CSWORD

Phishing Simulation Report

Reporting Period: August 02, 2025 – September 30, 2025

Table of Contents

Executive Summary

Compumacy faces a critical human-centric vulnerability: while employees are increasingly adept at identifying phishing attempts, a dangerous behavioral gap persists, leading many to click malicious links *before* reporting them.

- An average click rate of 27.7% significantly undermines our 50% average reporting rate, demonstrating widespread engagement with threats before reporting. The Human Resources department presents the most immediate risk, exhibiting an alarming 42.8% click rate.

- The IT department presents a unique paradox; while effective at reporting (57% report rate), they also exhibit a concerning 29% click rate, underscoring a potential desensitization or overconfidence despite their technical expertise.

- This behavioral failure is unequivocally highlighted by the time-series analysis, particularly in week 25W38, where a 100% reporting rate coincided with a 25% click rate, proving employees often interact with threats *before* reporting them.

To address this, Compumacy must urgently implement targeted training for the high-risk Human Resources department and fundamentally redesign its organization-wide cybersecurity awareness program to prioritize immediate protective action, fostering a 'report first, then verify' mindset to bridge this critical knowledge-action gap.

Key Performance Indicators (KPIs)

Average Click Rate	Average Reporting Rate	Repeat Clickers
27.78%	**50.00%**	**3**
		High-Risk Individuals

Total Emails Sent	Most Vulnerable Group	Most Effective Group
36	**HR**	**Sales**
5 Campaigns	42.86% Click Rate	72.73% Report Rate

- Compumacy faces a critical human-centric cybersecurity vulnerability: an average click rate of 27.7% significantly undermines our 50% average reporting rate. This indicates that a substantial portion of employees are clicking malicious links before reporting, creating a dangerous exposure window despite growing awareness.

• The Human Resources (HR) department is Compumacy's most immediate risk, exhibiting an alarming 42.8% click rate. Compounding this, their extremely low 14.2% reporting rate means successful attacks on HR may go undetected, presenting a severe threat to sensitive data and operations.

• While the Sales department is our most effective at reporting suspicious activity (72.7% report rate), their 18.1% click rate reveals a key insight: even our most diligent employees are still susceptible to initial phishing attempts. This underscores the need for preventative measures that stop clicks, not just enhance post-compromise reporting.

• The identification of 3 repeat clickers across campaigns highlights a persistent gap in user behavior adaptation, demanding targeted intervention and more intensive training to mitigate this recurring internal threat.

Departmental Breakdown

Department	Emails Sent	Click Rate	Report Rate
Finance	11	27.3%	45.5%
HR	7	42.9%	14.3%
IT	7	28.6%	57.1%
Sales	11	18.2%	72.7%

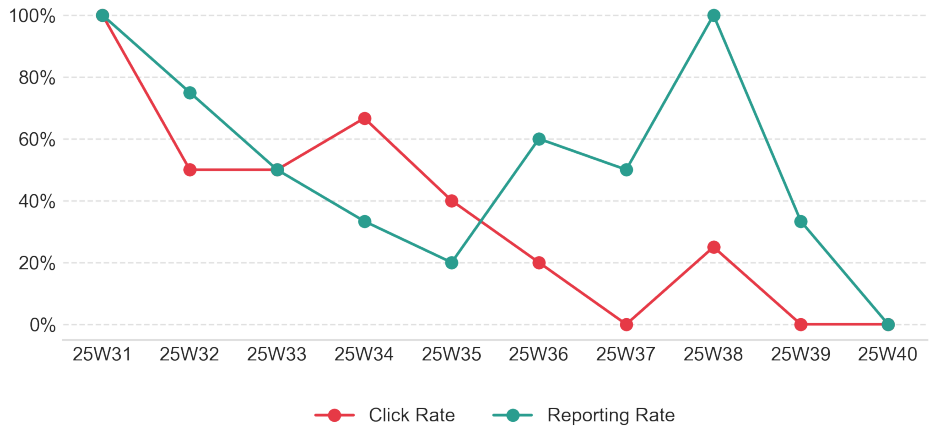
• **Highest-Risk Department:** The Human Resources (HR) department is identified as the highest-risk group within Compumacy, exhibiting a click rate of 42.9%. This signifies a significant vulnerability to phishing attempts.

