Information Systems Research
Vol. 25, No. 2, June 2014, pp. 385–400
ISSN 1047-7047 (print) | ISSN 1526-5536 (online)

http://dx.doi.org/10.1287/isre.2014.0522

Research Note

Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance

Ryan T. Wright
Isenberg School of Management, University of Massachusetts, Amherst, Massachusetts 01003,
rwright@isenberg.umass.edu

Matthew L. Jensen
Division of MIS, Center for Applied Social Research, University of Oklahoma, Norman, Oklahoma 73019,
mjensen@ou.edu

Jason Bennett Thatcher
Social Analytics Institute, Department of Management, Clemson University, Clemson, South Carolina 29634,
jthatch@clemson.edu

Michael Dinger
Johnson College of Business and Economics, University of South Carolina Upstate,
Spartanburg, South Carolina 29306, mdinger@uscupstate.edu

Kent Marett
Department of Management and Information Systems, College of Business, Mississippi State University,
Mississippi State, Mississippi 39762, kmarett@business.msstate.edu

Phishing is a major threat to individuals and organizations. Along with billions of dollars lost annually, phishing attacks have led to significant data breaches, loss of corporate secrets, and espionage. Despite the significant threat, potential phishing targets have little theoretical or practical guidance on which phishing tactics are most dangerous and require heightened caution. The current study extends persuasion and motivation theory to postulate why certain influence techniques are especially dangerous when used in phishing attacks. We evaluated our hypotheses using a large field experiment that involved sending phishing messages to more than 2,600 participants. Results indicated a disparity in levels of danger presented by different influence techniques used in phishing attacks. Specifically, participants were less vulnerable to phishing influence techniques that relied on fictitious prior shared experience and were more vulnerable to techniques offering a high level of self-determination. By extending persuasion and motivation theory to explain the relative efficacy of phishers' influence techniques, this work clarifies significant vulnerabilities and lays the foundation for individuals and organizations to combat phishing through awareness and training efforts.

Keywords: phishing; persuasion theory; influence techniques; motivation theory; self-determination; perceived locus of causality; social engineering; online deception; mediated deception; deception; field experiments
History: Shaila Miranda, Senior Editor; Glenn Browne, Associate Editor. This paper was received January 26, 2010, and was with the authors 31 months for 6 revisions.

1. Introduction

Phishing is a nuisance familiar to most email users. More than 80% of the 507 billion emails sent per day are likely spam, malware, or phishing messages (Radicati 2012). These emails arrive in a persistent stream at inboxes around the world. Phishers attempt to steal private information from a target (the phishing message recipient) by mimicking electronic communication from a trustworthy source (Myers 2007). Phishers carry out most attacks by sending single messages to large numbers of people expecting a subset of the recipients to respond (Hong 2012). For example, phishers direct email recipients to click on a malicious link, open an infected attachment, download a piece of malware, or reply with private information, with potentially disastrous consequences to follow.

Although phishing is a familiar nuisance, phishers successfully steal sensitive information. In 2014, the U.S. Internal Revenue Service (IRS) reported a 66% increase in attacks on U.S. taxpayers in one year, resulting in thousands of cases of identity theft (Barrett and McKinnon 2014). In a recent example, phishers posing as IRS employees contacted taxpayers with "official email inquiries" concerning their tax returns. When recipients responded to these inquiries, the phishers stole private information from taxpayers and in

some cases stole taxpayers' refunds by rerouting the deposits (Acohido 2013). A second example is the phishing attack on Target through its subcontractor, Fazio Mechanical. This attack lead to the exposure of 110 million consumers' credit cards and personal data (Harris et al. 2014). In yet another case, a phishing attack targeting defense contractor Booz Allen Hamilton resulted in a significant data breach (Grow et al. 2008). Although such phishing attacks result in extensive monetary damages (Cohen 2013, Hong 2012), they also result in lost corporate secrets (e.g., Healey 2013), misappropriation of classified information (e.g., Hesseldahl 2011), and espionage (e.g., Booz Allen Hamilton, Grow et al. 2008).

To combat phishing, many organizations turn to technical means, such as filtering out phishing messages, automating detection of fake websites (e.g., Abbasi et al. 2010), and deploying anti-phishing warning systems (e.g., Egelman et al. 2008). However, technical interventions cannot entirely remove the threat of phishing (Abbasi et al. 2012). Since phishers operate in legitimate communication channels, their messages can be very difficult to distinguish from genuine messages (Dhamija et al. 2006). Despite extensive attention being paid to technical solutions to phishing, organizations remain vulnerable to users receiving and responding to phishing messages.

To mitigate phishers' ability to steal information, email users must be able to detect phishing attacks. Successful phishing messages have content that is *believable* and that elicits *compliance* from recipients (Hong 2012). To be believable, phishers masquerade as a trustworthy source by crafting messages that attempt to mirror the content and tone of legitimate messages. To gain compliance from the message receiver, phishers employ a range of tactics to impel recipients' responses (e.g., click on a link, email back private information, or download a file). For instance, a phisher may pose as an authoritative source or offer a limited time to respond to a phishing message, thereby creating an impression of time scarcity.

Although many researchers have examined what makes phishing messages *believable* (e.g., Anti-Phishing Working Group 2013, Chen et al. 2011, Hong 2012), fewer have examined *why individuals comply* with phishers' requests. As a result, scant theoretical or practical guidance is available regarding how to avoid or mitigate phishing tactics that most effectively generate compliance and thus present the greatest danger to individuals and organizations. Such research is important because a deeper understanding of phishers' tactics and their relative efficacy can inform the design of effective countermeasures that directly address practicing professionals' security concerns (e.g., phishing training; see Dodge et al. 2007).

To deepen understanding of how phishers generate compliance, we draw on persuasion and motivation theory to explain the relative effectiveness of phishing strategies. We tested our hypotheses in a field experiment involving more than 2,600 participants at a Midwestern university. Our experiment consisted of phishing attacks that employed distinct influence techniques to solicit usernames and passwords from the participants. Our results indicated disparate response rates to different influence techniques, with some techniques eliciting much greater compliance. Our findings offer guidance to organizations seeking to help individuals recognize influence techniques that heighten their vulnerability to phishing attacks and thus resist phishers' attempts to elicit their compliance.

2. Theoretical Background

Phishing messages, like all deceptive messages, are sent with purposeful intent to mislead the receiver (Buller et al. 1996, Xiao and Benbasat 2011). However, three characteristics of phishing messages distinguish them from other types of deceptive messages. First, phishing attacks occur through mediated channels (e.g., text-based email), which both undermine and benefit phishers' goals. On one hand, receivers are able to process and reprocess an emailed phishing message, which has been shown to increase the likelihood the deception will be discovered (George et al. 2013). On the other hand, mediation permits the concealment or falsification of the actual message source (Donath 1999). Therefore, the mediated channel allows phishers significant latitude in mimicking messages from legitimate sources during an attack (Abbasi et al. 2010). Second, in contrast to other types of deception where a deceiver may have repeated interactions with the receiver, phishing attacks usually are one-time messages sent to a group of individuals with the expectation that a subset of recipients will respond (Hong 2012). Third, in contrast to other deceptions where the goal is to obfuscate or evade truth, a phisher's goal is to persuade the receiver to accept a falsehood *and* perform a specific action. Moreover, a phishing message is normally active for only a brief period (e.g., average of 26 hours and 13 minutes; Anti-Phishing Working Group 2013) before recipients are alerted and can take preventative action. Therefore, if the phishing message is to generate compliant responses, it must do so quickly.

To make phishing messages believable, phishers mimic the content of legitimate messages (Wright and Marett 2010) and tailor their messages to look like email "that people would ordinarily expect to receive" (Caldwell 2013, p. 12). Message recipients are sensitive to spelling mistakes and design inconsistencies between a phishing message and other legitimate messages, and such errors and inconsistencies increase recipient suspicion (Jakobsson 2007). To increase believability, phishers often personalize messages and associated

phishing websites (i.e., discuss content unique to the population of potential recipients; Wright et al. 2010, Wright and Marett 2010). Additionally, phishers often include forged ancillary cues to increase perceived message credibility. Considered to be separate from the content of a phishing message (e.g., text), ancillary cues include illicit use of graphics, logos, and forged security seals from trusted third parties such as the Better Business Bureau or Verisign (Dhamija et al. 2006). Finally, phishers increase believability by closely approximating technical features of legitimate messages through practices such as spoofing legitimate email addresses and replicating actual websites (Dinev and Hart 2006).

Believability alone, however, is not sufficient to generate responses to single, time-sensitive phishing messages; recipients also must be persuaded to actually respond. To induce responses, phishers employ diverse influence techniques. Messages appearing to come from an acquaintance have a higher likelihood of recipient compliance (Jagatic et al. 2007). Fabricated websites that employ coercive techniques (e.g., forcing a user to perform an action) often result in the disclosure of private information (Conti and Sobiesk 2010). However, messages with promises of future cash payments or threats to cut services tend to arouse recipients' suspicions (Jakobsson 2007). Although phishing research provides evidence that some influence techniques are more effective than others, no work has yet offered a theoretical explanation or an empirical examination of the relative effectiveness of phishing techniques.

