Journal of Risk and Control, Vol. 13, No. 1, 2026, 253-278
ISSN: 2056-3701 (print version), 2056-371X (online)
https://doi.org/10.47260/jrc/13110
Scientific Press International Limited

Adaptive Phishing Simulation and Longitudinal Employee Security Behavior: Evidence from a Global Enterprise

Cheng-Wen Lee[1] and Ming-Yung Chen[2]

Abstract

Phishing continues to be one of the most persistent cybersecurity threats, with employees remaining the primary target of social engineering attacks. Although phishing awareness training is widely implemented, limited empirical evidence exists regarding its long-term effectiveness in real organizational environments. This study investigates the impact of adaptive phishing simulations on employee cybersecurity behavior using longitudinal data collected from a multinational enterprise between 2023 and 2025. The dataset comprises 20 phishing simulation campaigns conducted across five organizational departments, enabling the examination of phishing click rates, credential submission rates, departmental behavioral differences, and security awareness improvement over time. The results demonstrate that repeated adaptive phishing simulations significantly reduce phishing susceptibility, with the greatest behavioral improvements observed in departments initially exhibiting the highest risk levels. The findings further reveal that phishing vulnerability varies across departments, supporting the need for risk-based and department-specific awareness strategies rather than uniform training programs. Based on the empirical evidence, this study proposes a Security Awareness Maturity Model to evaluate the progression of organizational cybersecurity behavior. The research contributes to the cybersecurity literature by providing rare longitudinal evidence from a real enterprise setting and offers practical guidance for designing adaptive phishing awareness programs that strengthen employee resilience, cybersecurity governance, and organizational cyber resilience.

JEL Classification: M15, M12, D83, L86.
Keywords: Adaptive Phishing Simulation, Cybersecurity Awareness, Social Engineering, Longitudinal Study, Employee Security Behavior, Cyber Resilience.

[1] Department of International Business, College of Business, Chung Yuan Christian University. Taoyuan City, Taiwan.
[2] Ph. D. Program in Business, College of Business, Chung Yuan Christian University. Taoyuan City, Taiwan.

Article Info: *Received:* July 2, 2026. *Revised:* July 13, 2026.
Published online: July 17, 2026.

1. Introduction

Modern cyber-attacks have become increasingly sophisticated and persistent, posing significant threats to organizations worldwide. Among various forms of cybercrime, phishing remains one of the most effective attack vectors for compromising enterprise systems, stealing credentials, and facilitating ransomware deployment (Weinz et al., 2025). Despite substantial investments in advanced security technologies such as Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and Zero Trust Architecture, human factors continue to represent one of the most critical vulnerabilities in organizational cybersecurity (Weinz et al., 2025).

Security awareness training is commonly conducted through online courses, workshops, and periodic educational campaigns. However, such programs do not necessarily produce sustainable behavioral changes and often fail to maintain employee vigilance against increasingly sophisticated phishing attacks (Lain et al., 2024). Existing studies suggest that traditional awareness programs frequently emphasize knowledge acquisition rather than long-term behavioral adaptation, thereby limiting their effectiveness in mitigating phishing risks (Rozema & Davis, 2025).

With the rapid evolution of phishing techniques, including AI-generated phishing emails, spear-phishing campaigns, and QR-code phishing (quishing), organizations require more adaptive and personalized security awareness approaches to maintain employee vigilance and resilience (Weinz et al., 2025). Adaptive phishing simulation has emerged as a promising solution because it enables organizations to adjust phishing scenarios, attack complexity, and thematic content according to employees' prior performance and risk profiles. Recent research suggests that adaptive and AI-powered cybersecurity training may improve user engagement and create more effective learning experiences than traditional one-size-fits-all awareness programs (Gulle et al., 2024).

Although adaptive phishing simulation has gained increasing attention, empirical evidence regarding its long-term implementation and effectiveness within enterprise environments remains limited. Most prior studies have relied on short-term experiments or cross-sectional designs, restricting the understanding of how employee cybersecurity behaviors evolve over time (Toth, 2024). Furthermore, a substantial proportion of phishing-awareness research has been conducted using university students rather than employees in real organizational settings, limiting the generalizability of findings to enterprise environments (Lain et al., 2024). Previous studies have also rarely examined behavioral differences among organizational departments or investigated how repeated phishing simulations contribute to cybersecurity maturity and organizational cyber resilience (Ho et al., 2026).

Another important yet underexplored issue concerns the potential existence of security fatigue. While repeated phishing simulations may improve awareness and vigilance, excessive exposure could potentially reduce employee engagement or lead to habituation effects over time. Recent longitudinal studies have emphasized the need for additional research examining both the benefits and unintended consequences of continuous phishing training programs in organizational settings (Toth, 2024).

To address these research gaps, the current study utilizes a unique longitudinal dataset collected from a multinational corporation over a three-year period through adaptive phishing simulation campaigns. By examining employee responses across multiple organizational units and simulation rounds, this study investigates how adaptive phishing training influences cybersecurity behavior, security awareness, and organizational cyber resilience. The findings are expected to contribute to cybersecurity awareness theory and organizational security management practices by providing empirical evidence regarding the effectiveness of adaptive training strategies in enterprise environments. Moreover, the study responds directly to recent calls for longitudinal and real-world organizational research on phishing awareness and behavioral cybersecurity interventions (Ho et al., 2026; Toth, 2024).

The objectives of this study are as follows:

1. To explore the long-term effects of adaptive phishing simulations on employee phishing click rates.
2. To examine behavioral differences among organizational departments.
3. To determine whether repeated phishing simulations improve employee cybersecurity awareness.
4. To identify cybersecurity behavioral maturity levels across organizational units.
5. To investigate the relationship between adaptive phishing training and organizational cyber resilience.

