Running head: MOBILE DEVICE AFFORDANCE

Mobile Device Affordance: Explicating How Smartphones Influence
The Outcome Of Phishing Attacks

Arun Vishwanath, Ph.D., MBA

University at Buffalo

Author Note. Arun Vishwanath, Ph.D., MBA is Associate Professor of Communication and Management Science & Systems, University at Buffalo (UB), Buffalo, NY 14260.

Please address all correspondence to Arun Vishwanath, phone: 716-645-1163, fax: 716-645-2064; email: avishy@buffalo.edu

Supported by NSF SaTC grant # 1227353

Abstract

Recent research has demonstrated that individuals fall victim to phishing because of the joint and independent influence of email habits and cognitive heuristics. Much of this work has, however, ignored the influence of smartphones and mobile devices—which are now utilized by the majority of the U.S. population—and it remains to be seen whether the manifestation of habits or heuristic processing is heightened on such devices. To this end, the current research conducted simulated phishing attacks that varied in the cues available in the email and examined how the devices used by subjects to access it influenced the outcome of the attack. The overall results point to a moderating role of device affordances on email habits rather than heuristic processing. It appears that the load of emails a person reads potentiates mobile device usage and thusly leads to the strengthening of email habits. The presence of graphical cues in the email heightened heuristic processing but this was not significantly enhanced on mobile devices. The overall results have important implications for our understanding of the affordances of smartphones, and how they enhance the likelihood of online deception.

Keywords: phishing, habit strength, heuristic processing, device affordance, deception

- Mobile Device Affordance: Explicating How Smartphones Influence

The Outcome Of Phishing Attacks

By now, almost all adult Internet users in the United States are already victims of a cyber attack—a sobering conclusion arrived at by cumulating the number of individuals whose personal information was compromised in 2014 (Walters, 2014). 2015 saw a continuation of this trend, with the much-publicized breach of one of the nation’s largest health insurance firms, Anthem Inc., in February alone compromising more than 20 million health records (Hiltzik, 2015). Following this were attacks into the Office of Personnel Management (OPM), breaches reported by over a dozen educational institutions including Harvard University (Kuranda, 2015), and even a major hack into the White House’s email servers (Schmidt & Sanger, 2015). Attacks of a similar scale have been reported in the U.K., Germany, Israel, Singapore, and India, highlighting the global scope of the problem (Martin, 2015).

And, the viciousness of these attacks has grown even more in 2016. In the first few months of this year, we have witnessed the rise of a new class of attacks called “ransomware” in which hackers encrypt individual computers and release the data only if a ransom is paid within a deadline. Such attacks have already netted over \$300 million in ransoms by victimizing many individuals, major hospitals, universities, and government institutions.¹

While the motives for these attacks range from theft to cyber vandalism, activism, and industrial and national espionage, almost all the attacks have one thing in common: they use spearphishing as the vector to initially gain access to an individual’s computer and infiltrate networks (“APT 1,” 2013).

¹ <https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise>

Today's spearphishing is different from "old school" phishing attacks. Those came in the form of the infamous Nigerian email, where the phisher claimed to be a wealthy benefactor needing the victim's help, usually in the form of their bank account details, to clear funds locked-up in some war-torn nation. These attacks necessitated correspondence and negotiation with the phishers—which usually revealed the deception and made these attacks minimally successful (Vishwanath, 2016).

Current spearphishing attacks come in the form of personalized emails purporting to be from reputable sources such as banks or universities. Emails carry a malware payload hidden within a hyperlink or attachment in the email along with a message egging the victim to click on them. Clicking on the links or attachments open backdoors into computer networks that are then used to mine the victim's computer or launch attacks onto others. This is precisely how many major attacks from the OPM breach to the hack into the White House's email servers took place.

Spearphishing does not require any interaction with the phisher prior to victimization and there are no technological protections that can stop such attacks. All it needs is for someone to open the email or click on the links and attachments, which 30-60% of the intended targets of such attacks do—making spearphishing a very effective cyber attack vector (Vishwanath, 2016). Stopping such attacks is hard and necessitates an understanding of the human actor who clicks on the links and attachments and falls prey to such attacks (Vishwanath, 2015a).

Extant research points to two reasons why people click on phishing links and attachments. One implicates people's cognitive processing and their reliance on mental short-cuts or heuristics. Thus, rather than reading the contents of the email and thinking through the request, individuals tend to focus on simple cues in the email—the sender's name, their email id, graphical trust symbols such as brand logos and signatures—that allow for cognitively effortless

heuristic judgments about the email's authenticity. The other reason is people's media habits that form overtime as they routinely use email and social media. Thus, as soon as an email or social media notification arrives, people with entrenched email habits tend to mindlessly react to it and click on its contents, without nary a thought about its ramifications (Vishwanath, Harrison, & Ng, 2015). Recent research on phishing has shown the use of heuristics and habits occurring independently of each other, with their cumulative effects overwhelming any advantage from anti-phishing training or education (Vishwanath, 2015c).

Much of this work has, however, examined heuristic processing and media habits' effects on people who access emails on personal computers, ignoring the rise of mobile devices. In recent years, the use of mobile devices have quickly outpaced the use of personal computers, with Pew Center polls reporting close to 60% of adult Internet users in the U.S. and U.K. using a smartphone to access the Internet ("Mobile technology fact sheet," 2014). But the extent to which smartphone use influences phishing-based information processing and habits remains unknown. Examining the effects of smartphone on these determinants of phishing-based victimization is the overarching goal of the current exploration.

The paper begins this examination by first explicating the concept of technology affordance—the usual starting point for research on technology-mediated effects (Sundar, 2008)—and examining the affordance of mobile phones and the constituent processes it potentiates.

Technology Affordances

Technology affordances stem from the manifest functions intentionally created by its developers and from users' expectations derived from their prior experience and interactions

with technologies (Gibson, 1977). Together these influence not only how people approach and use a technology but also their state of mind while utilizing it.

