Predicting User Susceptibility to Phishing Websites

David Dobolyi, Ahmed Abbasi, Mariam Zahedi, and Tony Vance

Abstract

User susceptibility to phishing websites is a significant security concern for organizations, both in terms of threats targeting employees and customer-facing attacks that undermine trust, satisfaction, and brand equity. At the root of the problem is the fact that users are ineffective at identifying and avoiding phishing websites. Even when using protective anti-phishing tools, many users remain vulnerable. Leveraging the observe-orient-decide-act (OODA) loop for decision-making in risky, adversarial, real-time environments, we develop a cumulative logit mixed model (CLMM) for predicting user susceptibility to phishing websites. The model incorporates relevant user, threat, and tool-related factors to predict decisions and actions pertaining to four key stages of the phishing process: visit, browse, consider legitimate, and intention to transact. In order to estimate the model, we used a cumulative link mixed model for representing users' decisions across funnel stages. We evaluated the proposed model relative to existing methods in two extensive laboratory experiments involving 1,388 participants and nearly 7,000 observations. Our model was significantly better at predicting users' phishing susceptibility behaviors, revealing that anti-phishing tool performance, tool perception, demographic, and prior experience-related variables were stronger indicators of users' phishing susceptibility relative to threat characteristic constructs, suggesting that existing training and education programs' emphasis on threat literacy might be misplaced.

Keywords: Phishing susceptibility, observe-orient-decide-act loop, predictive analytics, cumulative linked models, online security, longitudinal experiment

Introduction

Phishing—a type of semantic attack that exploits human as opposed to software vulnerabilities (Schneier 2000; Hong 2012)—is one of the most prevalent forms of cybercrime, impacting over 40 million Internet users every year (Symantec 2012; McAfee 2013; Verizon 2015). Phishing is consistently ranked as one of the top security concerns facing IT managers not only because of the number of employees falling prey to phishing attacks within organizations (Gartner 2011; Bishop et al. 2009; Siponen and Vance 2010; Cummings et al. 2012), but also because brand equity and trust are tarnished when companies' customers are targeted by spoof (i.e., fraudulent replica) websites (Hong 2012). The average 10,000 employee company spends approximately $3.7 million annually combating phishing attacks (Korolov 2015).

One potential solution to the phishing problem is the use of anti-phishing tools (Li and Helenius 2007; Abbasi et al. 2010; Zhang et al. 2014). Even when using these anti-phishing tools however, phishing success rates remain high because users often explain away or disregard tool warnings (Wu et al. 2006; Sunshine et al. 2009; Abbasi et al. 2012b; Akhawe and Felt 2013). Consequently, an effective solution to phishing prevention requires a better understanding of individuals' behavior, ideally leading to accurate prediction of user susceptibility (Downs et al. 2006; Bravo-Lillo et al. 2011). Such a solution would provide several benefits including: (1) improving curriculum for security education, training, and awareness (SETA) programs by identifying high-susceptibility factors; (2) promoting better usage of security technologies by addressing factors contributing to user-tool dissonance in SETA programs; and (3) personalizing access controls and data security policies using users' predicted susceptibility levels.

The research objective of this study is *to develop a model for predicting user susceptibility to phishing websites*. We adopted the design science paradigm (Hevner et al. 2004; Kitchens et al. 2018; Deng et al. 2019) to guide the development of the proposed model. Leveraging the observe-orient-decide-act (OODA) loop for decision-making in risky, adversarial, real-time environments as a kernel theory, our model emphasizes the importance of anti-phishing tool, phishing threat, and user-related factors in the decision-making process pertaining to four key funnel stages of the phishing attack: visit, browse, consider legitimate, and intend to transact. The model is estimated using a cumulative link mixed model that parsimoniously captures users' funnel stage decisions across multiple phishing website encounters.

This study addresses three important research gaps. First, we are unaware of prior work attempting to *predict* user susceptibility to phishing websites, as prior work has focused on developing or testing descriptive behavior models (e.g., Bravo-Lillo et al. 2011; Wang et al. 2012). The lack of predictive IT artifacts is a gap also noted by prior IS studies (Shmueli and Koppius 2011). Second, prior phishing studies and user susceptibility models have typically focused on a single decision or action such as considering a phishing website legitimate or being willing to transact with a phishing website (Grazioli and Jarvenpaa 2000; Dhamija et al. 2006; Sheng et al. 2010). However, falling prey to phishing website-based attacks entails a sequence of inter-related decisions and actions and thus modeling these sequences as a gestalt would provide deeper insight. Third, prior susceptibility models have placed limited emphasis on anti-phishing tool and phishing threat-related factors despite their considerable impact on susceptibility to phishing attacks (Wu et al. 2006; Dhamija et al. 2006; Akhawe and Felt 2013). From a design science perspective, our work represents a novel solution (Gregor and Hevner 2013; Goes 2014). Although phishing is a known problem, *predicting user susceptibility* to phishing attacks is a new challenge that falls under the umbrella of proactive "security analytics" recently emphasized by various academics and practitioners (Brown et al. 2015a; 2015b; Chen et al. 2012; Musthaler 2013; Taylor 2014; Abbasi et al. 2021). Accordingly, the knowledge contributions of our work can be considered both "improvement" and "innovation" based on recent design science guidelines (Gregor and Hevner 2013; Goes 2014). The proposed artifact and findings have important implications for IT security managers tasked with organizational security policies and procedures, security education, and training programs; the results are also important for Internet users in general.

Related Work

Traditionally, most of the research on anti-phishing has focused on benchmarking existing anti-phishing tools (Zhang et al. 2007; Abbasi and Chen 2009) and developing better detection capabilities (Li et al. 2009; Abbasi et al. 2010). Despite this research, phishing attacks have remained successful, so researchers and practitioners have increasingly turned their attention to user susceptibility. In recent years, several phishing susceptibility models have been proposed in an effort to describe the salient factors attributable to users' susceptibility to phishing attacks (Downs et al. 2006; Bravo-Lillo et al. 2011). A summary of these models is provided in Table 1.