To understand the relative impact of phishing influence techniques more clearly, we draw on research evaluating persuasion and motivation. Specifically, we build on the taxonomy of influence techniques first articulated by Cialdini (2009). The taxonomy includes six prototypical influence techniques: liking, reciprocity, social proof, consistency, authority, and scarcity. The effectiveness of these techniques has been studied in a number of fields, including sales and marketing (Cialdini 2001, Cialdini et al. 1979), health and self-improvement (Glasziou and Haynes 2005), and negotiations (Trotman et al. 2005). In security research, the techniques have been used to examine how cybercriminals gain physical access to secure locations (Sagarin and Mitnick 2012) and how social engineering can put information security at risk (Workman 2008). Cialdini's principles are germane to phishing because (1) they constitute a parsimonious list of compliance-generating influence techniques that explain human behavior across contexts and (2) phishers actually use these influence techniques in email messages (see Table 1).

Influence techniques take advantage of an individual's tendency to rely on experience-based or automatic information processing (Cialdini 2009, Cialdini and Trost 1998). Stanovich and West (2000) conceptualized such automatic information processing as System 1 thinking and distinguished it from System 2 thinking, which is more deliberative and analytic (also see Kahneman 2011). Although System 1 thinking enables quick decision making (Kahneman 2011), it can also be used to take advantage of unsuspecting individuals. Cialdini described the outcome of each influence technique in terms of "its ability to produce a distinct kind of automatic, mindless compliance from people, that is, a

Table 1 Definitions and Examples of Influence Techniques

Technique	Definition	Examples of actual phishing[a, b]
Liking	People prefer to say yes to individuals they "know and like" (Cialdini 2009, p. 142), and compliance practitioners use factors including physical attractiveness, perceived similarities, praise, and association with favorable events/outcomes to increase the chance of compliance.	After a password reset request, "We realize that this precaution may cause you some inconvenience. We'd really *like to keep you happy* by continuing to help."
Reciprocity	The tendency to "try to repay, in kind, what another person has provided us" (Cialdini 2009, p. 19).	"Our online security team has detected irregular activity on your American Express account. Please *help us* continue to keep your account secure by resetting your password . . ."
Social proof	People "view a behavior as correct in a given situation to the degree that we see others performing it" (Cialdini 2009, p. 99).	"Due to recent activity, we have issued the following security requirements for all account holders. *All account holders need to comply.*"
Consistency	Once people make a commitment, they will feel "personal and interpersonal pressure to perform consistently with that commitment" (Cialdini 2009, p. 52).	"*As you have done before*, please update your password using the following link . . ."
Authority	People's tendency to believe that obedience to proper authority is right and disobedience is wrong (Cialdini 2009, pp. 180–181).	"For your protection your account may be limited until you follow the following steps." *The email was signed by the "Senior Vice President"* of Chase Online Banking Team.
Scarcity	People tend to derive scarcity from their personal values; "opportunities seem more valuable to us when they are less available" (Cialdini 2009, p. 228).	"This email has been sent to inform you that your account will be *deactivated in the next 24 hours* . . ."

[a]Italic text indicates where the persuasion technique was utilized.
[b]Examples drawn from www.fraudwatchinternational.com/phishing/ on March 2, 2012.

willingness to say 'Yes' without thinking first" (2009, p. xiv). Cialdini and other influence researchers stop short of predicting which influence techniques are most effective, instead arguing that each technique's effectiveness is a product of the context and manner in which it is employed (Sundie et al. 2012). As a result, existing research provides little insight into which influence techniques will be effective in the phishing context where the message source is hidden, the persuasion effort is limited to one message, and there is a limited temporal window for compliance to be achieved.

Drawing on persuasion and motivation theory, we develop three hypotheses relating influence techniques used in phishing messages and the context of phishing attacks to recipients' motivations for complying with phishers' requests. We explore how influence techniques may be more or less effective depending on how well they satisfy the functional requirements of a phishing attack and how well they align with recipients' motivations to respond.

3. Development of Hypotheses

Prior research has shown that individuals use System 1 thinking to process information systems (IS) security threats (e.g., Vance et al. 2008) and System 1 thinking occupies a prominent role in IS security training research (Puhakainen and Siponen 2010). When confronted with a phishing message, recipients are prompted to respond in a rote manner as they do with legitimate messages (e.g., click on a link or open an attachment). Phishing research has found that unless alerted to potential harm, individuals rely on simple rules of thumb when processing emails (Abbasi et al. 2012, Jingguo et al. 2012). As a result, they rarely attend to cues distinguishing illegitimate email messages from legitimate ones (Dhamija et al. 2006). Our first set of hypotheses relates to how phishers take advantage of System 1 thinking to gain recipients' compliance with their requests. We contend that because individuals often process email by relying on System 1, Cialdini's (Cialdini 2009, Cialdini and Trost 1998) influence techniques will be effective in generating compliance with phishing requests.

3.1. Influence Techniques in Phishing

3.1.1. Liking. The technique of liking takes advantage of the heuristic that people "say yes to individuals they know and like" (Cialdini 2009, p. 172). To persuade users through the "liking" technique, a message sender must win the recipient's goodwill, trust, and friendship. A sender may do so through devices such as compliments (Howard et al. 1995) or by emphasizing similarities (Burger et al. 2004). Even modest attempts to earn liking, such as trivial or inauthentic flattery (Drachman et al. 1978), attempts at humor, or an emphasis on similarities such as a shared favorite sports team, elicit receivers' liking of persuaders and generate compliance with persuaders' requests (Cialdini 2009).

3.1.2. Reciprocity. The technique of reciprocity takes advantage of people's tendency to repay an earlier action "in kind," whether or not it is solicited (Cialdini 2009). The technique of reciprocity can be invoked by performing a relatively small favor that results in a similar or more substantial favor in return (Regan 1971). Perhaps because phishers do not actually intend to provide anything of value to their targets, they may commit their targets to "uninvited debts" by alerting them to fictitious opportunities or reporting that they have been working on their behalf. Although the sense of obligation is weaker when repaying uninvited favors, we expect the human tendency to repay favors to put the power of reciprocity in the phishers' control (Paese and Gilin 2000).

3.1.3. Social Proof. The technique of social proof takes advantage of people's tendency to "determine what is correct by finding out what other people think is correct" (Cialdini and Goldstein 2004, p. 110). To leverage this technique, phishers may claim endorsements from groups (e.g., a peer group), indicating that others have already performed the solicited action. Information on how others behave, especially unfamiliar others, serves as social proof because we "use the actions of others to decide on proper behavior for ourselves" (Cialdini 2009, p. 143). Cues that others are performing a behavior reduce uncertainty about the risk of performing that behavior (Cialdini 2009).

3.1.4. Consistency. The principle of consistency takes advantage of individuals' desire to appear consistent in their words, beliefs, and actions (Cialdini 2009). To use this influence technique, targeted individuals must be convinced to endorse a position or opinion, which then renders that individual more likely to comply with a subsequent request regarding that position (Vaidyanathan and Aggarwal 2005). Phishers can leverage this technique by creating the illusion of a prior commitment and then making a request that appears to be consistent with the commitment. For example, a phisher may send "reminders" encouraging individuals to perform a (fictitious) previously scheduled update of login information.

3.1.5. Authority. Cialdini (2009) proposed that people learn at an early age to defer to others with more experience, knowledge, or power; the authority technique takes advantage of this tendency. Persuasion research suggests that people respond more favorably to individuals or to their suggestions when they possess outward trappings of authority, as evidenced by things like job titles (Castilla 2011), appearance (Bushman 1984), and demeanor (Ward and Brenner 2006). Phishers may use references to authority (e.g., impersonation, name dropping) to gain compliance in their attacks.

3.1.6. Scarcity. The scarcity technique takes advantage of individuals' tendency to find an object, event, or experience more valuable when they perceive it as rare, inimitable, or available for a limited time. Scarce resources have higher value (Groves et al. 1992). When individuals perceive that an opportunity is limited in availability or that others may be competing for it, they are more susceptible to making poor decisions in order to gain or retain access to the opportunity (Sundie et al. 2012). Phishers use the principle of scarcity when making calls for urgent action, in which they introduce an element of time pressure in their requests for information (Wright et al. 2010).

Applying persuasion theory to the phishing context, we expect phishing messages using Cialdini's influence techniques to result in a greater compliance with phishers' requests.

Hypothesis 1 (H1). *Phishing messages that use* (a) *liking*, (b) *reciprocity*, (c) *social proof*, (d) *consistency*, (e) *references to authority, and* (f) *scarcity will increase the likelihood that recipients will respond to phishing attacks*.

3.2. Influence Categories in Phishing Attacks

Although the six different influence techniques are generally effective in producing compliance in mediated exchanges (Guadagno and Cialdini 2005, 2007), their effectiveness may vary depending on the context of the persuasion attempt (Guadagno and Cialdini 2005). The theoretical explanation for the variability in effectiveness has thus far been unclear. Therefore, we conceptualize two categorizations that explain the relative effectiveness of Cialdini's influence techniques within the phishing context. Specifically, we hypothesize that some influence techniques will vary in their effectiveness because of the functional requirements of the phishing task and the motivation of individuals who may respond to the phishing messages.

