Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards

Matthew Canham¹, Clay Posey¹, Delainey Strickland¹, and Michael Constantino¹

Abstract
Organizational cybersecurity efforts depend largely on the employees who reside within organizational walls. These individuals are central to the effectiveness of organizational actions to protect sensitive assets, and research has shown that they can be detrimental (e.g., sabotage and computer abuse) as well as beneficial (e.g., protective motivated behaviors) to their organizations. One major context where employees affect their organizations is phishing via email systems, which is a common attack vector used by external actors to penetrate organizational networks, steal employee credentials, and create other forms of harm. In analyzing the behavior of more than 6,000 employees at a large university in the Southeast United States during 20 mock phishing campaigns over a 19-month period, this research effort makes several contributions. First, employees’ negative behaviors like clicking links and then entering data are evaluated alongside the positive behaviors of reporting the suspected phishing attempts to the proper organizational representatives. The analysis displays evidence of both repeat clicker and repeat reporter phenomena and their frequency and Pareto distributions across the study time frame. Second, we find that employees can be categorized according to one of the four unique clusters with respect to their behavioral responses to phishing attacks—“Gaffes,” “Beacons,” “Spectators,” and “Gushers.” While each of the clusters exhibits some level of phishing failures and reports, significant variation exists among the employee classifications. Our findings are helpful in driving a new and more holistic stream of research in the realm of all forms of employee responses to phishing attacks, and we provide avenues for such future research.

Keywords
phishing, behavioral security, cybersecurity, organizational cybersecurity, longitudinal experiment, repeat clickers, repeat reporters

Introduction
Modern organizations face significant issues from threats to sensitive data, information, and systems. To help combat these ever-evolving issues, global spending on information security was estimated to be US$101.4 billion (Gartner, 2018) in their efforts to protect and defend organizational assets in 2017. This figure is estimated at US$123 billion in 2020 (Columbus, 2020) and is expected to total more than US$1 trillion from 2017 to 2021 collectively (Morgan, 2019). Unfortunately, successful cyberattacks have abounded despite these efforts and show little sign of slowing.

One prominent facet of organizational cybersecurity is the impact that internal employees have on their respective organizations’ efforts. Research showing how employees can influence the effectiveness of their respective organizations’ cybersecurity efforts is well documented (Crossler et al., 2013; Warkentin & Willison, 2009). In fact, a substantial body of literature has examined the detrimental impacts of employee behavior like computer abuse (Lee et al., 2004; Straub & Nance, 1990; Willison & Warkentin, 2013), non-compliance with information security policies (ISPs; Gwebu et al., 2020; Kajtazi et al., 2018; Lowry & Moody, 2015), and shadow IT utilization (Silic & Back, 2014; Zimmermann & Rentrop, 2014). Conversely, research has also shown how employees can act as “protective stewards” of sensitive organizational assets as they actively attempt to defend their organizations from threats (Burns et al., 2018; Posey et al., 2013, 2015). Thus, employees can have both negative and positive ramifications in the organizational cybersecurity domain.

¹University of Central Florida, Orlando, USA

Corresponding Author:
Clay Posey, University of Central Florida, P.O. Box 161400, Orlando, FL 32816-2368, USA.
Email: clay.posey@ucf.edu
As a specific context, email represents one of the most utilized contexts by which attackers gain entry to sensitive organizational systems, obtain confidential data, and negatively influence organizations. In fact, email was the overwhelming source of malware infections in 2018, accounting for 94% of all infections (Verizon, 2019). It is also the entry point for many of the most expensive ransomware attacks highlighted in the media today. While research on email-based attacks (most prominently, attacks known as online phishing) that attempt to trick individuals into performing an action that leads to personal or organizational harm) has existed for some time now, little is known about these attack mechanisms beyond the individuals’ characteristics that make them more susceptible to email-based attacks (e.g., Canfield et al., 2016; Dhamija et al., 2006; Moody et al., 2017; Wang et al., 2012; Workman, 2008) and the factors associated with these attacks that make them more likely to be successful and less likely to be detected (e.g., Abdelhamid et al., 2014; Khonji et al., 2013). Specifically, other than initial and recent industry reports from phishing platform providers (Proofpoint, 2020), we have limited knowledge about all types of responses—both negative and positive—when employees receive phishing threats through email. Given this gap, we explore the following research question:

**Research Question (RQ):** Which general categories of organizational employees exist with respect to their behaviors—both negative and positive—following online phishing attacks?