Affordances can be viewed along a continuum based on the degree to which the functions of a technology complement the actions required to utilize them. While some technologies have inter-referential functionalities, i.e., their functions match the actions necessary to use them (Gaver, 1991), many others are somewhere along the continuum, which necessitate cues to signal the function-action link. For instance, the functionality of a staircase that leads to another floor is clear but a hyperlink on a webpage pointing to another page needs a cue such as an underlined text indicating this possibility. Users, because of the equivocality of many online technologies, are also particularly sensitive to such cues, often seeking them out and reacting to them, when online. Much of the extant research on affordances has, therefore, focused on the available cues on technology interfaces and the heuristics they activate in users (Kim & Sundar, 2015).

But, arguably, the need for such cues diminishes as users frequently utilize a technology and get familiar with it. For instance, many webpages no longer underline hyperlinked pages. Likewise, email programs, which in the past used to spell-out functions like “compose” and “send,” now just display simple icons, because users require less cues to signal these possibilities. It is therefore foreseeable that as people’s utilization of technology functions become routinized, not only will their sensitivity to such cues diminish even more, but also that many users would be capable of automatically performing these actions in the absence of any cues, whenever the context presents itself.

A simple everyday technology example elucidating this possibility is the light switch. All children need to be taught what different light switches look like, where they are located, and how they work. Overtime, these actions are frequently repeated and get routinized so that most

adults whenever they are in a dark room switch on lights, oftentimes unaware that they did so. The behavior of switching-on lights, thus, becomes a dynamic action script that can be routinely and ritualistically performed on different types of light switches and in different rooms, even rooms or switches we have no prior experience with, whenever the context of darkness presents itself. This is a form of behavioral automaticity that does not require a cue or any cognitive involvement—that is, it is a habit.

Thus, there are two streams of research that allows us to speculate about the affordances of smartphones and their influence on the outcomes of a spearphishing attack. The first, a cognitive orientation focuses on affordances as cues within various aspects of technology-mediated interactions that trigger heuristics and influence perceptions. This line of thinking suggests that if users were more prone to processing emails on mobile phones rather than on computers heuristically, they would be more reactive to heuristic cues contained within spearphishing emails. The other approach argues for devices providing the contextual support for the enactment of habitual patterns. This line of thinking would suggest that if mobile device leads to stronger email habits than computer use, it would provide the context for people to fall prey to spearphishing attacks regardless of the specific content in the email. Given that habits and heuristic processing independently lead to phishing victimization (Vishwanath, 2015c), understanding whether mobile device affordances lead to heuristic processing or habitual reaction is important for theory as well as for better combating phishing.

Examining the relative effects of device affordances requires stimuli that vary in cues, so as to be able to discern whether heuristic processing is indeed heightened while using devices, and a natural media-use environment, where people's ritualistic email use patterns and cognitive processing can manifest. To this end, the study experimentally simulates two real-world phishing

attacks, a hyperlink attack and an attachment attack, both with and without graphic cues, on different samples of undergraduate students. The studies are conducted sequentially and build on each other, with the first study focusing on email habits and processing and the second also incorporating their known antecedents and covariates. Each study post-hoc assessed whether subjects accessed the attack on a smartphone or a personal computer and the extent to which this influenced their heuristic processing or email habits. Together, the studies provide a comprehensive understanding of how device affordances influence phishing and pinpoints exactly where these effects comes from.

The paper next explicates the cognitive view on device affordance followed by the media habits perspective. This is followed by a presentation of the two research studies and their findings, followed by an overall discussion of their implications in the ensuing section.

Device affordance influence through cognitive processing

The most influential line of research on the cognitive effects of technology affordances is by Sundar and the media effects lab at Penn State (Sundar, 2008). Sundar views technology as a repository of MAIN cues signaling the structure of information or Modality; Agency or sources of information; Interactivity or the types of actions the technology permits; and Navigability suggestive of how a user might be transported within the technology (Sundar, 2008). The underlying rationale for how these cues influence perceptions comes from the Heuristic-Systematic Model (HSM), which distinguishes between two co-occurring modes of cognitive processing that people utilize—an effortful, elaborate systematic processing and an efficiency motivated heuristic processing that relies on mental shortcuts. The HSM views people as information misers who eschew cognitive effort and therefore prefer or even look for simple cues

that allow for snap judgments. Drawing from this Sundar contends that technology affordances abound in rich MAIN cues that bias users towards heuristic processing (Kim & Sundar, 2015).

Take the Facebook friend-request as a case in point. For the receiver, it provides cues in the profile picture of the sender and a count of the number of friends and mutual friends, which ostensibly trigger heuristics about the familiarity or popularity of the requestor without the need to probe the sender's Facebook profile extensively (Vishwanath, 2014). Likewise, email programs prominently display adjunct cues such as the name of the sender, their email address, and oftentimes logos and signatures in the email's body that could trigger heuristics about the sender's credibility. Email interfaces also display drop-down navigation menus, and at times, hyperlinks to external sites or cues indicating the types of files attached (.doc, .PDF, .exe), which could trigger heuristics about the legitimacy of an email's request. For instance, seeing a hyperlink to a person's company homepage might trigger thoughts of the source's legitimacy. In contrast, seeing say an executable (.exe) program file attached to a person's email rather than a more routine Adobe (.PDF) or Word (.doc) file, which most people receive routinely and perceive as safe, could lead to a snap judgment about the email's authenticity.

