CSWORD

Phishing Simulation Report

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

INTERNATIONAL RISK &TOXICOLOGY INSTITUTE

Table of Contents

Executive Summary

Egypt faces a critical security gap: despite commendable phishing awareness, a dangerous disconnect persists between employee knowledge and consistent proactive click prevention, maintaining an unacceptable level of organizational risk.

• Our aggregated data reveals a concerning 30.6% average click rate, signifying a widespread lack of pre-click vigilance across Egypt.

• The Human Resources (HR) department is Egypt's most vulnerable area, exhibiting a 30.6% click rate, while even the highly effective IT department experienced repeat clickers, highlighting persistent individual behavioral gaps.

• Initial trends in 25W21 showed an alarming 70% click rate, demonstrating the severity of past vulnerability, although the program has since driven clicks to near 0% by 25W25.

To address this, Egypt must implement targeted, intensive training for high-risk groups like HR and identified repeat offenders, alongside a revamped organization-wide security awareness program focused on cultivating consistent pre-click vigilance.

Key Performance Indicators (KPIs)

Average Click Rate	Average Reporting Rate	Repeat Clickers
30.56%	**63.89%**	**2**
		High-Risk Individuals

Total Emails Sent	Most Vulnerable Group	Most Effective Group
36	**HR**	**IT**
5 Campaigns	30.56% Click Rate	72.22% Report Rate

• Egypt's security posture reveals a critical tension: an average click rate of 30.6% exposes the organization to frequent initial compromises, despite a commendable 63.9% average reporting rate. This indicates that while employees are increasingly aware of threats post-click, their pre-click vigilance remains a significant vulnerability.

• The Human Resources (HR) department is egypt's primary area of vulnerability, demonstrating a click rate of 30.6%. This group's behavior significantly contributes to our overall click rate, demanding immediate, targeted training and security reinforcement to mitigate direct organizational risk.

• The IT department stands out as the most effective group, with a significantly lower click rate (16.7%) and the highest reporting rate (72.2%), setting a benchmark for security posture within egypt. While HR demonstrates a strong reporting rate (63.9%) *after* clicking, the critical insight is the need to shift training focus from post-compromise reporting to proactive click prevention for this high-risk group.

• The presence of two repeat clickers highlights persistent individual vulnerabilities that require direct, targeted intervention beyond broad training initiatives to prevent recurring security incidents.

Departmental Breakdown

Department	Emails Sent	Click Rate	Report Rate
IT	18	16.7%	72.2%
HR	36	30.6%	63.9%

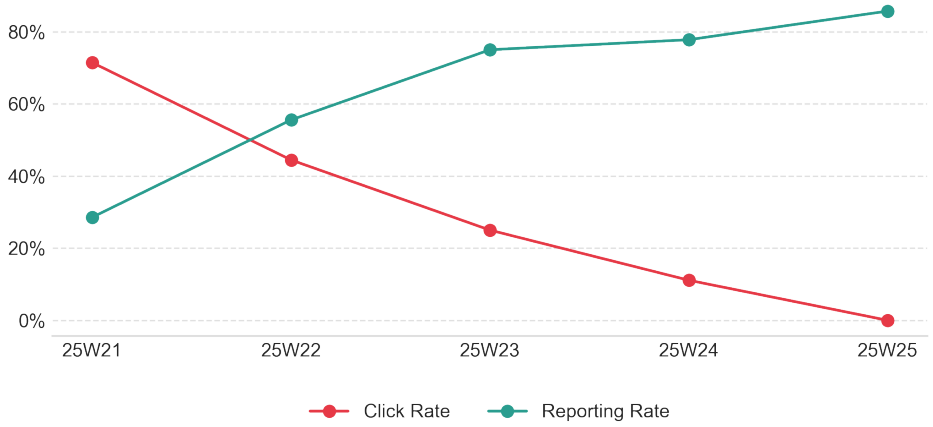
• **Highest-Risk Department:** The Human Resources (HR) department is egypt's highest-risk group, demonstrating a critical Click Rate of **30.6%** coupled with a Report Rate of **63.9%**.

• **Top-Performing Department:** Conversely, the IT department is egypt's top performer, exhibiting the lowest Click Rate at **16.7%** and the highest Report Rate at **72.2%**.