This study addresses the following research questions: **RQ1:** Can adaptive phishing simulations significantly reduce phishing click rates over time? **RQ2:** Are there significant behavioral differences among organizational departments? **RQ3:** Does repeated phishing training improve employee cybersecurity awareness? **RQ4:** Do high-risk departments demonstrate greater behavioral improvement over time? **RQ5:** Does long-term phishing simulation introduce security fatigue effects?

2. Literature Review

Considering the evolution of cybersecurity through digital transformation and advanced cyberattacks, phishing and social engineering continue to pose significant issues for enterprise cybersecurity strategies. Several studies have noted that phishing cannot be considered just another technical issue, but rather a behavioral aspect, where employees act as the last line of defense against deceptive messages. Franz et al. (2021) introduced a taxonomy of user-focused phishing intervention techniques and noted that the solution to phishing attacks is based on the involvement of users, timing of interventions, and human response, instead of using technology alone.

For the purpose of exploring adaptive phishing simulations and long-term security behaviors among employees, this literature review will cover five critical aspects including phishing and social engineering attacks, cybersecurity awareness training, simulated phishing attacks, adaptive personalization in security awareness, and long-term behavioral change.

2.1 Phishing and Social Engineering Attacks

The type of deception known as phishing is a very prevalent kind of social engineering trick that is used to fool the user to either reveal their credentials, click malicious links, download malicious software or perform business-related actions that are outside their responsibilities. Phishing, according to recent findings, is no longer generic deceptive emails but has evolved into complex and context-aware attacks targeting vulnerabilities arising from the human element. Jabir et al. (2025) indicated that generative AI technology has raised the bar for phishing, allowing criminals to generate highly convincing messages.

It can be seen that the human factor plays an important role in phishing risk. In fact, recent studies show that phishing attacks typically target human vulnerabilities such as urgency, authority, fear, curiosity, workload pressure and insufficient awareness of the issue. Jabir et al. (2025) reiterated that the lack of awareness and knowledge and insufficient resources on the part of the victim were also crucial in successful phishing attacks. This means that phishing prevention cannot be achieved solely with technical solutions. Despite having email filtering, endpoint security, and identity management technologies, the end-user may be fooled by highly contextualized phishing emails.

2.2 Cybersecurity Awareness Training

Awareness programs aimed at cybersecurity have become popular in minimizing the risks associated with human error and enhancing the capability of employees to detect and deal with phishing attacks.

According to Prümmer et al. (2024), the majority of cybersecurity studies indicate a positive impact, although many of these have been conducted using small sample sizes, non-experimental designs, or non-employee participants.

Another meta-analysis conducted by Prümmer et al. (2025) has concluded that cybersecurity training has a positive impact on end users, especially when considering the knowledge and attitudes of trainees. The impact on their behavior is much weaker and inconsistent, implying that raising awareness is not sufficient to ensure secure behavior.

Marshall et al. (2024) have also found that the existing measures to train people on phishing only reduce the vulnerability of around 23% of the users to phishing emails. As mentioned in the scoping review, the majority of these studies emphasize short-term outcomes while long-term effects have not yet been examined.

These results imply that awareness training may not be enough to minimize risk. Repeated exposure, engagement, and feedback have to be provided to make this training more effective. This can explain why simulated phishing exercises are important to implement in organizations.

2.3 Simulated Phishing Campaigns

One of the strategies employed to assess employee vulnerability to phishing attacks and develop appropriate security behavior is phishing simulations. This kind of strategy involves sending phishing emails to staff, analyzing how they respond, and offering further instruction based on their actions.

However, some studies suggest that the use of such phishing simulations may be ineffective. Brunken et al. (2023) discovered that while numerous organizations use such programs for education and to produce behavioral metrics, they should keep in mind that there could be associated costs, such as lowered staff morale, concerns about efficiency, and efforts required.

Moreover, Lain et al. (2024) performed a wide-ranging phishing experiment, engaging over 14,000 individuals in it during 15 months. The researchers found that employees became less vulnerable to phishing scams through the process of training after phishing failed, but they also noted that some unexpected consequences might arise from it. At the same time, employees themselves were capable of functioning as a collective monitoring mechanism.

In a related study, Schöps et al. (2024) analyzed simulated phishing attacks with regard to the employee's point of view. It was found that employees clicking on the simulated emails were more stressed out and had lower phishing self-efficacy compared to employees who reported those emails. Thus, it may be concluded that simulated phishing attacks should not be assessed simply by their click rates.

Consequently, simulated phishing attacks need to be constructed in such a way that they are not blame-oriented but are aimed at promoting learning, self-efficacy, and behavioral improvement.

2.4 Adaptive and Personalized Security Awareness

Adaptive security awareness relates to learning processes in which the type of content, frequency, complexity, and feedback is based on the individual's risk profile, department, and past behavior. Unlike generic training techniques, adaptive security awareness tries to make the learning process more personalized. Several recent findings show that personalized training contributes positively to cybersecurity awareness. Schöni et al. (2024) investigated personalized phishing training and determined that personalized phishing training is associated with better phishing skills due to customized training content corresponding to the participant's ability and requirements.

Salamah (2023) has developed a framework for adaptive cybersecurity training and highlighted the need for dynamic modification of the learning material in accordance with user behavior. The concept of adaptive training may be transferred from social media risks to phishing threats since they share similar concepts and approaches.

According to Bitrián et al. (2024), gamified e-training could significantly improve employee information security and data protection behaviors. For example, it can help reduce the percentage of employees who click on phishing attacks. Additionally, it was established that perceived usefulness, satisfaction, and self-efficacy serve as key mechanisms connecting training design and secure behavior. This means that an adaptive phishing simulation is expected not just to test but also to train employees to become more capable regarding their cybersecurity practices. In business organizations, for instance, various departments will be subject to different phishing topics depending on their processes, such as finances (payment), HR (document), IT (password reset), suppliers, etc.