3.2.1. Fictitious Shared Experiences. Past persuasion research has suggested that in mediated influence attempts, multiple exchanges between a persuader and target individual increase the likelihood of successful persuasion (Guadagno and Cialdini 2005). Previous mediated deception research has also shown that through multiple exchanges or shared experiences, a deceiver is able to increase the likelihood of successful deception (Burgoon et al. 1999, 2002; Carlson et al. 2004). Two of Cialdini's influence techniques depend on multiple exchanges or prior shared experiences: the consistency technique requires an individual to maintain a position that he or she has previously endorsed; the reciprocity technique requires an individual to repay a previous favor or incurred debt. However, most phishing attacks are conducted by a phisher sending a single message to a large group of people (Hong 2012). Therefore, the one-time nature of phishing exchanges may undermine these influence techniques that would be effective in other circumstances. A phisher may feign shared experience in order to invoke consistency and reciprocity when crafting a phishing message, but the necessity of alluding to a fictitious prior shared experience in a one-time and one-way message may reduce the efficacy of these influence techniques.

We offer two explanations for why phishing influence techniques referencing past interactions or shared experiences are less compelling or more easily identified as fraudulent. First, the shared experiences invoked can hold different meanings for the interacting individuals. Upon receiving a persuasive message invoking a purported shared experience, the target will attempt to relate the message to past experiences with the sender (Cialdini et al. 1981). If descriptions of the shared experience do not match the individual's recollections, resistance to persuasion will ensue (Greenwald 1968, Petty et al. 1981). Second, in fabricating prior shared experiences, the phisher must speculate about which experiences will be applicable to recipients and which details of the experience will be plausible to each recipient. However, the fictional nature of the shared experience increases the likelihood of a discrepancy between the description presented by the phisher and the recipient's actual experience (see Goffman 1959). This discrepancy will break the recipient's System 1 processing and increase his or her scrutiny of the phishing message.

Hypothesis 2 (H2). *Influence techniques where phishers must feign shared experiences with recipients will be less effective than techniques that do not require shared experiences*.

3.2.2. Motivation and Self-Determination. To understand the differential effects of the influence techniques, it is important to consider how they may interface with targeted individuals' motivations. Prior theorizing differentiates among four basic types of motivation: intrinsic, identification, introjected, and external (Deci and Ryan 1985). *Intrinsic motivation* is based on enjoyment and liking; *identification motivation* is driven by attainment of one's goals (e.g., gaining resources); *introjected motivation* is based on self-image pressures such as living up to societal expectations; and *external motivation* is driven by external authority. These motivations exist along a continuum based on the individual's perceived locus of causality (PLOC; see Figure 1). Separate from experience or knowledge, PLOC is a measure of how much control an individual has over his or her actions and directly determines whether the individual's actions are self-determined or non-self-determined (Ryan and Connell 1989). PLOC previously has been useful in explaining online privacy behaviors (Malhotra et al. 2008).

Linking influence techniques to underlying motivations to comply yields understanding about the relative efficacy of phishing attacks. Cialdini's influence

Figure 1 Influence Techniques, PLOC, and Motivation

techniques correspond well to the types of motivation identified by Deci and Ryan (Deci and Ryan 1985, Ryan and Deci 2000). Influence through invoked liking depends on intrinsic motivation. Intrinsic motivation has been shown to increase when a person likes a task or the person involved in it (Gerow et al. 2013; Venkatesh 1999, 2000). Influence based on social proof and scarcity depends on identification motivation: such tactics evoke goal-oriented behaviors because desire for a popular or scarce good encourages targets' action. Influence based on reciprocity and consistency depends on targets' introspective motivation. Here, compliance is impelled by individuals' view of themselves in comparison with societal expectations to repay past debts or be consistent with past positions (Cialdini and Trost 1998). Finally, authority-based influence depends on targets' external motivation; referencing a real or putative authority figure elicits compliance by motivating targets to seek external gratification or avoid negative consequences that the authority figure controls.

In summary, by considering the motivations invoked by efforts to induce compliance across the different influence techniques, we are able to order them along a PLOC continuum (see Figure 1). Specifically, we posit that liking, social proof, and scarcity influence techniques will be associated with a greater degree of PLOC and influence targets will comply because *they* think they want to comply. Liking, social proof, and scarcity therefore will result in a greater degree of compliance, which targets will perceive to be self-determined behavior. Conversely, reciprocity, consistency, and authority will be associated with a lower degree of PLOC and when targets comply, they will do so because *others* expect them to comply. Reciprocity, consistency, and authority techniques therefore will induce lower levels of compliance because targets will not perceive the expected behavioral response to be self-determined.

Although some characteristics of mediated communication associated with phishing may attenuate the effects of status differentials (Dubrovsky et al. 1991, Tan et al. 1998), previous in-person deception research has suggested that deceivers use *non*-self-determined influence techniques to successfully carry out their deception (e.g., Lindsey et al. 2011). For example, deceivers with higher power or status may use their position to increase the likelihood that their deception will be successful. Considering recipients' motivation to respond across the different phishing tactics highlights two reasons why self-determined influence techniques may be more effective in generating a response than non-self-determined ones. First, research comparing motivations (Gagné and Deci 2005) found higher self-determination generates a greater likelihood of following through with a requested action. On the other hand, activities permitting lower self-determination require a higher motivational threshold (e.g., threats from authority) to generate action (Gagné and Deci 2005). When applied to the time-sensitive context of phishing, these findings suggest that influence techniques offering higher self-determination (e.g., liking, social proof, scarcity) will be more effective than influence techniques offering lower self-determination (reciprocity, consistency, authority). Second, it may be more difficult for individuals to break out of System 1 processing when they encounter a phishing message using an intrinsically motivating influence technique than an externally motivating technique. Research has shown that individuals rarely notice when intrinsically motivating influence techniques (e.g., liking) are employed against them (Burger et al. 2004). Externally motivated influence techniques (e.g., authority) may generate reactance (Brehm 1989), thus inviting scrutiny of the request.

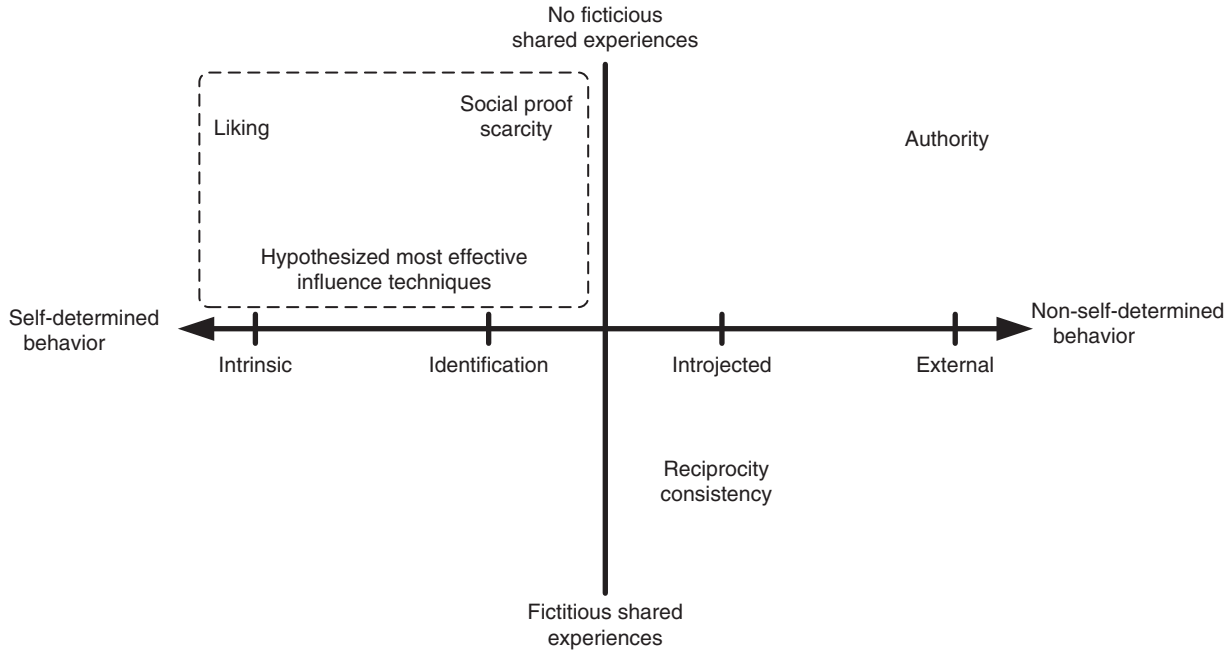
Hypothesis 3 (H3). *Influence techniques offering a high degree of self-determination will increase the likelihood that recipients will respond to phishing attacks more than those offering a low degree of self-determination.*

We summarize the three hypotheses in Figure 2. The area outlined by the dotted line highlights the influence techniques hypothesized to be most dangerous when employed by phishers.

