Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences

Jingguo Wang
Associate Professor
Information Systems and Operations Management
College of Business, University of Texas at Arlington
701 S. West Street, Box 19437
Arlington, Texas 76019
Email: jwang@uta.edu

Yuan Li
Assistant Professor
Department of MIS
College of Business and Management
University of Illinois at Springfield
One University Plaza, MS UHB 4021
Springfield, Illinois 62703
Email: yli295@uis.edu

H. Raghav Rao
AT& T Chair Professor
Department of ISCS
College of Business
Professor, Department of Computer Science (courtesy appointment)
NPB Building 3.126
One UTSA Circle
University of Texas at San Antonio
San Antonio, TX
Email: hr.rao@utsa.edu

Appendix A: Prior Literature on Phishing Susceptibility and Detection

As phishing is a relatively new phenomenon that has emerged with the development of the Internet technology in recent years, studies on how individuals process and detect phishing attacks are still limited. Table A1 presents a list of empirical studies on this topic. Early studies focusing on the phishing detection process were exploratory in nature and adopted descriptive analyses with relatively small sample sizes and narrow demographics (Anandpara et al. 2007; Dhamija et al. 2006; Downs et al. 2006, 2007; Furnell 2007). These studies mainly suggest that individuals are susceptible to phishing

attacks, and that they adopt simplifying heuristic decision rules to detect phishing attacks, where meanings and relative values are assigned to cues presented in the emails (such as sources of the emails, etc.). Although phishing emails have evolved over time, a number of cues still signal their deceptive nature (APWG 2010; Microsoft 2010; Public Safety Canada 2009).

The information processing perspective seems to dominate the phishing detection literature (Vishwanath et al 2011), and a range of information cues have been examined to understand how individuals identify phishing emails, such as sources of emails, grammar and spelling, email titles, security bar indicators, and other design features (Anandpara et al. 2007; Dhamija et al. 2006; Downs et al. 2007). Meanwhile, mechanisms that influence individuals' attentions to the information cues are also analyzed, such as knowledge, involvement, and computer self-efficacy (Vishwanath et al 2011; Wang et al 2012; Wright and Marett 2010). Nevertheless, studies also show that people often ignore information cues in emails, leading to misjudgment and falling prey to phishing (Dhamija et al. 2006; Pattinson et al 2012). This happens because the detection of phishing attacks is a cognitively demanding task (Vishwanath et al. 2011; Wang et al. 2012) due to the reliance on emails for business communications and the amount of emails one receives every day, so that "habitual media use patterns, where individuals inattentively respond to relevant emails, accounted for at least one half of the variance in phishing susceptibility" (Vishwanath et al. 2011, p. 583). As a phisher can manipulate receivers' information processing by cleverly crafting email content (Anandpara et al. 2007; Dhamija et al. 2006; Downs et al. 2006; 2007; Furnell 2007; Luo et al. 2013; Wang et al. 2012; Workman et al. 2008; Wright et al. 2014), these issues call for more theoretically driven studies on how individuals actually process and respond to phishing attacks.

Researchers have also examined how individual characteristics affect their susceptibility to phishing attacks, including personality traits (APWG 2010; Microsoft 2010; Moody et al. 2011; Pattinson et al. 2012; Public Safety Canada 2009; Workman et al. 2008; Wright and Marett 2010) and knowledge and efficacy beliefs regarding computers, the Internet, business domains, senders, and phishing scams (Burns et al. 2012; Downs et al. 2006; 2007; Moody et al. 2011; Sheng et al. 2010; Vishwanath et al.

2011; Wang et al. 2012; Wright and Marett 2010). But overall, how users' psychological and behavioral responses influence phishing detection and how they influence outcomes is an under studied area.

