A User-Centered Approach to Phishing Susceptibility: The role of a suspicious personality in protecting against phishing

Brynne Harrison
University at Buffalo
brynneha@buffalo.edu

Arun Vishwanath
University at Buffalo
avishy@buffalo.edu

Raghav Rao
University at Buffalo
mgmtrao@buffalo.edu

This research has been funded by NSF under grant #1227353.

Abstract

Generalized communicative suspicion (GCS) has been implicated in the deception literature as a trait that causes individuals to believe they can accurately detect deception in face-to-face settings. Separately, the online deception literature has implicated users’ heuristic processing as the reason for them failing to recognize deception and falling prey to cybercrimes like phishing attacks. Such online deception work, however, has yet to explore how GCS might affect individual abilities to detect deception in a mediated context. The current work connects these two streams of research by introducing information insufficiency as a mediator between GCS and processing and extending it to the phishing context. We find that high GCS increases uncertainty and leads to a desire for more information before making a judgment. Desiring more information leads to systematically processing available information and more accurate phishing deception detection.

1. Introduction

Phishing is a social engineering attack where a perpetrator, a phisher, sends a legitimate looking email with the goal of persuading a user to click on a link or an attachment in the email [16]. Clicking opens back doors to the user’s device or networks that are then used to surreptitiously gain access to otherwise private information. Such attacks have become increasingly common. The Anti-Phishing Working Group documented 125,215 reported attacks worldwide in the first three months of 2014, which amounts to almost 1,400 attacks daily—and these are merely the ones reported [1]. In fact, many major breaches in 2014 such as the Apple iCloud hack and the infamous Sony Pictures hacks have been attributed to phishing attacks [14, 15]. Not surprisingly, phishing has become the vector of choice among cyber criminals, making the need to study why people fall for such attacks pressing and urgent.

The current research on phishing has extended the Heuristic Systematic Model (HSM) of information processing and found that the type of cognitive processing mode individuals’ employ predicts whether they fall for the attack [17]. This line of work has linked cognitive processing to the amount of suspicion an email arouses. Separately, research on risk communication has connected cognitive processing to information insufficiency—perceptions of the adequacy of information [8]. Yet another line of research on interpersonal deception-detection has connected suspicion to an individual trait termed Generalized Communicative Suspicion (GCS)—a tendency to believe people are generally dishonest or deserving of wariness [11].

These three lines of research, however, remain separate, with research on phishing focusing on suspicion and cognitive processing, research on information sufficiency focusing on health-related risk communication, and GCS focusing on interpersonal lie-detection. The current paper combines these lines of inquiry and extends it to the email-based phishing domain with the aim of better understanding the mechanisms through which users base their behavioral decisions. We begin by extending GCS to the online domain by first exploring whether individuals high in GCS perceive a request for information face-to-face to be analogous to a request for information via email. We then consider how GCS is related to confidence in one’s ability to detect a deceptive email. Next, we examine whether GCS increases the threshold amount of information (i.e., perceived information insufficiency) needed when examining emails. Finally, we connect information insufficiency to the mode of cognitive processing people employ and its effects on trust of a phishing email.
The paper begins by explicating GCS and its relationships to deception-detection in the email context and its relationships to information insufficiency. Following this, we provide the rationale connecting information insufficiency to cognitive processing and trust.

2. Generalized Communicative Suspicion

Research on interpersonal lie-detection evidences a tendency among individuals to be suspicious about the intent of others. This preconception creates an expectancy of deceit and negatively influences subsequent judgments about the veracity of a sender. Levene and McCornak [10] identified this enduring personality trait among individuals and termed it Generalized Communicative Suspicion (GCS). This trait has been linked to the increased tendency of experts, such as police officers, in making deceptive judgments [12] and has even been shown to decrease the accuracy of such experts in detecting interpersonal deception [4]. Much of this work precedes the widespread use of the Internet, and therefore the extent to which GCS influences the outcome of email-based phishing remains unexplored. Furthermore, the underlying mechanism through which GCS influences judgment itself remains unclear.

