CSword Logo

Phishing Simulation Report

Reporting Period: May 28, 2025 – June 30, 2025

Table of Contents

Executive Summary

Despite significant strides in phishing awareness across Egypt, a critical behavioral gap persists where employees frequently identify phishing attempts only after compromising their security by clicking.

• An alarming average click rate of 37% persists across Egypt, indicating a widespread "click first, report later" habit that negates substantial awareness efforts.

• The Human Resources (HR) department is Egypt's most immediate vulnerability, exhibiting a 37% click rate (76% higher than IT), demonstrating a critical lack of pre-click discernment despite respectable reporting.

• While our trend analysis shows impressive progress towards a 0% click rate by 25W25, initially high click rates (over 70% in 25W21) and the persistent average of 37% confirm that initial compromises remain a significant and unacceptable risk.

To mitigate this risk, we must implement a targeted cybersecurity resilience program for the HR department, emphasizing pre-click verification, and launch an organization-wide campaign to cultivate a proactive "think before you click" culture across Egypt.

Key Performance Indicators (KPIs)

Average Click Rate	Average Reporting Rate	Repeat Clickers
37.04%	**59.26%**	**2**
		High-Risk Individuals

Total Emails Sent	Most Vulnerable Group	Most Effective Group
27	**HR**	**IT**
4 Campaigns	37.04% Click Rate	71.43% Report Rate

• **Core Conflict:** egypt's average reporting rate of 59% shows commendable employee awareness, yet this is critically undermined by a high average click rate of 37%. This signifies that a substantial portion of our workforce is identifying phishing attempts only *after* compromising their security posture by clicking, creating a significant window of vulnerability.

• **Primary Risk Area:** The Human Resources (HR) department represents egypt's most immediate and significant vulnerability, mirroring the organization's overall average click rate at 37%. Their susceptibility demands urgent and focused intervention given their access to sensitive employee data.

• **Key Insight:** While the IT department demonstrates strong pre-click vigilance (21% click rate) and leads in post-click awareness (71% report rate), the HR department's high click rate (37%) despite a respectable 59% reporting rate reveals a critical paradox: they are demonstrating post-compromise awareness (reporting) but lack sufficient pre-click discernment to prevent initial engagement. This indicates a pressing need to transition high-risk departments like HR from reactive reporting to proactive threat avoidance through enhanced training.

• **Persistent Vulnerability:** The presence of two repeat clickers necessitates targeted individual remediation to address persistent behavioral risks that evade current awareness initiatives.

Departmental Breakdown

Department	Emails Sent	Click Rate	Report Rate
IT	14	21.4%	71.4%
HR	27	37.0%	59.3%

• The HR department is identified as the single Highest-Risk Department for egypt, exhibiting a **37.0% Click Rate**. This group showed a **59.3% Report Rate**.

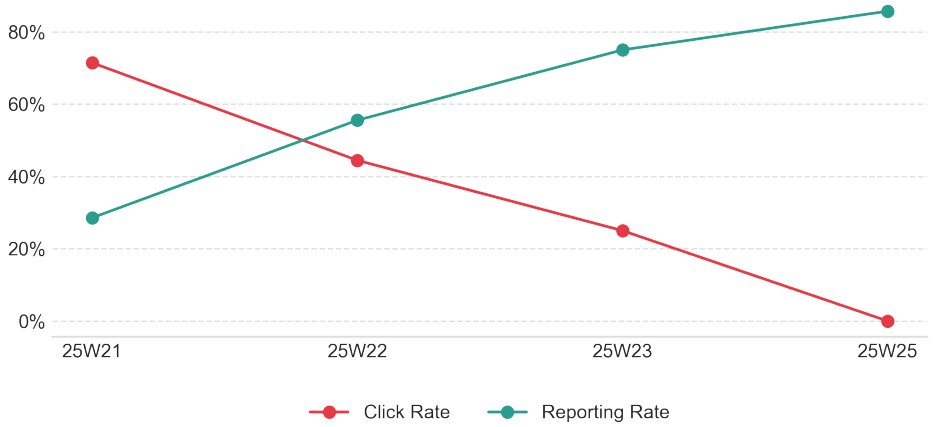
• The IT department is the Top-Performing Department with a significantly lower **21.4% Click Rate** and a robust **71.4% Report Rate**, demonstrating higher awareness and reporting vigilance within egypt.

• The HR department's high Click Rate of 37.0% signals a critical vulnerability to phishing attacks. This high susceptibility, combined with a Report Rate of 59.3% (lower than IT's), indicates that while some employees are reporting, a substantial number are clicking and not reporting. This represents a significant awareness and response gap that could severely impede incident response for a more sophisticated attack on egypt.