To answer this question and to better understand how employees react to online phishing attacks in a more holistic manner, we collected and analyzed data from 20 mock phishing campaigns, which spanned 19 months and included more than 6,000 employees at a large university in the Southeastern United States. Due to their size and scope, our efforts are among the most extensive academic research activities examining employee behaviors in response to email phishing attacks and are among the first to examine negative and positive employee behaviors in simultaneous fashion. In addition, we are able to shed light on groups of employees whose repeat phishing-response actions can adversely affect or safeguard their organizations. Our findings show that employees generally fall into one of the four unique clusters based upon whether they clicked, responded to, entered data after, and/or reported the perceived attack to the appropriate organizational authorities. We also find evidence that the number of repeat failures, clickers, and reporters follow a Pareto distribution. Furthermore, we find that 6% of our sample (i.e., the “repeat clickers,” or those who failed more than three phishing campaigns) accounted for 29% of the failures, whereas 33% of our sample (i.e., the “protective stewards,” or those who reported more than three phishing campaigns) accounted for 92% of all reports. About half of the sample never failed or never reported the phishing attacks. Our efforts thus extend research on employees’ responses to online social engineering tactics, and we provide several recommendations for organizational leaders as they attempt to become more knowledgeable about their employees.

**Background**

Human users represent the largest attack surface in most socio-technical systems (Sebescen & Vitak, 2017). Regardless of how secure designers attempt to build a system, limitations in human information processing and subsequent (in)action often lead to weaknesses in even the strongest systems. Effective strategies to deal with the risks arising from these insiders represent a significant research opportunity in information security (Crossler et al., 2013). Malicious cyber threat actors are acutely aware of this vulnerability and deliberately work to exploit it by employing social engineering techniques to influence individuals inside the organizations they target. Phishing is one of the most common remote online social engineering techniques employed to this end. Within the context of this discussion, we borrow from others (e.g., El Aassal & Verma, 2019) and define phishing generally as an attempt via email to influence, manipulate, or otherwise exploit individuals to get them to perform a behavior that results in negative outcomes for the individuals and/or the individuals’ respective organizations. Many of the highest profile cyber breaches (e.g., RSA, AT&T, and the Ukrainian power grid) were enabled via the phishing of employees (Edwards et al., 2017).

Numerous “flavors” of email phishing attacks exist (e.g., Gupta et al., 2016). For example, one common tactic is to trick a user into downloading and installing malware. This attack is often operationalized through an email attachment or link that appears relevant to a user’s organizational or personal life (e.g., payment invoice, order tracking, tax documents). Once installed on the user’s device, the infection can then attempt to propagate throughout the organizational systems.

Another leading method used in phishing attacks permits attackers to gain a user’s login credentials. For email credentials, once they have been retrieved by the threat actor, she or he will then be able to send additional phishing emails to others within the organization using the legitimate account of the user targeted in the original scam—an attack known as “lateral phishing” (Ashford, 2019; Hadnagy & Fincher, 2015). This technique means that any compromised email account can pose a significant threat to the entire organization, regardless of the access level of the employee associated with the compromised account. Such attacks can therefore escalate in severity as “low-access” accounts are then used to manipulate follow-on targets who might have access to more sensitive organizational information and/or systems. (Hadnagy & Fincher, 2015).
Organizational Remedies

Technical approach—Automated filtering. To help limit the number of phishing attacks to which employees are possibly exposed, many organizations employ automated filtering mechanisms within the email system. The goal of the filtering, then, is to prevent suspicious email message from reaching an employee’s inbox. However, such an approach has several shortcomings. First, automated filtering fails to catch all the malicious emails directed toward an individual, and the few that make their way through the filters might in fact make the targeted individual more susceptible because of their low numbers—a phenomenon termed the “prevalence paradox” (Sawyer & Hancock, 2018). In fact, while the total number of overall phishing attacks has declined in recent years, the proportion of successful attacks has increased (Symantec, 2019).

Second, automated filtering mechanisms often rely on simple rules such as disabling links, preventing the downloading of attachments, or flagging accounts that do not originate from within the target’s organization. This approach is partially based on the assumption that threat actors are constrained to manipulating users to follow one of these actions. However, many malicious emails seek to manipulate users to take actions that are consistent with their normal duties but are in fact unauthorized. An example of these types of emails is known as business email compromise (BEC) which attempts to manipulate a target into sending a wire transfer to an unauthorized recipient (FBI, 2015). These emails usually focus on an employee who is authorized to make wire transfers and thus are behaving in ways that are within their normal operations and capacity.