• **Diagnosing HR's Risk Profile:** HR's alarmingly high click rate is compounded by a critically low report rate of 14.3%. This combination indicates a severe awareness and response gap: employees are not only highly susceptible to clicking on malicious links but are also failing to report these incidents. This lack of reporting vigilance delays detection and mitigation efforts by our security teams, presenting a substantial internal threat, despite their smaller department size of 7 emails sent.

• **Top-Performing Department:** The Sales department is the top performer, demonstrating robust security awareness and vigilance. With a low click rate of 18.2% and an excellent report rate of 72.7% from 11 emails sent, this team effectively recognizes and reports phishing attempts.

• **Potential Silent Risks:** While not displaying the extreme vulnerability of HR, the Finance department (11 emails sent) warrants attention. Their moderate click rate of 27.3% is paired with a report rate of 45.5%. While not as critically low as HR's, this report rate is notably lower than IT and Sales, suggesting a potential for underreporting or complacency that could allow more sophisticated attacks to go undetected in the future.

Phishing Awareness Trend Analysis



• Compumacy's phishing awareness program shows a critical disconnect: while employees are becoming adept at identifying and reporting phishing attempts, a dangerous proportion are still clicking malicious links, culminating in a period where high reporting rates coexisted with alarming click rates.

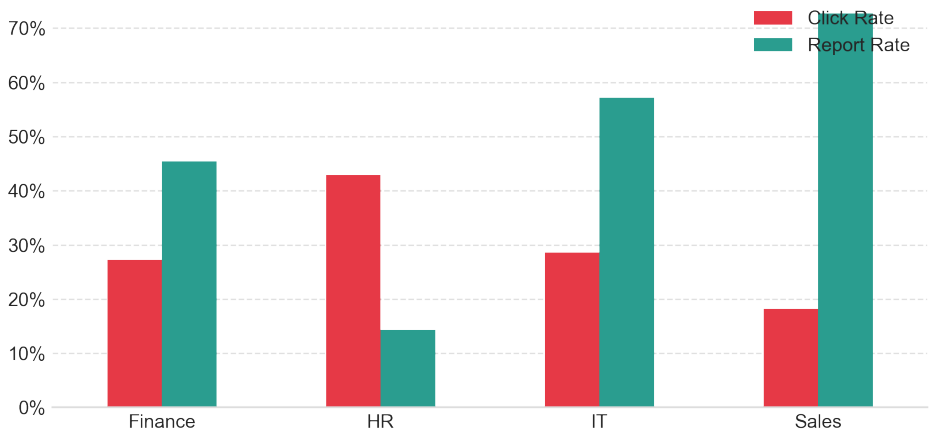
• The **Reporting Rate** (green line) demonstrates a generally positive and encouraging trajectory, indicating a growing diligence within Compumacy's workforce. Beginning at 100% in 25W31, and impressively returning to a peak of 100% in 25W38, this trend signifies that our awareness training is successfully enabling employees to recognize and report suspicious emails, which is a foundational element of our cybersecurity defense.

• Conversely, the **Click Rate** (red line) presents a highly alarming and volatile counter-narrative. Despite periods of significant improvement (reaching 0% in 25W37 and 25W39), the catastrophic spike to approximately 25% in 25W38 represents a severe behavioral failure. This indicates that a quarter of our employees, in that week, directly engaged with a simulated threat, representing a profound and direct risk of breach, data compromise, and operational disruption for Compumacy.