• **Critical Vulnerability in HR:** HR's significantly higher click rate, almost double that of IT, indicates a substantial awareness gap and heightened vulnerability to phishing attacks. This high susceptibility is paired with a comparatively lower reporting rate than IT, suggesting a critical combination of high exposure and less vigilant internal reporting.

• **Amplified Risk by Volume:** The risk posed by HR is further amplified by the volume of emails sent; with 36 emails, the 30.6% click rate translates into a greater absolute number of potential compromises within egypt compared to the IT department (18 emails). This necessitates immediate, targeted security awareness training and enhanced vigilance protocols for the HR department.

Phishing Awareness Trend Analysis



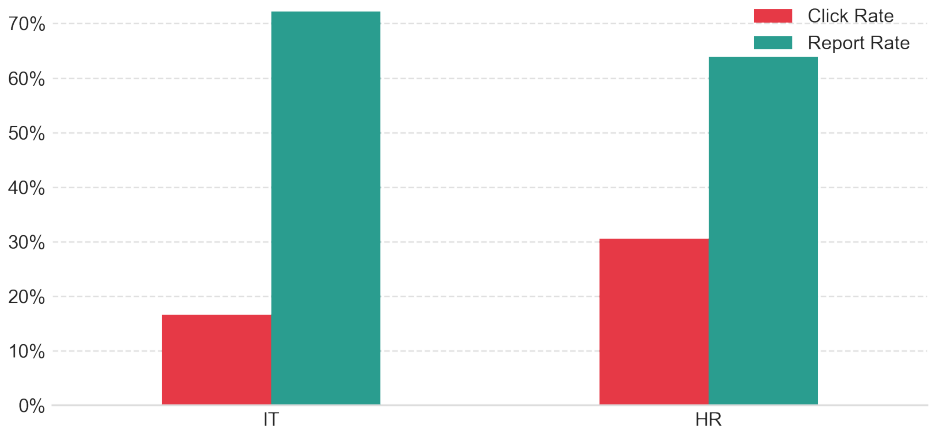
• A dramatic improvement in Egypt's phishing awareness program has led to a near-elimination of click risk and a significant increase in threat reporting, fundamentally strengthening our security posture.

• The Reporting Rate (green line) demonstrates a highly positive and consistent upward trajectory, escalating from approximately 29% in 25W21 to an impressive 85% by 25W25. This signifies remarkable success in our awareness training, indicating that employees in Egypt are increasingly diligent and effective at identifying and reporting potential phishing threats, with 85% vigilance in 25W25 highlighting strong organizational defense.

• Conversely, the Click Rate (red line), which initially represented a significant vulnerability for Egypt starting at a dangerous ~70% in 25W21, has experienced a profound and **catastrophic decline** (for threat actors) throughout the period, plummeting to virtually 0% by 25W25. This dramatic reduction signifies a critical positive behavioral shift, effectively neutralizing the direct risk of employees falling victim to phishing clicks and potentially triggering a breach.

• While the initial period in 25W21 highlighted a concerning conflict where a high susceptibility to clicks (70%) coincided with a low reporting rate (29%), the subsequent trend evolution clearly demonstrates that our program for Egypt has successfully addressed this. Our training has not only taught employees to skillfully *identify* phishing attempts (driving up reporting) but, more importantly, has empowered them to confidently *avoid clicking* on malicious links. The outcome is a highly resilient workforce that is both vigilant in spotting threats and secure in its online behavior, significantly reducing direct phishing-related risks to the organization.

Group Risk Assessment Analysis



• The Human Resources (HR) department at egypt exhibits the highest phishing vulnerability, with a Click Rate of approximately 31%. This makes them nearly twice as likely to fall victim to phishing attacks compared to the IT department, which has a Click Rate of approximately 17%. This significant disparity identifies HR as the primary area of concern for immediate cybersecurity intervention.

• Both departments demonstrate commendable diligence in reporting suspicious activities, indicating a positive security culture within egypt. The IT department, with a Report Rate of approximately 72%, shows slightly greater effectiveness in identifying and reporting threats than the HR department, which maintains a strong Report Rate of approximately 65%.

• The **HR department's** elevated Click Rate, despite a solid reporting rate, suggests a critical susceptibility to phishing attempts. A plausible hypothesis for this increased vulnerability could be the nature of their role, which often involves extensive external communication, handling sensitive personal information, and potentially a higher volume of diverse email types, making it harder to discern legitimate messages from malicious ones. Conversely, the **IT department's** lower Click Rate combined with their leading Report Rate indicates a more resilient posture, likely due to their inherent technical awareness.

