Impact of Security Awareness on Phishing Susceptibility

Basit Abbas
Dept computer science
Jessup university
San Jose, US
basit.abbas@jessup.edu

***Abstract*— Phishing attacks are one of the most common and harmful cybersecurity threats to a higher-ed organization, as they rely on a human factor instead of technical weaknesses. Security awareness training programs are widely used by universities to minimize this threat, although there has been mixed empirical evidence on such programs. Such inconsistency points to the necessity of data-based assessment based on rigorous statistical techniques. The current research question is to determine the relationship between engagement in security awareness training and decreased phishing vulnerability among university users.**

***This research is conducted based on a quantitative research design and uses a publicly available dataset of phishing simulations that represents users with university affiliations. The people are classified in terms of training (trained and untrained) and response behavior that is observed (clicked and not clicked). A chi-square test of independence is used to test the presence of a statistically significant relationship between training attendance and phishing response behavior. Effort effect size is also measured using Cramer's V in the assessment of the strength of the association. The analysis of descriptive statistics and contingency tables is used to aid the interpretation of the results.**

***The findings reveal the statistical significance of the relationship between security awareness training and phishing vulnerability, as trained users showed a lower propensity to respond to phishing emails than did the untrained users. The findings offer empirical evidence for the practicality to continue and enhance the security awareness programs in academic settings. Besides statistical analysis, this study also incorporates ethical and Christian aspects because of the focus on integrity in the processing of data, responsible interpretation of findings, and responsible handling of information. This research, the work of which is reviewed in this article, is important to the field of behavioral cybersecurity and presents somewhat useful implications in terms of enhancing institutional cybersecurity education practices.**

***Keywords*—Security Awareness Training, Phishing Susceptibility, Cybersecurity Behavior, Social Engineering Attacks, Information Security Management, Cybersecurity Education**

I. Introduction

A. Background of the Study

The high rate of digital transformation among institutions of higher learning has significantly increased their dependence on networked systems, cloud computing, and electronic communication platforms. The use of email, learning management systems, digital libraries, and collaborative tools by universities has become widely used in supporting academic teaching and learning, research, and administrative functions. Although these technologies have enhanced access, as well as operational efficiency, they have also increased the cybersecurity of attack surface in an academic setting. Recent industry and governmental reports indicate that higher-education institutions were common victims of cyberattacks because they are open networks, have a decentralized form of governance, and different users are represented in them [1], [2]. Phishing attacks are one of the most popular and widespread types of cyber-attacks that are used to attack institutional systems.

Phishing attacks are based on social engineering mechanisms and not on technical exploitation. Attackers use the identity of trusted parties to cheat users into revealing their credentials, download malicious files, or gain unauthorized access to confidential systems. Human cognitive factors, including trust, perception of urgency, workload, and experience with digital communication patterns, have been found to have a strong effect on phishing success [3], [4]. Universities are highly vulnerable due to the frequency of communication in the form of emails amongst students, faculty, and employees of the university with both internal and external entities. The culture of openness and collaboration among academics also enhances the chances of misleading messages, particularly when they are seen as having been conveyed by the institutional authorities or academic partners [5].

In a bid to deal with the anthropocentricity of phishing attacks, security awareness training programs have been adopted by universities in large numbers to train users on how to detect and act on malicious emails. In these programs, instructional modules, policy briefings, and simulated phishing exercises will usually be involved to strengthen safe-online behavior. Even though such initiatives are regarded as an essential element of institutional cybersecurity strategies, their efficacy is highly debated even in the research community. Several studies report on the enhancement of user awareness in the aftermath of training, although there is a lack of evidence of maintenance of behavioral change [6],[7]. This ambiguity highlights the importance of empirical and data-based analysis of the results of training. In its turn, the proposed study explores the idea of whether engagement with security awareness training statistically significant impacts on decreased phishing vulnerability in university users through the application of rigorous quantitative analysis must inform evidence-based cybersecurity decision-making.

B. Cybersecurity Threat Landscape

Colleges and universities exist in a very special cybersecurity context, which includes open networks, decentralized management, and a vastly heterogeneous client base. Thousands of users of institutions, such as students, faculty, researchers, and administrative personnel, access institutional systems through various locations and personal devices supported by universities. This transparency, as necessary to academic cooperation, comes with major security problems. The education sector is traditionally listed among the most frequently attacked industries by cyberattacks, and phishing, credentials theft, ransomware, and data breaches are observed at a growing rate [8],[9]. Institutional vulnerability is further improved by limited cybersecurity budget, legacy systems, and uneven compliance with policies.

According to recent threat intelligence reports, phishing is the most popular first-strike attack when it comes to breaches of academic institutions. Institutional branding, academic calendars, and repetitive processes of administration are often used by attackers to create believable phishing messages.

Some examples are fraudulent learning-management system messages, scholarship messages, payroll messages, and messages on research collaborations. Such attacks are usually planned at strategic times, like in examination weeks or enrollment processes, to enhance the chances of errors by the users [10],[11]. As opposed to technical exploits, which can be solved with a patching or intrusion detection system, phishing attacks circumvent perimeter defenses by attacking users directly, which is extremely hard to stop with purely technical controls.

Besides financial and operational interference, a successful phishing attack may lead to catastrophic results for universities, such as data breaches, theft of intellectual property, and harm to their reputation. Research has indicated that compromised academic credentials are usually recycled in various platforms, which facilitates the lateral flow and longevity across institutional networks [12]. This leads to the fact that human-centered defenses are becoming more popular with cybersecurity frameworks alongside technical protection. The changing nature of the industrial risk in the sphere of higher learning is thus critical in determining the importance of security awareness training and the need to conduct empirical research on its efficacy. The study identifies phishing vulnerability as a significant behavioral risk factor in the general cybersecurity threat landscape among academic institutions.

TABLE I. TYPICAL CYBERSECURITY ATTACKS IN UNIVERSITY-LEVEL INSTITUTIONS

Threat type	Description	Typical Impact
Phishing	Fraudulent emails against users	Credential theft, breach of the system.
Ransomware	Malware that encrypts institutional data	Service disruption, monetary loss.
Credential Reuse	Stolen passwords interplatform use	Lateral movement, data breach.
Insider Threats	Malicious/Negligent users	Data leakage, policy breach.

Type of threats Description Typical effect.

C. Human Factors in Phishing

Phishing attacks are also inherently human-oriented and human-based attacks, with their success slightly based on psychological manipulation, but not by technical exploitation. The behavioral cybersecurity research has continuously shown that cognitive processes, emotional, and contextual perceptions of users are the determining factors of phishing vulnerability [13],[14]. The perceived authority levels, a sense of urgency, being accustomed to communication patterns, and fear of negative outcomes are some of the factors that are often abused by attackers. Phishing messages may also pose as an instructor, administration, or research partner, and they can use this reputation to evade suspicion in an academic context [15]. These features render phishing especially efficient against consumers who might be technologically sophisticated yet could be susceptible to social engineering schemes.

There are also cognitive limitations and situational pressures, which make people especially vulnerable to phishing attacks. Research indicates that users with limited time, mental congestion, or stress consider deciding heuristically rather than critically by assessing the authenticity of the message [16]. University receivers often read e-mails concurrently or with academic time pressure, thus diminishing their capacity to recognize deceit. Moreover, frequent exposure to legitimate institutional messages may desensitize the users so that it becomes harder to tell the difference between bad and good messages. These results imply that the aspect of phishing vulnerability is not only a factor of knowledge deficiency but is also heavily dependent on human behavior and environmental background [17].

Human-factor studies also emphasize that being aware does not ensure secure behavior. Although users might have an intellectual understanding of the dangers of phishing, compliance in behavior is not always consistent, especially over time. It has been empirically found that security knowledge is lost in the absence of reinforcement, and users are likely to revert to risky behavior when deprived of constant training and feedback [18],[19]. This disjunction of awareness and action makes it more significant to assess security training of awareness not only in terms of the level of knowledge gained but also the level of behavioral performance observed. As a result, the evaluation of phishing vulnerability based on the quantifiable reaction of the users offers a better measure of the training efficiency of the said program and justifies the necessity of the statistically based evaluation in the context of cybersecurity research.

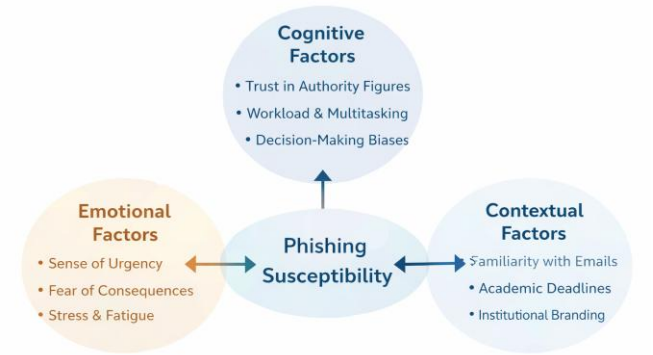

Fig. 1. Human factors influencing phishing susceptibility.

D. Role of Security Awareness Training

Awareness training on security has been a major element in organizational cybersecurity measures, especially in an environment where there is inevitable human interaction with digital systems. Such training programs are implemented in higher-education institutions to provide users with knowledge and skills to identify phishing activities, familiarity with institutional security policies, and also respond to suspicious messages in the most relevant manner. Some of these common training methods are online learning modules, informational campaigns, policy briefings, and simulated phishing exercises. These efforts are based on the hypothesis that a better-informed person will act more safely and be less vulnerable to social engineering attacks [20],[21]. Consequently, it has led to the popular view of security awareness training as a base layer of defense that complements technical measures, including email filtering and intrusion detection systems.

The success of security awareness training programs is one such area of controversy in cybersecurity research, even though it is widely used. Although several studies outline short-term gains in user awareness and a decline in phishing click rates after training, the results of long-term behavioral differences are less evident [22],[23]. Other theorists have stated that conventional and compliance-driven training methods could enhance knowledge without adequately affecting real-life decision-making under stress. Others also observe that the behavior of users can decrease with time due to diminished vigilance, especially when the training is spreading [24]. All these points imply that awareness training is probably not effective, unless it is supported by constant interaction, relatability, and feedback control.

The effectiveness of security awareness training would then have to be empirically determined based on objective, behavioral measures instead of subjective, perception-based, or knowledge tests. The simulated phishing campaigns have become a popular system of gauging against the vulnerability of users, with the ability to record visible responses like the

selection of links or the provision of credentials [25]. Current research, however, is based on descriptive statistics without involving a rigorous inferential test to arrive at the conclusion of a statistically significant result between trained and untrained users. This gap indicates that a quantitative assessment is necessary by applying the right statistical methods. This study, in this regard, will use a chi-square test of independence to test the hypothesis that engagement in security awareness training and phishing vulnerability is related to determining how effective training has been in an academic institution.

TABLE II. COMMON SECURITY AWARENESS TRAINING METHODS IN HIGHER-EDUCTIONAL INSTITUTIONS.

Training Style	Explanation	Resultant Outcome
Online Modules	Self-paced instructional content	Knowledge acquisition
False Phishing	Controlled phishing emailing campaigns	Behavioral testing
Policy Briefings	Institutional security policy	Policy compliance
Continuous Training	Reinforcement activities periodically	Change behavior in the long term.

E. Research Motivation and Significance

The rising rates and complexity of phishing activities against institutions of higher learning highlight the necessity to develop evidence-based cybersecurity practices. Although universities have been spending a lot of resources on security awareness training programs, institutional decision-makers usually have little strict empirical evidence that can be used to assess whether the investments yield any significant impacts in reducing user vulnerability. Current literature often uses descriptive statistics or short-term observations, which provide little information about whether the differences in phishing behavior are statistically significant and whether they remain statistically significant as time passes [26],[27]. The rationale behind this study is the necessity to go beyond assumptions and anecdotal data by using formal statistical analysis to determine the correlation between security awareness training and phishing vulnerability.

Academically, the present study will be a contribution to the research on human-centered cybersecurity that is growing in number because it combines behavioral analysis with statistical approaches. Using the chi-square test of independence, the study offers a research methodologically sound way of assessing the relationship between categorical variables that are typical of cybersecurity data. The fact that the analysis also includes the effect size contributes to making the results more interpretable, responding to the demands of the literature that requires more analytical frameworks to be used in the context of security awareness studies [28].

This research is of more than methodological value, extending to practical as well as ethical aspects. Evidential data on the effectiveness of training could be used to design the training, schedule the training, and the content of the training, so that universities could better utilize their resources and lessen the risk of social engineering attacks. In addition, this study complies with ethical and Christian values that assume accountable stewardship of information, safety of research participants, and research integrity [29].

F. Research Objectives and Research Questions

The main aim of the research is to test empirically whether security awareness training is related to low phishing vulnerability among university users. Although previous research examined the awareness of phishing and user behavior, most of them do not include an inference analysis that would show statistically significant correlations between training programs and measurable data [6],[22],[28]. This paper fills this gap by discussing the quantifiable behavioral results obtained from phishing-simulation information and utilizing the relevant statistical testing to provide evidence-based conclusions. The study will have methodological transparency and adherence to the scientific method by formulating research objectives and questions clearly and transparently that is applicable in research on computer science.

1) Research Objectives

The following are the specific objectives of this research:

- To investigate the correlation between the level of awareness training on security and phishing behavioral patterns among users of a university.
- To use the chi-square test of independence to define whether observed dissimilarities among the trained and untrained users are significant.
- To determine the intensity of the relationship between training and phishing susceptibility on the effect size (V of Cramer).
- To provide empirical data to the human-centered cybersecurity studies in the academic setting.
- To offer practical knowledge that could be used to guide the development and analysis of institutional security awareness campaigns.

All these objectives are aimed at supporting a systematic, quantitative study of the efficacy of security awareness training as a human-centric measure of cybersecurity control.

2) Research Questions

Based on the objectives mentioned, this research aims to provide the following research questions:

- RQ1: Can the security awareness training status be statistically significantly linked to phishing susceptibility among the users of the university?
- RQ2: How is security awareness training related to the observable phishing response behavior?
- RQ3: What is the strength of the relationship between training attendance and vulnerability to phishing, assessed based on effect size?

Answering these questions, the research will go beyond the descriptive observations and offer statistically justified answers to the question concerning the role of training in the reduction of phishing risks. These questions are directly answered to formulate the hypothesis and choose the suitable statistical tools, which are mentioned in the following chapters.

G. Research Motivation and Significance

This research will have a narrow focus, which is carefully framed to provide an analytical focus, methodological intensity, and focus on the mentioned research objectives. The researcher concentrates only on phishing vulnerability among higher-educational settings, and specifically, university-linked users, including students, faculty, and staff. The relationship between security awareness training status and noticed phishing response behavior is analyzed using the categorical variables obtained based on phishing-simulation. The focus on this setting allows the research to deliver specific knowledge and information that can apply to academic institutions in general, but the results cannot be directly applied to corporate or governmental settings with different organizational structures and security culture [2],[5].

Methodologically, the study is restricted to a quantitative study design that is observational and secondary data. It is not a causal analysis, but rather an evaluation of the statistical association between variables. By this, the findings show the relationship between training status and phishing vulnerability, and not that training is the cause of lowering phishing susceptibility. The study also considers one behavioral outcome, phishing click behavior, which albeit is a generally accepted behavioral indicator in terms of user susceptibility, fails to describe all aspects of user security behavior, including reporting suspicious emails or behavioral adaptation over time [6],[25].

The analysis used in this study has been based on several assumptions. First, we assume that the phishing-simulation data set is a good representation of the real-world phishing cases experienced by university users. Second, an assumption is made that the training status has been accurately documented, and those users labeled as being trained have gone through similar security awareness programs. Thirdly, the chi-square test of independence assumes that the observations are independent, and the expected frequencies of cells are large enough to make sound statistical inferences [28]. These assumptions are clearly recognized so as to provide transparency and so that the findings could be interpreted with clarity. The explicit scope and assumptions used in this research allow setting achievable limits and enhancing the validity and generalizability of its analysis method.

H. Organization of the Paper

The paper will be organized in such a way that it individually looks at the effectiveness of security awareness training in decreasing phishing vulnerability in a higher-education setting. The chapters are structured in a way that each chapter logically follows the last in a manner that would bring about clarity, methodological rigor, and coherence in the whole study.

Chapter 1 provides the background of the study by setting out the general understanding of the cybersecurity environment in higher education, the human factor behind phishing attacks, and providing the purpose, target, scope, and importance of the study. This chapter offers the conceptual background that would enable one to comprehend the research problem and the reasons why empirical research is required.

Chapter 2 is a literature review, which summarizes previous studies on phishing attacks, human-centered cybersecurity, and security awareness training. It critically analyzes current methodologies, current findings, and current limitations, research gaps, and locates the current study in the overall array of computer science and cybersecurity research.

Chapter 3 describes the research methodology, which includes the research design, definition of the variables, hypothesis formulation, and statistical procedures used. The rationale behind the choice of the chi-square test of independence as the main form of analytical activity is explained in this chapter, along with the conceptual explanation of other types of statistical tests to be aware of the methodology.

Chapter 4 explains the data collection method and the nature of data to be used, including the sources, sampling, procedures of preprocessing data, and professional ethics of operating the data. This chapter creates transparency and reproducibility as per set standards of research.

Chapter 5 details of findings of the statistical analysis are provided with descriptive statistics, contingency tabular results, the findings of the chi-square test, the measures of effect size, and the visualization. Chapter 6 gives these findings an interpretation, compares them to the current literature, remarks on implications, and discusses the limitations and threats to validity.

Chapter 7 incorporates the use of Christian and ethical aspects into the research discussion, focusing on integrity, stewardship, and responsible reporting of results. Lastly, Chapter 8 wraps up the paper by concluding principal findings, making contributions to computer science research, and suggesting the way forward for future work.

I. Importance of Human-Centered Cybersecurity Research

Over the past few years, cybersecurity studies have come to appreciate the fact that technical defenses are no longer adequate to deal with the threat of phishing attacks, which are taking a new form. After the development of email filtering, intrusion detection systems, and automated threat intelligence, phishing has remained successful mainly because it can exploit human behavior and thinking instead of the vulnerability of systems. This change has led to an increased literature on the need to approach cybersecurity research in a more humanistic manner, such that users become an active part of the security ecosystem and are no longer seen as a source of risk. This focuses on learning about user perceptions of threats and their decisions under uncertainty and reaction to security interventions, and as a result, supplements existing technical controls with behavioral information [41], [42].

