Habitual Facebook Use and its Impact on Getting Deceived on Social Media

Arun Vishwanath
Department of Communication, University at Buffalo, Buffalo, NY 14260

There are a billion Facebook users worldwide with some individuals spending 8 hours each day on the platform. Limited research has, however, explored the consequences of such overuse. Even less research has examined the misuse of social media by criminals who are increasingly using social media to defraud individuals through phishing-type attacks. The current study focuses on Facebook habits and its determinants and the extent to which they ultimately influence individual susceptibility to social media phishing attacks. The results suggest that habitual Facebook use, founded on the individual frequently using Facebook, maintaining a large social network, and being deficient in their ability to regulate such behaviors, is the single biggest predictor of individual victimization in social media attacks.

Keywords: Habit Strength, Deficient Self-Regulation, Facebook Habits, Media Addiction, Online Deception, Social Media Deception, Phishing, Social Media Abuse, Social Media Scams.

doi:10.1111/jcc4.12100

Cynthia Newton, a young mother reportedly spends 20 hours per week on Facebook—something that she tried unsuccessfully to cut-down (Cohen, 2009). Young adults in the U.K. report checking their Facebook feeds 20 times on average each day and spend upwards of 40 hours each month or a whole working week utilizing the platform (London, 2012). Other news stories of teens breaking into the offices of CNN to check their Facebook profiles and therapists and counselors reporting an increase in the number of Facebook “addicts” speak to a sort of compulsivity in the use of Facebook (Cohen, 2009; Kelly, 2012). While the news media present a number of such stories, academic research in this realm remains limited, with research instead focusing on the positive aspects of social media use (Effing, van Hillegersberg, & Huibers, 2011; Ellison, Steinfield, & Lampe, 2007). Even less research has focused on the misuse of social media by perpetrators of crime. This lack of coverage may stem from how closely Facebook controls information, mostly presenting positive stories about the use of its platform. Thus, information about security leaks, privacy breaches, or user problems on Facebook are only inadvertently revealed.

Recently, bloggers who were scrutinizing Facebook’s SEC filings prior to its initial public offering discovered that close to one in ten or approximately 100 million Facebook profile pages were duplicates or
fake accounts (Cluley, 2012). Although Facebook declined to comment on the duplicate accounts, anecdotal evidence from news reports suggests that many of these accounts are being used for phishing-type attacks. For instance, in a recent case, con artists used photographs and names of real U.S. army soldiers to create Facebook profiles, friend women using these profiles, and scam them (Quinn, 2011). In another, a high school teacher pretended to be a student by creating a fake Facebook profile and used it to procure pictures and other sensitive information from his students (Herbeck & Besecker, 2011). In addition to being used by criminals, such phishing type attacks have been implicated in cyber-espionage attacks. For instance, in a recent case that has been attributed to the Chinese government, a phony Facebook profile of a high-ranking U.S. navy commander was used to friend military personnel in the U.S. and U.K. in order to monitor their movements (Protalinksi, 2012). More recently, the Wall Street Journal hack, as well as the hacks of the New York Times, CBS, NPR and the Associated Press (AP) content management logins and journalist emails, have all been attributed to phishing attacks (Smith, 2013). In the AP attack, for instance, a tweet was sent from the AP’s Twitter account claiming there had been two explosions in the White House injuring President Obama. Although the AP sent out a correction in less than 15 minutes, the Dow Jones industrial average had already dropped by over 100 points, causing a loss of close to 150 billion U.S. dollars (ElBoghdady, 2013). Hence, phishing via social media seems to be the attack vector of choice for a variety of crimes. The wide-ranging disruptive potential of such attacks makes the need to study why individuals succumb to social media phishing attacks important from a law enforcement, public policy, and national security standpoint.

Unlike e-mail-based phishing attacks that have less than a 1% success rate, phishing attacks on social media appear to be far more successful and simulated attacks report more than a 40% success rate (Prince, 2009). The high victimization rate can be attributed to the unique nature of social media phishing attacks. For one, phishing attacks on social media occur over relatively new and evolving platforms such as Facebook and Google Plus, where the interface, its functionalities, and its user protections are constantly changing. Consequently individuals may be unable to achieve a degree of mastery over the use of the platform. Two, e-mail-based phishing is usually a one-stage attack, where the phisher sends an e-mail to a large number of individuals and awaits a response. In contrast, phishing attacks on social media are often two-stage attacks. In the first stage, the phisher sends a friend-request and attempts to friend (connect with) a potential victim. The acceptance of a friend-request could net a wealth of information about the victim. Given the networked nature of social media, the phisher could also gather information about every other person the victim is connected to and the friends of those other individuals as well. The phisher could then move to the second-stage of the attack and utilize Facebook’s in-built messaging function to request information directly from the victim. Such requests could be for personal information and could be tailored by using information from the victim’s profile, wall posts, and news feeds, making the request more personalized and, thus, persuasive. For instance, knowing that someone loves dogs could be used to ask for a small donation for a pet charity that might be a ruse to acquire their credit card information. Stage two messages could also contain URLs or innocuous-looking attachments with hidden scripts and viruses that could infect the device being used to access the message. These viruses could be programmed to deploy at certain times and data-mine the individuals’ smartphone, computer, or their organization’s network infrastructure for information. Besides this, social media attacks have the potential for contagion effects, where the first few victims result in many more victims who see their friends appear as connections to the phisher and believe in the legitimacy of the phisher.