4. Method

A field experiment was conducted at a medium-sized university in the Midwestern United States to test the hypotheses. The experiment was designed under close supervision of the university's institutional review board and was endorsed by the university's administration and information technology (IT) department. Our procedures adhered to Finn and Jakobsson's (2008) guidelines for designing ethical phishing experiments. Participants were randomly assigned to a treatment condition and then subjected to a phishing attack that employed Cialdini's (2009) influence

Figure 2 Summary of Predictions



techniques. Participants received phishing messages that directed them to a website fabricated to appear like a legitimate university website. Once participants reached the website, they were instructed to enter their university username and password. These credentials provided access to all electronic university resources (e.g., personal, academic, and financial information). The experiment used a full factorial design (2 [No]Liking × 2 [No]Reciprocity × 2 [No]Social Proof × 2 [No]Consistency × 2 [No]Authority × 2 [No]Scarcity) for a total of 64 treatment cells.

4.1. Participants

Participants were randomly drawn from the university student population: 2,624 participants were included in this study. Although students' contact information was publicly available through an online directory, the university provided email addresses and gender information. Fifty-three percent of the recipients were female, which reasonably approximates the university's population (54% female). To preserve the fidelity of the experiment, participants were not contacted prior to the experiment. Following the close of the experiment, participants were sent debriefing information and were invited to contact the researchers if they had concerns. To mitigate the influence of potential covariates (e.g., Web proficiency, security awareness; see Wright et al. 2010b), participants were randomly assigned to conditions using the SAS 9.0 Design of Experiment module. Therefore, we anticipated the effect of potential covariates to be approximately equivalent across conditions (Hoyle et al. 2002). To execute the design, 41 participants were assigned to each of the 64 conditions.

4.2. Stimulus Materials

Each condition used a baseline phishing message asking participants to visit the fabricated website and register their university username and password (see Appendix A). The message was signed by a fictional university employee and was sent from a spoofed university email account. For each experimental condition, the phishing message was tailored by adding several sentences corresponding to each of the influence techniques. The baseline phishing message and the message manipulations are displayed in Table 2 (see Appendix A for a description of message piloting).

When participants visited the website, entered their university credentials, and clicked the login button, their usernames were captured. However, their passwords were immediately deleted and were not transmitted or stored. Participants who logged in were informed that the website was still under construction and that they should return later to the website to view content.

4.3. Procedure

Prior to sending the phishing messages, the researchers solicited support from the IT helpdesk at the university. The helpdesk agreed not to reveal the true nature of the experiment to participants who might contact them prior to the close of the experiment. We then randomly assigned participants to one of 64 conditions and distributed the phishing messages (see Appendix A for a description of message dissemination). The phishing attack was active for four days. After a staff member at the university notified the entire student body of the phishing attack, we disclosed our involvement in

Table 2 Phishing Email Conditions[a]

Baseline phishing message	Dear <Subject>, <University> has now launched its beta web portal called <Phishing URL>. Please go to <Phishing URL> and login to activate your new account. You can also access your account directly by going to <Tracking URL[b]>. You may have to copy and paste the URL into your web browser. [Influence Technique Manipulations] Jason Roth <University> Administrator <Phishing URL> <Non-usable Campus Phone Number>

Influence technique	Fictitious shared experience	Self-determination	Manipulation in text[a]
Liking	No	Yes	This is an opportunity to help the university by logging into the new system. Your participation will be very much appreciated. For your security, this email will self-destruct in 30 seconds! Go <University Mascot>!
Reciprocity	Yes	No	For all the hard work we put into keeping your <University> systems working, please return the favor and verify your login for the new beta site.
Social proof	No	Yes	We currently have over 85% participation in the beta web portal. Log on today to be part of this launch with the goal of 100% participation.
Consistency	Yes	No	In using the email and <University> systems, you agreed to keep your credentials up to date. Please log in to setup your account in the end system.
Authority	No	No	<CIO Name>, CIO of <University>, hopes to have full participation in this new system this week. Please logon accordingly.
Scarcity	No	Yes	If you don't log in within the next 48 hours, you will lose access to <University> web services such as email.

[a]Content in angled brackets < > above has been redacted. Content with square brackets [ ] indicates where manipulations were added to the phishing message.
[b]A direct tracking URL with a unique parameter that identified each participant. The URL and parameter were embedded as a link in the phishing message; thus, if the participants clicked on the link, we would be able to determine if they had visited the phishing website (even if participants chose not to attempt a login). When the phishing emails were sent, however, the university's email system revealed the tracking URL in plain text, and only 12 subjects out of the entire sample used the tracking URL.

the experiment and distributed debriefing materials, which included resources for anti-phishing training and a description of the safeguards employed during the experiment. The responses from participants in each condition were then tallied, and links between individuals and their responses were destroyed.

5. Results

Of the 2,624 participants, 178 participants (6.8%) supplied their university usernames and passwords in response to the phishing attack. Table 3 shows the response rates by influence technique. For comparison, the response rate to the baseline phishing message (without any influence techniques) is also shown. Additional details about the website visitors are provided in Appendix A. To test H1, we conducted a logistic regression that can accommodate categorical predictor and outcome variables (Afifi et al. 2003). The number of responses to the phishing messages satisfied sample size recommendations for logistic regression (Hosmer and Lemeshow 2004). Therefore, a logistic regression was performed with the presence of liking, reciprocity, social proof, consistency, authority, and scarcity influence techniques in phishing messages as predictor variables and whether or not each participant logged into the fabricated website as the outcome variable. Since previous research in deception detection has indicated the potential for gender to impact the identification of deceptive messages (McCornack and Parks 1990) and the university provided the gender of participants, this was included as a control variable.

Table 3 Phishing Responses per Condition

Condition	*N*	Responses (%)[a]
Baseline phishing message	41	1 (2.4%)
Phishing messages using liking	1,312	135 (10.3%)
Phishing messages using reciprocity	1,312	104 (7.9%)
Phishing messages using social proof	1,312	111 (8.5%)
Phishing messages using consistency	1,312	98 (7.5%)
Phishing messages using authority	1,312	67 (5.1%)
Phishing messages using scarcity	1,312	120 (9.1%)

[a]This study used a full factorial design to test the main effects of the influence techniques on responses. Therefore, some participants were exposed to more than one influence technique.

The logistic regression (Table 4) revealed significant effects in the hypothesized direction from four of the six influence techniques examined in H1 (H1(a) liking, H1(b) reciprocity, H1(c) social proof, and H1(f) scarcity). There was no significant effect from consistency, and the effect from authority was significant, but in the opposite direction. Additionally, males were significantly less likely to respond than were females.

Table 4 Effects of Influence Techniques on the Likelihood to Respond

Variables	B	Wald	Sig. ($df = 1$)
Intercept	−4.065	227.209	<0.001
Liking	1.246	47.048	<0.001
Reciprocity	0.380	5.565	0.018
Social Proof	0.571	12.189	<0.001
Consistency	0.239	2.232	0.135
Authority	−0.561	11.776	0.001
Scarcity	0.818	23.637	<0.001
Gender[a]	−0.443	7.613	0.006

Notes. Omnibus test of model coefficients: χ^2 (7, $N = 2{,}624$) = 117.29, $p < 0.001$. −2 Log likelihood: 1,184.2 |Nagelkerke R^2: 0.112| Hosmer and Lemeshow test: 0.695.

[a]Female = 0, male = 1.

To interpret the influence techniques' impact on likelihood of responding to a phishing attack, we followed recent guidelines for interpreting logistic regression results (Hoetker 2007). Specifically, we examined the impact of significant coefficients in the logistic regression by calculating the predictor variable's marginal effect in place of estimating odds ratios, which are often misinterpreted (Kaufman 1996, Norton et al. 2004). Because of the logistic function, predictor variables in a logistic regression do not have consistent (linear) effects on an outcome variable. Additionally, the relationship between a predictor and outcome variable depends on the other predictor variables included in the regression (Hoetker 2007). Therefore, we calculated the marginal effect of introducing influence techniques on the probability that individuals will respond to the phishing attack (see Table 5). We calculate marginal effects of introducing a single influence technique for both males and females and assume other influence techniques are not present.

To determine whether there are disparities in the danger posed by some phishing influence techniques over others (as proposed by H2 and H3), we first plotted the marginal effect of each influence technique over a range of reference probabilities (0.1 to 0.9; see Kaufman 1996). In other words, if a participant is likely to respond to a phishing message with a certain probability (e.g., the reference probability), the plots show the marginal effect of including an influence technique in the phishing message. These plots are shown in Figure 3 and illustrate a clear separation between the categories of influence techniques (e.g., no fictitious shared experience, self-determined; fictitious shared experience, non-self-determined; fictitious shared experience, non-self-determined).

Table 5 Marginal Effect of Adding Influence Techniques

Participant sex	Baseline probability[a]	Marginal effects of influence techniques[b]			
		Liking	Reciprocity	Social proof	Scarcity
Female	0.016	0.039	0.008	0.013	0.021
Male	0.011	0.026	0.005	0.008	0.013

[a]Probability of responding to baseline message.

