IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 June 2022, accepted 4 July 2022, date of publication 12 July 2022, date of current version 18 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3190009

RESEARCH ARTICLE

Spear-Phishing Susceptibility Stemming From Personality Traits

SERGIU EFTIMIE, (Graduate Student Member, IEEE), RADU MOINESCU, AND CIPRIAN RĂCUCIU, (Member, IEEE)
Military Technical Academy "Ferdinand I," 050141 Bucharest, Romania

Corresponding author: Sergiu Eftimie (sergiu.eftimie@ieee.org)

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the General Data Protection Regulation (GDPR).

ABSTRACT This study explores the psychological aspects of social engineering by analyzing personality traits in the context of spear-phishing attacks. Phishing emails were constructed by leveraging multiple vulnerable personality traits to maximize the success of an attack. The emails were then used to test several hypotheses regarding phishing susceptibility by simulating a series of spear-phishing campaigns inside a software development company. The company's employees underwent a standard Big Five personality test, four different phishing emails over four weeks, and cybersecurity training. The results were aggregated before and after the cybersecurity course, and binary logistic regression analyses were performed at each phase of the phishing attack. The results show that personality traits correlate with phishing susceptibility under certain circumstances and pave the way for new methods of protecting individuals from phishing attacks.

INDEX TERMS Cyber security, human behavior, personality traits, social engineering, spear-phishing.

I. INTRODUCTION

Social engineering is a general term that encompasses the various methods that cybercriminals use to obtain sensitive information or access protected systems by taking advantage of human weaknesses. Phishing is one of the most popular social engineering techniques in which attackers construct emails that aim to manipulate a target to open a doorway for attacks [1]. The extensive use of email for business purposes has led to a large attack surface, and the ease with which these attacks can be performed has lowered the technical skill barrier for attackers, making it a prevalent option for cyber-attacks. Human factors are frequently recognized as the most vulnerable links in the information security chain. Human behavior often facilitates the success of cyberattacks [2].

The success of a phishing attack depends on multiple factors such as the skill of the attacker, the awareness of the target, deployed systems designed to avoid phishing techniques such as spam filtering, or the methods used by attackers to avoid automatic spam detection mechanisms. Moreover, private information exposed on social media platforms is used to make emails appear legitimate in so-called spear-phishing attacks [3], increasing the likelihood of manipulating the target to open a doorway to attack.

The spear-phishing process consists of multiple steps, as illustrated in Fig. 1. During the preparation phase (S1), an attacker gathers as much private information as possible regarding the target. The sources range from online databases containing leaks to social media platforms. Private information is needed to compose an email that maximizes the chances to convince the target to perform dangerous activities such as clicking a link or downloading and running a malicious attachment. At this stage, technical skills are required to implement the infrastructure to send an email that would appear legitimate to a spam detection/filtering algorithm. Modern email clients verify the legitimacy of the domain of the originating email. As a general rule, the content of the email should be clean, clear, and balanced to get past the

The associate editor coordinating the review of this manuscript and approving it for publication was Saqib Saeed.

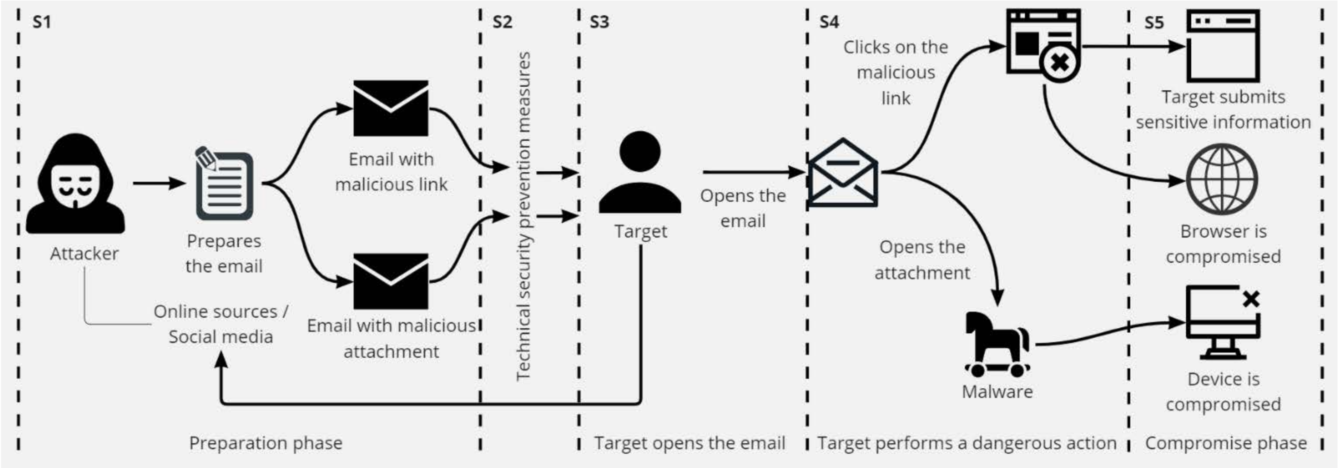
S1
S2
S3
S4
S5
Attacker
Prepares the email
Online sources / Social media
Email with malicious link
Email with malicious attachment
Technical security prevention measures
Target
Opens the email
Clicks on the malicious link
Opens the attachment
Malware
Target submits sensitive information
Browser is compromised
Device is compromised
Preparation phase
Target opens the email
Target performs a dangerous action
Compromise phase

FIGURE 1. Phases of a common Spear-Phishing attack.

filtering stage (S2). If the email reaches the inbox, the next goal of the attacker is to convince the target to open the email (S3). The subject of the email plays an essential part at this stage because it is the single visible part of the email. The actual opening of an email is considered a safe action on the part of the target because the content of the email is static, and most modern email clients block images that could enable the monitoring of opening the email by default. Once an email is opened, the content plays the role of convincing the target to perform the activity.

It should be noted that an attacker can send an initial email that does not contain dangerous items to establish trust with the target. The phase in which the target performs an activity, such as clicking a link or downloading an attached file, represents a dangerous part (S4). Mitigating a successful attack at this stage involves a complex set of measures that must be put in place by the security department, such as timely patching of the operating system and keeping the software updated, deploying antivirus solutions, and others. The final phase is where the compromise occurs either on the device, browser, or credentials submitted by the target (S5).

Although most modern browsers use sandbox technology that physically isolates the browsing activity from the local machine, there could be possible bugs in the browser and other applications that attackers can exploit with minimum effort or technical skills by using frameworks such as Metasploit. Because a link is a universal resource identifier, it can point to other objects that can be anything from a web page to an executable file. This opens the door to any bug in the software that automatically opens a file downloaded by the browser. Alternatively, any file can be a delayed trigger for another previously installed package in a more complex attack scenario. The lack of timely patching of software and operating systems increases the attack surface and danger associated with phishing attacks. Although security measures effectively reduce the success rate of attacks, it should be noted that 0-day vulnerabilities can make them ineffective. Since 0-day attacks are extremely valuable, they tend to be used more scarcely, including in so-called whaling attacks, where high-profile individuals such as CEOs are targeted.

Researchers have studied different aspects of human traits and behaviors to understand what raises phishing susceptibility. For example, a foundational study on unintentional insider threats [4] identified willingness to take risks as a contributing factor, measured using the Balloon Analogue Risk Task (BART). Other studies have investigated the susceptibility to phishing by investigating the impact of gender, age, and cultural factors [5], [6]. The impact of personality traits on the phishing susceptibility, particularly measured using the Big Five factor model was addressed in several papers [5], [7]–[11]. Individuals' personality traits contribute to their susceptibility to social engineering exploits such as persuasion, manipulation, and deceit [12]. The Big Five model is cross cultural and has some advantages when developing a security framework that is independent of a particular society or culture and has been acknowledged as relevant and valid across multiple fields [13]. A meta-analysis [14] of multiple psychological studies concluded that there is evidence that the Big Five personality traits are powerful predictors of actual manifestation of them in behavior. Although some results regarding traits, such as extraversion with regard to phishing susceptibility, are consistent, others are not. This variability, in our view, exists because few papers have addressed in detail the content of phishing emails as a driver for increasing phishing susceptibility. Papers such as [15] and [16], for example, have addressed the content of the phishing email but in a limited manner. Furthermore, [17] has emphasized the importance of email content in this type of study.

This study examines the impact of the Big Five traits on the phishing susceptibility of an individual by using specifically crafted emails that aim to take advantage of the entire spectrum of human vulnerability in the context of personality. This study is part of a larger effort to create a functional security system that integrates and automates the entire human profiling process to identify insider threats.

The remainder of this paper is organized as follows. A brief background is provided, followed by the proposed hypotheses generated during the literature review. Next, we describe the methodology used to simulate a phishing attack on a company's employees (n=235) and the methods used to aggregate the dataset. We then perform several statistical analyses on the data. Finally, the results are presented, and the paper ends with a conclusion.