2.5 Longitudinal Employee Security Behavior

It is essential to conduct a longitudinal study in order to assess if cybersecurity awareness training can induce sustainable behavioral change. Improvements in behavior following a training session might not necessarily show a high level of long-term security maturity. As stated by Marshall et al. (2024), few phishing training studies incorporate retention metrics other than short-term measurements, and annual training does not offer long-lasting benefits.

The same idea was supported by Franz et al. (2021). According to their review, while the majority of studies related to phishing interventions concentrate on short-term outcomes, long-term evaluation requires a longitudinal approach. It was noted that further studies will need to evaluate user-oriented solutions in the context of long-term performance.

One of the most significant longitudinal studies at an enterprise level was conducted by Lain et al. (2024). More than 14,000 employees were analyzed during 15 months. This study is particularly important since it shows that phishing behavior within organizations should be tested using practical workplace data and not experimental laboratory evidence.

Nevertheless, the literature is still deficient in providing adequate information on the basis of data obtained from multinational companies, various departments, and over multiple years. To fill this gap in the literature, the present research makes use of data gathered over three years from 2023 to 2025 from five different departments in a global firm.

2.6 Security Fatigue, Stress, and Behavioral Side Effects

While repeated phishing simulations may lead to increased caution among employees, too many or ill-thought-out phishing simulations can result in adverse consequences. As discovered by Schöps et al. (2024), employees who clicked on simulated phishing emails showed signs of increased stress and reduced self-efficacy when it comes to phishing attacks. This is an important aspect since self-efficacy and learning go hand-in-hand.

According to Brunken et al. (2023), phishing simulation campaigns might carry hidden costs for organizations, which include employee distrust and the necessity of preparing technical infrastructure and processes.

Hence, long-term phishing simulation campaigns must avoid sending any punishing messages and rather concentrate on constructive criticism, creating psychological safety, and focusing on learning. This will be especially true in adaptive training environments, where high-risk employees or departments receive more phishing simulations than others.

2.7 Research Gap

From the current body of literature, three key areas of concern remain to be addressed. To begin with, most of the research on cybersecurity awareness has been carried out within the context of immediate results, and there is very little data on long-term behavioral outcomes. In this case, Marshall et al. (2024) pointed out that no retention measures have been developed yet for assessing changes in people's behavior after going through phishing training.

Furthermore, it was shown by Prümmer et al. (2024) that many studies on cybersecurity training do not include employees as participants or utilize very small sample sizes. The latter was often associated with the use of non-experimental research designs as well. Lastly, even though more research on adaptive learning and training has emerged recently, there is little information about phishing simulation studies that incorporate such elements as personalization.

3. Research Methodology

3.1 Research Design

The current study employs a longitudinal empirical research methodology in order to explore the potential impacts of adaptive phishing simulations over time on the cybersecurity behavior of employees in an international organization.

Phishing simulation logs spanning from 2023 to 2025 will be evaluated in this study across five departments within the organization.

The unit of analysis for this study is departmental phishing simulation campaign. This consists of the date of the simulation, the department that underwent the simulation, number of participants, number of individuals that clicked the link, number of individuals that provided credentials, click rate, credential submission rate, and phishing template theme. This research methodology is appropriate since it will be useful in exploring behavioral change as opposed to evaluating a training program.

3.2 Data Collection

Dataset collection was conducted through a series of internal phishing simulation campaigns implemented by a multinational corporation between 2023 and 2025 (Figure 1). These campaigns were designed as part of the organization's cybersecurity awareness and risk management initiatives, aiming to evaluate employee susceptibility to phishing attacks and strengthen overall security awareness. The simulations were conducted periodically across five organizational departments and incorporated a variety of phishing scenarios that reflected common real-world attack techniques, including account suspension notifications, emergency approval requests, mailbox alerts, password expiration warnings, and other social engineering tactics.

For each simulation campaign, employee responses were systematically recorded to measure behavioral outcomes, including participation rates, phishing link click rates, and credential submission rates. The collected data enabled the organization to monitor behavioral trends over time, assess the effectiveness of phishing awareness training, and identify departments that exhibited higher levels of phishing susceptibility. By employing multiple phishing themes and varying levels of attack sophistication, the campaigns sought to replicate realistic threat environments and provide a robust assessment of employee cybersecurity behavior.

To protect organizational confidentiality and employee privacy, all department names were anonymized and labeled as Department 1 through Department 5. Furthermore, no personally identifiable information (PII), such as employee names, email addresses, user accounts, or other sensitive personal data, was included in the dataset. All analyses were performed using aggregated departmental data, ensuring compliance with organizational privacy policies and ethical research standards. Consequently, the dataset provides a valuable longitudinal perspective on organizational cybersecurity awareness while maintaining strict confidentiality and data protection requirements.

Variable	Description	Example
Simulation date	The month or period when the phishing simulation was conducted	June 2024
Department	The organizational unit participating in the simulation	Information Technology
Number of participants	Total employees included in each simulation	1,250
Number of link clickers	Employees who clicked the simulated phishing link	162
Number of credential submitters	Employees who entered account or password information	48
Click rate	Percentage of participants who clicked the phishing link	12.96%
Credential submission rate	Percentage of participants who submitted credentials	3.84%
Phishing template theme	Scenario or topic used in the simulated phishing email	Invoice Update Required

Campaign Overview

Period:
2023 – 2025

Departments:
5 departments

Phishing Techniques:
Account Suspension
Emergency Approval
Mailbox Notifications
Password Warnings

Purpose of the Data

These variables capture employee behavior and outcomes for each phishing simulation campaign and help organizations evaluate awareness levels, identify high-risk units, and measure improvement over time.

Phishing Simulation Data Flow

1. Campaign Design
Phishing scenarios are designed with different themes and techniques (e.g., account suspension, emergency approval).