Table 1: Select Prior Models for Internet Users' Susceptibility to Phishing Attacks

Model	**Study**	**Factors Incorporated**			**Susceptibility Criterion**
		Tool-Related	*User-Related*	*Threat-Related*	
Human-in-the-Loop Security Framework (HITLSF)	Cranor 2008; Bravo-Lillo et al. 2011	- Tool Warnings - Trust in Tool - Tool Usefulness	- Demographics - Knowledge and Experience - Self-Efficacy		Browsing phishing websites; Transacting with phishing websites
Ability and Awareness Model (AAM)	Alnajim and Munro 2009		- Technical Abilities - Phishing Awareness		Considering phishing websites legitimate
Phishing Susceptibility Framework (PSF)	Parrish Jr. et al. 2009		- Demographics - Knowledge and Experience - Personality Profile	- Threat Type	Likelihood of responding to phishing emails
Demographic, Risk, and Knowledge Model (DRKM)	Sheng et al. 2010		- Demographics - Risk Propensity - Knowledge and Experience		Considering phishing websites/emails legitimate or, conversely, considering legitimate websites/emails as phishing
Phishing Susceptibility Model (PSM)	Wang et al. 2012		- Demographics (controls) - Knowledge	- Visceral Cues - Deception Indicators - Detection Effort - Message Involvement	Likelihood of responding to phishing emails

The OODA-based CLMM for Predicting Susceptibility

As mentioned previously, we employed the observe-orient-decide-act (OODA) loop (Boyd 1976) to guide development of our proposed susceptibility prediction model, consistent with design science prescriptions for the development of IT artifacts, including constructs, models, methods, and instantiations (March and Smith, 1995; Hevner et al. 2004; Walls et al., 1992; Storey et al., 2008). The OODA loop—shown in Figure 1— was developed to explain the process guiding users' decision strategies when faced with risky, uncertain, and adversarial situations in combat operations (Boyd 1976). The loop is highly iterative: decisions and actions create new information and unfolding circumstances, resulting in the need for further observation, orientation, decision-making, and action (Brehmer 2005).

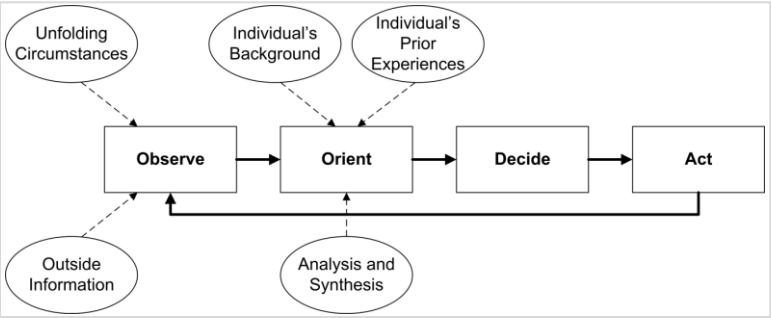

Figure 1: The Observe-Orient-Decide-Act (OODA) Loop

OODA was used to inspire the six categories of predictor variables in our model, operationalized via a cumulative link mixed model (CLMM). These categories relate to tool, threat, and user-related factors for the observe-and-orient stages of the OODA loop. The predictors drive ordinal response decisions for visiting, browsing, considering legitimate, and intending to transact with phishing websites. The OODA loop emphasizes the iterative nature of decision-making in situations involving risk and uncertainty. Once a decision is made and a corresponding action is undertaken (e.g., visiting the website), changes to the external environment warrant further observation and orientation, followed by subsequent decisions and actions that traverse the funnel further (e.g., whether or not to browse the website).

Table 2: Variables Related to the Observe-and-Orient Stages in Predictive Model

Category	Sub-category	Variables	References
Tool Factors	Tool Information	Tool Warning	Wu et al. 2006; Cranor 2008; Bravo-Lillo et al. 2011
		Tool Detection Rate	Abbasi and Chen 2009; Hong 2012
		Tool Run Time	Dhamija et al. 2006
	Tool Perceptions	Tool Usefulness	Moore and Benbasat 1991; Venkatesh et al. 2003; Cranor 2008; Egelman et al. 2008
		Tool Effort Required	Davis 1989; Venkatesh et al. 2003; Keith et al. 2009
		Cost of Tool Error	Cavusoglu et al. 2005; Liang and Xue 2009
Threat Factors	Threat Characteristics	Threat Domain	Grazioli and Jarvenpaa 2003; Bansal et al. 2008; Angst and Agarwal 2009
		Threat Type	Dhamija et al. 2006; Parrish Jr. et al. 2009
		Threat Severity	Lennon 2011; McAfee 2013; Zimbra et al. 2010
		Threat Context	Kaushik 2011; Vishwanath et al. 2011
	Threat Perceptions	Phishing Awareness	Downs et al. 2006; Alnajim and Munro 2009; Bravo-Lillo et al. 2011; Wang et al. 2012
		Perceived Phishing Severity	Downs et al. 2007; Camp 2009; Liang and Xue 2009; Zahedi et al. 2015
User Factors	Demographics	Gender	Venkatesh et al. 2003; Morris et al. 2005; Jagatic et al. 2007; Sheng et al. 2010; Netemeyer et al. 2020
		Age	Venkatesh et al. 2003; Morris et al. 2005; Cranor 2008; Parrish Jr. et al. 2009; Sheng et al. 2010
		Education	Porter and Donthu 2006; Sheng et al. 2010
	Prior Web Experiences	Trust in Institution	Pavlou and Gefen 2004; Zahedi et al. 2011a; 2011b
		Familiarity with Domain	Kumaraguru et al. 2010
		Familiarity with Site	Dhamija et al. 2006; Wu et al. 2006; Kumaraguru et al. 2010
		Past Losses	Downs et al. 2006

Guided by OODA, the model considers objective and perceptual factors pertaining to user, tool, and threat-related categories. During the observe stage, the unfolding circumstances include exposure to *threat characteristics,* such as the URL and anchor text prior to visiting (Wang et al. 2012), and the website itself prior to browsing (Bravo-Lillo et al. 2011). Outside information encompasses anti-phishing *tool information,* such as warnings and false negatives (Wu et al. 2006; Zhang et al. 2007). During the orientation stage, user-related factors such as *demographics* and *prior web experiences* influence analysis and synthesis (Cranor 2008; Sheng et al. 2010). Analysis and synthesis also involve perpetual considerations such as *tool and threat-related perceptions* (Wu et al. 2006; Dhamija et al. 2006). Table 2 presents an overview of the three categories of factors impacting the observe-and-orient stages, their sub-categories, and associated variables.

Evaluation

Table 3 summarizes two experiments we conducted to answer the following research questions:

1. How effectively can our proposed OODA-based CLMM model explain user phishing susceptibility relative to existing models?
2. Which tool, threat, and/or user categories within our model can significantly enhance our understanding of users' funnel stage behavior?
3. How effectively can the model predict users' susceptibility to phishing websites?

Table 3: Summary of Two Experiments

Laboratory experiment	University students & faculty; general public	908; 4,540	Cross-sectional	Intention to transact with phishing website
Laboratory experiment	Customers of a B2C Security Provider	480; 2,400	Cross-sectional	Intention to transact with phishing website

Experiment 1: Model Fit Evaluation of OODA-based CLMM

We performed a laboratory experiment to evaluate the fit performance for our model versus existing models (RQ1), as well as the additive impact of individual user, tool, and threat variables (RQ2). Data was collected from a total of 908 students, university staff, and the general public at two cities in the US who each encountered five phishing URLs, resulting in 4540 total data points. The mean age was 24.4, with approximately 15.5% over the age of 30. With respect to gender, 40.6% were female, and 28.1% of participants had attained a college degree.

Experimental Design

Our key experimental variables are summarized in Table 4: threat domain (bank or pharmacy), threat type (concocted or spoof), tool detection rate (90% or 60%), tool run-time (1s or 4s), and threat severity (high or low). This yielded 32 experimental conditions ($2 \times 2 \times 2 \times 2 \times 2$).