II. BACKGROUND AND HYPOTHESIS DEVELOPMENT

A foundational study [4] defined unintentional insider threats as current or former employees, business partners, or contractors who have or have had access to an organization's network, system, or data and who, through action or inaction (without malicious intent), cause harm or substantially increase the likelihood of severe future damage to the confidentiality, integrity, or availability of the company's information or information systems. Non-responders are a sub-category of unintentional insiders who fail to comprehend and apply security practices even after receiving cybersecurity training [18]. On the other hand, inadvertent insiders change their behavior following this type of training. These employees experience security breaches because of isolated mistakes and exhibit safe behavior.

To identify dangerous behaviors that people exhibit, we must examine their personalities. Significant relationships have been found between the Big Five personality factors and behavior [19], and the more pronounced a trait is, the more it manifests in behavior. To have a personality trait, individuals must be somewhat consistent across situations in their behaviors related to the trait, and individuals with a trait are also somewhat stable over time in their behaviors related to the trait [20]. The phishing process involves manipulating unintentional insider threats to facilitate an attack. Next, for each personality trait from the Big Five model (openness, conscientiousness, extraversion, agreeability, and neuroticism), we assessed its influence on vulnerability to being manipulated to specific contents of a phishing email. In addition, we also consider, the impact of personality on acquiring the technical abilities needed to detect a phishing email.

A. OPENNESS

Openness can be characterized as a personality dimension that reflects the inclination toward cognitive exploration [21]. Openness has been positively linked to responsible behavior regarding security best practices [5], so low openness would potentially facilitate dangerous security behavior.

B. CONSCIENTIOUSNESS

Conscientiousness is the tendency to pursue socially defined norms for impulse control, and to be goal-directed, plan, and postpone gratification [22]. Conscientiousness represents an inclination to think, judge, and conduct consistently over time. A highly conscientious individual may be manipulated by taking advantage of his or her inherent need to order things and tasks. On the other hand, conscientiousness may be the personality trait that is most negatively correlated with phishing vulnerability. Higher levels of conscientiousness would result in individuals being more likely to follow security guidelines and less likely to disregard policies. A study [23] found that low levels of conscientiousness predicted deviant workplace behavior in the form of irresponsible conduct or rule-breaking.

C. EXTRAVERSION

Extraversion can be characterized as a dimension of personality that reflects successful adaptation by satisfying interpersonal relationships [24]. Compared to introverts, extroverts view themselves as being more successfully and enjoyably involved in various parts of their lives. Extraverted people wish to surround themselves with others and become the center of attention. While this is typically a positive trait, it can lead to increased vulnerability in the context of phishing. An early study [25] found that a high score in affective commitment, a facet of extraversion, led to people giving up sensitive details because they wanted to gain approval or belong to a social group. In addition, another study [26] found that people who did not offer passwords to their peers were not seen as team players and were considered unsociable. More recent studies [10], [11], [27], [28] have shown that high extroversion is predictive of increased vulnerability to phishing attacks.

D. AGREEABLENESS

Agreeableness is a personality dimension that is concerned with how individuals pursue positive relationships with others. Agreeable people avoid conflicts, seek cooperation, and help their peers [29]. Agreeableness is the personality trait that is most associated with phishing [9] and multiple studies [7], [11], [30] have reached similar conclusions. Agreeable people may be manipulated by establishing trust with the target, as this represents a facet of agreeableness. By invoking the need for compliance, agreeable people can be exploited to perform actions that would reestablish their supposed lack of compliance.

E. NEUROTICISM

Neuroticism is a personality trait defined as the tendency to experience recurrent, powerful negative emotions associated with the perception of inadequate coping in response to stress [31]. Individuals with low neuroticism tend to be satisfied, self-assured, and stable. People with low neuroticism report fewer psychological and physical problems and less anxiety than highly neurotic individuals.

Neuroticism plays an essential role in impulsivity [32] and manifests itself in the form of anxiety about negative consequences. However, a recent review [33] on the role of neuroticism in phishing susceptibility concluded that a well-established psychological theory explaining the role of neuroticism in the phishing context is not yet available. The reasons for the lack of consensus were the use of non-representative samples and the lack of uniformity among the studies.

Considering the impact of each of the Big Five traits in increasing the susceptibility to phishing and in the capacity to acquire the technical abilities to detect phishing emails, we investigated whether an optimal dangerous phishing email can be created to take advantage of multiple vulnerable traits simultaneously. The premise behind this strategy is that if multiple personality traits can be exploited simultaneously, the likelihood that the target would fall victim increases. As described above, the resulting highly vulnerable profile would have low openness and conscientiousness and high extraversion, agreeableness, and neuroticism.

While a low level of openness and conscientiousness would provide the context (in which an individual does not have the technical ability to identify the attributes of a phishing email), we identified several strategies to manipulate high extraversion, agreeableness and neuroticism by combining specific knowledge about the person, work environment, managerial structure, infrastructure and habits.

The emails were designed to trigger or manipulate impulsivity or social interaction (high extraversion), conformity (high agreeableness), and anxiety regarding negative consequences (high neuroticism). Additionally, there is evidence that high neuroticism deteriorates decision performance under low openness and conscientiousness [34].

To simulate an insider attack, we cloned the identity platform's page, hosted it under a similar named real domain, and used it to record the submission of sensitive data (only the submission action, not the data). We designed all phishing emails to manipulate individuals to click on a specifically designed link. Each unique link directed them to the clone on the identity platform's page. Employees frequently use the original page, being a single point of access for all the company's online tools such as Jira, Gitlab, and others. Repetitive daily password insertion (caused by a security policy that prevented credentials from being saved in the browser) produced a dangerous situation by creating an unconscious process in which employees would enter their passwords without paying much attention.

The content of the email was not designed to manipulate a target's risk-taking proclivity. Although previous studies have addressed risk-taking in regular phishing [35], we argue that spear-phishing has more destructive potential, and that more focus should be directed to this type of attack. Phishing emails were devised to mimic the content employees usually receive during their work activities. We aimed to create circumstances in which negative consequences would arise if the employees did not engage in the activities presented by the emails. The resulting emails are presented in Appendix A.

We define phishing susceptibility as the likelihood of being manipulated by opening an email (engaged targets), clicking on a malicious link (vulnerable targets), and submitting sensitive data (highly vulnerable targets). We argue that phishing susceptibility must be accounted for in relation to email content, and not as a general trait. As we are interested in phishing susceptibility across the different phases of the phishing process, we formulate our hypothesis as follows:

H1: Given that a phishing email is designed to take advantage of or manipulate certain pronounced personality traits (high extraversion, agreeableness, and neuroticism) if a target's personality profile matches those individual traits, then the likelihood of being susceptible to phishing will increase.

H1a Susceptibility to the Open Email phase

H1b Susceptibility to the Link Clicking phase

H1c Susceptibility to the Sensitive Data Submission phase

H2: If a highly vulnerable (submitted sensitive data) target's personality profile matches the non-responder profile (low openness, low conscientiousness, and high neuroticism), the target is more likely to exhibit the same dangerous behavior despite attending cybersecurity training.

The maturity principle of personality development [36] states that as people age, they adapt their personalities to better accommodate the tasks associated with the responsibilities of adult life. Adults become more agreeable, conscientious, and emotionally stable with age [37]. Since our phishing emails targeted high extraversion, agreeability, and neuroticism, we expect that as people age, their susceptibility will remain the same (agreeability will increase, but neuroticism will decrease). However, an increase in conscientiousness means better compliance with security policies. Consequently, we formulated the following hypothesis regarding age:

H3: Given that a phishing email is designed to take advantage of or manipulate certain pronounced personality traits (high extraversion, agreeableness, and neuroticism), age does not play a significant role in phishing susceptibility.

Women have been found, on average, to be more agreeable than men [38]. Consequently, we formulated our hypothesis regarding gender-biased phishing susceptibility:

H4: Given that a phishing email is designed to take advantage of or manipulate certain pronounced personality traits (high extraversion, agreeableness, and neuroticism), women will be more susceptible to phishing than are men.

III. RESEARCH METHODOLOGY

This research aimed to investigate the effects of the Big Five personality traits on the phishing susceptibility of individuals. For this purpose, we sought to obtain qualified results regarding the Big Five assessment using a specialized independent company that handled the testing part and simulated a sophisticated spear-phishing attack as close to reality as possible. For example, a recent report on spear-phishing emphasized that the most successful attacks are delivered in the period after lunch when energy is low, thus increasing the chance that malicious emails may pass undetected. The emails in our study were sent randomly from 2:00 PM to 6:00 PM to replicate this strategy [39]. The morning period is generally avoided in these attacks because of the high alertness of the employees. Other aspects of designing the email included using the manager's email address, suggesting that the email was legitimate. The domains from which the emails were sent were valid and legitimate domains with SSL certificates, and we used an external service to send the emails to increase the chances that the emails reached the inbox. The study began with a personality test administered to all employees by a third-party company specializing in Big Five traits assessment [40]. We then planned and performed a simulated spear-phishing campaign to determine phishing susceptibility at each stage in the context of personality (see Fig. 1), opening the email (S3), clicking on the provided link (S4), and presenting sensitive details (S5). The campaign lasted four weeks, during which four different phishing emails were sent to the targeted employees. In the second week, the employees attended a cybersecurity course that addressed the dangers of phishing and the different techniques used by attackers. The cybersecurity course was important for investigating the hypothesis regarding the non-responder profile.