Surprisingly, limited research examines social media-based phishing. The extant research in this area tends to focus on e-mail-based deception and more on how to detect online deception (Biros, George, & Zmud, 2002; Joinson, Hancock, & Briggs, 2008) rather than on why individuals fall victim to such attacks. Moreover, the focus among scholars has been on the proximate factors such as cognitive processing and deceptive cues in the phishing attack that are the immediate causes of individual victimization
(Vishwanath, Herath, Chen, Wang, & Rao, 2011; Workman, 2008). The cumulative evidence from this line of work suggests that individuals fall victim to phishing attacks because they fail to adequately attend to the cues in the email that reveals its deception. Therefore, policy makers have created interventions aimed at improving individuals’ ability to identify, evaluate, and effectively process these clues (Biros et al., 2002). Such interventions, however, seem to have limited success in reducing individual susceptibility over the long term. In a series of studies conducted from 2004–2007, called the “Carronade experiments,” army cadets at West Point were trained on various ways to effectively detect phishing emails before being subjected to real phishing attacks (Ferguson, 2005). The research found that education and training were only effective in the short-term and their effects wore off within a few hours when the cadets relaxed back into their regular patterns of email use. Consequently, most of the cadets were successfully phished within 4 hours after the educational intervention was administered. Thus, while the proximate cause of victimization appears to be information processing, the ultimate cause appears to be the individuals’ habitual pattern of email use—an issue that has yet to be examined within the phishing-based deception context.

To this end, the current research examines the extent to which individuals’ social media habits ultimately influence their susceptibility to level 1 and level 2 phishing attacks on Facebook. Besides habits, two other ultimate causes, individuals’ levels of attitudinal commitment and their concern for privacy, both of which have been shown to increase individual motivations and how they process information, are also examined.

Because limited research has examined Facebook habits, the next section defines the Facebook habit construct and examines its theoretical antecedents. This is followed by the extant literature on attitudinal commitment and individual privacy concerns along with the key hypotheses that ground the investigation.

Theoretical Premise

Antecedents of Facebook Habits

Habitual Facebook use is defined as the automaticity in consumption and use of the social media platform that develops as individuals repeatedly and routinely access, interact, and utilize Facebook because of the gratifications received from such action. This definition is in line with the current thinking about habitual media use from the media attendance perspective where habits are seen to be acquired by repeating media consumption in stable circumstances (LaRose, 2010; Verplanken & Wood, 2006). Overtime, when enacted repeatedly, behaviors become action-scripts that are applied without conscious reflection about its antecedents, consequences, or even its enactment (LaRose & Eastin, 2004).

While there is some disagreement over the correct terminology to describe out of control media use—with some referring to it as media addiction (Young, 1988), others preferring media abuse (Morahan-Martin, 1999), and still others problematic media use (Caplan, 2002)—there is general consensus that habitual media use involves repeated use of a medium or platform, motivations that cause, or in the past led to repeated use, and some feelings of inability to limit usage (Chen & Kim, 2013; Chittaro & Vianello, 2013; Morahan-Martin, 2008). Based on this, the current research identifies three likely antecedents for Facebook habits: consumption frequency, gratifications, and automaticity. First, habitual behaviors tend to be enacted repeatedly. Hence, one indicator of the presence of a Facebook habit is frequent consumption of the Facebook platform. Not all behaviors that occur frequently are, however, indicative of habits. For instance, some individuals might regularly visit an online financial website because they are invested heavily in the stock market; commercial pilots and recreational boaters might check an online weather app often; a graduate student might regularly visit an online site that
has academic job postings. Hence, the frequency of occurrence or the sheer number of an individual’s actions of Facebook is not necessarily indicative of a habit. In addition to regular enactment, habits take shape as individuals receive gratifications from the behavior.

Within the field of Communication, the uses and gratifications paradigm has identified a number of different gratifications that drive individual media consumption (Rosengren, Wenner, & Palmgreen, 1985). These range from surveillance gratifications to communication, entertainment, and ritualistic consumption. Although some research has extended this paradigm to explain social media use (Raacke & Bonds-Raacke, 2008), it is difficult to accurately assess the gratifications sought by all Facebook users in a valid and consistent manner (Quan-Haase & Young, 2010). This is partly because the platform is still in the early stages of diffusion and newer segments of users, each attracted by different gratifications, are still adopting Facebook. For instance, the Pew Center reports that one of the fastest-growing new segments of Facebook users is adults who are 50 plus years of age who are adopting the platform to not only to stay connected with their family but also to seek social support for chronic illness (Madden, 2010). Besides this, Facebook, in its bid to keep individuals interested in the platform, is constantly expanding the functions and services it offers. Its newer services such as Graph Search and social gaming could prompt newer, unexplored gratifications being sought and obtained by users. Finally, Facebook incorporates many different functions ranging from news feeds to photo sharing, instant messaging, e-mail, gaming, and shopping. Hence, the reasons that individuals utilize Facebook could range based on the specific function being used at any given time. For instance, the gratifications sought by individuals while using the messaging function on Facebook is perhaps more similar to that of using Web 1.0 instant messaging services (Flanagin, 2005), while those sought by individuals reading news feeds are probably akin to the gratifications sought from watching and reading online news (Vishwanath, 2008).

