Decision Support Systems 103 (2017) 70–81

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Getting phished on social media

Arun Vishwanath

Department of Communication, University at Buffalo (UB), Buffalo, NY 14260, United States

ARTICLE INFO

Article history:
Received 1 February 2017
Received in revised form 14 July 2017
Accepted 14 September 2017
Available online 19 September 2017

Keywords:
Phishing
Social media
Social networking-based phishing
Online deception
Heuristic-systematic model (HSM)
Cognitive processing
Interface affordance
Device affordance

ABSTRACT

The study experimentally simulated a level-1 social networking-based phishing (SNP) attack, where a phisher using a phony profile attempts to friend an individual on Facebook, and a level-2 SNP attack, where a phisher attempts to extract information directly. The results implicate the use of cognitive shortcuts triggered by the cues afforded in Facebook's interface. Individuals appeared to be using the phisher's friend count as a heuristic for judging the authenticity of a level-1 request. They, thus, responded to a phisher displaying a large friend count even in the absence of a profile picture. Interestingly, the affordance of smartphones used to access social media—an issue that has received little academic attention—increased the odds of considering such requests sevenfold.

Phishing is a type of online deception where a perpetrator, a phisher, utilizes social engineering techniques to procure information of a personal or sensitive nature from a victim [1]. With the rapid diffusion of Web 2.0 technologies, phishers have begun to deploy attacks through social media. For instance, in a recent attack that has been attributed to espionage by the Chinese government, senior military officials from the U.S. and U.K. were tricked into becoming Facebook friends with someone masquerading as U.S. Navy Admiral James Stavridis [2]. Similar reports from different parts of the world of the use of social media by phishers posing as other people, legitimate businesses, politicians, and famous personalities on Twitter, LinkedIn, and Google Plus, to extract sensitive information from others, are evidence of the growing number of such attacks [3–6]. These scams all utilize similar techniques to directly or surreptitiously acquire sensitive information from users, making the need to understand why individuals fall victim to social networking-based phishing (SNP) important from an organizational security, law enforcement, and national security standpoint.

Though similar in some respects to an email-based phishing attack, SNP scams are distinct in at least three important ways. First, SNP attacks occur within relatively new social media environments where the platform features, protections, and policies are constantly evolving [7], which make it difficult for users to achieve any mastery over the technology—a factor known to increase susceptibility to online deception [8].

Second, email-based phishing is usually a one-step process where a phisher casts a wide net by sending out millions of email requests that act as bait. In contrast, SNP could be conceptualized as a two-level attack. In the first level, the perpetrator attempts to connect with or friend a person using a fake persona. In fact, the use of such fake personas to lure victims into romance scams—called Catphishing—is so rampant that Facebook's CEO Mark Zuckberg recently promised to create tools to make it harder to create fake profiles and impersonate others [9]. A successful level-1 SNP attack is, however, also far more virulent than a successful email-based phishing attack because of the access a perpetrator gets to the victim's personal information in addition to information about the victim's Facebook friends and even their friends that could be used for subsequent phishing attacks. A Level-2 attack usually involves requesting personal or sensitive information from the victims using Facebook's messaging platform. In some cases, such messages include a hyperlink or attachment that hides a payload, which when clicked installs malware into the victim's computer. Because people tend to interpret messages based on the sender [10] as well the medium on which they receive it [11], users who receive a level-2 request might respond ostensibly because it was sent by a Facebook friend or sent from within Facebook where they expect people to be honest [12].

Third, SNP attacks present fewer ready clues about its deceptive intent when compared to email-based phishing attacks. Research that has examined the content of various phishing emails has found that there are many clues in the email's content that point to their deceptive intent [13,14], and the sensitivity to such clues is often at the heart of training programs designed to teach individuals to detect deception [15,16]. In contrast, Facebook provides the option of sending the request

E-mail address: avishy@buffalo.edu.

https://doi.org/10.1016/j.dss.2017.09.004
0167-9236/

using its formatted template, limits content, emphasizes a few graphical cues, and restricts the variances in information necessary for contrasting between legitimate requests and fake ones [17]. Together, the limited number of cues as well as their presentation by the Facebook interface makes SNP attacks more likely to be successful.

Understanding why individuals fall victim to SNP attacks, thus, requires an examination of how cues are presented by Facebook as well as how individuals access and react them. Of course such attacks could occur in other social media platforms as well, but given that Facebook is the most popular with close to 2 billion users and with almost 83 million fake profiles pages also the most likely conduit for phishing scams,[1] our focus was solely on its users. And while research on phishing via Facebook has examined the role of user habits [18] and even how such attacks propagate [19], none have addressed this important question: *What are the underlying cognitive processes that lead to individuals falling victim to SNP attacks on Facebook*? Answering this is the goal of the present study.

To this end, the research extends the concept of technology affordances, which are the real and implied capabilities of media that shape how information is typically presented via the medium and the receiver's state of mind while interacting with it [20,21]. Facebook's affordances can be further categorized into interface affordances [21], that is, the platform specific features that dictate the cues available in the friend-request, and device affordances [22]—a facet of media use that has received limited academic attention—that stem from the gadget individuals use to access Facebook.

To understand how Facebook interface cues and device affordances influence deception, the present study subjected matched samples of student social media users to a real-world level-1 attack, which varied in the cues available in the request, followed by a level-2 SNP request, and tracked the device they used to access and respond to them. Following the consensus in the academic literature that people fall prey to phishing attacks because they fail to effectively process the information that could reveal the deception [15,23,24], the research applies the Heuristic-Systematic Model (HSM)—a theoretical framework that explains how individuals cognitively process information leading to phishing victimization [25] and the role of cues during this process. The paper begins by presenting the HSM framework along with the research hypotheses in the next section followed by the methods, measures, results, and discussion in ensuing sections.

1. Theoretical premise

1.1. The heuristic-systematic model (HSM)

The HSM distinguishes between two modes of information processing that individuals engage in while making judgments [26–28]. At the upper end of the information processing continuum is systematic processing, where individuals scrutinize the content of a persuasive message to reach their judgment [29]. This form of processing is detailed and connects data in the content to information encoded in memory and involves substantial cognitive effort. The other mode is heuristic processing, where individuals utilize simple decision rules, or cognitive heuristics, triggered by cues in the decision-context to reach judgments.

Over two decades of research on social-cognition illustrate the dominance of heuristic processing over cognitively effortful systematic processing during decision-making [30]. Heuristic processing dominates because individuals tend to be cognitive misers [31] who are motivated to economize on mental resources [26]. Thus, systematic processing occurs only when heuristics do not provide adequate judgment confidence and when individuals have substantial motivation as well as cognitive capacity in terms of knowledge and ability to commit to the task. Even in such circumstances, the HSM posits that the two modes of information processing co-occur and heuristic processing precedes and biases systematic processing.

This reliance on heuristics is especially strong among online audiences who are condition to rely entirely on symbolic cues for online navigation and interaction [30]. Online environments also contain a preponderance of textual content usually mixed in with graphical information that is by design more visible and attractive to individuals driven by cognitive economy considerations. More recent research has implicated heuristic processing triggered by graphical cues in phishing emails as one of the major reasons why people fall victim to spearphishing [25]. The present study, therefore, began by focusing on the cues available in a level-1 SNP attack that which could trigger heuristic shortcuts and leading to individual victimization.

1.2. Level-1 SNP attack

1.2.1. Interface affordances

A level-1 SNP attack begins with a friend-request from a phony Facebook profile. When an individual receives any friend-request, Facebook sends an email notification that can be accessed via a personal computer (PC) or a mobile device. In this notification, Facebook affords receivers with a brief statement that remains invariant across requests along with two graphical cues that change based on the sender's profile: The picture and a cue about the number of friends shared with the sender.[2] Fig. 1A presents an example of the friend-request notification viewed on a PC.

Merely clicking on the "Confirm Request" icon accepts the request. Scrutinizing the notification by clicking on the picture or name of the sender directs the user back to the sender's profile page, requiring the receiver to navigate multiple layers of information and entailing significant more cognitive effort. Going to the user's profile page might provide little additional information because Facebook allows profiles to remain locked until the receiver accepts the request. The HSM would argue against social media users engaging in any such effortful actions and suggest that they would instead simply rely on the heuristics triggered by the picture and friend cues in the notification.