Table 4: Operationalization of Experiment 1 Study Variables

Variable	Inclusion Rationale and Details
Threat Domain: Banks and Pharmacies	Both banks and pharmacies are areas where phishing attacks are pervasive. Financial institution websites are among the most common category for phishing attacks (Ramzan and Wuest 2006; Prince 2009), and similarly, studies conducted by the World Health Organization and U.S. Food and Drug Administration have found that 11,000 of the 12,000 online pharmacies they examined represented phishing (Hellerman 2013). The number of people visiting such websites continues to increase dramatically (Krebs 2005; Easton 2007; Greenberg 2008). In the online pharmacy domain, the experimental task was to purchase Rogaine, a popular over-the-counter hair restoration drug, for an elderly family member. This product was chosen because it is familiar, carried by all online pharmacies, and often sold by phishing websites. In the online banking domain, the experimental task was to open an online savings account, which is a relevant and basic online function provided by most banks that is commonly performed online (Freed 2011).
Threat Type: Concocted or Spoof	Concocted and spoofed sites used in the experiment were replicas of actual sites reported by non-profit anti-phishing organizations PhishTank and LegitScript. See section 3.1.3 for clarification on the difference between concocted and spoof and/or the Appendix for additional details.
Tool Detection Rate: High or Low	We operationalized high and low settings as 90% and 60%, respectively, to be consistent with the range typically found in the literature as discussed in section 3.1.1. Tool warnings for both settings were simulated using actual tool performance; see the Appendix for details.
Tool Run Time: Fast or Slow	As discussed in section 3.1.1, findings from anti-phishing tool benchmarking studies have shown that existing tools have run times ranging from just under 1s to slightly over 3s (Chou et al. 2004; Abbasi and Chen 2009). Accordingly, we used tool run times of 1s (fast) and 4s (slow).
Threat Severity: High or Low	As previously noted in section 3.1.3, median losses attributable to phishing in B2C contexts vary on an order of magnitude depending on whether the losses encompass only direct monetary losses or also include identity theft (i.e., $300 versus $3000; Lennon 2011; McAfee 2013). In order to operationalize these possible costs, we provided subjects with a virtual cash box of $200 and a damage cost (per error) of either $1 (low threat severity) or $10 (high threat severity). Subjects were made aware of their remaining cash box balance at the end of the experiment.

Experimental Procedure

First, participants completed a pre-experiment survey asking about their tool and threat perceptions, demographics, and prior web experiences. These independent variables correspond to ones listed previously in Table 2. Next, each user was randomly assigned to one of the 32 experimental conditions discussed in the prior section. Each participant encountered 10 URLs from the pharmacy or bank domain presented in randomized order as a page of search engine results; we chose this format not only because Internet users spend considerable time using search engines (Goel et al. 2012), but also because search engines have consistently been exploited by phishing and other types of illicit websites (Gyongyi and Garcia-Molina 2005; Catan 2011; Selinger 2013). Five of the 10 URLs displayed were for legitimate sites while the other 5 were for phishing sites; the 5 phishing URLs were either all concocted or all spoof, depending upon random assignment.

Participants were provided an anti-phishing tool with either a fast (1s) or slow (4s) run time. The tool triggered each time the user clicked on any of the 10 URLs. If the tool considered the URL to be a phish, the user's web browser redirected to a standard Microsoft Internet Explorer warning page; at this point, participants had the option of either (1) heeding the warning and returning to the URL list without visiting the site or (2) ignoring the warning and proceeding to the website by clicking on a URL on the warning page. URLs deemed legitimate by the tool were displayed in the web browser without a warning.

For each URL, Participants were asked whether they considered the website legitimate and if they would consider transacting with the website. Furthermore, web analytics software was used to deduce

whether they visited and/or browsed the URL. Users were scored based on their performance with respect to decisions made and actions undertaken in regards to the 10 URLs. More specifically, performance was evaluated based on users' decisions to visit or avoid the 5 phishing websites, to consider phishing websites legitimate (or legitimate websites as phish), and willingness to transact with the 5 phishing sites (Grazioli and Jarvenpaa 2000; Dhamija et al. 2006; Wu et al. 2006). Based on their performance, participants were paid a minimum of $10 and a maximum of $30. The experiment task had to be finished within a time frame of 20 minutes (Herzberg and Jbara 2008). This time frame was established by pre-testing and pilot testing to ensure that the allotted time was reasonable for performing the necessary tasks.

Comparison of OODA-based CLMM versus Existing Susceptibility Models

Model comparisons are important for understanding the state-of-the-art, identifying challenges, and exploring the operational utility of opportunities (Zimbra et al. 2018). Based on our review of existing phishing susceptibility models, three comparison models were also evaluated: Human-in-the-Loop Security Framework (HITLSF; Cranor 2008); Ability and Awareness Model (AAM; Alnajim and Munro 2009); and Demographic, Risk, and Knowledge Model (DRKM; Sheng et al. 2010). Appropriate items pertaining to these models' constructs were included in the survey instrument.

All models were evaluated using a mixed effects approach to concordant with our experimental design and evaluated following multi-model comparison guidelines outlined by Burnham and Anderson (2002) as well as recommendations from within the IS literature (e.g., Shmueli and Koppius 2011; Vance et al. 2015). We used Akaike Information Criterion (AIC) and Bayesian Information Criterion (BIC) as evaluation metrics. To demonstrate the utility of the six variable categories incorporated in our OODA-based CLMM estimation method, we fit all models using both flexible (CLMM-Flex) and equidistant (CLMM-Equi) thresholds (Christensen 2015).

Table 5: AICs and BICs for the Competing Models using CLMMs

Model	Model Type	df	AIC	ΔAIC	BIC	ΔBIC
OODA	CLMM Flexible	26	12605.60	0.00	12772.53	0.00
HITLSF	CLMM Flexible	19	12765.46	159.86	12887.45	114.92
DKRM	CLMM Flexible	19	12962.78	357.18	13084.77	312.23
AAM	CLMM Flexible	11	12966.48	360.88	13037.10	264.57
Null	CLMM Flexible	6	12983.03	377.44	13021.56	249.02
OODA	CLMM Equidistant	24	13504.21	898.62	13658.31	885.77
HITLSF	CLMM Equidistant	17	13665.26	1059.66	13774.41	1001.87
DKRM	CLMM Equidistant	17	13858.50	1252.90	13967.65	1195.11
AAM	CLMM Equidistant	9	13863.57	1257.97	13921.35	1148.82
Null	CLMM Equidistant	4	13881.00	1275.41	13906.68	1134.15

Table 5 shows the model comparison results sorted in descending order based on AIC. The OODA-CLMM outperformed all other models within each threshold type, and the ΔAIC differences between models were consistently non-trivial. Additionally, all flexible threshold models outperformed all equidistant counterparts, suggesting that users' perceptions regarding decision threshold across funnel stages are unevenly spaced. The observed funnel stage traversal frequencies (left chart) and percentages (right funnel) are depicted in Figure 3. Participants were most likely to stop traversing the funnel at the first, third, and fifth funnel stages. Because these frequencies indicate final stopping points, it is worth noting that although many users elected to not visit the phishing websites, those that did visit were highly likely to browse and/or exhibit an intention to transact, consistent with prior studies (e.g. Grazioli and Jarvenpaa 2000; Jagatic et al. 2007).