[b]The marginal effect of each influence technique is calculated assuming all other influence techniques are not present and is shown in probabilities.

Consistent with H2 and H3, phishing messages employing techniques that did not require fictitious prior shared experiences and that offered self-determination increased the likelihood of responding by the greatest amount. Next, phishing messages employing techniques that required fictitious prior shared experiences and still offered self-determination were the second most effective. The least effective self-determined technique with no fictitious shared experience (social proof) was between 1.50 and 1.51 times more impactful on likelihood to respond than the most effective shared-experience, self-determined technique (reciprocity). The most effective self-determined technique involving no fictitious shared experience (liking) was between 3.41 and 3.19 times more impactful on participants' likelihood to respond than the most effective self-determined technique with fictitious shared experience (reciprocity). Finally, no-fictitious-shared-experience messages that did not offer self-determination were shown to be the least dangerous. The least effective self-determined technique with fictitious shared experiences (consistency), was between 2.37 and 2.33 times more impactful on participants' likelihood to respond than the non-self-determined technique with no fictitious shared experience (authority). Second, to determine whether the differences between the categories of influence techniques we observed in the plots (Figure 3) were statistically significant, we performed another logistic regression. We recoded each of the influence techniques so that they fell under one of the following three categories: no fictitious shared experience, self-determined; fictitious shared experience, self-determined; and no fictitious shared experience, non-self-determined. Then we used these variables as predictors with whether or not each participant logged in to the fabricated website as the outcome variable (see Appendix B for additional analyses). Again, gender served as a control variable.

The results of the logistic regression are shown in Table 6. Again, gender was a significant predictor, with males being less likely to respond than females. The category not requiring prior shared experiences and offering self-determination was the only significant category that positively affected participants' likelihood of responding to phishing messages. This test confirmed the first stage of our analysis and again was consistent with H2 and H3. These findings demonstrate disparity in the effectiveness of phishing influence techniques and show that the most dangerous techniques are those that do not require prior shared experiences and those offering self-determination.

6. Discussion

This work extends existing security research by presenting a theory-based, empirical examination of phishing

Figure 3 Marginal Effects of Influence Techniques

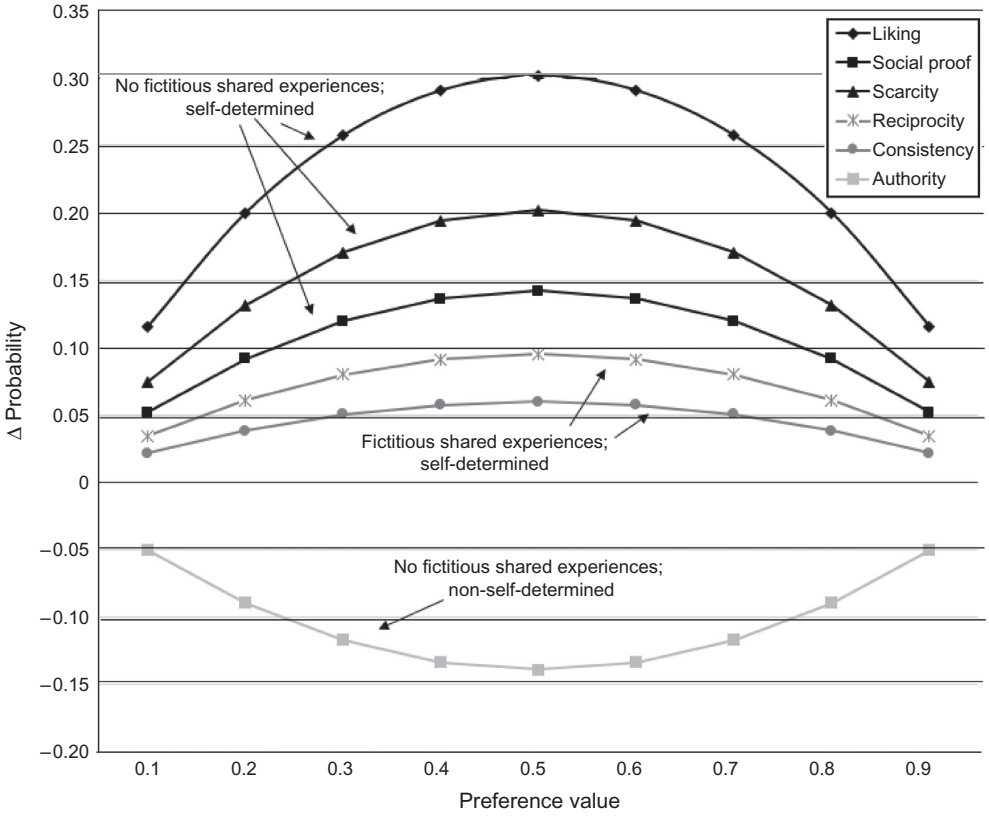


Table 6 Effects of Influence Categories on the Likelihood to Respond

Variables	B	Wald	Sig. ($df = 1$)
Intercept	−3.458	42.602	<0.001
No Fictitious Shared Experience, Self-determined	1.679	13.428	<0.001
Fictitious Shared Experience, Self-determined	0.333	2.910	0.088
No Fictitious Shared Experience, Non-self-determined	−0.542	11.375	0.001
Gender[a]	−0.421	7.133	0.008

Notes. Omnibus test of model coefficients: χ^2 (7, $N = 2{,}624$) = 44.65, $p < 0.001$. −2 Log likelihood: 1,256.87 |Nagelkerke R^2: 0.043| Hosmer and Lemeshow test: 0.703.

[a]Female = 0, male = 1.

tactics. No work, to our knowledge, has yet offered a theoretical explanation or an empirical examination of the relative effectiveness of phishing techniques. Our results indicate that four of the six influence techniques exerted significant effects on recipients' responses to phishing attacks. The findings also confirm differences in relative efficacy of influence techniques. Our research extends understanding of phishing and deception in three ways.

First, because individuals tend to process emails using System 1 thinking, the drawbacks of mediated deception notwithstanding (George et al. 2013), liking, social proof, scarcity, and reciprocity *do* increase the likelihood that individuals will respond to phishing attacks. These findings address a central question posed by past researchers concerning which influence techniques are most effective when individuals use System 1 thinking (Eagly and Chaiken 1993). These findings also support literature describing pitfalls of System 1 processing when dealing with potential security threats (Abbasi et al. 2012, Jingguo et al. 2012).

Second, consistent with past observations, our work also demonstrates variability in the techniques' persuasive efficacy (Guadagno and Cialdini 2005). Prior deception theory (e.g., Buller and Burgoon 1996, Carlson and George 2004) has highlighted the importance of pre-interaction factors such as individual characteristics and context in explaining behavior during deceptive interactions. This work suggests that pre-interaction factors may facilitate or impede the actual *success* of specific strategies deceivers employ (i.e., outcomes of the attempted deception). The categorizations based on fictitious shared experiences and self-determination explain much of the variability in efficacy among the influence techniques. Prior theoretical (e.g., Buller and Burgoon 1996, Carlson and George 2004) and empirical investigation (e.g., Zhou et al. 2004) of deception has focused on interactions where the deceiver and receiver exchange several messages. During repeated message exchange, deceivers may tune their message content to increase their likelihood of successful deception (Burgoon et al. 1999, 2002; Carlson et al. 2004). However, in phishing attacks that entail one-time messages,

influence techniques implying repeated exchanges (reciprocity and consistency) are less effective and more easily identified as fraudulent.

Further, contrary to past literature proposing that deceivers often utilize non-self-determined influence techniques (e.g., Lindsey et al. 2011), our results demonstrate that when the message source is technologically obscured and compliance must be speedily achieved, self-determined influence techniques are more effective. Phishers elicit greater compliance using liking, social proof, and scarcity. Thus, in a similar fashion to the context, self-determination also directly affects the success of a deception attempt. Because these factors are common characteristics in other mediated exchanges, it is likely that they will affect deception outcomes in similar settings.

Third, the negative coefficient for authority was unexpected. We offer two possible explanations for this finding. First, during a phishing attack, a fictitious or impersonated sender must appear to have legitimate authority over something that is important to the recipient (e.g., a bank closing down a recipient's account). It is possible that our participants did not view the impersonated CIO as having legitimate authority or thought it unlikely the CIO would take action against individual students. Second, authority is extensively used in phishing; after repeated exposure to the same phishing tactic, individuals eventually catch on (Jakobsson 2007). Because of the prevalence of such attacks, recipients possibly were resistant to this form of attack.

6.1. Implications for Practice

Although the experimental manipulations presented here were simple changes embedded in a phishing message, they meaningfully affected recipients' susceptibility to phishing attacks. In particular, liking was especially influential among all of the techniques. Phishers who are able to gain the liking of their targets through humor; feigned similarity; or an affiliation with attractive people, desirable groups, or events will likely generate a higher response to their phishing messages. As preferences, social interactions, and relationships increasingly move online (e.g., voluntary sharing through social media), the technique of liking may increase in use among those seeking to influence others.