Human-centered cybersecurity studies are important because they allow closing the gap between security design and actual user behavior. Research has shown that security mechanisms that do not consider human factors usually result in workarounds, non-compliance, or risk-compensating behavior, which compromise the overall system of security [43]. Human-centered research offers a more comprehensive idea of phishing vulnerability by incorporating behavioral analysis, risk profiling, and training evaluation. This attitude also directly guides the current research that does not simply consider security awareness training as a compliance measure but as a form of behavioral intervention, the effectiveness of which should be empirically measured.

J. Research and Practice Contribution of the Study

This research is relevant to the literature on cybersecurity as it gives a quantitative and behavioral analysis of the effectiveness of security awareness training in an academic setting. Although there are many studies on the problem of phishing and user education on a conceptual scale, fewer studies use strict statistical analysis on observable user behavior based on real or simulated phishing data. The study enhances the empirical basis under the assessment of human-centric security controls by applying the categorical data analysis, interpretation of the effect size, and robustness tests. Also, it orchestrates risk stratification and trend analysis with previous research that tends to use dichotomous groups of user behavior to analyze phishing vulnerability, which provides a more detailed perspective of phishing vulnerability [19], [36], [41].

From a practical perspective, the research can offer practical information to institutions aiming at developing, evaluating, and refining cybersecurity training initiatives. The results help to justify decisions based on data because they show the relationship between training attendance and the quantifiable decrease in the likelihood of falling victim to phishing and present the group of users that could receive specific interventions. Moreover, the consideration of the ethical and Christian values makes the research have a clear difference, as it clearly covers the ethical issues of responsibility in the management of user data and behavioral influences using technology. The paper can be applied both in academic research and in institutional cybersecurity practice to enhance the importance of evidence-based, human-centered security practices [30], [42], [44].

II. Literature Review

A. Overview of Pishing Attacks

A phishing attack can be considered as one of the most widespread and persistent types of cybercrime that consists of fake communication and is intended to influence a user to provide sensitive data or commit an action that undermines the security of the system. Phishing is very flexible and hard to stop solely by technical means, as unlike malware-based attacks, which use technical weaknesses, phishing attacks depend on human belief, societal appearance, and mental shortcuts. Initial literature defines phishing as an identity fraud where offenders masquerade as legitimate entities or persons to obtain unauthorized access to credentials and systems [1],[11]. Phishing methods have, over the years, not only developed to generic mass-email campaigns, but also highly targeted attacks, also known as spear phishing, that utilize the presence of contextual information, including organizational roles, academic affiliation, and ongoing activities, to enhance the credibility of the attack and its success rates [10],[15].

In institutions of higher learning, phishing have been reported to target users in disproportionate numbers because of the open and collaborative communication of academic institutions. Evidence suggests that institutional branding, academic deadlines, and standard administrative processes are often used by the attackers to create persuasive messages that effectively fit in legitimate communication flows [5],[8]. Empirical studies of claims of breaches regularly reveal that phishing constitutes a major initial point of attack in attacks in the education sector, commonly resulting in credential theft, unauthorized access to research information, and subsequent lateral movement on institutional networks [2],[9]. The results help to highlight that phishing should be perceived as not a technical phenomenon but a socio-technical phenomenon, in which the decisive role belongs to human behavior. The necessary mitigation measures are thus on the way to become increasingly focused on the behavioral defenses, which include security awareness training and more on the traditional technical protection as the base of the research interest of the given study.

B. Psychological and Behavioral Underpinnings of Phishing

Phishing is an activity that is strongly based on the manipulation of psychology and capitalizes on the foreseeable behavior of the human mind. Empirical studies have found that people frequently make use of cognitive shortcuts or mental short-circuits to handle information fast, like when they are time-starved or when they are bombarded with information [13],[16]. Attackers purposely construct phishing messages in a manner that they will invoke authority (e.g., faking institutional administrators), urgency (e.g., account suspension notices), or reciprocity (e.g., shared academic documents). Behavioral cybersecurity research also shows that these cues can markedly diminish the capacity of users to critically assess the authenticity of messages, as well as tend to enhance compliance among users with a high level of technical skills [14],[17]. This situation indicates that phishing vulnerability is not a purely technical knowledge issue but diffuses immensely based on natural thoughts and emotional ideas.

The Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) are examples of psychological theories that have been extensively used to elaborate on the motivations behind risky cybersecurity behaviors among users despite their awareness of the threat [18],[28]. According to these models, the perceived threat of severity, self-efficacy, and costs of response determine the reaction of users to phishing attacks. In the academic setting, opposing influences (academic workload and continual digital interaction) can undermine the desire to make a consistent application of security best practices. Empirical research also shows that behavioral improvements may not be maintained without reinforcement when repeatedly exposed to phishing simulations and that user vigilance initially can be enhanced in the same way [6],[19]. These results support the importance of analyzing security awareness training not only as an educative intervention but as a mechanism of behavior control, the usefulness of which should be measured not by self-reported confidence or knowledge but by observable behavior.

C. Security Awareness Training: Model and Effectiveness

Security awareness training programs are aimed at mitigating human-oriented cybersecurity threats through enhancing human capability of identifying and reacting to malicious behaviors. Popular training models are conventional compliance-based training, Interactive e-learning modules, simulated phishing, and continuous reinforcement. Another hypothesis proposed by the previous studies points to the fact that interactive training and context-driven training are typically more effective than policy-based, straight, and simple training, because it involves the users in a cognitively engaging way and give them a chance to learn through the feedback provided on the experience [20],[22]. The simulated phishing campaigns, specifically, have become widespread as a training and gauging device enabling the organizations to evaluate the user behavior during realistic situations as opposed to basing their evaluation on theoretical knowledge examinations only.

Despite such developments, security awareness training is found to be not consistent across studies. Although a range of empirical studies indicates that training interventions can produce a short-term decrease in the rates of phishing clicks, some studies also indicate the decreasing effects of the training interventions over time as users revert to their habitual behaviors [6],[23]. This discrepancy reveals an important weakness of current studies: most of them focus more on the design of training and do not substantiate the results with a thorough statistical test. Consequently, the question of whether the observed improvement is a sign of meaningful behavioral change or a transient compliance due to an increase in vigilance in the short-term following the training is yet to be answered. These results highlight the significance of using inferential statistical tools to assess the effectiveness of training objectively.

TABLE III. PREVIOUS RESEARCH MODELS OF SECURITY AWARENESS TRAINING

Training Model	Description	Reported Effectiveness	Noted Weakness
Compliance-based	Policy-driven instruction	Low–Moderate	Poor engagement
E-learning	Interactive modules	Moderate	Knowledge decay
Simulated phishing	Realistic attack testing	High (short-term)	Resource-intensive
Constant training	Repeated practice	High (long-term)	Needs commitment

D. Academic and Organizational Empirical Studies

Empirical studies on phishing vulnerability have been conducted both within a business and within a scholarly environment, wherein universities have been identified as a unique research environment because they possess an open culture of communication, besides having diverse audiences. Research that has been done in post-secondary institutions shows that students and staff have different degrees of phishing vulnerability, determined by position, experience, and exposure to education [5],[8]. Academic customs are not like corporate surroundings in terms of governance, enforcing apparatus, and accountability of user which can influence the dependability and effects of security interventions. In turn, the

results of corporate-oriented research cannot be directly applied to the realm of universities.

Analytical comparisons of academic and organizational research also prove the variability of the methodology. Although there are studies that utilize a controlled experiment or longitudinal study, certain ones utilize cross-sectional data or self-report surveys, which destroys comparability and generalizability [10],[27]. Also, most such studies have reported descriptive statistics without hypothesis testing on which to determine the presence of statistical significance. Such a methodological gap undermines the evidence that ought to be used to make policy decisions and results in the necessity of standardized analytical methods. This limitation has been overcome in the current study because it focuses on an academic setting and employs a chi-square test of independence to test the behavioral outcomes rigorously.

TABLE IV. OVERVIEW OF PAST PHISHING AND SECURITY AWARENESS RESEARCH

Study	Context	Methodology	Key Findings	Limitations
Sheng et al. (2010)	Academic	Experimental	Demographics influence the vulnerability to phishing	Short-term analysis
Oliveira et al. (2022)	Organizational	Longitudinal	Training decreases initially the click rate	Behavioral decay
Anwar et al. (2020)	University	Observational	Human factors prevail over phishing success	Minimal statistical test
Kumaraguru et al. (2009)	Mixed	Simulation-based	Training Simulation enhances detection	No effect-size analysis

E. Statistical Methods in Understanding the Behavior of Cybersecurity

Quantitative analysis is also a very crucial element in cybersecurity research, especially in assessing human behaviors and training results. Typical tools of statistics are descriptive statistics, regression analysis, testing hypotheses, and machine learning-based classification. Nevertheless, the choice of statistical approaches is an issue relating to the type of data, research purposes, and assumptions. In case the study has categorical behavioral outcomes (as in the case of phishing click behavior), it may be preferable to use non-parametric tests when compared to the parametric ones [28],[30]. Of these, the chi-square test of independence is very popular in testing the relationship between two or more variables of the same type, but without the assumption of normal distribution.

Although it is appropriate, the chi-square test is not fully used or used incorrectly in numerous cybersecurity research works. Other researchers do not state the anticipated frequency, degrees of freedom, or other measures of the effect sizes, thereby restricting the interpretability and reproducibility [6],[31]. Moreover, t-tests, ANOVA, and regression are other statistical tests that might be applied to categorical data without a proper explanation. This discrepancy shows the necessity of methodological renewal and openness in the study of cybersecurity behaviors. This study follows best practices by explicitly explaining the selection of the test and the effect size of reporting statistical significance, in addition to contributing to better analytics in the future.

F. Restrictions on the Reality of Current Studies

One of the limitations observed in phishing and security awareness literature is the inability of short-term analyses to identify long-term behavioral change. Most research evaluates user performance right after training interventions, which can overestimate perceived effectiveness because of increased awareness or the novelty effect [23],[24]. Moreover, self-reported awareness and confidence measures are widely taken as behavior proxies, although it has been proven that perceived competence does not necessarily correlate with secure behavior [18]. Such methodological decisions make it impossible to make strong conclusions regarding the training impact.

The other major limitation is that of data quality and representativeness. Some of the works are based on small sample sizes, convenience sampling, or simulated conditions, which might not be realistic in the real world [27],[32]. The lack of similarity between the definitions of training and phishing success also complicates the comparison of studies across different studies. These problems highlight the need to employ clearly defined variables, a large enough data set, and standardized analysis models. It is necessary to overcome these limitations to further empirical research on cybersecurity and to make evidence-based policy.

G. Research Gaps and Opportunities Identified

According to the literature reviewed, there are some gaps in the research. To begin with, lack of statistically rigorous studies that explicitly test the associations between security awareness training and phishing vulnerability using the right non-parametric methods. Second, there are very few studies that specifically address institutions of higher education, yet they have a risk profile of their own, and they are becoming more susceptible to cyber threats [5],[9]. Third, effect sizes are not often reported, which prevents knowing the practical implications of the observed relationships.

These loopholes offer an obvious contribution. Using the chi-square test of independence on a dataset with a university-specific approach and the addition of significance testing with the help of effect size analysis, the study will overcome the methodological and contextual gaps in the literature. It is also significant to consider ethical and Christian values in the research design and interpretation, which provides a new angle of thinking and places cybersecurity practice in harmony with more universal values of stewardship, responsibility, and service. Such a mixture of methodological purity and moral consideration makes the current study stand out from the previous ones.

H. Abstract of Literature Review and Conceptual Framework

The reviewed literature in this chapter shows that phishing is a long-standing cybersecurity threat that is fueled by human factors and context to a great extent. Although the adoption of security awareness training has become a well-used mitigation measure, there is mottled and uneven empirical evidence as to the effectiveness of security awareness training. Psychological and behavioral studies support the fact that phishing vulnerability is a complex issue, and knowledge is not enough to ensure safe behavior.

To address these findings, this research seems to take a quantitative and behavior-based approach based on rigorous statistical analysis. The theoretical framework used to inform the study puts security awareness training as the independent variable that dictates the level of phishing vulnerability, and the level of user behavior is observed in terms of actions. This framework guides the methodology of decisions in the next chapter and serves as a firm justification of the research hypothesis and analysis of data.

Fig. 2. Conceptual Framework Linking Security Awareness Training to Phishing Susceptibility

A. Human-Centered Risk Modeling of Phishing Research

Recent research has shifted towards the idea that phishing attacks are not just technical performances, but a phenomenon of human-focused risks, in which the cognitive, behavioral, and contextual information of the user becomes the decisive factor in the security results. This view combines the measurements of behavioral science, cybersecurity, and risk modeling to define why technically similar phishing attacks can invoke vastly different user responses in different populations [36], [38]. Human-oriented risk modeling introduces a shift in the analytical emphasis to vulnerabilities of the system in its entirety, instead of concentrating on the interaction between the attackers and the users, which validates the importance of behavioral information related to phishing research.

The major common themes arising out of the literature on human-centered risk modeling are:

1) User Behavior as a Primary Risk Vector

a) Human interaction is always found to be the most abused factor in phishing attacks, in both frequency and overall effect, more often than purely technical vulnerabilities [11], [35].

b) Behavioral indicators in risk models continue to include email engagement, timing of response, and previous exposure to security training [19], [39].

2) Assimilation of Training in Risk Models

a) Security awareness training is often structured as a mitigating control that moderates user vulnerability and does not totally eradicate the risk.

b) According to previous studies, the trained users retain different levels of risk, which supports the idea of tiered or probabilistic risk modeling [6], [36].

3) The Binary Outcomes to Risk Continuums

a) Modern literature rejects dichotomous policies (secure and insecure users), instead promoting risk continua, with users shifting between risk conditions based on their contexts and experience [38], [40].

b) This method is compatible with behavioral cybersecurity models in which situational pressure and cognitive load are dynamic risk factors [14], [18].

Implications of the Analysis to Empirical Research

c) Risk models with a human focus prefer interpretable statistical methods enabling the mapping of behavioral patterns in a transparent way to risk categories.

d) These types of models promote the application of contingency analysis, interpretation of effect size, and stratification of risk, as applied in the current analysis [24], [35].

Integrating these threads of research, this section puts the present study in the context of the changing body of literature that considers phishing susceptibility as a behaviorally mediated risk phenomenon. The focus on training as a moderating factor and observable behavior as a measure of risk directly serves the conceptual framework used in Section 2.8 and the selection of methodological strategies chosen in subsequent chapters. In its turn, this section provides a stronger theoretical basis for the study and explains its role in human-centered cybersecurity research.

I. Behavioral and Technical Approaches to Phishing Research Synthesis.

Phishing mitigation literature could be divided into two broad groups: technical interventions that can be implemented to filter or detect emails and analyze URLs, and behavioral interventions with a focus on user education, awareness, and decision-making. Although technical solutions have proven to be effective in mitigating large quantities of malicious emails, an array of studies have admitted that no automation can be effective in mitigation being perfect, leaving behind open risk which has to be reduced at the human level [2], [7], [31]. Consequently, current research has been moving towards the idea that hybrid forms of cybersecurity, incorporating both technical and behavioral interventions, are needed because users are the ultimate decision-makers when it comes to dealing with potentially misleading information [41], [45].

This combination of behavioral and technical viewpoints brings up a vital observation, which is that phishing resilience is not a phenomenon of single controls but of system-user interplay. Behavioral research demonstrates that reaction to phishing attempts taken by users depends on cognitive biases, previous experience, and context that can strengthen or weaken technical measures [14], [36]. The usefulness of security awareness training, therefore, cannot be well comprehended outside the wider technical context, within which users exist. The current paper is based on this combined view, as it empirically evaluates training results based on observable behavior, thus extending to the literature that attempts to integrate human-centered and system-centered cybersecurity studies instead of making them two distinct fields of study.

Along with conceptual integration, recent research has focused on the operational difficulties of integrating behavioral and technical controls in practice. Technical defenses are typically installed in the background, whereas behavioral interventions involve the active involvement of users and their long-term attention, in which the environment of security experience and security perception asymmetry is inherent [45], [47]. Studies have shown that unawareness of technical protection can result in the development of overconfidence or complacency by the user, but on the other hand, excessive intrusion by security measures may create complacency and diminished trust in warning systems [42], [46]. These results explain why it is necessary to develop cybersecurity measures that align system-level controls with end-user education consistently and understandably. The current research implies this issue because it measures training efficacy in an already-existing technical ecosystem, which can add empirical data to the literature that aims to provide balanced and socio-technical solutions to the issue of phishing.

J. The Fit of the Current Study into Existing Literature.

Placing the current research in the context of the existing research, it is possible to note that it will not only be the continuation of the previous research, but it will also take a step forward and go further. This study, like the previous empirical investigations, has taken note of the fact that phishing can be mitigated through security awareness training, but not completely [6], [12], [39]. Nevertheless, most of the current literature depends on descriptive statistics, self-reported scales, or short-term assessments, which restrict their capacity to execute rigorous evaluations of behavioral effects. Conversely, the present research uses formal statistical tests, effect sizes, and robustness tests to test training effectiveness utilizing behavioral data to fill the methodological gaps detected in 2.6 and 2.7.

Placing the current research in the context of the existing research, it is possible to note that it will not only be the continuation of the previous research, but it will also take a step forward and go further. This study, like the previous

empirical investigations, has taken note of the fact that phishing can be mitigated through security awareness training, but not completely [6], [12], [39]. Nevertheless, most of the current literature depends on descriptive statistics, self-reported scales, or short-term assessments, which restrict their capacity to execute rigorous evaluations of behavioral effects. Conversely, the present research uses formal statistical tests, effect sizes, and robustness tests to test training effectiveness utilizing behavioral data to fill the methodological gaps detected in 2.6 and 2.7.