While the gratifications that drive social media consumption could vary based on the service utilized and the individuals’ motivations, arguably, the overarching use that drives individuals to utilize Facebook is to connect to people and maintain or increase the size of their social network (Ellison et al., 2007). The size of an individual’s social network on Facebook is indicative of their past use of the platform and also serves as an impetus for continued use of the platform. It can, thus, be thought of as a primary or first-order gratification sought that subsumes the various context-specific gratifications that different individuals might seek. For instance, an individual who has a large number of Facebook friends might have more reasons to visit the platform, more people with feeds to follow, as well as more individuals with whom to share information. Further, because media gratifications are recursive and reinforced by the gratifications obtained (Rosengren et al., 1985), having more friends on Facebook might further drive social and status needs such as wanting to inform friends of life events, or wanting to know what others think about some behavior. An individual who has many friends on Facebook has more reasons to visit the platform regularly and therefore more likely to develop patterns of using Facebook that could support habitual Facebook usage. Thus, the first two markers for the existence of habitual social media use lead to the following hypotheses:

\[ H1: \] Individuals with higher habitual Facebook use scores are significantly more likely to frequently utilize the Facebook platform.

\[ H2: \] Individuals with higher habitual Facebook use scores are significantly more likely to have a large social network of friends on Facebook.

Habits occur at the intersection of the conscious, goal-directed intentions and unconscious, unregulated reactions. So while goals are implicit to the development and the triggering of habits, the enactment of habits involves an automaticity of action. Such automaticity of action occurs when individuals are
unable to exercise control over their media-related actions. LaRose and colleagues (LaRose, 2010; LaRose & Eastin, 2002, 2004; LaRose, Lin, & Eastin, 2003) use the term deficient self-regulation to describe the state in which individual self-control over media use is diminished resulting in a lack of awareness, attentiveness, intentionality, and control over their actions. For instance, one individual with many friends on Facebook might exercise self-control and resist checking their social-feeds, while another, whose self-control is relatively ineffective, might check newsfeeds even while driving a car, with nary a concern about its consequences. Thus, in addition to being a frequent consumer and having a large number of friends on social media, a third marker of a habitual Facebook user is their inability to regulate their social media uses. The leads to the following hypothesis:

$$H3: \text{Individuals with higher habitual Facebook use scores are significantly more likely to be deficient in their ability to regulate their social media use.}$$

Impact of Facebook Habits on Social Media Deception
The consequences of Facebook habits have received limited scholarly attention. Even among scholars who study media habits and addiction, the focus has been on clarifying the theoretical prominence of media habits (Lee & Perry, 2004) rather than on its outcomes. The premise of the present study is that individuals who are habitual Facebook users are significantly more likely to fall victim to level 1 social media phishing scams, where phony individuals attempt to friend the target, and level 2 social media scams, where the phisher procures information from the target. This is because once a media behavior becomes habitual, it usually leads to patterned actions that are enacted whenever the situation or urge presents itself, without further reflection on the merits of the behavior (LaRose, 2010). Thus it is likely that individuals who are habitual Facebook users have formed ritualized patterns of usage and have relaxed their cognitive involvement while utilizing the platform. This makes it more likely that habitual Facebook users would mindlessly accept a level 1 request or comply with a level 2 request without consciously reflecting on the details of the request or the consequences of complying with it.

$$H4: \text{Individuals with higher habitual Facebook use scores are significantly more likely to fall victim to a) level 1 friend-request attack, and b) level 2 information-request attack on Facebook.}$$