Table A1. Summary of Empirical Studies in Users' Phishing Susceptibility and Detection (in chronological order)

Table 1. Summary of Empirical Studies in Users' Phishing Susceptibility and Detection (in chronological order)			
Reference	**Research Methodology**	**Research Participants**	**Major Findings**
Dhamija et al. (2006)	A survey on judging 20 website images whether they were fraudulent	22 university students	Participants often ignored browser-based cues such as the address bar, the status bar, and the security indicators when making their judgment.
Jagatic et al. (2007)	Experiment with a mock phishing attack	1731 university students aged 18 to 24 years old	The study tested the effects of context-specific phishing attacks. Emails that appeared to originate from friends produced a high victimization rate. Age and gender contributed to an individual's vulnerability.
Downs et al. (2007)	A survey on the behavioral response (e.g., reply, delete) to 5 email images	232 members of a university community	Users who had a better knowledge of the Internet environment were less susceptible to phishing attacks. Perceived severity of the consequences predicted behavior responses.
Furnell (2007)	An survey on judging 20 email images on their legitimacy	179 members of the general public (mostly in the 18–29 age group)	Participants had significant problems in discriminating between messages on the basis of the content alone, and could not use visual, technical, and language cues for their judgment reliably.
Anandpara et al. (2007)	A survey on judging 5 email images	40 subjects	The study argued that phishing education may make participants more suspicious and, in turn, result in a bias toward "phishing" decisions.
Dodge et al. (2007)	Training evaluation method development and experiment on students' response to mock phishing attacks	512 students in a military academy	This paper described how to implement an evaluation of the effectiveness of phishing education program in a military academy.
Sheng et al. (2007)	Training tool development and evaluation experiment	42 experiment participants recruited on campus	The study introduced an online game called "Anti-Phishing Phil" for user training and illustrated its effectiveness via an experiment.
Workman et al. (2008)	Survey and observations on behavioral responses to mock phishing attacks	588 employees of a company	The study explored the use of social engineering tactics such as commitment, reciprocation, and social proof in phishing attacks.
Kumaraguru et al. (2008)	Experiment on evaluating anti-phishing training	211 employees of a large Portuguese company	A large percentage of people who clicked on links in simulated emails proceeded to give some form of personal information to fake phishing websites. Participants who received PhishGuru training were significantly less likely to fall for subsequent simulated phishing attacks one week later.

Kumaraguru et al. (2010)	Training tool development and evaluation experiment	28 to 30 participants for each experiment recruited around campus	Introduced an email-based anti-phishing education system called "PhishGuru" and an online game called "Anti-Phishing Phil" that teaches users how to use cues in URLs to avoid falling for phishing. It demonstrated the effectiveness of these tools to train users to recognize phishing.
Sheng et al. (2010)	A survey on judging 14 email images	1001 online respondents (with an average age around 30)	The study explored the relationship between demographics and phishing susceptibility. Gender, age, and prior exposure to phishing education were found to be important factors influencing one's phishing susceptibility.
Wright and Marett (2010)	Survey and observation on behavioral responses to a mock phishing attack	299 undergraduate business students	Participants' experiential factors (such as computer self-efficacy, web experience, and security knowledge) and dispositional factors (such as suspicion) influenced their detection success.
Moody et al. (2011)	Survey and observation on behavioral responses to a mock phishing attack	595 undergraduate students	The study investigated whether message characteristics, personality traits, and Internet experience affected users' susceptibility to phishing attacks. Mixed results were found.
Vishwanath et al. (2011)	A survey on the likelihood of responding to a targeted phishing email image	161 university students	Most phishing emails are peripherally processed and individuals make decisions based on simple cues embedded in the email. Computer self-efficacy significantly influences message elaboration, but its influence is diminished by domain-specific knowledge.
Burns et al. (2012)	Proposed to use online survey	Proposed to use 400 students and nonstudents	The study proposed to examine users' vigilance toward phishing attempts through the theoretical lens of a hybrid continuum-stage behavior change model.
Pattinson et al. (2012)	A survey presenting 50 email images for participants to indicate their behavioral response, half of which were genuine emails	117 university students	The study investigated the behavior response (e.g., delete the email, leave the email in the inbox) of users to phishing emails and compared this to their response to genuine emails. Familiarity with computers, cognitive impulsivity, and personality traits affected behavioral responses to both types of emails.
Mohebzada et al. (2012)	Phishing experiments with two mock phishing attacks targeting a university community	Mock phishing emails were sent to 10,917 valid email addresses related to a university	User demographics alone do not predict users' susceptibility to phishing attacks. Many users tend to ignore the warnings regarding phishing.
Wang et al. (2012)	A survey on the likelihood of responding a targeted phishing email image	321 university students	The study investigated the processing of a spear phishing email targeted at members of a public university. Scam knowledge, users' attention to "visual triggers," and "phishing deception indicators" played critical roles in email processing and forming the intention to respond.
Wright et al. (2014)	A field experiment that involved sending phishing messages to participants	2624 students in a university	The study examined the effects of influence techniques employed in by phishers in their attacking emails.