• The most critical insight is the simultaneous peak of both the Reporting Rate and the Click Rate in 25W38. This paradoxical scenario reveals that our program is effectively teaching employees *how to identify* phishing attempts, but critically failing to prevent them from *interacting with* these threats in the first place. Compumacy's workforce is demonstrating an ability to recognize and

report a phish, but often only *after* they have already clicked the malicious link, transforming a moment of successful identification into a near-miss or even a potential incident, underscoring a urgent need to shift focus from mere detection to robust prevention behaviors.

Group Risk Assessment Analysis



• The Human Resources (HR) department exhibits the highest Click Rate at approximately 43%, making them the most vulnerable to phishing attempts within Compumacy. This rate is significantly higher than other departments; for instance, it's about 2.4 times higher than Sales (18%), and approximately 1.5 times higher than both Finance (28%) and IT (29%). This highlights HR as a primary area of concern for immediate intervention.

• Regarding reporting effectiveness, Sales demonstrates the strongest vigilance with an excellent Report Rate of approximately 68%. The IT department also shows a robust reporting culture at approximately 57%. Finance maintains a moderate Report Rate of around 46%. In stark contrast, HR lags significantly with the lowest Report Rate at only about 14%, indicating a critical gap in their ability or willingness to report suspicious emails, which compounds their high click rate risk.

• **HR Synthesis:** The HR department presents the most critical overall risk profile at Compumacy, characterized by the highest click rate (approximately 43%) combined with the lowest report rate (approximately 14%). This dual vulnerability suggests a pressing need for enhanced awareness and procedural reinforcement among HR staff.

• **IT Synthesis & Hypothesis:** While HR exhibits the highest click rate, the IT department's Click Rate of approximately 29% is still a significant concern, especially given their technical role. Although their Report Rate of approximately 57% is commendable, their susceptibility to clicking highlights a specific vulnerability. A plausible hypothesis for IT's higher click rate despite their technical proficiency could be exposure to an exceptionally high volume of technical communications, which may lead to a form of desensitization to common phishing indicators, or

perhaps an overconfidence in their ability to discern and safely interact with suspicious content.

• Given these findings, Compumacy must implement targeted cybersecurity awareness and training initiatives. The HR department requires immediate and comprehensive intervention focusing on identifying phishing attempts and reinforcing reporting protocols. Furthermore, a specialized awareness program for IT personnel, addressing potential desensitization and emphasizing vigilance despite their technical proficiency, is crucial to mitigate their specific risk profile.

Key Findings & Conclusion

While Compumacy's workforce is increasingly adept at *identifying* phishing attempts, a critical and dangerous behavioral gap persists, leading a substantial portion of employees to *click* malicious links before reporting them. This concerning trend is clearly evidenced by our KPIs, where an average click rate of 27.7% significantly undermines our 50% average reporting rate, demonstrating that many employees engage with threats before reporting them. The time-series analysis further amplifies this paradox, with the alarming peak in week 25W38 showing both click and report rates simultaneously at their highest, definitively proving that our program is teaching employees how to recognize a phish, but often only *after* they have already interacted with it. This behavioral failure is not isolated, as highlighted by departmental risks: HR, despite our training efforts, exhibits a dire 42.8% click rate paired with a minimal 14.2% reporting rate, while even the technically proficient IT department shows a concerning 29% click rate, underscoring a potential desensitization. Furthermore, the persistent identification of repeat clickers across campaigns confirms that for some, the behavioral adaptation remains elusive.

This body of evidence points to a fundamental problem: Compumacy's challenge is not primarily a lack of *awareness* but a critical disconnect between knowledge and secure *action*. The issue is a behavioral failure, an inability to consistently translate learned information into immediate, protective responses. This knowledge-action gap renders our substantial investments in cybersecurity awareness training less effective, leaving Compumacy unacceptably vulnerable to data breaches, financial loss, and reputational harm. It represents a pervasive human-centric vulnerability that directly negates our proactive security measures and demands urgent, targeted intervention.