Impact of Attitudinal Commitment on Social Media Deception
Habits are regularized patterns of behaviors that become routinized in the form of action scripts and enacted without any conscious reflection about the action. Thus, habitual actions require little to no cognitive processing prior to enactment. This view of human action is in contrast to the cognitive perspective, where information processing, which varies along a continuum from detailed or systematic at one end and more cursory or peripheral at the other, mediates behavior. Researchers espousing the information processing perspective have implicated the amount of cognitive resources expended by the individual as the proximate cause of phishing-based victimization (Vishwanath et al., 2011). Thus, the cognitive processing perspective suggests a parallel route through which individuals fall victim to phishing type attacks. What defines how much cognitive energy an individual is willing to commit to a processing task is their degree of attitudinal commitment to the event (Allen & Meyer, 1990; Chaiken & Eagly, 1989; Salancik & Pfeffer, 1978). Attitudinal commitment is considered a stable personality trait that defines the individuals’ choice of information processing strategy (Allen & Meyer, 1990). Hence, attitudinal commitment is another likely ultimate cause of individual victimization through social media phishing attacks.
Three types of attitudinal commitments have been show to result in phishing-based victimization: normative commitment, continuance commitment, and affective commitment (Workman, 2008). Normative commitment is the expectations of reciprocity that forms as individuals exchange information with others. It is similar to the principle of reciprocation that results in peripheral route persuasion (Cialdini, 2001) and stems from the sense of obligation that individuals feel when they are given something or begin to exchange something. Continuance commitment is the urge to continue behaviors once begun because individuals become psychologically vested in the behavior. It stems from some individuals’ tendency to believe that persistent efforts will eventually pay off, resulting in an escalation of commitment (Cialdini, 2001). Affective commitment stems from the individuals’ self-worth and their need for a psychological attachment to others with whom they identify. It results in the individual modeling behaviors and performing the actions expected by the significant target (brand, organization, group, individual) and expending effort in exchange for the emotional satisfaction of maintaining the relationship.

In e-mail-based phishing attacks, perpetrators often provide easily winnable prizes or rewards to create a token exchange; others attempt to arouse curiosity or get individuals to answer some fairly routine questions in order to start a dialogue with the intended victim. These are attempts at utilizing the principle of reciprocity to entice individuals who are highly susceptible to normative pressure into processing the information peripherally, keep responding to the request, and escalating their commitment. Likewise, some phishers offer a sum of money or a valuable item in lieu of a small “bank-clearing” fee or shipping costs paid by the intended victim. These are attempts at utilizing the principle of consistency and enticing individuals high in continuance commitment to continue escalating their involvement, while peripherally considering the negative consequences of their behavior. Finally, phishers engineer attacks to take advantage of individuals’ high in affective commitment by personalizing the e-mails and invoking brand familiarity, using fear appeals in the form of threats and warnings, appealing to individuals’ sense of patriotism (such as in scams involving wounded veterans), or to individuals’ sense of charity (such as when there is a natural disaster). Again, the emphasis is on peripheral route persuasion where images and symbolic cues distract attention away from detailed and thoughtful cognition. While empirical evidence suggests that these types of attitudinal commitment make individuals more susceptible to e-mail-based phishing attacks (Workman, 2008), their influence of individual susceptibility to level 1 and level 2 social media phishing scams remains unexplored. Because the social media attack comes from a “legitimate” individual with identifiable information along with pictures and other social network information attached to the profile, one would expect normative behavioral expectations, the drive to continue and maintain behavioral consistency, and the drive towards conformity to be felt much stronger in social media phishing attacks compared to traditional e-mail-based phishing attacks. This leads to the following hypothesis:

\[ H_5: \text{Individuals with higher levels of normative commitment, continuance commitment, and affective commitment are significantly more likely to fall victim to a) level 1 friend-request attacks, and b) level 2 information-request attacks on Facebook.} \]

**Impact of Online Privacy Concerns on Social Media Deception**

Finally, individuals’ concern for online privacy is another scope condition that could influence their likelihood of victimization in social media phishing attacks. Concern for online privacy is defined as individuals’ apprehensiveness about the disclosure of their personal information online (Buchanan, Paine, Joinson, & Reips, 2007). It is a relatively stable individual-level characteristic that stems from one’s self-evaluative assessment of personal information, the medium or platform in which it is available,
and the implications of its disclosure (Joinson & Paine, 2007). At the psychological level, concern for privacy provides opportunities for self-evaluation; behaviorally, it results in individuals protecting access to their personal information (Joinson & Paine, 2007). Thus, it is likely that individuals who are concerned about their privacy are more liable to scrutinize requests for information, especially when they emanate from a platform such as Facebook where the individual presents personal and identifiable information. Individuals with high privacy concerns are thereby expected to pay more attention to all online requests, and either notice the cues in the phishing attack that reveal deception or just reject all requests from strangers. Either way, the net effect would be a reduced likelihood of victimization.

H6: Individuals with higher levels of concern for online privacy are significantly less likely to fall victim to a) level 1 friend-request, and b) level 2 information-request attacks on Facebook.

Methods and Measures

One hundred and fifty senior undergraduate Communication students at the University of Buffalo were subjected to a real level 1 and level 2 phishing attack on Facebook. IRB approval was procured prior to the start of the study. In the beginning of the semester, students were asked to participate in an online survey about their general technology use where, buried among the questions, were measures for their Facebook usage, habitual Facebook use, deficient self-regulation, total size of their Facebook social network, their concern for privacy, and their levels of attitudinal commitment. Six weeks after the survey was completed, all the participants' Facebook accounts were located and each student was sent a friend request using a phony Facebook account created for the study (presented in the appendix). All level 1 friend-requests were sent from that account using Facebook's built-in friend-request function, which automates the sending of the requests. All requests were sent within minutes of each other. Two weeks after the level 1 attacks all subjects who were sent the level 1 request were sent a level 2 information-request from within the phony profile used to friend them, using Facebook's e-mail functionality. To appear similar to a phishing e-mail attack (Jakobsson, Finn, & Johnson, 2008), the level 2 attack (presented in the appendix) had a grammatical error and a deadline in it. The phisher stated that someone he knew was looking for interns and interested individuals should respond within three days with their student ID number, e-mail user name, and date of birth. Two weeks after the information request was sent, all the study participants were debriefed, and students were asked how likely they were to accept the level 1 friend-request and the level 2 information-request.