Several facets of the design of smartphones suggest a heightened reliance on such afforded heuristic cues. For one, smartphones are designed primarily for media consumption. Compared to the average PC, smartphones have smaller screens and utilize mobile "apps" (applications) that are designed for quick downloads and to be frugal in what they display in the constrained space. Further, smartphone navigation is mostly touch-based that due to smaller screen sizes necessitates menus and navigational icons to be readily available and prominently displayed. Viewing a lengthy page or toggling between multiple pages is an effortful process made even more tedious depending on the device's processing ability, the organization of a

webpage, and the contents of the page. As a consequence, smartphone design and layout emphasize rich graphical cues over textual content, which the MAIN model argues potentiates heuristic processing (Sundar, 2008). This was demonstrated in a recent experiment where subjects whose attention was focused on a video ad with more cues versus a plain text ad on different sized smartphones, heuristically processed the video content, and due to the immersive nature of video, invoked more transportation and realism heuristics while viewing it on the larger screen (Kim & Sundar, 2015). A second facet relates to how smartphones are used in the real world. Most people utilize smartphones while on the go, often while simultaneously engaging in multiple tasks ranging from talking to texting and driving. Such multitasking on smartphones reduces the cognitive resources available for effortful systematic processing (Chaiken, 1987; xxx, xxx). Thus, not only does smartphone design emphasize cues, but the nature of how people use these devices leads to a preference for heuristic cues that are readily accessible and easy to decode with minimal cognitive effort.

This heightened reliance on heuristics on smartphones is particularly problematic when it comes to phishing email processing where heuristic processing has been shown to be among the leading reasons for individual victimization. Data from simulated attacks suggest that heuristic processing makes people significantly times more likely to fall prey to a phishing attack on email and on Facebook (Vishwanath et al., 2015). While much of this research focuses on individuals using personal computer to access the phish, the use of a smartphones could likely enhance such deception in three important ways.

For one, while phishers seldom utilize videos in their emails, most embed hyperlinks or PDF attachments into emails to hide malware, which smartphone email apps by design tend to prominently display in the email's body along with action menus (reply, forward, delete) that

impel a snap response rather than foster focused processing. Two, the design of smartphone email apps limits the information about the email's source to simple cues such as the sender's name and email id, both of which are easily spoofed by phishers. Authenticating the sender requires an examination of the email's full-header that reveals the path and originating server. While this can be made a default setting on most PC-based email programs, many smartphone email apps (e.g., iOS) just do not provide this information, while on others it is a tedious task requiring multiple navigational steps that most economy minded users are unlikely to engage in. Finally, reading message content on the smaller screen of a smartphone's email application requires navigating down the page, which conceals the sender's email ID and name but brings into prominent focus the sender's company-logo or signature that could trigger source credibility heuristics. Such logos are easily spoofed and commonly accompany phishing emails, making it significantly more likely that such emails when accessed on smartphones are heuristically processed. Together, these make a case for device affordances stimulating heuristic processing and such processing being heightened when emails contain such graphical cues.

H1. Individuals are significantly more likely to heuristically process phishing emails, even more so when the email contains a rich cue such as a logo, when accessing them on a mobile device than on a personal computer.

Device affordances influence through habits

A competing explanation for device effects comes from the media habits literature. Media habits are defined as a person-centered automaticity that develops overtime as people routinely use a medium, platform, or device. Media habits begin as purposeful behaviors (such as checking email on your smartphone), often in response to specific cues (such as notification sounds or having a smartphone on hand), and the actions provide some level of gratifications

(such as getting information or passing time) (Verplanken, 2006; Verplanken & Wood, 2006).

Through frequent repetition, these form a behavioral loop leading to a pattern of gratifying behavior in response to the stimulating cues. Overtime the relationship between the stimuli, the gratifications sought, and the actions get blurred such that they are performed independent of the cues, the original context within which the behavior was conducted, and the gratifications that were sought—at which point scholars believe a media habit has taken hold (LaRose, 2010; Wood & Neal, 2007).

Habitual patterns by themselves are not problematic because they are formed for behavioral efficiency (LaRose, 2010). For instance, patterns like wearing seat-belts as soon as we sit in a car or checking email, visiting a news website, or viewing our social media feeds as soon as we are awake, become routinized so as not have to reassess the details of our morning routines each and every day. But the same routines could also lead to dangerous outcomes such as when people check their phones or reply to messages while they drive. Thus, on the one hand habits are necessary in order to reduce the cognitive strain of needing to reevaluate every behavior we perform, but on the other, habits could lead to carelessness and mistakes in judgment.

More recent research on media habits finds evidence of habits leading to deception via phishing on social media (Vishwanath, 2015b). It appears that people with strong Facebook habits tend to be significantly more likely to accept a friend-request from a phisher's phony profile and even provide information to this individual when asked. Email habits likewise appear to enhance victimization (Vishwanath, 2014). When individuals receive a phishing email with a hyperlink in it or even an attachment, individuals with strong email habits are significantly more likely to click on them (Vishwanath et al., 2015).

Emerging research suggests that habits are rooted in distinct parts of human behavior and separate from cognitive processing (Vishwanath, 2015c). Habits are rooted longer-term stable facets of individual experience (personality, self-regulation) while cognitive processing is contingent on immediate, contextual considerations such as the importance of the specific decision, the amount of information available, and the amount of information accessible. Furthermore, habits, because they are routinized, consistently manifest themselves (such as reaching for our smartphone to check email as soon as we wake up every morning) in contrast to information processing that is predicated on users and their information environment (such as cue availability, heuristic accessibility, and applicability) (Vishwanath, 2015c). Thus, although both habits and processing lead to deception through phishing, they appear to have significantly different antecedents and paths of influence. Direct evidence from neurological research also supports this contention finding habitual patterns stored in a more primitive area of the human brain, distinct from where cognitively mediated actions are manifested (Graybiel, 2008; Yin & Knowlton, 2006). Demonstrating the independent and distinct nature of habitual patterns, the medical literatures provides a number of cases where individuals having lost their ability to create or store new memories, continue to recreate and enact complex patterns of habitual behaviors (Bayley, & Squire, 2002). Thus, email habits provide an alternative conduit for device affordance.