References for Appendix A

Anandpara, V., Dingman, A., Jakobsson, M., and Liu, D. 2007. Phishing IQ tests measure fear, not ability. FC"07/USEC"07 Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security. 362–366.

APWG. 2010. Consumer Advice: How to Avoid Phishing Scams. *Anti-Phishing Working Group, http://www.antiphishing.org/resources/overview/avoid-phishing-scams* (retrieved on March 30, 2017).

Burns, M. B., Durcikova, A., and Jenkins, J. L. 2012. On Not Falling For Phish: Examining Multiple Stages Of Protective Behavior Of Information Systems End-Users. *in the Proceedings of International Conference on Information Systems*.

Dhamija, R., Tygar, J. D., and Hearst, M. 2006. Why phishing works. Grinter R, Rodden T, Aoki P, Cutrell E, Jeffries R and Olson G (ed.), *in the Proceedings of SIGCHI*, Montreal, Canada. 581–590.

Dodge, R. C., Jr, Carver, C., and Ferguson, A. J. 2007. Phishing for user security awareness. *Computers & Security* **26**(1) 73–80.

Downs, J. S., Holbrook, M. B., and Cranor, L. F. 2006. Decision strategies and susceptibility to phishing. *in the SOUPS '06 Proceedings of the second symposium on Usable privacy and security*. Pittsburgh, PA, July 12-14.

Downs, J. S., Holbrook, M., and Cranor, L. F. 2007. Behavioral response to phishing risk. *in the Proceedings of APWG 2nd Annual eCrime Researchers Summit*. Pittsburgh, PA, October 04 - 05.

Furnell, S. 2007. Phishing: can we spot the signs? *Computer Fraud & Security* **2007**(3):10–15.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. 2007. Social phishing. *Communications of the ACM* **50**(10) 94–100.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., and Hong, J. 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology* **10**(2) 1–31.

Luo, X. R., Zhang, W., Burd, S., and Seazzu, A. 2013. Investigating Phishing Victimization with the Heuristic-Systematic Model: A Theoretical Framework and an Exploration. *Computers & Security* **38**(1) 28–38.

Microsoft. 2010. How to recognize phishing e-mails or links. *https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx* (retrieved on March 30, 2017).

Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., and Darwish, A. 2012. Phishing in a university community: Two large scale phishing experiments. *in the Proceedings of 2012 International Conference on Innovations in Information Technology (IIT)*, AbuDhabi, Al-Ain, UAE. March 10-12.

Moody, G., Galletta, D. F., Walker, J., and Dunn, B. K. 2011. Which Phish Get Caught? An Exploratory Study of Individual Susceptibility to Phishing. *in the Proceedings of International Conference on Information Systems*.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., and Butavicius, M. 2012. Why do some people manage phishing e-mails better than others? *Information Management & Computer Security* **20**(1) 18–28.