The old adage "a picture is worth a thousand words" speaks to the heuristic effect of pictures. Pictures are graphical cues that foster cognitive efficiency by helping make snap decisions without needing to review detailed content [32]. Online environments are rife with photographs, from the pictures of products on online shopping portals to profile pictures on dating website [33]. In fact, there is almost an expectation that websites carry such graphical cues and evidence suggests that online consumers look for and are extremely reactive to such cues [34]. For instance, on online auction portals, the mere presence of photographs when compared to its absence triggers user interest and higher valuations by ostensibly triggering heuristics such as "the picture means the product is genuine" or "the picture implies the product really exists" [35]. Similarly, impressions of online dating profiles are positively impacted by the presence of pictures and other rich graphics [36].

Almost every user on Facebook—91% of teens in a recent Pew Center poll—provide a profile picture [37], making it likely a normative expectation that a photograph accompanies a Facebook profile. Again, following the HSM's cognitive efficiency principle, the expectation is that the mere presence of this profile picture could trigger a "Profiles with pictures are genuine" or "I only friend people with pictures on their profile," and result in an acceptance of the request. Of course, the photograph could also cue a *recognition heuristic*, where users realize the person is a stranger and trigger the "stranger equals danger" heuristic and lead to more detailed scrutiny [38] that ultimately results to the profile being rejected. But because most Facebook users maintain weakties by connecting to people they may not be very familiar with [39], it is

[1] https://zephoria.com/top-15-valuable-facebook-statistics/.

[2] Notifications are resent to the individual's chosen email address until the friend-request is attended to and the friend count cue in the request reflects the actual number of friends the sender has at the time of resending the notification.

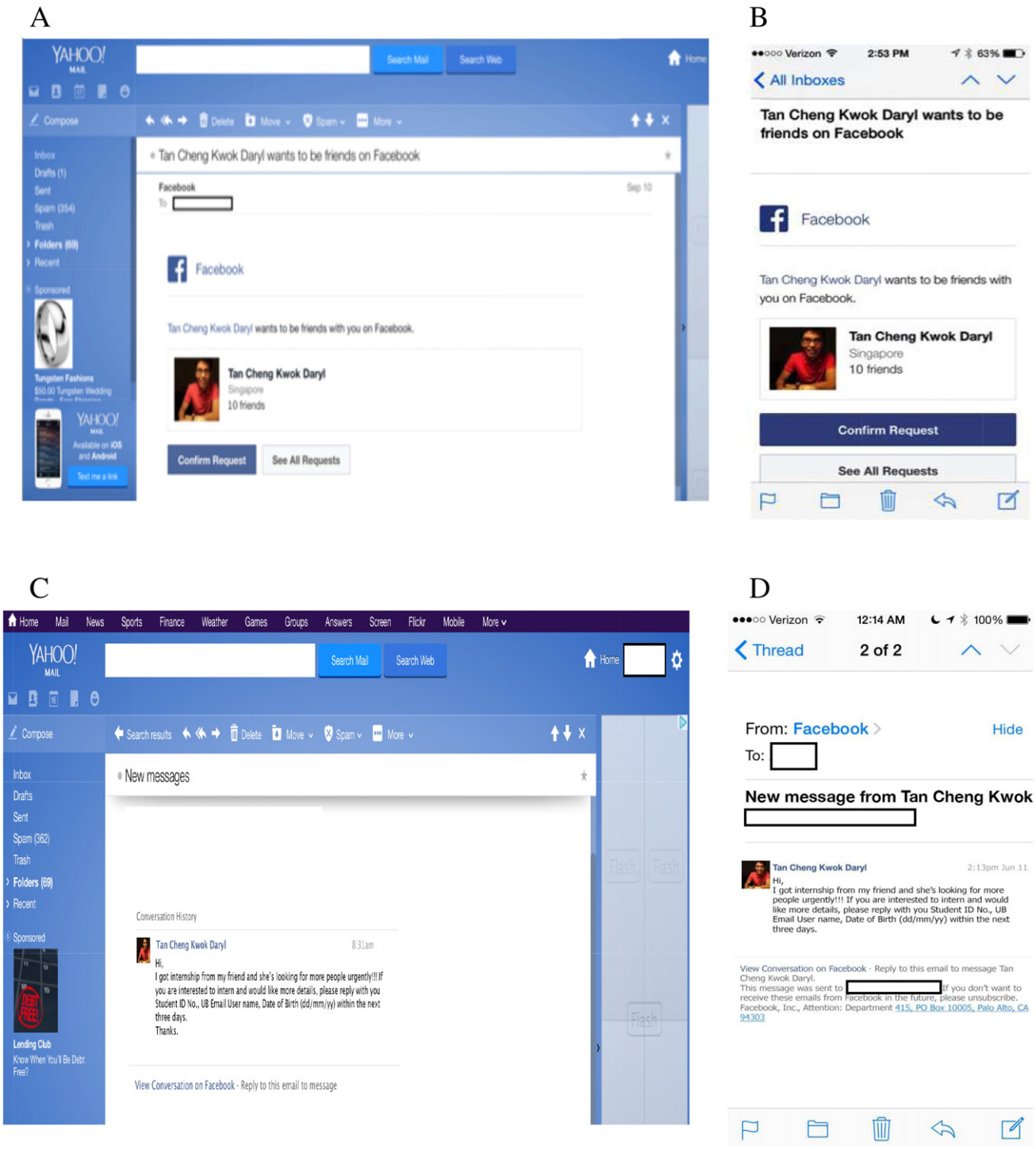

Fig. 1. A. Friend-request accessed on a PC. B. Friend-request accessed on a smartphone. C. Information-request accessed on a PC. D. Information -request accessed on a smartphone. *Note.* Rectangular white boxes used to conceal victim's name and email ID.

less likely that people go beyond assessing the presence of the photograph into distinguishing their relationship with the person on the profile. Thus, Facebook users are doubly motivated, by cognitive efficiency considerations and by their very motivation for using Facebook, to accept requests with pictures.

Also, routinely presented online are cues in the form of likes, stars, and comments that suggest that popularity of a page, product, or service. Such cues are important because they provide social proof about other individuals performing these behaviors and spread the decision risk across these users [40]. Reacting to them often leads to a herd behavior where people perform actions just because there are others doing it. This, for instance, leads to people in online auctions, rather than examining each product, gravitating to those that already have many bidders [41]. It also leads to people thinking a news story that has many comments is more credible [42]. HSM explains this effect through the activation of *bandwagon heuristics*, where the mere count of others allows for a quick estimate of the legitimacy of an action without much cognitive effort [21]. Following this, the research expects the count of the number of friends connected to the sender of a level-1 request triggering bandwagon heuristics such as "I only friend people

with many friends," or "Popular people are credible," and resulting in individuals blindly accepting the request.

Additionally, Facebook allows the profile picture to appear along with the friend count in the request, which should logically lead to a "cue-cumulation effect" ([42], p. 370), where multiple complementary cues additively activate more heuristics. Hence, a phishing profile with a picture in conjunction with a friend count could activate multiple heuristics ("S/he looks like my friend and has many friends" or "Profiles with pictures and friends are authentic") that lead to the acceptance of the request. Finally, the Facebook interface also allows for requests without a profile picture or a cue about the number of friends of a sender. Such profiles could, however, appear anomalous to most users who are routinely presented such cues in almost all Facebook friend-requests. Thus, the absence of cues in the profile could trigger *realism heuristics* (e.g., "Profiles without friends are suspect" or "I never friend someone without a picture") that lead individuals to question the veracity of the profile and probe the interface for further information, which could reveal the deception. Altogether, the rationale presented so far leads to following:

H1. An individual will accept a level-1 SNP request in the presence of a) a picture cue, b) a cue indicating the number of friends, or c) both picture and cue indicating the number of friends.

1.2.2. Device-based affordance

An aspect of new media consumption that has been ignored in online-deception research is the affordance of the device typically used by the potential victim to access the medium. This is a new and important area of inquiry particularly because devices such as smartphones and tablets are widely diffused and are quickly becoming the dominant device for accessing the Internet [43]. Device-based affordances are particularly important from the SNP point of view because the experience of accessing and responding to social media on devices such as smartphones and tablets are distinctly different from doing the same on a PC or laptop.