In highlighting individuals' susceptibility to phishing influence techniques, we call attention to another finding from Cialdini's work, namely, that influence techniques lose some of their potency when the targets are aware of the techniques and their susceptibility to them. In other words, when individuals "gain persuasion knowledge, they may experience a change in meaning and disengage from or even counter argue against the communication" (Pechmann and Wang 2010, p. 140). Hence, through investigating persuasive phishing techniques and their relative effectiveness, research can raise awareness of phishing influence techniques, thereby reducing the effectiveness of phishing attacks. Additionally, the findings underscore the importance of training email users to resist phishing. By highlighting the influence techniques used during phishing and demonstrating which influence techniques are the most dangerous, we direct attention to the development of training programs that trigger defenses against automatic compliance.

Although forewarning has been shown to induce resistance to persuasion, its effects quickly fade (Cameron et al. 2002). Therefore, it is necessary to develop resistance that does not rapidly decline, especially since self-determined influence techniques (e.g., liking) will likely remain robust over time (Deci and Ryan 1985). One potential avenue worthy of exploration is the notion of inoculation against persuasion attempts (McGuire 1970). Researchers have found that inoculating targets to persuasive techniques increases their resistance (Crowley and Hoyer 1994, Friestad and Wright 1994, Szybillo and Heslin 1973). Similar to its immunological analogue, inoculation to persuasion must be contextually specific, and this research is a first step to address that need. However, even the resistance conferred by inoculation wanes after extended periods (Banas and Rains 2010) and inoculation is less effective against self-determined influence techniques (Miller et al. 2013). Therefore, additional research is needed to investigate methods of resistance to self-determined influence techniques that do not fade over time.

6.2. Theoretical Contributions

Although the purview of our investigation was phishing, our work has implications not only for future conceptualizations of phishing but also for theorizing deception and influence. First, for future research on deception, we have demonstrated the usefulness of theories of cognitive processing, influence, and motivation in understanding individuals' susceptibility to deception and phishing. Specifically, using Kahneman's (2011) work on biases in cognitive processing and Cialdini's work on influence, we theorized that because individuals are likely to process emails using System 1, Cialdini's influence techniques would elicit compliance in phishing attacks. This theorizing explains why, despite noted drawbacks of mediated deception (George et al. 2013), influence techniques such as liking, social proof, scarcity, and reciprocity increase the likelihood of recipients' response to phishing attacks.

Second, we extend theory on Cialdini's (2009) influence techniques by viewing them in conjunction with motivation theory. In doing so, we offered an ordering of the previously nominal categories. Specifically, we theorized that the influence tactics evoke an increasing level of targets' PLOC as they move from authority to reciprocity/consistency to social proof/scarcity to liking. We extended this theorizing by positing a second ordering of the influence techniques based on

the requirement that the phisher construct a fictitious backstory. Specifically, we posited that liking, social proof, scarcity, and authority, which do not require the construction of such a backstory, would reveal fewer miscues (Goffman 1959) relative to reciprocity and consistency techniques, which require a backstory. Empirically, we found liking especially influential, followed by scarcity, social proof, and reciprocity; consistency did not significantly influence compliance and authority encouraged *non*compliance.

6.3. Limitations

This study has several limitations that bound the generalizability of our work. First, we did not capture and statistically control for many individual factors (e.g., Web proficiency, security awareness) germane to understanding individuals' susceptibility to phishing attacks. Because of restrictions imposed by the institutional review board, we were not able to gather demographic information. Furthermore, we did not collect other individual factors because we were concerned that questions about proficiency or security beliefs would prime participants to the possibility of a phishing attack. Therefore, we controlled for these factors by randomly assigning participants to experimental conditions, thereby ensuring that individual factors' influence would be evenly distributed across conditions.

Additionally, this field experiment was conducted at a university with student participants. We note that universities are frequent targets of actual phishers because contact emails are often publically listed. The study avoided the artificiality of the lab setting, but our findings are limited by participants' homogeneity. Further, there was no implied financial incentive with the phishing attack and we acknowledge that participants were influenced only by portions of the message they read. However, we anticipate that these findings will be applicable in other populations where members are younger, somewhat "tech savvy," and have some college education. Past phishing research has found that students between ages 18 and 25 fall for phishing more than other age groups (Sheng et al. 2010), although additional research is likely needed to understand the effect of influence techniques on other groups.

6.4. Future Research Directions

There are several ways that future researchers can expand on the findings presented here. First, further attention to the negative coefficient for the authority influence technique is needed. This finding was unexpected; although we have presented two possible explanations for its occurrence, additional research is needed to verify if, in fact, individuals have become more resistant to phishing attempts relying on authority and to understand the reason for this increased resistance.

Second, we have highlighted contextual and motivational reasons for why some influence attempts are more effective in phishing attacks. Other types of mediated message exchanges may exhibit similar characteristics to phishing (e.g., one time, one way deceptive messages, persuasive purpose, and short message life). To the extent that other message exchanges mirror phishing's characteristics, the efficacy ordering of influence techniques presented here is likely to apply. However, additional research is needed to verify this possibility.

Finally, when considered in the broader context of motivation theory, our findings on self-determination merit additional attention. Previous research has shown that intrinsic motivation and self-determined action are robust to the effects of time (Deci and Ryan 1985), meaning that individuals may remain vulnerable to phishing attacks. Training must take care to not undercut participants' intrinsic motivation as a means to counter these phishing tactics. Such attempts could constrict legitimate exchanges, an undesirable and perhaps counterproductive outcome (Jakobsson 2007). Rather than evoking fear, training must sensitize individuals to their vulnerability to liking, social proof, and scarcity influence techniques (Cialdini 2009). Additionally, research may guide the development of inoculation against influence techniques that prompt intrinsic motivation (McGuire 1970) and may investigate methods for encouraging System 2 evaluation, especially when processing requests for private information.

7. Conclusion

Phishing is a scourge on individuals and organizations. By performing this study, we hoped to cast light on why phishing induces individuals to disclose private information and thereby lay the foundation for more effective ways to mitigate such threats. We synthesized cognitive processing, persuasion, and motivation theory and have provided evidence for which influence techniques in phishing messages are especially dangerous. Understanding and recognizing phishing messages are important components of a layered approach to mitigate phishing. Insights from this study can help individuals understand their own vulnerability to phishing attacks and can guide training approaches oriented at reducing vulnerability to phishing.

Acknowledgments

The authors thank the senior editor, Shaila Miranda, associate editor, Glenn Browne, and the anonymous review team for their constructive feedback and guidance through the review process. We would like to thank John Wells at the University of Massachusetts, Izak Benbasat, Ron Cenfetelli, Hasan Cavusoglu, Ning Nan, Kafui Monu and the other participants at the University of British Columbia MIS Research Seminar, Munir Madiwalla, Paul Pavlou, Steve Johnson and the other participants at the Temple FOX MIS Distinguished Speakers Series for providing feedback for this paper.

Figure A.1 Phishing Website

Appendix A. Stimulus Materials

To construct the phishing website (Figure A.1), we purchased a domain name that was very similar to the university's domain name from a popular web hosting provider. We then created a website that was similar in design and appearance to other legitimate university Web pages. The website URL was included as a hyperlink in the message body and in the email signature.

To ensure that our manipulations accurately represented Cialdini's influence techniques, we tested our manipulations using the closed card sorting technique (Coxon 1999) and gathered responses from three executives in Internet companies and four academics (two cognitive psychology faculty and two information systems faculty). This panel was given the definition for each influence technique and then asked to categorize the manipulations into the six influence techniques. All but one panel member sorted the manipulations in the expected categories.[1] Taken together, this initial test provided evidence of face validity (Zimmerman and Akerelrea 2002) and suggested that we accurately represented Cialdini's influence techniques with our manipulations. To improve the realism of the experiment, tools and techniques commonly employed by phishers were used to disseminate the messages. Mass-emailing software was used to distribute the phishing email to participants, and in order to avoid spam filters, the software sent phishing messages to a random group of participants every 10 minutes. The mass-emailing software also had the capability to track emails that were returned as undeliverable or had bounced for some other reason; however, no emails in the sample were returned.

The fabricated website was visited 197 times by unique visitors. Table A.1 presents the operating systems used to access the phishing website. Interestingly, over 30% of the operating systems used to access the site were mobile. With the desktop and laptop machines, 49% utilized Microsoft Internet Explorer, 26% accessed the website via Google Chrome, 18% Apple Safari, and 7% Mozilla Firefox. Further, only 42% (82 subjects) of those who visited the website were attached to the university network. In other words, most participants who fell for the phishing message did so outside of the campus network.