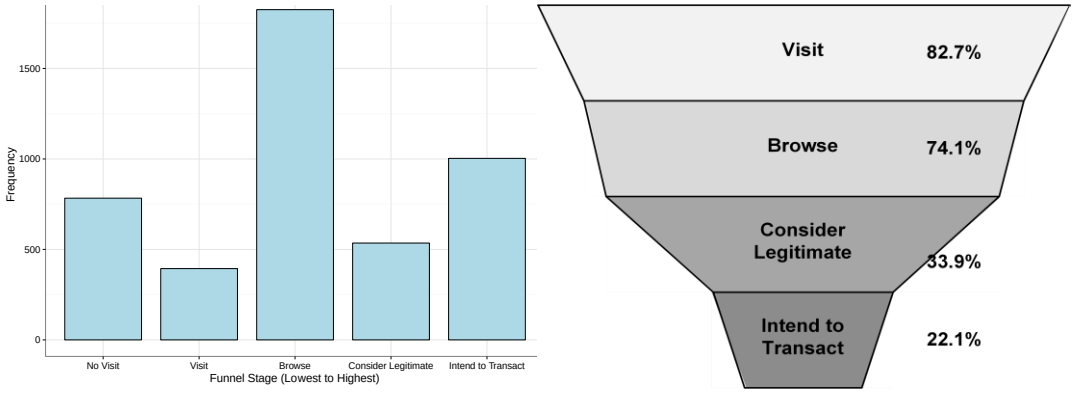

Figure 3: Ordinal Response DV Traversal Statistics Across User-Phish Encounters

Table 6: Likelihood Ratio Tests for Impact of OODA-CLMM Subcategories

Subcategory	df	AIC	ΔAIC	LR	p	
Tool Performance	3	12734.82	129.22	135.22	0.00	***
Tool Perceptions	2	12732.19	126.59	132.59	0.00	***
Prior Web Experience	4	12662.80	57.21	65.21	0.00	***
Threat Characteristics	3	12655.30	49.71	55.71	0.00	***
Demographics	3	12611.31	5.72	11.72	0.01	**
Threat Perceptions	3	12603.08	-2.52	1.48	0.48	

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

OODA-CLMM Subcategory Comparison Results

In order to evaluate the benefit of the user, tool, and threat-related variable subcategories within OODA-CLMM, we conducted a series of chi-square comparisons that compared the full model to ones in which an entire subcategory of predictors was excluded, as shown in Table 6. The AIC of the full model was 12605.60, which represents the baseline in the ΔAIC column; higher positive ΔAIC values for a dropped subcategory indicate greater value of that subcategory within the saturated model. P-values for the LRTs were computed based on the χ^2 statistic. The table is sorted in descending order relative to the likelihood ratio (LR) statistic. Overall, tool-related subcategories offer the greatest explanatory potential.

We also examined the significance of fixed effect model terms within our model using LRTs in which individual terms were dropped from the saturated model as shown in Table 7. Again, the AIC of the full model was 12605.60, which represents the baseline for ΔAIC; higher positive ΔAIC values indicate a greater benefit of including the term. A summary of the significant terms is presented in Table 8, with two illustrative effect plots also provided in Figure 4.

Table 7: Likelihood Ratio Tests for Impact of Individual Variables in the OODA-CLMM

Description	Category	Subcategory	df	AIC	ΔAIC	LR	p
Tool Run Time	Tool Factors	Tool Performance	1	12604.25	-1.35	0.65	.42
Tool Warning	Tool Factors	Tool Performance	1	12698.05	92.45	94.45	.00 ***
Tool Detection Rate	Tool Factors	Tool Performance	1	12618.50	12.90	14.90	.00 ***
Tool Effort Required	Tool Factors	Tool Perceptions	1	12605.78	0.18	2.18	.14
Cost of Tool Error	Tool Factors	Tool Perceptions	1	12687.53	81.93	83.93	.00 ***
Tool Usefulness	Tool Factors	Tool Perceptions	1	12628.95	23.35	25.35	.00 ***
Threat Domain	Threat Factors	Threat Characteristics	1	12603.85	-1.75	0.25	.61
Threat Type	Threat Factors	Threat Characteristics	1	12604.29	-1.30	0.70	.40
Threat Severity	Threat Factors	Threat Characteristics	1	12658.25	52.66	54.66	.00 ***
Phishing Awareness	Threat Factors	Threat Perceptions	1	12604.96	-0.63	1.37	.24
Perceived Phishing Severity	Threat Factors	Threat Perceptions	1	12603.66	-1.94	0.06	.81
Age	User Factors	Demographics	1	12604.20	-1.40	0.60	.44
Gender	User Factors	Demographics	1	12611.76	6.16	8.16	.00 **
Education	User Factors	Demographics	1	12603.90	-1.70	0.30	.58
Trust in Institution	User Factors	Prior Web Experience	1	12610.39	4.79	6.79	.01 **
Familiarity with Domain	User Factors	Prior Web Experience	1	12609.22	3.63	5.63	.02 *
Familiarity with Site	User Factors	Prior Web Experience	1	12660.56	54.97	56.97	.00 ***
Past Losses	User Factors	Prior Web Experience	1	12605.14	-0.46	1.54	.21
Order	Control	Control	2	12617.69	12.09	16.09	.00 ***

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Table 8: Summary of Significant OODA-CLMM Model Terms

Description	Category	Effect
Tool Warning	Tool Factors: Tool Performance	Tool warnings increased the likelihood of no-visit and decreased the probability of consider legitimate and intend to transact.
Tool Detection Rate	Tool Factors: Tool Performance	Higher tool accuracy increased the likelihood of no-visit and decreased the probability of consider legitimate and intend to transact.
Cost of Tool Error	Tool Factors: Tool Perceptions	Higher perceived cost of tool error increased the likelihood of ignoring the tool and considering legitimate and intending to transact.
Tool Usefulness	Tool Factors: Tool Perceptions	Higher perceived tool usefulness increased the likelihood of no-visit and decreased the probability of consider legitimate and intend to transact.
Threat Severity	Threat Factors: Threat Characteristics	Higher threat severity increased likelihood of no-visit and decreased probability of consider legitimate and intend to transact.
Gender	User Factors: Demographics	Females show an increased likelihood of no-visit and decreased probability of consider legitimate and intend to transact, in contrast to prior studies suggesting that women are more susceptible to phishing attacks (Sheng et al. 2010; Halevi et al. 2013); however, unlike our study, these studies did not provide an anti-phishing tool, and work has shown women may be more likely to heed tool warnings (Morris et al. 2005).
Trust in Institution	User Factors: Prior Web Experience	Higher trust in institution increased the likelihood of considering legitimate and intending to transact.
Familiarity with Domain	User Factors: Prior Web Experience	Higher familiarity with domain increased the likelihood of no-visit and decreased the probability of consider legitimate and intend to transact.
Familiarity with Site	User Factors: Prior Web Experience	Higher familiarity with site increased the likelihood of considering legitimate and intending to transact.