A. DEMOGRAPHICS

The participants in the study (n=235) were employees of a software consultancy company that provided project-based externalization services on all aspects of software development. Consequently, people's roles were specific to agile scrum teams, such as product owners, business analysts, developers, and quality assurance analysts, as well as additional roles, such as project managers, accounting, human resources, and tech support. All employees regularly use computers and online environments for their work activities. At the time of the study, the employees had been working fully remote for at least one year. Employees' ages ranged from 21 to 56 years old. Some studies have considered age as a factor in phishing susceptibility [35], and although there is relative stability of personality traits across time [41] the maturity principle [36] was considered during the study.

The sex distribution was fairly balanced (123 M and 112 F). Although men prefer the software domain [42], diversity hiring campaigns have altered the gender distribution in the company we studied. Previous studies have also looked at gender as a factor in phishing susceptibility [35], finding women on average more susceptible. In our view, the reason behind these findings is based on fundamental differences between men and women on a personality level (for example women tend to be more agreeable than men [38]).

B. PERSONALITY TESTS

The Big Five model is a scientifically reliable model of personality [43]. These traits are identifiable, exist cross-culturally, and are related to different forms of mental illness and health. The Big Five personality tests used in this study, which consisted of 97 questions with true-false answers, were provided by an independent specialized company [40]. GDPR consent was obtained before taking the tests. The employees received results consisting of their scores on each trait, a brief guide to analyzing the information, and a detailed psychological description and interpretation of the results.

The company's management encouraged the examination, leading to a 100% completion rate for the personality test. The results were extracted in tabular form (in the form of T-scores for each personality trait) and a unique ID was attributed to each employee by hashing its email address. After aggregation of the results, the hash keys were removed to protect the identity of the participants, and the data were made available online [44].

C. CYBERSECURITY COURSE

A cybersecurity awareness course with topics related to the dangers of phishing and the methods used by attackers was distributed to employees at the beginning of week 3, after the first two phishing campaigns. Course completion was mandatory. The security team had already planned this course, and we collaborated to set the timing of the phishing campaigns so that we could obtain the results before and after its completion. The reason behind this strategy was to investigate its effect on phishing susceptibility and to look for further proof of our hypothesis concerning non-responders (H2). The course had an online format, and several topics were addressed:

- Risks of clicking on malicious links
- Attack techniques
- Types of phishing scams
- Phishing email identification
- Planning and execution of a phishing attack
- Protection against ransomware

D. PHISHING CAMPAIGNS

The first step in preparing the phishing simulation was to gather all the email addresses and prepare details, such as the employees' manager email address to include it in the content of the email. Next, we set up a web server to host all required scripts. The email address of each employee was hashed using the SHA-256 algorithm, and the resulting hash key was used to create unique URLs for items that were placed inside the phishing email. This step was needed to identify an individual and each of his or her actions. We used a convenient external service to send emails [45]. This approach is close to reality because attackers use public email campaign services to maximize their chances of reaching an inbox. These services regularly manage blacklisted IPs and update their templates to avoid formatting problems inside email clients.

To maximize the chances of the email reaching the inbox, we whitelisted the domains from which the phishing emails were sent. The phishing campaign was conducted under the supervision of the company's security officers and in accordance with the company's security policy.

We cloned the identity provider's page for the step in which the subjects were asked to submit sensitive details. The targeted sensitive data were the primary password used to access the company's internal tools (although we did not record the actual data, just the submission). By providing identical visual cues, we set up to take advantage of the habit

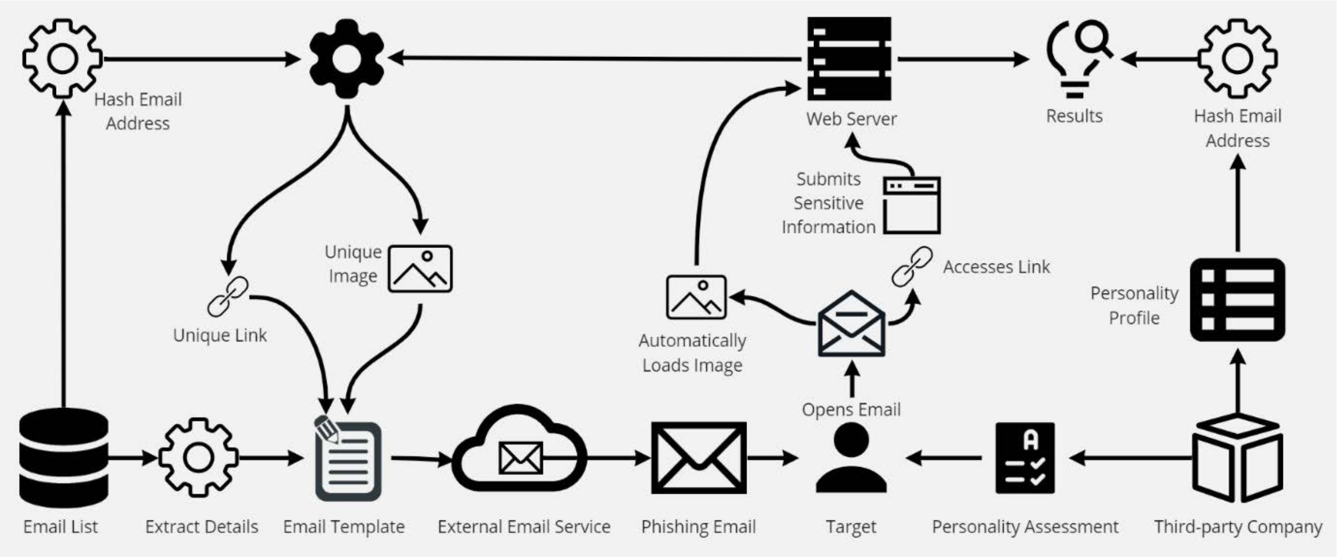

FIGURE 2. Spear-Phishing campaign.

of writing one's password each time to access a resource from the intranet.

IV. DATA ANALYSIS AND RESULTS

Several analyses were performed on the resulting datasets using IBM SPSS Statistics. Descriptive statistics for all the personality trait scores are listed in Table 1.

TABLE 1. Descriptive Statistics For Personality Traits.

	N	Minimum	Maximum	Mean	Std. Deviation
Openness	235	21.78	78.61	50.0673	10.16338
Conscientiousness	235	22.19	76.03	50.5209	10.39464
Extraversion	235	26.15	76.46	50.0027	9.76497
Agreeableness	235	23.12	74.35	49.6421	9.66752
Neuroticism	235	23.40	76.97	50.5960	10.30664

The results of all four campaigns for each phase of the phishing attack are listed in Table 2.

TABLE 2. Phishing Campaign Results.

	Open Email	Click Link	Submit Data
Phishing Campaign 1	68.1%	30.6%	15.3%
Phishing Campaign 2	56.6%	26.8%	13.2%
Phishing Campaign 3	61.3%	14.0%	8.1%
Phishing Campaign 4	69.8%	21.7%	8.1%

Logistic regression was used to analyze the relationship between demographic factors (age and gender) and personality profiles (openness, conscientiousness, extraversion, agreeableness, neuroticism) and phishing susceptibility, considering each phase of a spear-phishing attack (both before and after attending a cybersecurity course).

Logistic regression is used to predict the probability that an observation falls into one of two categories of a dichotomous dependent variable [46] (in our case, the result of one of the three phases of the phishing attack) based on one or more independent variables that can be either continuous (personality trait scores and age) or categorical (gender).

The results from the first two phishing campaigns were merged into a single set (*Phishing Campaign A* - results before the cybersecurity course). The results from the last two phishing campaigns were merged into a single set (*Phishing Campaign B* - results after the cybersecurity course). We then verified several assumptions in order to be able to perform binary logistic regression for each phase of the phishing process:

a. To perform a binary logistic regression, the observations should be independent (no relationship between the observations in each category of the dependent variable or the observations in each category of any nominal independent variable). In our case, in each step of the phishing attacks, the dichotomous dependent variable has only two values (1 for yes and 0 for no) concerning the email opening, clicking on the link, and submitting sensitive data. The same is the case for the gender independent variable where the categories were mutually exclusive: male (1) and female (0).

b. After aggregation, our sample size consisted of 470 (2 × 235) cases. According to [46] there should be a bare minimum of 15-50 cases per independent variable in order to be able to perform a logistic regression. Therefore, our aggregated sample is suitable for this type of analysis.

c. There should be no multicollinearity among the continuous predictor variables. Therefore, we examined the variance inflation factors (VIFs) (Table 3) for all continuous predictor variables to detect a possible issue of multicollinearity in our study. The results indicate no issues of this type within the regression models. As all VIFs are below the threshold of 10 [47], we can conclude that none of the independent continuous variables cause multicollinearity.