Because personality traits are not contextually bound, we expect individuals high in GCS to perceive requests for information via email, such as a phishing email, as analogous to a face-to-face information request. Similar to other personality traits [13], for it to endure, GCS must be reinforced by life events that justify and validate its continued manifestation. Although leading to a biased interpretation of others, for people with high GCS, the variable reinforcement from life events, where the individual successfully avoided a negative outcome due to such beliefs, could overtime lead to a heightened feeling of prescience in the ability to detect deception. We thus expect GCS to influence a person's confidence or efficacy in detecting a deceptive person. Due to the fact that GCS should remain consistent regardless of context, we propose the following hypotheses:

H1a. An individual with high GCS is likely to perceive an information request in an email as analogous to an information request face-to-face.

H1b. An individual with high GCS is likely to have high self-efficacy in detecting a deceptive email.

3. Information Insufficiency

People with high GCS tend to be suspicious about others [10, 11]. This suspicion is likely to increase their uncertainty or anxiety when dealing with people. Reducing this uncertainty would require more information [3]. In other words, the threshold amount of information that individuals high in GCS need would be potentially higher.

Separately, the risk communication literature has introduced the concept of information insufficiency—the perceived gap between the amount of information present and the amount of information required [8]. While information insufficiency has been connected to risk information processing, the extant literature locates its antecedents among external factors such as subjective norms and social influence [8]. The internal, individual factors that predict information insufficiency, however, remain unexplored. In the current study, we connect information insufficiency to trait GCS and hypothesize that individuals high in GCS are likely to suffer greater uncertainty and anxiety when evaluating emails and are thereby likely to perceive a larger gap between the information available and the information needed to make a decision regarding the deceptive nature of the email.

H2. An individual with high GCS is likely to perceive higher levels of information insufficiency.

4. Information Processing: The Heuristic Systematic Model

The perceived need for information in the decision context, or the perception of information insufficiency, defines the information processing mode employed in that context [5]. The cognitive processing literature distinguishes between two modes of information processing. One, termed systematic processing, involves a detailed assessment of available information and connecting it to prior knowledge. The other, heuristic processing, entails the use of cognitive shortcuts (heuristics) that are triggered by cues in the context.

Heuristic processing is the dominant processing strategy because people are mostly motivated by cognitive efficiency. Systematic processing is thus seldom employed, and even when used is biased by prior heuristic processing. Heuristic processing is cognitively efficient because it arrives at a decision by utilizing minimal cognitive and informational resources. For instance, it is quicker to judge the quality of an argument based on the length of the text
using the simple “length equals strength” heuristic, rather than reading the entire message. Doing so, however, would lead to misapprehensions about the true quality of the narrative. Hence, the expectation is that individuals who feel that the amount of information available is adequate are likely to heuristically process it. In contrast, individuals who feel the amount of information provided is insufficient (perhaps motivated by the aforementioned suspicion trait) would be expected to process information more carefully and perhaps even seek out more information before feeling as though there is a sufficient amount of information to make a decision regarding the veracity of the email.

H3a. The lower the perceived information insufficiency the higher the likelihood of heuristic processing.

H3b. The higher the perceived information insufficiency the higher the likelihood of systematic processing.

5. Information processing outcome

A significant body of research has implicated the mode of cognitive processing individuals employ as a determinant of their likelihood of falling prey to a phishing attack where higher levels of heuristic processing led to a higher likelihood of victimization [16,18]. Other research has shown that online users who rely on heuristic cues on a webpage tend to trust the website [9]. Emerging research points to phishing emails, in a bid to appear authentic, also imbibing heuristic cues in them [7]. If individuals rely on these cues, which they are likely to because they tend to eschew effortful processing, they are more likely to judge phishing emails as truthful and fall victim to such attacks. If, on the other hand, individuals elaborate on the page content (via systematic processing), perhaps because of higher levels of trait GCS, they are less likely to trust and therefore fall prey to the attack. Following this logic, we expect heuristic processing to lead to the suboptimal outcome of trusting the phishing email and eventually falling for the deception. This rationale leads to the following hypotheses:

H4a. Higher levels of systematic processing will lead to decreased trust in a phishing email.