• While neither department perfectly fits the profile of a "silent risk" (low click, critically low report), the HR department's Report Rate of 59.3% highlights an area for improvement. Given their high vulnerability, it is crucial that every clicked incident is reported to enable prompt action and minimize potential impact on egypt.

• The scale of exposure for the HR department further amplifies the risk. With 27 emails sent, the 37.0% click rate translates to a more widespread compromise potential compared to the IT department, which received 14 emails. This larger footprint means a higher number of individuals within egypt were directly affected.

Phishing Awareness Trend Analysis



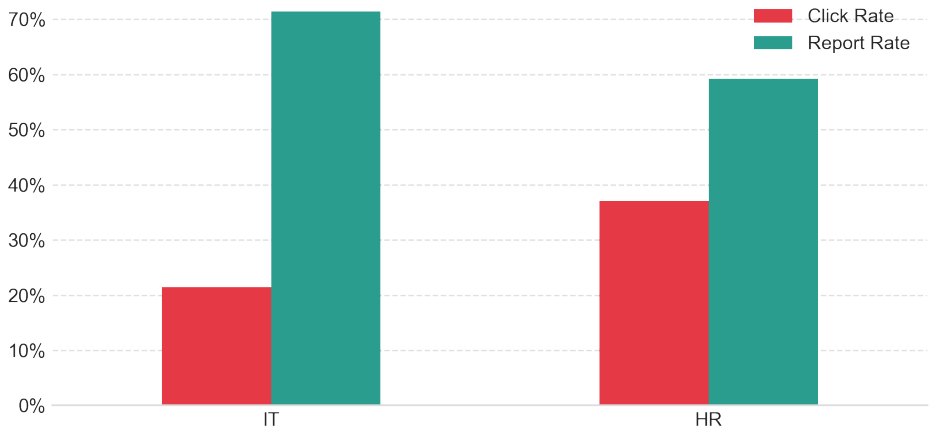
• **Egypt's phishing awareness program demonstrates exceptional success, achieving near-zero click rates while significantly boosting employee reporting diligence.**

• The Reporting Rate (green line) shows a consistently positive and steep upward trajectory, indicating a highly successful awareness training program for Egypt's employees. Starting at approximately 29% in 25W21, the rate climbed steadily, reaching a strong 75% in 25W23, and culminating in an impressive peak of approximately 85% by 25W25. This demonstrates a significant and increasing capability among employees to identify suspicious emails and report them promptly.

• While initially representing a significant vulnerability, the Click Rate (red line) has shown a remarkable and consistent decline throughout the period. Starting at a concerning approximately 72% in 25W21, this direct measure of behavioral failure and organizational risk dropped significantly to about 44% by 25W22, further to 25% by 25W23, and, crucially, reached an exemplary 0% by 25W25. This dramatic reduction in employees clicking on malicious links signifies a profound positive shift in behavior, directly mitigating the risk of breaches for Egypt.

• The concurrent rise in Reporting Rate and the dramatic fall in Click Rate reveal a powerful and overwhelmingly positive transformation in Egypt's phishing awareness posture. The key insight is that our program has not only successfully taught *identification* (leading to more reports) but, more importantly, has achieved nearly perfect *avoidance* (leading to zero clicks). This indicates Egypt's workforce can now effectively spot a phish and, crucially, prevent triggering a breach by not clicking on malicious links, vastly improving our overall cybersecurity resilience.

Group Risk Assessment Analysis



• **Highest-Risk Group Identified:** The Human Resources (HR) department exhibits the highest phishing risk with a Click Rate of approximately 37%. This makes them 16 percentage points higher, or approximately 76% more likely to click on a phishing attempt, than the IT department (Click Rate of ~21%). This significant disparity highlights HR as egypt's primary area of concern for immediate cybersecurity intervention.

• **Reporting Effectiveness Comparison:** Both departments demonstrate commendable diligence in reporting potential phishing attempts. The IT department shows superior reporting effectiveness with a Report Rate of approximately 71%, which is 12 percentage points higher than HR's Report Rate of approximately 59%. While both figures are positive, IT's higher rate indicates a stronger proactive posture in identifying and flagging threats.

• **Synthesized Findings and Hypothesis:**

  • **HR Department:** Despite generally high email volumes, the HR department's elevated Click Rate (37%) combined with a comparatively lower Report Rate (59%) suggests a significant vulnerability. A plausible hypothesis for this heightened risk is that HR professionals frequently handle urgent, sensitive, or high-stakes communications (e.g., employee data, benefits, compliance) which could make them more susceptible to socially engineered phishing attacks that exploit urgency, authority, or sensitive topics. Their slightly lower reporting rate might also indicate a less ingrained habit or awareness in identifying sophisticated phishing lures compared to a technical department.

  • **IT Department:** The IT department demonstrates a lower Click Rate (21%) and a strong Report Rate (71%), indicating a better overall security posture against phishing threats compared to HR.