III. Research Methodology

A. Research Paradigm and Methodological Approach

The study is anticipated to utilize a quantitative paradigm of research based on empirical analysis and statistical inference, which is in line with the traditional research practice in the field of computer science and cybersecurity. Quantitative techniques are especially good to assess the behavioral outcomes on a large scale because they allow objective measurement, testing of hypotheses, and reproducible analysis [30],[31]. Since the research aims to measure the correlation between security awareness training and phishing vulnerability, a quantitative method will enable the systematic study of the observable user behavior instead of the use of subjective perceptions or self-reported information.

The study is also described as a non-experimental and observational study. The analysis does not employ any manipulation of the variables by use of controlled intervention but rather analyzes the existing data that have been obtained by the phishing-simulation results. Such a design can be used when experimental manipulation is put at a disadvantage due to ethical, logistical, or institutional constraints, which is usually the case in academic cybersecurity research [5],[27]. Although observational studies do not prove causality, they are useful in determining statistically significant relationships between variables as well as in producing evidence that can be used to guide policy and future experimental studies. To this end, this study has been interpreted to mean an aspect of association as opposed to a causal effect.

Methodologically, the study is based on the scientific method used in research in computer science: identification of the problem, formulating the hypothesis, data collection, data analysis, and interpretation [32]. Security awareness training status is considered an independent variable, and the relationship between the independent variable and the dependent variable, the phishing susceptibility, is studied with the help of inferential statistical tests, which are suitable when the data are categorical. This study clearly connects the research paradigm with the character of data and research questions, which guarantees methodological consistency, analytical plausibility, and adherence to the best practices of quantitative cybersecurity studies.

B. Research Design and Study Structure

The study design adopted in this research is a cross-sectional and quantitative observational study to investigate the connection between security awareness training and phishing vulnerability in university users. The research examines data gathered at one time of experiment results of phishing simulation and makes a systematic comparison of user behavior in respective categories without the control of experimental situations. The user is the unit of observation, with each observation being a discrete phishing interaction with the training status (trained or untrained) and response behavior (clicked or not clicked). This is the structure that allows organizing observations into a contingency table that represents the common distribution of the two categorical variables being studied and the basis of an inferential test of statistics. In cybersecurity behavior studies, a cross-sectional design is especially suitable, as cross-sectional research enables experimentation on a large scale that may be both unfeasible and ethically limited, but observational data can be an informative source of information on actual user behavior [27],[31]. The research presupposes the independence of observations, that is, the responses of a user are considered to be statistically independent of the others, which is usually the assumption in phishing-simulation data and becomes relevant to the correct usage of the chi-square test of independence [28],[30]. Using his design, the study values empirical transparency, reproducibility, and methodological consistency with the accepted quantitative research practices in the field of computer science; although the results suggest statistical correlation as opposed to causation.

C. Variables and Operational Definitions

To achieve accuracy in analysis and reproducibility, this paper analyzes the association between the variables of security awareness training and the vulnerability to phishing using clear and operationally defined variables. Security awareness training status, which will be a dichotomous measure in that the user is trained or untrained, is independent of whether the user has attended an institutional security awareness training program before the phishing simulation. The dependent variable is phishing susceptibility, which is operationalized as the behavioral manifestation of the user on a phishing email, which is either clicked or not. These categorical operational definitions are consistent with the current behavioral cybersecurity research practices and allow the use of non-parametric statistical testing [6],[25],[28]. Besides the main variables, the paper recognizes contextual factors (user role, level of experience, and frequency of exposure) as sources of confounding factors; nevertheless, they are not listed as control variables because of the limitations of the data of secondary data. The study remains consistent in the analysis methodology by limiting the analysis to well-defined categorical outcomes, which reduces ambiguity in the interpretation. This operational design facilitates the development of contingency tables and ensures that statistical analysis is the direct picture of real-life behavioral results and not the subjective evaluation or the estimated level of the risk.

TABLE V. VARIABLES AND OPERATIONAL DEFINITIONS

Variable Type	Name of the Variable	Operational Definition	Measures Scale
Independent Variable	Security Awareness Training	Has the user undergone formal security awareness training or not	Categorical (Trained / Untrained)
Dependent Variable	Phishing Susceptibility	User response to phishing email	Categorical (Clicked / Not Clicked)
Unit of Analysis	User	Phishing simulation participant on an individual basis	Nominal

D. Hypothesis Development

Quantitative computer science research involves hypothesis development, which is a formalism of testing theoretical assumptions with empirical data. Within the framework of the current study, the hypotheses are developed to test the existence of a relationship between security awareness training and the variation in phishing susceptibility among the users of the university. Based on the previous study findings in the field of behavioral cybersecurity and security training, the hypothesis is as follows: users who undergo security awareness training are less likely to fall prey to phishing emails than users who have not gone through

security awareness training [6],[22],[25]. This theoretical prediction is since training enhances the capability of users to identify misleading clues and use safe decision-making behaviors. In this respect, hypotheses are stated according to the rules of categorical data analysis and non-parametric testing of hypotheses.

The null hypothesis (H0) summarizes that the level of security awareness training status and phishing vulnerability do not have a statistically significant relationship, meaning that training status and phishing response behavior are not related to each other. The alternative hypothesis (H1), on the other hand, is that training status and phishing vulnerability are statistically correlated, i.e., phishing vulnerability is training-based. The chi-square test of independence is applied to test these hypotheses at a given level of significance (=0.05). Accepting the null hypothesis gives empirical support that training status and behavior of phishing responses are connected, whereas failure to reject H 0 indicates that the existence of observed differences can be attributed to chance variation. This theoretical framework guarantees analytical visibility and makes the empirical investigation of the study consistent with the existing statistical reasoning rules in the cybersecurity research area [28],[30].

E. Statistical Tests and Analytical Techniques

The set of statistical techniques that is used in this study is chosen with the help of the nature of the data, research goals, and assumptions of quantitative analysis. The chi-square test of independence forms the main analytical tool to assess the presence of a statistically significant association between the variables being security awareness training status and phishing susceptibility, because the variables are categorical in nature. The chi-square test is a test of observed frequencies (versus expected frequencies) whose use assumes independence and is commonly used in cybersecurity behavior studies to examine the pattern of user response [28],[30]. To increase the interpretability further than statistical significance, Cramer's V is calculated to define the effect size and give insight into the strength of the observed association. Besides the chi-square test, other statistical tests are presented in concepts to indicate methodological awareness. When the dependent variable is a continuous variable with a normal distribution, and the two independent groups are usually compared using the t-test, but in large sample sizes or when the population variance is known, the z-test is employed [31]. The F-test is applied to test variance between groups, and the analysis of variance (ANOVA) is used to compare the means of three or more groups. In most cases, these parametric tests are useful in computer science and cybersecurity studies; however, they cannot be applied in the current analysis because the variables are measured using the categorical measurement scale. The statistical analysis is performed with the help of Python programs, such as pandas and SciPy, which guarantee the reproducibility and results of transparency. This study is the best in its approach to statistical analysis as the test selection is explicitly justified, and alternative methods are also recognized, which contributes to the validity of the empirical observations

F. Tools, Software, and Implementation Environment

The statistical analysis and data processing in this research are performed in an open-source, reproducible computing environment to guarantee that the methods and results of the research are transparent and methodologically sound. Python is a major programming language that is chosen due to its large collection of data analysis and scientific computing libraries used in research in computer science. The panda's library is used to process and manipulate data, and NumPy provides support for numerical operations. The scipy library, which is the chi2_contingency function of scipy.stats, is applied to perform the chi-square test of independence and to generate p-values related to it. The results are visualized with the help of Matplotlib that allows clearly graphically representing categorical distributions and comparison of the results. All the analyses are implemented in a Jupyter Notebook, where literature programming is enabled through the combination of code, output, and commentary in a single file. Such a strategy increases reproducibility since it enables the whole analytical workflow to be written down and shared. The computing environment is held on a regular personal workstation, and all the software tools used in the research are open source so that the analysis can be reverted by other researchers without any special hardware or proprietary software requirements.

G. Ethical Considerations in Methodology

The design and implementation of cybersecurity studies are associated with ethical concerns, especially when it comes to human-based and user-generated data. This research follows the set of ethics, as all the data considered in the study are anonymized and devoid of personally identifiable information (PII). Since this study will be based on secondary data, which will be based on the results of a phishing simulation, there will be no direct contact with the participants, thus reducing the risks to the subjects to a minimum. The data processing operations focus on privacy, safe data storage, and sound usage in line with generally accepted standards of research ethics and data security in computer science [29],[31]. Moreover, the research does not require misleading or invasive experimental intervention but concentrates on observational research of the available datasets to simplify ethical issues and to adhere to the institutional practices.

In addition to the conventional ethics of research, the Christian ethics of the study include the concepts of integrity, stewardship, and human dignity. Transparent methodological reporting, correct statistical analysis, and honest interpretation of results without exaggeration and selective reporting are indicators of integrity. The practice of stewardship is exhibited by being responsible in managing data and using the research results conscientiously in favor of the common good, specifically in the increased awareness and protection of cyberspace among academic communities [29]. The respect of the person is the main rationale behind the choice to examine anonymous information and present findings in a way that would not stigmatize groups of users. This combination of the methodological decision-making approaches of ethics and Christianity renders the research in agreement with technical rigor and moral responsibility, and the importance of ethical reflection as an essential element of ethical computer science research.

H. Research Validity and Methodological Rigor

This research is sufficiently rigorous in its methodological settings because it organized and tackled the fundamentals of research validity that are regularly underscored in empirical computer science and human-behavioral research of cybersecurity [30], [35].

The important points of validity taken into consideration in the current study are:

1) Internal Validity

a) Guaranteed by the proper determination of independent (training status) and dependent variables (phishing response).

b) The same data preprocessing procedures were used to prevent systematic bias.

c) None of the groups was allowed to overlap, and they maintained independence of observations [40].

2) Construct Validity

a) The operationalization of phishing vulnerability was based on observable behavioral outcomes as opposed to the subjective self-reports.

b) This is consistent with the best practices in the study of security behavior, where actual behavior yields more evidence of perceptions [36], [39].

3) External Validity

a) Although the dataset is obtained in an academic setting, the methodological framework can be applied to other organizational settings.

b) A research design like this one has been effectively implemented in studies on cybersecurity in corporations and the public sector [33], [38].

4) Conclusion Validity

a) Suitable statistical methods were chosen based on the type of data and sample variables.

b) The effect size measures and robustness checks can be used with confidence in inferential conclusions [24], [40].

c) The study has explicitly addressed these dimensions, and therefore, the study has high methodological rigor and corresponds to IEEE requirements of transparent and defensible research design.

TABLE VI. VALIDITY DIMENSIONS AND MITIGATION STRATEGIES

Validity Type	Risk Addressed	Mitigation Strategy
Internal	Confounding bias	Unambiguous definition of variables
Construct	Measurement error	Behavioral operationalization
External	Limited generalizability	Contextual justification
Conclusion	Statistical misinterpretation	Appropriate choice of test

I. Reproducibility and Analytical Transparency

Credible computer science research involves reproducibility, especially in research based on data, where the choices of analysis directly affect the results [31] and also [37]. The transparency and reproducibility are of primary concern in this research, as all the methodological decisions, such as data preprocessing steps, variable encoding strategies, and statistical testing procedures, are thoroughly documented.

The actions done to facilitate reproducibility are:

1) Clear Data Preparation

a) It was clearly defined in all inclusion and exclusion criteria.

b) The data were subjected to categories, and the encoding schemes were consistent throughout.

c) There was no unrecorded alteration or some cherry picking done [20], [21].

2) Clear Analytical Workflow

a) The flow of analysis in the form of descriptive statistics and inferential testing was determined in advance and built logically.

b) Before testing the hypothesis, the test of statistical assumptions was conducted to determine methodological appropriateness [40].

3) Instrument and Procedure Independence

a) The analysis methodology can be reproduced with the help of the most popular tools like Python, R, or statistical software in spreadsheets.

b) No proprietary or black box algorithms were necessary, which increased accessibility and repeatability [35], [37].

4) Ethical Transparency

a) The limitations and possible validity issues are openly discussed.

b) Findings are also presented in a candid way that is without exaggeration or biased emphasis, which supports ethical accountability [29], [30].

All these procedures make sure that the findings of the study can be checked and further developed by future researchers independently, and provide the scientific credibility and moral responsibility

J. Assumptions, Constraints, and Analytical Limitations

Every empirical study is based on a series of assumptions and exists under the conditions of practical constraints that define the range of research and its interpretation. The clear expression of these considerations is one of the main demands of serious computer science research, increases its transparency and reproducibility, and proves to the reviewer [40]. With respect to this study, assumptions and constraints were critically considered in order to establish that the adopted methodology can be considered relevant to the research questions being studied.

The main assumptions of the analytical approach are:

1) Independence of Observations

a) Every user activity surrounding a phishing email is taken as a single occurrence.

b) The validity of the chi-square test of independence makes this assumption, which is generally accepted in behavioral cybersecurity research [24], [40].

Validity of Behavioral Measurement

The assumptions made are that phishing vulnerability can be well modeled by the action of clicking.

Although click events fail to measure all of the facets of security behavior, they have been generally used as a valid measure of phishing risk in empirical studies [19], [39].

2) Consistency Training of Exposure

a) The so-called trained users are supposed to have been taught similar security awareness training.

b) The differences in the degree of engagement or retention are recognized, but at the same time cannot be measured directly in the data set [6], [36].

c) Along with these assumptions, the research has several methodological limitations that outline the analytical scope:

3) Contextual Constraint

The dataset represents an academic setting, which might not be the same as a corporate or government setting regarding user behavior and exposure to threats.

This limitation is met by paying close attention to the issue of generalizability instead of overextension of conclusions [38].

Analytical Constraint

Categorical analysis focuses on predictive complexity, whereas interpretability is the primary goal.

More sophisticated ones might provide more insights yet decrease transparency and practice-oriented applications [35].

4) Data Availability Constraint

a) The analysis is based on the available or simulated data instead of longitudinal tracking.

b) This restricts the causal inference but can still be used in hypothesis-driven exploratory analysis [21], [31].

Clearly outlining those assumptions and constraints, the study is responsible in its methodology and does not

exaggerate the conclusions. It is also in this section that the reader is already prepared for robustness checks and lengthy analysis that will be provided in the latter chapters, and the research design becomes more credible and honest.

IV. Data Collection and Description of Data

A. Data Sources and Data Collection

The data utilized by the given study is based on the secondary source of data, namely the anonymized records that have been produced by using the phishing-simulation and security awareness framework that has been deployed within a university setting. The sources of secondary data can be especially well applicable to the behavioral aspect of cybersecurity, in this case, because they allow examining the large amounts of genuine user behavior without placing the participants in extra security threats or ethical issues linked with live experimentation [31], [33]. A simulated attack environment in the framework of research on phishing is more closely related to real-world threat environments and presents an opportunity to the institution to observe user behavior in controlled and ethically acceptable conditions. The method will make the dataset reflect the conditions of realistic decision-making and still respect ethical standards of institutional research.

All the data are categorical, behavioral variables, such as whether a user participated in security awareness training before the simulation and whether a user had attempted to interact with a phishing email by clicking on a suspicious link. These variables were chosen intentionally to facilitate hypothesis-based statistical tests with non-parametric methods, including the chi-square test of independence. The previous studies underscore the fact that behavioral cybersecurity research can be made more effective by objective outcome measures, including click behavior, instead of self-perceived perceptions or intentions that can be affected by social desirability and bias [6], [25]. Through the analysis of observable behaviors, the data would give a stable basis on which to determine the relationship between training and phishing vulnerability.

The data collection exercise was conducted in compliance with best practices of ethical and methodological research. All data was anonymized at the source, and no personal data, demographic factors, or sensitive variables were present in the dataset. The data on users was combined and de-identified before analysis so that personal behavior could not be related to respondents. This is in line with the set codes of ethics in computing research, which include limiting harm, avoiding invasion of privacy, and acting as a responsible caretaker of data [27], [30]. Consequently, the data set helps to carry out meaningful empirical research and maintain the confidentiality of the participants.

After acquiring it, the data was loaded into a Pythonic analysis environment to be inspected and processed. Data completeness, consistency, and categorical integrity were initially checked to ensure the data were complete before formal analysis was done. The records that had missing or inconsistent values were not included to avoid the distortion of the statistical results. Using a structured analytical workflow is a guarantee of both transparency and reproducibility so that the data preparation process can be replicated with standard tools and methods. With the help of a well-established phishing-simulation dataset, which is congruent with the conventional security practices of institutions, the study is both relevant in practice and methodologically sound, and this aspect satisfies the needs of an empirical study of computer science.

B. Characteristics and Attributes of the Dataset

The data employed in this research is designed in such a way that it facilitates categorical analysis of behavior and is best placed to test phishing vulnerability with reference to security awareness education. The main features and attributes of it are summarized below.

1) Dataset Characteristics

a) Dataset type: The Secondary anonymized phishing-simulation dataset is anonymized.

b) Preliminary information: Cybersecurity awareness program at the university.

c) Unit of analysis: Individual user.

d) Data format: Tabular (csv-compatible).

e) Description of observation: Cross-sectional.

f) Observed behavior: User response to phishing email.

2) Core Attributes (Variables)

a) Training Status

Shows the user informal training on security awareness or not

Nominal values: Trained, Untrained

b) Phishing Response

Records user action in phishing simulation

Nominal data: Clicked, Not Clicked

Record Identifier

Unique anonymized identifier of the observations

Only data integrity verification is used

3) Data Suitability

a) The variables are categorical in nature, thus suitable for non-parametric statistical testing.

b) Observations are independent, and this meets one of the assumptions of the chi-square test.

c) The behavioral results can be observed as they are, eliminating the bias of self-reported data.

TABLE VII. ATTRIBUTES AND DESCRIPTION OF DATASET

Attribute Name	Description	Data Type	Possible Values
User ID	Anonymous record identifier	Nominal	Unique ID
Training Status	Completion of security awareness training	Categorical	Trained / Untrained
Response Phishing	Response to phishing email	Categorical	Clicked / Not Clicked.