H4b. Higher levels of heuristic processing will lead to increased trust in a phishing email.

In summary, the paper hypothesizes a link between trait GCS and information insufficiency, information insufficiency and cognitive processing, and between processing and the amount of trust in a phishing email. Figure 1 presents a visual of the research hypotheses.

![Figure 1. A model of GCS in an email phishing context](image)

6. Methodology

The hypotheses were tested using an experiment in which undergraduate students from a large northeastern public university were targeted in a real phishing attack. We chose college students because they are often the targets of phishing attacks, making students an important population for our study [2]. Additionally, the focus of the study was on internal validity, which is more easily achieved using college students.

To simulate a real phishing attack, we mimicked an attack that was recently discovered by the university information security office. We created a free email account with the university’s name: xxx@gmail.com and used it to send a phishing email to the students asking them to verify their email account by clicking on a link in the email. The attack was deployed using an email marketing software that allowed for tracking of individuals who opened and/or clicked on the link provided in the email. Many phishers utilize such hyperlinks in the email that, when clicked, immediately deploy malware and open virtual back doors—successfully phishing a user. Clicking this link directed subjects to a web survey where they were debriefed and asked the reasons for their actions using a battery of measures derived from prior research.

A total of 200 subjects were sent the phishing email. Subjects who did not click on the phishing link were contacted separately and asked to complete the follow-up survey. Only 192 subjects who recalled seeing the phishing email (through a manipulation check question within the web survey) and correctly identified the email were retained for the study.

7. Measures
Most of the measures were obtained from prior research; some item wordings were changed to fit the context of the study.

7.1. Face-to-face information request as analogous to an email information request

A single item measured whether subjects perceived a face-to-face information request as analogous to an information request via email: “When compared to a request for information that comes face-to-face, a request for information via email is...”. Subjects’ responses ranged from 1—5, with 1 = very different and 5 = very similar.

7.2. Efficacy in detecting a deceptive email

A single-item asked respondents: “How well can you judge whether an email is trustworthy or deceitful?” Subjects’ responses ranged from 1—7, with 1 = with no confidence at all and 7 = very confidently.

7.3. Generalized Communicative Suspicion (GCS)

GCS was measured using five-items derived from Levine and McCornack [10] reworded to measure generalized suspicion of email-based communication. Sample items read: “Anyone who trusts someone else’s emails is asking for trouble”; “People seldom lie to me on email”; “I often feel as if people are not completely truthful via email”. Each item was scored on a 1 (strongly disagree)—5 (strongly agree) response scale, and the overall scale achieved an alpha reliability of 0.76.

7.4. Information insufficiency

Following the approach used in prior research examining information insufficiency [8], one item asked, “How much did you really need to know in order to make your decision about whether or not to respond to the phishing email?” Subjects were asked to provide a number from 0 (little to none)—100 (as much as possible).

7.5. Heuristic processing

Heuristic processing was measured by adapting a 6-item scale used in prior research [6]. Sample items read: “I skimmed through the email”; “I briefly looked at the sender/source of the email”; “I disregarded the email message content”. Each item was scored on a 1 (strongly disagree)—5 (strongly agree) response scale. The overall scale achieved an alpha reliability of 0.72.

7.6. Systematic processing

Systematic processing was measured using a 7-item scale adapted from prior research [17]. Sample items read: “I thought about the action I took based on what I saw in the email”; “I found myself making connections between the email’s request and what I have heard about emails requesting such information”; “I spent some time thinking about the request before I made my decision”. Each item was scored on a 1 (strongly disagree)—5 (strongly agree) response scale. The overall scale achieved an alpha reliability of 0.79.

7.7. Email trust

A single-item scored from 1 (strongly disagree)—5 (strongly agree) measured email trust by asking respondents the extent to which they trusted the email.

8. Analysis and Results

Table 1 presents the means and standard deviations of the measures in the study.