From the HSM standpoint, smartphones influence the availability of cues and the cognitive capacity of individuals in two important ways. For one, most smartphones have smaller aspect ratios and screen sizes than PCs and laptops, which restrict the amount of textual information users can easily read on smartphones. Users interact with a stripped-down mobile version of a website or utilize mobile "apps" (applications) to access sites, which are specifically constructed for easier viewing on these smaller screens. To achieve this, many textual elements on the webpage are stripped and graphical icons (action cues for sending, replying, forwarding emails or accepting requests) are prominently displayed. This makes it all the more likely that smartphone users will even more so rely on heuristic cues in the SNP request when making their decision. Second, many people check email as well as respond and update their social media feeds using smartphones on the go, often while simultaneously engaged in other tasks. The HSM suggests that multitasking determinately influences individuals' cognitive resources available for in-depth processing and leads to an increased reliance on heuristics [32], which again suggests an increased likelihood of individuals relying on heuristics while accessing SNP requests on smartphones.

To illustrate the likely influence of device-affordances on level-1 request-acceptance, Fig. 1B presents the same friend-request seen in Fig. 1A, on a smartphone. The figure demonstrates the Facebook notification's more constrained presentation and the prominence of graphic cues (e.g., the Confirm Request icon) that could be inadvertently triggered when the individual is multitasking or if the user is not sufficiently motivated to check through the profile. Thus, the research posits a moderating role for the device of access such that when compared to the same request viewed on a personal computer, smartphones, because they increase the reliance on heuristics, significantly increases the likelihood of victimization.

H2. The use of a smartphone to access a level-1 SNP request will enhance the heuristic effect of cues, increasing the individual's likelihood to accept the level-1 request.

1.3. Level-2 SNP attack

A level-2 SNP attack is when the phisher requests information that is personal or sensitive directly using the messaging function of social media. Facebook allows such requests from current, confirmed friends as well as from strangers who know the email address linked to the receiver's Facebook account. Unlike Facebook friend-requests that require the intended victim to merely click on a graphical-button afforded on the notification to fall prey to the attack, level-2 SNP notifications requires the recipient to read the content of the message, and either navigate back to the messaging window on the Facebook website or respond to the message via email.[3] Fig. 1C and D show the level-2 message as seen on PC and a smartphone.

As apparent, level-2 messages are similar to traditional emails, in that they can be sent by anyone and their content could vary based on the discretion of the sender. Unlike emails, however, social media notifications prominently display the name of the sender and the profile picture of the sender along with the message, which could exert a heuristic influence on the individuals' processing of the level-2 request. Even in email-based spear phishing, research has shown the presence of a friend's email or name to increase the victimization rate significantly—by as much as 56% compared to a control group Jagatic et al. [44]—likely because the friend's email address cued the receivers about their relational commitments and framed how they systematically processed the message [10]. People also likely felt obligated to respond to the request because it was from a friend—a need for consistency with prior cognitive or behavioral commitments, which is thought to be a central driver for why individuals, once lured to respond to an initial phishing request, continue to escalate their behavior [24, 45]. Following this, acceptance of the level-1 request, cued by recognizing the name and picture of the sender, could likewise frame the interpretation of the level-2 request and result in victimization. As in the level-1 request, device affordances in the form of device-based technical restrictions (due to download speeds, data costs, screen size, visibility, pixel-density, and icon size) and device-driven cognitive constraints (due to multitasking) could continue to constrain what the users actually view and evaluate in the level-2 request. Hence, device-based affordances could moderate the processing strategy employed by the recipient of a level-2 SNP request. All these influences are potentially stronger when the individual has already accepted a level-1 request. For individuals who have yet to accept the friend-request, the level-2 request would appear similar to a general phishing email sent by a stranger, which because they lead to increased uncertainty and spur systematic processing that usually reveals the deception [23], tend to be minimally successful [46]. Together, these lead to the following:

H3. An individual is more likely to accept a level-2 SNP: a) when using a mobile device to access the request, b) the request contains a picture, and c) the individual already accepted a level-1 SNP request from this requestor.

2. Methods

2.1. Sample

Senior undergraduate students from four different sections of required theory classes at the University of xxx's Singapore program in

[3] Facebook no longer allows individuals to respond directly via the email notification but requires users to access the Facebook platform's mobile website or messaging app in order to respond to messages.

fall'11 were recruited for the study and subjected to a level-1 SNP attack on Facebook followed by a level-2 SNP attack.[4] In the beginning of the semester, students in each class were asked to participate in an online survey where buried among 50 questions about their general technology use were three questions that asked respondents about their preferred social media platforms, their Facebook login, and the email addresses they had linked to their Facebook accounts. Using the login information, 127 students were located on Facebook and about 6 weeks into the semester, students were randomly selected and sent a friend-request from one of four fake Facebook accounts that were created for the study.[5] All requests were sent within a few minutes of each other using Facebook's built-in friend-request function that automates the sending of requests. Two weeks after the friend-request was sent, everyone who was sent the original request was sent a request for personal information (a level-2 SNP attack) from within the respective profiles used to friend them, using Facebook's built-in email functionality. Two weeks after the level-2 attack, all subjects were sent a link to a web survey and subsequently debriefed about the study.

2.2. Stimulus

Four Facebook accounts were created for the study: one without a picture or any friends connected to the person, one with a picture but with no friends, one without the picture but with 10 friends, and one with a picture and 10 friends. In order to reduce the likelihood that attractiveness or gender preferences contaminate the results, the four Facebook profiles were of moderately attractive males.[6] The level-2 attack used the lure of an internship opportunity and asked interested individuals to provide their date of birth, email ID, and university student ID number.[7] Appendix A presents a sample of the stimulus material.

2.3. Measures

The key measures in the study were a combination of behavioral measures collated from the Facebook profiles used in the attacks and self-reports provided by subjects in the follow-up web survey. Table 1 presents the measures used in the study. Additional measures used to test whether heuristics were indeed activated in response to level-1 and level-2 attack are presented in Appendix B.

3. Results

Table 2A summarizes the analysis strategy. From a device of access point of view, 52% of the overall subjects in the study indicated that they used a smartphone to access the SNP notifications. Overall, 18% of all subjects confirmed the level-1 request, 50% were still considering it, and 32% had decided not to friend the person. From the overall level-2 SNP attack standpoint, 14% of the subjects in the study responded with information, 41% were still considering it, and 45% had decided against it (how many of these also accepted the level-1 request is reported further along in the paper). Table 2B presents the descriptive statistics of each group in the study. Table 3 summarizes the results of the hypotheses testing and Table 4 presents the ordinal regression results.

The regression model examining hypotheses H1 and H2 found two significant interactions. First, a picture × friend interaction indicating that the presence of pictures along with friend cues appeared to lower individuals' odds of victimization. The examination of the interactions revealed that individuals who received the friend-request with the presence of only friend cues were twice more likely to respond compared to individuals who received both friend and picture information in the friend-request. Second, a friend × device interaction, supporting the moderating hypothesis (H2), suggesting that friend count cue mattered and the odds of getting victimized increased sevenfold when the individual used a mobile device. The moderating role of devices on response to the level-1 request is visually presented in Fig. 2A.

Finally, the regression model examining hypothesis 3 found a significant effect for the covariate *Response to the level-1 attack* and a subsequent covariate × device interaction. The descriptive statistics for the interaction between access-device and prior-friend acceptance on likely response to a level-2 request are presented in Table 5. Overall, more subjects denied the level-2 request if they also denied the level-1 request when they accessed the requests on the PC (60%) instead of a smartphone (52%). Further illustrating the device effects, 12% of the subjects who accessed the requests on a PC had accepted the level-2 request although they had denied the level-1 request, compared to 20% of the subjects who accessed the request using a smartphone. These results are visually presented in Fig. 2B. The chi-square test of dependence testing whether the likelihood of accepting the level-1 request influenced the level-2 request's likelihood of acceptance was significant for subjects accessing the requests on a PC, $\chi^2\ (4) = 18.28$, $p < 0.001$, and smartphones, $\chi^2\ (4) = 17.52$, $p < 0.001$, further validating the covariate × device effects.

4. Discussion

The overall results support the central thesis of the study: heuristic cues transmitted by the affordance of the friend-request and moderated by the affordance of the device used to access social media determine whether individuals fall prey to SNP attacks.