Measures

Response to the level 1 friend request and level 2 information request

Using a 1-5 response scale that ranged from Not at all likely to Very likely, the survey conducted after the two attacks posed one question each that measured where the respondent was in their likelihood of accepting the friend request (mean = 3.10, s.d. = 1.36) and in their likelihood of accepting the information request (mean = 2.79, s.d. = 0.97). Behavioral data from subjects who were successfully phished (accepted the friend request or provided the requested information) were used to test the validity of the self-report responses.

Frequency of Facebook use

Using a 1-5 response scale that ranged from Not at all frequently (maybe once a day or rarely) to Very frequently (one or more times every hour), three items in the survey measured individual participants'
frequency of Facebook use. Items measured how often individuals check their Facebook account for updates from friends, how often they update their own status each day, and how often they use Facebook to communicate with others on a given day (using instant messaging, replying to posts, comments on walls, and such). The overall scale (mean = 2.20, s.d. = 0.85) achieved an alpha reliability of 0.74.

**Facebook habit strength**

Habitual Facebook use was measured using three items from the literature on media habits (LaRose & Eastin, 2002, 2004; LaRose et al., 2003) and two additional items, all of which were reworded to suit the Facebook use context. Sample items include “I feel my Facebook use has gotten out of control,” “I would miss checking my Facebook page if I could no longer do it,” and “I find myself checking my Facebook account (posting or checking other people's status updates) around the same time each day.” Subjects used a 1–5 response scale that ranged from Strongly disagree to Strongly agree and the overall scale (mean = 3.35, s.d. = 0.88) achieved an alpha reliability of 0.84.

**Deficient self-regulation**

Using the same response scale, deficient self-regulation was measured using a 13-item scale derived from the prior literature on media habits (LaRose & Eastin, 2002, 2004; LaRose et al., 2003) with additional items incorporated to fit the Facebook use context. Sample items include “I feel I have to continue creating postings on my Facebook account to get a thrill,” “I check my Facebook account whenever a device that I can go online is available to me,” “I feel tense, moody, or irritable when my Facebook friends do no respond to my posts on my Facebook account.” The overall scale (mean = 1.94, s.d. = 0.79) achieved an alpha reliability of 0.89.

**Total number of Facebook friends**

Subjects were asked how many total friends they had on Facebook (mean = 482.68, s.d. = 122.55). The information was also compared against actual data on the size of social network gleaned from the subjects’ Facebook profile pages.

**Concern for privacy**

Concern for privacy was measured using a 14-item scale developed by Buchanan et al. (2007). The scale provides a unidimensional measure of individuals' general concerns about privacy on the Internet. Again some scale items were reworded to suit the Facebook context. Sample items in the scale were posed as follows: “Are you concerned about a person on Facebook not being who they say they are?” “Are you concerned that information you post on Facebook will be inappropriately forwarded to others?” “Are you concerned that strangers might know too much about you?” Items were scored by respondents using a 1-5 Not at all concerned to Very concerned response scale (mean = 3.90, s.d. = 0.78) and achieved an overall alpha of 0.94.

**Attitudinal commitment**

Based on the phishing literature (Workman, 2008) four items each measured normative commitment (mean = 4.10, s.d. = 0.48; alpha = 0.69), affective commitment (mean = 3.81, s.d. = 0.56; alpha = 0.72), and continuance commitment (mean = 3.77, s.d. = 0.63; alpha = 0.61). A sample item measuring normative commitment read “When someone gives me something, I feel like I should return the favor,” an
Table 1  Summary of Multivariate Regressions

<table>
<thead>
<tr>
<th>Variables Predicting Habitual Facebook Usage:</th>
<th>B</th>
<th>SE B</th>
<th>β</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency of Facebook use</td>
<td>.52</td>
<td>.07</td>
<td>.50</td>
</tr>
<tr>
<td>Total number of Facebook friends</td>
<td>.01</td>
<td>.00</td>
<td>.17</td>
</tr>
<tr>
<td>Deficient self-regulation</td>
<td>.26</td>
<td>.08</td>
<td>.22</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variables Predicting Likelihood of Responding to a Level 1 Friend Request:</th>
<th>B</th>
<th>SE B</th>
<th>β</th>
</tr>
</thead>
<tbody>
<tr>
<td>Habitual Facebook usage</td>
<td>.39</td>
<td>.13</td>
<td>.26</td>
</tr>
<tr>
<td>Normative commitment</td>
<td>.55</td>
<td>.25</td>
<td>.19</td>
</tr>
<tr>
<td>Continuance commitment</td>
<td>.52</td>
<td>.18</td>
<td>.24</td>
</tr>
<tr>
<td>Affective commitment</td>
<td>−.33</td>
<td>.21</td>
<td>−.13</td>
</tr>
<tr>
<td>Concern for privacy</td>
<td>−.43</td>
<td>.14</td>
<td>−.25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variables Predicting Likelihood of Responding to a Level 2 Information Request:</th>
<th>B</th>
<th>SE B</th>
<th>β</th>
</tr>
</thead>
<tbody>
<tr>
<td>Habitual Facebook usage</td>
<td>.22</td>
<td>.10</td>
<td>.21</td>
</tr>
<tr>
<td>Normative commitment</td>
<td>.30</td>
<td>.19</td>
<td>.14</td>
</tr>
<tr>
<td>Continuance commitment</td>
<td>.15</td>
<td>.14</td>
<td>.09</td>
</tr>
<tr>
<td>Affective commitment</td>
<td>.01</td>
<td>.16</td>
<td>.01</td>
</tr>
<tr>
<td>Concern for privacy</td>
<td>−.15</td>
<td>.11</td>
<td>−.12</td>
</tr>
</tbody>
</table>