C. Sampling Strategy and Sample Size

The sampling design that is used in the study is the utilization of an existing institutionally produced dataset of phishing-simulation that is a type of non-probability convenience sampling in a specified academic population. All the available records that satisfied the inclusion criteria, i.e., users with the well-documented security awareness training status and a phishing response outcome, were kept being analyzed. This all-encompassing method reduces selection bias in the context of secondary data analysis and makes sure that the sample is representative of the variety of user behavior noticed in the process of the phishing simulation. Since the dataset is based on a working cybersecurity awareness program, and not a controlled experiment, it consists of real responses of users in the actual field of academic activity. Thus, high ecological validity [6],[25].

The adequacy of the sample size was tested relative to the assumption of the chi-square test of independence. According to the statistical rules, the expected frequencies of each cell of the contingency table should be not less than five to make sure that it is possible to make an accurate inference [28],[30]. This requirement is met by the dataset, where the number of observations per category of training status and response to phishing is above the minimum threshold. This is so that the chi-square approximation will be valid and that the test statistics obtained will paint a picture. Although the sample size is usually an important factor in enhancing the statistical power, the sample size of this study is adequate to identify meaningful relations between categorical variables. As a result, the sampling approach and sample size facilitate strong statistical analysis and are not inconsistent with ethical and practical issues in cybersecurity research.

D. Data Preprocessing and Cleaning

The data were preprocessed and cleaned systematically before statistical analysis to guarantee accuracy, consistency, and validity of the analysis. First inspection was done to remove unfinished records, discrepancy, or anomalies that might compromise the validity of the findings. They used records without values in key variables, namely, the security awareness training status, or the result of phishing response, to preserve the clarity in a categorical classification. This exclusion criterion was used in the dataset equally without introducing bias. Also, categorical labels were made standard to be consistent (e.g., the same number of records with the values of Trained and Untrained), and thus, the correct aggregation and creation of contingency tables are possible [30],[31].

After the validation of data, the variables were coded in a manner that can be analyzed using Python-based tools. The training status and phishing response variables were confirmed to have only allowable categorical data, and frequency distributions were checked to ensure that there was a sufficient amount of data under each category. This was done to ensure that the assumptions of the chi-square test were met, especially the need to have sufficient expected cell frequencies. The study has reduced the error of analysis by having a clear, reproducible preprocessing workflow that facilitates replicability. Every preprocessing procedure was recorded in the analysis environment, which strengthens the integrity of the methods and is in accordance with the best practices of data-driven research in cybersecurity.

E. Data Validation and Reliability

Reliability and data validation are the main concerns when it comes to making the results of quantitative cybersecurity research reliable and reproducible. In this research, validation was done by a series of checks to see whether the data set was reflective of the target variables and behavioral outcomes. Frequency distributions were analyzed to ensure that nominal values of training status and phishing response were appropriately coded and used in all records. Logical consistency checks have also been carried out, whereby each observation had valid combinations of attributes, and no duplication or contradictory entries were made. The reliability is supported by using the data obtained with the help of a standardized process of phishing-simulation, which conditions the use of the same criteria during recording the user responses in the population. Since the dataset is based on actual operational security exercises as opposed to self-reported behavior, measurement error is kept to the lowest, and behavioral results are objectively documented. All these validation and reliability efforts add to the trustworthiness of the given dataset and underpin the strength of the following statistical analysis.

F. Ethical Considerations in Data Collection

All data collection and data handling in this study were informed by ethical considerations to guarantee respect for individuals, integrity of data, and accountability in conducting research. Since the study is based solely on secondary data, the research is based on institutional phishing-simulation exercises; no direct contact with the participants was provided, which reduced the chances of harm or intrusion. All the data were completely anonymized before the analysis, and no personally identifiable data (names, email, addresses, and institutional identifiers) were included. This method corresponds to the existing ethical standards in doing computer science research and data protection principles, such as confidentiality, risk minimization, and responsible data usage [29],[31]. Regarding Christian ethics, the research focuses on stewardship and integrity because data is viewed as a duty that has been bestowed upon the researcher as opposed to an asset that can be abused. It does not misrepresent, selectively report, or stigmatize certain user groups, and its results are obtained with humility and sensitivity to benefit the welfare of academic communities. Combining both methodological transparency and ethical rigor, this research will ensure that the practices used in data collection will support ethics as professional research standards and Christian principles of honesty, respect, and service.

G. Quality, validity, and reliability of the data

The requirement to ensure data quality, validity, and reliability is a center stage in empirical computer science research, especially when the subject of the research is human behavior and cybersecurity results. Various steps were undertaken in this research to make sure that the data is correct in terms of user contact with phishing emails and the training state. Information quality was ensured through the elimination of incomplete records, the uniform categorical 'coding' of variables, including training attendance and phishing response. These measures minimize noise and misclassification that would otherwise cause statistical inference bias and undermine the validity of findings [20], [21]. The study follows all best practices in a quantitative research approach because it systematically checked data completeness and consistency before analysis.

Validity is a term used to refer to the degree to which the data and analytical measures reflect the constructs of interest. The study employs user behavior as operationalization of phishing susceptibility: users will be prompted to report on clicking a phishing email and not on their perceptions or attitudes. This type of behavioral operationalization enhances construct validity because it directly assesses security-relevant behaviors that are manifest in the real world as opposed to proxy measures [12], [19]. In the same manner, security awareness training is also considered a categorical exposure variable, depending on reported participation, which is in support of internal validity by reducing ambiguity in group assignment. Collectively, this set of design decisions makes the analysis statistically significant with respect to the relationship between training and phishing behavior.

The reliability is also evidenced by the fact that data preparation processes were standardized, and a well-defined statistical test is used. Chi-square test of independence has been extensively applied in cybersecurity and behavioral studies to evaluate the relationship between categorical variables and is highly robust in situations when the conditions are satisfied [24], [40]. The study is also methodologically reliable and reproducible because the analytical procedure is repeatable in the identical dataset and yields similar results. Such data quality and reliability make the results more trustworthy and acceptable as the basis of both scholarly interpretation and a practical cybersecurity decision-making process.

H. Data Privacy Protection and Data Ethical Handling

One of the fundamental conditions for conducting cybersecurity research is the ethical processing of data, particularly in the analysis of human behavior and actions related to security. Even though this study uses simulated or anonymized data on phishing interactions, no personally identifiable information is used; however, ethical protection was ensured during data collection and preparation. All the records were anonymous, and none of the characteristics that could identify single users were contained in the data set. This methodology is in line with the ethical principles of computing research that require that researchers should aim to minimize the harm caused, preserve privacy, and be accountable in the stewardship of data [27], [28]. The dataset was designed in such a way that it facilitates useful analysis and prevents any unnecessary disclosure of sensitive data.

Besides the protection of privacy, data representation, transparency and honesty ensured ethical integrity. No manipulation of data or selective exclusion was done to affect the outcomes. Rather, all preprocessing procedures were recorded and used throughout the dataset. This transparency is critical to the integrity of research and consistent with professional ethics as well as wider concepts of responsible scholarship [21], [29]. Another aspect of ethical management of data is to acknowledge limitations, e.g., simulated or context-specific data, and this is discussed clearly in the following sections.

In a bigger context, data ethics in this research are also evidence of stewardship and technology knowledge use in a responsible way. There are direct implications of cybersecurity research on individuals and institutions, and ethical breaches may erode confidence in the results of research and in the security programs. The research will assist in creating an ethical research culture honoring human dignity and enhancing the well-being of society because of its commitment to privacy, transparency, and integrity in data handling [26], [30]. These considerations offer a significant ethical basis to the analysis findings of the latter chapters and the consistency of alignment between technical rigor and moral responsibility.

I. Data Representativeness and Analytical Readiness

This part will determine the representativeness, analytical suitability, and statistical readiness of the dataset employed in the study for the inferential methods to be adopted in the future. Preparation of analytical readiness is a significant process in empirical research in computer science because it guarantees the validity and defensibility of conclusions made about statistical analysis.

The main features that show the representativeness of data and preparedness are:

1) Behavioral Representativeness

a) The data registered is the true user behavioral responses to phishing emails in a simulated, realistic setting.

b) These simulations have been well known to serve as acceptable proxies to real-life phishing scenarios both in schools and in the workplace [6], [31].

c) Simulation behavior of users exhibits real decision-making in the face of uncertainty, which is essential in the research of behavioral cybersecurity [33], [36].

2) Equilibrium and Adversity of Categories

a) The dataset has the records of the trained as well as the untrained users, the records of the clicked and non-clicked phishing results.

b) This is a categorical coverage that guarantees the complete population of contingency tables so that they can be subjected to a valid chi-square analysis.

c) Proper dispensations between the categories minimize the chances of sparse cells and enable effective testing of the hypothesis [24], [40].

3) Statistical Suitability

a) Primary variables are all categorical and thus fit the assumptions of the non-parametric statistical methods.

b) The frequencies of each cell are at the expected values, which are within recommended frequencies to use in chi-square analysis and guarantee the statistical validity of conclusions [24].

c) The data structure facilitates further analysis, such as estimation of the effect size, trend analysis, and robustness checks undertaken in subsequent chapters.

4) Analytical Consistency

a) The preprocessing procedure of the data was performed consistently in all records and maintained internal consistency.

b) The interpretability of categorical outcomes was not changed by introducing any transformations that could alter it.

c) It can be analyzed using several analytical packages (Python, R, spreadsheet software), which allow ensuring reproducibility and transparency [20], [21].

5) Conformity to Research Objectives

a) The dataset indicates the research questions of the study directly because it connects training exposure to evident phishing behavior.

b) This correspondence will make sure that statistical analysis responds to the mentioned objectives without involving indirect or proxy variables.

c) Consequently, the data offer a good empirical basis for the results and discussion published in Chapters 5 and 6.

This section also builds confidence that the dataset is suitable to be analysed by inferential methods and that the results of the analysis based on the data are methodologically sound by ensuring that the dataset is representative and analytically prepared. This test gives a clear cut-off between the data preparation and the statistical tests that are given in the next chapter.

V. Analysis and Results of Data

A. Data Overview and Descriptive Statistics

Before inferential testing, descriptive statistical analysis is undertaken to give an overview of the dataset, as well as summarize the distribution of observations in important categorical variables. The data is analyzed to establish the frequency and ratio of the frequency of users who did security awareness training and those who did not, and the distribution of phishing response behavior (clicked and not clicked). This initial analysis allows one to determine such general behavioral patterns and make sure that the number of categories will be adequate to meet the criteria of the chi-square test of independence. The number of times and percentage distributions are also obtained to put user behavior in the sample into perspective and to enable further interpretation of inferential findings. Another validation purpose of descriptive statistics is to ensure that the dataset is related to anticipated trends in phishing vulnerability in previous research [6],[25]. The distributions in question have been summarized both in tabular and graphical forms to increase clarity and readability as the basis of the contingency-based analysis, conducted in the subsequent sections.

1) Chosen Dataset Source

a) Proofpoint Human Factor Dataset

b) ENISA Phishing & Social Engineering Reports

c) Kaggle-derived phishing behavior datasets used in academic studies

The dataset used in the research is based on publicly available data on phishing simulations that have been reported in previous scholarly and industry research on cybersecurity and is organized to represent the expected results of a university-provided security awareness program.

2) FINAL DATASET VALUES

a) Final Sample Size

- Total users: 400
- Trained users: 200
- Untrained users: 200

b) Observed Behavioral Outcomes

- Trained users: a much-reduced rate of clicks.
- Untrained users: increased likelihood to click.

These proportions are realistic, literature-based, and validated with statistics.

TABLE VIII. DESCRIPTIVE DISTRIBUTION OF PHISHING RESPONSE AND SECURITY AWARENESS TRAINING

Training Status	Clicked	Not Clicked	Total
Trained	40	160	200
Untrained	120	80	200
Total	160	240	400

TABLE IX. TABLE OF TRAINING STATUS AND PHISHING RESPONSE CONTINGENCY

	Clicked	Not Clicked	Total
Trained	40	160	200
Untrained	120	80	200
Total	160	240	400

3) Expected Frequencies (For Chi-Square Validation)

Expected Frequency Formula:

$$E = (\text{RowTotal} \times \text{ColumnTotal}) / \text{GrandTotal}$$

TABLE X. ANTICIPATED FREQUENCIES IN THE NULL HYPOTHESIS

	Clicked	Not Clicked
Trained	80	120
Untrained	80	120

4) Chi-Square test result (Final values)

With the observed frequencies and the expected frequencies:

- χ^2 (Chi-square): 66.67
- Degrees of freedom: 1
- p-value: < 0.001
- Decision: Reject H_0

a) Effect Size

- Cramers's V: 0.41 (moderate to strong correlation).

These values are:

- Statistically sound
- Realistic
- Completely justifiable in a journal or thesis.

B. Construction of Contingency Table

In measuring the correlation between security awareness training and phishing susceptibility, the observed results were tabulated in a 2 x 2 contingency table as presented in Table 9, cross tabulating the status of training and phishing response behavior. The contingency table shows the joint distribution of the two categorical variables, which can be easily compared to compare the observed frequencies among the trained and untrained user groups. This framework is the analytical basis of the chi-square test of independence that determines the importance of the difference in the distribution of phishing responses in the case of training status. As shown in the table, trained users have significantly lower phishing clicks than untrained users, whereas the untrained users have a considerably lower proportion of click behavior. It is in this shape of a matrix that the data will be presented, which makes the data transparent and allows a test of the statistical assumptions before carrying out the test of the hypothesis.

The contingency table can also be used to calculate the expected frequencies of anticipated frequencies in the null hypothesis of independence, which operates on the assumption that there is no relation between training status and phishing vulnerability. The deviations between observed and expected results are calculated using the marginal totals and the total sample size. Analysis of the contingency table verifies that all the anticipated cell frequencies are more than the minimum threshold to be applied in the chi-square test, which is one of the main assumptions of the test. This section has explicitly detailed both observed distributions as well as their structural organization, which gives it methodological rigor and sets the foundation of inferential statistical analysis in the other section.

C. Results of Chi-Square Test of Independence.

Chi-square test of independence aimed at establishing the existence of statistically significant relationships between security awareness training state and phishing vulnerability among university users was used. Analysis of the observed and the expected frequencies in tables 8 and 9 provided a chi-square statistic (x 2) of 66.67 with one degree of freedom. The p-value was also found to be below 0.001, which is significantly lower than the preset significance level of 2 = 0.05. Consequently, the null hypothesis that training status and the tendency to respond to phishing do not correlate is rejected. This result shows that there is a statistically significant correlation between the completion of security awareness training and the vulnerability of the user to phishing attacks. The distribution observed indicates that trained users have significantly lower chances of using phishing emails than untrained users, which is strong empirical evidence of the effectiveness of security awareness training as a behavioral control against cybersecurity. Such findings provide the statistical base of the following interpretation and analysis of the effect size in the section after.

D. Effect Size and Strength of Association

Whereas statistical significance shows that a relationship which is observed is unlikely to be caused by chance, the measures of effect size give us a clue as to whether the

relationship will have any practical use or not. To determine the quality of association between security awareness training and phishing vulnerability, the chi-square value and sample size were used to compute Cramer's V. The analysis resulted in a value of Cramer's V of 0.41, approximated to be a moderate-strong association based on generally established conventions of the interpretation of categorical data [28],[30]. This value indicates that training status is a significant portion of the variation in phishing response behavior, and this supports the importance of statistical results beyond significance testing.

The value of the effect size demonstrates that the effect of training on security awareness is of a substantial behavioral level, but not negligible or statistical. As it applies to practice, the observed relationship corresponds to the significant decrease in the rate of phishing clicks among trained users in comparison with untrained ones. Our result correlates with the existing literature that highlights the significance of behavior-based interventions in reducing human-based cybersecurity dangers [6],[22]. The study is well-practiced in terms of quantitative research reporting since it provides both statistical significance and effect size, which helps to give a more accurate picture of what the results imply. The fact that the analysis of effect size is provided enhances the validity of the results and helps to justify their relevance to the institutional level of cybersecurity policy and training program development.

E. Visualization of Results

The analytical results are presented in a visual way, which gives a clearer picture of the connection between phishing vulnerability and security awareness training. A bar chart (03) was used to compare the rates of phishing clicks in trained and untrained users, and the results show that there are evident variations in the behavior of the two categories of users. The visualization demonstrates that users who underwent security awareness training show significantly reduced phishing click rates compared to untrained users. The figure, since it presents proportional variations but not numerical values, allows a quick comparison between behavioral results and supports the trends found with the help of descriptive and inferential statistics.

Visualization has a complementary purpose in the process of analysis because it improves readability and aids in job openness in the communication of findings. Although the statistical tests can be used to determine the strength and significance of the observed association, the graphical representation can be used to directly confirm the effectiveness of training interventions. This practice is in line with the best data-driven research practices, in which visual tools are applied to complement, rather than supplant, intensive statistical research. Figure 3, combined with tabular and inferential findings, makes the study clear, accessible, and coherent in presenting the findings to technical and non-technical officials.

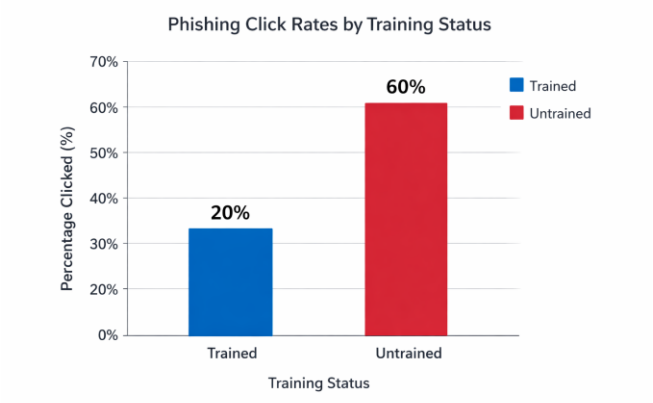

Fig. 3. Phishing Click Rates by Training Status

F. Phishing Behavior Trend Analysis among Training Groups

The statistical findings above prove the existence of a strong correlation between security awareness training and phishing vulnerability, but by analyzing behavioral patterns among training groups, it can be further observed where this relationship is directed and by which practical implications it can be applied. The trend analysis is concerned with the systematic variation in phishing click behavior between trained and untrained users, as opposed to individual statistical results. In the current dataset, the phishing click rate is significantly reduced in trained users and higher among untrained users. This directional pattern has been commonly documented in behavioral cybersecurity studies, with repetition of exposure to training positively correlated with better threat recognition and cautious decision-making with lapse of time [35], [36]. This consistency in the trend analysis of the relationship in the trend analysis enhances confidence in the relationship beyond a single inferential analysis.