First, the research found that the count of the phisher's Facebook friends was the defining cue in the notification that influenced deception in a level-1 SNP attack. Its presence singularly increased the likelihood of victimization four-fold. Thus, it appears that individuals were using the mere count of the number of friends of the phisher as a cue about his authenticity. The friend count likely cues *bandwagon heuristics* or *source credibility heuristics* and spurs acceptance perhaps because individuals believe that a popular person is trustworthy and less likely to be deceptive. Or, the friend count signals that other Facebook users have already vetted the profile's authenticity and individuals presumably feel that a collection of Facebook users are less likely to be deceived. The

[4] Communication Theory is a required 300-level theory course from which students were recruited. Selection from different sections of the same course ensured there was no overlap among students between the classes.

[5] There were 153 students across the four sections and the research team managed to locate and clearly identify 141 students on Facebook who became the target of the attack. The average age of the students across the sections was 21 years (*S.D.* = 1.90), 72% of participants were female. There was no systematic difference in age or gender across the sections. Six subjects provided mostly incomplete responses to the web survey conducted after the attack and were excluded from the analysis. From the remaining, 5 of the respondents stated they used a smartphone to access the friend-request notification but a computer to access the information-request, and another 3 stated vice-versa. These individuals were excluded from the study.

[6] Males were used instead of female profiles because of the preference for females as friends by both males and females [55], making any findings more likely to be conservative and less likely to be biased. To ensure that the names used in the profiles were fairly similar and authentic, and to control for variance in attractiveness, ten potential male names were considered along with ten pictures that were found online. The names and pictures of males were pre-tested on a separate sample of 32 undergraduate students and 4 names that appeared most authentic and felt least dissimilar to respondents were selected. Using the same process, 2 pictures that had average ratings for attractiveness were selected. The two popular profile pages with friends had 10 friends (5 male and 5 female friends) each with pictures, and none of the friends overlapped between profiles. Besides this, the information on each of the four Facebook pages was kept the same and only the name and location information on the profiles were visible.

[7] The information requested in the level-2 attack was considered sensitive because many online services use these pieces of information for account setup and verification. As a case in point, until March 2013, a phisher could reset an Apple iCloud user's online password by using just their date of birth and email ID, and illegally purchase products using the credit card of the user stored on the account [56].

Table 1
Measures used in the study.

Measure	Procedure	Items	Scoring
Response to a level-1 attack	All accepted friend-requests were coded as 3 = accepted. Subjects who did not accept were asked a follow-up question in web-survey.	Where are you in your decision regarding the friend-request? Response scale: 1 = decided to deny the request; 2 = still considering the request	The final measure that was partly behavioral and partly self-report based had 3 ordinal levels: 1 = denied the request, 2 = considering the request, 3 = confirmed the request
Response to a level-2 attack	All subjects who responded or provided the information were coded as 3 = responded. Subjects who did not respond were asked an open-ended question in the follow-up web survey about where they were in their decision regarding the information request.	Open-ended responses coded by two independent coders, who agreed on 89% of their categorizations. Responses such as "I could not be bothered…" "I thought the request was odd," "I don't care for this internship" were coded as 1 = denied it. Responses such as "I was waiting to see if my schedule would allow for it," "I was looking more information on the offer," or "I was waiting to see if my friends would join too" were coded as 2 = considering it.	The final measure that was partly behavioral and partly self-report had 3 ordinal levels: 1 = denied the request, 2 = considering the request, 3 = responded to the request
Access-device	In the web survey that was conducted after the attack, one question measured which device the respondent used to view the friend-request notification; another measured which device they used to view the information-request notification.	What device did you use to access the friend-request notification? What device did you use to access the information-request notification?	The self-reported responses were coded as Mobilephone/smartphone coded as 1 = smartphone; computer or laptop coded as 0.

Table 2A
Analysis strategy.

Hypothesis	Independent variables/design	Dependent variable	Analysis strategy
H1 & H2: Response to a level-1 attack	2 (no picture vs. picture) × 2 (no friends vs. 10 friends) × 2 (smartphone vs. computer)	Ordinal dependent variable *Response to a level-1 attack*	Ordinal regression
H3: Response to a level-2 attack	2 (no picture vs. picture) × 2 (no friends vs. 10 friends) × 2 (smartphone vs. computer) with the *Response to a level-1 attack* as a covariate	Ordinal dependent variable *Response to a level-2 attack*	Ordinal regression

finding of a strong heuristic effect of the Facebook friend count runs contrary to research that suggests that individuals use Facebook to maintain off-line ties [47], which implies some level of conscious decision-making and requires the examination of senders' profiles prior to acceptance. It appears people are less conscious in their decisions and are instead focused on enhancing the size of their social network by accepting requests by popular individuals. This might be because some people feel that they have fewer friends than others [48] and because being connected to someone popular increases the size of one's own social network, and on Facebook leads to more attention from others [39]. The heuristic effect of the friend count cue also suggests that a phisher with more friends would likely spur acceptances and gather many more victims overtime. This leads to the possibility of an upward cascade in the number of victims, with each victim cueing the acceptance of more victims, in a process of social contagion. Researchers at the Pew Center approximate that an average Facebook user could reach 30,000–150,000 other users through their friend's friends and as many as 7 million users through those friend's friends (2-degrees of separation) [39]. Thus, the cascade of victims cueing other victims spurred by a phony friend-request with a few friends could quickly escalate into a widespread attack and net millions of victims, making a level-1 SNP attack with a friend cue extremely virulent.

In contrast to the phisher's friend count, the research found that the phisher's Facebook profile picture in a notification significantly *decreased* the likelihood of deception, with users being two times less

Table 2B
Counts of respondents in each condition based on response status and access-device.

Condition	Response status	Level-1 friend-request		Level-2 information-request	
		Access-device PC	Access-device mobile	Access-device PC	Access-device mobile
No cues	Denied	4	8	6	7
	Considering	6	1	3	1
	Responded	1	1	2	2
Picture only cue	Denied	5	5	6	6
	Considering	6	10	5	8
	Responded	2	0	2	1
Friend only cue	Denied	3	2	5	7
	Considering	10	12	9	12
	Responded	2	9	1	4
Picture and friend cue	Denied	10	3	13	7
	Considering	9	10	6	8
	Responded	3	5	3	3

Table 3
Summary of the results of the study.

Hypotheses	Results of the analysis
H1 & H2: Response to a level-1 attack	The regression model excluding the three way interactions was most parsimonious and significant (χ^2 (6) = 24.50, $p < 0.001$; Nagelkerke's Pseudo R^2: 20%): the parameter estimates for the presence of friend count ($\beta = 1.39$, $SE = 0.61$, *Wald* (1) = 5.01, $p < 0.05$, $OR = 4.01$) and for using a mobile device ($\beta = 1.43$, $SE = 0.56$, *Wald* (1) = 6.04, $p < 0.05$, $OR = 4.17$) were significant. Among the interactions, the picture × friend interaction ($\beta = -1.64$, $SE = 0.74$, *Wald* (1) = 4.82, $p < 0.05$, $OR = 0.19$); and the friend × access device interactions ($\beta = 1.97$, $SE = 0.74$, *Wald* (1) = 7.15, $p < 0.05$, $OR = 7.16$) were significant. Thus, the presence of a picture with friend count *reduced* the odds of victimization, while the friend count alone when viewed on a mobile device *increased* the odds of victimization. Picture × friend count interactions: When estimated separately, although the odds of responding to a request with a picture and friend count was significantly higher than that of responding to a request with no profile picture and no friend counts ($\beta = 1.02$, $SE = 0.53$, *Wald* (1) = 3.75, $p < 0.05$, $OR = 2.77$), the odds of responding to a request with only friend count was higher than those of responding to a request with both friend count and picture cues ($\beta = 0.88$, $SE = 0.44$, *Wald* (1) = 3.98, $p < 0.05$, $OR = 2.41$). Finally, the odds of responding to a request with a picture cue only were statistically no different from the odds of responding to request with neither picture nor friend counts. Friend × device interactions: Odds of accepting a request with friend count were significantly higher when accessed on a mobile device than on a personal computer ($\beta = 1.19$, $SE = 0.45$, *Wald* (1) = 7.05, $p < 0.05$, $OR = 3.28$). Odds of accepting a friend-request with friend count rather than one without friend count were significantly higher when accessed on a mobile device ($\beta = 1.96$, $SE = 0.52$, *Wald* (1) = 14.23, $p < 0.05$, $OR = 7.09$).
H3: Response to a level-2 attack	The ordinal regression was significant (χ^2 (7) = 26.04, $p < 0.001$; Nagelkerke's Pseudo R^2: 21%) and only the parameter estimate for covariate, prior response to the level-1 attack, was significant ($\beta = 1.34$, $SE = 0.30$, *Wald* (1) = 19.60, $p < 0.05$, $OR = 3.81$). The parameter estimate for the effect of pictures, friend cues, device, and the interactions between friend cues × device, friend cues × picture, and picture × friend cues were not significant. To tease out the covariate effects further, the two-way interactions between the covariate and the friend count cues, picture cues, and devices were estimated separately. Only the covariate × device interaction was significant ($\beta = 1.45$, $SE = 0.51$, *Wald* (1) = 7.97, $p < 0.05$, $OR = 4.26$) suggesting that individuals were significantly more likely to provide information in a level-2 attack received on a mobile device if they had already accepted the level-1 friend-request.

