI* = .96; *TLI* = .95; *RMSEA* = .04
Six control variables (Age, Gender, Education, Computer Experience, Online Hours, Security Breach Experience) were included on the endogenous constructs.

Figure I1. Robustness Test with PFC Intention as the Dependent Variable

References

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613-643.

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

Armstrong, J. S., and Overton, T. 1977. "Estimating Nonresponse Bias in Mail Surveys," *Journal of Marketing Research* (14), pp. 396-402.

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

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., and Cotten, S. 2015. "Determinants of Online Safety Behaviour: Towards an Intervention Strategy for College Students," *Behaviour & Information Technology* (34:10), pp. 1022-1035.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837-864.

Carver, C. S., Scheier, M. F., and Weintraub, J. K. 1989. "Assessing Coping Strategies: A Theoretically Based Approach," *Journal of Personality and Social Psychology* (56:2), pp. 267-283.

Cenfetelli, R. T., and Bassellier, G. 2009. "Interpretation of Formative Measurement in Information Systems Research," *MIS Quarterly* (33:4), pp. 689-707.

Chen, Y., and Zahedi, F.M. 2016. "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China," *MIS Quarterly* (40:1), pp. 205-222.

Crossler, R., and Bélanger, F. 2014. "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument," *ACM SIGMIS Database* (45:4), pp. 51-71.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 285-318.

Diamantopoulos, A. 2011. "Incorporating Formative Measures into Covariance-Based Structural Equation Models," *MIS Quarterly* (35:2), pp. 335-358.

Diamantopoulos, A., and Siguaw, J. A. 2006. "Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration," *British Journal of Management* (17:4), pp. 263-282.

Folkman, S., and Lazarus, R. S. 1985. "If it Changes it Must be a Process: Study of Emotion and Coping During Three Stages of a College Examination," *Journal of Personality and Social Psychology* (48:1), pp. 150-170.

Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A., and Gruen, R. J. 1986a. "Dynamics of a Stressful Encounter: Cognitive Appraisal, Coping, and Encounter Outcomes," *Journal of Personality and Social Psychology* (50:5), pp. 992-1003.

Folkman, S., Lazarus, R. S., Gruen, R. J., and DeLongis, A. 1986b. "Appraisal, Coping, Health Status, and Psychological Symptoms," *Journal of Personality and Social Psychology* (50:3), pp. 571-579.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.

Gefen, D., Rigdon, E. E., and Straub, D. 2011. "An Update and Extension to SEM Guidelines for Administrative and Social Science Research," *MIS Quarterly* (35:2), pp. iii-xiv.

Gefen, D., Straub, D., and Boudreau, M. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the AIS* (4:7).

Gerbing, D. W., and Anderson, J. C. 1984. "On the Meaning of Within-Factor Correlated Measurement Errors," *Journal of Consumer Research* (11:1), pp. 572-580.

Gross, J., and Thompson, R. A. 2007. "Emotion Regulation: Conceptual Foundations," in *Handbook of emotion regulation,* J. J. Gross (ed.), New York: Guilford Press, pp. 3-24.

Hair, J., Anderson, R., Tatham, R., and Black, W. 1998. *Multivariate Data Analysis* (5th ed.), Englewood Cliffs, NJ: Prentice Hall.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., and Rao, H. R. 2014. "Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service," *Information systems journal* (24:1), pp. 61-84.

Hu, L., and Bentler, P. M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1-55.

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

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

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

Koufterosa, X., Babbar, S., and Kaighobadi, M. 2009. "A Paradigm for Examining Second-Order Factor Models Employing Structural Equation Modeling," *Structural Equation Modeling: A Multidisciplinary Journal* (120:2), pp. 633-652.

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

Law, K. S., Wong, C., and Mobley, W. H. 1999. "Toward a Taxonomy of Multidimensional Constructs," *Academy of Management Review* (23:4), pp. 741-755.

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

Lee, Y., and Larsen, K. R. 2009. "Threats or Coping Appraisal? Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems Research* (18), pp. 177-187.

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

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

Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of Applied Psychology* (86:1), pp. 114-121.

Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp. 192-222.

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

Nunnally, J. 1978. *Psychometric Theory* (2nd ed.), New York: McGraw-Hill.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31:4), pp. 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

Sharma, S., Mukherjee, S., Kumar, A., and Dillon, W. R. 2005. "A Simulation Study to Investigate the Use of Cutoff Values for Assessing Model Fit in Covariance Structure Models," *Journal of Business Research* (58), pp. 935-943.

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

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

Workman, M., Bommer, W. H., and Straub, D. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6), pp. 2799-2816.