Table 1. Means and standard deviations of measures

<table>
<thead>
<tr>
<th>Measures</th>
<th>Mean</th>
<th>Std. dev</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face-to-face information request as analogous to an email information request</td>
<td>4.24</td>
<td>0.80</td>
</tr>
<tr>
<td>Efficacy in detecting a deceptive email</td>
<td>4.03</td>
<td>1.43</td>
</tr>
<tr>
<td>GCS</td>
<td>2.89</td>
<td>0.67</td>
</tr>
<tr>
<td>Information insufficiency</td>
<td>54.42</td>
<td>28.19</td>
</tr>
<tr>
<td>Heuristic processing</td>
<td>3.21</td>
<td>0.82</td>
</tr>
</tbody>
</table>
individuals to differ in individuals who have higher susceptibility. As a personality trait GCS is a robust factor in processing information insufficiency when faced with a deceptive email. However, the lack of information to make a decision when faced with a deceptive email was significant: $F(2, 191) = 9.12, p < .05, R^2 = .08$. As expected, when systematic processing was high subjects were significantly less likely ($\beta = -.27, p < .05$) to trust the phishing email. When heuristic processing was high subjects were significantly more likely ($\beta = 0.13, p < .10$) to trust the phishing email.

9. Discussion

The current research brings together two previously separate lines of research to better understand why people fall victim to phishing attacks via email. It combines three lines of research on interpersonal lie detection, risk communication and phishing email victimization. The data were in support of the overall premise of the study. It appears that individuals who have higher generalized communicative suspicion have higher efficacy in detecting deceptive emails than individuals with low generalized communicative suspicion. Individuals with high GCS suffer higher levels of uncertainty and therefore tend to perceive a lack of information to make a decision when faced with a deceptive email. In other words, they perceive a larger gap between the amount of information present in the email and the amount of information necessary to make a decision regarding the veracity of the email. These differences in perceptions of information insufficiency lead individuals to differ in how they subsequently process the information contained in the email. Subjects with high GCS and therefore high perceptions of information insufficiency were more likely to process information systematically by connecting it to existing knowledge and prior experiences. Contrarily, subjects with low GCS perceived low levels on information insufficiency and therefore were significantly more likely to process the email information by using mental shortcuts and heuristics. Finally, the systematic processing of the email was found to significantly reduce trust in the phish email, while the heuristic processing of the email was found to significantly increase trust of the phish.

Thus, it appears that GCS plays a rather important albeit indirect role in determining individual phishing susceptibility. As a personality trait GCS is a robust factor in processing information insufficiency when faced with a deceptive email. However, the lack of information to make a decision when faced with a deceptive email was significant: $F(2, 191) = 9.12, p < .05, R^2 = .08$. As expected, when systematic processing was high subjects were significantly less likely ($\beta = -.27, p < .05$) to trust the phishing email. When heuristic processing was high subjects were significantly more likely ($\beta = 0.13, p < .10$) to trust the phishing email.

9. Discussion

The current research brings together two previously separate lines of research to better understand why people fall victim to phishing attacks via email. It combines three lines of research on interpersonal lie detection, risk communication and phishing email victimization. The data were in support of the overall premise of the study. It appears that individuals who have higher generalized communicative suspicion have higher efficacy in detecting deceptive emails than individuals with low generalized communicative suspicion. Individuals with high GCS suffer higher levels of uncertainty and therefore tend to perceive a lack of information to make a decision when faced with a deceptive email. In other words, they perceive a larger gap between the amount of information present in the email and the amount of information necessary to make a decision regarding the veracity of the email. These differences in perceptions of information insufficiency lead individuals to differ in how they subsequently process the information contained in the email. Subjects with high GCS and therefore high perceptions of information insufficiency were more likely to process information systematically by connecting it to existing knowledge and prior experiences. Contrarily, subjects with low GCS perceived low levels on information insufficiency and therefore were significantly more likely to process the email information by using mental shortcuts and heuristics. Finally, the systematic processing of the email was found to significantly reduce trust in the phish email, while the heuristic processing of the email was found to significantly increase trust of the phish.