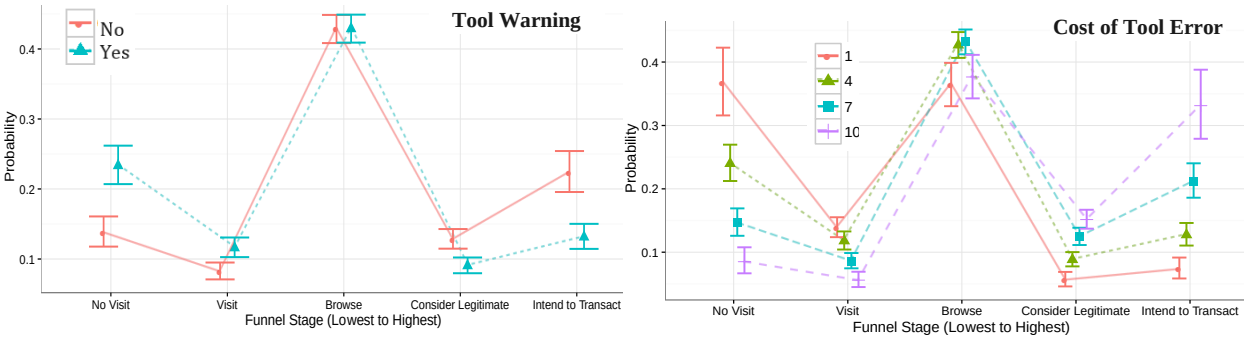

Figure 4: The Effect of Tool Warning (left) and Cost of Tool Error (right) on Funnel Stage Traversal

Experiment 2: Predictive Evaluation of OODA-CLMM

Our third research question asked, "How effectively can our model predict users' susceptibility to phishing websites?" As previously noted, accurately predicting funnel end stages for various user-phish encounters could facilitate proactive anti-phishing strategies pertaining to security training and personalized access control policies. Because evaluation of predictive IT artifacts requires assessing accuracy of out-of-sample predictions (Shmueli and Koppius 2011), we conducted a second laboratory experiment involving a new sample of 490 individual customers of in the San Francisco Bay Area. This sample was chosen to enhance the generalizability relative to the university sample used in Experiment 1.

As with Experiment 1, participants were recruited via email offering $10, with the possibility of earning up to $30 for a 20-minute experiment. The same pre-survey and experimental design from Experiment 1 were used to collect data from these "test-set" participants. Experiment 2 included 480 usable participants who each contributed data on 5 phishing URLs encountered, resulting in 2400 total data points. Their mean age was 31.6, 40.1% were female, and 48.8% had attained a college degree.

Two analyses were conducted. In the first, we evaluated the predictive power of OODA-CLMM relative to the competing DRKM, AAM, and HITLSF models. In the second, we compared the model with existing benchmark methods for behavior prediction using the same set of variables; these methods included Bayesian Network (BayesNet), Support Vector Machines (SVMs), a CLMM variant with equidistant thresholds and a linear mixed model (LMM) baseline. Given that predicting users' end funnel stages is an imbalanced multi-class classification problem, we employed multi-class receiver operating characteristic (ROC) curves and area-under-the-curve (AUC; Hand and Till 2001; Fawcett 2006) to assess predictive model tradeoffs between true positives and false positives (Bardhan et al. 2015). The use of these measures is consistent with prior design science studies pertaining to predictive artifacts (Prat et al. 2015). All models were trained using the 908-participant data from Experiment 1 and tested on the 480 subjects' phishing encounters from Experiment 2.

Comparing OODA-CLMM's Predictive Capabilities to Existing Susceptibility Models

Table 9 presents the AUC values from both analyses, which range from 0.5 to 1; higher values indicate better performance. Our model outperformed the three other susceptibility models (i.e., HITLSF, DRKM, and AAM) in terms of predictive power with an AUC 30% to 50% higher than its peers. OODA-CLMM also outperformed the comparison prediction methods (i.e., SVM, CLMM-Equi, BayesNet, and LMM) with an AUC lift between 8% and 30% relative to these competitors. In order to quantify the practical significance of a 30% lift in susceptibility prediction, recall that that the average 10,000 employee company spends $3.7 million annually dealing with phishing attacks, including the cost of malware, productivity losses, etc. (Korolov 2015). For such an organization, proactive detection of phishing susceptibility could reduce phishing-related expenses by over $1 million annually, and this number does

not even take into account the bigger picture involving loss mitigation relative to reputation and brand equity-related costs.

Table 9: AUC Values on Prediction ROC Curves for OODA-CLMM and Comparison Methods

Method	AUC
OODA-CLMM	0.7851
CLMM-Flex-HITLSF	0.6028
CLMM-Flex-DRKM	0.5318
CLMM-Flex-AAM	0.5211
SVM	0.7280
CLMM-Equi	0.7088
BayesNet	0.6663
LMM	0.6098

Figure 5 depicts the multi-class ROC curves for OODA-CLMM and comparison models (left) and methods (right), with the y-axis indicating true positives and the x-axis representing false positives. Curves closer to the top left corner signify better performance due to higher ratios of true positives relative to false positives. From Figure 5 it is again evident that OODA-CLMM garnered better predictive performance compared to all other models and methods, with higher true positive rates for virtually every level of false positives, lending further credence to our model's effectiveness. By incorporating tool, threat, and user-related variables, OODA-CLMM is better able to model and predict user decisions and actions pertaining to various stages of the phishing funnel relative to existing susceptibility models. In addition, the model's use of CLMM-Flex enables it to outperform all comparison prediction methods.

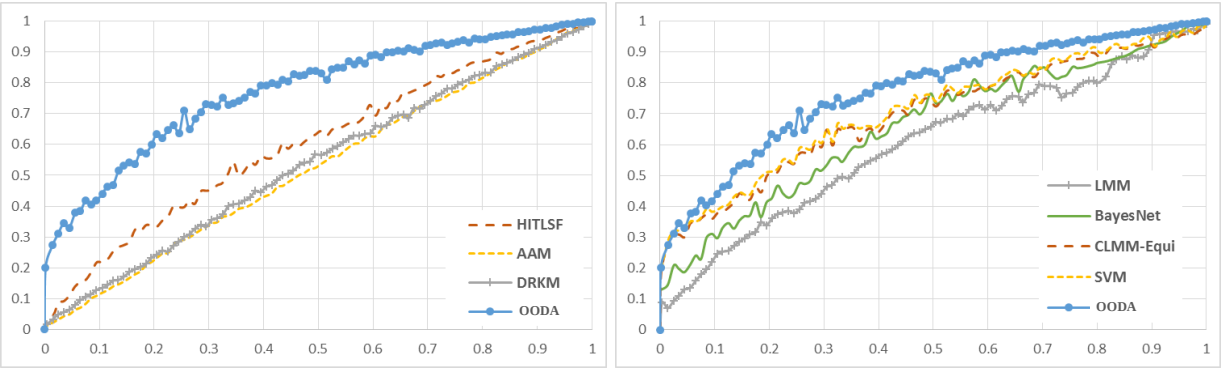

Figure 5: ROC Curves of Funnel Stage Predictions Across Models and Methods

Discussion and Conclusions

Our three experiments demonstrate the utility of OODA-CLMM, which incorporates tool, threat, and user-related variables to model the interplay between phishing funnel stages and user decisions guided by principles of the OODA loop kernel theory and estimated using a CLMM-Flex method capable of parsimoniously considering user-phishing interactions and funnel stage traversal behaviors. Table 10 summarizes our key findings.