TABLE 3. Variance Inflation Factors.

Variable	VIF
Age	1.016
Openness	1.006
Conscientiousness	1.019
Extraversion	1.003
Agreeableness	1.038
Neuroticism	1.041

d. A linear relationship should exist between the continuous independent variables and the logit transformation of the dependent variable, which will be analyzed during each logistic regression for each of the dependent variables using the Box-Tidwell [48] approach.

e. Check significant outliers, leverage, or influential points – this is addressed during each logistic regression for each of the dependent variables.

These assumptions will provide information on the accuracy of predictions, test how well the regression model fits the data, determine the variation in the dependent variable explained by the independent variables and finally test hypotheses.

A. PHISHING CAMPAIGN A - STEP 1 (EMAIL OPENED)

Binary logistic regression was performed to ascertain the effects of age, gender, and personality traits on the likelihood that users will open the phishing email. The linearity of the continuous variables with respect to the logit of the dependent variable (email opened) was assessed via the Box-Tidwell [48] procedure. Bonferroni correction was applied using all 14 terms in the model, resulting in statistical significance being accepted when p <.003571 [49]. Based on this assessment, all continuous independent variables were linearly related to the logit of the dependent variable. There was one standardized residual with a value of -2.544 standard deviations, which was retained in the analysis. The logistic regression model was statistically significant, $\chi 2(7) = 30.742$, p <.0005. The model explained 8.6% (Nagelkerke R2) of the variance in the email-opening action and correctly classified 64.5% of the cases. The sensitivity was 87%, specificity was 27.1%, positive predictive value was 66.4% and negative predictive value was 55.8%. Of the seven predictor variables, age and neuroticism were statistically significant (Table 4). Increasing neuroticism was associated with an increased likelihood of opening the phishing email, whereas increasing age was associated with a decrease in the likelihood of opening the email.

The area under the ROC curve (Fig. 3) was .651 (95% CI,.601 to .701), which is considered a poor discrimination according to [50].

TABLE 4. Logistic Regression Predicting Likelihood of Opening a Spear-Phishing Email based on age, gender and personality traits.

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
							Lower	Upper
Age	-0.027	0.012	5.014	1	0.025	0.974	0.951	0.997
Gender	0.041	0.216	0.036	1	0.850	1.042	0.682	1.592
O	-0.014	0.010	2.017	1	0.156	0.986	0.967	1.005
C	-0.019	0.010	3.707	1	0.054	0.982	0.963	1.000
E	0.008	0.010	0.671	1	0.413	1.008	0.988	1.029
A	0.020	0.011	3.597	1	0.058	1.020	0.999	1.042
N	0.031	0.011	8.701	1	0.003	1.032	1.011	1.053
Constant	0.081	1.238	0.004	1	0.948	1.084		

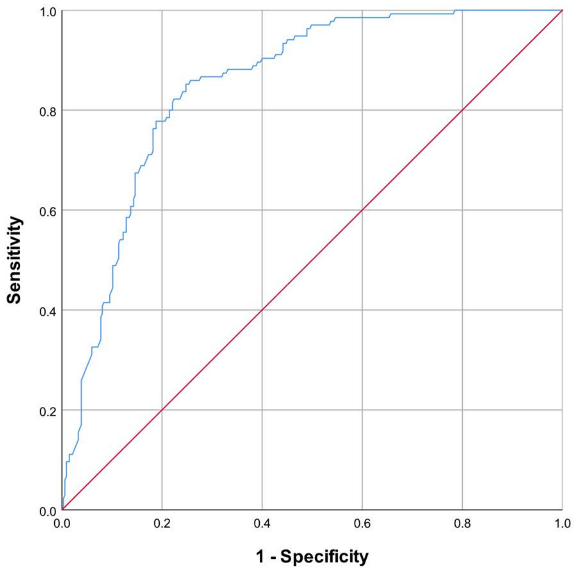

FIGURE 3. ROC curve for predicting Open Email step.

B. PHISHING CAMPAIGN A - STEP 2 (LINK CLICKED)

Binary logistic regression was performed to ascertain the effects of age, gender, and personality traits on the likelihood that users will click on a malicious link. The linearity of the continuous variables with respect to the logit of the dependent variable (link clicked) was assessed using the Box-Tidwell [48] procedure. Bonferroni correction was applied using all 14 terms in the model resulting in statistical significance being accepted when p <.003571 [49]. Based on this assessment, all continuous independent variables were linearly related to the logit of the dependent variable. Eight standardized residuals were retained in the analysis.

The logistic regression model was statistically significant, $\chi 2(7) = 150.997$, p < .0005. The model explained 39.3% (Nagelkerke R2) of the variance in the link clicking action and correctly classified 76.8% of the cases.

The sensitivity was 44.4%, specificity was 89.9%, positive predictive value was 63.8% and negative predictive value was 80%.

All the personality traits were statistically significant (Table 5). Increasing openness and conscientiousness was associated with a decreased likelihood of clicking the malicious link while increasing extraversion, agreeableness and neuroticism were associated with an increased likelihood of clicking the link.

TABLE 5. Logistic Regression Predicting Likelihood of Clicking on a malicious link based on age, gender and personality traits.

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
							Lower	Upper
Age	-0.011	0.016	0.436	1	0.509	0.989	0.959	1.021
Gender	-0.009	0.263	0.001	1	0.974	0.991	0.592	1.661
O	-0.062	0.013	23.384	1	0.000	0.940	0.917	0.964
C	-0.063	0.013	23.430	1	0.000	0.939	0.916	0.963
E	0.064	0.013	23.430	1	0.000	1.066	1.039	1.095
A	0.073	0.014	26.758	1	0.000	1.076	1.047	1.106
N	0.070	0.014	25.600	1	0.000	1.073	1.044	1.102
Constant	-5.080	1.561	10.586	1	0.001	0.006		

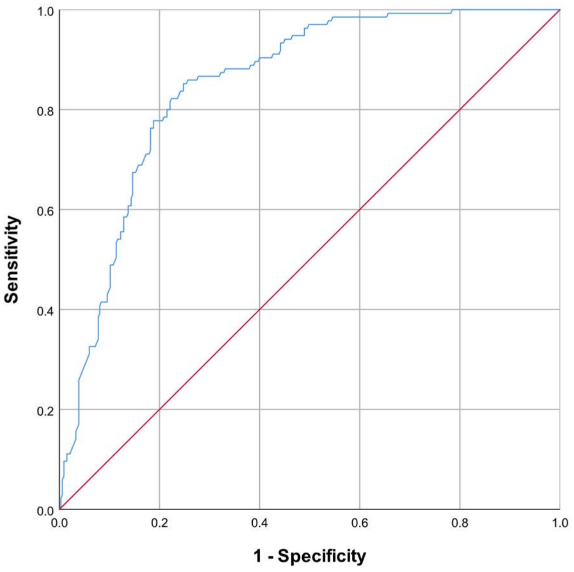

FIGURE 4. ROC curve for predicting the Link Clicking step.

The area under the ROC curve was .850 (Fig. 4) (95% CI, .815 to .885), which is considered excellent discrimination according to [50].

C. PHISHING CAMPAIGN A - STEP 3 (SUBMIT SENSITIVE DATA)

Binary logistic regression was performed to ascertain the effects of age, gender, and personality traits on the likelihood that users will submit sensitive data. The linearity of the continuous variables with respect to the logit of the dependent variable (data submitted) was assessed using the Box-Tidwell [48] procedure. Bonferroni correction was applied using all 14 terms in the model resulting in statistical significance being accepted when p <.003571 [49]. Based on this assessment, all continuous independent variables were linearly related to the logit of the dependent variable. There were 12 standardized residuals which were kept in the analysis.

The logistic regression model was statistically significant, $\chi 2(7) = 121.213$, $p < .0005$. The model explained 40.7% (Nagelkerke R2) of the variance in the sensitive data submission and correctly classified 86.6% of the cases.

The sensitivity was 26.9%, specificity was 96.5%, positive predictive value was 56.2% and negative predictive value was 88.8%.

All the personality traits were statistically significant (Table 6). Increasing openness and conscientiousness was associated with a decreased likelihood of sensitive data submission while increasing extraversion, agreeableness and neuroticism were associated with an increase in the likelihood of submitting sensitive data.

TABLE 6. Logistic Regression Predicting Likelihood of Submitting Sensitive Data Based on age, gender and personality traits.