Note. *p < .05

item measuring continuance commitment read “I believe in finishing what I start,” and a sample item measuring affective commitment read “It’s important to be part of the in-group.” Items were scored on a 1-5 response scale that ranged from Strongly disagree to Strongly agree.

Results

Table 1 summarizes the results of the regressions testing hypotheses 1–6. Hypotheses 1–3 were tested using a multivariate regression with Facebook habit-strength as the dependent measure and individuals’ size of social network, frequency of Facebook use, and deficient self-regulation as independent measures. The overall regression was significant, F(3, 152) = 49.58, p < .05, and explained (R^2) 49% of the variance in habitual Facebook use. All three independent constructs significantly predicted habitual Facebook usage. Individuals who frequently utilized Facebook for multiple activities were significantly more likely to be habitual Facebook users: β = 0.50, t = 7.46, p < .05, supporting Hypothesis 1. Individuals who had a large social network were also significantly more likely to be habitual Facebook users: β = 0.17, t = 2.87, p < .05, supporting hypothesis 2. In support of Hypothesis 3, individuals who were deficient in their ability to self-regulate were also significantly more likely to be habitual Facebook users: β = 0.22, t = 3.22, p < .05.

Hypotheses 4a, 5a, and 6a were tested using a multivariate regression with response to level 1 friend-request as the dependent measure and habit strength, the three types of commitment, and concern for privacy as the independent measures. The overall regression was significant, F(5, 122) = 6.67, p < .05, and explained (R^2) 19% of the variance in likelihood to fall victim to a level 1 attack. Facebook habit strength significantly predicted the individuals’ likelihood of falling victim to a level 1 attack: β = 0.26, t = 3.10, p < .05. Hence, Hypothesis 4a was supported. Among the three types of commitment, normative commitment significantly predicted likelihood of level 1 deception: β = 0.19, t = 2.19, p < .05;
continuance commitment significantly predicted likelihood of deception: $\beta = 0.24$, $t = 2.85$, $p < .05$; while affective commitment did not significantly predict likelihood of deception: $\beta = -0.13$, $t = -1.59$, $p = .12$. Hence, Hypothesis 5a was partly supported. Finally, the test of Hypothesis 6a suggested that individuals with high concern for privacy were significantly less likely to fall victim to level 1 phishing attacks: $\beta = -0.25$, $t = -3.04$, $p < .05$.

Hypotheses 4b, 5b, and 6b were tested using a multivariate regression with response to level 2 information request as the dependent measure and habit strength, the three types of commitment, and concern for privacy as the independent measures. The overall regression was significant, $F(5, 126) = 2.29$, $p < .05$, and explained ($R^2$) 6% of the variance in likelihood to fall victim to a level 2 attack. Facebook habit strength significantly predicted individuals’ likelihood of falling victim to a level 2 attack: $\beta = 0.21$, $t = 2.31$, $p < .05$. None of the three types of commitment significantly predicted the individuals’ likelihood of level 2 deception: normative commitment: $\beta = 0.14$, $t = 1.54$, $p = .13$; continuance commitment: $\beta = 0.09$, $t = 1.08$, $p = .28$; affective commitment: $\beta = .01$, $t = 0.01$, $p = .99$. Hence, Hypothesis 5b was not supported. Finally, concern for privacy did not significantly predict the individuals’ likelihood of level 2 deception: $\beta = -0.12$, $t = -1.35$, $p = .18$. Hence, Hypothesis 4b was supported while Hypotheses 5b and 6b were not supported.

**Discussion**

The research began by examining habitual Facebook use and its antecedents. Based on the significance tests and size of the standardized regression weights, it appears that Facebook habits are contingent on individual’s frequency of checking, responding, and interacting with Facebook, followed by individual’s inability to regulate such actions, and the large network of Facebook friends that an individual maintains. They altogether directly determine Facebook habituation and indirectly influence individuals’ susceptibility to level 1 friend-request attacks. Perhaps constant interaction with the Facebook platform makes individuals more likely to automatically accept friend requests; maybe having a number of friends makes accepting friend requests routine and enacted without conscious reflection; or conceivably the inability to regulate habitual consumption reduces individuals’ ability to regulate frequent interaction and causes an automaticity of responding to friend requests. In any case, habitual Facebook users are significantly more likely to succumb to level 1 friend-request attacks.