likely to accept requests with pictures from strangers compared to a request with no cues. This finding again runs contrary to the extant theorizing about heuristics: most cognitive scientists tend to have a bias against the use of heuristics in information processing, using pejorative terms such as cognitive misers [31], lazy organisms [26,49], and limited information processors [50,51], to describe their users. Instead it appears that the profile picture, perhaps because it contains facial images that individuals are innately good at recognizing [52], cues effective heuristics, such as "Stranger equals danger" or "I don't know the person and I don't friend strangers," that efficiently help reduce individual susceptibility. Besides challenging the conventional understanding of heuristics, the finding also opens the door for future research that identifies effective versus ineffective heuristics and moves beyond the current trend of educating people about online deception—which is aimed at

Table 4
Ordinal regressions predicting likely response to friend-request and to information request.

	Parameter estimates predicting likely response to friend-request			Parameter estimates predicting likely response to information-request		
	Logit B	Std. error	Exp. B	Logit B	Std. error	Exp. B
Threshold (1)	−1.61*	0.46	0.19	2.35*	0.77	10.48
Threshold (2)	1.00*	0.41	2.71	4.65*	0.86	104.5
Picture cue (base: no pictures)	−0.49	0.55	0.61	−0.13	0.56	0.87
Friend cue (base: no friend)	1.39*	0.61	4.01	−0.38	0.63	0.68
Device (base: computer)	1.43*	0.56	4.17	0.09	0.65	1.09
Picture cue × access-device	−0.62	0.73	0.54	−0.28	0.72	0.76
Friend cue × access-device	1.97*	0.74	7.16	0.26	0.59	1.30
Picture cue × friend cue	−1.64*	0.74	0.19	−0.60	0.75	0.54
Covariate (likely response to friend-request)				1.34*	0.30	3.81
Model fit	Model χ^2 (6) = 24.50, $p < 0.001$			Model χ^2 (7) = 26.04, $p < 0.001$		

Note 1. To check whether unequal sample proportions between experimental conditions could explain the ordinal regression results, the proportional odds assumption was tested using the test of parallel lines (where the null hypothesis is that the slope coefficients in the model are the same across response categories). The test was not significant for the ordinal regression predicting likely response to a friend-request ($\chi^2(6) = 5.71$, $p = 0.46$) or for the regression predicting likely response to an information request ($\chi^2(7) = 9.75$, $p = 0.20$). Hence, differences in groups due to unequal cases did not influence the regression results.

Note 2. A post-hoc power analysis was conducted to ascertain whether the sample size used in the study had adequate power (0.80) (Cohen 1992), to detect the likelihood of responding to a level-1 friend-request and level-2 information request. For the regression model estimating individual response to the level-1 attack, the effect size approximated using Pseudo R^2 of 0.20 translated to Cohen's f^2 of 0.25. For this regression with 3 predictors, the minimum sample threshold for achieving a power of 0.80 at the 0.05 significance level was 59. For the regression model estimating individual response to the level-2 attack, the R^2 of 0.21 translated to Cohen's f^2 of 0.26. For this regression with 4 predictors, the minimum sample threshold for achieving a power of 0.80 at the 0.05 significance level was 62. Thus, the sample size of 127 used in the current study was deemed sufficient.

Note 3. To assess whether the categorization of individuals into the ordinal categories might have influenced the regression results, the research also conducted logistic regressions by coding those who accepted the friend-request as 1 and the rest has having denied it (coded 0). The overall regression was significant: χ^2 (6) = 19.73, $p < 0.001$; Nagelkerke's Pseudo R^2: 36%. As in the ordinal regression, the friend × device interaction was significant ($\beta = 3.38$, SE = 1.59, Wald (1) = 4.52, $p < 0.05$, OR = 29.29). Likewise, coding all those who accepted the information-request as 1 and comparing them against those who denied the request also netted a significant regression: χ^2 (7) = 15.15, $p < 0.05$, Nagelkerke's Pseudo R^2: 23%. Again, as in the ordinal regression, the effect of accepting the friend-request remained significant ($\beta = 1.43$, SE = 0.49, Wald (1) = 5.16, $p < 0.05$, OR = 4.17). The logistic regressions are presented in Appendix C.

* $p < 0.05$.

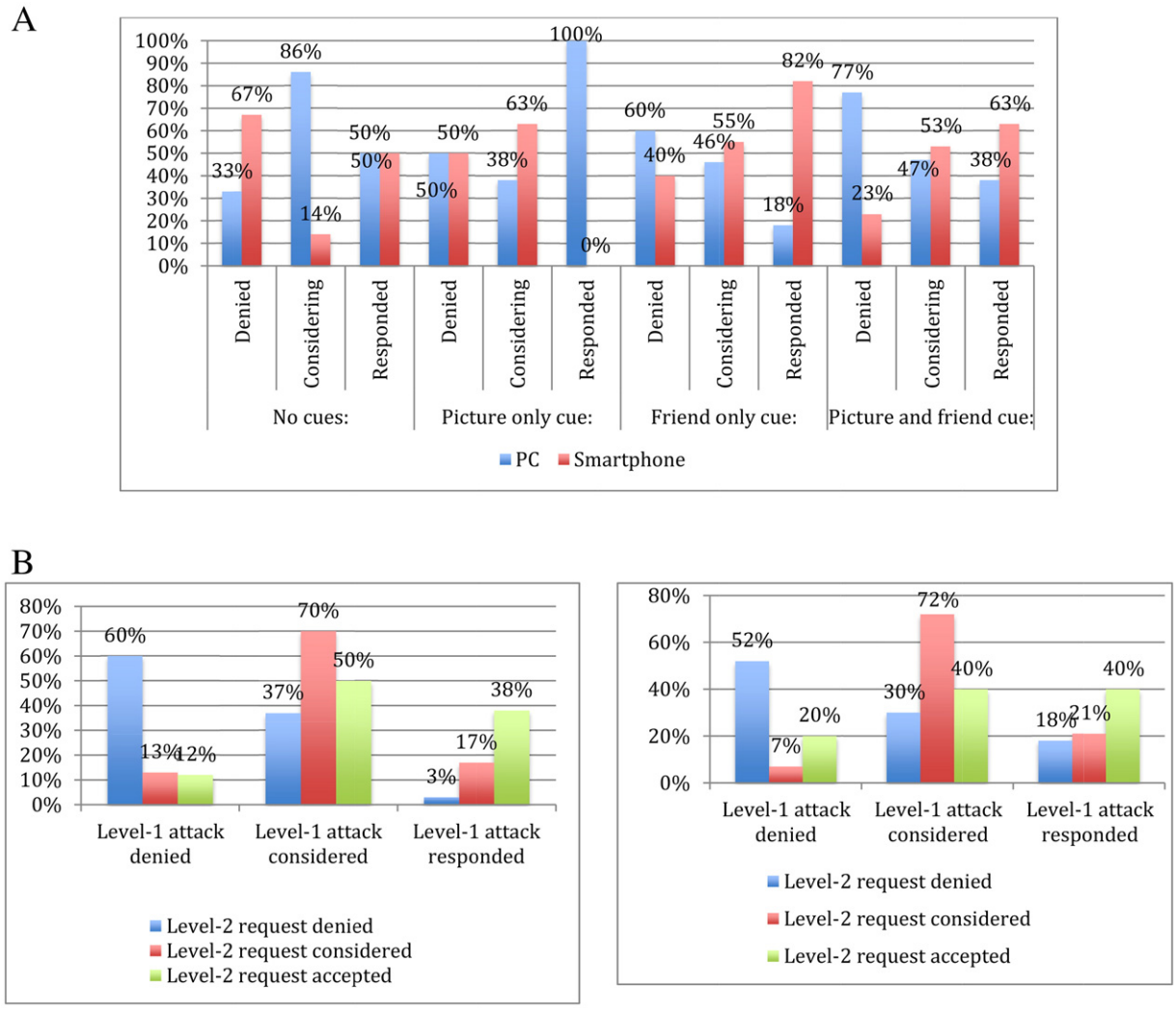

Fig. 2. A. Level-1 SNP request: Response status by condition and access-device. B. Percentage of individuals who accepted the level-2 request and level-1 request on a PC (left) and on a smartphone (right).

improving systematic processing and requires cognitive effort to detect deception [16,53]—to providing people with heuristics that efficiently detects deception.