Public Safety Canada. 2009. Phishing: A new form of identity theft. *https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-phshng/index-en.aspx* (retrieved on March 30, 2017).

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. 2010. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. ,Mynatt E (ed.), *in the Proceedings of the 28th international conference on Human factors in computing systems*. Atlanta, GA, April 10-15.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. 2007. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. *in the Proceedings of the 3rd Symposium On Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, July 18-20.

Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. 2011. Why do people get phished?

Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision support systems* **51**(3) 576–586.

Wang, J., Herath, T., Chen, R., Vishwanath, A., and Rao, H. R. 2012. Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication* **55**(4) 345–362.

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) 2799–2816.

Wright, R. T., and Marett, K. 2010. The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems* **27**(1) 273–303.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., and Marett, K. 2014. Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research* **25**(2) 385–400.

Appendix B. Online consent form and an Example of Email Judgment

ONLINE CONSENT FORM

TITLE OF PROJECT
Cognitive biases and judgment errors in phishing email recognition

INTRODUCTION
You are being asked to participate in a research study about human's recognition of phishing emails. Your participation is voluntary. Refusal to participate or discontinuing your participation at any time will involve no penalty or loss of benefits to which you are otherwise entitled. Please ask questions if there is anything you do not understand..

PRINCIPAL INVESTIGATOR
…

PURPOSE
The specific purpose(s) of this research study is to understand the process of how individuals detect phishing emails.

DURATION
Participation in this study will last approximately 15 minutes.

PROCEDURES
In this survey, you will be asked to judge 16 emails whether they are legitimate or not and answer a set of related questions. All these emails are actual ones that arrived in someone's mailbox who is known to the researchers. For privacy purpose, the receiver's name has been changed to "JIM CARREY", and the email address changed to jim@yahoo.com or jim@netbanker.com (if these appeared in the original email). If you believe the email was truly sent from the business entity it claims to be, you choose "Yes". If you believe the email is from someone pretending to be what the emails claims to be (i.e., it is a phishing email that pretends to be from a legitimate business entity), you choose "NO".

You will also be asked a number of questions on your judgment process. There are no right or wrong answers to the questions presented in the questionnaire. We are only interested in your candid thoughts and opinions. Your participation is voluntary, but please be assured that the answers you provide will remain anonymous and confidential. No information related to your identity (such as name, personal ID, etc.) will be collected.

POSSIBLE BENEFITS
Phishing causes significant economic damage. It also erodes consumer trust in email-based business communication, increasing consumer resistance towards online communication and the cost of doing business online. This study will help us deepen our understanding in human cognitive process of phishing detection and recognition, and develop proper strategies to prevent individuals from falling victims of phishing attacks.

POSSIBLE RISKS/DISCOMFORTS
There are no perceived risks or discomforts for participating in this research study. Should you experience any discomfort please inform the researchers, you have the right to quit any study procedures at any time at no consequence.