→

2. Simulation Delivery
Simulated phishing emails are sent to employees across the five departments during the campaign period.

→

3. Employee Response
Employees may open emails, click links, and/or submit credentials depending on their behavior.

→

4. Data Collection
Key variables (e.g., clickers, submitters, rates, theme) are recorded for each simulation.

→

5. Analysis & Reporting
Results are analyzed by department and over time to assess trends and improve awareness strategies.

Figure 1: Data Collection from Internal Phishing Simulation Campaigns

Table 1: Operational Definitions of Research Variables

Item	Description
Research setting	A global enterprise environment
Study period	2023–2025
Data type	Internal phishing simulation records
Unit of analysis	Department-level phishing simulation campaign
Number of departments	Five departments
Main behavioral indicators	Click rate and credential submission rate
Data granularity	Campaign-level aggregated data
Privacy protection	Departments anonymized as Department 1 to Department 5
Personal data usage	No personally identifiable employee information used

Table 1 presents the operational definitions of the research variables employed in this study. **Table 2** presents the distribution of phishing simulation campaigns conducted across five organizational departments during the period from 2023 to 2025. The results indicate that a total of 20 phishing simulation campaigns were implemented during the study period, providing a longitudinal dataset for analyzing employee cybersecurity behavior and phishing susceptibility across different organizational units.

Table 2: Distribution of Phishing Simulation Campaigns by Year and Department

Department	2023 Campaigns	2024 Campaigns	2025 Campaigns	Total Campaigns
Department 1	2	1	2	5
Department 2	0	0	3	3
Department 3	0	0	2	2
Department 4	2	1	2	5
Department 5	2	1	2	5

3.3 Research Variables

3.3.1 Independent and Dependent Variables

As presented in Table 3, the independent variables comprise both simulation-related factors and organizational characteristics that may influence employees' susceptibility to phishing attacks. The dependent variables represent employees' behavioral responses to phishing simulation campaigns, including click behavior and credential submission activities.

Table 3: Operational Definitions of Research Variables

Variable Type	Variable	Operational Definition	Formula / Measurement
Independent Variable	Simulation period	Year and month when the phishing simulation was conducted	2023/06–2025/12
Independent Variable	Department	Organizational unit participating in the simulation	Department 1–Department 5
Independent Variable	Training frequency	Number of simulations received by each department	Count of campaigns
Independent Variable	Scenario type	Theme of simulated phishing email	Account suspension, emergency approval, mailbox notification, etc.
Independent Variable	Adaptive intensity	Degree of repeated or targeted simulation based on prior risk	Low / Medium / High
Dependent Variable	Click rate	Percentage of participants who clicked the phishing link	Link clickers / Participants × 100
Dependent Variable	Credential submission rate	Percentage of participants who submitted credentials	Credential submitters / Participants × 100
Dependent Variable	Behavioral improvement rate	Reduction in click rate over time	Initial click rate − later click rate / initial click rate × 100
Control Variable	Number of participants	Total employees included in each campaign	Count
Control Variable	Campaign scale	Size category of simulation	Small / Medium / Large

3.4 Adaptive Phishing Simulation Procedure

Phishing simulations took place as adaptive awareness tests rather than standard training courses. The topic and frequency of these awareness courses depended on performance history, departmental risks, and levels of threat. For instance, those departments that had a high percentage of clicks or password submissions got extra training or different phishing tests. If a department were considered low-risk, it would still be evaluated for possible improvements in security awareness levels. Table 4 presents the adaptive simulation process.

Table 4: Adaptive Phishing Simulation Procedure

Stage	Procedure	Purpose	Output
Stage 1	Baseline simulation	Identify initial departmental phishing risk	Baseline click rate
Stage 2	Risk classification	Classify departments based on click and credential submission rates	High / Medium / Low risk groups
Stage 3	Scenario adjustment	Adjust phishing themes according to department risk and behavior	Targeted simulation templates
Stage 4	Repeated simulation	Conduct repeated phishing exercises	Behavioral response data
Stage 5	Feedback and reinforcement	Provide awareness reminders or follow-up training	Improved security awareness
Stage 6	Longitudinal evaluation	Compare results across time periods	Behavioral improvement trend

3.5 Research Model

The suggested research model offers the basis for studying the effect of adaptive phishing simulation on cybersecurity behavior in the organization over time. For the sake of methodological consistency, Table 5 demonstrates a link between every research question and the respective data variables, analysis procedures, and outcomes.

Table 5: Alignment between Research Questions and Data Analysis Methods

Research Question	Data Used	Analysis Method	Expected Output
RQ1: Can adaptive phishing simulations reduce click rates over time?	Click rate by date and department	Longitudinal trend analysis	Click-rate decline trend
RQ2: Are there behavioral differences across departments?	Department-level click and credential submission rates	Comparative departmental analysis	Departmental risk differences
RQ3: Does repeated phishing training improve awareness?	Training frequency and click rate	Repeated measures analysis	Behavioral improvement pattern
RQ4: Do high-risk departments improve more significantly?	Initial high-risk departments and later results	Improvement rate analysis	Risk reduction percentage
RQ5: Does long-term simulation introduce fatigue effects?	Click-rate fluctuation over time	Pattern and anomaly analysis	Potential fatigue or regression signals

3.6 Methodological Limitations

Although this study utilizes longitudinal data obtained from a real enterprise environment, several limitations should be acknowledged. First, the dataset is aggregated at the departmental level rather than at the individual employee level. Consequently, the analysis cannot account for employee-specific characteristics, such as age, organizational tenure, educational background, or prior cybersecurity training, which may influence phishing susceptibility. Second, the number of phishing simulation campaigns varies across departments and observation periods, potentially affecting the comparability of the results. Third, the difficulty and sophistication of the simulated phishing emails may differ across campaigns. Therefore, observed changes in click rates may reflect not only improvements in employees' security awareness but also variations in campaign design and complexity. Despite these limitations, the study offers important practical value by

employing longitudinal data collected from an operational enterprise environment, thereby providing findings with strong ecological validity and real-world relevance.

