The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites

Ahmed Abbasi, David G. Dobolyi, Anthony Vance, and Fatemeh Mariam Zahedi

Appendix A – PFM Survey Instrument

Table A1: Survey Items for Tool Perceptions (all items on a scale of 1-10)

Construct	Items	Sources
Tool Usefulness	In evaluating the detection performance of the anti-phishing tool to assist me in successfully avoid phishing websites, I believe that the tool was: not helpful at all/very helpful for sure not valuable at all/very valuable for sure not useful at all/very useful for sure	New items informed by Venkatesh et al. 2003; Cranor 2008; Egelman et al. 2008
Tool Effort Required	When it comes to my efforts needed to follow the advice given by the anti-phishing tool, I believe that: the level of my inconvenience was (very low/very high) my time spent was (very low/very high) the extent of the interruption of my online activities was (very low/very high)	New items informed by Davis 1989; Venkatesh et al. 2003; Keith et al. 2009
Cost of Tool Error	When it comes to the cost of following a wrong recommendation made by the anti-phishing tool, I believe that: the extent of my loss was (very low/very high) the amount of money I lost was (very low/very high) In general, the consequence of errors made by the anti-phishing tool was (not severe at all/very severe for sure)	New items informed by Cavusoglu et al. 2005; Liang and Xue 2009

Table A2: Survey Items for Threat Perceptions (all items on a scale of 1-10)

Construct	Items	Sources
Phishing Awareness	When it comes to my awareness of phishing websites, I: don't know anything about them/ know a lot about them haven't heard about them at all/ have heard a lot about them for sure am not familiar with them at all/ am very familiar with them for sure	Zahedi et al. 2015
Perceived Phishing Severity	When it comes to the severity of damage due to phishing websites, I believe that: the extent of my potential damages due to phishing websites is (very low/very high)* my possible loss due to phishing websites is (very low/very high) for me, the extent of the negative consequences of phishing websites is (very low/very high)	Zahedi et al. 2015

Table A3: Survey Items for Prior Web Experiences

Construct	Items	Sources
Trust in Institution	When it comes to my trust in bank/pharmacy websites, I believe that such websites are: not trustworthy at all/very trustworthy for sure not reliable at all/very reliable for sure In general, my trust in bank/pharmacy websites is (very low/very high)	New items informed by Pavlou and Gefen 2004
Familiarity with Domain	When it comes to my familiarity with bank/pharmacy websites, I am (not familiar at all/very familiar for sure)	New item informed by Kumaraguru et al. 2010
Familiarity with Site	Please rate your familiarity with the following website: (very low/very high)	New item informed by Dhamija et al. 2006;

		Wu et al. 2006; Kumaraguru et al. 2010
Past Losses	When it comes to my past experiences with phishing websites: the negative consequences I have suffered due to such encounters are (none/very high) my losses due to phishing websites have been (none/very high) in general, my negative experiences due to phishing websites have been (none/very high)	New items informed by Downs et al. 2006

Appendix B – Exploratory Factor Analysis and Reliability Check of Survey Items

Table B1: Exploratory Factor Analysis of Tool Perception Survey Items

Construct	Items	1	2	3
Tool Usefulness	tu1	**0.96**	0.10	-0.03
	tu2	**0.97**	0.09	-0.02
	tu3	**0.98**	0.10	-0.01
Tool Effort Required	ter1	0.10	0.03	**0.94**
	ter2	0.01	0.06	**0.93**
	ter3	0.06	0.01	**0.95**
Cost of Tool Error	cte1	0.09	**0.98**	0.01
	cte2	0.12	**0.97**	0.07
	cte3	0.10	**0.97**	0.03
Eigenvalue		3.80	2.17	1.89
Cumulative Variance Explained (%)		40.47	66.01	86.78

Table B2: Exploratory Factor Analysis of Threat Perception Survey Items

Construct	Items	1	2
Phishing Awareness	pa1	**0.97**	0.01
	pa2	**0.96**	0.01
	pa3	**0.98**	0.02
Perceived Phishing Severity	pps1	0.01	**0.98**
	pps2	0.02	**0.99**
	pps3	0.00	**0.96**
Eigenvalue		3.21	2.72
Cumulative Variance Explained (%)		53.56	97.82

Table B3: Exploratory Factor Analysis of User Perception Survey Items

Construct	Items	1	2
Trust in Institution	ti1	**0.98**	0.02
	ti2	**0.98**	0.01
	ti3	**0.99**	0.02
Past Losses	pl1	0.01	**0.97**
	pl2	0.02	**0.96**
	pl3	0.03	**0.97**
Eigenvalue		3.16	2.61
Cumulative Variance Explained (%)		52.06	95.62