Two factors unique to today's smartphone design and use make a case for its influence on email habits. First, unlike personal computers, smartphones are always on, easy to carry, and power efficient. Portability and all-day-battery life make smartphones and tablets among the last devices people view prior to getting into bed and often the first device many people ritualistically reach for upon waking-up. Second, unlike many personal computers, smartphones pull data and

social feeds from servers and make people aware of incoming messages through notification sounds and other signals. Depending on the smartphone, the email-app, and the server, the data-pulls occur at various irregular intervals, making it almost necessary to check one's smartphone throughout the day and manually refresh (or ping) the servers for new data intermittently. Such frequent interactions oftentimes net new emails that provide a sense of gratification and stimulate continued checking. This hand-in-hand with notification sounds and indicator lights creates a Pavlovian behavioral loop of constant checking interspersed with moments of gratification, which overtime leads to continued email checking whenever the mobile device is accessible, regardless of the notification sounds or other cues. Thus, email use on smartphones is designed on a variable-reinforcement mechanism—the same underlying principle at the core of devices such as slot machines that foster compulsivity (Blaszczynski, & Nower, 2002). Based on this, a case can be made for device affordances influence on phishing-based deception through email habits.

The influence of device affordances on habits could be in one of two ways. Devices could enhance habits, after all having a smartphone or tablet provides the contextual support for the formation of habits. Having an always on smartphone or tablet and having it close or on-person does make habits easier to enact. Thus as soon as a phishing email arrives on a smartphone, it is plausible that an individual with strong email habits would ritualistic open emails and click on hyperlinks or attachments on it. These effects could also be in the other direction, with email habits leading to people owning devices that can go online quickly, that have apps to check email, and that provide an easy means to access social feeds and emails. The net effect of either of these would be a moderating effect for devices due to their affordances, leading to the following:

H2. Email habit strength rather than heuristic processing will be moderated by the use of mobile device.

Overall Methods

The study conducted simulated phishing attacks on undergraduate students enrolled in the University at Buffalo's Singapore program. IRB approval was procured prior to the start of the res. Students were used because they are often targeted by phishers, and most higher-education institutions in the U.S. expend significant IT resources to protect them (Kuranda, 2015), making them a particularly important group to study. For example, Penn State University students' personal records were recently compromised ostensibly using a phishing attack as the entry vector (Schwartz, 2015). The study also needed a controlled test environment where the different types of phishing emails' could be deployed and studied; where the subject pool would be mostly homogenous in experience and access, providing high internal validity; and where participation rates would not hinder conclusion validity.

Study 1

Method

A common vector used by phishers is to embed a hyperlink into an email, with a short message egging potential victim to click on it ("APT1", 2013). For instance, the Syrian Electronic Army (SEA) used a hyperlink to hack into the networks of Forbes (Greenberg, 2014). Usually such hyperlinks open websites that run scripts or forms that directly poll for credentials, which are used to compromise the victim's computer. Many phishing attacks also utilize brand names, logos, and names of well-known organizations to enhance the credibility of the phishing request.

In the spring semester, two identical emails were created, one incorporating the logos of the University along with a message and another with just the textual-message. Each email asked respondents to click on a hyperlink, which was concealed using an URL-shortner. The link when clicked deployed the websurvey for the study. Figure 1A and B present the stimuli.

Email IDs of subjects were procured from the course instructors and an email marketing software was used that allowed us to track who opened the email. All emails were sent using a free email account that was created specifically for the study using the subject line. Individuals receiving the email saw “UB Admin” as the sender’s name. The simulated attack lasted for a period of 2 weeks at the end of which anyone who opened the email but did not respond to the survey was contacted by the research team and asked to respond to the websurvey. This process lasted for another two weeks at the end of which all subjects were debriefed.

Measures

Email habits. Email habits were measured using a 11-item scale developed by Verplanken and Orbell (2003). Sample items read, “Checking email is something... I do automatically,” “I do without thinking,” “I start doing before I realize I’m doing it.” All items were scored on a 1-5 strongly disagree to strongly agree scale. The overall scale realized a Cronbach’s alpha of 0.91.

Heuristic processing. The measurement of heuristic processing varies considerably because the original work by Chaiken does not prescribe a measurement approach. Her approach utilized thought listing where subjects are asked to write-out their thoughts after reading a persuasive message. Phishing emails tend to be short and there are many more heuristic cues in them, making it difficult to parse out accurately the few content elements recalled from the many heuristic cues. Due to these limitations, some scholars have developed and used multi-item

scales, which, however, tend to net lower reliabilities. One such measure developed by Schemer, Matthes, & Wirth, 2008) provides a six-item measure for heuristic processing, which was adapted and used in the study. Sample items, all rated on a 1–5, Strongly Disagree to Strongly Agree scale read, “I skimmed through the email,” “I didn’t spend much time thinking about the email after I read it,” “I ignored the email message content.” The overall scale achieved a Cronbach’s alpha of 0.71.

Device Affordance. Device used to access the phishing email was asked with a self-report question that measured whether the individual used a smartphone/mobile phone or a personal computer/laptop to access the phishing email.

Results

Table 1 presents the descriptive statistics of the study measures. The influence of device used on heuristic processing was examined with a 2 (text vs. images cues) x 2 (accessed on PC vs. Mobile device) ANOVA. The overall model was significant [$F(3, 103) = 2.64, p < .05$] and only the main effect of cues was significant [$F(1, 103) = 4.53, p < .05$]. Neither the main effect of device [$F(1, 103) = 0.51, p = .47$] nor the interaction effect [$F(1, 103) = 1.53, p = .22$] was significant. Thus, subjects appeared significantly more likely to heuristically process emails in the presence rather the absence of cues [$MD = 0.29, SE = 0.14$].