4. Research Results and Discussion

4.1 Longitudinal Click Rate Trends

From the longitudinal study, it was found that the average click rate had been declining over time within most departments, but the pattern of decline varied by department. From the findings, it becomes evident that employee susceptibility to phishing can be continuously lowered through repeated simulation exposure. It can be observed from Table 6 below that certain departments were showing a declining trend in the number of clicks after several simulations. In particular, Department 2 had the highest level of improvement in the number of phishing clicks, as its average click rate declined from 15.92% in the initial simulation to 0.35% in subsequent phishing simulation. Similarly, Department 4 also managed to achieve considerable improvements. While the click rate in this department had once been at the maximum of 21.13%, it later fell to 4.64%. Such a trend demonstrates the potential for improvement that can be achieved even in highly risky departments through sustained and adaptable awareness programs.

Department 5 experienced comparatively lower click rates during the majority of the observation period. Despite a temporary rise in the click rate during the year 2024, the rate fell back in 2025. As demonstrated, even the most aware departments may face temporary risk increases; nevertheless, sustained reinforcement will allow such departments to return to secure behaviors. All in all, based on the longitudinal trend, there are solid grounds to conclude that adaptive phishing simulations yield better results. At the same time, the presented data show that improvements are not necessarily a linear process. Temporal rises in the click rate may happen due to various factors like increasing complexity, changing employees' workloads, the time of campaigns, and scenario relevance. From a theoretical standpoint, the results support the idea of behavioral reinforcement. Frequent phishing tests give employees opportunities to identify fraudulent behavior, learn from past experience, and develop healthy decision-making habits. The theory suggests that cybersecurity awareness must be viewed as a learning process, not merely an annual exercise.

Table 6: Departmental Phishing Click-Rate Improvement Analysis

Department	Highest Click Rate (%)	Latest Click Rate (%)	Click-Rate Improvement from Peak (%)
Department 1	17.71	8.88	49.86
Department 2	15.92	0.35	97.80
Department 3	5.67	2.37	58.20
Department 4	21.13	4.64	78.04
Department 5	5.52	1.36	75.36

4.2 Departmental Behavioral Differences

These findings show distinct behavioral differences between departments. Such differences imply that susceptibility to phishing attacks does not depend only on personal awareness of the employees but is affected by other factors such as the organization itself, the type of work, processes, etc. Some departments had a higher initial rate of clicking, which means they were exposed to or sensitive to particular types of phishing attacks. The departments where approval, notification, accounts, and operational request messages are often seen can have a higher probability of responding promptly to a phishing email. This is another aspect of human behavior in the workplace that plays an essential role in enterprise-level cybersecurity: employees need to act fast in terms of making security decisions.

According to the data provided in Table 7, the two most interesting departments to analyze are Departments 2 and 4. Both had relatively high initial click rates; however, a considerable improvement was achieved later. The results suggest that high-risk departments may be more responsive to adaptive and repeated training because there is more room for behavioral change. On the contrary, Department 5 remains low-risk, which implies certain advantages in terms of behavior and awareness.

The results indicate the importance of department-based approaches to phishing awareness campaigns. Using a single strategy to educate all departments on phishing might not take into account their unique levels of vulnerability. Departments that deal heavily with external communications, require urgent approvals, are responsible for money transactions, collaborate with suppliers, or communicate via IT system notifications would benefit from more frequent and relevant phishing simulations.

From a practical perspective, departmental variance should be leveraged when creating risk-based training programs. Rather than providing the same phishing exercises for all employees, organizations should divide departments based on the risk level and conduct relevant phishing simulations based on their needs.

Table 7: Departmental Behavioral Risk Profile

Department	Observed Risk Pattern	Key Evidence	Behavioral Interpretation	Training Implication
Department 1	Large-scale fluctuating risk	2025/07 click rate 17.71%; 2025/12 declined to 8.88%	Large user base and high exposure to urgent approval scenarios	Continue large-scale monitoring and scenario diversification
Department 2	Rapid improvement	15.92% → 9.50% → 0.35%	Strong learning effect after repeated simulations	Maintain adaptive reinforcement
Department 3	Moderate improvement	5.67% → 2.37%	Lower initial risk but still improved after repeated exposure	Strengthen reporting behavior
Department 4	High-risk but improved	21.13% → 19.00% → 4.64%	High sensitivity to urgent approval and credential-related scenarios	Prioritize targeted credential protection training
Department 5	Stable low risk after early fluctuation	5.52% → 3.18% → 1.36%	Awareness relatively stable after reinforcement	Maintain periodic monitoring

4.3 Adaptive Training Effectiveness

The results indicate that adaptive phishing simulations are better at achieving their goals compared to regular awareness training programs, due to the fact that adaptive simulations allow training frequency and content to be tailored to the department's behavioral risk factors. During this study, the organizations' departments that demonstrated a higher number of clicks and/or submissions of credentials were exposed to further phishing simulations.

The significant decrease in the click rate among Department 2 users demonstrates the high level of effectiveness of adaptive training programs. This is evidenced by the fact that after multiple repetitions, the number of clicks dropped from 15.92% to 0.35%. The same conclusion can be drawn from the results regarding Department 4, which decreased its number of clicks from 21.13% to 4.64%.

This can be attributed to three factors. Firstly, frequent repetition promotes recognition ability. As employees become accustomed to recognizing typical signs of phishing emails, such as suspicious hyperlinks, urgent language, unusual behavior on the part of senders, and requests for credentials.