Table B4: Cross Loadings of Measurement Items to Latent Constructs

Construct	Item	1	2	3	4	5	6	7
Cost of Tool Error (1)	cte1	**0.90**	0.06	0.14	-0.02	0.21	-0.13	0.04
	cte2	**0.92**	0.05	0.11	-0.03	0.18	-0.24	0.03
	cte3	**0.89**	0.04	0.10	-0.01	0.27	-0.22	0.04
Past Losses (2)	pl1	0.09	**0.93**	0.16	0.12	0.08	0.05	-0.01
	pl2	0.07	**0.90**	0.14	0.11	0.12	0.03	-0.02
	pl3	0.06	**0.95**	0.15	0.08	0.14	0.02	-0.01
Perceived Phishing Severity (3)	pps1	0.10	0.14	**0.98**	0.07	0.05	0.09	0.04
	pps2	0.13	0.14	**0.97**	0.05	-0.04	0.10	0.02
	pps3	0.12	0.17	**0.87**	0.03	0.01	0.07	0.02
Phishing Awareness (4)	pa1	-0.03	0.14	0.09	**0.97**	-0.03	0.01	-0.01
	pa2	0.01	0.12	0.10	**0.65**	-0.01	0.03	0.00
	pa3	-0.02	0.11	0.09	**0.84**	-0.01	0.04	-0.01
Tool Effort Required (5)	ter1	0.23	0.09	-0.03	0.05	**0.87**	-0.03	0.04
	ter2	0.24	0.13	0.02	0.02	**0.84**	0.02	0.03
	ter3	0.18	0.14	-0.08	0.07	**0.80**	0.01	0.02
Tool Usefulness (6)	tu1	-0.19	0.10	0.05	0.00	-0.02	**0.96**	0.04
	tu2	-0.20	0.01	0.04	-0.02	-0.01	**0.95**	0.03
	tu3	-0.28	0.03	0.06	0.00	-0.03	**0.98**	0.02
Trust in Institution (7)	ti1	0.05	0.01	0.05	-0.05	0.04	0.03	**0.98**
	ti2	0.03	-0.04	0.06	-0.03	0.03	0.01	**0.95**
	ti3	0.02	-0.03	0.05	-0.04	0.01	0.02	**0.97**

Table B5: Correlation of the Latent Variable Scores with the Square Root of AVE

Construct	1	2	3	4	5	6	7
Cost of Tool Error (1)	**0.90**						
Past Losses (2)	0.06	**0.93**					
Perceived Phishing Severity (3)	0.12	0.13	**0.91**				
Phishing Awareness (4)	-0.01	0.10	0.03	**0.82**			
Tool Effort Required (5)	0.23	0.10	-0.02	0.04	**0.82**		
Tool Usefulness (6)	-0.20	0.05	0.08	0.02	-0.05	**0.95**	
Trust in Institution (7)	0.05	-0.01	0.06	-0.01	0.03	0.01	**0.96**

Table B6: Cronbach's Alpha Values for Survey Constructs

Construct	Cronbach's α
Tool Usefulness	0.98
Tool Effort Required	0.79
Cost of Tool Error	0.85
Phishing Awareness	0.88
Perceived Phishing Severity	0.91
Trust in Institution	0.98
Past Losses	0.90

Table B7: Summary Statistics for Prediction Field Study Variables (statistics were computed across the 12-month time period)

PFM Factors and Sub-categories		PFM Variables	Min	Max	Mean	Med.	Std. Dev.
Tool Factors	Tool Information	Tool Warning (1 = displayed)	0	1	0.96	1	-
		Tool Detection Rate (1 = high/FinOrg)	0	1	0.58	1	-
		Processing Time (in seconds)	0.35	3.13	1.52	1.61	0.65
	Tool Perceptions	Tool Usefulness	1	10	7.12	7.25	2.33
		Tool Effort Required	1	10	4.01	4.21	1.71
		Cost of Tool Error	1	10	4.88	4.67	2.40
Threat Factors	Threat Characteristics	Threat Domain – *Financial Services*	0	1	0.48	0	-
		Threat Domain – *Information*	0	1	0.18	0	-
		Threat Domain – *Retail*	0	1	0.11	0	-
		Threat Domain – *Entertainment*	0	1	0.05	0	-
		Threat Domain – *Prof. Services*	0	1	0.11	0	-
		Threat Domain – *Transportation*	0	1	0.02	0	-
		Threat Domain – *Health*	0	1	0.05	0	-
		Threat Type (1 = concocted)	0	1	0.28	0	-
		Threat Context	1	10	5.42	5.01	2.86
		Threat Severity (1 = high)	0	1	0.07	0	-
	Threat Perceptions	Phishing Awareness	1	10	5.44	5.56	2.25
		Perceived Severity	1	10	6.18	6.60	2.82
User Factors	Demographics	Gender (1 = female)	0	1	0.37	0	-
		Age	19	62	35.42	38	9.46
		Education	2	7	5.13	5	0.91
	Prior Web Experiences	Trust in Institution	1	10	6.45	6.55	1.39
		Familiarity with Domain	1	10	6.47	5.91	2.58
		Familiarity with Site	1	10	4.91	3.82	3.04
		Past Losses	1	10	2.38	1.77	1.71