Thus, it appears that GCS plays a rather important albeit indirect role in determining individual phishing susceptibility. As a personality trait GCS is a robust factor in processing information insufficiency when faced with a deceptive email. However, the lack of information to make a decision when faced with a deceptive email was significant: $F(2, 191) = 9.12, p < .05, R^2 = .08$. As expected, when systematic processing was high subjects were significantly less likely ($\beta = -.27, p < .05$) to trust the phishing email. When heuristic processing was high subjects were significantly more likely ($\beta = 0.13, p < .10$) to trust the phishing email.

9. Discussion

The current research brings together two previously separate lines of research to better understand why people fall victim to phishing attacks via email. It combines three lines of research on interpersonal lie detection, risk communication and phishing email victimization. The data were in support of the overall premise of the study. It appears that individuals who have higher generalized communicative suspicion have higher efficacy in detecting deceptive emails than individuals with low generalized communicative suspicion. Individuals with high GCS suffer higher levels of uncertainty and therefore tend to perceive a lack of information to make a decision when faced with a deceptive email. In other words, they perceive a larger gap between the amount of information present in the email and the amount of information necessary to make a decision regarding the veracity of the email. These differences in perceptions of information insufficiency lead individuals to differ in how they subsequently process the information contained in the email. Subjects with high GCS and therefore high perceptions of information insufficiency were more likely to process information systematically by connecting it to existing knowledge and prior experiences. Contrarily, subjects with low GCS perceived low levels on information insufficiency and therefore were significantly more likely to process the email information by using mental shortcuts and heuristics. Finally, the systematic processing of the email was found to significantly reduce trust in the phish email, while the heuristic processing of the email was found to significantly increase trust of the phish.

Thus, it appears that GCS plays a rather important albeit indirect role in determining individual phishing susceptibility. As a personality trait GCS is a robust factor in processing information insufficiency when faced with a deceptive email. However, the lack of information to make a decision when faced with a deceptive email was significant: $F(2, 191) = 9.12, p < .05, R^2 = .08$. As expected, when systematic processing was high subjects were significantly less likely ($\beta = -.27, p < .05$) to trust the phishing email. When heuristic processing was high subjects were significantly more likely ($\beta = 0.13, p < .10$) to trust the phishing email.

9. Discussion

The current research brings together two previously separate lines of research to better understand why people fall victim to phishing attacks via email. It combines three lines of research on interpersonal lie detection, risk communication and phishing email victimization. The data were in support of the overall premise of the study. It appears that individuals who have higher generalized communicative suspicion have higher efficacy in detecting deceptive emails than individuals with low generalized communicative suspicion. Individuals with high GCS suffer higher levels of uncertainty and therefore tend to perceive a lack of information to make a decision when faced with a deceptive email. In other words, they perceive a larger gap between the amount of information present in the email and the amount of information necessary to make a decision regarding the veracity of the email. These differences in perceptions of information insufficiency lead individuals to differ in how they subsequently process the information contained in the email. Subjects with high GCS and therefore high perceptions of information insufficiency were more likely to process information systematically by connecting it to existing knowledge and prior experiences. Contrarily, subjects with low GCS perceived low levels on information insufficiency and therefore were significantly more likely to process the email information by using mental shortcuts and heuristics. Finally, the systematic processing of the email was found to significantly reduce trust in the phish email, while the heuristic processing of the email was found to significantly increase trust of the phish.

Thus, it appears that GCS plays a rather important albeit indirect role in determining individual phishing susceptibility. As a personality trait GCS is a robust factor in processing information insufficiency when faced with a deceptive email. However, the lack of information to make a decision when faced with a deceptive email was significant: $F(2, 191) = 9.12, p < .05, R^2 = .08$. As expected, when systematic processing was high subjects were significantly less likely ($\beta = -.27, p < .05$) to trust the phishing email. When heuristic processing was high subjects were significantly more likely ($\beta = 0.13, p < .10$) to trust the phishing email.