• **Recommended Next Step:** The data clearly indicates that the Human Resources department requires immediate and targeted cybersecurity awareness training and enhanced phishing simulation exercises. These interventions should be specifically tailored to address the unique social engineering tactics and urgent communication scenarios that HR personnel are most likely

to encounter, aiming to significantly reduce their Click Rate and improve their reporting vigilance within egypt.

Key Findings & Conclusion

Despite significant strides in phishing awareness across Egypt, a critical behavioral gap persists, transforming our employees' commendable ability to identify threats into reactive reporting rather than proactive avoidance. Our core performance indicators underscore this challenge: while Egypt boasts a respectable 59% average reporting rate, a high average click rate of 37% indicates that a substantial portion of our workforce is identifying phishing attempts only after compromising their security posture by clicking. While the time-series trend chart demonstrates remarkable progress – showing our reporting rates peaking at an impressive 85% and click rates dramatically falling to an exemplary 0% by 25W25 as a testament to our training effectiveness – these aggregate improvements do not negate the overall behavioral vulnerabilities. The persistence of a significant average click rate, even as reporting vigilance has soared, underscores the challenge of consistently translating this enhanced recognition into proactive threat avoidance across Egypt. This paradox is acutely visible in our departmental risk assessment, where the Human Resources department, despite a respectable 59% reporting rate, exhibits a concerning 37% click rate—mirroring the organization's overall vulnerability. This makes HR 76% more likely to click than the IT department, providing a tangible example of how vital employee awareness can still be undermined by behavioral gaps, particularly in roles susceptible to social engineering. The core problem, therefore, is not a deficit in knowledge or the ability to recognize a threat, but rather a critical disconnect between awareness and action. Our employees are largely aware of phishing dangers and are diligent in reporting them post-compromise, yet a significant segment continues to fall prey to initial clicks, revealing a fundamental knowledge-action gap. This behavioral vulnerability represents an unacceptable level of risk to Egypt. It negates a substantial portion of our investment in cybersecurity awareness training by allowing an initial compromise to occur, exposing our sensitive data, financial assets, and operational continuity to significant harm. Without addressing this critical behavioral gap, we remain unnecessarily exposed to sophisticated social engineering attacks that exploit human fallibility.

Actionable Recommendations

Targeted HR Department Cybersecurity Resilience Program

- **Specific Action:** Implement a specialized, mandatory cybersecurity awareness and phishing simulation program for Egypt's Human Resources (HR) department. This program must be tailored to address the unique social engineering tactics prevalent in HR-specific communications (e.g., urgent benefits updates, compliance directives, sensitive employee data requests) and emphasize pre-click verification over post-click reporting. Include frequent, high-fidelity phishing simulations that mimic scenarios HR personnel are most likely to

encounter, aiming to significantly reduce their click rate and improve their reporting vigilance.

• **Justification:** The HR department represents "Egypt's most immediate and significant vulnerability," exhibiting a 37% click rate which makes them "76% more likely to click" than the IT department. Despite a respectable reporting rate, their high click rate reveals a critical lack of "pre-click discernment," indicating they are identifying threats "only after compromising their security posture by clicking." This targeted intervention is vital given their access to highly sensitive employee data.

Cultivate a Proactive "Think Before You Click" Culture Across Egypt

• **Specific Action:** Launch a sustained, organization-wide campaign focused on shifting the ingrained "click first, report later" behavior to a "verify first, click never (if suspicious), and report immediately" paradigm. This initiative should leverage a blend of more frequent, short, high-impact micro-training modules, real-time feedback mechanisms during simulations, and positive reinforcement for employees who identify and report suspicious emails *before* clicking. Integrate "stop and think" reminders into daily digital workflows and communications.

• **Justification:** Egypt's "core problem... is a critical disconnect between awareness and action," evidenced by a "high average click rate of 37%" even with a 59% reporting rate. This signifies that a "substantial portion of our workforce is identifying phishing attempts only *after* compromising their security posture by clicking," revealing a "fundamental knowledge-action gap." This initiative aims to directly address this pervasive behavioral vulnerability that "negates a substantial portion of our investment in cybersecurity awareness training."

Fortify Technical Defenses Against Phishing Threats

• **Specific Action:** Conduct a comprehensive review and enhancement of Egypt's existing email security gateways, endpoint detection and response (EDR) systems, and network segmentation controls. Prioritize the implementation of advanced threat protection features such as URL rewriting, attachment sandboxing, and AI-driven anomaly detection capabilities that can automatically block or quarantine suspicious emails *before* they reach an employee's inbox or prevent malicious payloads from executing post-click.

• **Justification:** The "persistence of a significant average click rate," despite improved awareness and reporting vigilance, confirms that initial compromises are still occurring, representing "an unacceptable level of risk to Egypt." While human awareness is crucial, human fallibility means technical safeguards are a necessary and critical safety net to protect "sensitive data, financial assets, and operational continuity" when behavioral controls inevitably fail.