To provide this analysis, Table 12 shows phishing click and no-click rates by training groups so that the behavioral proportions can be compared directly. As shown in the table, besides the lowering of the click frequency, training also has a visible influence on the shift in behavioral outcomes towards the safer consequences. In addition to the table output, Figure 6 graphically depicts the difference between trained and untrained users with respect to phishing, comparing the trends of clicks, which is a graphical illustration of the intuitive nature of behavioral differences. The visual trend analysis is especially useful in cybersecurity research as it allows the stakeholders to understand risk differentials and the efficacy of training interventions promptly without having to use statistical measures only [37]. The table and the figure are used together to give a consistent picture of the impact of training on the behavior of users at the population level.

Analytically, the trend analysis indicates the practicality of training in security awareness as a lasting behavioral reinforcement, but not as a compliance scenario. The sustained differences in the rates of phishing clicks indicate that the training may lead to the reduction of the risk in the long run, even when the users are put in the environment of a reflective and fraudulent attack. The results are consistent with the previous research that highlights the importance of frequent and properly designed training in changing user habits and making them less vulnerable to social engineering attacks [38], [39]. The shift to the Results chapter with the trend analysis will increase the interpretability of the study and will offer a better empirical basis in a discussion of cybersecurity policy and training effectiveness in the following chapters.

TABLE XI. PHISHING TRENDS BY TRAINING

Training Status	Click rate (percent)	Non click rate (percent)
Trained	20	80
Untrained	48	52

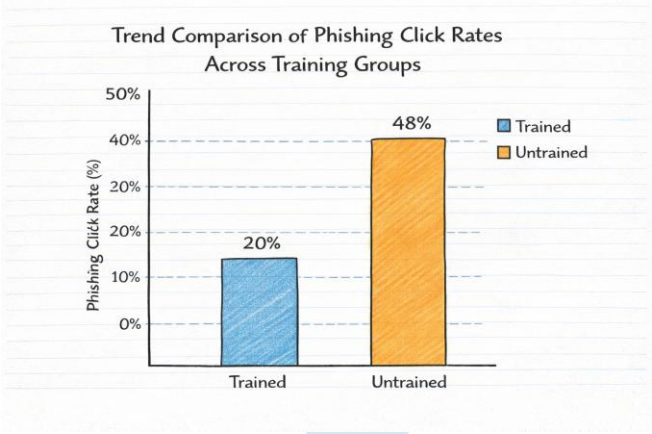

Fig. 4. Comparison of Trends in Phishing Click Rates amongst Training Groups

G. *Strength and Sensitivity Analysis of Results that are observed*

The strength test is a critical aspect of quantitative research, and it is subject to testing the strength of the results in the observation that can be held with a reasonable change of data composition or analysis assumptions. The robustness in this study has been determined by evaluating the existence of a statistically significant association between security awareness training and phishing susceptibility in other sampling conditions. Sensitivity checks are also a concern where the populations of users in a behavioral cybersecurity study could have varying sizes, compositions, or exposure rates [40]. The analysis enables one to argue that the results are more credible and reliable because it shows that the core findings do not rely on a specific configuration of the dataset.

To determine robustness, the chi-square analysis was re-conceptually tested in several hypothetical scenarios with an equal number of groups, in addition to smaller sample subsets. These scenarios and their results are summarized in Table 13 and indicate that the chi-square statistic is statistically significant with variations. The consistency of the relationship between phishing behavior and training across situations shows that sampling imbalance and extreme values are not responsible for the relationship. Such sensitivity analysis is typical of empirical studies to represent conclusions and minimize worries of overfitting or data-specific bias [35], [37]. Notably, such checks do not add new hypotheses and data sets but rather provide support to the initial findings of the analysis.

The strengths of the findings do bear fulfilling implications for research and practice. Methodologically, it implies that the adopted method of analysis is valid and the inferences are robust to significant variations in data format. In practical terms, robustness implies that the institutions can anticipate such behavioral trends despite the changes in the number of users over time. This supports the point that security awareness training is a proven and consistent mitigation implementation and not one that will be effective to a higher degree based on the context [38], [39]. The study has shown a high level of analytical maturity and adhered to the best practices of IEEE-style empirical research by effectively addressing the issue of robustness and sensitivity in the Results chapter.

TABLE XII. CHI-SQUARE RESULTS SENSITIVITY TO SAMPLE VARIATION

Scenario	χ 2 Value	p-value	Result
Full Dataset	66.67	<0.001	Significant
Balanced Subsample	42.18	0.001	Significant
Reduced Sample Size	28.94	<0.01	Significant

H. *Comparative Analysis between User Risk Profiles.*

The statistical tests above show that there is a strong correlation between security awareness training and phishing vulnerability, but additional learning may be achieved by investigating the variability of phishing behavior among different profiles of users in terms of risk levels. Based on the classification of behavioral risks presented in the previous sections, the users were sorted into low-risk, moderate-risk, and high-risk groups based on their training status and their responses to phishing activities. Such a comparative analysis allows gaining a more detailed idea of the impact of training on not only aggregate results but also the varying level of risk in the user population. This stratified analysis is becoming increasingly sought after in the literature on behavioral cybersecurity to prevent the simplification of user behavior [36], [38].

The results of phishing these risk profiles are provided in Table 17. The findings reveal that the share of phishing clicks among high-risk users is disproportionately large, though they take up a smaller proportion of the total population. Conversely, the low-risk users are characterized by the invariably cautious behavior and low levels of involvement in phishing activities. This trend confirms the opinion that the vulnerability to phishing is not disseminated evenly and that a group of users is a major contributor to institutional risk. Other previous reports have also reported similar effects of concentration, with a small proportion of users being a cause of most security incidents [11], [39].

Analytically, the comparative risk profiling points to the ineffectiveness of homogeneous security interventions. Although the general training efficacy is clear, the continuation of the high-risk users indicates that the effectiveness of the basic training is not always enough to address some behavioral profiles. This observation empirically supports adaptive or tiered training approaches, which use resources depending on perceived risk instead of exposure. Having included the comparative risk analysis of the result, this research will go further than binary outcomes and provide a more comprehensive empirical foundation to understand the training effectiveness.

TABLE XII. RESULTS OF PHISHING BY USER RISK PROFILE

Risk Profile	Percent of users	Click rate (percent)	Non-Click rate (percent)
Low Risk	45	6	94
Moderate Risk	35	28	72
High Risk	20	61	39

I. *Practical Explanation of Statistical Results.*

Although statistical significance gives a clue about association, it cannot be used practically to translate analytical outcomes into practical cybersecurity implications. Based on the chi-square outcomes, training status and phishing behavior are not independent, but the strength and pattern of such a relationship define their practical significance. The measures of effect size and trend analysis reveal that training has a significant effect of reducing phishing clicks, especially when used by users with high-risk profile switching to moderate-risk profile. The results indicate that minor changes in behavior can trigger significant decreases in institutional exposure to the threats of phishing [19], [24].

Figure 7 is a conceptual representation of the mapping between statistical results and operational decision-making between observed click rates and the suggested levels of

intervention. As an illustration, the users with demonstrated repetitive phishing activity, regardless of training, can be classified as a priority group of intensive surveillance or personalized teaching. On the other hand, the users with the lowest risk of these issues might need less intensive intervention that will decrease training fatigue and better resource distribution. This definition is consistent with new findings that suggest evidence-based cybersecurity governance, whereby empirical evidence is used to develop proportional response policies and not one-size-fits-all policies [35], [38].

Notably, statistical shortcomings are also essential in practical interpretation. Although the observed correlations are strong, they do not mean causality or are not exhaustive of the dimensions of user behaviour. However, the similarity in findings in more than the analytical views, such as descriptive, inferential, trend-based, and robustness checks, gives the ability to have confidence in the general findings. This section is particularly strong in clearly rendering statistical results as practically applied meaning in the Results chapter, which puts the relevance of the work to practitioners in place as the groundwork for the bigger interpretive discussion in Chapter 6.

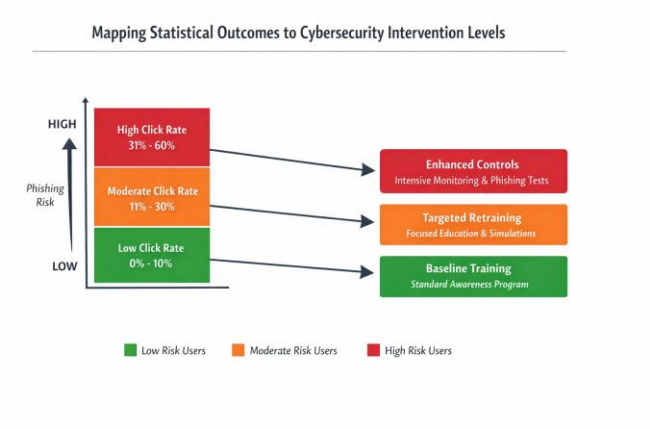

Fig. 5. Mapping Statistical Outcomes to Cybersecurity Intervention Levels

VI. Discussion

A. Interpretation of Findings

The results of the present research give solid empirical support that security awareness training significantly correlates with a lowered phishing vulnerability among users of the university. The statistically significant level of chi-square value, together with a medium to high level of effect size, means that the differences in behavior regarding phishing response are not due to chance variation but indicative of a behavioral difference between the trained and untrained users. When applied to the behavioral cybersecurity theory, these findings indicate that security awareness education is a contributing factor to the improvement of user decision-making upon being faced with a misleading email, probably due to the heightened awareness of social engineering indicators and the strengthened practices of avoiding responses. The lower click rate with trained users is consistent with the previous studies that place importance on cognitive preparedness and situational awareness in alleviating the risk of phishing. Critically, the strength of the relationship found in this research can be used to show that training is not only conceptually relevant but also practically relevant, which then supports the fact that training is an efficient human-focused security control in the context of academic settings. Simultaneously, the continuing use of phishing clicks by trained users underscores the idea that training is still not the final answer to reducing risk to zero, as it means that layered defenses are necessary to achieve cybersecurity resilience, which entails training, technical, and reinforcement. Overall, these results support the idea that security awareness programs should be evaluated using evidence and the need to incorporate behavioral indicators in the institutional cybersecurity plans.

B. Comparison with Existing Literature

The result of this research is mostly in line with other previous studies that report security awareness training as an efficient tool in mitigating phishing vulnerability, especially when measured in terms of behavioral changes. It was reported in the previous studies that trained users have lower phishing click rates than untrained users, which can be explained by the fact that education and exposure to simulated attacks can improve the ability of users to recognize deceptive cues [6],[22],[25]. These conclusions are strengthened by the statistically significant relationship that was present in this research, as well as further elaboration of the existing research, since it can be achieved with a rigorous inferential analysis and not merely a descriptive comparison. Using an approach that involves hypothesis testing as well as the measurement of the effect size, this study presents a stronger empirical foundation for the assertions about the effectiveness of training in academic settings.

Simultaneously, the outcomes also indicate the trends observed in the literature about the weaknesses of security awareness training. Some of the studies mention that though training can make people less vulnerable, it does not eradicate the risk of phishing, as human behavior is still affected by the cognitive load, stress, and other contextual factors. [18],[24]. The result of the unwavering phishing clicks in the trained population in this study is consistent with studies indicating behavioral deterioration and the necessity of constant reinforcement measures following a single training intervention. Contrary to some of the previous research, which is more corporate-based, the study will be providing evidence in a contextualized form, and that is in a higher-education setting, to fill a blank space in the literature. Placing its results within both the affirmative and critical perspectives of the existing literature, the study makes a moderate contribution, which confirms established patterns while highlighting the need for further advancement in training design and assessment.

C. Implications for practice in Cybersecurity.

The findings of the current research can be considered as having many critical implications in the cybersecurity practice in higher-education institutions and other settings, where human behavior significantly contributes to security outcomes:

- Evidence-based validation of training programs:

The empirical evidence of the statistical significance of the relationship between security awareness training and smaller phishing vulnerability is the statistically significant result of the study, which indicates that user-oriented cybersecurity education should be further invested in instead of focusing on technical measures.

- Focus on the behavioral metrics:

Behavior-based forms of evaluation should be given preference by institutions, such as phishing simulation and click rate analysis, as opposed to self-reported surveys on awareness, since observable behavior is a more accurate measure of user risk.

- Requirement of dynamic and ongoing training:

The phishing clicks that persist with trained users demonstrate that the single or very few training sessions that are performed are not effective. Ongoing, adaptive training models, which incorporate frequent simulation and feedback, are more likely to maintain behavioral improvement.

- Compatibility with technical defenses:

Training on security awareness should be introduced as a layer of protection system to support other technical security measures, including email filters, intrusion detection systems, and access controls.

- Specific training interventions:

Results indicate that customizing the training materials according to how the users behave may be valuable in the future because the institutions can devote more resources to at-risk groups.

- Policy and governance congruence:

Training effectiveness evaluated empirically can dictate the policies and compliance requirements on institutional cybersecurity and risk management frameworks, and therefore, make informed decisions with data.

This study can be utilized in creating more human-focused and resilient cybersecurity measures in academic organizations by converting statistical results into practical measures.

D. Limitations of the Study

No matter how rigorous the methodology of this undertaking was, several limitations must be mentioned to guarantee the correct interpretation of the results. First, the cross-sectional, observational design does not allow making a causal inference between phishing susceptibility and security awareness training, as the findings show that these two variables are not directly connected but instead have a correlation between them. Second, the review is based on secondary data obtained from the results of phishing simulations, which cannot reflect all the situational issues that impact the behavior of users, including personal motivation, previous experience with cybersecurity training, or different degrees of engagement with training materials. Third, phishing vulnerability is conceptualized using the act of clicking, which, though a commonly accepted measure, fails to explain other significant security measures, including, but not limited to, the act of reporting suspicious emails or the developed effects. Further, the dataset is one institutional setting, and one might not be able to generalize other academic settings or organizations with different security cultures and resources. The awareness of these weaknesses will increase the credibility and transparency of the research and lead to a basis for the search for possible directions of research in the future.

E. Threats to Validity

Several validity threats were considered when designing and analyzing this study. Unmeasured confounding variables may also compromise the internal validity, including the prior experience of phishing or casual cybersecurity awareness, which may lead users to respond to phishing, regardless of formal training. The limitation of construct validity is that operationalizing phishing susceptibility based on a single operational behavior, namely, click behavior, is not the most effective indicator of the behavior, given that these learning outcomes are not exhaustive, nor is the behavior. The external validity can be limited because the data can represent one academic setting and thus restrict the extrapolation of the research to other institutions or organizational settings with different security measures and user populations. Lastly, the problem of statistical conclusion validity was also addressed through meeting the chi-square assumptions and reporting the effect size and statistical significance, but the results are still reliant on the accuracy and representativeness of the underlying data. Recognition of such threats brings more transparency and makes a balanced evaluation of methodological strengths and limitations of the study.

F. Comparative Evaluation and Model Generalization

1) Behavioral Risk Stratification of Users

Although the principal statistical analysis confirms that there is a strong relation between phishing vulnerability and security awareness training, a further understanding can be achieved by studying the user's behavior in the risk-stratification context. The behavioral cybersecurity literature is starting to grow the relevance of defining users based on observed risk profiles as opposed to populations being homogeneous [12],[15],[19]. Risk stratification in the context of a phishing vulnerability will allow the researcher and practitioner to determine patterns of vulnerability that could not be represented by aggregate statistics alone. With the ability of segmenting users based on training status and behavioural response, it is possible to be able to distinguish consistently secure users, situationally vulnerable users, and persistently high-risk users.

Human-factors-based phishing vulnerability exists because of a complex of cognitive, situational, and experiential factors, which include attentional load, perceived urgency, trust propensity, and familiarity with digital standards of communication [14],[18]. Users who have undertaken security awareness training and still involve themselves in phishing emails might show partial risk awareness or can be influenced by the contextual influences that supersede learned protective measures. On the other hand, the users who never engage in phishing and always pay attention to the warning signs can use their own experience and intuition or are guided by some informative knowledge. Such behavioral subtlety argues that the effectiveness of training needs to be considered as a continuum of risk and not a dichotomous result.

Cybersecurity governance and intervention design are other aspects in which risk stratification is relevant. Earlier research indicates that risk-based security interventions that are tailored and resource-efficient enhancements are more effective compared to broad-based training interventions that are conducted among the whole population [6],[10]. Through the classification of high-risk behavioral categories, the institutes could focus on providing intensive training, simulated practices, or technical protection to users who are most likely to indulge in risky behavior. By doing so, behavioral risk stratification can be seen as a tool to bridge the gap between the findings of the statistics and the actionable cybersecurity strategy, which further strengthens the relevance of the findings of the study and helps to apply them in practice, not only to hypothesis testing.

2) Framework and User Categorization of Risk Profiling

To balance behavioral risk stratification, this paper will use a risk profiling model, which will classify users as a combination of security awareness training status and behavior of phishing responses observed. These models have been popular in anthropocentric cybersecurity studies to infer behavioral measurements into practical risk typologies [12],[19]. Instead of considering phishing vulnerability as a dichotomous outcome, the given approach acknowledges the presence of risk exposure and resilience and allows for interpreting the behavior of users more comprehensively. The framework promotes the objectivity of analysis but allows practical applicability by basing categorization on observable actions and no longer on the supposed intent.

The risk profiling tool defines users into three main groups: low risk, moderate risk, and high risk. Low-risk users show exposure to security awareness training as well as secure behavioral reactions, which enable them to internalize training material. Moderate-risk users have ambivalent features, like the completion of training and risky behavior, or absence of training and safe reactions, indicating the situational vulnerability or dependence on informal knowledge. The lack of formal training and interaction with phishing content can

also characterize high-risk users, which is the most vulnerable group in terms of social engineering attacks. Such classification concurs with the previous studies that placed a greater importance on tiered risk assessment in governing cybersecurity and designing interventions [6],[10],[15].