Table A.1 Operating Systems of Devices That Visited the Website

Operating system	Count	Percentage (%)	Device type	Count	Percentage (%)
Windows	102	51.78	Desk-/ Laptop	125	63.45
Mac OSX	22	11.17			
Linux OS	1	0.51			
iPhone OS	30	15.23	Mobile	62	31.47
Android OS	18	9.14			
iPad OS	7	3.55			
Windows Phone OS	6	3.05			
Blackberry OS	1	0.51			
Unknown	10	5.08	Unknown	10	5.08
Total	197	100.0	Total	197	100

Appendix B. Additional Analysis

Since none of Cialdini's influence techniques can be classified in the repeated, non-self-determined category and the only difference between non-self-determined and shared experience categories is the authority influence technique, we performed the test of H2 and H3 using quadrants of Figure 3 and reported the findings in Table 6. To ensure that our hypotheses were supported, we performed two additional logistic regressions with one regression testing no

[1] The one panel member categorized four of six influence techniques correctly, but mismatched reciprocity and social proof.

Table B.1 Effects of Fictitious Shared Experiences on Likelihood of Responding

Variables	B	Wald	Sig. ($df = 1$)
Intercept	−3.472	252.627	<0.001
No Fictitious Shared Experiences	0.482	35.467	<0.001
Gender[a]	−0.434	7.568	0.006

Notes. Omnibus test of model coefficients: χ^2 (7, $N = 2{,}624$) = 43.838, $p < 0.001$. − 2 Log likelihood: 1,257.683 |Nagelkerke R^2: 0.042| Hosmer and Lemeshow test: 0.695.
[a]Female = 0, male = 1.

Table B.2 Effects of Self-determination on Likelihood of Responding

Variables	B	Wald	Sig. ($df = 1$)
Intercept	−3.918	306.723	<0.001
Self-determination	0.858	74.509	<0.001
Gender[a]	−0.447	7.871	0.005

Notes. Omnibus test of model coefficients: χ^2 (7, $N = 2{,}624$) = 89.344, $p < 0.001$. − 2 Log likelihood: 1,212.178 |Nagelkerke R^2: 0.082| Hosmer and Lemeshow test: 0.562.
[a]Female = 0, male = 1.

fictitious shared experiences versus fictitious shared experiences (H2) and the other testing self-determined versus non-self-determined (H3). The first test demonstrated a significant effect for no fictitious shared experiences, which was consistent with H2 (see Table B.1). The second test demonstrated a significant effect for self-determination, which was consistent with H3 (see Table B.2).

References

Abbasi A, Zahedi F, Chen Y (2012) Impact of anti-phishing tool performance on attack success rates. *IEEE Internat. Conf. Intelligence and Security Informatics, Washington, DC*, 12–17.

Abbasi A, Zhang Z, Zimbra D, Chen H, Nunamaker JFJ (2010) Detecting fake websites: The contribution of statistical learning theory. *MIS Quart.* 34(3):435–461.

Acohido B (2013) Bogus IRS e-mail swamps the Internet yet again. *USA Today* (April 15), Retrieved May 15, 2013, http://www.usatoday.com/story/tech/2013/04/15/irs-tax-fraud-cybercrime-phishing-attack/2078927/.

Afifi A, May S, Clark VA (2003) *Computer-Aided Multivariate Analysis* (CRC Press, Boca Raton, FL).

Anti-Phishing Working Group (2013) Phishing Activity Trends Report: Global Phishing. Retrieved January 2, 2014, http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf.

Banas JA, Rains SA (2010) A meta-analysis of research on inoculation theory. *Comm. Monographs* 77(3):281–311.

Barrett D, McKinnon JD (2014) Identity theft triggers a surge in tax fraud. *Wall Street Journal* (February 23), Retrieved March 11, 2014, http://online.wsj.com/news/articles/SB10001424052702304834704579401411935878556.

Brehm JW (1989) Psychological reactance: Theory and applications. *Adv. Consumer Res.* 16(1):72–75.

Buller D, Burgoon JK (1996) Interpersonal deception theory. *Comm. Theory* 6(3):203–242.

Buller D, Burgoon J, Buslig A, Roiger J (1996) Testing interpersonal deception theory: The language of interpersonal deception. *Comm. Theory* 6(3):268–289.

Burger JM, Messian N, Patel S, Prado AD, Anderson C (2004) What a coincidence! The effects of incidental similarity on compliance. *Personality Psych. Bull.* 30(1):35–43.

Burgoon JK, Bonito JA, Bengtsson B, Ramirez A, Dunbar N (1999) Testing the interactivity model: Communication processes, partner assessments, and the quality of collaborative work. *J. Management Inform. Systems* 16(3):33–56.

Burgoon JK, Bonito JA, Ramirez A, Dunbar NE, Kam K, Fischer J (2002) Testing the interactivity principle: Effects of mediation, propinquity, and verbal and nonverbal modalities in interpersonal interaction. *J. Comm.* 52(3):657–677.

Bushman B (1984) Perceived symbols of authority and their influence on compliance. *J. Appl. Soc. Psych.* 14(6):501–508.

Caldwell T (2013) Spear-phishing: How to spot and mitigate the menace. *Comput. Fraud and Security* 2013(1):11–16.

Cameron KA, Jacks JZ, O'Brien ME (2002) An experimental examination of strategies for resisting persuasion. *Current Res. Soc. Psych.* 7(12):205–225.

Carlson J, George J (2004) Media appropriateness in the conduct and discovery of deceptive communication: The relative influence of richness and synchronicity. *Group Decision Negotiation* 13(2):191–210.

Carlson JR, George JF, Burgoon JK, Adkins M, White CH (2004) Deception in computer-mediated communication. *Group Decision Negotiation* 13(1):5–28.

Castilla EJ (2011) Managerial influence in workplace inequality. *Amer. Sociol. Rev.* 76(5):667–694.

Chen Y, Zahedi F, Abbasi A (2011) Interface design elements for anti-phishing systems. Jain H, Sinha A, Vitharana P, eds. *Service-Oriented Perspectives in Design Science Research* (Springer, Berlin, Heidelberg), 253–265.

Cialdini R (2001) Harnessing the science of persuasion. *Harvard Bus. Rev.* 79(9):72–79.

Cialdini R, Goldstein NJ (2004) Social influence: Compliance and conformity. *Annual Rev. Psych.* 55(3):591–621.

Cialdini R, Cacioppo JT, Bassett R, Miller JA (1979) Low-ball procedure for producing compliance: Commitment then cost. *J. Personality Soc. Psych.* 36(5):463–476.

Cialdini RB (2009) *Influence: Science and Practice*, 5th ed. (Scott-Foresman, Glenview, IL).

Cialdini RB, Trost MR (1998) Social influence: Social norms, conformity, and compliance. Gilbert D, Fiske ST, Lindzey G, eds. *The Handbook of Social Psychology* (McGraw-Hill, Boston), 151–193.

Cialdini RB, Petty RE, Cacioppo JT (1981) Attitude and attitude change. *Annual Rev. Psych.* 32(1):357–404.

Cohen D (2013) Online fraud report. EMC, New York, December 2013, p. 5. Accessed May 19, 2014, http://www.emc.com/collateral/fraud-report/rsa-fraud-report-062013.pdf.

Conti G, Sobiesk E (2010) Malicious interface design: Exploiting the user. *19th Internat. Conf. World Wide Web* (ACM, Raleigh, NC), 271–280.

Coxon A (1999) *Sorting Data: Collection and Analysis* (Sage Publications, Thousand Oaks, CA).

Crowley AE, Hoyer WD (1994) An integrative framework for understanding two-sided persuasion. *J. Consumer Res.* 20(4):561–574.

Deci EL, Ryan RM (1985) *Intrinsic Motivation and Self-Determination in Human Behavior* (Plenum, New York).

Dhamija R, Tygar JD, Hearst M (2006) Why phishing works. *Comput. Human Interaction Conf. Association Comput. Machinery, Montreal*, 581–590.

Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Inform. Systems Res.* 17(1):61–80.

Dodge RC, Jr, Carver C, Ferguson AJ (2007) Phishing for user security awareness. *Comput. Security* 26(1):73–80.

Donath JS (1999) Identity and deception in the virtual community. Smith MA, Kollack P, Heywood I, eds. *Communities in Cyberspace* (Taylor & Francis, Inc., London), 29–59.

Drachman D, deCarufel A, Inkso CA (1978) The extra credit in interpersonal attraction. *J. Experiment. Soc. Psych.* 14(5):458–467.

Dubrovsky VJ, Kiesler S, Sethna BN (1991) The equalization phenomenon: Status effects in computer-mediated and face-to-face decision-making groups. *Human-Comput. Interaction* 6(2):119–146.

Eagly AH, Chaiken S (1993) *The Psychology of Attitudes* (Harcourt Brace Jovanovich College Publishers, Orlando, FL).

Egelman S, Cranor LF, Hong J (2008) You've been warned: An empirical study of the effectiveness of Web browser phishing warnings. *Twenty-Sixth Annual SIGCHI Conf. Human Factors Comput. Aystems* (ACM, Florence, Italy), 1065–1074.

Finn P, Jakobsson M (2008) Designing and conducting phishing experiments. *IEEE Tech. Soc.* 6(2):66–68.

Friestad M, Wright P (1994) The persuasion knowledge model: How people cope with persuasion attempts. *J. Consumer Res.* 21(1):1–31.

