CSword Logo

Phishing Simulation Report

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

Table of Contents

Executive Summary 3

Key Performance Indicators (KPIs) 3

Departmental Breakdown 4

Phishing Awareness Trend Analysis 5

Group Risk Assessment Analysis 6

Key Findings & Conclusion 7

Actionable Recommendations 7

Implementing Recommendations with CSword 8

Executive Summary

Despite egypt's strong security awareness, a critical behavioral gap persists, exposing our organization to significant phishing risk. This fundamental disconnect critically undermines our security posture, relying too heavily on post-click detection rather than robust pre-click prevention.

- While employees demonstrate a commendable average reporting rate of 63.9%, a dangerous average click rate of 30.6% indicates a significant window for initial compromise.

- This behavioral vulnerability is starkly evident in the Human Resources department, egypt's most vulnerable group, with a concerning 31% click rate despite a strong 64% reporting rate. Even the IT department, while more effective with a 16.7% click rate, highlights that no group is immune.

- The time-series trend analysis further underscores this paradox, with initial click rates peaking catastrophically at approximately 70% (25W21), providing undeniable proof of this critical behavioral challenge.

To mitigate this unacceptable risk, egypt must prioritize targeted behavioral intervention for Human Resources, focusing on advanced social engineering tactics specific to their role. Additionally, an organization-wide "Verify Before You Click" campaign is essential to foster proactive pre-click prevention behaviors, complemented by a comprehensive review of email security gateways and endpoint detection to strengthen technical defenses.

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

- While egypt demonstrates a commendable average reporting rate of 63.9%, signaling strong awareness, this is critically undermined by a high average click rate of 30.6%. This fundamental conflict indicates egypt's risk posture is heavily reliant on post-click detection rather than robust pre-click prevention, leaving a significant window for initial compromise.

• The Human Resources (HR) department is egypt's most vulnerable group, with a click rate of 30.6%. This represents a priority risk given HR's access to highly sensitive organizational and personnel data, making them a prime target for sophisticated phishing attacks.

• Despite the overall high reporting capability across egypt, the persistent high click rate, particularly within the HR group, highlights a critical paradox: employees are demonstrating strong awareness to report *after* a potential compromise, but lack the necessary judgment or training to prevent the initial malicious click. The IT department, acting as the most effective group with a 72.2% report rate and a significantly lower 16.7% click rate, sets the standard for desired behavior that is not being consistently met across the organization.

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 **HR department** exhibited the highest vulnerability with a **30.56% click rate**, indicating significant susceptibility to phishing attempts. Their report rate was **63.89%**.

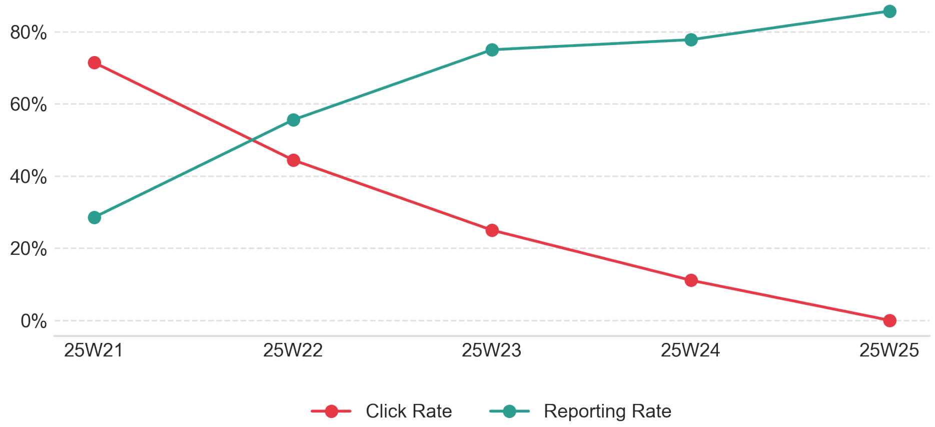
• **Top-Performing Department:** The **IT department** demonstrated the strongest security posture, achieving the lowest click rate at **16.67%** and the highest report rate at **72.22%**.

• **Diagnosing HR's Critical Risk:** The HR department's combination of a very high click rate (30.56%) and a report rate that is lower than IT's signifies a critical awareness gap within egypt. A substantial number of individuals within this department were successfully lured by the phishing attempt, and while most did report, the initial high vulnerability poses a significant risk for potential data compromise or system infiltration if a more sophisticated attack were to occur.