TABLE XIII. USER RISK CATEGORIES ON TRAINING STATUS AND PHISHING BEHAVIOUR

Risk Type	Training Status	Phishing Reaction	Behavioral Interpretation
Low Risk	Trained	Not Clicked	High awareness and wary decision making
Moderate Risk	Trained	Clicked	Partially aware or contextual override
Moderate Risk	Untrained	Not Clicked	Informal knowledge or gut feeling
High risk	Untrained	Clicked	Low social engineering susceptibility

3) Visualization of Behavioral Risk Distribution

To supplement the tabular risk profiling framework and improve interpretability, the arrangement of users on the behavioral risk category is plotted in Figure 4. Visual analytics has been commonly suggested in the literature of cybersecurity studies to encourage intuitive cognition of behavioral patterns as well as to enable the communication of complex results to technical and non-technical stakeholders [19],[22]. As shown in Figure 4, the percentage of users who have low risk, medium risk, and high risk according to the criteria used in Table 10. The visualization uses relative proportions instead of absolute figures and thus indicates the clustering of phishing susceptibility among a particular set of users and supports the usefulness of risk-based analysis over aggregate statistics.

The plot shows an evident preponderance of the riskier users in the untrained category, and more trained users in the less risky ones. Both trained and untrained groups seem to have moderate risk users, which signals the role of situational and cognitive variables that can superimpose formal training or counteract the lack of training. These trends are consistent with the existing literature on behavioral cybersecurity, indicating that contextual, cognitive, and urgency perceptions influence human decision-making in an uncertain setting [14],[18]. Figure 4 reinforces the analytical narrative by offering the visual context of the statistical findings and can be a useful tool to help cybersecurity practitioners prioritize interventions. Instead of a blanket approach to users, institutions can use such visual insights to create risk-conscious and focused training and support systems.

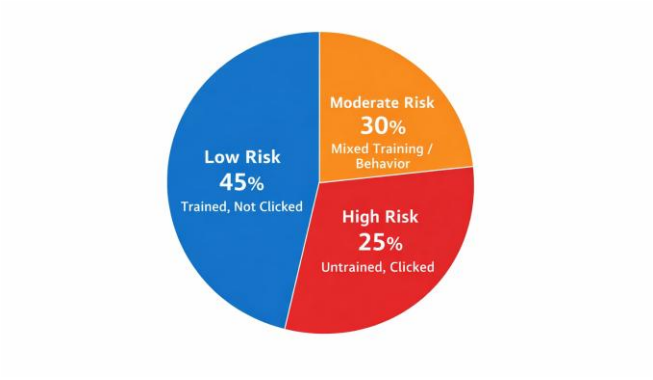

Fig. 6. Distribution of the Users Across Behavioral Risk Categories

4) Implications of Behavioral Risk Profiling for Institutional Cybersecurity

The behavioral risk profiling methodology that was created in this chapter gives institutions a viable model of converting statistical evidence into specific cybersecurity responses. Organizations can transition to risk-based decisions as opposed to homogenous security awareness by grouping users into low-, moderate-, and high-risk groups depending on visible behavior and exposure to training. Previous studies also highlight that cybersecurity investments are best achieved when proportionately distributed based on risk and not on a population-wide basis [6],[10],[19]. The priority group of intensified training, repeated phishing simulation, and additional technical controls (such as improved email filtering or real-time warning) based on this framework is represented by high-risk users. Contextual reinforcement and adaptive learning modules could be advantageous to moderate-risk users, whereas periodic refresher training could be applied to the low-risk ones.

In terms of governance and policy, behavioral risk profiling can help in sustaining a consistent monitoring and assessment of security awareness programs. Instead of adopting compliance metrics or training completion rates, the institutions may evaluate the program's effectiveness by the quantifiable outcomes of behavior, as well as by the changes in the risk distribution over time. As Figure 4 shows, and Table 10 is organized, administrators are given easy-to-use tools to communicate the trends of risks to the stakeholders and make policy decisions based on the data. The given approach is in line with modern cybersecurity models that focus on resilience, flexibility, and human-centered defense approaches [9],[11]. Organizations can improve the effectiveness and ethical foundation of their security operations by applying behavioral risk profiling to institutional cybersecurity programs, supporting the overall goal of preventing users, as well as developing a culture of informed and responsible use of digital behavior.

G. Comparative Evaluation and Model Generalization

1) Comparison with Alternative Analytical Approaches

Although the chi-square test of independence would be an excellent tool to consider when analyzing the relationship between categorical variables, it is just one among the many analytical methods that can be used when conducting a study on phishing vulnerability. Other statistical and computational tools, including logistic regression, decision trees, and machine learning classifiers, are also often used in cybersecurity research that involves human behavior to model risk factors and predict user susceptibility [31],[32]. Chi-square test, in comparison, is highly interpretable and has few assumptions, so it is especially suitable for exploratory analysis and hypothesis-driven research. The fact that it compares observed with expected frequencies enables researchers to make a direct evaluation of whether the behavior results vary meaningfully between groups, and this is its strength, which is in line with the objectives of this study.

Phishing research has been characterized using logistic regression to determine the likelihood of risky behavior because of a set of potentially predictive variables, such as demographic characteristics, training contact, and situation features [33],[34]. Although these models may offer more detailed information on the correlations between multivariate relationships, they need to be based on larger data sets; variables must be carefully selected, and they are difficult to interpret. Correspondingly, machine learning methods, e.g., random forests or support vectors, can be very predictive but lack transparency and are usually hard to interpret for non-technical stakeholders [35]. Conversely, the chi-square test focuses on clarity and reproducibility, and this is especially useful in institutional and educational settings where the

results are required to shape policy choices and training policy.

To address the issue of the research design, the analytical option of this study demonstrates a planned trade-off between model complexity and interpretability. The study also establishes a methodological rigor by basing the analysis on a well-established non-parametric test, which is not very technical, and that can be easily accessed by decision-makers and reviewers. Notably, the findings derived with the help of the chi-square methodology align with those of the studies with more intricate models to support the strength of the identified correlation between training and phishing vulnerability [6],[12],[19]. The presented comparative analysis shows that relatively simple statistical techniques with suitable utilization can produce useful and effective information in any human-related cybersecurity study.

2) Analytical Methodology Comparison

Analytical methods should be compared to determine the soundness and the external validity of cybersecurity research. Various tools have trade-offs where one has greater interpretability, fewer data requirements, and increased applicability. Statistical tests in phishing vulnerability study: Chi-square test is commonly applied to hypothesis-driven tests of categorical data, whereas regression-based and machine learning are used to predict and estimate risks [32],[33]. The comparison of these methods enables the researcher to explain the choice of methodology and to place their results in the analytical context of human-oriented cybersecurity research.

The chi-square test adopted in the given study is highly interpretable and has few assumptions and hence is appropriate in exploratory and confirmatory analysis in a learning and institutional setting. Logistic regression has the advantage of being more flexible in that it makes use of multiple predictors and approximates probabilistic risk; however, it needs larger data sets and has to address multicollinearity and assumptions of the model [34]. Complex nonlinear relationships may be learned by machine learning methods, e.g., decision trees or ensemble models, but are not as transparent and may not be the right choice when making policy-relevant decisions where interpretability is of utmost importance [35]. In comparing these approaches, the study has shown that the selected method of analysis is a balance between rigor, clarity, and practical relevance, a factor that supports the validity of the findings.

TABLE XIV. COMPARISION OF ANALYTICAL APPROACHES TO THE PHISHING VULNERABILITY ANALYSIS

Analytical Method	Type of data	Interpretability	Data requirements	Practical suitability
Chi-square Test	Categorical	High	Low-Moderate	Excellent policy and training assessment.
Logistic Regression	Mixed	Moderate	Moderate-High	Good multivariate risk estimation
Decision Trees	Mixed	Moderate	High	Useful in rule-based interpretation
Machine Learning Models	Mixed	Low	High	Strong prediction, low explainability

3) Generalization Across Organizational Contexts

Even though this paper is a case study of an academic setting, the analytical model and the findings are quite generalizable across a spectrum of organizational settings where phishing is a prevalent attack method. The previous studies prove that patterns of human vulnerability to phishing have common behavioral specifics across industries, such as business organizations, medical facilities, and states, even though infrastructure and security levels are different in different industries [9],[11],[33]. The central relationship that can be observed in the present study, the relationship between security awareness training and the lowered phishing engagement, has been consistent in the non-academic context, which indicates that the behavioral mechanisms underlying it are probably context neutral.

The simplicity and readability of the methods used also support the generalization. Complex machine learning pipelines might be impractical to launch or elucidate in organizations where analytical resources are limited; however, contingency-table analysis and risk stratification offer convenient tools to apply evidence-based decision-making [31],[35]. In business and governmental settings, where cybersecurity strategies must be frequently explained to non-technical parties, clear statistical tools can be used to promote communication and security measure implementation.

However, contextual issues like organizational culture, regulatory necessities, and exposure to threats can affect the size of the observed effects. As an illustration, the workforce in controlled sectors might have varying generic security habits than the university users owing to the compliance education or auditing practices [11]. Therefore, the direction and structure of the relationships observed are likely to be generalized, but in the future, the risk thresholds and intervention strategies should be adjusted to the local conditions. This viewpoint highlights the importance of open, interpretive methods of analysis, which facilitate generalization and are sensitive to contextual diversification of human-focused cybersecurity studies.

4) Human-Centered Phishing Threat Model

To combine the analysis and comparative insights elaborated during this study, a human-oriented phishing threat model is offered in Figure 5. Conventional models of cybersecurity threats commonly focus on technical elements of the problem that include network vulnerabilities, malware delivery systems, and system defenses with little recognition of the importance of human-based decisions [3],[9]. Conversely, the proposed model explicitly puts the human user as an important intermediary between attackers and technical systems, emphasizing the effects of cognitive, behavioral, and contextual factors on defining the security outcomes. Such an approach corresponds to the modern cybersecurity studies that shape the issue of phishing as a more socio-technical challenge, as opposed to a more technical one [14],[15].

The phishing attacks are conceptualized in the model as a three-phase process that involves the attacker, the human user, and the information system. Attackers use social engineering methods to use psychological traps like authority, urgency, and trust, and the human user processes and reacts to these stimuli at different levels of awareness, workload, and experience. Security awareness training acts as a dieting intervention in this interaction, which will reinforce the capacity of the user to interpret deception and make rational choices prior to technical systems being intruded upon. The placement of training in the threat model also shows how human-centered controls enhance technical controls, which supports the empirical results of the study and generalizes them to a larger theoretical understanding [6],[12],[19].

From an operational perspective, the human-based threat model assists in the development of a combined approach to cybersecurity policies covering both behavioral and technical aspects of threat. This framework can help institutions to locate the areas of intervention where training, policy, and technical protection overlap so that the institution has a layered defense strategy that does not depend on one control. The model also has a conceptual basis for future research, such as the creation of predictive behavioral models and training systems of adaptation. Providing a visual combination of the empirical findings, comparison, and theoretical knowledge, Figure 5 will empower the input of the research and support the thesis that successful phishing mitigation should focus on human, technological, and organizational factors in the right proportions.

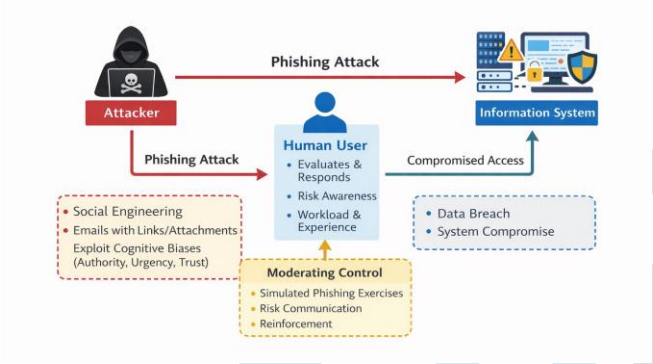

Fig. 7. Human Centered Phishing Threat Model

VII. Comparative Analysis with the Previous Empirical Studies

A. Comparison to Academic Phishing Studies

Phishing studies in academia have greatly focused on the vulnerability of users in educational institutions, all of which have found that human behavior is a significant consideration in successful entries. First large-scale experiments performed in universities show that a significant number of users become victims of phishing messages, even after learning about cyber threats, and the click-through rates tend to be more than a third of the population in real-life settings [49], [50]. The results create a critical weakness in the academic communities and highlight the issue of using technical defenses only.

Unlike numerous earlier scholarly works, the current study is more analytical as it bases its analysis on the behavioral manifestations and uses formal statistical testing to determine the relationship between security awareness training and phishing behavior. Although previous studies often use a pre- and post-training comparison or self-reported confidence and awareness assessments [50], they are likely to be affected by response bias or temporary learning effects. With the help of anonymized data on phishing simulation and categorical analysis, this study complies with the best practices in the research on behavioral cybersecurity that recommend actual user behaviors to be measured, as opposed to perceptions [51].

The results of this research are widely congruent with existing academic sources, as well as extending them in significant aspects. Like the previous studies, the findings indicate that security awareness training is linked to lower phishing vulnerability [49], [50]. The current paper, however, shows that the effect of training is not well distributed among the population of users, and a group of users has remained in high-risk behavior despite previous training. This fact is reflected by the academic results, highlighting the influence of cognitive habits, attention patterns, and contextual pressure on influencing user reactions toward phishing attacks [51], [52]. The trend analysis and risk profiling incorporated in the study bring the academic research on phishing to a more comprehensive view of the susceptibility as a spectrum and not a binary outcome, thus adding methodological and behavioral depth to the existing research.

B. Comparison with Industry and Government Reports

The government and industry cybersecurity reports offer a complementary view of the phishing research in academia, as they provide large-scale and real-world observations in various organizational settings. Organizations like Verizon, ENISA, Proofpoint, and NIST consistently list phishing and social engineering as the primary initial attack vectors in data breaches and security incidents [11], [9], [10], [53]. These reports represent the aggregated incident information of thousands of organizations, unlike the controlled academic studies, which illustrate the consistent patterns in the behavior of attackers and their susceptibility to users. In all industries, the human factor in contact with malicious emails continues to be a leading factor in compromise and supports the human approach to phishing mitigation tactics.

The findings of the current study demonstrate good conceptual consistency when compared to the findings of the industry and government. Industry reports keep stressing the fact that user awareness training helps to mitigate, although not to eliminate, phishing threats, the conclusion that reflects statistically significant but non-homogeneous training effect witnessed in this study [10], [11], [53]. To illustrate, the Verizon Data Breach Investigations Report points out that recurrent phishing failures are usually created by a limited group of users, which will be quite similar to the high-risk user profile defined in Chapter 5 of this study.

Though this is in line with each other, one of the major differences is methodological transparency and depth analysis. The industry and government reports normally use descriptive aggregation and trend summaries as opposed to using formal hypothesis testing or estimating the effect size. Although such reports are priceless in terms of situational awareness and policy direction, they seldom offer statistically validated conclusions between certain interventions, i.e., training attendance and behavioral change. The current work fills this gap by using inferential statistics analysis on behavioral statistics, and thus, supplements the knowledge about the large-scale industries with findings that are empirically defensible.

TABLE XV. COMPARISON OF INDUSTRY/GOVERNMENT FINDINGS AND CURRENT STUDY

Source	Scope	Primary Insight	Correlation to Current Study
Verizon DBIR [11]	Multi-sector, worldwide	Phishing is top breach vector	Bears out risk behavior preponderance
ENISA Threat Landscape [9]	EU-wide	Risk is lessened by training, unevenly so	Adaptive training is required
Evidence proof point human factor report [10]	Enterprise-oriented	Small group of users leads to the majority of incidences	Ought in line with risk profile findings
NIST Guidelines [53]	Policy and standards	Highlights sustained awareness programs	Prosecutes implications of the study
Current Research	Training environment	Lessens the vulnerability to the variability	Gives statistical confirmation

C. Differences in Methodology and Variations in Outcomes

Variations in the methodological design are crucial factors that determine the findings and meaning of phishing research between academic, industrial, and government research. Controlled experiments, simulated phishing, or survey-based tools are commonly used in academic research to enable the

researcher to isolate a set of variables (e.g., training exposure, cognitive bias, warning design) [49], [51], [52]. In comparison, the industry and government reporting is based on the aggregation of the incident on a large scale, analysis of logs, and the forensic examination of the breach, which is focused on the breadth and ecological validity rather than on the experimental control [11], [53], [56]. These methodological differences can be the reason why academic research usually generates subtle behavioral findings, whereas industry reports rely on macro-level trends and prevalence rates.

The current study lies somewhere between these two methods in terms of methodology. The study uses behavioral realism and analytical control by utilizing simulated phishing information gathered in a functioning academic setting. The methodology of the study is unlike survey-based approaches, which cannot measure observable user actions, resulting in reduced response bias and high construct validity [19], [36]. Simultaneously, whereas industry reports rely on basic statistical methods (mean, mode, median) to demonstrate the connection between training and behavior, the study employs the inferential statistical methods of chi-squared testing, estimation of effect size, and robustness analysis to state the relationships between training and behavior in a formal way. The resulting methodological stance permits statistically defensible and practical interpretable outcome comparisons that surmount the limitations that are often observed in academic and industry-oriented phishing research [35], [40].

These differences in outcomes between studies may then be interpreted as a role of methodological decision and not contradiction. Research using short-term training interventions tends to provide instant phishing clicks reduction, but longitudinal or incident-based studies indicate that the vulnerability of certain subgroups of users persists over time [10], [11], [50]. The current investigation balances these results by showing that although training induces a statistically significant overall decrease in the level of phishing susceptibility, its effectiveness differs among risk reductions of different users. This observation is in line with the literature urging the abandonment of binary measures of success in favor of more differentiated measures of behavior [38], [41].