The influence of device use on email habits was next examined with a 2 (text vs. images cues) x 2 (accessed on PC vs. Mobile device) ANOVA. The overall model was significant [$F(3, 103) = 3.94, p < .05$] and this time the main effect of access device was significant [$F(1, 103) = 10.17, p < .05$]. However, neither the main effect of cues in the email [$F(1, 103) = 0.36, p = .55$] nor the interaction between cues and access devices [$F(1, 103) = 2.06, p = .15$] were significant.

Thus, individuals with stronger email habits were significantly more likely to utilize a mobile device rather than a PC [$MD = 0.49$, $SE = 0.15$].

Discussion

The effect of devices were not on heuristic processing but instead were on email habits. This suggests that individuals who have stronger email habits likely utilize devices or that habitual email use is reinforced by device use. Answering which is the case would help further our understanding of device affordances. An effective way to answer this would be to look for the antecedents of habits and locate which of them the device used significantly influenced.

The literature on media habits locates three determinants: gratifications sought, which are the benefits derived from utilizing the medium or platform; deficient self-regulation, which is the individuals' ability to exercise control over the use of the medium; and load or the number of repeated interactions the individual has with the technology (LaRose, Mastro, & Eastin, 2001). From these, gratifications sought from emails vary considerably based on an email's context; hence, gratifications sought are often not the focus of investigations in established media habits (Vishwanath, 2015b). Instead, Communication research on habits tends to focus on frequency of media use and deficient self-regulation (LaRose et al., 2001). Frequency of email use or load tends to co-vary with gratifications sought, making it a more robust, first-order antecedent of habit (Vishwanath, 2015b). The second antecedent, deficient self-regulation, stems from the recursive influences of self-observation, self-reaction, and self-judgment, and focuses on the individual inability to control their enactment of firmly entrenched patterns of behavior, which is at the root of unconscious, reactive enactment of learned patterns (LaRose, 2010).

A moderating effect of device use on either of these antecedents would tell a distinct story. If device use moderates deficient self-regulation, it would suggest that individuals who are

unable to exercise control over their media use are perhaps more prone to using mobile devices. In contrast, if email load were moderated by device use, it would suggest that individuals' who frequently check and respond to email are significantly more prone to utilizing devices.

A separate line of research on cognitive processing has demonstrated a connection between heuristic processing and co-presence. Co-presence is the psychological sense of being accessible and available with another person in a virtual environment (Goffman, 1963; Nowak, 2001). Communication technology scholars contend that users perceive co-presence based on the heuristic cues present in the virtual environment (Sundar, Oeldorf-Hirsch, & Garga, 2008). For instance, cues such as logos, telephone numbers, and help-desk icons (suggesting someone can be called or messaged instantly from within the virtual environment) trigger co-presence heuristics that influence the interpretation of messages. Many spearphishing emails have logos and other graphical cues indicating co-presence, ostensibly to deceive victims into feeling that the message is credible.

Thus, an alternative mechanism to understand heuristic processing can come from examining whether emails with such logos and graphics indicating the presence of others communicate more co-presence than ones without such information. Again, if presence was communicated to the same extent regardless of whether that email was accessed on a PC or mobile device, it would give us greater confidence in concluding that device affordances did not trigger heuristics about presence. With this in mind, the research also measured heuristic processing and social presence in study 2.

Study 2

Method

Besides hyperlinks, another vector commonly used by phishers is to hide malware-carrying payload behind attached files in the email. The commonest file-type used is Adobe's PDF, which is a file format that is both widely recognizable and easy to spoof ("APT 1," 2013). For instance, a recent compromise of the Israeli Defense Forces used a publicly available PDF document to hide malware (Fisher-Ilan, & Finkle, 2014). Following this, the research replaced the hyperlink from the first attack with a PDF attachment and deployed it using an email with either cues or just plain text. All other aspects of the attack were identical to study 1. Figure 2A and B present the stimuli. Study 2 used another section of the same introductory communication course in the following fall semester, which ensured that the subjects in the study had not already participated in the first study.

Measures

In addition to measures for device of access, email habits (which achieved an alpha of 0.93), and heuristic processing (which achieved an alpha of 0.72), Study 2 included three additional measures.

Deficient Self-Regulation. Deficient self-regulation was measured using an 8-item scale derived from the prior literature on media habits (LaRose & Eastin, 2004; LaRose, Lin, & Eastin, 2003). Sample items read "I feel my email use has gotten out of control," "I check my email account whenever a device that can go online is available to me," "I feel tense, moody, or irritable when I am not able to check my email accounts." The overall scale achieved an alpha reliability of 0.88.

Email Load. One ratio-level measure asked how many emails the respondent read on any given day.

Co-presence. Using items developed by Slater, Steed, McCarthy, and Maringelli (1998), a seven-item measure of perceived co-presence was created to suit the study context. Sample items read, “Before responding to the email...I had a strong sense of being there with the sender of the email,” “...I had a sense that there was someone real at the other end who sent me the email.” Respondents scored each item from 1 = Strongly Disagree to 5 = Strongly Agree, and the overall scale achieved an alpha reliability of 0.90.

Results

Table 2 presents the descriptive statistics of the study measures. As in study 1, the influence of device used on heuristic processing was examined with a 2 (text vs. images cues) x 2 (accessed on PC vs. Mobile device) ANOVA. The overall model was not significant [$F(3, 104) = 1.80, p = .14$] but only the main effect of cues was significant [$F(1, 104) = 2.64, p < .05$]. Neither the main effect of device [$F(1, 104) = 1.27, p = .47$] nor the interaction effect [$F(1, 104) = 0.03, p = .87$] was significant. Thus, subjects appeared significantly more likely to heuristically process emails in the presence rather the absence of cues [$MD = 0.35, SE = 0.17$]. Likewise, the 2 x 2 model testing device effects on social presence perceptions was also not significant [$F(3, 104) = 2.05, p = .11$] but the main effect of cues was significant [$F(1, 104) = 5.27, p < .05$], with significantly more of presence felt when such cues were available [$MD = 0.44, SE = 0.19$]. Again, neither the main effect of device [$F(1, 104) = 0.06, p = .81$] nor the interaction effect [$F(1, 104) = 0.01, p = .96$] was significant. .