When the phisher's Facebook profile picture and friend count appeared together, their combinatorial cueing effect was noteworthy from a HSM and interface affordance standpoint. The profile picture, potentially because of the effective heuristics it triggers, attenuated the effect of the heuristics triggered by the phisher's friend count, and the request was less successful than a request with just the friend count. Users were seven times more likely to fall for a request with just friend counts while they were five times *less* likely to fall for a SNP request with a picture that accompanied the friend count. Thus, rather than witness the hypothesized *cue-cumulation effect*, where the presence of each cue additively increased the net victimization rate, the study evidenced a *cue-attenuation effect* when the two cues appear together. A potential explanation for the attenuation is that heuristically processing many cues, especially cues that trigger contrasting (or oppositional) heuristics, where one supports the decision and another rejects it, likely engenders more cognitive effort, and the net effect of this might be a reduction in the likelihood of deception. In other words, having many oppositional heuristic cues presumably results in a reasoned response, which although not as effective as systematic processing or as effective as the cueing effect of the profile photo by itself, appears to be relatively effective for deception-detection. The dampening effect of oppositional heuristics suggests that one solution to SNP victimization could be to redesign social media interfaces with many cues—more than just the two afforded by Facebook—that trigger oppositional heuristics (such as displaying a network chart of a sender with profile pictures) and altogether help establish the validity of a request.

Next, the research finding on the moderating role of access-devices is particularly noteworthy. Here the research found that the use of smartphones instead of a PC increased the likelihood of victimization four-fold. The consequences of smartphone use on deception, or for that matter, information processing, have received little academic attention [22]. Smartphone use appears to increase individual susceptibility to level-1 attacks by moderating the cueing effect of the phisher's Facebook friend count. The moderating effect was premised on smartphones' relative visual restrictions (small screen size) that increase the presentation and prominence of graphical cues and cognitive constraints due to user behavior (walking, talking, driving and such) that enhance the reliance on existing graphical cues. To some extent the visual limitations were manifested in all the study conditions because the interface-icons such as the confirm button was present in all the attacks. And, quite plausibly, global competition between cellular networks and smartphone device manufactures (e.g., SingTel vs. M1, Apple vs. Samsung, reflecting each other's offerings) equalized any device related variances in the study. Thus, the more likely explanation for the device effects was the individuals' behavioral patterns of how

Table 5
Counts and percentages of respondents who accepted the level-1 attack and the level-2 attack either on a PC or smartphone.

		Count and % within level-2 request acceptance status	Level-2 attack acceptance status		
			Denied	*Considering*	*Accepted*
Level-1 attack acceptance status among individuals using a PC for access	*Denied*	N	18	3	1
		%	60%	13%	12%
	Considering	N	11	16	4
		%	37%	70%	50%
	Responded	N	1	4	3
		%	3%	17%	38%
Level-1 attack status among individuals using a smartphone for access	*Denied*	N	14	2	2
		%	52%	7%	20%
	Considering	N	8	21	4
		%	30%	72%	40%
	Responded	N	5	6	4
		%	18%	21%	40%

they used smartphones, what else users were doing simultaneously while they used these devices, and consequently, how rushed or how much time they felt was available for processing the request. Anecdotal evidence of how people text on their smartphone while driving causing numerous accidents each year speaks to the urgency that many people feel when they receive messages on their smartphone. In the level-1 attack context, similarly high levels of perceived urgency to respond perhaps heightens the values of a cue in the request that allows for a snap-decision. In other situations involving uncertainty, such as in online auctions when people have to choose from many comparable used products, individuals tend to be especially reliant on the count of the number of people who have already bid on a product to guide their decision [41]. Perhaps using a smartphone and the sense of urgency it fosters similarly makes people rely on bandwagon cues that allow for a quick assessment of the authenticity of the profile, but the net effect of this is a seven-fold increase in their likely victimization in such attacks. With more than the majority of U.S. adults using smartphones [43], these results call for more serious attention to device affordances with a focus on how people's patterns of using such devices influence their cognitive capacity and deception-detection.

Finally, when it came to level-2 SNP attacks, the research had hypothesized a co-occurrence of heuristic and systematic processing premised on the availability of content and heuristic cues. Support for the hypothesis came from the relatively lower overall victimization rates in the level-2 vis-à-vis the level-1 attacks. The victims in level-2 tended to be mostly those who already accepted the level-1request; the odds of falling victim were four times more if you already accepted the level-1 request. Thus, it appears that individuals fell victim because they trust trusted their Facebook friends, which perhaps evoked a need to maintain consistency with their prior action of accepting the level-1 request [10,12,24,45]. What makes these results particularly interesting is the fact that the individuals in the study barely knew the phisher for two weeks. The findings may thus be reflective of the types of weak-tie networks that people appear to form and maintain on Facebook [39]. Facebook's interface affordances foster relationship maintenance through clicking, tagging, and brief posts, and there are limited personal interactions, which perhaps makes it difficult to discern whether a sender would really pose such a question or request information in a certain manner. This could be the reason why the receivers of information-requests on Facebook, once they peripherally assess whether a person is a friend using the profile picture or sender's name easily visible in the request, respond to the request. The likelihood of such peripheral processing (as well as of maintaining social relationships by clicking and brief posts) is conceivably greater on a smartphone because of the aforementioned ways in which people use these devices. This might explain why subjects in the study using smartphones were four-times more likely to comply with a level-2 request if they had already accepted the level-1 request.

Being one of the first explorations of the SNP phenomenon, the study necessitated design and measurement decisions that limit the generalizability of some of these results. Among these was the use of all average looking males in the profiles, which compared to say using attractive females, likely provides a lower bound estimate of victimization rates. Another limitation stems from the experimental approach, where the focus was on internal validity, made possible by the use of a homogenous sample of students, which somewhat restricts the generalizability of the findings. That said, students and younger individuals are an at risk group make up >88% of all Facebook users[8] and are increasingly the target of phishing attacks [54]. Also, the study was conducted in Singapore, whose citizens although similar in many respects to the U.S. on the key metrics of interest (e.g., social media penetration: 82% in Singapore versus 74% in the U.S., and the dominance of English in both nations[9]) are in a distinctly different culture from the U.S. Yet another limitation is the use of HSM as the sole explanatory framework. HSM provides a first-order theoretical explanation of many other cognitive processes such as social presence or information richness [30], but other explanations like the role of habits on explaining device affordance effects [22] remains unexamined.

All of these limitations can be overcome future research. Future research could expand the study to other social networks to examine any differences stemming from why people use a particular social media. For instance, perhaps the number of victims is higher on LinkedIn if a job is offered on that network, because many people use that platform for career enhancement. Such research could be conducted using real world samples so as to test the generalizability of the present results as well. Research needs to also examine the optimum friend counts that cues credibility and enhances victimization. More friends might ostensibly enhance victimization even more and there is surely and likely optimum count below or beyond which the realism heuristic steps in to influence the rate of victimization. Finally, future research needs to also further explore the role of mobile devices. Questions such as whether tablets users are more susceptible to SNP attacks compared to smartphone and computer users, and whether devices influence SNP victimization by solely enhancing heuristic processing or by instead triggering habitual reactions [22], also need to be examined.