Implement Individualized Remediation for Repeat Clickers

• **Specific Action:** Identify and engage the two documented repeat clickers in a personalized, hands-on remediation program. This program should go beyond standard awareness training, involving one-on-one coaching sessions, detailed analysis of their specific click incidents, and customized reinforcement exercises designed to address their persistent behavioral risks and identify underlying causes for their repeated susceptibility.

• **Justification:** The report explicitly notes that the "presence of two repeat clickers necessitates targeted individual remediation to address persistent behavioral risks that evade current awareness initiatives." This direct intervention is crucial to mitigate specific, ongoing vulnerabilities that general training has not resolved.

Implementing Recommendations with CSword

Implementing comprehensive security recommendations at scale, particularly those involving significant behavioural shifts and technical enhancements, can indeed be complex and resource-intensive for egypt. At CSword, we understand these challenges and offer a holistic suite of solutions designed to address precisely these kinds of findings.

• **To address the Targeted HR Department Cybersecurity Resilience Program:**

• Our **AI-Powered Training Platform** is uniquely positioned to deliver the specialized, mandatory cybersecurity awareness and phishing simulation program for egypt's HR department. We can create highly customized learning paths and role-based module assignments that specifically focus on social engineering tactics prevalent in HR communications (e.g., urgent benefits updates, sensitive data requests).

• We can configure frequent, high-fidelity phishing simulations that mimic scenarios HR personnel are most likely to encounter, with immediate "Just-in-Time" micro-lessons after failed attempts, directly emphasizing pre-click verification.

• Our rich analytics will provide granular data to prove the behavioural change and reduction in click rates specifically within the HR department, demonstrating improved pre-click discernment.

• For deeper engagement, we can conduct **Interactive Awareness Sessions** tailored specifically for the HR team, focusing on scenario-based workshops around sensitive data handling and advanced social engineering techniques.

• **To cultivate a Proactive "Think Before You Click" Culture Across Egypt:**

• The **AI-Powered Training Platform** is core to shifting egypt's "click first, report later" behavior. Our adaptive content delivers short, high-impact micro-training modules.

• Crucially, our platform provides real-time "Just-in-Time" feedback mechanisms during simulations, directly addressing the behavioural gap by prompting employees to verify *before* clicking. We can integrate "stop and think" reminders into the training experience.

• **Digital Awareness Deliverables**, such as customized infographics and short videos, can reinforce the "verify first, click never (if suspicious), and report immediately" paradigm across all internal communications, embedding the message into daily digital workflows.

• Rich analytics from our platform will allow egypt to track the overall reduction in click rates and improved reporting vigilance, providing evidence of a cultivated "think before you click" culture.

• **To fortify Technical Defenses Against Phishing Threats:**

• Our **Risk & Security Assessments** are designed to conduct a comprehensive review of egypt's existing email security gateways, EDR systems, and network segmentation controls. We perform baseline and gap analyses that quantify your current posture and feed data directly into actionable remediation plans for implementing advanced threat protection features.

• **Penetration Testing & Threat Simulation** services can then rigorously test these enhanced technical controls (like URL rewriting, attachment sandboxing, AI-driven anomaly detection) to identify any exploitable weaknesses *before* attackers do, ensuring they are effective in blocking or quarantining suspicious emails.

• Our **Data-Driven Control Reviews** provide dashboard and report outputs that justify technical-control investment and guide precise tuning efforts for your security systems, ensuring they provide the necessary safety net when behavioral controls fail.

• **To implement Individualized Remediation for Repeat Clickers:**

• The **AI-Powered Training Platform** allows for the identification of repeat clickers and the assignment of highly personalized learning paths. This goes beyond standard awareness training, adapting content based on their specific past click incidents and persistent behavioral risks.

• Our **Interactive Awareness Sessions** can be leveraged for the one-on-one coaching sessions and detailed analysis of their specific click incidents mentioned in the report. These can be customized, hands-on, scenario-based workshops designed to address their unique vulnerabilities and reinforce secure behaviors.

• The platform's analytics will provide granular data on the progress of these individuals, allowing for continuous adjustment and verification of their improved security posture.

CSword is not just a platform; we are a long-term partner dedicated to enhancing egypt's cybersecurity posture through a blend of advanced technology and expert-led services. We can help you transition from identifying vulnerabilities to proactively mitigating them, fostering a truly resilient security culture.

We'd welcome the opportunity to discuss these solutions in more detail and demonstrate how they can be tailored to egypt's specific needs. Please consider booking a tailored demo or exploring a combined assessment-training engagement with us.

This report is prepared by CSword for egypt

[CSword Official Stamp]