Finally, automated filtering mechanisms and other technologies fail to alert organizations when employees receive social engineering attacks via out-of-band channels (i.e., communication through a medium other than email), which can be just as damaging as emails directed at an organizational email because these create the potential for both intentional and unintentional insider threats. For example, in February 2019, the U.S. Department of Justice filed an indictment against four Iranian hackers for their role in attempting to befriend and then compromise the social media accounts of several U.S. Air Force intelligence specialists (Marks, 2019). These out-of-band communications will not be detected by automated email phishing detection applications because the organization has no control or influence over the outside platforms.

As these examples illustrate, the sole reliance on automated mechanisms to prevent employees from becoming victims of phishing provides at best a false sense of security, and worse, might in fact make an organization more vulnerable to these attacks. For the reasons outlined above, it is critical to improve scientific understanding of the human vulnerabilities to phishing attacks to provide a more solid basis upon which to build human-centric defenses.

Nontechnical approach—Security education, training, and awareness (SETA) programs. The major nontechnical approach used in organizational cybersecurity is the design and implementation of SETA programs for employees (Y. Chen et al., 2015; D’Arcy & Hovav, 2009; Yoo et al., 2018). SETA programs have the goals of making employees aware of the various cyber threats that affect their organizations, provide information as to how an employee can perform his or her daily tasks securely against those risks, and other important information. In general, these programs are an integral part in the development of an overall security culture (Y. Chen et al., 2015), build users’ perceptions of the desirability and efficacy of organizational cybersecurity efforts (Burns et al., 2018), encourage employees to comply with organizational ISPs (Barlow et al., 2018), and help employees become more aware of targeted phishing attacks (Burns et al., 2019), among other important outcomes.

One major element utilized by security professionals in SETA programs to help inoculate employees against phishing susceptibility is simulated phishing email campaigns (Jansson & von Solms, 2013; Mäses et al., 2019). Several companies have begun offering software platforms that allow security professionals to design and send simulated phishing emails to the users in their organizations. Examples of these commercial phishing simulation platforms would be PhishMe (now Cofense), Wombat Security Awareness, Proofpoint, and KnowBe4. These simulated phishing campaigns can be an effective method of preparing users to handle real phishing attacks as the campaigns mimic attacks that have successfully and adversely affected other organizations (Carella et al., 2017).

Employee Behavior

When faced with a phishing attack, simulated or not, employees can take one or more actions. From a negative standpoint, users can click on hyperlinks embedded in the phishing email, enter data on the site to which the clicked hyperlink directed them, and/or reply to the sender, among others. One interesting group of employees within this perspective is termed repeat clickers. These individuals represent employees who continually fall victim to phishing attacks, regardless of message content or environmental influences (Canham et al., 2019). In an analysis of more than 8 million simulated phishing emails, “67% of employees who respond to simulated phishing attacks are repeat victims and therefore are likely to respond to phishing emails more than once” (PhishMe, 2015). Thus, while some in the general population might fall for phishing attacks occasionally, there are others whose susceptibility is much higher than the average.

Despite the need to better understand these repeat offenders (Proofpoint, 2020), research on the matter is surprisingly limited. For example, the few studies that have examined repeat victimization have considered situations with fewer than five trials only (Caputo et al., 2013; Li et al., 2020) or
have not reported differences between repeat and nonrepeat victims (Workman, 2008). A study of 1,359 employees from a Washington, DC, organization was sent three simulated phishing emails over a 90-day period. The researchers found that approximately 11% of the participants clicked the embedded hyperlink in all three emails, while approximately 22% did not click the link in a single simulated phishing email (Caputo et al., 2013; Li et al., 2020). Another study of nearly 7,000 employees at a major university looked at responses to simulated phishing emails across three campaigns over 3 weeks. These researchers found that employees who clicked an embedded hyperlink in the previous week’s campaign were more likely to click the link on the next week’s campaign (Caputo et al., 2013; Li et al., 2020). This effect could be due to individual differences in phishing-detection overconfidence from previous campaigns (R. Chen et al., 2020). Correlations between phishing and voice-based social engineering (i.e., vishing) were examined in another study that exposed 588 employees to 12 simulated social engineering attacks (six phishing and six vishing) over a 6-month period. While this study reported individual differences in phishing susceptibility, it did not report the numbers or proportions, nor were any individual differences between repeat victims and nonrepeat victims reported (Workman, 2008).

Opposite of individuals who repeatedly fall victim to phishing attacks are those who are actively seeking out details to determine whether an email is phishing and desire to help protect the organization and their fellow colleagues from those threats. Such employees are akin to the “protective stewards” found in other research whose actions help assist rather than detract from organizational cybersecurity efforts (Burns et al., 2018; Posey et al., 2013). When believing they have detected deception, employees have the option of ignoring the email or reporting the email as a suspected attack. When reporting, some organizational security departments ask users to forward the emails to their representatives so that they can inspect the message for possible phishing activity, and others have activated technological solutions that make it easier for user reports of suspected phishing attacks to take place. For example, the inclusion of report buttons within email interfaces greatly simplifies this task by quarantining the email, alerting the security staff of the potential threat, and releasing the email back to the employee if the security staff deems it a false alarm. Despite these employees’ potential to alert organizational security staff of harmful social engineering activities on a continuing basis, we are among the first to examine this detection-notification cycle in detail.