Secondly, the high degree of relevance of simulations promotes learning transfer. Phishing simulations that resemble real-life work situations increase the likelihood that training experiences will translate into workplace behaviors. Thirdly, timely feedback ensures the correction of behavior. When an employee clicks on a phishing link during a simulated attack, they are reminded of their actions and gain insights into why it was not the right thing to do.

On the other hand, the results of the study must not be seen as proof that increased training is always preferable. Adaptive training works if it is risk-based, relevant, and appropriately paced. Otherwise, it can result in loss of confidence among employees, cause boredom, and even encourage resistance to training. Consequently, the adaptation of phishing simulation becomes crucial.

4.4 Cybersecurity Behavioral Maturity

This shows that employee cybersecurity behaviors may take time to develop due to continuous adaptive learning. From the observations noted by the five departments in this longitudinal study, the Security Awareness Maturity Model is presented in order to describe the progression of departments from susceptibility to vigilant state. The four levels of maturity of this model are illustrated in Table 8. The maturity model offers an effective way to interpret the outcomes of phishing simulations. Rather than focusing only on the rate at which people click the link, click rate becomes one aspect of maturity.

Department 2 might well fit into the scenario where there was an extremely fast transition from Level 1 to Level 3 due to the significant decrease in the rate of clicking over time. In the case of Department 4, one can see a department that, despite initial high risk, eventually progressed towards higher levels of maturity through prolonged efforts at intervention. As for Department 5, one can assume that this was a highly mature department characterized by consistently lower click rates throughout different periods of time, although not without fluctuation.

Such an approach is relevant because, instead of punishment, it focuses on employee maturity. People who click phishing links should not be considered a failure; rather, it is part of the development process. The whole idea behind conducting phishing simulations is building up the organization's defensive capacity.

Table 8: Security Awareness Maturity Model Based on Phishing Simulation Outcomes

Maturity Level	Stage	Behavioral Characteristics	Quantitative Indicators	Recommended Strategy
Level 1	High Risk and Low Awareness	Employees show high click and credential submission behavior	Click rate > 15% or credential leakage rate > 10%	Immediate targeted training
Level 2	Initial Awareness Improvement	Click rate begins to decline but remains unstable	30%–60% reduction from peak	Continue adaptive simulation
Level 3	Stable Behavioral Improvement	Click rate and leakage rate remain relatively low	Click rate < 5% across repeated simulations	Maintain periodic reinforcement
Level 4	Mature Security Vigilance	Employees avoid clicking and proactively report suspicious emails	Low click rate, low leakage rate, high reporting rate	Integrate into security culture metrics

4.5 Credential Submission Risk

Click rate is another indicator in Table 9 of behavioral risks, while the submission of credentials is an even higher degree of such risks. The former demonstrates susceptibility to phishing attempts; however, the latter is indicative of higher vulnerability since a user submits his or her credentials in response to a potentially dangerous message and increases the risk for the whole enterprise.

The presence of the metric of credential submission helps make conclusions about the risk level of phishing attempts more accurate and thus makes this paper better. It could be assumed that some departments will have low click rates but high credential submission rates. It means that the staff there has higher levels of danger than mere curiosity and carelessness.

Such behavior may mean that employees are not aware of the dangers associated with entering credentials, fail to recognize fake login pages, or have a very high trust towards notifications that come from the system. In the future, all these factors need to be discussed in awareness campaigns.

In regard to the governance of cybersecurity for enterprises, the credential submission rate should be taken into account rather than just the click rate. There can be some urgent measures needed in departments where the credential submission rate is very high, such as simulated login page practice and MFA awareness campaign.

Table 9: Credential Submission Risk Analysis

Department	Highest Credential Leakage Rate (%)	Campaign Period	Scenario Type	Latest Credential Leakage Rate (%)	Risk Interpretation
Department 1	9.19	2025/07	Emergency approval request	5.11	Large-scale credential exposure risk remains
Department 2	10.45	2025/03	Emergency approval request	0.18	Significant reduction after repeated simulations
Department 3	2.01	2025/03	Emergency approval request	1.98	Low but persistent credential submission risk
Department 4	18.47	2025/03	Emergency approval request	4.23	Highest credential risk; requires targeted intervention
Department 5	1.84	2024/09	Malicious website warning	0.91	Low residual credential risk

4.6 Security Fatigue Considerations

While the results show a favorable trend towards improved behavior, some departments were seen to display temporary fluctuations in terms of click rates. The fluctuations could be attributed to changing template difficulty levels, workload of the employees, timing of the campaign, and possibly even security fatigue.

Security fatigue refers to the state of employees who become increasingly immune to repetitive security messages and alerts, and training drills. In cases of a phishing attack simulation system, security fatigue can result from a feeling of repetition or punishment associated with these simulated attacks.

These observations imply that organizations need to take extra care when conducting such campaigns, as they need to strike a fine balance between too many and too few training sessions for employees in order to mitigate risks effectively. Organizations must consider the following guidelines to ensure that phishing simulation training does not cause security fatigue:

1. Phishing scenarios should be diversified to keep employees on their toes.
2. Feedback must be positive and constructive, not punitive.
3. The frequency of training programs should depend on the risk level.
4. Training programs should encourage positive behavior through rewards.
5. Phishing simulations need to form part of the overall organizational security culture.

As such, adaptive phishing simulation not only requires an increase in training intensity but also in training quality.

4.7 Discussion of Research Questions

As shown in Table 10, the results provide evidence for answering the five research questions proposed in this study.