The development of our method follows guidelines mentioned in recent design science papers, which promote the development of novel design artifacts (Gregor and Hevner 2013; Goes 2014). Based on these guidelines, out method's enhanced phishing susceptibility model performance represents an "improvement" contribution over existing models, better addressing the problem of understanding user susceptibility to phishing website attacks. Given the lack of prior work on prediction of user susceptibility, OODA-CLMM's contribution also embodies elements of "innovation" since security behavior prediction is a relatively new problem.

We also make several contributions to the online security domain. The predictive possibilities afforded by OODA-CLMM have important implications for various practitioner groups, particularly in light of the recent industry trend towards security analytics (Chen et al. 2012; Musthaler 2013; Taylor 2014). Our findings could be leveraged in several ways towards future employee and/or customer-facing anti-phishing strategies, including custom training programs for potential high-susceptibility users, personalized security policies and procedures, and inclusion of customized warnings in anti-phishing tools. Future work can extend our study in several ways. Our threat variables did not include many advanced network and signature-based features (Fu et al. 2010; Koepke et al. 2012; Benjamin et al. 2013; Benjamin et al. 2014). Susceptibility might also be impacted by design elements of the anti-phishing warnings (Chen et al. 2011; Chen et al. 2021). Follow-up work could also examine susceptibility in other phishing domains (Dobolyi and Abbasi 2016). In conclusion, we believe the current study constitutes an important first step towards improving predictions of user susceptibility to phishing—a problem that continues to exact significant monetary and social costs.

Table 10: Summary of Key Findings Pertaining to Proposed OODA-CLMM

Research Question	**Key Results**
RQ1: How effectively can our proposed OODA-based CLMM model explain user phishing susceptibility relative to existing models?	By parsimoniously including phishing funnel stages, mixed effects, and flex thresholds, the OODA-based model better explains users' phishing funnel stage behavior relative to existing models.
RQ2: Which tool, threat, and/or user categories within our model can significantly enhance our understanding of users' funnel stage behavior?	• Tool performance and perception variables were most influential, followed by users' prior experiences, threat characteristics, and demographics. This finding has important implications for training programs that focus predominantly on threat-related education. • As expected, tool warnings and overall detection rates are essential deterrents to extended funnel traversal. Similarly, tool perceptions such as usefulness encourage warning adherence, whereas perceived cost of tool error increases likelihood of considering phishing sites legitimate and intending to transact • In general, threat characteristic and perception variables were not significant – except threat severity. • Consistent with prior studies, gender was a significant consideration. However, in contexts involving tools, men are more likely to traverse deeper stages of the phishing funnel. • Institutional trust and site familiarity both increased the likelihood of considering legitimate and intending to transact. These predispositions are often exploited in spoofing attacks.
RQ3: How effectively can the model predict user susceptibility to phishing websites?	OODA-CLMM outperformed existing susceptibility models and machine-learning-based prediction methods, attaining an 8% to 30% lift in AUC. Given the hefty costs associated with phishing in both organizational and household settings, proactive susceptibility detection could result in significant monetary savings and social benefits.

References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., and Nunamaker Jr., J. F. (2010). Detecting Fake Websites: The Contribution of Statistical Learning Theory. *MIS Quarterly*, 34(3), 435-461.

Abbasi, A. and Chen, H. (2009). A Comparison of Tools for Detecting Fake Websites. *IEEE Computer*, 42(10), 78-86.

Abbasi, A., Zahedi, F., and Kaza, S. (2012a). Detecting Fake Medical Web Sites Using Recursive Trust Labeling. *ACM Transactions on Information Systems*, 30(4), no. 22.

Abbasi, A., Zahedi, F. M., and Chen, Y. (2012b). Impact of anti-phishing tool performance on attack success rates. *In Proceedings of the IEEE International Conference on Intelligence and Security Informatics*, 12-17.

Abbasi, A., Lau, R. Y., and Brown, D. E. (2015). Predicting behavior. *IEEE Intelligent Systems*, 30(3), 35-43.

Abbasi, A., Dobolyi, D.,Vance, T., and Zahedi, F. M. (2021). The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites, *Information Systems Research*, forthcoming.

Brown, D. E., Abbasi, A., and Lau, R. Y. K., (2015a). Predictive Analytics: Predictive Modeling at the Micro Level, *IEEE Intelligent Systems*, 30(3), pp. 6-8.

Brown, D. E., Abbasi, A., and Lau, R. Y. K., (2015b). Predictive Analytics, *IEEE Intelligent Systems*, 30(2), pp. 6-8.

Akhawe, D. and Felt, A. P. (2013). Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In Proceedings of the 22nd USENIX Security Symposium.

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, Innsbruck, Austria, 120-125.

Angst, C. M. and Agarwal R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion, *MIS Quarterly*, 33(2), 339-370.

Bansal, G. Zahedi, F. M. and Gefen, D. (2010). The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online. *Decision Support Systems*, 49(2), 138-150.

Bardhan, I., Oh, J. H., Zheng, Z., and Kirksey, K. (2015). Predictive Analytics for Readmission of Patients with Congestive Heart Failure. *Information Systems Research*, 26(1), 19-39.

Bazerman, M. H., and Moore, D. A. (2008). *Judgment in Managerial Decision Making*. 7th edition, New York: Wiley.

Benjamin, V., Chung, W., Abbasi, A., Chuang, J., Larson, C., and Chen, H. (2013). "Evaluating Text Visualization: An Experiment in Authorship Analysis," In the *11th IEEE International Conference on Intelligence and Security Informatics (IEEE ISI)*, Seattle, Washington, June 4-7.

Benjamin, V., Chung, W., Abbasi, A., Chuang, J., Larson, C. A., and Chen, H. (2014). Evaluating Text Visualization for Authorship Analysis, *Security Informatics*, 3(10), 2014.

Bishop, M., Engle, S., Peisert, S., Whalen, S., and Gates, C. (2009). Case Studies of an Insider Framework. *In Proceedings of the 42nd Hawaii International Conference on System Sciences*, 1-10.

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.

Boyd, J. R. (1976). Destruction and creation. *A Discourse on Winning and Losing*.

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.