Employee behaviors following phishing threats, both negative and positive, deserve more attention. Research examining employees who are able to detect deception in phishing emails has been conducted but does not always examine actual employee behaviors following the detection (e.g., R. Chen et al., 2020; Wright et al., 2010). Accordingly, we aim to explore employee reactions to phishing attacks in a more longitudinal fashion than before while also assessing the possibility of individuals who report the threats more often than others—the repeat reporters. It is also possible that employee reactions follow patterns not found in previous research efforts.

Data Collection and Analysis

To assess our research question, we analyzed a data set generated from a series of mock email phishing campaigns involving more than 6,000 faculty and staff at a large university in the Southeastern United States. While the generalizability of findings from a single organization is a potential limitation, a university ecosystem is diverse in the various roles that employees perform (e.g., marketing, payment processing, maintenance operations, legal). Despite being able to assess employee behaviors from multiple organizations, we believe that unique insight still can be gained using data from a single university.

The first campaign was launched in June 2018, and the last campaign ran in early December 2019. Employees were each exposed to up to 20 mock phishing attacks that were randomly chosen from a wider set of more than 60 email phishing templates of varying levels of difficulty and contexts (e.g., technical support requesting changes to credentials, images sent from departmental scanner, order shipment, authoritative communication). The KnowBe4 platform was used to conduct the simulated attacks and collect subsequent behavioral metrics. We worked very closely with that university’s centralized information security department to create these campaigns and obtain the resulting data. To protect the identity of the faculty and staff, individuals in the security department provided anonymized data to the researchers as the employees were linked by their work email addresses for the purposes of matching responses across the various phishing campaigns. Our sample consisted of a wide variety of employees, including individuals from academic, business development, facility, finance, IT, police, and research departments, among others. Forty-seven percent of our sample was nonacademic.

The data that we used to perform our analyses were limited to high-level behavioral metrics (i.e., failures and reports) for each employee’s actions during each phishing campaign. A campaign “failure” was defined as occurring when an employee (a) clicked on a phishing link, (b) replied to the address from which that email originated, or (c) entered data once she or he clicked on the phishing link. Any one or combination of these actions would constitute a single failure for that employee during that campaign. Conversely, employees reporting the simulated phishing to the centralized information security department as a suspected phishing attack also had their responses recorded. This generated four behavioral metrics (i.e., clicked, replied, data entered, and email reported), with an additional derivative behavioral...
metric (Failure) being created from the first three metrics. Because it was not appropriate for all our campaigns to simulate credential theft, only a portion of the campaigns (i.e., three of 20) allowed employees to enter data once the phishing link was clicked; therefore, data on this behavior were more limited than the other user behaviors. As will be shown, this behavioral metric will prove vital in classifying employees relative to their behaviors.

Findings

Frequency Analysis

The number of campaign failures followed a power law distribution with nearly half of all users not failing a single email campaign, almost one third failing at least once, nearly one sixth failing two campaigns, less than one twelfth failing three campaigns, and then significantly fewer users failing more than three, as Figure 1 illustrates. From this pattern, we derived three user behavioral patterns that we labeled loosely after Caputo et al (2013) as: never clickers—users who never failed a campaign, occasional clickers—users who failed three or fewer of the 20 campaigns, and repeat clickers—users who failed more than three of the campaigns. Because those who fail are likely different from those who do not, and the distribution in Figure 1 can be used similar to a scree plot whose bend is around 3, we chose the values of 0, 1 to 3, and >3 above for creating the groups. It should be noted that all categories of failures are here labeled as clickers, regardless of the type of failure.

As presented in Table 1, never clickers represented 51% of the user population and none of the failures, occasional clickers represented 44% of the population and 71% of the failures, and repeat clickers represented 6% of the population but 29% of the failures. In considering the ratio of percentage of total failures over the percentage of the total population, we observe that repeat clickers represent a nearly fivefold risk factor, whereas occasional clickers represent a 1.6 risk factor, and never clickers represent a nearly zero risk.