Information processing is a parallel process that, unlike automatic responses, causes some amount of conscious reflection about a decision prior to its enactment. Among the ultimate causes examined in the present study were three types of attitudinal commitment and individuals’ concern for privacy. Because they result in a peripheral processing of certain aspects of the attack rather than a detailed assessment of the entire message, attitudinal commitment was expected to enhance individuals’ susceptibility to level 1 friend-request attacks. In contrast, concern for privacy, because it enhances fear, was expected to motivate a more detailed consideration of the phishing request and significantly reduce individual susceptibility. Here, individuals who were high in continuance commitment and felt compelled to complete tasks once it began were found to be significantly more likely to accept the friend request. Individuals who felt socially pressured to reciprocate a friend request by accepting it were also significantly more likely to accept it. Because individuals high in normative and continuance commitment have been shown to be particularly susceptible to peripheral route persuasion, it is likely that subjects in the study were peripherally processing the friend request. Thus, while concern for privacy had a dampening effect by reducing individuals’ susceptibility to level 1 attacks, automatic response patterns because of
habitual Facebook use followed by the perceived pressure of accepting a friend request because of individuals’ high normative and continuance commitment resulted in people making suboptimal decisions on social media.

In contrast to a level 1 attack, only individuals who are habitual Facebook users seem susceptible to level 2 information-request attacks. In social media platforms such as Facebook, messages sent within the platform show the picture of the sender. Thus, it is conceivable that habitual Facebook users see the picture, presume it is from a friend, and automatically respond to such requests without considering how they are connected with the person, how long they have known him, or who else is connected to that individual. Perhaps being connected to a large number of people makes it difficult to discern a friend from a stranger; or frequently interacting with the platform makes individuals more likely to overlook the nuances in the message that might reveal deception. Hence, habitual Facebook users appear significantly more likely to be inattentive and automatically provide the information requested by a phisher in a level 2 attack.

While Facebook habits appear to significantly predict deception likelihood to about the same extent in both attacks, neither the different types of attitudinal commitments nor individuals’ concern for privacy seem to matter when judging level 2 requests. The lack of significant effects was perhaps a reason why the regression explaining the level 2 request had relatively lower overall variances explained. Some cognitive scientists who espouse the dual-processing perspective (e.g., Chaiken & Eagly, 1989) distinguish between central route, elaborate processing and peripheral, heuristic processing, and consider them as two separate modes of information processing that could at times co-occur. Co-occurrence of information processing modes requires the availability of message elements as well as heuristic cues in the persuasive context, both of which are prevalent in level 2 social media requests rather than level 1 requests; in the latter case, the content cues are restricted by the preformatted friend-request template that Facebook provides. The different types of commitment examined in the present study are known to influence peripheral route persuasion (Workman, 2008), but the extent to which they explain central route persuasion and the extent to which their effects are attenuated by the potential co-occurrence of information processing modes remain unexplored and suggest another possible explanation for the relatively lower variance explained in the regressions for the level 2 information request relative to the level 1 request.

As one of the first studies to examine social media habits and its effects on victimization through phishing, the research necessitated a host of decisions, some of which limit the generalizability of these conclusions. First, because of the validity issues related to the behavioral measures culled from Facebook, the research relied on self-report measures of phishing likelihood. The findings of the study are limited by the validity of these measures. Second, the research did not utilize a control group of subjects because of the challenges of creating a legitimate request that was similar in all respects to those used by the phisher but from a genuine person that everyone in the sample knew and trusted to the same extent. The lack of a control group, however, makes it difficult to pinpoint the extent to which the stimulus influenced individual phishing susceptibility. Third, the focus of the study was limited to only social media deception. Thus, it remains unclear whether media habits are traits, that is, a habitual social media user is also likely to be a habitual e-mail user; or whether the consequences of social media habits are polymorphic, that is, individuals susceptible to social media scams are also likely to be susceptible to e-mail scams. Fourth, because of the relatively small sample size used in the current study the study could not test for the mediating role of social media habits on deception.

Another limitation stems from the convenience sample of undergraduate students that was used. Students are an important group for study because they are increasingly the targets of many phishing
attacks (RSA, 2010, February). They are also an important audience of social media users; after all, Facebook was developed and deployed first in college campuses and undergraduate students were its early adopters. Consequently, students tend to have more experience with social media, which might perhaps explain the relatively lower victimization rate evidenced in the current study when compared to other simulations that have utilized working adults (e.g., Prince, 2009) who are perhaps less familiar with the medium. Hence, although the findings of the study using student samples are important, their generalizability is restricted to similar audiences. Finally, the research focused exclusively on the ultimate predictors of online deception rather than the proximate information-processing factors. Thus, while habitual Facebook use makes individuals significantly more susceptible to phishing attacks on social media, the extent to which specific cues in the attack influence this victimization process remains unexplored.