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
							Lower	Upper
Age	-0.011	0.023	0.204	1	0.652	0.989	0.945	1.036
Gender	-0.191	0.349	0.299	1	0.585	0.826	0.417	1.637
O	-0.072	0.017	18.861	1	0.000	0.931	0.901	0.961
C	-0.065	0.017	15.386	1	0.000	0.937	0.907	0.968
E	0.075	0.017	19.565	1	0.000	1.078	1.043	1.114
A	0.100	0.020	26.029	1	0.000	1.106	1.064	1.149
N	0.063	0.018	12.961	1	0.000	1.065	1.029	1.102
Constant	-7.330	2.031	13.022	1	0.000	0.001		

The area under the ROC curve was .886 (Fig. 5) (95% CI,.853 to .919), which is considered excellent discrimination according to [50].

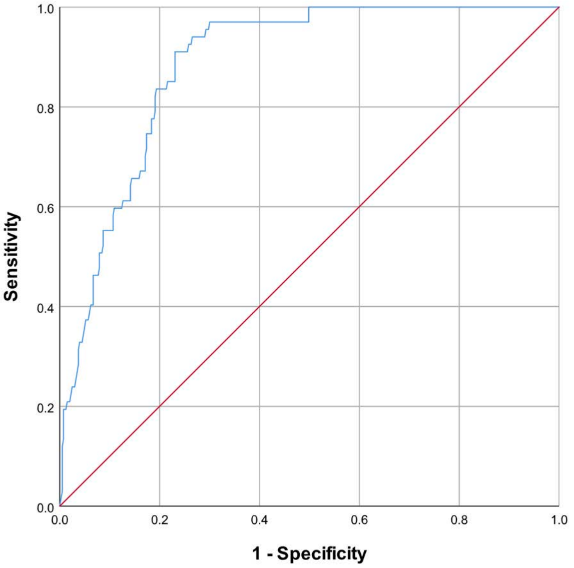

FIGURE 5. ROC curve for predicting the Data submission step.

D. PHISHING CAMPAIGN B - STEP 1 (EMAIL OPENED)

Binary logistic regression was performed to ascertain the effects of age, gender, and personality traits on the likelihood that users will open the phishing email. The linearity of the continuous variables with respect to the logit of the dependent variable (email opened) was assessed via the Box-Tidwell [48] procedure. Bonferroni correction was applied using all 14 terms in the model, resulting in statistical significance being accepted when p <.003571 [49]. Based on this assessment, all continuous independent variables were found to be linearly related to the logit of the dependent variable. There were five standardized residuals, which were kept in the analysis. The logistic regression model was statistically significant, $\chi 2(7) = 54.761$, $p < .0005$. The model explained 15.2% (Nagelkerke R2) of the variance in the email-opening action and correctly classified 66.8% of the cases. The sensitivity was 88.3%, specificity was 25.9%, positive predictive value was 69.3% and negative predictive value was 53.8%. Increasing agreeableness and neuroticism was associated with an increased likelihood of opening the phishing email while an increase in openness and conscientiousness was associated with a decrease in opening the email (Table 7).

TABLE 7. Logistic Regression Predicting Likelihood of Opening the Phishing Email Based on Age, Gender and Personality Traits.

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
							Lower	Upper
Age	0.016	0.012	1.571	1	0.210	1.016	0.991	1.041
Gender	0.254	0.228	1.238	1	0.266	1.289	0.824	2.014
O	-0.046	0.011	18.605	1	0.000	0.955	0.935	0.975
C	-0.035	0.010	11.713	1	0.001	0.965	0.946	0.985
E	0.019	0.011	3.169	1	0.075	1.019	0.998	1.041
A	0.032	0.011	8.525	1	0.004	1.033	1.011	1.056
N	0.030	0.011	7.227	1	0.007	1.030	1.008	1.053
Constant	0.082	1.290	0.004	1	0.949	1.086		

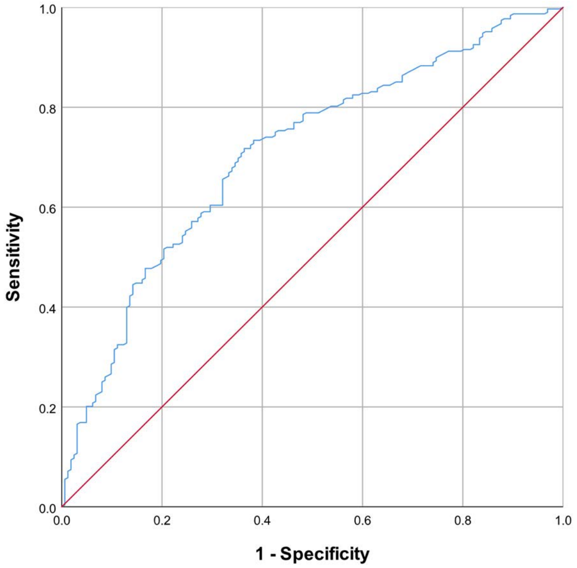

FIGURE 6. ROC curve for predicting the Open Email step.

The area under the ROC curve was .707 (95% CI, .658 to .755), which is considered an acceptable discrimination according to [50].

E. PHISHING CAMPAIGN B - STEP 2 (LINK CLICKED)

Binary logistic regression was performed to ascertain the effects of age, gender, and personality traits on the likelihood that users will click on a malicious link. The linearity of the continuous variables with respect to the logit of the dependent variable (link clicked) was assessed using the Box-Tidwell [48] procedure. Bonferroni correction was applied using all 14 terms in the model resulting in statistical significance being accepted when p <.003571 [49]. Based on this assessment, all continuous independent variables were linearly related to the logit of the dependent variable. Ten standardized residuals were retained in the analysis.

The logistic regression model was statistically significant, $\chi 2(7) = 101.256$, $p < .0005$. The model explained 31.8% (Nagelkerke R2) of the variance in the link clicking action and correctly classified 82.1% of the cases.

The sensitivity was 23.8%, specificity was 94.8%, positive predictive value was 50% and negative predictive value was 85.1%.

All the personality traits were statistically significant (Table 8). Increasing openness and conscientiousness was associated with a decreased likelihood of clicking the malicious link while increasing extraversion, agreeableness and neuroticism were associated with an increased likelihood of clicking the link.

TABLE 8. Logistic Regression Predicting Likelihood of Link Clicking Based on Age, Gender and Personality Traits.

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
							Lower	Upper
Age	-0.012	0.018	0.416	1	0.519	0.988	0.953	1.025
Gender	0.391	0.304	1.657	1	0.198	1.478	0.815	2.680
O	-0.075	0.015	26.563	1	0.000	0.927	0.901	0.954
C	-0.071	0.014	24.140	1	0.000	0.931	0.905	0.958
E	0.036	0.014	6.517	1	0.011	1.037	1.008	1.066
A	0.045	0.015	8.465	1	0.004	1.046	1.015	1.077
N	0.070	0.016	20.057	1	0.000	1.073	1.040	1.106
Constant	-2.083	1.704	1.494	1	0.222	0.125		

The area under the ROC curve was .84 (Fig. 7) (95% CI,.800 to .881), which is considered an excellent discrimination according to [50].

F. PHISHING CAMPAIGN B - STEP 3 (SUBMIT SENSITIVE DATA)

Binary logistic regression was performed to ascertain the effects of age, gender, and personality traits on the likelihood that users will submit sensitive data. The linearity of the continuous variables with respect to the logit of the dependent variable (data submitted) was assessed using the Box-Tidwell [48] procedure. Bonferroni correction was applied using all 14 terms in the model resulting in statistical significance being accepted when p <.003571 [49]. Based on this assessment, all continuous independent variables were linearly related to the logit of the dependent variable. Sixteen standardized residuals were retained in the analysis.

The logistic regression model was statistically significant, $\chi 2(7) = 76.474$, $p < .0005$. The model explained 34.9% (Nagelkerke R2) of the variance in sensitive data submission and correctly classified 91.9% of the cases.

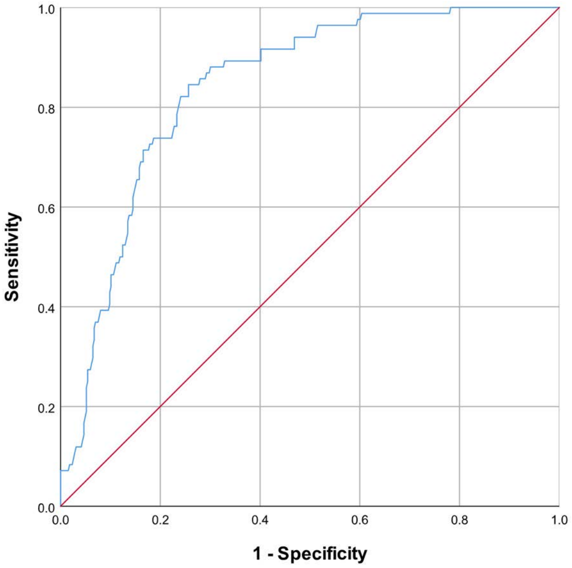

FIGURE 7. ROC curve for predicting the Link Clicking step.