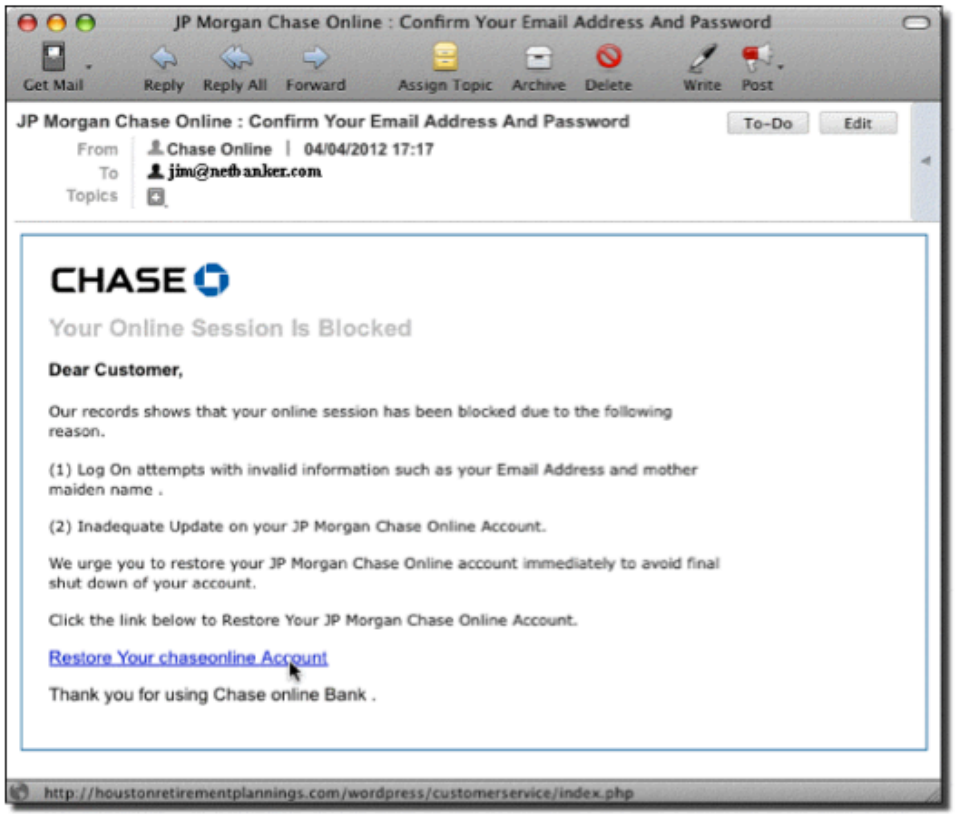
CONFIDENTIALITY
…
CONTACT FOR QUESTIONS
….

CONSENT
By choosing to continue with the survey below, you confirm that you are 18 years of age or older and you are providing your implied consent to voluntarily participate in this survey.

AN EXAMPLE OF EMAIL JUDGMENT

Is this a legitimate email?

Yes	No
○	○



How familiar do you think you are with the business entity indicated in the email?

Not at All	A Little	Some	Much	A Lot
○	○	○	○	○

Have you personally received or seen this particular email before this survey?

Yes	No
○	○

Appendix C. Measurement Items

Unless specified, all items were measured with a 5-point Likert scale (1-Strongly Disagree, 2-Disagree, 3-Neither Agree nor Disagree, 4-Agree, 5-Strongly Agree):

1. Perceived susceptibility to phishing attacks
Item 1: It is likely that I will become a victim of phishing attacks.
Item 2: It is likely that I will reply to the request of a phishing email.

2. Perceived severity of phishing victimization
Item 1: The loss for me would be significant if I fall a victim to a phishing attack.
Item 2: The consequences of an identity theft (for example, losing my bank account and password) are severe for me.

3. Perceived detection efficacy
Item 1: I can recognize phishing emails.
Item 2: I can differentiate phishing emails from legitimate ones.

4. Phishing Anxiety
Item 1: When I think about being phished, I feel nervous.
Item 2: When I think about being phished, I get upset.
Item 3: When I think about being phished, I get depressed.
Item 4: When I think about being phished, I get jittery.
Item 5: When I think about being phished, my heart beats faster.
Item 6: When I think about being phished, I feel uneasy.
Item 7: When I think about being phished, I feel anxious.

5. Coping responses:
Please indicate to what extent you agree with each of the following statements regarding your goal of judging the emails (differentiating phishing e-mails from genuine business e-mails).

5.1. Task-focused coping
Item T1: I made every effort to achieve my goals.
Item T2 (Dropped): I was single-minded and determined in my effort to overcome any problems.
Item T3: I concentrated hard on doing well.

5.2. Emotion-focused coping
Item E1: I worried about my inadequacies.
Item E2: I blamed myself for not doing better.
Item E3: I blamed myself for not knowing what to do.

5.3. Avoidance coping
Item A1: I acted as though the task wasn't important.
Item A2: I didn't take the task too seriously.
Item A3: I decided there was no point in trying to do well.