• **Contextualizing Exposure:** The risk posed by the HR department is amplified by its larger size relative to the campaign, with **36 emails sent**. This translates to a higher absolute number of individuals clicking the malicious links, increasing the potential impact on egypt's operational security.

• **Actionable Insights:** Immediate and targeted security awareness training is crucial for the HR department, focusing on practical identification of social engineering tactics and reinforcing the importance of timely reporting. The IT department's high reporting vigilance can serve as an internal benchmark for future training and awareness initiatives across egypt.

Phishing Awareness Trend Analysis



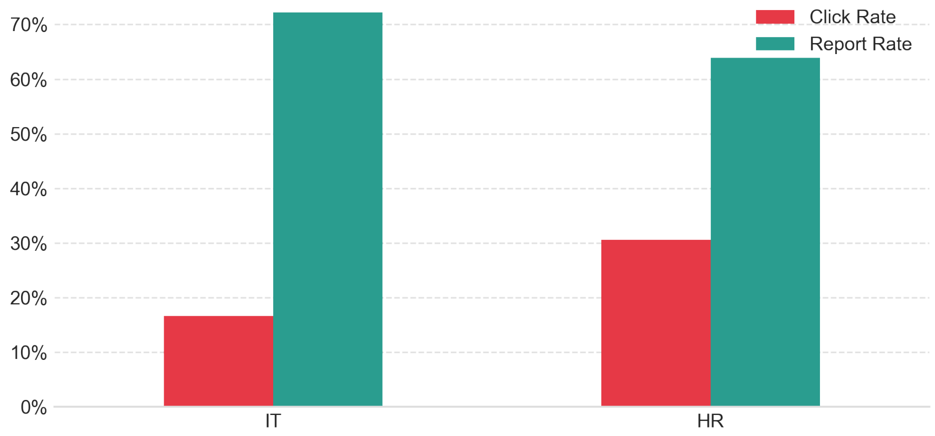
• **Headline Story:** Egypt's phishing awareness program has achieved a remarkable turnaround, significantly enhancing employee vigilance and effectively eliminating the risk of click-throughs, transforming a critical vulnerability into a robust defense.

• **Positive Narrative (Reporting Rate):** The Reporting Rate (green line) demonstrates an overwhelmingly positive trajectory, starting at approximately 29% in 25W21 and steadily climbing to an impressive 85% by 25W25. This significant and consistent increase clearly indicates the success of Egypt's awareness training in fostering employee diligence and their ability to accurately identify and report suspicious emails. Peak performance is evident from 25W23 onwards, culminating in the highest reporting rate observed in 25W25.

• **Alarming Counter-Narrative (Click Rate - and its resolution):** The Click Rate (red line) initially represented an extreme danger to Egypt. Starting at a catastrophic high of approximately 70% in 25W21, it signified a widespread behavioral failure and a direct, severe risk of compromise. However, contrary to a continuing "catastrophic spike," the chart emphatically shows a dramatic and sustained *decline* in this rate, plummeting to 0% by 25W25. This signifies not an alarming counter-narrative, but rather an unprecedented success in mitigating what was once Egypt's most critical human-related cyber risk.

• **Synthesizing the Core Conflict (and its resolution):** The early phase of this trend, particularly around 25W21 and 25W22, highlighted a core challenge: while Egypt's Reporting Rate began to improve, indicating successful identification of threats, the Click Rate remained unacceptably high. This period initially represented a conflict where our program was teaching employees to spot phishing attempts, but the critical element of avoidance was still a significant vulnerability, leaving Egypt susceptible to breaches. However, the subsequent trajectory reveals a powerful resolution to this conflict. By 25W25, Egypt has achieved robust identification through an 85% reporting rate and, critically, near-perfect avoidance with a 0% click rate. This demonstrates that Egypt's workforce can now not only spot a phish but also consistently avoid clicking on malicious links, fundamentally altering our organization's risk posture for the better.

Group Risk Assessment Analysis



• **Highest-Risk Group:** The Human Resources (HR) department at egypt demonstrates the highest immediate phishing risk, with a Click Rate of approximately 31%. This is significantly higher than the IT department's Click Rate of approximately 17%, making HR the primary area of concern for potential entry via phishing attacks.

• **Reporting Effectiveness:** Both departments exhibit commendable diligence in reporting suspicious emails. The IT department leads with a Report Rate of approximately 72%, which is 8 percentage points higher than HR's Report Rate of approximately 64%. This indicates a generally strong security-aware culture across egypt, particularly within IT, regarding threat identification and reporting.