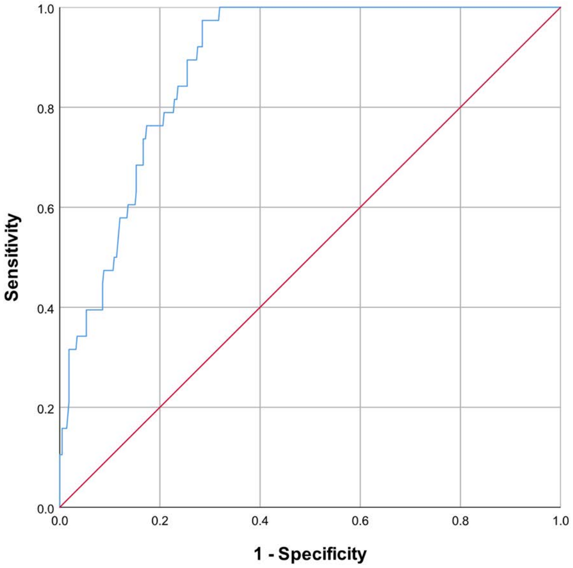

FIGURE 8. ROC curve for predicting the sensitive data submission.

The sensitivity was 18.4%, specificity was 98.4%, positive predictive value was 50% and negative predictive value was 93.2%.

Age was found to be statistically significant. Increasing age was associated with a decreased likelihood of sensitive data submission. Increasing openness and conscientiousness was associated with a decreased likelihood of sensitive data submission, whereas increasing extraversion and neuroticism was associated with an increase in the likelihood of submitting sensitive data (Table 9).

TABLE 9. Logistic Regression Predicting Likelihood of Submitting Sensitive Data Based on Age, Gender and Personality Traits.

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
							Lower	Upper
Age	-0.092	0.032	8.343	1	0.004	0.912	0.857	0.971
Gender	0.696	0.441	2.491	1	0.115	2.006	0.845	4.763
O	-0.066	0.020	10.457	1	0.001	0.936	0.900	0.974
C	-0.072	0.021	12.226	1	0.000	0.931	0.894	0.969
E	0.060	0.021	7.711	1	0.005	1.061	1.018	1.107
A	0.025	0.021	1.401	1	0.237	1.025	0.984	1.068
N	0.114	0.024	22.905	1	0.000	1.121	1.070	1.175
Constant	-3.870	2.541	2.320	1	0.128	0.021		

The area under the ROC curve was .884 (Fig. 8) (95% CI,.847 to .921), which is considered excellent discrimination according to [50].

Additionally, we included the *Submit Data* step results in Phishing Campaign A (as an independent variable) and performed logistic regression again to investigate the recurring behavior of submitting sensitive data despite attending a cybersecurity course.

The linearity of the continuous variables with respect to the logit of the dependent variable (link clicked) was assessed using the Box-Tidwell [48] procedure. Bonferroni correction was applied using all 15 terms in the model, resulting in statistical significance being accepted when $p < .003333$ [49]. Based on this assessment, all continuous independent variables were found to be linearly related to the logit of the dependent variable. Fifteen standardized residuals were retained in the analysis.

The logistic regression model was statistically significant, $\chi 2(8) = 84.153$, $p < .0005$. The model explained 38.1% (Nagelkerke R2) of the variance in the data submission step and correctly classified 93% of cases.

The sensitivity was 21.1%, specificity was 99.3%, positive predictive value was 72.7% and negative predictive value was 93.4%.

People who submitted data before attending a cybersecurity course were 3.4 times more likely to submit data after the course.

Age was found to be statistically significant. Increasing age is associated with a decreased likelihood of sensitive data submission. Increasing openness and conscientiousness was associated with a decreased likelihood of sensitive data submission, whereas increasing extraversion and neuroticism was associated with an increase in the likelihood of submitting sensitive data (Table 10).

The area under the ROC curve was .893 (Fig. 9) (95% CI,.855 to .931), which is considered excellent discrimination according to [50].

The results showed that out of the five personality traits, only neuroticism was statistically significant when considering the open email step (H1a). This suggests that anxiety about negative consequences might play a role when the email's subject denotes importance since this is the only content presented to the target at this stage.

The results support H1b and H1c, as extraversion, agreeableness, and neuroticism are statistically significant and

TABLE 10. Logistic Regression Predicting Likelihood of Submitting Sensitive Data Based on Age, Gender, Previous Sensitive Data Submission and Personality Traits.

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
							Lower	Upper
Age	-0.089	0.032	7.664	1	0.006	0.915	0.859	0.974
Gender	0.761	0.454	2.808	1	0.094	2.141	0.879	5.218
O	-0.055	0.021	6.782	1	0.009	0.946	0.908	0.986
C	-0.064	0.021	8.960	1	0.003	0.938	0.900	0.978
E	0.048	0.022	4.472	1	0.034	1.049	1.003	1.096
A	0.006	0.022	0.081	1	0.776	1.006	0.963	1.052
N	0.108	0.025	18.407	1	0.000	1.115	1.061	1.171
Data Submitted	1.246	0.450	7.660	1	0.006	3.477	1.439	8.404
Constant	-3.372	2.754	1.499	1	0.221	0.034		

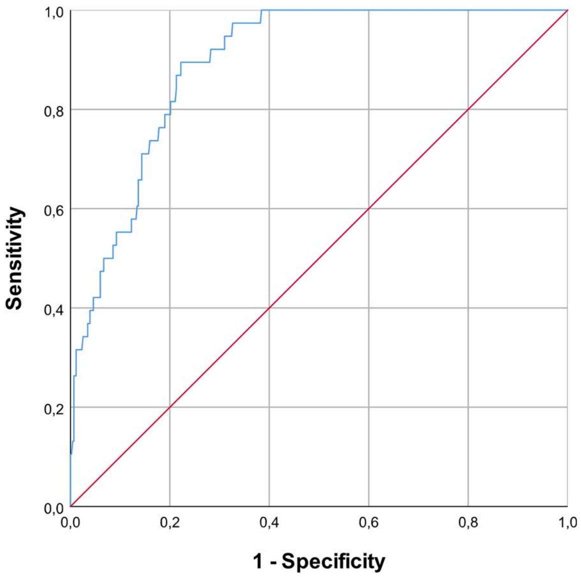

FIGURE 9. ROC curve for predicting the sensitive data submission.

positively correlated with link clicking and sensitive data submission. This suggests that specifically created email content plays an important role in susceptibility to phishing. Furthermore, the remaining traits, openness and conscientiousness, were negatively correlated with the two dangerous actions, further supporting the idea that both traits are associated with responsible behavior regarding security practices.

Although the cumulative success rate of the phishing campaigns dropped after the cybersecurity course (Table 1), all personality traits remained statistically significant at the link-clicking action and sensitive data submission, except for agreeableness, which was statistically insignificant at the sensitive data submission. This suggests that the cybersecurity course might affect the behaviors associated with agreeableness. Non-responder personality traits (low openness, low conscientiousness, and high neuroticism) were statistically significant at the sensitive data submission step following the cybersecurity course, supporting H2. However, extraversion was also statistically significant, suggesting that it also played a role in the non-responder profile. Employees who submitted data before attending the cybersecurity course were three times more likely to submit data after the course.

Increasing age was associated with a decrease in the likelihood of opening the email (before attending the cybersecurity course), which can be explained by the maturity principle that states that people become more emotionally stable with age [37]. Age was also negatively correlated with data submission (after the cybersecurity course). Consequently, H3 is not supported because age appears to play a limited protective role in phishing susceptibility.

Although previous studies have found that women, on average, are more susceptible to phishing [51], [52] and have weaker security behavior intentions [53], gender was not statistically significant in any of the logistic regressions performed during the study. Consequently, we cannot conclude a gender bias towards phishing susceptibility, so H4 is not supported.

V. DISCUSSION

This study shows that when a phishing email is designed to manipulate certain pronounced vulnerable personality traits, statistically significant correlations exist between the presence of individual traits, link clicking and sensitive data submission actions. We took a different approach than traditional phishing, where risk-taking [35] might play a more significant role in phishing susceptibility. instead, we planned and executed a spear-phishing attack with internal knowledge about specific workflows inside the targeted company, including the managerial hierarchy among the targets.

The findings suggest that cybersecurity training only affected the behaviors associated with agreeableness (at the data submission step). Non-responder traits remained statistically significant after the cybersecurity training. Furthermore, the decline in the success rate of the attack following the cybersecurity course suggests an overall organizational awareness increase of phishing. Similar results have been found in the literature [54].