Actionable Recommendations

Implement Urgent, Targeted Training for Human Resources (HR)

• **Specific Action:** Launch an immediate, mandatory, and highly interactive cybersecurity awareness program specifically for the HR department. This program must intensely focus on advanced phishing identification techniques, the critical importance of *not clicking* suspicious links, and robust, rapid reporting protocols. Tailor content to common HR-specific phishing lures and scenarios.

• **Justification:** The report conclusively identifies HR as Compumacy's most critical and immediate risk, exhibiting an alarming 42.8% click rate paired with a critically low 14.2% reporting rate. This targeted intervention is essential to protect the highly sensitive data and operational integrity associated with HR functions.

Revamp Cybersecurity Awareness Program to Prioritize "Think Before You Click"

• **Specific Action:** Redesign Compumacy's organization-wide cybersecurity awareness training to fundamentally shift its focus from simply identifying threats to proactively instilling a "verify, then click" or "report first, then verify" mindset. This includes implementing more frequent, shorter, scenario-based modules, emphasizing the immediate protective action of *not clicking* and promptly reporting. Integrate interactive exercises and positive reinforcement for zero-click behaviors.

• **Justification:** The report's core finding is a "critical disconnect between knowledge and secure action," evidenced by Compumacy's average 27.7% click rate significantly undermining the 50% reporting rate. The paradoxical peak in 25W38, where high click rates coincided with high reporting rates, definitively proves that employees are often interacting with threats *before* reporting them, highlighting a pervasive "knowledge-action gap" that demands a strategic shift in training focus.

Conduct Specialized Training for IT Personnel

• **Specific Action:** Develop and deliver a specialized cybersecurity awareness program tailored specifically for Compumacy's IT department. This training should explicitly address the potential for desensitization or overconfidence due to high message volume, focusing on reinforcing hyper-vigilance, recognizing sophisticated and targeted phishing attempts, and emphasizing strict adherence to security protocols regardless of technical proficiency or perceived threat.

• **Justification:** While highly technical, the IT department exhibits a concerning 29% click rate. The report hypothesizes this may stem from desensitization or overconfidence. Given IT's elevated access and critical role, mitigating this specific vulnerability is crucial to Compumacy's overall security posture.

Establish a Program for Persistent Behavioral Non-Compliance

• **Specific Action:** For any Compumacy employees identified as repeat clickers across multiple phishing simulation campaigns, implement a mandatory, individualized, in-depth coaching and retraining program. This program should include personalized feedback on their specific behavioral patterns, a comprehensive review of cybersecurity best practices, and a clear articulation of the heightened risks posed by their actions.

• **Justification:** The report specifically highlights the persistent identification of repeat clickers across campaigns, confirming that for a subset of the workforce, the behavioral adaptation remains elusive. Targeted, intensive intervention is required to mitigate this recurring internal threat and ensure consistent adherence to security protocols.

Review and Enhance Technical Phishing Defenses

• **Specific Action:** Conduct an immediate, comprehensive review and optimization of Compumacy's existing email gateway filters, endpoint detection and response (EDR) solutions, and web filtering technologies. Prioritize the deployment and enforcement of multi-factor authentication (MFA) across all critical systems where feasible, and actively explore advanced security solutions such as browser isolation or link sandboxing to act as an additional layer of defense.

• **Justification:** While the primary challenge is behavioral, the report indicates that "even our most diligent employees are still susceptible to initial phishing attempts," and the "catastrophic spike to approximately 25% in 25W38" demonstrates that human error *will* occur. Robust, multi-layered technical defenses are essential as a critical safety net and last line of defense to prevent successful breaches when human actions fail to prevent the initial click.

Implementing Recommendations with CSword

• We understand that transforming security recommendations into scalable, impactful actions can be a complex and resource-intensive undertaking for an organisation like Compumacy. Bridging the gap between identified risks and effective, sustainable solutions is precisely where CSword excels.