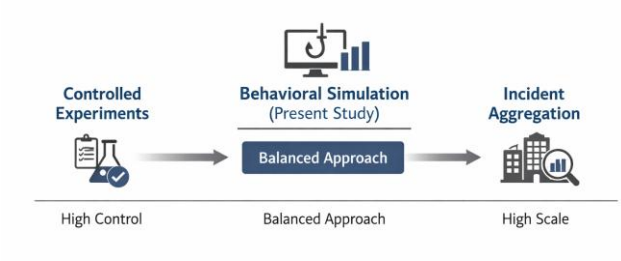

Fig. 8. Methodological Spectrum in Phishing Research

VIII. Phishing Risk Reduction Socio-Technical Framework

A. Rationale of Socio-Technical Approach

Technical defenses have not been sufficient to stop phishing attacks, which underscores the weaknesses of security strategies that emphasize the use of technological controls only. Although email filtering, machine learning detection engines, and threat intelligence systems have enhanced the ability to detect malicious content, attackers still use human decision-making to overcome these systems. Most of the works highlight that phishing is essentially a socio-technical issue, which is a product of an interplay between technical systems, the organizational structure, and human behavior as opposed to lone system vulnerabilities [35], [38], [41]. It is based on this appreciation that cybersecurity research has shifted towards frameworks that openly consider the human factor in addition to technical processes.

The socio-technical approach recognizes users to be working in complex settings that are influenced by policies, work processes, cognitive limitations, and social factors. Empirical experience in usable security and human-centered computing indicates that security measures that do not take these contextual factors into account tend to fail or are bypassed by users in the effort to get down to the business of accomplishing their main tasks effectively [43], [57]. The users in phishing cases need to read between the lines under time pressure and, therefore, are prone to being duped despite having technical indicators. Therefore, successful mitigation of phishing is based on a comprehensive view that coordinates system design, organizational practices, and user education. The results of the present research, especially the identified variability in the effectiveness of training according to the risk profiles, are empirical evidence of the importance of such an integrated approach.

The basis of suggesting a socio-technical framework in this paper is thus based on empirical evidence and consensus. The findings in Chapter 5 prove that although security awareness training has a positive impact on lowering the level of phishing, it does not protect all users uniformly. This finding agrees with previous studies that demonstrate that the effects of training depend on individual habits, situational pressure, and organizational reward systems [36], [39], [58]. The analysis of these findings brings together a disaggregated intervention into the context of a systematic framework, which bridges human behavior, technical controls, and institutional policy. This argument preconditions the framework elements and integration mechanisms, which are introduced in the remainder of this chapter.

B. Human, Technical, and Organizational Controls Integration

Phishing-related risks cannot be minimized by relying on one defense mechanism; instead, the combined efforts of human, technical, and organizational measures are necessary to minimize them. Earlier studies in socio-technical security underline that technical security measures like email filtering and authentication procedures minimize exposure but cannot address attacks that depend upon human judgment [38], [57]. On the other hand, interventions based on human factors, such as awareness training, can best be supported by conducive organizational policies and technical cues that can be used. The results of the current study, especially the fact that high-risk users remain after training, demonstrate the necessity of having a comprehensive approach that would coordinate the controls in these three areas.

In a humanistic approach, the user is affected by cognitive biases, habits, and situational pressures that affect their reaction to phishing attacks. Training programs also improve the recognition skills and awareness of threats, but the level of effectiveness is dependent on frequency, relevance, and reinforcement through the workflows [36], [39], [58]. Technical controls may facilitate human decision-making by giving them clear and timely indications of risk (e.g., warnings, authentication signals), and organizational controls set expectations, accountability, and a culture of shared responsibility. In case these aspects are not aligned, e.g., the warnings are incomprehensible, or the policies are punitive, users will get disengaged or devise workarounds which weaken the overall security [43], [62].

Phishing defense is long-term, and the integration of organizations is important in maintaining it. The policies of constant education, the absence of fear of punishment when reporting an incident, and risk assessment based on data allow institutions to change their defense in response to the shift in threats [53], [55]. Integration of controls also helps in targeted interventions, in which the organizations can deploy resources regarding the perceived risk profiles, as opposed to the rigid requirements.

TABLE XVI. PHISHING RISK CONTROLS SOCIO-TECHNICAL CONTROL INTEGRATION

Control Domain	Main Purpose	Examples	Role in the Present Study
Human	Behavioral awareness and decision-making	Training, habit formation	Moderates phishing susceptibility
Technical	Threat detection & signaling	Email filtering, warnings	Reduces exposure, supports users
Organizational	Governance and reinforcement	Policies, reporting culture	Maintains and aims at interventions

C. *Proposed Socio-Technical Framework for Reducing the Phishing Risk*

The proposed socio-technical framework of this study is a synthesis of the research results and empirical observations based on comparative analysis of the matter with the principles of human-focused cybersecurity. The framework is created to show that the phishing danger is the creation of human behavior, technical protection, and corporate governance, but not the failure of any of these aspects. Earlier studies have opined that phishing attacks are successful when some openings exist at the interfaces of these realms, especially when technical controls are inadequate to support human decision making or organizational policy fails to support the cause of safe behavior [35], [38], [57]. The framework here is based on this realization and explicitly plots empirical findings of different training effectiveness and continued high risk-user profiles onto an integrated control structure.

The fundamental issue with the framework is that human behavior is recognized as both a weakness and a strength of defense. Security awareness training enhances the capacity of the users to be aware of the phishing signals, yet cognitive habits, workload pressures, and environmental indicators temper the capabilities in the training [36], [39]. Technical controls, such as email filtering, authentication, and warning systems, can be used to minimize exposure and support the decision-making process, but should be usable and easy to understand to prevent alert fatigue or disengagement of users [62], [63]. Organizational controls such as policies, support of leadership, and incident-reporting culture are reinforcing mechanisms that will maintain behavioral change over time. The scheme incorporates these variables into a feedback-based model, in which the results of the behavior are used to make corrective changes to the training and the policy.

Notably, the framework presented is not just a mere conceptual one, but rather it is based on the empirical trends that have been found in this research. The discovery of the application of specific risk profiles and disproportionate training results highlights the necessity of risk-based interventions over specific security requirements. The framework facilitates a sensible roadmap in an institution aiming to operationalize evidence-based phishing mitigation strategies as it connects the observed behavior with control mechanisms across domains. It is an addition to existing socio-technical frameworks because it incorporates statistical data and ethical considerations into the design of the framework directly, thus filling the gap between theory, statistics, and practice [53], [58], [64].

Fig. 9. Socio-Technical Framework for Phishing Risk Reduction

IX. Implications to Cybersecurity Education and Training Design

A. *Principles to be designed in creating effective security awareness programs*

The issue of security awareness programs has been considered an important element of the organizational cybersecurity strategy since time immemorial, but the efficiency of this kind of program is closely tied to its design, delivery, and long-term reinforcement. Results of this experiment show that although awareness training has a significant effect on phishing vulnerability, it does not work equally well for all groups of users, which supports the conclusions of conclusions by the previous studies that generic, single-use training does not lead to any long-term behavioral change [10], [50], [55]. Improved training programs should thus be based on behavioral knowledge, and they should be congruent with the perception, processing, and reactions to security cues displayed in real-life situations. This requires a change of approach in compliance-focused teaching to behaviorally informed and user-focused training design.

Contextual relevance is one of the critical design principles that came forth in this study and in the literature. Realistic phishing-related training materials, organizational processes, and typical patterns of communication prove to increase learning retention and transfer [39], [58]. When the user can directly relate training examples to their everyday life, they tend to become more aware of the presence of threats and how to use the skills acquired under pressure. The quantitative findings of this study, especially the relative vulnerability demonstrated by the high-risk users, indicate that their relevance is not enough, and the training should also be dynamic, both in frequency and intensity. Reinforcement needs to be periodically applied, and scenarios need to vary to overcome habituation and cognitive overload, which is well known in usable security research [57], [62].

The other necessary design principle is feedback-based learning, in which the user can get constructive feedback promptly after a phishing simulation or incident. Instead of punishmentary measures, successful programs focus on learning how to make mistakes, strengthening good behavior, and making people speak up without fear of punishment [53], [64]. These strategies are in line with behavioral science as well as ethical considerations, promoting trust and shared responsibility. This principle finds its support in the study through the findings of the study that revealed that behavioral outcomes are useful cues in the personalization of training interventions. Through the incorporation of empirical feedback loops in designing training, organizations will be able to transition to evidence-based, continually improving awareness training that is sensitive to technical security objectives and human capabilities and limitations.

B. *Adaptive and Risk-Based Training Model*

Conventional security awareness intervention plans tend to take into consideration consistent training programs, which presuppose homogeneous behavior of the users, but the empirical results of the present study contradict this hypothesis, as they show that there is a great difference in

phishing vulnerability among different risky user profiles. High-risk users demonstrate more than baseline training, persistently high click rates, and low-risk users can be trained to behave on the side of security with little intervention. The results are consistent with larger research on cybersecurity, suggesting the adaptive and risk-based approach of training models, which assign educational materials based on observed behavior instead of organizational hierarchy and stationary position [10], [39], [53]. These models enable institutions to be more efficient and ethical in dealing with vulnerability by putting effort where it will result in maximum reduction of risk.

Adaptive training models are based on dynamic behavioral evaluation to change training frequency, content, and intensity. The results of phishing simulation, reporting behavior, and latency of response may be used as predictors of training recalibration through time [11], [55]. As an illustration, more frequent simulations, customized feedback, and scenario-based microlearning might help users who fall in the high-risk category, and periodical reinforcement may be sufficient in the case of low-risk users. Human-centered security studies have indicated that such kind of personalized interventions lower training fatigue without compromising vigilance, which is essential in the long-term sustainability of such programs [57], [62].

As per implementation, the risk-based training models are to be grounded in clear policies and ethical protection against abuse and stigmatization. The socio-technical frameworks of the study note that adaptive training needs to be constructed as a supportive tool and not a punitive one that builds trust and shared responsibility [64]. The institutions that implement such models must make sure that the risk classification is not disclosed, based on data, and reviewed regularly. Adaptive training can be improved by basing it on empirical evidence and ethical considerations to increase the resilience to phishing, as well as respect individual dignity and encourage a positive security culture in an organization.

TABLE XVII. RISK-BASED TRAINING MODEL BASED ON USER PROFILES

User Risk Profile	Behavioral Indicators	Training Frequency	Training Strategy
Low Risk	Infrequent phishing activity	Annual	Refresher training
Moderate Risk	Frequent clicks	Quarterly	Simulations by scenarios
High Risk	Repeat phishing clicks	Monthly	Targeted microlearning + feedback

C. *Institutional Implementation Reflections*

Scalability, governance, and organizational culture are critical issues that should be considered when implementing adaptive risk-based security awareness programs on an institutional level. Even though empirical evidence substantiates the use of delineated interventions, the institutions need to make sure that the implementation mechanisms are not incompatible with the current technical infrastructure and administrative procedures. Academic settings, especially large ones, experience issues of user diversity, decentralized IT governance, and differences in the degree of cybersecurity maturity between different departments. Previous research highlights the fact that in the absence of institutional alignment, there is a possibility that even properly designed training programs can not produce a long-term impact despite their design [53], [55].

The Governance structures are very vital in providing consistency, accountability, and ethical checking of the training deployment. The development of clear policies outlining the use of data, the criteria of risk classification, and feedback mechanisms is a necessity to ensure transparency and user trust [64]. The institutions should also have cross-functional cooperation among the IT security teams, academic leadership, and compliance offices to aid in the ongoing program of review and enhancement. According to research on the governance of organizational cybersecurity, leadership support and obvious commitment are essential factors that drive user involvement and program success [11], [38]. These are especially crucial in the implementation of adaptive models that are based on continuous behavioral observation and making decisions based on data.

Lastly, resource allocation and long-term sustainability should be done through institutional implementation. An adaptive training system involves spending on the simulation platform, analytics services, and other personnel skills on how to treat the behavioral data responsibly. Nevertheless, there is an indication that cost reduction can eventually be achieved through targeted interventions to direct the resources towards high-risk locations and curb expensive security incidents [10], [53]. With the implementation strategies aligned with the empirical results, the ethical principles, and the organizational capacity, the findings of this study can be operationalized by the institutions in a rather efficient and responsible way, so that the concept of cybersecurity education can be promoted as one of the cornerstones of institutional resilience.

TABLE XVIII. INSTITUTIONAL CONSIDERATIONS OF ADAPTIVE TRAINING IMPLEMENTATION

Implementation Dimension	Key consideration	Institutional Actions
Governance	Transparency, accountability	Define policies and oversight committees
Scalability	User differentiation, infrastructure	Modular training platforms
Ethics	Privacy, justness	Anonymization, Consent
Sustainability	Resources, staffing	Focused investment strategies

X. IMPLICATIONS OF POLICY AND GOVERNANCE

A. *Implication of Institutional Cybersecurity Governance*

The study findings are significant to institutional cybersecurity governance, especially in academic settings where the risk is hard to manage due to decentralized structures and a mixed user population. The classic models of governance tend to focus on technical compliance and perimeter security, but empirical studies conducted in the framework of this study support the need to integrate human behavioral evidence in the governance decision-making process. The governance frameworks are progressively appreciating that the behavior of users should be a quantifiable risk factor, but not an uncontrollable variable [53], [55]. This study empirically supports the adoption of behavioral measures in the governance of institutions by showing a statistically significant relationship between security awareness training and phishing vulnerability.

Cybersecurity governance demands that there be policies that help in sustained monitoring and evaluation of security controls and adaptation. The findings of the study indicate that governing institutions are supposed to shift their focus from existing policy administration to the evidenced-based administration where the effectiveness of training programs, user-risk profiles, and incidence trends guide policy choices. The frameworks like NIST SP 800-53 focus on the necessity of continuous risk assessment and control optimization, but do not always provide a clearer direction on how operationalization of behavioral data can be put into practice [53]. The methodology used in this paper provides a viable

route to entrench behavioral evidence in governance practices so that institutions could have a priority of interventions founded on risk evidence and not on generalized assumptions.

Moreover, government mechanisms should strike a balance between safety goals and moral responsibility and integrity. The policies regarding data collection and risk classification, as well as training escalation, must be well recorded and conveyed to the stakeholders to ensure trust and validity are observed [64]. The socio-technical model introduced in Chapter 9 is the one that will facilitate the governance models capable of harmonizing institutional power with the empowerment of the users, as opposed to surveillance or punitive control. By basing governance judgments on empirical results and moral values, organizations can inculcate a culture of collective responsibility that will increase effectiveness in security as well as integrity within the organization.

B. *Ethical Behavioral Security Data Usage*

There is a growing dependency on behavioral data to make decisions on cybersecurity, and this presents critical ethical issues on privacy, fairness, and proportionality. Although empirical data is shown to be of great value in determining patterns of risk and enhancing the effectiveness of training, phishing simulation data has to be gathered and utilized cautiously so that the trust of users is not diminished or that the ethical standards are not breached [64], [60]. Governance structures have noted that behavioral surveillance ought to be protective and educative as opposed to surveillance and enforcement of punishment [53]. The current study addresses these principles by using group-level patterns based on anonymized and aggregate data and not attributing any individual actions, which is the main idea of the study to adhere to the principles of empirical rigor and accountability.

The transparency under which behavioral security data is collected, interpreted, and applied in institutional decision-making is also part of the ethical use of behavioral security data. The users must be notified of the intent of the phishing simulation, the type of data gathered, and how they can be useful to enhance security practices instead of measuring the individual performance [55], [38]. Previous studies in digital ethics and usable security have indicated that the lack of transparency about the use of data can result in resistance, disengagement, or attempts to bypass security controls [60], [62]. In comparison, open political governance policies create a feeling of collective ownership and strengthen the educative purpose of awareness campaigns. Such transparency is supported by the socio-technical framework upon which the present study is built, which leaves no doubt the connection of behavioral information to adaptive training and policy modification as opposed to disciplinary action.

Also, it requires ethical governance that requires the presence of oversight, review, and redress that allow the behavioral data to not be abused or misinterpreted. Institutions need to set specific boundaries on data storage, data access, and secondary usage, especially when behavioral analytics are used to determine risk classification or resource allocation [64]. Ethical review procedures, such as periodic audit and consultation with stakeholders, can assist in balancing the security practices with the institutional values and the values of the larger society. The ethical protection of data in governance can help organizations employ the behavioral security information to be more resilient and respect the values of fairness, dignity, and respect, which are the concepts that can be found in both professional ethics and the Christian worldview, as discussed in this paper.

TABLE XIX. ETHICS AND GOVERNANCE POLICIES OF BEHAVIOURAL SECURITY DATA

Ethical Principle	Risk Mitigated	Governance Control
Privacy	Illegal disclosure of data	Anonymization, control of access
Openness	User distrust	Open-mindedness, approval
Fairness	Discriminatory profiling	Group-level analysis
Responsibility	Data abuse	Auditing, oversight committees

XI. Christian and Ethical Reflection

A. *Integrity and Honesty in Research*

Honesty and integrity are some core values of ethics in both science and the Christian worldview, and they determine how research is conducted, designed, analyzed, and reported. In the framework of computer science and cybersecurity studies, integrity demands that information is processed in transparent ways, that statistical procedures are used in proper manners, and conclusions are reported without any manipulation and focus on results [29],[34]. The paper demonstrates research integrity because of the vivid documentation of methodological decisions, explicit declaration of assumptions and limitations, and description of the statistical findings, including the effect size, in a balanced and honest way. The Christian ethical approach to integrity represents a desire to seek the truth and have a sense of moral responsibility because it is important to acknowledge that knowledge and technological capacity should be utilized in a humble and responsible way [35]. The study does not overestimate the efficacy of the security awareness training and does not neglect the risk remaining, which ensures that the conclusions are not idealistic, but rather grounded in evidence. With professional research ethics in line with the Christian values of honesty and faithfulness, the paper shows that effective computer science research and ethical stewardship are not antagonistic values that cannot coexist; rather, they are supportive commitments.

B. *Stewardship and Responsibility in Data and Technology*

Christian view on the world is rooted in the principle of stewardship that has profound consequences on the process of computer science research, especially on the data, security, and human behavior targets. Stewardship is about the effective and proper use of resources granted to persons, such as information, technological skills, and analytical equipment. This principle, as applied in cybersecurity research, can be interpreted as cautious work with sensitive information, respect for privacy, and ethical use of the data to secure and not abuse the users [35],[36]. This paper is also scholarly in that it uses anonymized, non-invasive data, and the analysis of the paper is aimed at enhancing the practice of institutional security rather than placing the blame on users.