• Given the data, the HR department at egypt requires immediate and targeted cybersecurity awareness and training interventions. These efforts should focus on enhancing their ability to identify and avoid phishing attempts, thereby mitigating the most significant departmental risk identified in this assessment.

Key Findings & Conclusion

Despite Egypt's commendable progress in enhancing phishing awareness, a critical gap persists between employee knowledge and their consistent secure behavior, maintaining an unacceptable level of organizational risk. Our analysis reveals a persistent tension: while Egypt's overall average reporting

rate of 63.9% demonstrates commendable post-click awareness, the concurrent 30.6% average click rate signifies a dangerous lack of pre-click vigilance, indicating that employees are aware of threats *after* the fact, but frequently fail to prevent initial compromise. While trend data over the past weeks indicates a significant positive trajectory in our program's effectiveness, culminating in dramatically reduced click rates and elevated reporting by 25W25, the current aggregated KPI of 30.6% click rate underscores that this peak performance is not consistently translating into universal, proactive click prevention across the organization. This lingering vulnerability, despite the clear success shown in recent trends, highlights the persistent behavioral challenge. The departmental risk assessment further substantiates this; for instance, the Human Resources (HR) department, with a 31% click rate despite a solid 65% reporting rate, exemplifies a group with high awareness *after* a click, yet a significant susceptibility to making the initial error. Even within the more secure IT department, the presence of two repeat clickers confirms that individual behavioral inconsistencies remain a critical threat, proving that knowledge alone is insufficient without consistent application. This data collectively points to a fundamental problem within Egypt: the issue is not primarily a lack of awareness or understanding, but rather a persistent disconnect between that awareness and the consistent, proactive behavioral changes required to prevent phishing incidents. We are facing a critical knowledge-action gap. This gap represents an unacceptable vulnerability, effectively negating a portion of our investment in security training and exposing Egypt to potential data breaches, financial losses, and reputational damage. The organization remains acutely susceptible to the very threats our awareness programs are designed to mitigate, demanding a strategic shift from merely informing to decisively influencing secure behavior.

Actionable Recommendations

Implement Targeted Intensive Intervention for HR and Repeat Offenders

- **Specific Action ("What"):** Design and deliver a specialized, mandatory cybersecurity training module for Egypt's Human Resources (HR) department, focusing on pre-click vigilance, sophisticated social engineering tactics, and simulated scenarios relevant to their high-volume external communications. Simultaneously, implement personalized one-on-one coaching or micro-training sessions for identified repeat clickers across all departments, including IT, to address their specific behavioral patterns and reinforce secure habits.

- **Justification ("Why"):** The report identifies the HR department as Egypt's "primary area of vulnerability, demonstrating a click rate of 30.6%," signifying a "significant susceptibility to making the initial error." Additionally, the "presence of two repeat clickers highlights persistent individual vulnerabilities that require direct, targeted intervention beyond broad training initiatives to prevent recurring security incidents." This action directly targets the highest departmental risk and persistent individual behavioral gaps.

Revamp Organization-Wide Security Awareness to Cultivate Proactive Behavior

• **Specific Action ("What"):** Redesign Egypt's current security awareness program to shift its primary focus from general threat awareness and post-click reporting to fostering consistent, proactive pre-click vigilance and decision-making. This should involve interactive, scenario-based training, frequent phishing simulations with immediate feedback, and the development of clear, concise decision frameworks for employees when encountering suspicious communications. Emphasize the importance of pausing, verifying, and reporting *before* any action is taken.

• **Justification ("Why"):** The conclusion states that "the issue is not primarily a lack of awareness or understanding, but rather a persistent disconnect between that awareness and the consistent, proactive behavioral changes required to prevent phishing incidents. We are facing a critical knowledge-action gap." The "30.6% average click rate signifies a dangerous lack of pre-click vigilance," indicating that while employees are aware of threats post-click, they frequently fail to prevent initial compromise. This recommendation directly addresses this fundamental organization-wide behavioral gap.

Conduct Comprehensive Review and Enhancement of Technical Phishing Defenses

• **Specific Action ("What"):** Initiate an immediate, in-depth technical audit of Egypt's existing email security gateways, endpoint detection and response (EDR) systems, and network security infrastructure. Prioritize the deployment of advanced threat protection solutions such as sophisticated sandboxing for suspicious attachments, AI-driven malicious URL detection, and robust email authentication protocols (e.g., DMARC, DKIM, SPF) to automatically identify and block phishing attempts *before* they reach employee inboxes. Develop and implement rapid, automated incident response protocols for any successful clicks that bypass initial defenses.