Next, the influence of device use on email habits was examined with a 2 (text vs. images cues) x 2 (accessed on PC vs. Mobile device) ANOVA. The overall model was significant [$F(3, 104) = 2.94, p < .05$] and this time the main effect of access device was significant [$F(1, 104) = 6.39, p < .05$]. However, neither the main effect of cues in the email [$F(1, 104) = 2.26, p = .14$]

nor the interaction between cues and access devices [$F(1, 104) = 0.93, p = .34$] were significant. Thus, individuals with stronger email habits were significantly more likely to utilize a mobile device rather than a PC [$MD = 0.44, SE = 0.18$].

The ANOVA testing the cues x device effects on deficient self-regulation found no significant main or interaction effects. The same ANOVA testing the 2 x 2 effects on email load was, however, significant [$F(3, 104) = 4.96, p < .05$]. While the main effect of cues and the interaction effects were not significant, the main effect of device was significant [$F(1, 104) = 14.08, p < .05$], with individuals who read more emails significantly more likely to utilize a mobile device than a personal computer [$MD = 4.61, SE = 1.63$].

Discussion

Study 2 results were generally in consonance with those of study 1. Mobile device use significantly moderated the influence of email habits. Rather than influence individual self-regulation, which would signal a likely deficiency in individuals' ability to either observe, judge, or react to incoming emails, the findings points to device usage being heightened among individuals who receive many emails each day. Thus, it appears that the load of emails a person reads potentiates mobile device usage and thusly leads to the strengthening of email habits. The presence of graphical cues in the email heightened heuristic processing and significant enhanced perceptions of co-presence. Interestingly, the reliance on heuristics was not greater on mobile devices.

Overall Discussion

Overall, the study examined two competing perspectives on how devices could influence the key mediators of victimization through phishing attacks. One backed by the cognitive literature looked at device affordances stimulating heuristic processing while the other stemming

from the media habits literature suggested an influence through the strengthening of habits. The former could be considered a constraint view, where mobile devices because of their smaller screen sizes and because of how they are used by people, i.e., while on the go or simultaneously while doing others activities, reduces the amount of cognitive resources the individual would have available for deployment—leading to the reliance on cognitive shortcuts. The latter is more of a behavioral view, where mobile devices, due to their portability, ease of use, and ready availability, leads to a relaxation of users' cognitive involvement such that cues don't matter overtime, and strengthening of ritualistic behavior—leading to reactive actions. Both these perspectives were examined using experiments that varied in the cues available in the email.

Findings support the behavioral view: it appears that device affordances enhance habituation. They do so by fostering frequent interactions with email, which are promoted by the design of today's smartphones and mobile email programs. In many ways today's smartphones work like slot-machines, intermittently and unpredictably pulling email from servers. This is coupled with notification sounds alerting users of incoming information that is at times mood altering, leads to a Pavlovian behavioral loop, which overtime leads to the habit of checking phones for message even in the absence of notifications. While heuristic processing and habits both simultaneously and independently lead to phishing victimization, prior research has shown email habits as having a much stronger influence. This makes the findings of the current study particularly important.

That said, besides strengthening habits, devices affordances might still influence heuristic processing. Recent work applying the MAIN model has found that individuals who use larger screen-sized smartphones tend to heuristically process video content (Kim & Sundar, 2015). While this work was within a laboratory setting where users' attention was focused on the

content within devices rather than in the naturalistic device-use environment where habits are likely to manifest, these findings could be indicative of an interaction effect between habits, screen size and modality. Thus it is possible that habitual reactions occur on smartphones when the email is similar to others the individual routinely receives, making ritualistic opening and clicking possible. When individuals, however, receive certain types of content, such as animated graphics and video, maybe because the content is different from what they usually receive, or maybe because the size of the device and how immersive the content appears, perhaps individuals snap-out of their habitual reactions and heuristically process the information.

The extent to which device screen size and modality influence habits or processing remains unexplored. At this point, phishing emails seldom include videos or animations, but this might not be the case in the future, when bandwidth and mobile device processing speeds makes such content routine. Hence, how different aspects of the MAIN (modality, interactivity, and navigability) model (Sundar, 2008), including device size stimulate or short-circuit the manifestation of habits is a question ripe for future exploration. Also, it appears that the design and physical characteristics of most of today's handsets and mobile operating systems have somewhat coalesced. For instance, popular Apple and Samsung handsets have similar screen dimensions and the positions of physical keys are roughly the same; likewise, iOS and Android also have similar notification systems and uniform mechanisms of displaying pages. Yet, it is possible that some subjects used a different or perhaps an older handset, which could have influenced how the study stimuli appeared to them. This is a limitation of the current study that needs to be addressed by future research.

Research also needs to pinpoint the smartphone design elements that specifically foster habits. Here research needs to explore whether notification sounds and the unpredictability of

data-pulls enhance habits. Such research can inform device designers most of who tend to focus on user convenience and portability rather than information security. Furthermore, a potential variant that was not accounted for in the current research setup was users who might have viewed the email on one device while responding on another, making it unclear which affordance was impacting their response. This again needs to be addressed in future research. Finally, research must also find ways to change habit. These could be through design initiatives that interrupt habitual patterns or through interventions that promote better cyber hygiene

All said the overall findings of the study are noteworthy. The study is the first to explicate how and why mobile devices could lead to deception via spearphishing. In doing so, the results contribute to our understanding of habits and the science of cyber security. The results are also timely. From smart watches to smartphones, more people today rely on mobile devices for communicating than ever before. Given this trend, it is likely that habits are only likely to get strengthened with time—which means that phishing attacks that take advantage of people's habits are also likely to become more successful with time. Couple this with newer trends in computing like bringing-your-own-device (BYOD) to work and location tracking on phones, future attacks are likely to bring malware from homes to offices, increasing the chances of vulnerability, and net richer personal information, increasing the scope of future breach.