The protective stewards, the converse of repeat clickers, were employees who did not fail a single campaign, and may have reported simulated phishing emails as suspicious. A distinction should be made between the protective stewards and employees who simply reported the simulated phishing emails. An employee who clicked on a link (or otherwise failed the simulation) could later report that email as suspicious, even after learning that the email was a simulated phishing email. These occurrences account for only 2.8% of the overall report counts. Furthermore, protective stewards were those employees who never failed a campaign and reported more than three simulated phishing emails. The distribution of reports by the never clickers is similar to that of the campaign failures with nearly half of the users neglecting to report a single email, nearly one in 12 reporting a single email, one in 24 reporting two emails, and then nearly half reporting three or more emails. An encouraging finding from a security perspective is that while this distribution also follows a Pareto form, the tail is much fatter and longer than that of the failures, as can be seen in Figure 2. Table 2 displays important data regarding three categories of reporters, which categories were formed using the earlier rationale for our categorization of the clickers.

These protective stewards have the potential to enhance organizational information security by reporting threats to the information security department, while also not falling victim to these same threats. From this perspective, a security enhancement factor (SEF) may also be obtained from the ratio of the population percentage over the percentage of reported phishing emails, providing a metric for organizational security enhancement.

Cluster Analysis

In addition to frequency analysis, we utilized cluster analysis to better determine what unique categories of employees existed within our sample. To first ascertain how many clusters were present, we created a scree test plot from the results of an agglomerative hierarchical cluster analysis using Ward’s method and squared Euclidean distances. This effort indicated that four clusters reasonably explained the ways that employees in our sample tended to respond to the simulated phishing attacks using the four metrics mentioned above. We then used k-means cluster analysis set at four clusters to determine which participants belonged to which clusters. The resulting clusters contained the following subsamples: “Gaffes” ($n_1 = 344$), “Beacons” ($n_2 = 1,361$), “Spectators” ($n_3 = 4,050$), and “Gushers” ($n_4 = 371$). Gaffes had the propensity to click on links at a higher rate than other clusters and exhibited a low reporting rate. Beacons tended not to click on links but reported suspicious emails at high rates. Spectators tended to do nothing (from an information security perspective) as they neither clicked at a high rate nor reported phishing emails at a high rate. And finally, Gushers not only clicked on links 4 to 5 times more than Beacons and
Spectators but only about half as much as Gaffes, they also entered their credentials into simulated malicious websites. Table 3 highlights this information.

Because of our extensive longitudinal data set, we were also able to assess how employees within the clusters performed over the 20 email campaigns in quarters. We used quarters because if variation existed in the behavioral metrics of individuals among the clusters, four time periods would help uncover the changes without being too detailed and overly complex. Each quarter thus represents 4 to 5 months and four to five phishing campaign exposures. Looking at the cluster behavior over time (Table 4 and Figure 3), reporting of phishing emails decreased slightly over time for all the clusters. Clicking also decreased over time except for Gaffes which showed a bump in the fourth quarter. Replying to phishing remained relatively stable across the four quarters, with Gushers showing the largest decline from Q1 through the remaining campaigns.

**Discussion**

**Scientific Implications**

To our knowledge, this research represents the first time that all forms of employee responses to phishing attacks—both negative and positive—have been explored simultaneously from a repeat perspective. While a handful of research studies have explored repeat clicking in a limited number of campaigns (Caputo et al., 2013; Li et al., 2020; Workman, 2008), we have not been successful at locating previous research that has explored the opposite, repeat reporting (i.e., protective stewardship) in relation to phishing emails. We will mention, however, that Caputo et al (2013) suggested a potential cause of repeat clicking behavior: email usage habits.

Extending the perspective on repeat clickers and repeat reporters, our research demonstrates that employees fall into one of the four general categories relative to the mix of behavioral metrics in which they tend to engage following phishing campaigns. While members of the Gaffe cluster represent a significant proportion of the failures in the university organization examined, the Gushers represent the employees who end up divulging important information like login credentials when they are phished through those types of attacks. Those in the Beacons group are the reporters in the organization, whereas, a bit surprisingly, about two thirds of our sample population fell into the Spectator group, which tended to provide little negative and positive influence to the organization during the phishing campaigns, almost as if they did not care. However, some employees in this large group might believe that an effective way of dealing with a phishing attack is to ignore and/or delete it. While they might not be the ones who succumb to such an attack through a misplaced click, they surely are not notifying the appropriate authorities that something got through the defenses. The differences among these employee groups provide quantitative, behavior-driven evidence that a single organization can simultaneously contain repeat offenders and protective stewards. Furthermore, our results demonstrate that some employees are more likely than others to provide external attackers with sensitive credentials, and there is a significant segment of the employee population that is likely difficult to motivate to any action whatsoever. Of course, this assertion deserves future attention.