Table 10: Summary of Research Questions and Empirical Findings

Research Question	Empirical Evidence	Finding	Interpretation
RQ1: Can adaptive phishing simulations reduce click rates over time?	Department 2, 3, 4, and 5 showed lower latest click rates than peak values	Supported	Repeated adaptive simulations contribute to behavioral improvement
RQ2: Are there significant behavioral differences among departments?	Departments showed different peak risks, improvement speeds, and residual risks	Supported	Departmental context influences phishing susceptibility
RQ3: Does repeated phishing training improve awareness?	Department 2 declined from 15.92% to 0.35%; Department 4 from 21.13% to 4.64%	Supported	Repeated exposure and feedback improve recognition capability
RQ4: Do high-risk departments demonstrate greater behavioral improvement?	Department 2 and Department 4 showed the largest improvement	Supported	High-risk groups benefit most from adaptive intervention
RQ5: Does long-term simulation introduce security fatigue effects?	Department 1, 4, and 5 showed temporary fluctuations	Partially supported	Fatigue, scenario difficulty, or campaign timing may affect outcomes

5. Conclusion and Recommendations

5.1 Conclusion

The current study was aimed at exploring the effects of adaptive phishing simulations on the cybersecurity behavior of employees for up to three years. Using a dataset gathered from a global enterprise, we observed that adaptive phishing simulations could have an effect on employee behavior, especially in cases where phishing susceptibility is high.

The outcomes suggest that phishing simulations conducted consistently and based on risk analysis could reduce click rates, promote awareness, and encourage the growth of cybersecurity behavioral maturity in employees. In general, departments characterized by a higher click rate showed significantly more progress, implying that the use of adaptive training programs is especially important for such organizations.

Furthermore, we proved that different departments can be characterized by their own profiles of phishing susceptibility. The importance of this conclusion lies in the fact that it opposes a common belief about conducting identical cybersecurity awareness training for all organizational units. Namely, the work-related practices of different departments differ, and therefore, employees in various departments face different phishing threats.

Additionally, the use of multiple indicators for evaluation of phishing behavior is crucial. In particular, we concluded that a higher credential submission rate indicates a more severe case compared to a click rate only.

In conclusion, this study reinforces the idea that employees' cybersecurity behavior can be enhanced through the implementation of continuous, adaptive, and contextualized awareness initiatives. Human-centered security must become a part of cyber resilience frameworks in the corporate sector.

5.2 Practical Recommendations

Based on the findings, some of the key recommendations for practice include:

1. Use of adaptive phishing simulation

Organizations should go beyond traditional annual awareness training and consider adaptive phishing simulation. The design of the simulation program should be determined by its previous performance, risk profile of specific departments, and behavior patterns of users.

2. Designing specific training programs for each department

Departments within an organization have different risks. For instance, invoice and payment fraud simulations may be needed in finance departments, while password reset or privileged access may be required in IT departments. Thus, it is important to design simulation programs according to departments' specific requirements.

3. Using both click rate and credential submission rate as indicators

Only click rate does not reveal how risky a situation is. Credential submission rate should be considered as the indicator that reflects a greater risk, since it indicates that employees tend to trust phishing content.

4. Frequency of training depending on risk level

The departments with the highest clicks or credentials submission rates should undergo simulations more frequently than others. Departments with low-risk levels of performance should undergo reinforcement training at specified times. Over-training and under-training should be avoided through a proper assessment of risks and performance metrics.

5. Give constructive feedback

The organization needs to ensure that simulations are conducted not to penalize employees but to help them learn and stay prepared. Employees who clicked simulated phishing emails should be given immediate and constructive feedback.

6. Incorporate phishing awareness into security governance, risk management, and compliance

Simulation results should be shared with cybersecurity governance committees, risk management committees, and departmental management for the integration of simulations with organizational security governance, risk management, and compliance.

7. Security fatigue detection

Behavioral trends, feedback from employees, and simulation effectiveness should be carefully monitored. Increase in clicks after intensive simulation sessions can mean increased fatigue or changes in template difficulties. Training programs should be modified accordingly.

5.3 Research Contributions

The contribution of this study to cybersecurity research is numerous.

Firstly, it is one of those studies that present empirical data collected from a live, functioning, global enterprise. While many researches on the matter have used lab experiments, student population, or temporary observation periods, the current study presents a long-term analysis of three years of phishing simulations across five departments.

Secondly, the research broadens phishing awareness research, transitioning from a short-term evaluation of training effects to longitudinal behavioral analysis. With data collected in 2023, 2024, and 2025, the study shows how employees' behavior develops over time and can change under the influence of repetitive simulations.

Thirdly, the study emphasizes the significance of departments when researching cybersecurity matters, with the results showing department-dependent variance in phishing susceptibility.

Fourthly, the paper offers the Security Awareness Maturity Model, which will allow organizations to see phishing awareness through the lens of progress towards developing the proper skills and attitude.

Finally, the study is helpful for human-centric cybersecurity research, as it emphasizes that while technology is essential in combating phishing attempts, people will always remain a critical line of defense.

5.4 Managerial Implications

The implications of the research findings for cybersecurity executives and enterprise leaders include the following. First, awareness of phishing is best viewed as an actionable risk management process and not a tick-box compliance exercise. Measures such as click rate, credential submission rate, improvement rate, and reporting activity can act as performance measures for human cyber risks.
Second, cybersecurity leadership should focus on high-risk departments. High-risk departments in terms of high click rate and credential submission rate should get extra awareness and training.
Third, phishing simulation results should be used to enhance overall enterprise resilience initiatives. In light of the fact that most ransomware attacks start with a phishing attack, and credential stealing leads to business email compromise, raising employee phishing resistance helps prevent incidents and promote business continuity.
Fourth, management should cultivate a learning-based security mindset. Employees would be more receptive to learning and change if training was constructive, useful, and psychologically secure. Punitive training can lead to employees withholding information.
Fifth, adaptive training should complement technical controls. Awareness should be complemented by technical security controls like email security, multifactor authentication, endpoint protection, SOC, and IR.