Facebook and for that matter all social media platforms are constantly evolving in terms of features and functionality, making some of the conclusions of the study bound by the points in time when the data were gathered. In recent months, Facebook has expanded its services through acquisitions (Instagram, Whatzapp), refined older services (spinning-off of Facebook Messenger) and developed newer offerings (Graph Search and social gaming) that whilst changing some of the interface affordances have also expanded the user experience. Consequently, today there are more users using Facebook for more uses, making the potential universe of victims all the more vast.

The overall findings of the current study are, thus, noteworthy and pertinent even in the face of the many changes to Facebook. The results stress the need for future research on the SNP phenomenon with a focus on the cues afforded by the Facebook interface and the heuristics they trigger, and on device affordances with a focus on how people use mobile devices to access Facebook. Taken together, the findings of the study contribute to the extant literature, yield important insights into social media deception, and mark an important first step towards combating this new form of deception.

[8] http://www.pewinternet.org/2016/11/11/social-media-update-2016/.

[9] Social media penetration data was retrieved from Socialbaker.com: Singapore http://www.socialbakers.com/facebook-statistics/singapore; U.S.A. http://www.socialbakers.com/facebook-statistics/united-states. Data on Internet penetration was retrieved from http://www.internetworldstats.com/top25.htm.

Appendix A. Sample Facebook profile of the phisher with a profile picture and phony friends

Appendix B. Were heuristics activated in a level-1 and level-2 SNP attack?

If heuristics were activated prior to people responding to the respective level-1 requests, it would provide direct evidence that the cues in the attacks were being attended to and indirect evidence of their influence on heuristic processing.

To check this assumption, two six-item scales were developed to measure *Heuristics activated in a level-1 SNP attack* and *Heuristics activated in a level-2 SNP attack* in subjects' cognition while reviewing the respective attacks. Items were created based on the HSM literature [26,32] and derived using interviews of students on the heuristics they generally use while reviewing friend-requests and information requests on social media. Sample items used to assess heuristics activated while reviewing the level-1 attack read "I don't friend anyone on Facebook I haven't personally met before," "I don't friend people who don't already have many friends on Facebook." Items used to assess heuristics activated while reviewing the level-2 attack read "I never respond to emails/electronic messages asking for personal information," "I only respond to emails/electronic messages from people I am friends with on Facebook," "I never respond to emails/electronic messages with deadlines on the request," and so on.

Subjects scored each item on a 1–5 response scale (1 = strongly disagree) and the overall scales achieved an acceptable alpha reliability (level-1 heuristics activated: $\alpha = 0.78$; level-2 heuristics activated: $\alpha = 0.79$).

B.1. The extent to which heuristics activated in a level-1 SNP attack

The extent to which heuristics were activated during a level-1 SNP attack was tested using $2 \times 2 \times 2$ ANOVA with pictures (no picture vs. picture), friend cues (no friends vs. 10 friends), and access-device (smartphone vs. computer) as the independent factors and *Heuristics activated in a level-1 SNP attack* as the dependent variable. The ANOVA ($F(7,119) = 6.26$, $p < 0.05$, $\eta^2 = 0.30$) showed a significant main effect for heuristics activated in presence of pictures ($F(1,119) = 8.51$, $p < 0.05$, $\eta^2 = 0.07$), friend cues ($F(1,119) = 9.51$, $p < 0.01$, $\eta^2 = 0.07$), and based on access device ($F(1,119) = 16.49$, $p < 0.01$, $\eta^2 = 0.12$).

The mean differences suggested that more heuristics were activated in the presence rather than the absence of picture cues ($MD = 0.32$, $SE = 0.12$, $p < 0.05$); the presence rather than the absence of friend cues ($MD = 0.38$, $SE = 0.12$, $p < 0.05$); and on mobile devices rather than computer ($MD = 0.50$, $SE = 0.11$, $p < 0.05$). Among the interactions, only the friend cues × access-device interaction was significant: $F(1,119) = 5.22$, $p < 0.01$, $\eta^2 = 0.04$. Thus, the presence of cues about the number of friends of the sender rather than the absence of such cues activated significantly more heuristics when the request was accessed on a mobile device rather than a computer.

B.2. The extent to which heuristics activated in a level-2 SNP attack

The extent to which heuristics were activated during a level-2 SNP attack was tested using a $2 \times 2 \times 2$ (picture vs. friend cues vs. device) ANOVA with *Heuristic activated in a level-2 SNP attack* as the dependent variable. The $2 \times 2 \times 2$ ANOVA ($F(7,118) = 3.49$, $p < 0.05$, $\eta^2 = 0.08$) only netted a significant two-way interaction between pictures and friend cues ($F(1,116) = 4.36$, $p < 0.05$, $\eta^2 = 0.04$) on the heuristics activated by the level-2 information request. Although the follow-up tests were not statistically significant, picture cues alone seemed to activate more heuristics ($M = 3.81$, $SE = 0.14$) than picture and friend cues together ($M = 3.51$, $SE = 0.12$) and friend cues ($M = 3.50$, $SE = 0.12$). Thus picture cues appear to activate more heuristics in level-2 attacks.

Appendix C. Logistic regressions predicting likely response to friend-request and to information-request

	Parameter estimates predicting likelihood of confirming (1) vs. denying (0) friend-request			Parameter estimates predicting likelihood of responding (1) vs. denying (0) the information-request		
	Logit B	Std. error	Exp B	Logit B	Std. error	Exp B
Constant	−1.15	0.99	0.32	−3.65*	1.24	0.03
Picture cues (base: no pictures)	0.09	1.23	1.09	−0.46	1.13	0.63
Friend cues (base: no friends)	0.58	1.26	1.78	−0.56	1.12	0.57
Access-device (base: computer)	−1.17	0.72	0.31	0.61	1.11	1.85
Picture cues × friend cues	−0.64	1.49	0.52	0.92	1.30	2.51
Friend cues × access-device	3.37*	1.59	29.28	−0.46	1.43	0.63
Picture cues × access-device	−0.95	1.36	0.38	−0.48	1.27	0.62
Covariate (response to friend request)				1.43*	0.49	4.19
Model fit	Model χ^2 (6) = 19.73, $^*p < 0.05$			Model χ^2 (7) = 15.15, $^*p < 0.05$		
R^2	Nagelkerke's = 0.36, Cox & Snell = 0.37			Nagelkerke's = 0.23, Cox & Snell = 0.15		