A couple of additional items are worth noting here. First, all four of our employee groups fell victim to phishing attacks at some point, hovering between a 3% and 4% click base rate for Beacons and Spectators. Thus, as expected, perfect security is not possible in socio-technical systems, even among those employees who show active involvement in their protection. It could be possible that the 3% to 4% is simply due to human error as employees perform their daily tasks while utilizing the email system, and traditional interventions via SETA programs might prove futile in this effort. Rather, it is effortful attention to job processes and demands that would likely have the most impact. Second, with the exception of Gushers, the behaviors of the clusters are fairly stable over time. One
possibility for the Gushers’ variation could be due to those employees’ emotional instability or variations in stress levels, though these are assertions that deserve additional consideration as well.

**Practical Implications**

Resources within information security departments are often severely limited. Being able to better allocate the limited resources that are available would provide significant benefit to security operations staff. Security awareness has nearly achieved buzzword status within the security industry, but there is scarce understanding about how to best implement security awareness training and programs. Our work suggests that resources should not be uniformly distributed but rather should consider the relative strengths and weaknesses of an organization’s user population. The university participating in this study often employed defanged versions of actual phishing emails, and because of this fact, it is very likely that users who routinely fall victim to simulated phishing emails are also very likely to fall victim to real phishing attacks. Security departments need to tailor their SETA efforts toward their respective employee subpopulations. By adding additional training and interventions for the most vulnerable users (e.g., Gaffes and Gushers), while also empowering those who show the most promise toward protecting the organization (i.e., Beacons), security departments will increase their own effectiveness and see a better return on investment with already limited resources. Again, a significant concern is the employees in the Spectator group as they represent the majority and appear to be doing very little. For the security professionals who might say “well, at least they...”

**Table 2.** Percentages of Population and Reporting Groups.

| Category            | Number of campaigns reported | Percentage of population | Percentage of reports | Security enhancement factor (% reports / % population) |
|---------------------|------------------------------|--------------------------|-----------------------|--------------------------------------------------------|
| Protective stewards | >3                           | 33                       | 92                    | 2.79                                                   |
| Occasional reporters| 1–3                          | 17                       | 8                     | 0.47                                                   |
| Never reporters     | 0                            | 50                       | 0                     | 0.00                                                   |

**Table 3.** Behavior Means by Cluster.

| Cluster         | n   | Reported | Clicked | Replied | Entered |
|-----------------|-----|----------|---------|---------|---------|
| Gaffes          | 344 | 0.032    | 0.302   | 0.006   | 0.000   |
| Gushers         | 371 | 0.061    | 0.149   | 0.005   | 0.359   |
| Beacons         | 1,361 | 0.579    | 0.036   | 0.002   | 0.008   |
| Spectators      | 4,050 | 0.050    | 0.033   | 0.002   | 0.000   |

**Table 4.** Behavior Means by Cluster (Longitudinal).

| Cluster         | Time periods | 1   | 2   | 3   | 4   |
|-----------------|--------------|-----|-----|-----|-----|
| Reported        | Gaffes       | 0.070 | 0.039 | 0.029 | 0.026 |
|                 | Beacons      | 0.529 | 0.670 | 0.546 | 0.535 |
|                 | Spectators   | 0.072 | 0.055 | 0.041 | 0.040 |
|                 | Gushers      | 0.077 | 0.085 | 0.055 | 0.050 |
| Clicked         | Gaffes       | 0.212 | 0.287 | 0.256 | 0.297 |
|                 | Beacons      | 0.034 | 0.040 | 0.027 | 0.028 |
|                 | Spectators   | 0.029 | 0.046 | 0.031 | 0.033 |
|                 | Gushers      | 0.281 | 0.130 | 0.114 | 0.113 |
| Replied         | Gaffes       | 0.006 | 0.007 | 0.004 | 0.007 |
|                 | Beacons      | 0.002 | 0.001 | 0.000 | 0.002 |
|                 | Spectators   | 0.002 | 0.001 | 0.001 | 0.004 |
|                 | Gushers      | 0.010 | 0.003 | 0.002 | 0.009 |
are not engaging in ‘bad’ behavior,” we warn that these individuals might be easy to tip one way or the other, and if current SETA efforts are not reaching them effectively, then time will tell whether malicious, external agents reach them before the organization.

As an example, employees who belong to Beacons are not likely to benefit much from extensive discussion on the purpose of the report button in the email interface. Rather, taking time to understand the motivations for their actions and then attempting to build those motivations in other employees belonging to other clusters would likely prove much more fruitful. Likewise, SETA programming strongly centered on phishing would be more beneficial for the 6% of employees who are repeat clickers rather than forcing the 33% who are protective stewards to endure the same intervention. Such an approach indicates the need for organizational SETA programs to go beyond decreasing risk by also incorporating aspects that help build, strengthen, and maintain employee motivations to engage in positive behaviors.