5.5 Limitations

There are various limitations associated with this study. First, the dataset is an aggregate at the department level, as opposed to an individual employee level. Consequently, there is a limit to the study in determining the impact of individual characteristics like age, tenure, position held, education level, and security experience in shaping employees' susceptibility to phishing.
Second, there were variations in the number of simulation campaigns conducted between departments and over years, as some departments had many simulations conducted compared to other departments. Third, there could be differences in the difficulty of phishing templates used in each campaign. The increase in clicking rate might not be due to low employee awareness, but due to a highly effective phishing scenario.
Lastly, this study focused on two key behaviors – click rate and credentials submission rate. While these two are critical in gauging individual behavior toward phishing emails, future research will need to explore additional measures like reporting rate, time-to-report, repeat clicking behavior, and post-training survey results.

5.6 Future Research

There could be several extensions to the study in the future. For instance, future research could involve the use of individual-level anonymized data to develop predictive models of phishing susceptibility. The ability to predict which employees fall victim to phishing attacks repeatedly will give us the opportunity to study learning curves and risk stratification.

Additionally, future research could involve adaptive phishing simulations driven by artificial intelligence. AI algorithms will aid in identifying employees' risk levels, recommending relevant training material, and adapting the difficulty level in the simulation.

Another possible extension to this study is an investigation of industry differences. Organizations in manufacturing, finance, healthcare, education, and government agencies could have differing risk profiles depending on their workflow processes, regulatory environments, and cybersecurity cultures.

Moreover, psychological variables such as self-efficacy, severity of threat perceptions, usefulness of training programs, trust in the security team, and security fatigue could provide us with explanations for rapid improvements among employees.

Fifth, future research could be done on reporting behavior. While avoiding clicks is an important factor, reporting is even more advanced in terms of security maturity. Future researchers can thus investigate factors such as the rate and speed of reporting as significant determinants of organizational resilience against phishing attacks.

Lastly, future studies can focus on exploring the effects of simulation outcomes in reducing real-life phishing incidents. This will reveal the degree to which simulation success impacts phishing attack incidences.

5.7 Final Remarks

Overall, this paper shows that adaptive phishing simulation can be regarded as an effective method for fostering the cybersecurity behavior of employees in the long run. In particular, regular risk-driven simulations prove their ability to diminish the rate of clicks and thus lower vulnerability in risky departments. It is also worth mentioning that the results of this study indicate that there is a need to consider cybersecurity from the standpoint of behavioral maturity rather than just lowering the click rate during a campaign. Therefore, companies should create sustainable human-centered approaches to cybersecurity based on continuous monitoring, adaptation, feedback, and integrated governance. Through longitudinal measurements, comparison among departments, and behavioral maturity assessment, this paper provides both theoretical and practical conclusions related to cyber resilience against phishing and other similar threats.

References

[1] Bitrián, P., Buil, I., Catalán, S., & Merli, D. (2024). Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours. Journal of Business Research, 179, 114685.

[2] Brunken, L., Buckmann, A., Hielscher, J., & Sasse, M. A. (2023). "To do this properly, you need more resources": The hidden costs of introducing simulated phishing campaigns. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), 4105-4122.

[3] Franz, A., Zimmermann, V., Albrecht, G., Hartwig, K., Reuter, C., Benlian, A., & Vogt, J. (2021). SoK: Still plenty of phish in the sea—A taxonomy of user-oriented phishing interventions and avenues for future research. In Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021), 339-358.

[4] Gulle, B. T., Kiran, P., Celik, S. G., Varol, Z. S., Siyve, N., Emecen, A. N., & Duzel, H. (2024). Awareness and acceptance of human papillomavirus vaccine in the Middle East: A systematic review, meta-analysis, and meta-regression of 159 studies. Epidemiology & Infection, 152, e165.

[5] Ho, M., Ang, S., Huy, S., & Janarthanan, M. (2026). Cybersecurity Risks and Challenges in Smart Cities: A Review with Insights for Cambodia. Growth, 7, 8.

[6] Jabir, R., Le, J., & Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. AI, 6(8), 174.

[7] Lain, D., Jost, T., Matetic, S., Kostiainen, K., & Capkun, S. (2024, December). Content, nudges and incentives: A study on the effectiveness and perception of embedded phishing training. In Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security (pp. 4182-4196).

[8] Marshall, N., Sturman, D., & Auton, J. C. (2024). Exploring the evidence for email phishing training: A scoping review. Computers & Security, 139, 103695.

[9] Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585.

[10] Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: A meta-analysis. Computers & Security, 150, 104206.

[11] Rozema, A. T., & Davis, J. C. (2025). Anti-Phishing Training Does Not Work: A Large-Scale Empirical Assessment of Multi-Modal Training Grounded in the NIST Phish Scale. Assessment, 7, 8.

[12] Salamah, F. B. (2023). Adaptive cybersecurity training framework for social media risks. University of Plymouth.

[13] Schöni, L., Carles, V., Strohmeier, M., Mayer, P., & Zimmermann, V. (2024). You know what? Evaluation of a personalised phishing training based on users' phishing knowledge and detection skills. In Proceedings of the 2024 European Symposium on Usable Security (EuroUSEC '24).

[14] Schöps, M., Gutfleisch, M., Wolter, E., & Sasse, M. A. (2024). Simulated stress: A case study of the effects of a simulated phishing campaign on employees' perception, stress and self-efficacy. In Proceedings of the 33rd USENIX Security Symposium (USENIX Security 24), 4589-4606.

[15] Toth, A. (2024). Critical Infrastructure Dependencies: Cybersecurity Challenges in Supply Chains. In International Conference on Central European Infrastructure Protection (pp. 505-526). Cham: Springer Nature Switzerland.

[16] Weinz, M., Zannone, N., Allodi, L., & Apruzzese, G. (2025). The impact of emerging phishing threats: Assessing quishing and llm-generated phishing emails against organizations. In Proceedings of the 20th ACM Asia Conference on Computer and Communications Security (pp. 1550-1566).