Stopping attacks, thus, requires us to address the root of the problem: this means improving the affordance of mobile devices that strengthen habits and ultimately lead to victimization.

References

- 2015 saw 888 data breaches, 246 million records compromised worldwide (9 September 2015). Net-Security. Org. Retrieved from <http://www.net-security.org/secworld.php?id=18832>
- APT 1. Exposing One of China's Cyber Espionage Units*, Report by Mandiant (2013)
Available from Intelreport. mandiant. com/Mandiant_APT1_Report. pdf.
- Bayley, P. J., & Squire, L. R. (2002). Medial temporal lobe amnesia: gradual acquisition of factual information by nondeclarative memory. *The Journal of Neuroscience*, 22, 5741–5748.
- Blaszczynski, A., & Nower, L. (2002). A pathways model of problem and pathological gambling. *Addiction*, 97(5), 487-499.
- Chaiken, S. (1987). *The Heuristic Model of Persuasion*, Hillsdale, NJ: Lawrence Erlbaum Associates.
- Fisher-Ilan, A., & Finkle, J. (26 January 2014). Israeli defense computer hacked via tainted email: cyber firm. *Reuters*. Retrieved from <http://www.reuters.com/article/2014/01/26/us-israel-cybersecurity-idUSBREA0P0ON20140126?feedType=RSS&feedName=technologyNews>
- Gaver, W. W. (1991, April). Technology affordances. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems* (pp. 79-84). ACM.
- Gibson, J. J. (1977). *The theory of affordances*. Hilldale, USA.
- Goffman, E. (1963). *Behavior in public places*. New York: The Free Press.
- Graybiel, A. M. (2008). Habits, rituals, and the evaluative brain. *Annual Review of Neuroscience*, 31, 359–387.

- Greenberg, A. (2014). How The Syrian Electronic Army Hacked Us: A Detailed Timeline. *Forbes*,
<http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/>
- Hiltzik, M. (March 6, 2015). Anthem is warning consumers about its huge data breach. Here's a translation. *Los Angeles Times*,
<http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html>
- Kim, K. J., & Sundar, S. S. (2015). Mobile Persuasion: Can Screen Size and Presentation Mode Make a Difference to Trust?. *Human Communication Research*, doi:10.1111/hcre.12064
- LaRose, R., Mastro, D., & Eastin, M. S. (2001). Understanding Internet usage a social-cognitive approach to uses and gratifications. *Social Science Computer Review*, 19(4), 395–413.
- LaRose, R., Lin, C. A., & Eastin, M. S. (2003). Unregulated Internet usage: Addiction, habit, or deficient self-regulation? *Media Psychology*, 5(3), 225–253.
- LaRose, R., & Eastin, M. S. (2004). A social cognitive theory of Internet uses and gratifications: Toward a new model of media attendance. *Journal of Broadcasting & Electronic Media*, 48(3), 358–377.
- LaRose, R. (2010). The problem of media habits. *Communication Theory*, 20(2), 194–222.
- Mobile Technology Fact Sheet* (October 2014) Pew Research Center for Internet,

- Science & Technology. Available from <http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/>
- Martin, Z., (2015). 888 data breaches compromising 245.9 million records. *SecureID News*.
<http://www.secureidnews.com/news-item/2015-888-data-breaches-compromising-245-9-million-records/#sthash.1hHp76ex.dpuf>
- Nowak, K. (2001, May). Defining and differentiating co-presence, social presence and presence as transportation. Paper presented at the *4th International Workshop on Presence*, Philadelphia, PA.
- Robert, L. P., & Dennis, A. R. (2005). Paradox of richness: A cognitive model of media choice. *Professional Communication, IEEE Transactions on*, 48(1), 10-21.
- Schemer, C., Matthes, J., & Wirth, W. (2008). Toward improving the validity and reliability of media information processing measures in surveys. *Communication Methods and Measures*, 2(3), 193-225.
- Schmidt, M.S., & Sanger, D. E. (2015). Russian Hackers Read Obama's Unclassified Emails, Officials Say. *The New York Times*. http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html?_r=0
- Schwartz, F. (May 16, 2015). Penn State's Engineering School Computers Hacked. *The Wall Street Journal*. <http://www.wsj.com/articles/penn-states-engineering-school-computers-hacked-1431804110>
- Slater, M., Steed, A., McCarthy, J., & Maringelli, F. (1998). The influence of body movement on presence in virtual environments. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 40(3).
- Sundar, S. S. (2008). The MAIN Model: A Heuristic Approach to Understanding

- Technology Effects on Credibility. In M. J. Metzger & A. J. Flanagin (Eds.), *Digital Media, Youth, and Credibility* (pp. 73-100). , Cambridge, MA: The MIT Press. doi: 10.1162/dmal.9780262562324.073
- Sundar, S. S., Oeldorf-Hirsch, A., & Garga, A. (2008). *A cognitive-heuristics approach to understanding presence in virtual environments*. PRESENCE, 219-228.
- Verizon 2012 Data Breach Investigations Report. Retrieved June, 25, 2013.
- Verplanken, B. (2006). Beyond frequency: Habit as mental construct. *British Journal of Social Psychology*, 45(3), 639–656
- Verplanken, B., & Wood, W. (2006). Interventions to break and create consumer habits. *Journal of Public Policy & Marketing*, 25, 90–103.
- Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: A self-report index of habit strength. *Journal of Applied Social Psychology*, 33(6), 1313–1330.
- Vishwanath, A. (8 June 2015a). Why the cyberattacks keep coming. *CNN.com*
Retrieved from <http://www.cnn.com/2015/06/08/opinions/vishwanath-stopping-hacking>
- Vishwanath, A. (2015b). Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication*, 20(1), 83-98.
- Vishwanath, A. (2015c). Examining the Distinct Antecedents of E-Mail Habits and its Influence on the Outcomes of a Phishing Attack. *Journal of Computer-Mediated Communication*.
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & 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.