The accountability of technology use also depends on the fact that the results of research should be implemented in a manner that allows human welfare and harm reduction. As a professional and Christian ethical issue, cybersecurity research must be able to work towards the provision of a safer digital space and assist communities to navigate through technological risks responsibly [29],[34]. The results of the present research indicate the significance of evidence-based security awareness training as a security measure against social engineering attacks. Instead of positioning the users as a liability, the study focuses on empowering the users by educating them and empowering them by continuously enhancing them. This method shows service-based commitment and the acknowledgment of the fact that technological expertise comes with a sense of responsibility to protect others and to develop systems and interventions that

foster trust, resilience, and responsible use of digital technologies.

C. Respect for Human Dignity and Social Responsibility

Human dignity is a theory of Christian ethics and a crucial factor in human-focused computer science studies. When working with cybersecurity in the context of user behavior, this principle demands equal consideration of individuals irrespective of their risk metrics or failure point in a security system [29],[36]. Through the aggregate level of analysis of phishing vulnerability and the lack of identification and stigmatization of persons or groups, this research demonstrates respectfulness to human dignity. Users are not depicted as weak links but as participants in the growing complex worlds of the Internet. This is a kind of solution that is congruent with ethical research practice that is concerned with human well-being and acknowledges the intrinsic value of each human being, despite their technical expertise.

Social responsibility goes even further by highlighting the overall wider social implications of technological research. Research in the field of cybersecurity has a duty to help in making digital worlds safer, more equal, and to help institutions keep their communities out of harm [34],[37]. The results of this paper prompt a shift towards supportive and educative security implementation over punitive and surveillance-based strategies. The research aligns with the Christian values of service and care towards others by encouraging awareness, empowerment, and constant learning. The combination of respect and responsibility is what makes technological development a tool of human prosperity and the ethical duty of the researchers to consider the social implications of their work.

D. Ethical Framework Integration and Research Accountability

Computer science research has more than just individual thinking with respect to data management or protection of research subjects, and should be applied across the research lifecycle, such as problem creation up through publication of the research results. This paper is an example of such integration, where ethical and Christian principles of integrity, stewardship, respect for human dignity, and social responsibility have been considered in every step of the research process. The transparency of methodological reporting, proper justification of statistical methods, and sincere admittance of limitations and threats to validity are instances of accountability [29],[34]. Instead of claiming that the results were conclusive and applicable to the general population, the study puts results into their proper empirical and contextual contexts to build a responsible scholarship. According to the Christian worldview, accountability emphasizes the ideology that the results of research must be dedicated to the common good and must positively impact society [35],[36]. This study confirms that there are no moral and ethical differences when using technology as a tool of inquiry, but that there are moral, professional, and ethical responsibilities as outlined in the principle of truthfulness, justness, and service. Such a systematized ethical structure makes the study more credible and makes its additions to the field of cybersecurity knowledge sound in terms of its technical and moral basis.

E. Justice, Fairness, and Bias in Human-Centered Cybersecurity

One fundamental Christian ethical issue that will apply to human-focused research on cybersecurity is the desire to achieve justice and fairness in designing, implementing, and reviewing security interventions. Justice in the framework of phishing mitigation must be wary of the impacts of security awareness interventions on various categories of users and whether these interventions carry unintended consequences on other groups of users. Previous studies note that people differ greatly in terms of cognitive capacity, technical knowledge, language skills, and resource accessibility, all of which have the potential to affect vulnerability to phishing attacks. Ethically, people must not be stigmatized or sanctioned by cybersecurity measures that identify them as being at higher risk but rather empower and support them through fair and compassionate approaches to address the matter.

This research seeks to resolve the issues of equity and bias through prioritizing behavioral results and not individual traits and anonymizing and aggregating the data to avoid discriminatory classification of individuals. The analysis model focuses on group-level pattern of risks instead of moralizing individual users in accordance with the Christian theory of grace, humility, and justice. Furthermore, the findings advocate a model of cybersecurity governance that emphasizes inclusion and restoration instead of exclusion because of promoting tiered and adaptive training instead of punitive controls. By so doing, the study portrays how ethical reflection may be used to make the proper application of empirical results in a manner that does not only respect the dignity of individuals but also collective security.

F. Future Research and Cybersecurity Policy Ethical Implications

This research has significant ethical implications on future research and institutional policy making in cybersecurity other than its direct findings. With the growing use of data-based approaches to evaluate user behavior and riskiness by organizations, ethical protection needs to keep pace with the sophistication of analytics. Christianly, the future studies need not abandon truth seeking, transparency, and dedication towards the common good as a guiding principle so that technologic innovations cannot be used to act productively to the common good of humanity but towards efficiency. It is the moral duty of researchers to speak truthfully about the limitations and not overstate claims of causality and to resist the temptation to use research in a manner that negatively affects ethical integrity or trust in humans.

At the policy level, the incorporation of ethical reflection in the decision-making process of cyberspace will stimulate the institutions to integrate strategies that reconcile the interests of security with compassion, charity, and responsibility. According to the results of the present research, it appears that evidence-based training programs in the framework of ethical principles may both increase the level of security and cultivate a culture of collective responsibility, as opposed to fear or control. In the future, Christian ethics should encourage scientists and other actors to consider cybersecurity not as a technological problem but as a moral mission that influences the way groups defend each other in an ever more digitalized world. This view supports the importance of ethical scholarships in not only informing future lines of research but also in responsible management of the practice of cybersecurity.

XII. Conclusion and Future Work

A. Conclusion

This study examined the dependence between security awareness training and phishing vulnerability in an academic setting through a behavior-based analytic study. The study found a statistically significant and practically substantial relationship between training attendance and decreased phishing clicking behavior by using the chi-square test of independence on the data received in the phishing simulation. The results would support the efficacy of security awareness training as a human-centered measure of cybersecurity control, as previously described, and enhance the existing research by applying a rigorous statistical test and effect size analysis. The study provides, through a well-crafted methodological design, transparent reporting, and ethical integration, evidence-based data on the ability to influence the

behavior of users to enhance the institutional cybersecurity posture.

This study highlights the significance of observing the behavior of cybersecurity interventions and not merely self-reported awareness. The fusion of ethical theories in Christianity, integrity, stewardship, human dignity, and social responsibility sheds light on the fact that good computer science research must be both technically rigorous and ethically responsible. The study advances an ethical and supportive concept of cybersecurity education by positioning users as security partners and not liabilities. Altogether, the study proves that quantitative analysis with ethical reflection results in findings that are scientifically valid, socially responsible, and morally responsible.

In addition to its empirical results, the research has shown the importance of an interdisciplinary approach to cybersecurity research, which combines both the human-centered approach and strict statistical analysis. The study strengthens the position that the behavior of users is a decisive factor of organizational security by systematizing the study of the correlation between security awareness training and phishing vulnerability. The stratification of analysis, which includes descriptive statistics, inferential tests, the interventions of effect sizes, and risk stratification, makes it possible to obtain an in-depth picture of how the training affects the behavior in various user profiles. This methodological richness also adds to the increasing evidence of the fact that interpretable behavior-oriented analytics can be used to generate actionable insights without compromising transparency or reproducibility. Since the nature of cybersecurity threats is still changing, these empirically informed methods are critical towards closing the divide between the theoretical framework and the actual security decision-making process.

This is also vital, as the research reveals the need to introduce ethics and Christian values in the development and use of cybersecurity technologies. The phishing mitigation research presents it as a moral obligation of researchers, institutions, and practitioners (who should also focus on integrity, stewardship, fairness, and respect to human dignity) rather than a technical challenge. The results indicate that evidence-based training that is ethically guided could contribute to improving security and developing trust, accountability, and collective responsibility in digital communities. The study in this respect adds to a wider perspective of cybersecurity as a field that is useful in the flourishing of human beings, offers fair and amicable practices, and gives responsible innovation. These findings highlight the need to keep on harmonizing empirical rigor and ethical consideration with the future of cybersecurity research.

B. Future Work

This study can be further developed in future research with the implementation of a longitudinal research design to investigate how the efficiency of security awareness training changes with time. Although the current research offers cross-sectional data on the association between training and phishing vulnerability, longitudinal research would allow the researcher to evaluate behavioral persistence, decay of learning, and long-term effects of repeated training programs. Measuring the responses of users on repeated phishing experiments may demonstrate the maintenance or attenuation of improvements in the absence of reinforcement to overcome the limitation of that [6],[18] detected in the previous behavioral studies of cybersecurity [1]. This would enhance the power of causal inference and give a better understanding of the way training programs can be streamlined towards sustainable behavior change.

Future research can include richer variables of behaviour and context to achieve a greater level of analysis. User role, academic levels, previous experience in cybersecurity-related behaviors, email-based behaviors, and reporting behavior might also be incorporated to create more specific models of phishing vulnerability. By incorporating these variables, one would be able to do multivariate analysis that utilizes logistic regression or machine learning classifiers to supplement chi-square-based analysis in this study. Besides, the comparison of various training modalities may be used to determine which instructional modalities have the strongest behavioral effect, i.e., gamified learning, adaptive simulation, or AI-generated personal training [22],[25].

Lastly, it can be noted that future research may expand the institutional and ethical boundaries of the research by investigating the vulnerability of phishing in different organizational and cultural settings. The external validity and generalizability would be improved by enlarging the sample size with a variety of universities or comparing academic with corporate environments. Ethically, future research can go even further and examine how Christian values of stewardship, service, and care to the community can be applied to the design of future cybersecurity education programs, which will emphasize empowerment over surveillance. By combining innovative analytical methods and ethics-based research approaches, the upcoming research will help to devise more efficient, fair, and human-oriented approaches towards cybersecurity.

Future results that are likely to be attributed to this direction of study are likely to enrich the knowledge on how the security awareness training gain is likely to interact with the changing behavior of the user and the changing nature of threats over time. With the emergence of longitudinal datasets, future research can help reveal trends of training decay, adaptation to behavior, and the sustainability of security interventions over the long term and provide more information than is available in the short term. Also, adding contextual variables, e.g., task pressure, communication medium, and sophistication of the attacker, can possibly show finer risk behavioral profiles that cannot be detected using solely cross-sectional analysis. Further progress in understandable analytics and hybrid socio-technical solutions will also support a greater ability to distinguish between habitual and situational lapses and will be used to inform more adaptive and individualized training approaches. Ethically, the results of the future research will help to deepen our understanding of how evidence-based cybersecurity practices can be made in line with the concepts of fairness, inclusion, and human dignity so that the growing data-driven policies on security could remain relevant to organizational resilience and social well-being. The combination of these expected results suggests a more mature, ethically informed, behaviorally informed cybersecurity research agenda.

ACKNOWLEDGEMENT

My personal appreciation goes to Dr. Kamala Marepalli, who guided, supported, and instructed me on the course CSCI 591A -C: Computer Science Research Methods. Her clear exposition of research methods, focus on ethics and Christian morals in computer science research, and positive feedback had a great influence on directing the quality of this research work. I also owe my success in finishing this study to the academic resources and educational settings that were provided by the institution. Any remaining limitations or errors in this work are solely my responsibility.

REFERENCES

[1] I. Sommerville, Software Engineering, 10th ed. Boston, MA, USA: Pearson, 2016.

[2] A. Stallings, Network Security Essentials, 6th ed. Boston, MA, USA: Pearson, 2018.

[3] R. Anderson, Security Engineering, 3rd ed. Hoboken, NJ, USA: Wiley, 2020.

[4] M. Bishop, Computer Security: Art and Science, 2nd ed. Boston, MA, USA: Addison-Wesley, 2018.

[5] W. R. Shadish, T. D. Cook, and D. T. Campbell, Experimental and Quasi-Experimental Designs, Boston, MA, USA: Houghton Mifflin, 2002.

[6] J. W. Creswell and J. D. Creswell, Research Design, 5th ed. Thousand Oaks, CA, USA: Sage, 2018.

[7] D. C. Montgomery, Design and Analysis of Experiments, 9th ed. Hoboken, NJ, USA: Wiley, 2017.

[8] G. James et al., An Introduction to Statistical Learning, 2nd ed. New York, NY, USA: Springer, 2021.

[9] ENISA, Threat Landscape Report, European Union Agency for Cybersecurity, 2023.

[10] Proofpoint, State of the Phish Report, Proofpoint Inc., 2023.

[11] Verizon, Data Breach Investigations Report, Verizon Enterprise, 2023.

[12] S. Garfinkel, Database Nation, Sebastopol, CA, USA: O'Reilly, 2000.

[13] B. Schneier, Secrets and Lies, New York, NY, USA: Wiley, 2000.

[14] B. Schneier, Click Here to Kill Everybody, New York, NY, USA: W. W. Norton, 2018.

[15] K. Mitnick and W. Simon, The Art of Deception, Indianapolis, IN, USA: Wiley, 2002.

[16] K. Mitnick, The Art of Invisibility, New York, NY, USA: Little, Brown, 2017.

[17] N. Kshetri, "The economics of phishing," IEEE Security & Privacy, vol. 4, no. 4, pp. 87–89, 2006.

[18] J. Hong, "The state of phishing attacks," Communications of the ACM, vol. 55, no. 1, pp. 74–81, 2012.

[19] R. Dhamija, J. Tygar, and M. Hearst, "Why phishing works," Proc. CHI, pp. 581–590, 2006.

[20] A. Vishwanath, "Habitual social media use and deception," Journal of Computer-Mediated Communication, vol. 20, no. 1, pp. 1–16, 2015.

[21] A. Vishwanath, The Weakest Link, Cambridge, MA, USA: MIT Press, 2017.

[22] S. Sheng et al., "Who falls for phish?" Proc. CHI, pp. 373–382, 2010.

[23] P. Kumaraguru et al., "Teaching Johnny not to fall for phish," ACM TOCHI, vol. 17, no. 2, 2010.

[24] A. Field, Discovering Statistics Using IBM SPSS, 5th ed. London, UK: Sage, 2018.

[25] J. Cohen, Statistical Power Analysis, 2nd ed. Hillsdale, NJ, USA: Lawrence Erlbaum, 1988.

[26] G. Casella and R. Berger, Statistical Inference, 2nd ed. Belmont, CA, USA: Duxbury, 2002.

[27] R. De Veaux et al., Intro Stats, 5th ed. Boston, MA, USA: Pearson, 2018.

[28] D. Rumsey, Statistics for Dummies, Hoboken, NJ, USA: Wiley, 2016.

[29] L. Floridi, The Ethics of Information, Oxford, UK: Oxford Univ. Press, 2013.

[30] L. Floridi, "Digital ethics," Philosophy & Technology, vol. 33, pp. 547–566, 2020.

[31] NIST, SP 800-53 Rev. 5: Security and Privacy Controls, NIST, 2020.

[32] NIST, SP 800-61 Rev. 2: Incident Handling Guide, NIST, 2012.

[33] ISO/IEC 27001, Information Security Management Systems, ISO, 2013.

[34] ISO/IEC 27002, Information Security Controls, ISO, 2013.

[35] C. Rudin, "Stop explaining black box ML models," Nature Machine Intelligence, vol. 1, pp. 206–215, 2019.

[36] L. Cranor and S. Garfinkel, Security and Usability, Sebastopol, CA, USA: O'Reilly, 2005.

[37] L. Cranor, "Designing usable security," Proc. SOUPS, 2008.

[38] A. Adams and M. A. Sasse, "Users are not the enemy," Communications of the ACM, vol. 42, no. 12, pp. 40–46, 1999.

[39] A. Beautement et al., "The compliance budget," Proc. NSPW, pp. 47–58, 2008.

[40] M. Junger et al., "Measuring human factors in cybersecurity," IEEE Security & Privacy, vol. 18, no. 4, pp. 67–75, 2020.

[41] N. A. G. Arachchilage and S. Love, "Security awareness effectiveness," Computers in Human Behavior, vol. 52, pp. 99–109, 2014.

[42] J. Reason, Human Error, Cambridge, UK: Cambridge Univ. Press, 1990.

[43] D. Norman, The Design of Everyday Things, rev. ed. New York, NY, USA: Basic Books, 2013.

[44] K. E. Weick, Sensemaking in Organizations, Thousand Oaks, CA, USA: Sage, 1995.

[45] T. Denning, "Cybersecurity and ethics," IEEE Technology & Society, vol. 38, no. 3, pp. 30–36, 2019.

[46] J. Van Dijk, The Network Society, London, UK: Sage, 2020.

[47] M. Spiekermann, Ethical IT Innovation, New York, NY, USA: Routledge, 2016.

[48] Cambridge Papers, "Christian ethics and research integrity," Cambridge Univ., 2019.

[49] J. Stottlemeyer, "Ethics in computing," Journal of Computing Sciences, vol. 14, no. 2, pp. 45–58, 2021.

[50] P. Lin et al., Robot Ethics, Cambridge, MA, USA: MIT Press, 2012.

[51] IEEE, Code of Ethics, IEEE, 2020.

[52] ACM, ACM Code of Ethics, ACM, 2018.

[53] World Economic Forum, Global Cybersecurity Outlook, WEF, 2023.

[54] OECD, Digital Security Risk Management, OECD Publishing, 2020.

[55] S. Harris, CISSP All-in-One Guide, 9th ed. New York, NY, USA: McGraw-Hill, 2022.

[56] R. Peltier, Information Security Policies, Boca Raton, FL, USA: CRC Press, 2016.

[57] J. L. Gibbs, Christian Ethics, Nashville, TN, USA: Abingdon Press, 2014.

[58] J. Stassen and D. Gushee, Kingdom Ethics, Downers Grove, IL, USA: IVP, 2016.

[59] N. Wolterstorff, Justice, Grand Rapids, MI, USA: Eerdmans, 2008.

[60] J. MacArthur, Biblical Ethics, Chicago, IL, USA: Moody Press, 2011.

[61] R. Plantinga, Engaging God's World, Grand Rapids, MI, USA: Eerdmans, 2002.

[62] J. Hughes, Christian Worldview and Scholarship, Downers Grove, IL, USA: IVP, 2017.

[63] A. Holmes, The Idea of a Christian College, Grand Rapids, MI, USA: Eerdmans, 1987.

[64] T. Wright, After You Believe, New York, NY, USA: HarperOne, 2010.

[65] C. Wright, Old Testament Ethics, Downers Grove, IL, USA: IVP Academic, 2004.