6. Dispositional optimism
Item 1: In uncertain times, I usually expect the best.
Item 2: It's easy for me to relax. (Filler)
Item 3: If something can go wrong for me, it will. (Reverse)
Item 4: I'm always optimistic about my future.
Item 5: I enjoy my friends a lot. (Filler)
Item 6: It's important for me to keep busy. (Filler)
Item 7: I hardly ever expect things to go my way. (Reverse)
Item 8: I don't get upset too easily. (Filler)
Item 9: I rarely count on good things happening to me. (Reverse)

Item 10: Overall, I expect more good things to happen to me than bad.
(Scoring: Items 3, 7, and 9 are reverse scored. Items 2, 5, 6, and 8 are fillers and are not counted into the sum.)

7. Internet experience
These items were measured with a 5-point Likert scale (1-Never, 2-Rarely, 3-Sometimes, 4-Most of the Time, 5-Always):
Item 1: Buying products or services online with a credit card, a debit card, or a payment service such as PayPal.
Item 2: Accessing bank accounts (such as checking, savings, or mortgage) online.
Item 3: Paying bills (such as electronic, utility, credit cards, or loans) online.
Item 4: Buying and selling stocks or mutual funds online.
Item 5: Posting messages at social sites (such as Facebook or Twitter).
Item 6: Searching for product/service information online.
(Scoring: Sum of the 6 items)

8. Prior victimization
(Yes/No)
Item 1: Someone used or attempted to use your credit cards without permission.
Item 2: Someone used or attempted to use your accounts such as your wireless phone account, bank account, or debit/check cards without your permission.
Item 3: Someone used or attempted to use your personal information without permission to obtain new credit cards or loans, run up debts, open other accounts, or commit other fraud.
(Scoring: Sum of the 3 items)

All other variables were measured with single items.

Appendix D Descriptive Statistics and Item-loadings for principle constructs

Table D1 Correlations, Reliability Statistics, and Average Variance Extracted

	Principal Construct	**Mean**	**STD**	**AVE**	**CR**	**CA**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	Perceived susceptibility	2.47	0.97	0.81	0.89	0.77	**0.90**								
2	Perceived severity	3.91	0.84	0.77	0.87	0.71	0.14	**0.88**							
3	Perceived detection efficacy	3.62	0.84	0.88	0.94	0.86	-0.27	0.09	**0.94**						
4	Phishing Anxiety	2.89	0.98	0.76	0.96	0.95	0.41	0.27	-0.17	**0.87**					
5	Task-focused coping	4.10	0.71	0.79	0.88	0.74	-0.08	0.27	0.25	0.01	**0.89**				
6	Emotion-focused coping	2.56	0.96	0.70	0.88	0.79	0.33	0.05	-0.23	0.34	-0.13	**0.84**			
7	Avoidance coping	1.86	0.86	0.79	0.92	0.86	0.38	-0.10	-0.10	0.24	-0.39	0.45	**0.89**		
8	Detection effort	1.31	0.46	—	—	—	-0.21	0.01	0.07	-0.11	0.10	-0.19	-0.31	—	
9	Detection accuracy (%)	67.00	15.36	—	—	—	-0.21	-0.01	0.18	-0.16	0.15	-0.26	-0.27	0.40	—

STD: standard deviation; CR: composite reliability; CA: Cronbach's alpha. The diagonal elements (in bold) represent the square root of AVE.