Notes on Summary Statistics:

1. As noted in Table 4 in the main paper, there were two tool detection rate settings: 0 = LegOrg tool; 1 = FinOrg tool. The FinOrg tool had the higher observed detection rates. Approximately 58% of total user-phish encounters in the prediction field study occurred at FinOrg.
2. All tool perception, threat perception, and prior web experience variables were collected via the four quarterly surveys. Responses for these items (described in Appendix A) were on a 1-10 scale.
3. Since the seven threat domains were categorical, each category was dummy encoded.
4. See Table 4 in the main paper for details on how the threat context variable was range transformed to a 1-10 scale.
5. As discussed in Table 4 and Section 5.2.1 in the main paper, high severity threats were websites with malware. These accounted for slightly under 7% of all phishing instances in the field study.
6. Education was an ordinal response variable: some school, no degree = 1; high school graduate = 2; some college = 3; associate's/professional degree = 4; bachelor's degree = 5; master's degree = 6; doctoral degree = 7
7. Standard deviations are not reported for binary variables.

Appendix C – Additional Survey Items for Comparison Models

The additional survey items related to HITLSF, AAM, and DRKM appear in Table C1 below. For reader convenience, we also include a table showing the full set of variables included in all susceptibility models. As noted in the paper, threat domain, threat context, and threat type were added to all three comparison models (HITLSF, DRKM, and AAM) as fixed effects, as part of the CLMM mixed model to allow proper representation and comparison.

For HITLSF, we relied on the original conceptual models proposed by Cranor (2008) and Bravo-Lillo et al. (2011). Since HITLSF is a conceptual model that was not formally evaluated or operationalized (Cranor 2008; Bravo-Lillo et al. 2011), in addition to objective variables, we used our survey items to measure tool usefulness, knowledge, and experience (measured via phishing awareness and past losses). We also developed items for self-efficacy, trust in tool, and past encounters (added as an additional experience variable) based on prior IS literature. The survey items for self-efficacy, trust in tool, and past encounters are presented in Table C1. We discussed our survey items with one of the co-authors of Bravo-Lillo et al. (2011), and they felt that our operationalizations for perceptual items were reasonable.

Consistent with Alnajim and Munro (2009), for AAM, we used our phishing awareness items presented in Table A3 of Appendix A. For web-related technical abilities, we asked them for their items (which were not reported in their paper), and combined these with the technical ability items from DRKM (Sheng et al. 2010) since there was some overlap. These questions, appearing in Table C1, asked users about several Internet-related activities, including use of email, search engines, social networking sites, online banking, online shopping, etc. Users checked the boxes corresponding to activities they performed frequently. The average number of checked boxes was used as a measure of technical ability, standardized to a 1-10 scale.

For DRKM (Sheng et al. 2010), in addition to demographic variables (age, gender, and education), we used our survey items to measure past losses and phishing awareness. It is important to note three differences between our adaptation of DRKM and items included in the original study (Sheng et al. 2010). For technical ability, Sheng et al. (2010) used a self-reported survey item for technical savviness plus some additional technical ability items. In our piloting, we did not find this item to be as useful. Consequently, we combined their other technical ability items with the ones used in AAM. For risk propensity, Sheng et al. (2010) presented items from the risk-taking scale for adults (Blais and Weber 2006), with items such as riding a motorcycle without a helmet or betting a day's income at the horse races. However, with the exception of these two examples, they did not specify the specific items used in their instrument. Consequently, we instead used the risk propensity and security habit survey items depicted in Table C1. Furthermore, Sheng et al. (2010) also included a phishing training manipulation in which some groups were exposed to certain training materials. Incorporating such manipulations into our study was infeasible due to time constraints. However, we believe that this constitutes an important and interesting direction for future research. We discussed our survey items with one of the co-authors of Sheng et al. (2010) and they felt that our operationalizations for perceptual items were reasonable.