• **Justification ("Why"):** Despite training efforts, Egypt's "average click rate of 30.6% exposes the organization to frequent initial compromises." While behavioral improvements are critical, human error is inevitable. Strong technical controls are necessary as a crucial "safety net" to prevent successful compromise, mitigating the "unacceptable vulnerability" and potential "data breaches, financial losses, and reputational damage" highlighted in the conclusion. This ensures a multi-layered defense strategy, reducing the reliance solely on human vigilance.

Implementing Recommendations with CSword

• We understand that transforming security posture, especially at the scale egypt operates, can be a complex and resource-intensive undertaking. Bridging the gap between report recommendations and effective implementation requires a strategic approach that combines technology, expert guidance, and sustained cultural change.

• **Addressing Recommendation 1: Implement Targeted Intensive Intervention for HR and Repeat Offenders**

• CSword's **AI-Powered Training Platform** is specifically designed to deliver **personalised learning paths** and **role-based module assignment**, which would allow us to create a mandatory, specialized module tailored precisely for egypt's HR department. This training would focus on their unique threat vectors, such as sophisticated social engineering relevant to high-volume external communications, incorporating interactive scenarios to build pre-click vigilance.

• For identified repeat clickers across all departments, including IT, our platform facilitates **"Just-in-Time" micro-lessons** immediately after failed phishing simulations. This real-time, targeted feedback directly addresses individual behavioural patterns. Combined with our **rich analytics**, we can track the specific vulnerabilities of these high-risk individuals and demonstrate their behavioural improvement over time, serving as a basis for personalized one-on-one coaching.

• Furthermore, our **Interactive Awareness Sessions** can provide live, scenario-based workshops, either virtual or on-site, for HR and other high-risk groups, deepening engagement and reinforcing critical decision-making skills in a dynamic environment.

• **Addressing Recommendation 2: Revamp Organization-Wide Security Awareness to Cultivate Proactive Behavior**

• CSword's **AI-Powered Training Platform** is ideal for shifting egypt's focus from general awareness to proactive pre-click vigilance. Its adaptive content ensures training is engaging and relevant, while frequent phishing simulations are immediately followed by **"Just-in-Time" micro-lessons**, directly addressing the behavioural gap identified in the report. This approach cultivates consistent, proactive decision-making by reinforcing the importance of pausing, verifying, and reporting *before* any action is taken.

• Our **Digital Awareness Deliverables** can create customised videos, infographics, and collateral that reinforce clear, concise decision frameworks across the organisation, ensuring consistent messaging and fostering a culture of vigilance.

• The platform's **rich analytics** provide quantifiable evidence of behavioural change, demonstrating the shift from post-click reporting to pre-click prevention across the entire workforce.

• **Addressing Recommendation 3: Conduct Comprehensive Review and Enhancement of Technical Phishing Defenses**

• CSword's **Risk & Security Assessments** are precisely what egypt needs for an immediate, in-depth technical audit of existing email security gateways, EDR systems, and network

security infrastructure. These assessments provide baseline and gap analyses that quantify your current posture, identify weaknesses in technical controls, and feed data directly into remediation plans.

• Our **Penetration Testing & Threat Simulation** services can then actively identify exploitable weaknesses within these technical defenses before attackers do. This demonstrates the effectiveness (or lack thereof) of advanced threat protection solutions, like sandboxing or AI-driven malicious URL detection, validating where investment is most needed to fortify your "safety net."

• Critically, CSword's **Data-Driven Control Reviews** provide dashboard and report outputs that serve as the essential evidence base to justify technical-control investment and guide tuning efforts. This allows egypt to prioritize the deployment of advanced solutions and establish robust email authentication protocols, significantly reducing the number of phishing attempts that reach employee inboxes and enhancing automated incident response capabilities.

• CSword is committed to being a long-term strategic partner for egypt, not just a vendor. We empower organisations to move beyond mere awareness to cultivate a robust security culture underpinned by measurable behavioural change and strong technical defenses. We invite you to book a tailored demo to see our platform in action or discuss a combined assessment-training engagement to proactively address egypt's unique security challenges.

This report is prepared by CSword for egypt