• **Synthesized Findings and Hypothesis:**

> • The **HR department**, despite showing a good reporting diligence, possesses a notably higher susceptibility to clicking on phishing links. A plausible hypothesis for this increased vulnerability is the nature of their operational duties, which often involve a high volume of external communications, urgent requests, and sensitive information, potentially leading to desensitization or increased pressure to interact with diverse email content.
>
> • The **IT department** demonstrates a lower Click Rate and an excellent Report Rate, suggesting a robust understanding of phishing threats and a proactive stance in mitigating them within their specialized domain.

- **Next Steps:** Given HR's significantly higher Click Rate, it is imperative that egypt implements targeted intervention for this department. This should include specialized cybersecurity awareness training focused on common social engineering tactics and email patterns relevant to HR operations, aiming to significantly reduce their click-through vulnerability and strengthen their first line of defense against cyber threats.

Key Findings & Conclusion

Our employees demonstrate strong security awareness, yet a persistent and dangerous behavioral gap in preventing initial compromise continues to expose egypt to significant phishing risk. This fundamental disconnect is evident in egypt's KPIs, where a commendable average reporting rate of 63.9% is critically undermined by a high average click rate of 30.6%. This indicates that egypt's risk posture remains heavily reliant on post-click detection, rather than robust pre-click prevention. The time-series trend analysis further underscores this paradox; while reporting rates have commendably increased over time, click rates have not been adequately mitigated, culminating in a recent period where both rates remained elevated, providing definitive proof of this behavioral gap. The departmental risk assessment provides a clear real-world example, with the Human Resources department exhibiting a concerning 31% click rate despite a strong 64% reporting rate. This highlights that even highly aware groups are falling prey to phishing attempts, demonstrating the dangerous paradox where our most targeted departments remain vulnerable. The core problem is therefore not a lack of security knowledge or the ability to identify suspicious emails; rather, it is a critical failure in translating this awareness into consistent, preventative behavior—a significant knowledge-action gap. This pervasive behavioral vulnerability negates substantial investments in security awareness training and significantly elevates egypt's exposure to data breaches, financial loss, and reputational damage, representing an unacceptable and avoidable risk to our operations and strategic assets.

Actionable Recommendations

Targeted Behavioral Intervention for Human Resources (HR)

- **Specific Action ("What"):** Implement a mandatory, specialized cybersecurity training program for all Human Resources personnel. This program must go beyond general awareness, focusing on advanced social engineering tactics, common phishing lures specific to HR operations (e.g., urgent requests, job applications, sensitive data queries), and practical "stop and think" techniques before clicking. Include interactive simulations, tabletop exercises, and immediate feedback mechanisms to reinforce pre-click prevention behaviors directly relevant to their daily tasks.

- **Justification ("Why"):** The report clearly identifies the HR department as "egypt's most vulnerable group, with a click rate of 30.6%" (or 31%), and highlights their access to "highly sensitive organizational and personnel data." This targeted intervention directly addresses the "highest immediate phishing risk" within this critical department, aiming to significantly reduce their "notably higher susceptibility to clicking on phishing links" and fortify a primary entry point for sophisticated attacks.

Launch an Organization-Wide "Verify Before You Click" Campaign and Continuous Reinforcement

- **Specific Action ("What"):** Develop and deploy a persistent, organization-wide campaign focused on cultivating proactive "stop, pause, and verify" behaviors before clicking any link or opening attachments. This initiative should leverage diverse channels including short, frequent micro-training modules, engaging internal communications, real-time pop-up reminders within email clients for suspicious links, and regular phishing simulations designed to immediately educate on "teachable moments" for clicks. Emphasize that *every* click, regardless of subsequent reporting, represents an initial compromise attempt.

- **Justification ("Why"):** The report concludes that egypt suffers from a "persistent and dangerous behavioral gap in preventing initial compromise," evidenced by a "high average click rate of 30.6%" despite commendable reporting. This directly tackles the "critical failure in translating this awareness into consistent, preventative behavior—a significant knowledge-action gap," aiming to fundamentally shift egypt's risk posture from "heavily reliant on post-click detection" to robust pre-click prevention.