- Vishwanath, A., Harrison, B., & Ng, Y. J. (2015). *Suspicion, Cognition, Automaticity Model (SCAM) of Phishing Susceptibility*. Paper presented at the annual conference of the International Communication Association held in San Juan, Puerto Rico.
- Vishwanath, A. (2016). Spearphishing: The Tip of the Spear Used by Cyber Terrorists. In M. Kader et al. *Combating Violent Extremism and Radicalization in the Digital Era*, (pp. 469-484), IGI Global.
- Walters, R. (2014). Cyber Attacks on U.S. Companies in 2014. *The Heritage Foundation*. <http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014>
- Wood, W., & Neal, D. T. (2007). A new look at habits and the habit-goal interface. *Psychological Review*, 114(4), 843.
- Yin, H. H., & Knowlton, B. J. (2006). The role of the basal ganglia in habit formation. *Nature Reviews Neuroscience*, 7, 464–476.

Table 1.*Measures used in study 1: hyperlink attack*

	Hyperlink attack without image				Hyperlink attack with image			
	PC		Mobile		PC		Mobile	
	<i>Mean</i>	<i>s.d.</i>	<i>Mean</i>	<i>s.d.</i>	<i>Mean</i>	<i>s.d.</i>	<i>Mean</i>	<i>s.d.</i>
Email habit	3.30	0.78	4.01	0.60	3.43	0.81	3.69	0.86
Heuristic processing	3.00	0.69	3.07	0.94	3.46	0.61	3.20	0.49

Table 2.*Measures used in study 2: attachment attack*

	Attachment attack without image				Attachment attack with image			
	PC		Mobile		PC		Mobile	
	<i>Mean</i>	<i>s.d.</i>	<i>Mean</i>	<i>s.d.</i>	<i>Mean</i>	<i>s.d.</i>	<i>Mean</i>	<i>s.d.</i>
Email habit	3.55	0.78	3.82	0.95	3.64	0.87	4.25	0.66
Heuristic processing	3.16	0.77	2.94	0.79	3.48	0.75	3.32	0.81
Deficient self-regulation	1.91	0.75	2.09	1.02	2.12	0.74	2.32	0.74
Email load	6.61	5.13	10.95	6.67	7.00	4.42	11.93	8.05
Social Presence	2.66	0.86	2.72	1.08	3.12	0.79	3.15	0.95
<i>N</i>	45		19		25		15	

Figure 1A.*Phishing hyperlink attack with textual message*

Verification Needed

Sent on behalf of: UniversityatBuffalo1@gmail.com

Dear student,

A verification of your records shows an error with your UB email account settings. To prevent closure of your account, please see attached PDF for instructions to access your account settings and resolve the problem. You need to complete the request within two days of receiving this email in order to continue accessing your email account.

UB Email Administrator

Figure 1B.*Phishing hyperlink attack with graphical cues*

If you cannot see the email or images clearly, please click on your email/browser settings and allow images to be displayed.

Do not respond to this email. Please see attached PDF for instructions to update your records.

Click the live chat icon to chat with a UB representative.

Have Skype? Click the icon to video chat with a UB representative.

Phone: 716-645-2000 Email: UniversityatBuffalo1@gmail.com

Verification Needed

Sent on behalf of: UniversityatBuffalo1@gmail.com

Dear student,

A verification of your records shows an error with your UB email account settings. To prevent closure of your account, please see attached PDF for instructions to access your account settings and resolve the problem. You need to **complete the request within two days** of receiving this email in order to continue accessing your email account.

UB Email Administrator

This document contains information confidential and proprietary to buffalo.edu

LEARN MORE: [New Features](#) | [Tips & Tricks](#) | [Video Tutorials](#)

DocuSign. The fastest way to get a signature.®

If you have questions regarding this notification or any enclosed documents requiring your signature, please contact the sender directly. For technical assistance with the signing process, you can email support.

This message was sent to you by administrator@buffalo.edu who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

Copyright © 2014 University at Buffalo, All rights reserved.

Figure 2A.

Phishing attachment-attack with textual message

Verification Needed

Sent on behalf of: UniversityatBuffalo1@gmail.com

Dear student,

A verification of your records shows an error with your UB email account settings. To prevent closure of your account, please click the following link <http://svy.mk/XCPLDP> to access your account settings and resolve the problem. You need to complete the request within two days of receiving this email in order to continue accessing your email account.

UB Email Administrator

Figure 2B.*Phishing attachment-attack with only graphical cues*

If you cannot see the email or images clearly, please click on your email/browser settings and allow images to be displayed.

Do not respond to this email. Please see attached PDF for instructions to update your records.

Click the live chat icon to chat with a UB representative.

Have Skype? Click the icon to video chat with a UB representative.

Phone: 716-645-2000 Email: UniversityatBuffalo1@gmail.com

Verification Needed

Sent on behalf of: UniversityatBuffalo1@gmail.com

Dear student,

A verification of your records shows an error with your UB email account settings. To prevent closure of your account, please click the following link <http://svy.mk/XCPLDP> to access your account settings and resolve the problem. You need to **complete the request within two days** of receiving this email in order to continue accessing your email account.

UB Email Administrator

This document contains information confidential and proprietary to buffalo.edu

LEARN MORE: [New Features](#) | [Tips & Tricks](#) | [Video Tutorials](#)

DocuSign. The fastest way to get a signature.®

If you have questions regarding this notification or any enclosed documents requiring your signature, please contact the sender directly. For technical assistance with the signing process, you can email support.

This message was sent to you by administrator@buffalo.edu who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

Copyright © 2014 University at Buffalo, All rights reserved.