Table C1: Survey Items for Comparison Susceptibility Models (All Items Created for this Study)

Model	Construct	Values
HITLSF (Based on Cranor 2008; Bravo-Lillo et al. 2011)	Self-efficacy	When it comes to my ability to take protective actions against phishing websites, I believe that: my knowledge for taking protective actions is (not adequate at all/very adequate for sure) my ability to take protective actions is (very low/very high) for me, taking protective actions is (very difficult/very easy)
	Trust in Tool	When it comes to my trust in the anti-phishing tool, I believe that it is: not dependable at all/ very dependable for sure not reliable at all/ very reliable for sure not trustworthy at all/ very trustworthy for sure
	Past Encounters	When it comes to my past encounters with phishing websites: the number of my encounters has been (very low/very high) the number of phishing websites I visited has been (very low/very high) the frequency of my encounters with phishing websites has been (very low/very high)
AAM (Based on Alnajim and Munro 2011 and Sheng et al. 2010)	Technical Ability	Activities I am frequently involved in include: use of email services receiving RSS feeds searching for information using search engines playing online games or downloading music/videos visiting social networking sites shopping online (i.e., actually buying products/services) using online banking and/or investment websites
DRKM (Based on Sheng et al. 2010)	Risk Propensity	When it comes to my tendency to take risks, I believe that: my propensity to undertake risky propositions is (very low/very high) my tendency to choose riskier alternatives is (very low/very high) In general, my tendency to take risks is (very low/very high)
	Web Reliance	When it comes to my reliance on the Web, I believe that: the level of my dependence on the Web is (very low/very high) as part of my daily life, the Web is (not essential at all/very essential for sure) In general, my level of reliance on the Web is (very low/very high)
	Security Habit	When using the web, for me, taking security precautions is not in my nature at all/in my nature for sure not routine at all/very routine for sure not habitual at all/very habitual for sure

Table C2 provides a summary of which variables were incorporated in which models. Two variables (marked with an asterisk [*]) were included in all CLMM models to facilitate fair comparisons when constructing those models: a participant random intercept, i.e., (1|Participant); and a quadratic polynomial for ThreatContext to account for order effects, i.e., poly(ThreatContext, 2).

Table C2: List of Variables Used in Each of the Models

Model Term	PFM-CLMM	HITLSF	DRKM	AAM
(1|Participant)*	X	X	X	X
Age	X	X	X	
CostOfToolError	X			
Education	X	X	X	
FamiliarityWithDomain	X			
FamiliarityWithSite	X			
Gender	X	X	X	
PastEncounters		X	X	
PastLosses	X	X	X	
PerceivedPhishingSeverity	X			
PhishingAwareness	X	X	X	X
poly(ThreatContext, 2)*	X	X	X	X
RiskPropensity			X	
SecurityHabit			X	
SelfEfficacy		X		
TechnicalAbility			X	X
ThreatDomain	X			
ThreatSeverity	X			
ThreatType	X			
ToolDetectionRate	X			
ToolEffortRequired	X			
ToolProcessingTime	X			
ToolUsefulness	X	X		
ToolWarning	X	X		
TrustInInstitution	X			
TrustInTool		X		
WebReliance			X	

Note. * denotes terms included in all models beyond the fixed intercept term (i.e., 1 in Wilkinson-Rogers notation; Wilkinson and Rogers 1973). ThreatContext was not originally part of HITLSF, DRKM, and AAM.

References Appearing in Appendices

Alnajim, A., and Munro, M. (2009). Effects of Technical Abilities and Phishing Knowledge on Phishing Websites Detection. In Proceedings of the IASTED International Conference on Software Engineering, Austria, 120-125.

Blais, A. R. and Weber, E. U. (2006). A domain-specific risk taking (DOSPERT) scale for adult populations. *Judgment and Decision Making* 1(1), 33–47.

Bravo-Lillo, C., Cranor, L. F., Downs, J. S., and Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security and Privacy*, 9(2), 18-26.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2005). The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research*, 16(1), 28-46.

Cranor, L. (2008). A framework for reasoning about the Human in the Loop. *In Proceedings of the 1st Conference on Usability, Psychology, and Security*, Usenix Association.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, 13(3), 319–340.

Dhamija, R., Tygar, J. D., and Hearst, M. (2006). Why phishing works. *In Proceedings of the SIGCHI conference on Human Factors in computing systems*, Montreal, Canada, 581-590.

Downs, J. S., Holbrook, M. B., and Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *In Proceedings of the symposium on Usable privacy and security*, Pittsburgh, PA, 79-90.

Egelman, S., Cranor, L. F., and Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. *In Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems*, 1065-1074.

Keith, M., Shao, B., and Steinbart, P. (2009). A behavioral analysis of passphrase design and effectiveness. *Journal of the Association for Information Systems*, 10(2), 63-89.

Kumaraguru, P., Sheng, S., Aquisti, A., Cranor, L. F., and Hong, J. (2010). Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology*, 10(2), no. 7.

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

Pavlou, P. A., and Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1), 37-59.

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. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382.

Venkatesh, V., Morris, M., Davis, G. and Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), 397-423.

Wu, M., Miller, R. C. and Garfunkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? *In Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, Montreal, Canada, 601-610.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, *16*(6), 448.