However, our study had some limitations. Although we conducted a phishing campaign as close to reality as possible, we disabled an enterprise-level policy on the images displayed inside the email client to record the email's opening and whitelisted the domains from which the phishing emails were sent. Consequently, the emails looked more legitimate to the users, which is something different from the real setting, where there is an extra step where users are asked if they want to display the images. Another limitation is related to the accuracy of the sensitive data submission. We did not record or verify the credentials submitted; therefore, it may be possible that some individuals submitted false data to test the legitimacy of the cloned identity provider's page. Another limitation is regarding the employees' schedule, and is possible that they did not open the phishing email because they had a day off or vacation, which might have affected the results. We were unaware of other external variables that could affect the users, such as personal stress or technical tools, such as different plugins installed on the browser for phishing detection. The duration of the study was limited, and we had limited visibility or control over the user environments.

VI. CONCLUSION

Spear phishing is a sophisticated targeted attack in which attackers use various sources of information in the attack preparation phase to maximize the success of the attack. The usual strategy employed in these attacks is to convince the target of submitting sensitive data by presenting a convincing page or submission form.

By understanding the reasons behind phishing susceptibility, we can devise methods to protect individuals from attacks. The personality profile of an individual represents an essential instrument, especially in the context of current advances in artificial intelligence-based personality profiling [55]–[57], where an attacker can identify a target's personality traits by using publicly available social media information. Consequently, there is a need to personalize the next generation of phishing prevention solutions. This study is part of a larger effort to create an automatic system that would identify insider threats using these types of services to analyze the employee population, identify vulnerable profiles and further justify security measures.

We designed this study to investigate the impact of personality traits on each phase of a phishing attack. The opening of an email is generally considered safe. Clicking on a link becomes dangerous because 0-day exploits may be used in the attack. Because these attacks are expensive, only high-level targets such as CEOs may represent targets. Submitting sensitive data is the most dangerous phase, and has severe consequences for the targeted company. Future studies could use the same process to create emails to explore the relationships between other vulnerable personality profiles and phishing susceptibility. This can ultimately help to build a complete framework to proactively prevent the success of phishing attacks.

The findings of this study have implications for institutional security management. Companies can address the risks involved in sophisticated attacks by identifying vulnerable personality profiles inside an organization, adapting and promoting specific company policies designed to improve security posture, and providing cybersecurity training regarding phishing (especially for vulnerable users and highly vulnerable employees).

APPENDIX

The phishing campaigns used four different email addresses from temporarily acquired domains. There was close collaboration with the security officers from the target company, and the domains from which the emails were sent were whitelisted. A policy flag was set up such that the images were displayed as soon as the email was opened without any other interaction. The emails were designed to trigger or manipulate impulsivity or social interaction (high extraversion), conformity (high agreeableness), and anxiety regarding negative consequences (high neuroticism).

Phishing Email 1
Subject: Important!
Title: Assertiveness Training
Content: Congratulations!

You have been enrolled by your manager [manager] to participate in our flagship assertiveness training session.

Please confirm your attendance here until the end of the day.

Phishing Email 2
Subject: Important! Review the following documents
Title: Please review the following documents
Content: To ensure our operations' safety and efficiency, you are required to

review the following files: Access Procedure and General Rules.

The files are available here.

Please review the documents and provide your signature by EOD.

Failure to comply will escalate to [manager]
Regards,
Operations Team

Phishing Email 3
Subject: Team Building
Title: It's time for Team Building!
Content: Choose the next team-building location!

You have been selected by [manager] to choose the location of the next team building! Complete the following survey here[link].

Choose wisely!
Cheers,
HR Team

Phishing Email 4
Subject: Approved Software: Response needed
Title: Approved Software: Response needed
Content: To provide better support and better management of the versions and their updates, we have established a list of operating systems and software applications that can run on [company name] computers laptops, desktops, servers, etc.). Any other version, apart from those defined, is strictly forbidden. Please review this list[link] by EOD and confirm that the computer runs only the approved software.

Failure to comply will escalate to [manager]
Regards,
Operations Team.

REFERENCES

[1] *IBM Security X-Force Threat Intelligence Index 2022 Full Report*, Int. Bus. Mach., Armonk, NY, USA, 2022.

[2] J. Borwell, J. Jansen, and W. Stol, "Human factors leading to online fraud victimisation: Literature review and exploring the role of personality traits," in *Psychological and Behavioral Examinations in Cyber Security*. Hershey, PA, USA: IGI Global, 2018, pp. 26–45.

[3] R. Montañez, E. Golob, and S. Xu, "Human cognition through the lens of social engineering cyberattacks," *Frontiers Psychol.*, vol. 11, p. 1755, Sep. 2020.

[4] CERT Insider Threat Team, "Unintentional insider threats: A foundational study," Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Cahier de recherche Tech. Rep. CMU/SEI-2013-TN-022, 2013.

[5] F. Sudzina and A. Pavlicek, "Propensity to click on suspicious links: Impact of gender, of age, and of personality traits," in *Proc. BLED*, 2017, pp. 1–11.

[6] T. Halevi, N. Memon, J. Lewis, P. Kumaraguru, S. Arora, N. Dagar, F. Aloul, and J. Chen, "Cultural and psychological factors in cybersecurity," in *Proc. 18th Int. Conf. Inf. Integr. Web-Based Appl. Services*, Nov. 2016, pp. 318–324.

[7] A. Syarulnaziah, D. L. Kunasegaran, M. Z. Mas'ud, and N. A. Zakaria, "Analysis of phishing susceptibility in a workplace: A big-five personality perspectives," *J. Eng. Sci. Technol.*, vol. 14, no. 5, pp. 2865–2882, 2019.

[8] S. G. A. van de Weijer and E. R. Leukfeldt, "Big five personality traits of cybercrime victims," *Cyberpsychol., Behav., Social Netw.*, vol. 20, no. 7, pp. 407–412, Jul. 2017.

[9] J. L. Parrish, Jr., J. L. Bailey, and J. F. Courtney, "A personality based model for determining susceptibility to phishing attacks," Univ. Arkansas, Little Rock, AR, USA, 2009, pp. 285–296.

[10] P. Lawson, O. Zielinska, C. Pearson, and C. B. Mayhorn, "Interaction of personality and persuasion tactics in email phishing attacks," in *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 61, no. 1. Los Angeles, CA, USA: Sage, Sep. 2017, pp. 1331–1333.

[11] A. Darwish, A. E. Zarka, and F. Aloul, "Towards understanding phishing victims' profile," in *Proc. Int. Conf. Comput. Syst. Ind. Informat.*, Dec. 2012, pp. 1–5.

[12] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11895–11910, 2021.

[13] B. D. E. Raad and M. E. Perugini, *Big Five Factor Assessment: Introduction*. Cambridge, MA, USA: Hogrefe & Huber, 2002.

[14] W. Fleeson and P. Gallagher, "The implications of big five standing for the distribution of trait manifestation in behavior: Fifteen experience-sampling studies and a meta-analysis," *J. Pers. Social Psychol.*, vol. 97, no. 6, pp. 1097–1114, 2009.

[15] N. Pantic and M. Husain, "A decision support system for personality based phishing susceptibility analysis," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 3066–3071.

[16] H. S. Jones, J. N. Towse, N. Race, and T. Harrison, "Email fraud: The search for psychological predictors of susceptibility," *PLoS ONE*, vol. 14, no. 1, Jan. 2019, Art. no. e0209684.

[17] T. Lin, D. E. Capecci, D. M. Ellis, H. A. Rocha, S. Dommaraju, D. S. Oliveira, and N. C. Ebner, "Susceptibility to spear-phishing emails: Effects of internet user demographics and email content," *ACM Trans. Comput.-Hum. Interact.*, vol. 26, no. 5, pp. 1–28, Oct. 2019.

[18] S. Eftimie, R. Moinescu, and C. Racuciu, "Insider threat detection using natural language processing and personality profiles," in *Proc. 13th Int. Conf. Commun. (COMM)*, Jun. 2020, pp. 325–330.

[19] S. V. Paunonen, "Big five factors of personality and replicated predictions of behavior," *J. Pers. Social Psychol.*, vol. 84, no. 2, pp. 411–424, Feb. 2003, doi: 10.1037/0022-3514.84.2.411.

[20] E. Diener, R. E. Lucas, and J. A. Cummings, "16.1 personality traits," in *Introduction to Psychology*. Saskatoon, SK, Canada: Univ. of Saskatchewan, 2019.

[21] S. B. Kaufman, L. C. Quilty, R. G. Grazioplene, J. B. Hirsh, J. R. Gray, J. B. Peterson, and C. G. DeYoung, "Openness to experience and intellect differentially predict creative achievement in the arts and sciences," *J. Pers.*, vol. 84, no. 2, pp. 248–258, Apr. 2016.

[22] B. W. Roberts, J. J. Jackson, J. V. Fayard, G. Edmonds, and J. Meints, "Conscientiousness," in *Handbook of Individual Differences in Social Behavior*, M. R. Leary and R. H. Hoyle, Eds. New York, NY, USA: The Guilford Press, 2009, pp. 369–381.