9. Discussion

The current research brings together two previously separate lines of research to better understand why people fall victim to phishing attacks via email. It combines three lines of research on interpersonal lie detection, risk communication and phishing email victimization. The data were in support of the overall premise of the study. It appears that individuals who have higher generalized communicative suspicion have higher efficacy in detecting deceptive emails than individuals with low generalized communicative suspicion. Individuals with high GCS suffer higher levels of uncertainty and therefore tend to perceive a lack of information to make a decision when faced with a deceptive email. In other words, they perceive a larger gap between the amount of information present in the email and the amount of information necessary to make a decision regarding the veracity of the email. These differences in perceptions of information insufficiency lead individuals to differ in how they subsequently process the information contained in the email. Subjects with high GCS and therefore high perceptions of information insufficiency were more likely to process information systematically by connecting it to existing knowledge and prior experiences. Contrarily, subjects with low GCS perceived low levels on information insufficiency and therefore were significantly more likely to process the email information by using mental shortcuts and heuristics. Finally, the systematic processing of the email was found to significantly reduce trust in the phish email, while the heuristic processing of the email was found to significantly increase trust of the phish.

Thus, it appears that GCS plays a rather important albeit indirect role in determining individual phishing susceptibility. As a personality trait GCS is a robust factor in processing information insufficiency when faced with a deceptive email. However, the lack of information to make a decision when faced with a deceptive email was significant: $F(2, 191) = 9.12, p < .05, R^2 = .08$. As expected, when systematic processing was high subjects were significantly less likely ($\beta = -.27, p < .05$) to trust the phishing email. When heuristic processing was high subjects were significantly more likely ($\beta = 0.13, p < .10$) to trust the phishing email.
predictor, better than efficacy, which tends to be contextually bound. GCS influences how much information one feels is necessary when faced with a mediated decision. This, in turn, influences how many processing resources one is willing to commit, which ultimately predicts the outcome of a phishing attack. This paper is the first to connect the personality trait of GCS with cognitive processing. While research has connected GCS to suspicion and the lack of trust in people, none have explicated the underlying mechanism of processing through which this occurs. Connecting GCS to trust through the mechanism of information insufficiency and cognitive processing is an important contribution of the current piece.

Given its antecedent role, GCS could serve as a measurable marker of the people most likely to fall victim to a phishing attack. Because individuals with low GCS are more likely to process heuristically, educational and anti-phishing training interventions could be targeted at them. Conversely, since people with high GCS tend to be less trusting of emails, they are more likely to net many false positives when they wrongly mistrust a legitimate email. Over time, this could lead to inefficient email use, which could be mitigated by targeting email deception detection training and education at such individuals to improve their detection accuracy. In this way, rather than trying to improve cognitive effort among all individuals, we can create targeted interventions based on the specific personality profile of the likely victim. This could help improve the overall effectiveness of extant anti-phishing training and education.

While the study findings are noteworthy, the following limitations need to be taken into account. First, the study used a sample of university students. This ensured internal validity by allowing experience and attitude toward technology to remain relatively consistent across the sample. Students also tend to be the targets of many phishing attacks with most universities in the United States dedicating resources toward protecting students. That said, it is likely that the general adult population might vary in GCS and its related outcomes. The extent to which this is the case remains unknown and a topic for future research. Second, some of the measures used in the study were single items; others, such as the cognitive processing measures, had lower reliability. Although this is another limitation of the study, it is important to remember that low reliability makes it harder to find significant relationships, making the significant relationships netted in the current study particularly salient. Finally, the research focused on email trust as the outcome measure rather than victimization rates. This was because trust could be measured using an interval scale across the victimized and non-victimised subjects and because victimization could not be reliably ascertained within the study set-up. Although trust is often utilized as a valid outcome by researchers interested in technology use and cognitive processing (e.g., [9]), the extent to which it predicts actual phishing victimization is another topic for future exploration.

In closing, much of the work on GCS precedes the Internet and focuses on interpersonal deception detection. This work has yet to examine whether GCS influences phishing-based victimization. Our paper melds multiple lines of research in cognitive processing and email phishing and explicates the underlying mechanism of information insufficiency through which GCS influences phishing victimization. In doing so, the paper provides theoretical insights into why people fall victim to phishing and practical guidance for policymakers on how to better target interventions to reduce individual susceptibility.

10. References


[7] Harrison, Brynne., et al. Examining the impact of presence on individual phishing victimization. (January,
2015) Presented at the annual meeting of 48th Hawaii International Conference on System Sciences.