Table D2 Item Loadings and Cross-Loadings of First-Order Constructs

	Perceived Susceptibility	Perceived Severity	Perceived Detection Efficacy	Phishing Anxiety	Task-Focused Coping	Emotion-Focused Coping	Avoidance Coping	Detection Effort	Detection Accuracy
Susp1	**0.91**	0.18	-0.24	0.39	-0.06	0.26	0.28	-0.14	-0.16
Susp2	**0.89**	0.05	-0.24	0.35	-0.08	0.33	0.40	-0.24	-0.22
Cons1	0.08	**0.81**	0.09	0.17	0.25	-0.02	-0.14	0.08	0.00
Cons2	0.15	**0.94**	0.07	0.28	0.24	0.08	-0.07	-0.05	-0.01
Effi1	-0.25	0.08	**0.94**	-0.15	0.23	-0.21	-0.11	0.08	0.16
Effi2	-0.25	0.09	**0.94**	-0.17	0.24	-0.21	-0.07	0.04	0.17
Anxi1	0.34	0.26	-0.17	**0.91**	0.04	0.29	0.17	-0.06	-0.12
Anxi 2	0.25	0.20	-0.06	**0.78**	-0.01	0.22	0.17	-0.04	-0.12
Anxi 3	0.41	0.18	-0.14	**0.87**	-0.03	0.33	0.31	-0.13	-0.18
Anxi 4	0.40	0.24	-0.21	**0.91**	-0.05	0.35	0.25	-0.15	-0.19
Anxi 5	0.40	0.21	-0.16	**0.89**	-0.05	0.34	0.27	-0.14	-0.17
Anxi 6	0.29	0.32	-0.11	**0.82**	0.10	0.23	0.08	-0.01	-0.05
Anxi 7	0.35	0.25	-0.17	**0.90**	0.05	0.30	0.19	-0.08	-0.12
Task1	-0.10	0.26	0.22	-0.02	**0.91**	-0.13	-0.39	0.10	0.15
Task3	-0.03	0.23	0.23	0.04	**0.87**	-0.09	-0.29	0.09	0.11
Emot1	0.29	0.10	-0.17	0.37	-0.03	**0.76**	0.28	-0.09	-0.15
Emot2	0.23	0.01	-0.15	0.23	-0.11	**0.87**	0.38	-0.18	-0.26
Emot3	0.30	0.02	-0.25	0.28	-0.16	**0.88**	0.45	-0.20	-0.23
Avoi1	0.36	-0.07	-0.06	0.25	-0.29	0.41	**0.89**	-0.26	-0.22
Avoi2	0.25	-0.09	-0.09	0.17	-0.39	0.36	**0.88**	-0.26	-0.22
Avoi3	0.38	-0.11	-0.11	0.22	-0.35	0.41	**0.89**	-0.29	-0.27
Log(Time)	-0.21	0.00	0.07	-0.11	0.10	-0.19	-0.31	**1.00**	0.40
Correct %	-0.21	-0.01	0.18	-0.16	0.15	-0.26	-0.27	0.40	**1.00**

Appendix E

Table E1 A Horizontal Comparison Of Judgmental Accuracy Across Studies

Study	Research Profile	Judgmental task	Mean Detection Accuracy
Dhamija et al. (2006)	7 legitimate webs and 12 phishing websites	To identify legitimate and fraudulent sites and describe the reasoning for the decisions	61%
Downs et al. (2006)	3 legitimate emails and 5 phishing emails	To read and react to messages as one normally would in own life	79%
El-Din et al. (2014)	6 legitimate mobile messages and 6 phishing messages	To make a distinction between phishing messages and genuine ones	73%
Furnell (2007)	9 legitimate email messages and 11 illegitimate messages	To judge the legitimacy of each email	42% (and 26% "Don't know")
Sheng (2009)	10 legitimate websites and 10 phishing websites (see Chapter 5)	To state whether a web site is legitimate or phishing	69%
Sheng et al. (2007)	10 legitimate websites and 10 phishing websites (further divided into 2 subsets each containing 5 phishing websites and 5 legitimate websites)	To state whether a web site is legitimate or phishing,	Pre-training: 66%, 65%, and 69% for three treatment groups
Our study	8 legitimate emails and 8 phishing emails (randomly drawn from a pool of 25 legitimate and 25 phishing emails)	To judge whether an email is legitimate or not	67%