References

[1] I. Bose, A.C.M. Leung, Unveiling the mask of phishing: threats, preventive measures, and responsibilities, Communications of the AIS 19 (2007) 544–566.
[2] E. Protalinski, Chinese spies used fake Facebook profile to friend NATO officials, ZD Net, 2012.
[3] J.C. Dvorak, LinkedIn account hacked, PC Magazine, 2011.
[4] D. Herbeck, A. Besecker, Hardworking Teacher Masked His Sinister Side, The Buffalo News, Buffalo, NY, 2011.
[5] R. Jha, ISI used Facebook to honeytrap IAF airman into spilling secrets, The Times of India, 2015 December 30http://timesofindia.indiatimes.com/india/ISI-used-Facebook-to-honeytrap-IAF-airman-into-spilling-secrets/articleshow/50373342.cms.
[6] S. Miller, Sen. Grassley's Twitter account hacked by SOPA protesters, ABC News, 2012http://abcnews.go.com/blogs/politics/2012/01/sen-grassleys-twitter-account-hacked-by-sopa-protesters/.
[7] K. Opsahl, Facebook's Eroding Privacy Policy: A Timeline, Electronic Frontier Foundation, 2010.
[8] R.T. Wright, K. Marett, The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived, J. Manag. Inf. Syst. 27 (2010) 273–303.
[9] K. Yurieff, Facebook tests tool to prevent catfishing, CNN, 2017 Monday, June 23, 2017 http://money.cnn.com/2017/06/22/technology/facebook-protect-profile-picture/index.html.
[10] Gerald R. Miller, Paul A. Mongeau, Carra Sleight, Fudging with friends and lying to lovers: deceptive communication in personal relationships, J. Soc. Pers. Relat. 3 (1986) 495–512.
[11] B. Reeves, C. Nass, How People Treat Computers, Television, and New Media Like Real People and Places, CSLI Publications and Cambridge University Press, 1996.
[12] J.B. Hancock, Social Media Make Us More Honest, https://www.ted.com/talks/jeff_hancock_3_types_of_digital_lies?language=en 2013.
[13] M. Jakobsson, The human factor in phishing, Privacy & Security of Consumer Information, Bloomington, IN, 2007.
[14] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, Y.-K. Lim, What instills trust? A qualitative study of phishing, Usable Security (USEC'07), Lowlands, Scarborough, Trinidad/Tobago, 2007.
[15] S. Grazioli, Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet, Group Decis. Negot. 13 (2004) 149–172.
[16] P.E. Johnson, S. Grazioli, K. Jamal, G. Berryman, Detecting deception: adversarial problem solving in a low base rate world, Cogn. Sci. 25 (2001) 355–392.
[17] C.D. Wickens, Processing resources and attention, Multiple-Task Performance 1991, pp. 3–34.
[18] A. Vishwanath, Habitual Facebook use and its impact on getting deceived on social media, J. Comput.-Mediat. Commun. 20 (2015) 83–98.
[19] A. Vishwanath, Diffusion of deception on social media: social contagion and its antecedents, Inf. Syst. Front. (2014) 1–15.
[20] J.J. Gibson, The Concept of Affordances. Perceiving, Acting, and Knowing, 1977 67–82.
[21] S.S. Sundar, The MAIN model: a heuristic approach to understanding technology effects on credibility, in: Miriam J. Metzger, Andrew J. Flanagin (Eds.), The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, MIT Press, Cambridge, MA 2008, pp. 73–100.
[22] A. Vishwanath, Mobile device affordance: explicating how smartphones influence the outcome of phishing attacks, Comput. Hum. Behav. 63 (2016) 198–207.
[23] A. Vishwanath, T. Herath, R. Chen, J. Wang, H.R. Rao, Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model, Decis. Support. Syst. 51 (2011) 576–586.
[24] M. Workman, Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security, J. Am. Soc. Inf. Sci. Technol. 59 (2008) 662–674.
[25] A. Vishwanath, B. Harrison, Y.J. Ng, Suspicion, cognition, and automaticity model of phishing susceptibility, Commun. Res. 0093650215627483 (2016).
[26] S. Chaiken, Heuristic versus systematic information processing and the use of source versus message cues in persuasion, J. Pers. Soc. Psychol. 39 (1980) 752.
[27] S. Chaiken, The Heuristic Model of Persuasion, Lawrence Erlbaum Associates, Hillsdale, NJ, 1987.
[28] S. Chaiken, A. Liberman, A.H. Eagly, Heuristic and systematic processing within and beyond the persuasion context, in: J.S. Uleman, J.A. Bargh (Eds.), Unintended Thought, Guilford Press, New York 1989, pp. 212–252.
[29] W.P. Eveland, D.V. Shah, N. Kwak, Assessing causality in the cognitive mediation model: a panel study of motivations, information processing, and learning during campaign 2000, Commun. Res. 30 (2003) 359–386.
[30] S.S. Sundar, A. Oeldorf-Hirsch, A.K. Garga, A cognitive-heuristics approach to understanding presence in virtual environments, PRESENCE 2008: Proceedings of the 11th Annual International Workshop on Presence, 2008, 2008.
[31] S.T. Fiske, S.E. Taylor, Social Cognition, 2nd ed. McGraw-Hill, NY, 1991.
[32] A. Zuckerman, S. Chaiken, A heuristic-systematic processing analysis of the effectiveness of product warning labels, Psychol. Mark. 15 (1998) 621–642.
[33] L. Humphreys, Photographs and the presentation of self through online dating services, in: Paul (Ed.), Digital Media: Transformations in Human Communication, 2004.
[34] Y.J. Koh, S.S. Sundar, Heuristic versus systematic processing of specialist versus generalist sources in online media, Hum. Commun. Res. 36 (2) (2010) 103–124.
[35] A. Vishwanath, Comparing online information effects, Commun. Res. 30 (2003) 579–598.
[36] S. Lee, Y. Sun, E. Thiry, Do you believe in love at first sight: effects of media richness via modalities on viewers' overall impressions of online dating profiles, Proceedings of the 2011 iConference, ACM 2011, February, pp. 332–339.
[37] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith, M. Beaton, Teens, social media, and privacy, Pew Internet & American Life Project, 2013http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.
[38] C.S. Dodson, D.L. Schacter, When false recognition meets metacognition: the distinctiveness heuristic, J. Mem. Lang. 46 (4) (2002) 782–803.
[39] K.N. Hampton, L.S. Goulet, C. Marlow, L. Rainie, Why most Facebook users get more than they give, Pew Internet & American Life Project 2012, p. 3http://www.pewinternet.org/2012/02/03/why-most-facebook-users-get-more-than-they-give/.
[40] B. Latane, S. Nida, Ten years of research on group size and helping, Psychol. Bull. 89 (1981) 308–324.
[41] U.M. Dholakia, K. Soltysinski, Coveted or overlooked? The psychology of bidding for comparable listings in digital auctions, Mark. Lett. 12 (2001) 225–237.
[42] S.S. Sundar, S. Knobloch-Westerwick, M.R. Hastall, News cues: information scent and cognitive heuristics, J. Am. Soc. Inf. Sci. Technol. 58 (2007) 366–378.
[43] A. Smith, Nearly half of American adults are smartphone owners, Pew Center & American Life Project, 1, 2012, p. 4http://www.pewinternet.org/2012/03/01/nearly-half-of-american-adults-are-smartphone-owners/.
[44] T.N. Jagatic, N. Johnson, M. Jakobsson, Phishing attacks using social networks, Indiana University Subject Study 05-9892 & 05-9893, 2005.
[45] R.B. Cialdini, Influence, HarperCollins, 2009.
[46] B. Prince, Phishing attacks cost millions despite low success rate, E-Week, 2009.
[47] N.B. Ellison, C. Steinfield, C. Lampe, The benefits of Facebook "friends:" social capital and college students' use of online social network sites, J. Comput.-Mediat. Commun. 12 (2007) 1143–1168.
[48] S.L. Feld, Why your friends have more friends than you do, Am. J. Sociol. (1991) 1464–1477.
[49] W.J. McGuire, The nature of attitudes and attitude change, The Handbook of Social Psychology, 3, 1969, pp. 136–314.
[50] R.R. Lau, D.O. Sears, Political Cognition: The 19th Annual Carnegie Symposium on Cognition, Routledge, 1986.
[51] S. Lee, Y. Sun, E. Thiry, Do you believe in love at first sight: effects of media richness via modalities on viewers' overall impressions of online dating profiles, Proceedings of the 2011 iConference, ACM 2011, February, pp. 332–339.

[52] H.A. Simon, Models of Man: Social and Rational, Wiley, New York, 1957.
[53] D.P. Brios, J.F. George, R.W. Zmund, Inducing sensitivity to deception in order to improve decision making performance: A field study, MIS Quarterly 26 (2002) 119–144.
[54] V. Stephen, Common College Scams, Nerd Wallet, 2012http://www.nerdwallet.com/blog/education/common-college-scams.
[55] B.J. Bank, S.L. Hansford, Gender and friendship: why are men's best same-sex friendships less intimate and supportive? Pers. Relat. 7 (2000) 63–78.
[56] C. Welch, Apple confirms password vulnerability, says its working on a fix, The Verge, 2013, March 22http://www.theverge.com/2013/3/22/4137068/apple-confirms-security-threat-working-on-fix.

Arun Vishwanath, Ph.D., MBA, is Associate Professor of Communication at the University at Buffalo and a Faculty Associate at the Berkman Center for Internet and Society at Harvard University. His research is on phishing and spoofing attacks and on finding ways to mitigate them. This work has led to an understanding of the joint role of conscious cognitions and automatic habits in determining individual victimization through such attacks. He is presently developing strategies for mitigating breaches and interventions that lead to better cyber hygiene.

Arun has authored over two dozen peer-reviewed research papers and his opinions on cybersecurity have been featured on CNN, BBC World News, The Conversation, The World Economic Forum, USA Today, and a host of other media outlets. His research on phishing has been funded by the National Science Foundation and he is also working with teams from the NSA, NIST, DHS, and The White House's OSTP in testing strategies for better protecting computer networks in the federal government.