[23] J. F. Salgado, "The big five personality dimensions and counterproductive behaviors," *Int. J. Selection Assessment*, vol. 10, nos. 1–2, pp. 117–125, Mar. 2002.

[24] D. Watson and L. A. Clark, "Extraversion and its positive emotional core," in *Handbook of Personality Psychology*. New York, NY, USA: Academic, 1997, pp. 767–793.

[25] M. Workman, "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security," *J. Amer. Soc. Inf. Sci. Technol.*, vol. 59, no. 4, pp. 662–674, Feb. 2008.

[26] D. Weirich and M. A. Sasse, "Pretty good persuasion: A first step towards effective password security in the real world," in *Proc. Workshop New Secur. Paradigms*, 2001, pp. 137–143.

[27] S. M. Albladi and G. R. S. Weir, "Personality traits and cyber-attack victimisation: Multiple mediation analysis," in *Proc. Internet Things Bus. Models, Users, Netw.*, Nov. 2017, pp. 1–6.

[28] P. A. Lawson, A. D. Crowson, and C. B. Mayhorn, "Baiting the hook: Exploring the interaction of personality and persuasion tactics in email phishing attacks," in *Proc. Congr. Int. Ergonom. Assoc.* Cham, Switzerland: Springer, Aug. 2018, pp. 401–406.

[29] W. G. Graziano and R. M. Tobin, "Agreeableness," in *Handbook of Individual Differences in Social Behavior*, M. R. Leary and R. H. Hoyle, Eds. New York, NY, USA: The Guilford Press, 2009, pp. 46–61.

[30] D. Modic, D. Modic, and S. E. G. Lea. (Sep. 10, 2012). *How Neurotic are Scam Victims, Really? The Big Five and Internet Scams*. [Online]. Available: https://ssrn.com/abstract=2448130, doi: 10.2139/ssrn.2448130.

[31] D. H. Barlow, K. K. Ellard, S. Sauer-Zavala, J. R. Bullis, and J. R. Carl, "The origins of neuroticism," *Perspect. Psychol. Sci.*, vol. 9, no. 5, pp. 481–496, Sep. 2014.

[32] R. E. Settles, S. Fischer, M. A. Cyders, J. L. Combs, R. L. Gunn, and G. T. Smith, "Negative urgency: A personality predictor of externalizing behavior characterized by neuroticism, low conscientiousness, and disagreeableness," *J. Abnormal Psychol.*, vol. 121, no. 1, pp. 160–172, Feb. 2012.

[33] P. Lopez-Aguilar and A. Solanas, "Human susceptibility to phishing attacks based on personality traits: The role of neuroticism," in *Proc. IEEE 45th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jul. 2021, pp. 1363–1368, doi: 10.1109/COMPSAC51774.2021.00192.

[34] J.-H. Cho, H. Cam, and A. Oltramari, "Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis," in *Proc. IEEE Int. Multi-Disciplinary Conf. Cogn. Methods Situation Awareness Decis. Support (CogSIMA)*, Mar. 2016, pp. 7–13.

[35] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process," *IEEE Access*, vol. 9, pp. 44928–44949, 2021.

[36] T. Schwaba, W. Bleidorn, C. J. Hopwood, S. B. Manuck, and A. G. C. Wright, "Refining the maturity principle of personality development by examining facets, close others, and comaturation," *J. Pers. Social Psychol.*, vol. 122, no. 5, pp. 942–958, 2022.

[37] A. L. Van den Akker, M. Dekovic, J. Asscher, and P. Prinzie, "Mean-level personality development across childhood and adolescence: A temporary defiance of the maturity principle and bidirectional associations with parenting," *J. Pers. Social Psychol.*, vol. 107, no. 4, p. 736, 2014.

[38] M. G. Luchs and T. A. Mooradian, "Sex, personality, and sustainable consumer behaviour: Elucidating the gender effect," *J. Consum. Policy*, vol. 35, no. 1, pp. 127–144, Mar. 2012.

[39] *Spear Phishing Report 2021*, Tessian Res., San Francisco, CA, USA, 2021.

[40] *Decas*. Accessed: Feb. 5, 2022. [Online]. Available: https://www.decas.ro/

[41] D. A. Cobb-Clark and S. Schurer, "The stability of big-five personality traits," *Econ. Lett.*, vol. 115, no. 1, pp. 11–15, Apr. 2012.

[42] G. Berger and A. Fritzler. (2016). *Measuring The Professional Gender Gap*. Accessed: May 5, 2022. [Online]. Available: https://www.linkedin.com/pulse/measuring-professional-gender-gap-guy-berger-ph-d-/

[43] *Discovering Personality With Dr. Jordan B. Peterson*. Accessed: Jan. 2, 2022. [Online]. Available: https://courses.jordanbpeterson.com/

[44] Kaggle. *Spear Phishing Susceptibility Study*. Accessed: Jun. 1, 2022. [Online]. Available: https://www.kaggle.com/datasets/5abb90203db58b6fa5e3a5e8a4ac51e641b9bd17122c65a0bdbf3eacbc0331c4

[45] *Sendinblue*. Accessed: Jun. 1, 2022. [Online]. Available: https://sendinblue.com/

[46] Laerd Statistics. (2017). *Binomial Logistic Regression Using SPSS Statistics. Statistical Tutorials and Software Guides*. [Online]. Available: https://statistics.laerd.com/

[47] S. Gokmen, R. Dagalp, and S. Kilickaplan, "Multicollinearity in measurement error models," *Commun. Statist., Theory Methods*, vol. 51, no. 2, pp. 474–485, Jan. 2022.

[48] G. E. P. Box and P. W. Tidwell, "Transformation of the independent variables," *Technometrics*, vol. 4, no. 4, pp. 531–550, Nov. 1962.

[49] B. G. Tabachnick and L. S. Fidell, *Using Multivariate Statistics*, 6th ed. Harlow, U.K.: Pearson, 2014.

[50] D. W. Hosmer, Jr., S. Lemeshow, and R. X. Sturdivant, *Applied Logistic Regression*, 3rd ed. Hoboken, NJ, USA: Wiley, 2013.

[51] T. Halevi, N. Memon, and O. Nov. (Jan. 2, 2015). *Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks*. [Online]. Available: https://ssrn.com/abstract=2544742,doi: 10.2139/ssrn.2544742.

[52] K. W. Hong, C. M. Kelley, R. Tembe, E. Murphy-Hill, and C. B. Mayhorn, ‘‘Keeping up with the Joneses: Assessing phishing susceptibility in an email task,’’ in *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 57, no. 1. Los Angeles, CA, USA: Sage, 2013, pp. 1012–1016.

[53] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, ‘‘Correlating human traits and cyber security behavior intentions,’’ *Comput. Secur.*, vol. 73, pp. 345–358, Mar. 2018.

[54] A. J. Burns, M. E. Johnson, and D. D. Caputo, ‘‘Spear phishing in a barrel: Insights from a targeted phishing campaign,’’ *J. Org. Comput. Electron. Commerce*, vol. 29, no. 1, pp. 24–39, Jan. 2019.

[55] *Symanto*. Accessed: Apr. 11, 2022. [Online]. Available: https://www.symanto.com/

[56] *Humantic AI*. Accessed: Jun. 1, 2022. [Online]. Available: https://humantic.ai/

[57] *Crystal Knows*. Accessed: Jun. 1, 2022. [Online]. Available: https://www.crystalknows.com/

SERGIU EFTIMIE (Graduate Student Member, IEEE) received the master’s degree in computer and information systems security/information assurance, in 2013. He is currently pursuing the Ph.D. degree with the Military Technical Academy ‘‘Ferdinand I,’’ Bucharest. He has over ten years of experience in the IT, information security, and software development fields in the financial, automotive, and aerospace sectors. His research interests include social engineering and psychological aspects of cybersecurity.

RADU MOINESCU received the master’s degree in security and defense studies from the Faculty of Political Science, Dimitrie Cantemir Christian University, and the master’s degree in security of IT systems and networks from the Faculty of Informatics, Titu Maiorescu University. He is currently pursuing the Ph.D. degree with the Military Technical Academy ‘‘Ferdinand I.’’ He has over 15 years of experience in IT, information security, and radio communication. He holds several professional certifications, including management of cryptographic material, handling, use, and protection. His research interests include social engineering, psychological aspects of cybersecurity, and advanced methods of data exfiltration.

CIPRIAN RĂCUCIU (Member, IEEE) is currently a Full Professor with over 34 years of experience in higher education. He also supervises the Ph.D. research at the Military Technical Academy ‘‘Ferdinand I.’’ His research interests include coding information methods, information security methods, communications security systems, and radio-relay communications systems. He has managed several international research projects and has published 15 books and numerous journal articles. He has held several positions, such as the International Relations and Community Programs Institutional Coordinator, the Director of International Relations Department, and the Head of the Communications Department.