What is necessary next is for research to combine these two perspectives and build an integrated model of phishing victimization. Such a model would provide conclusive evidence of the importance of cues in the phishing attack in triggering a response as against habitual patterns of responding that are enacted regardless of the message. In testing the model, the research could also utilize a control group and alternative measures of phishing susceptibility, which would help triangulate the results of the current study. Finally, future research needs to conclusively study the genesis of Facebook habits, particularly its mediating role on deception-likelihood, and the extent to which social media habits correlate with other media habits. This stream of research could also employ samples of adults and newer Facebook adopters to examine how habits emerge, how they differ across groups, and the extent to which susceptibility to deception in one medium influences likely victimization in another.

Overall the findings of research are noteworthy on two levels. At one level it identifies the antecedents to habitual Facebook usage. In this the research implicates frequent interactions with the platform, large number of friend connections, and the individuals’ inability to regulate their social media consumption as key predictors of habitual Facebook use. At the other level, the present research is the first to examine the determinately consequences of such habitual use in making individuals susceptible to level 1 and level 2 social media phishing attacks. The findings reveal that the automaticity of responding that stems from habitual Facebook use is the ultimate factor that determines the individuals’ susceptibility to social media phishing scams.

Notes
1 Six subjects provided partial response to some questions and were dropped from the analysis.
2 The behavioral data indicated that 33 subjects accepted the level 1 request and 19 responded to the level 2 request. Although the behavioral data correlated with the respective self-report measures, the behavioral measures were not utilized for the main analysis. During exit interviews, some subjects who accepted the friend-request indicated they had subsequently unfriended the phisher; some others mentioned they were planning to do the same; few others were about to accept the request but were waiting for their friend(s) to first accept the request. Likewise, some subjects indicated that they were about to accept the level 2 request but had not gotten down to it. A few subjects responded to the request but asked for clarification about the specifics of the internship and it was unclear whether to classify these subjects as phished or likely to be phished. Thus, the behavioral measures appeared to have limited validity and did not accurately reflect the variance in individuals’ likelihood of responding to the phishing requests.
3 In the regression predicting habit strength, the researcher replaced total number of Facebook friends with the number of close friends (mean = 31.85, s.d. = 21.83) and number of shared friends, i.e.,
friends from the same class ($mean = 21.83, s.d. = 23.86$), respectively, in order to explore whether another facet of individual social network better predicted habitual Facebook use. Neither the number of close friends ($\beta = 0.05, t = 0.92, p = .36$) nor the number of shared friends ($\beta = -0.07, t = -1.16, p = .25$) significantly predicted habit strength.

4 Statistically testing for the mediating role of Facebook habits on deception involves three steps (Baron & Kenny, 1986): regressions between Facebook habits and its three antecedents (which were tested in $H1 – 3$); regressions between Facebook habits and likelihood of victimization in a level 1 and level 2 attacks (tested in $H4a – b$); and regressions testing the unmediated relationship between the three antecedents of Facebook habits (size of social network, frequency of Facebook use, and deficient self-regulation) and the likelihood of victimization in a level 1 and level 2 attack. If the relationship between the antecedents of habits on individuals’ likelihood of deception were significantly reduced by the inclusion of Facebook habits in the regression, it would be considered a mediator. The significance in the reduction of variance is usually also confirmed using Sobel tests (Sobel, 1986). The regressions testing the direct unmediated effects of the antecedents of Facebook habits on likelihood of deception resulted in only frequency of Facebook use significantly predicting likelihood of accepting a level 1 friend-request ($\beta = 0.35, t = 3.49, p < .001; Sobel = 2.46, p < .05$) and level 2 information-request ($\beta = 0.25, t = 2.34, p < .05; Sobel = 2.23, p < .05$). On the face of it, these results would suggest that Facebook habits completely mediate the effect of only frequency of Facebook use on the likelihood of deception via social media phishing, and the effects of deficient self-regulation and size of social network on the likelihood of deception are not mediated by habits. Power issues stemming from relatively low sample sizes have, however, been known to influence the direct, unmediated effect computations (Shrout & Bolger, 2002). Hence, at this stage, given the relatively small size used in the current study, the question of whether Facebook habits significantly mediate the individuals’ likelihood of deception remains inconclusive.

References


**About the Author**

**Arun Vishwanath** is Associate Professor of Communication at the University at Buffalo. His research examines the role of microlevel, individual and macrolevel, societal factors in determining the utilization and mis-utilization of new communication technologies.

**Address:** Department of Communication, University at Buffalo, Buffalo, NY 14260. **E-mail:** avishy@buffalo.edu
Appendix

Screenshots of the Level 1 Friend-Request Profile and Level 2 Information-Request.

---

Jie How Tan

Hi,

I got internship from my friend and she’s looking for more people urgently!!! If you are interested to intern and would like more details, please reply with you Student ID No., UB Email User name, Date of Birth (dd/mm/yy) within the next three days.

Thanks.