Brehmer, B. (2005). The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control. *In Proceedings of the 10th International Command and Control Research and Technology Symposium*, 1-15.

Camp, L. J. (2009). Mental models of privacy and security. *IEEE Technology and Society Magazine*, 28(3), 37-46.

Catan, T. (2011). Google Forks Over Settlement on Rx Ads, *The Wall Street Journal*, August 25.

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.

Chen, H., Chiang, R. H., and Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, 36(4), 1165–1188.

Chen, Y., Zahedi, F. M., Abbasi, A., and Dobolyi, D. (2021). Trust Calibration of Security IT Artifacts: A Multi-Domain Study of Phishing-Website Detection Tools, *Information and Management*, conditionally accepted.

Chen, Y., Zahedi, F. M., and Abbasi, A. (2011). Interface Design Elements for Anti-Phishing Systems, *In the 6th International Conference on Design Science Research in Information Systems and Technology (DESRIST)*, Milwaukee, Wisconsin, May 5-6.

Chou, N. Ledesma, R., Teraguchi, Y., Boneh, D. and Mitchell, J. C. (2004). Client-side Defense Against Web-based Identity Theft. *In Proceedings of the Network and Distributed System Security Symposium*.

Christensen, R. H. B. (2015). Analysis of ordinal data with cumulative link models—estimation with the ordinal package. *R-package version*, *13*.

Chua, C. E. H. and Wareham, J. (2004). Fighting Internet Auction Fraud: An Assessment and Proposal," *IEEE Computer* 37(10), 31–37.

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.

Cummings, A., Lewellen, T., McIntire, D., Moore, A., and Trzeciak, R. (2012). Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector, *Software Engineering Institute*, Carnegie Mellon University, (CMU/SEI-2012-SR-004).

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

Deng, S., Zhang, P., Zhou, Y., and Abbasi, A. (2019). Using Discussion Logic in Analyzing Online Group Discussions: A Text Mining Approach, *Information and Management*, 56(4), pp. 536-551.

Dennis, A. R., and Valacich, J. S. (2001). Conducting experimental research in information systems. *Communications of the Association for Information Systems*, 7 (5), pp. 1-41.

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.

Downs, J. S., Holbrook, M., and Cranor, L. F. (2007). Behavioral response to phishing risk. *In Proceedings of the ACM Anti-phishing working groups annual eCrime researchers summit*, 37-44.

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.

Dinev, T. (2006). Why spoofing is serious Internet fraud. *Communications of the ACM*, 49(10), 76-82.

Dobolyi, D. and Abbasi, A. (2016). PhishMonger: A Free and Open Source Public Archive of Real-World Phishing Websites, *In the 14th IEEE International Conference on Intelligence and Security Informatics (IEEE ISI)*, Tucson, Arizona, Sept. 27-30.

Easton, G. (2007). Clicking for Pills, *British Medical Journal* (334: January 6), 14-15.

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.

Fawcett, T. (2006). An introduction to ROC analysis. *Pattern recognition letters*, 27(8), 861-874.

Fu, T., Abbasi, A., and Chen, H. (2010). A Focused Crawler for Dark Web Forums, *Journal of the American Society for Information Science and Technology*, 61(6), 2010, pp. 1213-1231.

Freed, L. (2011). Managing Forward: Customer Satisfaction as a Predictive Metric for Banks. *U.S. ForeSee Results 2011 Online Banking Study*, May 18.

Gartner, (2011). Magic Quadrant for Web Fraud Detection, April 19, 2011.

Gefen, D. and Straub, D. (1997). Gender Differences in the Perception and Use of E-Mail: An Extension to the Technology Acceptance Model, *MIS Quarterly*, 21(4), 389-400.

Goel, S., Hofman, J. M., and Sirer, M. I. (2000). Who Does What on the Web: A Large-scale Study of Browsing Behavior, *In Proceedings of the 6th International Conference on Weblogs and Social Media*.

Goes, P. (2014). Editor's Comments: Design Science Research in Top Information Systems Journals, *MIS Quarterly*, 38(1), iii-viii.

Grazioli, S., and Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 30(4), 395-410.

Grazioli, S. and Jarvenpaa, S. L. (2003). Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence. *International Journal of Electronic Commerce*, 7(4), 93-118.

Greenberg, A. (2008). Pharma's Black Market Boom, *Forbes.com*, August 26.

Gregor, S. and Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, 37(2), 337-355.

Grilli, L., and Rampichini, C. (2012). Multilevel models for ordinal data. *In: Kenett R and Salini S (eds.) Modern Analysis of Customer Surveys: with Applications using R*. Wiley.

Gyongyi, Z. and Garcia-Molina, H. (2005) Spam: It's Not for Inboxes Anymore. *IEEE Computer*, 28-34.

Hand, D. J., and Till, R. J. (2001). A simple Generalisation of the Area Under the ROC curve for Multiple Class Classification Problems, *Machine Learning*, 45(2), 171-186.

Hedeker, D., and Gibbons, R. D. (1994). A random-effects ordinal regression model for multilevel analysis. *Biometrics*, 933-944.

Hedeker, D., Berbaum, M., and Mermelstein, R. J. (2006). Location-scale models for multilevel ordinal data: Between- and within-subjects variance modeling. *Journal of Probability and Statistical Science*, 4(1), 1-20.

Hellerman, C. (2013). FDA shuts down 1,677 online pharmacies. *CNN Health*, June 27.

Herzberg, A., and Jbara, A. (2008). Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology*, 8(4), no. 16.

Hevner, A. R., March, S. T., Park, J., and Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 28(1), 75-105.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74-81.

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

Jenkins, J., Anderson, B., Vance, A., Kirwan, C., Eargle, D. (2016). More Harm Than Good? How Messages That Interrupt Can Make Us Vulnerable, *Information Systems Research*, forthcoming.

Jobber, D., and Ellis-Chadwick, F. (1995). *Principles and practice of marketing*, 599-602, Maidenhead: McGraw-Hill.

Kahneman, D., and Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, 263-291.

Kaushik, A. (2011). *Web Analytics 2.0: The Art of Online Accountability and Science of Customer Centricity*, Wiley Publishing.

Krebs, B. (2005). Few Online 'Canadian Pharmacies' Based in Canada, FDA Says, *Washington Post*.

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.

Kitchens, B., Dobolyi, D., Li, J., and Abbasi, A. (2018). Advanced Customer Analytics: Strategic Value through Integration of Relationship-Oriented Big Data, *Journal of Management Information Systems*, 35(2), pp. 540-574.

Koepke, J., Kaza, S., and Abbasi, A. (2012). Exploratory experiments to identify fake websites by using features from the network stack. *In Proceedings of the IEEE International Conference on Intelligence and Security Informatics*, 126-128.

Kolari, P., Finin, T., and Joshi, A. (2006). SVMs for the Blogosphere: Blog Identification and Splog Detection. In AAAI Spring Symposium: Computational Approaches to Analyzing Weblogs, 92-99.

Korolov, M. (2015). Phishing is a $3.7-million annual cost for average large company, *CSO*, August 26.