Gagné M, Deci EL (2005) Self-determination theory and work motivation. *J. Organ. Behav.* 26(4):331–362.

George JF, Carlson JR, Valacich JS (2013) Media selection as a strategic component of communication. *MIS Quart.* 37(4):1233–1251.

Gerow JE, Ayyagari R, Thatcher JB, Roth PL (2013) Can we have fun @ work? The role of intrinsic motivation for utilitarian systems. *Eur. J. Inform. Systems* 22(3):360–380.

Glasziou P, Haynes B (2005) The paths from research to improved health outcomes. *Evidence Based Nursing* 8(2):36–38.

Goffman E (1959) *The Presentation of Self in Everyday Life* (Doubleday, New York).

Greenwald AG (1968) Cognitive learning, cognitive response to persuasion, and attitude change. Greenwald AG, Brock TC, Ostrom TM, eds. *Psychological Foundations of Attitudes* (Academic Press, New York), 147–170.

Groves RM, Cialdini RB, Couper MP (1992) Understanding the decision to participate in a survey. *Public Opinion Quart.* 56(4): 475–495.

Grow B, Epstein K, Tschang C-C (2008) The new e-spionage threat. *BusinessWeek* (April 9), Retrieved May 15, 2013, http://www.businessweek.com/stories/2008-04-09/the-new-e-spionage-threat.

Guadagno R, Cialdini R (2005) Online persuasion and compliance: Social influence on the internet and beyond. Amichai-Hamburger Y, ed. *The Social Net: Understanding Human Behavior in Cyberspace* (Oxford University Press, London), 91–114.

Guadagno R, Cialdini R (2007) Persuade him by email, but see her in person: Online persuasion revisited. *Comput. Human Behav.* 23(2):999–1016.

Harris EA, Perlroth N, Popper N, Stout H (2014) A sneaky path into Target customers' wallets. *New York Times* (January 18), Retrieved March 11, 2014, http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html?_r=0.

Healey J (2013) China is a cyber victim, too. *Foreign Policy* (April 16), Retrieved April 18, 2013, http://www.foreignpolicy.com/articles/2013/04/16/china_is_a_cyberwar_victim_too.

Hesseldahl A (2011) Lockheed Martin confirms it came under attack. Retrieved May 15, 2013, http://news.cnet.com/8301-1009_3-20067190-83.html.

Hoetker G (2007) The use of logit and probit models in strategic management research: Critical issues. *Strategic Management J.* 28(4):331–343.

Hong J (2012) The state of phishing attacks. *Comm. ACM* 55(1):74–81.

Hosmer DW, Lemeshow S (2004) *Applied Logistic Regression* (John Wiley & Sons, Hoboken, NJ).

Howard DJ, Gengler C, Jain A (1995) What's in a name? A complimentary means of persuasion. *J. Consumer Res.* 22(2):200–211.

Hoyle RH, Harris MJ, Judd CM (2002) *Research Methods in Social Relations*, 7th ed. (Wadsworth Publishing Company, Belmont, CA).

Jagatic T, Johnson N, Jackobsson F (2007) Social phishing. *Comm. ACM* 50(10):94–100.

Jakobsson M (2007) The human factor in phishing. Privacy and security of consumer information. Retrieved May 15, 2013, http://www.informatics.indiana.edu/markus/papers/aci.pdf.

Jingguo W, Herath T, Rui C, Vishwanath A, Rao HR (2012) Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *Professional Comm., IEEE Trans.* 55(4): 345–362.

Kahneman D (2011) *Thinking, Fast and Slow* (Farrar, Straus, and Giroux, New York).

Kaufman RL (1996) Comparing the effects of dichotomous logistic regression: A variety of standardized coefficients. *Soc. Sci. Quart.* 77(1):90–109.

Lindsey LLM, Dunbar NE, Russell JC (2011) Risky business or managed event? Perceptions of power and deception in the workplace. *J. Organ. Culture, Comm. Conflict* 15(1):55–79.

Malhotra Y, Galletta DF, Kirsch LJ (2008) How engogenous motivations influence user intentions: Beyond the dichotomy of extrinisic and instrinsic user motivation. *J. Management Inform. Systems* 25(1):267–299.

McCornack SA, Parks MR (1990) What women know that men don't: Sex differences in determining the truth behind deceptive messages. *J. Soc. Personal Relationships* 7(1):107–118.

McGuire WJ (1970) A vaccine for brainwash. *Psych. Today* 3(9):36–39.

Miller CH, Ivanov B, Sims J, Compton J, Harrison KJ, Parker KA, Parker JL, et al. (2013) Boosting the potency of resistance: Combining the motivational forces of inoculation and psychological reactance. *Human Comm. Res.* 39(1):127–155.

Myers S (2007) Introduction to phishing. Jakobsson M, Myers S, eds. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (John Wiley & Sons, Hoboken, NJ), 1–29.

Norton EC, Wang H, Ai C (2004) Computing interaction effects and standard errors in logit and probit models. *Stata J.* 4(2):154–167.

Paese PW, Gilin DA (2000) When an adversary is caught telling the truth: Reciprocal cooperation versus self-interest in distributive bargaining. *Personality Psych. Bull.* 26(1):75–90.

Pechmann C, Wang L (2010) Effects of indirectly and directly competing reference group messages and persuasion knowledge: Implications for educational placements. *J. Marketing Res.* 47(1):134–145.

Petty RE, Ostrom TM, Brock TC (1981) Historical foundations of the cognitive response approach to attitudes and persuasion. Petty RE, Ostrom TM, Brock TC, eds. *Cognitive Responses in Persuasion* (Erlbaum, Hillsdale, NJ), 5–29.

Puhakainen P, Siponen M (2010) Improving employees' compliance through information systems security training: An action research study. *MIS Quart.* 34(4):757–778.

Radicati S (2012) Email statistics report 2011–2015. Retrieved May 15, 2013, http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf.

Regan RT (1971) Effects of a favor on liking and compliance. *J. Experiment. Soc. Psych.* 7(6):627–639.

Ryan RM, Connell JP (1989) Perceived locus of causality and internalization: Examining reasons for acting in two domains. *J. Personality Soc. Psych.* 57(5):749–761.

Ryan RM, Deci EL (2000) Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *Amer. Psych.* 55(1):68–78.

Sagarin BJ, Mitnick K (2012) The path of least resistance. Kenrick DT, Goldstein N, Braver S, eds. *Six Degrees of Influence: Science, Application, and the Psychology of Robert Cialdini* (Oxford University Press, Oxford, UK), 27–38.

Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J (2010) Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *28th Internat. Conf. Human Factors Comput. Systems* (ACM, Atlanta), 373–382.

Stanovich KE, West RF (2000) Individual differences in reasoning: Implications for the rationality debate? *Behav. Brain Sci.* 23(5): 645–665.

Sundie JM, Cialdini RB, Griskevicius V, Kenrick DT (2012) The world's (truly) oldest profession: Social influence in evolutionary perspective. *Soc. Influence* 7(3):1–20.

Szybillo GJ, Heslin R (1973) Resistance to persuasion: Inoculation theory in a marketing context. *J. Marketing Res.* 10(4):396–403.

Tan BC, Wei KK, Watson RT, Walczuch RM (1998) Reducing status effects with computer-mediated communication: Evidence from two distinct national cultures. *J. Management Inform. Systems* 15(1):119–142.

Trotman KT, Wright AM, Wright S (2005) Auditor negotiations: An examination of the efficacy of intervention methods. *Accounting Rev.* 80(1):349–367.

Vaidyanathan R, Aggarwal P (2005) Using commitments to drive consistency: Enhancing the effectiveness of cause-related marketing communications. *J. Marketing Comm.* 11(4):231–246.

Vance A, Elie-Dit-Cosaque C, Straub DW (2008) Examining trust in information technology artifacts: The effects of system quality and culture. *J. Management Inform. Systems* 24(4):73–100.

Venkatesh V (1999) Creation of favorable user perceptions: Exploring the role of intrinsic motivation. *MIS Quart.* 23(2):239–260.

Venkatesh V (2000) Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Inform. Systems Res.* 11(4):342–346.

Ward A, Brenner L (2006) Accentuate the negative. The positive effects of negative acknowledgment. *Psych. Sci.* 17(11):959–965.

Workman M (2008) Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *J. Amer. Soc. Inform. Sci. Tech.* 59(4):662–674.

Wright R, Marett K (2010) The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *J. Management Inform. Systems* 27(1):273–303.

Wright R, Chakraborty S, Basoglu A, Marett K (2010) Where did they go right? Investigating deception cues in a phishing context. *Group Decision Negotiation* 19(4):391–416.

Xiao B, Benbasat I (2011) Product-related deception in e-commerce: A theoretical perspective. *MIS Quart.* 35(1):169–195.

Zhou L, Burgoon JK, Twitchell DP, Qin T, Nunamaker J (2004) A comparison of classification methods for predicting deception in computer-mediated communication. *J. Management Inform. Systems* 20(4):139–166.

Zimmerman DE, Akerelrea C (2002) A group card sorting methodology for developing informational Web sites. *IEEE Professional Comm. Conf., Portland, OR*.