Figure 3. Graphical depiction of cluster means (longitudinal).
Finally, organizations should work closely with their HR departments to help identify individual differences that might be associated with individuals within the individual clusters and especially the 6% who are the repeat clickers. That a small number of users persistently fail phishing simulations is suggestive of individual differences playing a primary role in this extremely detrimental behavior. It is unlikely that contextual factors are driving this behavior because context fluctuates, and cultural factors suggest a more widespread repeat clicking behavior pattern that is inconsistent with the small numbers observed for this phenomenon. Because of the vulnerabilities these users present, it is important that more organizations collaborate with researchers to more fully understand the causal and predictive factors of this behavior. Such is also the case with the protective stewards. These users whom we believe could be positive influences on their peers are very likely underutilized by security operations staff as a security resource.

**Conclusion and Future Research**

At the beginning of our research, we set out to determine whether different classes of organizational employees exist in relation to employees’ phishing-related behaviors. In addition, we were interested in assessing the negative user actions (e.g., clicking, entering data) alongside the positive behaviors (i.e., reporting the emails to the organization’s security team). Our results demonstrate that when employees’ phishing-related behaviors are viewed in a significant longitudinal fashion, four distinct classifications emerge, with each classification focusing on a unique behavioral characteristic of the employees assigned to them. Unfortunately, we were unable to uncover potential underlying causes of behaviors that formed these clusters. For example, significantly more work is needed to understand whether repeat clicking behaviors are trait driven (e.g., the Big Five personality traits), result from email behavior patterns, are caused by work role, or are influenced by something else not yet considered. Likewise, future research should also focus efforts on the protective behaviors, exploring the reasons why the repeat reporters and the “protective stewards” do what they do. Are these individuals acting in a protective fashion because they feel a strong sense of commitment to their organization as previous research (Posey et al., 2015) has shown? Has the pressing of a report button within the email interface become more of a habit that is enacted when the employee perceives any potential for phishing, or if they are working from home, how much of an impact are work–life interference, conflict, and stress having on phishing rates? Do these individuals believe that they will be rewarded by their organization or supervisor for acting in a protective fashion? These and other questions remain and could be examined from a qualitative or quantitative methodological approach.

Finally, despite our extensive 19-month, 20-campaign effort, the attacks under examination were in fact simulated events. It is possible that “real” attacks might potentially elicit different reactions, but one of the main issues associated with a reliance on data from actual attacks is a lack of coverage for all employees under examination. We cannot think of a reason why an organization would allow a known attack to spread within its network simply to gauge how its employees might respond. Through simulated phishing attacks, researchers can obtain information about responses from employees across an entire organization (in our case, more than 6,000 employees) rather than only a select few. From this, the number of times an entire employee base fails or reports suspected attacks can be derived. Another issue when relying on data from actual phishing attacks is that it can be extremely difficult to determine how the attack was initiated and/or progressed. Furthermore, there are no doubt times when actual phishing attacks occur without the organization being aware of their presence. Thus, we believe research based on simulated phishing campaigns are effective proxies both because users are not typically warned immediately beforehand that a simulation campaign is about to be launched and because these simulated campaigns closely mimic actual attacks and are sometimes copies of actual phishing attacks that have had the malware removed. Whether employees would respond in similar ways to social engineering tactics via other communication channels (e.g., vishing through phone systems, smishing through SMS text messages) remains to be seen. We expect that the four unique categories of employees uncovered by our research will play important foundational roles in that research, and we eagerly await the results.

**Declaration of Conflicting Interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was in part sponsored by the National Institute of Standards and Technology (NIST) under Financial Assistance Award Number: 60NANB19D123. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of NIST or the U.S. Government.

**Human Subjects Review Board**

Given that no identifying information of the participants was collected during the study, University of Central Florida’s (UCF) Institutional Review Board (IRB) committee deemed the study presented herein as being exempt.

**ORCID iD**

Clay Posey https://orcid.org/0000-0001-6704-0750

**References**

Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). Phishing detection based associative classification data mining. *Expert Systems with Applications, 41*(13), 5948–5959.
Ashford, W. (2019). Lateral phishing used to attack organisations on global scale. https://www.computerweekly.com/news/252466945/Lateral-phishing-used-to-attack-organisations-on-global-scale

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don’t even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems, 19*(8), 689–715.

Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce, 29*(1), 24–39.