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.

Lennon, M. (2011). Cisco: Targeted Attacks Cost Organizations $1.29 billion annually. *Security Week*, June 30.

Li, L. and Helenius, M. (2007). Usability Evaluation of Anti-Phishing Toolbar. *Journal in Computer Virology*, 3(2), 163-184.

Li, L., Berki, E., Helenius, M., and Ovaska, S. (2014). "Towards a Contingency Approach with Whitelist-and Blacklist-based Anti-phishing Applications: What do usability tests indicate?" *Behaviour & Information Technology* (33:11), pp. 1136-1147.

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

Liu, W., Deng, X., Huang, G., and Fu, A. Y. (2006). An Antiphishing Strategy Based on Visual Similarity Assessment, *IEEE Internet Computing* 10(2), 58-65.

March, S. T., and Smith, G. 1995. Design and Natural Science Research on Information Technology. *Decision Support Systems*, 15(4), December, 251-266.

McAfee, (2013). *McAfee Threats Report: First Quarter 2013*, April 10.

McCullagh, P. (1980). Regression models for ordinal data. *Journal of the Royal Statistical Society. Series B (Methodological)*, 109-142.

McGrath, J. E. (1981). Dilemmatics: The study of research choices and dilemmas. *American Behavioral Scientist*, 25, pp. 179-210.

McKelvey, R. D., and Zavoina, W. (1975). A statistical model for the analysis of ordinal level dependent variables. *Journal of Mathematical Sociology*, 4(1), 103-120.

Middelfart, M. (2007). Improving Business Intelligence Speed and Quality through the OODA Concept. *In Proceedings of the 10th ACM International Workshop on Data Warehousing and OLAP*, 97-98.

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, 192-222.

Morris, M., Venkatesh, V. and Ackerman, P. (2005). Gender and Age Differences in Employee Decisions About New Technology: An Extension to the Theory of Planned Behavior. *IEEE Transactions on Engineering Management*, 52(1), 69 – 84.

Musthaler, L. (2013). Security analytics will be the next big thing in IT security. *Network World*, May 31.

Netemeyer, R., Dobolyi, D., Abbasi, A., Clifford, G., and Taylor, H. (2020). Health Literacy, Health Numeracy and Trust in Doctor: Effects on Key Consumer Health Outcomes, *Journal of Consumer Affairs*, 54(1), pp. 3-42.

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

Parrish Jr, J. L., Bailey, J. L., and Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. Little Rock: University of Arkansas.

Porter, C.E. and Donthu, N. (2006). Using the technology acceptance model to explain how attitudes determine Internet usage: The role of perceived access barriers and demographics. *Journal of Business Research*, 59, 999-1007.

Prat, N., Comyn-Wattiau, I., and Akoka, J. (2015). A taxonomy of evaluation methods for information systems artifacts. *Journal of Management Information Systems*, 32(3), 229-267.

Prince, B. (2009). Phishing Attacks Cost Millions Despite Low Success Rates, *eWeek*, December 7, 2009.

Ramzan, Z. and Wuest, C. (2007). Phishing Attacks: Analyzing Trends in 2006, *In Proceedings of the 4th Conference on Email and Anti-Spam*.

R Core Team (2016). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL https://www.R-project.org/.

Ransbotham, S., and Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, 20(1), 121-139.

Richards, C. (2004). *Certain to Win: The Boyd Strategy Applied to Business*. Xlibris.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91, 93-114

Santhanam, R., Sethumadhavan, M., and Virendra, M. (2010). *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives*. IGI Global.

Schneier, B. (2000). Inside risks: semantic network attacks. *Communications of the ACM*, 43(12), 168.

Selinger, M. (2013). Google vs. Bing: Search Engines Deliver Infected Websites as Their Top Results, *A New AV-TEST Study: Search Engines as Malware Providers*, April.

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 Proceedings of the ACM Symposium on Usable Privacy and Security*, 88-99.

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.

Shmueli, G. and Koppius, O. (2011) Predictive Analytics in Information Systems Research, *MIS Quarterly*, 35(3), 553-572.

Siponen, M., and Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 34(3), 487–502.

Storey, V., Burton-Jones, A., Sugumaran, V., and Purao, S. 2008. CONQUER: A Methodology for Context-Aware Query Processing on the World Wide Web, *Information Systems Research* 19(1), 3-25.

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. (2009). Crying Wolf: An Empirical Study of SSL Warning Effectiveness. *In Proc. of the USENIX Security Symposium*, Montreal, 399-416.

Symantec. (2012*). Norton cybercrime report: The human impact,* April 10.

Taylor, B. (2014). How Big Data is changing the security analytics landscape. *TechRepublic*, January 2.

Thompson, F. (1995). Business strategy and the Boyd cycle. *Journal of Contingencies and Crisis Management*, 3(2), 81-90.

Vance, A., Lowry, P. B., and Eggett, D. (2015). Increasing Accountability through User-Interface Design Artifacts: A New Approach to Address the Problem of Access-Policy Violations, *MIS Quarterly*, 39 (2), pp. 345-366.

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.

Verizon (2015). Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2015/

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.

Walsh, S. (2010). Bank/customer lawsuits over phishing scams rising. *All Spammed Up: Anti-Spam in a Business Environment*, March 8.

Wang, J., Chen, R., Herath, T., 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.

Wang, J., Gupta, M., and Rao, H. R. (2015). Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly*, 39(1), 91-112.

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.

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., and Song, J. (2008). Dynamics of trust revision: using health infomediaries. *Journal of Management Information Systems*, 24(4), 225-248.

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), 448-484.

Zahedi, F. M., Abbasi, A., and Chen, Y. (2011). Design Elements that Promote the use of Fake Website Detection Tools, *In the 10th AIS SIG-HCI Workshop*, Shanghai, China, December 4.

Zahedi, F. M., Abbasi, A., and Chen, Y. (2011). Trust Calibration of Security IT Artifacts: The Case of Fake Website Detection Tools, *In the Workshop on Information Security and Privacy (WISP)*, Shanghai, China, December 4.

Zhang, D., Yan, Z., Jiang, H., and Kim, T. (2014). A Domain-Feature Enhanced Classification Model for Detection of Phishing E-Business Websites. *Information & Management*. 51(7), 845-853.

Zhang, Y., Egelman, S., Cranor, L. and Hong, J. (2007). Phinding Phish: Evaluating Anti-phishing Tools. *In Proceedings of the 14th Annual Network and Distributed System Security Symposium* (NDSS), San Diego, CA, 1-16.

Zimbra, D., Abbasi, A., and Chen, H. (2010). A Cyber-Archaeology Approach to Social Movement Research: Framework and Case Study, *Journal of Computer-Mediated Communication*, 16, pp. 48-70.

Zimbra, D., Abbasi, A., Zeng, D., and Chen, H. (2018). The State-of-the-Art in Twitter Sentiment Analysis: A Review and Benchmark Evaluation, *ACM Transactions on Management Information Systems*, 9(2), no. 5.