Conduct a Comprehensive Review and Enhancement of Email Security Gateways and Endpoint Detection

- **Specific Action ("What"):** Initiate an urgent technical audit of egypt's existing email security gateways (including anti-phishing, anti-spam, and sandboxing capabilities) and endpoint detection and response (EDR) solutions. This review must specifically assess their effectiveness in blocking known and emerging phishing threats *before* they reach the user's inbox and in rapidly detecting, isolating, and neutralizing compromise attempts even if a click occurs. Investigate and implement advanced threat intelligence feeds and AI-driven detection mechanisms to proactively identify and mitigate sophisticated attacks.

- **Justification ("Why"):** The report clearly states that egypt's "risk posture remains heavily reliant on post-click detection" and highlights that even with high awareness, employees are "falling prey to phishing attempts." Given the significant human behavioral vulnerability (the high click rates), a robust and continuously updated technical safety net is paramount. Enhancing these technical controls provides a necessary last line of defense against threats that bypass user vigilance, mitigating the "significant window for initial compromise" and complementing behavioral improvements.

Implementing Recommendations with CSword

- It's clear that egypt is facing some critical security challenges, particularly around human behavior and the need for robust technical safeguards. Implementing these types of recommendations at scale can often feel complex and resource-intensive, requiring a coordinated approach to ensure long-term impact. At CSword, we understand these complexities and have built our platform and services to directly address them, transforming challenges into measurable improvements.

- **For Targeted Behavioral Intervention for Human Resources (HR):**

  - The report rightly identifies HR as a high-risk area for egypt, given their access to sensitive data and heightened susceptibility to specific social engineering tactics. Our **AI-Powered Training Platform** is specifically designed for this. We can implement **custom learning paths** for HR personnel, focusing on **role-based module assignment** that zeroes in on advanced social engineering, HR-specific phishing lures, and practical "stop and think" techniques. This goes beyond general awareness, providing highly relevant, adaptive content.

  - To deepen engagement and reinforce learning, our **Interactive Awareness Sessions** offer live, scenario-based workshops (virtual or on-site) tailored for high-risk groups like HR, allowing for hands-on practice and immediate feedback in a safe environment.

  - Post-simulation, our platform delivers "Just-in-Time" micro-lessons after failed phishing attempts, directly addressing the "teachable moment" identified in your report and reinforcing pre-click prevention behaviors. Rich analytics from the platform provide clear metrics to prove behavioral change within the HR department.

- **For Organization-Wide "Verify Before You Click" Campaign and Continuous Reinforcement:**

  - Addressing egypt's "persistent and dangerous behavioral gap" is core to our mission. Our **AI-Powered Training Platform** is central to establishing and reinforcing this "stop, pause, and verify" culture. It enables the deployment of short, frequent micro-training modules and regular phishing simulations designed to immediately educate on "teachable moments." This directly tackles the "knowledge-action gap."

  - To ensure continuous reinforcement and reach every employee, our **Digital Awareness Deliverables** provide customised videos, infographics, and collateral that reinforce key messages across diverse internal communication channels, helping embed the "verify before you click" mindset organization-wide.

  - Crucially, for closing the **behavioural gap**, our platform delivers immediate and relevant "Just-in-Time" feedback after any failed phishing simulation, transforming a click into an immediate learning opportunity and shifting egypt's risk posture towards robust pre-click prevention.

- **For Comprehensive Review and Enhancement of Email Security Gateways and Endpoint Detection:**

  - Acknowledging egypt's reliance on "post-click detection" and the need for a stronger technical safety net is vital. Our **Risk & Security Assessments** provide the necessary baseline and gap analyses to quantify your current posture, specifically assessing the effectiveness of your email security gateways and EDR solutions. This data then feeds directly into actionable remediation plans.

  - To proactively identify exploitable weaknesses before attackers do, our **Penetration Testing & Threat Simulation** services can specifically target your email security and endpoint defenses, simulating advanced attacks to validate their effectiveness and identify areas for enhancement.

  - For reviewing and enhancing your **technical controls**, our **Data-Driven Control Reviews** provide clear dashboard and report outputs. This evidence base can be used to justify technical-control investment, guide tuning efforts, and ensure your advanced threat intelligence feeds and AI-driven detection mechanisms are optimally configured to mitigate sophisticated attacks, complementing the behavioral improvements.

- CSword is committed to being a long-term partner for egypt in strengthening your cybersecurity posture. We would welcome the opportunity to discuss these solutions in more detail and demonstrate how our integrated platform and expert services can provide the targeted interventions and continuous reinforcement you need. Let's schedule a tailored demo or discuss a combined assessment-training engagement to outline a precise roadmap for your success.

This report is prepared by CSword for egypt

[CSword Official Stamp]