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders’ awareness of organizational SETA efforts. *Decision Sciences, 49*(6), 1187–1228.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors, 58*(8), 1158–1172.

Canham, M., Constantino, M., Hudson, I., Fiore, S. M., Caulkins, B., & Reinerman-Jones, L. (2019, August). The enduring mystery of the repeat clickers [Paper presentation]. 15th Symposium on Usable Privacy and Security, Santa Clara, CA, United States.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy, 12*(1), 28–38.

Carella, A., Kotsovei, M., & Truta, T. M. (2017, December). Impact of security awareness training on phishing click-through rates [Paper presentation]. 2017 IEEE International Conference on Big Data, Boston, MA, United States.

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems, 133*, Article 113287.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer and Information Systems, 55*(3), 11–19.

Columbus, L. (2020). Cybersecurity spending to reach $123B in 2020. https://www.forbes.com/sites/louiscolumbus/2020/08/09/cybersecurity-spend-to-reach-123b-in-2020/#56b0eac705f

Crosier, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101.

D’Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(1), 59–71.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works [Paper presentation]. Proceedings of the SIGCHI conference on Human Factors in Computing Systems, Montreal, Quebec, Canada.

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security, 69*, 18–34.

El Aassal, A., & Verma, R. (2019, March). Spears against shields: Are defenders winning the phishing war? [Paper presentation]. Proceedings of the ACM International Workshop on Security and Privacy Analytics, Richardson, TX, United States.

FBI. (2015). *Business Email compromise: An emerging global threat*. https://www.fbi.gov/news/stories/business-e-mail-compromise

Gartner. (2018). *Gartner forecasts worldwide information security spending to exceed $124 billion in 2019*. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack [Paper presentation]. 2016 International Conference on Computing, Communication and Automation (ICCQA), Noida, India.

Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal, 30*(2), 220–269.

Hadnagy, C., & Fincher, M. (2015). Phishing dark waters: The offensive and defensive sides of malicious Emails. Wiley Online Library.

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology, 32*(6), 584–593.

Kajtazi, M., Cavusoglu, H., Benbasat, I., & Haftor, D. (2018). Escalation of commitment as an antecedent to noncompliance with information security policy. *Information & Computer Security, 26*(2), 171–193.

Khонji, M., Iraji, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials, 15*(4), 2091–2121.

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707–718.

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020, January). Experimental investigation of demographic factors related to phishing susceptibility [Paper presentation]. Proceedings of the 53rd Hawaii International Conference on System Sciences, Maui, HI, United States.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal, 25*(5), 433–463.

Marks, J. (2019, February 14). The Cybersecurity 202: Iran indictments show even U.S. intelligence officials are vulnerable to basic hacking schemes. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/02/14/the-cybersecurity-202-iran-indictments-show-even-u-s-intelligence-officials-are-vulnerable-to-basic-hacking-schemes/5c6462af1b326b71858ec6b78/

Mäses, S., Kikerpill, K., Jüristo, K., & Maennel, O. (2019, August). The enduring mystery of the repeat clickers [Paper presentation]. 2016 International Conference on Computing, Communication and Automation (ICCQA), Noida, India.

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? An exploratory study of individuals’ susceptibility to phishing. *European Journal of Information Systems, 26*(6), 564–584.

Morgan, S. (2019). Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021. https://cybersecurityventures.com/cybersecurity-market-report/
Canham et al. (2015). Enterprise phishing susceptibility report. https://cofense.com/wp-content/uploads/2017/10/PhishMe_EnterprisePhishingSusceptibilityReport_2015_Final.pdf
Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders’ motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179–214.
Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders’ protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, 37(4), 1189–1210.
Proofpoint. (2020). 2020 state of the phish: An in-depth look at user awareness, vulnerability and resilience. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish.
Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors*, 60(5), 597–609.
Sebescen, N., & Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the Association for Information Science and Technology*, 68(9), 2237–2247.
Silic, M., & Back, A. (2014). Shadow IT—A view from behind the curtain. *Computers & Security*, 45, 274–283.
Straub, D. W., Jr., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 14(1), 45–60.
Symantec. (2019). Internet security threat report. https://www.broadcom.com/support/security-center
Verizon. (2019). 2019 data breach investigations report. https://enterprise.verizon.com/resources/reports/dbir/
Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4), 345–362.
Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), 101–105.
Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1–20.
Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662–674.
Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation*, 19(4), 391–416.
Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, 108, 107–118.
Zimmermann, S., & Rentrop, C. (2014, June). On the emergence of shadow IT—A transaction cost-based approach [Paper presentation]. European Conference on Information Systems (ECIS), Tel Aviv, Israel.