• **Implementing Urgent, Targeted Training for Human Resources (HR)**

• Our **AI-Powered Training Platform** can immediately deploy a mandatory, highly interactive program specifically for Compumacy's HR department. We'll leverage personalised learning paths with role-based module assignment to intensely focus on advanced phishing identification and rapid reporting protocols tailored to common HR-specific lures.

• For a deeper impact, our **Interactive Awareness Sessions** can deliver live, scenario-based workshops for HR, ensuring high engagement and practical application of "not clicking" and prompt reporting behaviours.

• Post-phishing simulations, our "Just-in-Time" micro-lessons will provide immediate, corrective feedback, directly addressing the critical reporting gap identified in the report.

• **Digital Awareness Deliverables** can provide customized infographics and short videos reinforcing HR-specific security best practices across Compumacy.

- **Revamping Cybersecurity Awareness Program to Prioritize "Think Before You Click"**

  - The **AI-Powered Training Platform** is designed to fundamentally shift Compumacy's security culture. Its adaptive content allows for frequent, shorter, scenario-based modules that emphasize "report first, then verify" and reinforce zero-click behaviours through interactive exercises.

  - We directly address the "knowledge-action gap" by providing "Just-in-Time" micro-lessons immediately after failed phishing simulations, turning moments of vulnerability into actionable learning experiences.

  - Our **Penetration Testing & Threat Simulation** capabilities include advanced phishing campaigns designed to test and reinforce the "think before you click" mindset across the entire Compumacy workforce, providing rich analytics to track this behavioural shift.

- **Conducting Specialized Training for IT Personnel**

  - Through our **AI-Powered Training Platform**, we can develop a specialised program for Compumacy's IT department, utilising custom learning paths and content that specifically address desensitization, overconfidence, and the recognition of sophisticated, targeted phishing attempts relevant to their elevated access.

  - **Interactive Awareness Sessions** can be tailored to IT, featuring scenario-based workshops that reinforce hyper-vigilance and strict adherence to protocols, fostering an environment of continuous scrutiny.

  - Our **Penetration Testing & Threat Simulation** team can design highly sophisticated, targeted attacks that challenge IT's perceived threat immunity, providing invaluable insights into their real-world responses.

- **Establishing a Program for Persistent Behavioral Non-Compliance**

  - The **AI-Powered Training Platform** provides rich analytics that allow Compumacy to identify repeat clickers across campaigns. For these individuals, we can automatically assign mandatory, individualized, in-depth coaching programs consisting of specific learning modules.

  - Our "Just-in-Time" feedback mechanism is crucial here, providing immediate, personalized corrective action after each non-compliant action.

  - For the most resistant cases, our **Interactive Awareness Sessions** can facilitate targeted one-on-one or small-group coaching, driven by the platform's data on their specific behavioral patterns and risks.

• **Reviewing and Enhancing Technical Phishing Defenses**

  • CSword's **Risk & Security Assessments** provide the immediate, comprehensive review Compumacy needs. We conduct baseline and gap analyses of your email gateway filters, EDR solutions, and web filtering technologies, identifying weaknesses and providing data-driven remediation plans.

  • Our **Penetration Testing & Threat Simulation** services can actively test the effectiveness and resilience of your multi-factor authentication (MFA) deployments and explore the efficacy of advanced solutions like browser isolation or link sandboxing, ensuring they provide a robust last line of defense.

  • Our **Data-Driven Control Reviews** provide continuous dashboard and report outputs, giving Compumacy the evidence base required to justify technical-control investments, guide tuning efforts, and ensure optimal performance of your security stack.

• Compumacy's commitment to addressing these critical findings is commendable. CSword stands ready to be your long-term partner in transforming these recommendations into demonstrable security uplift and a resilient culture. We invite you to book a tailored demo to see our platform in action or discuss a combined assessment-training engagement that directly addresses your unique challenges.

This report is prepared by Csword for Compumacy