Phishing Simulation Report

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

Table of Contents

Executive Summary

Compumacy faces a critical security paradox: while employees are increasingly aware of phishing threats and report them effectively, they often do so only *after* engaging with malicious links, leaving the organization significantly vulnerable.

- A concerning average click rate of 28% across Compumacy severely undermines a commendable 50% average reporting rate, highlighted by three repeat clickers.

- The Human Resources (HR) department is exceptionally vulnerable, exhibiting an alarming 43% click rate and a critically low 14% reporting rate, posing an immediate risk due to access to sensitive data.

- Trend analysis strikingly confirms this behavioral gap, showing the click rate surging to approximately 27% in week 25W38, even as the reporting rate simultaneously peaked at 100%.

To address this critical knowledge-action gap, immediate actions are essential: implement targeted security immersion for the HR department and overhaul organization-wide awareness training to instill a mandatory "stop-and-verify" protocol *before* any engagement with suspicious content.

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 tension in its phishing defense: while a commendable 50% average reporting rate indicates good employee awareness, this is severely undermined by a high 28% average click-through rate. This signifies that a significant portion of employees are still falling victim to simulated phishing attempts, despite potentially recognizing the threat later, exposing the organization to continued risk. The presence of 3 repeat clickers further compounds this persistent vulnerability.

- The Human Resources (HR) department is Compumacy's most critical area of vulnerability, exhibiting an alarming 43% click-through rate. Given their access to highly sensitive employee data, this represents a significant and immediate business risk that demands urgent intervention and targeted security awareness improvements.

• A clear and actionable disparity exists across departments: while the Sales team demonstrates strong security hygiene with the lowest click rate (18%) and the highest reporting rate (73%), the HR department shows the inverse, possessing the highest click rate and the lowest reporting rate (14%). This stark contrast underscores a profound need for tailored training and enhanced security protocols within HR to elevate their awareness and behavioral responses to the level of our more effective departments.

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 demonstrated the highest vulnerability with a 42.9% click rate from 7 emails sent.

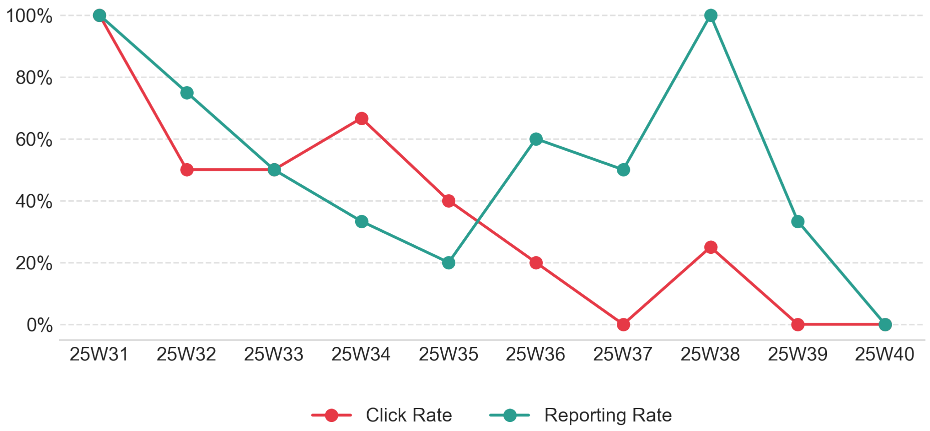
• **Top-Performing Department:** The **Sales** department showcased the strongest performance, achieving the lowest click rate at 18.2% and the highest report rate at 72.7% from 11 emails sent.

• **Diagnosing the Highest-Risk Group (HR):** The HR department's 42.9% click rate, combined with an alarmingly low 14.3% report rate, signifies a critical awareness and reporting vigilance gap. This indicates high vulnerability paired with low reporting, suggesting a profound inability to identify and respond to phishing threats effectively, posing a significant risk to Compumacy's sensitive employee data.

• **Identifying Silent Risks:** The **Finance** department, with a 27.3% click rate and a 45.5% report rate across 11 emails, presents a notable silent risk. While their click rate is moderate, their reporting vigilance is considerably lower than top-performing departments. This suggests a potential complacency where incidents might not be reported quickly, increasing Compumacy's exposure to future, more sophisticated attacks due to delayed response.

- **Contextual Exposure:** While HR's individual vulnerability is highest, the Finance department's moderate click rate across a larger volume of emails (11 emails sent, equivalent to Sales) indicates a broader potential impact if a real threat were to target this group.

Phishing Awareness Trend Analysis



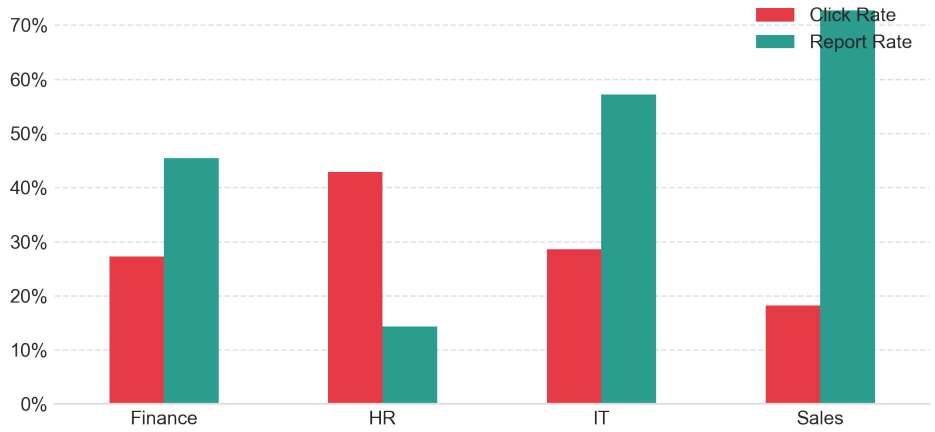
- **Compumacy faces a critical paradox:** while our employees are increasingly able to *identify* and report phishing attempts, they are often doing so *after* clicking malicious links, indicating a severe failure in behavioral avoidance despite improved awareness.

- The Reporting Rate (green line) demonstrates a generally positive underlying trajectory for employee diligence. After an initial 100% in 25W31, and a mid-period dip, it shows significant recovery, reaching peak performance again at 100% in 25W38. This indicates our awareness training is effectively fostering the ability to recognize and report suspicious activity among Compumacy personnel.

- Conversely, the Click Rate (red line) presents an alarming and volatile counter-narrative, representing direct behavioral failure and significant risk to Compumacy. After an initial 100% click rate in 25W31, and reaching a commendable 0% in 25W37, this progress was severely undermined by a catastrophic spike to approximately 27% in 25W38. This means over a quarter of employees clicked a simulated phishing link in that week, exposing Compumacy to potential breaches and data loss.

- The most critical insight from this data is the concurrent rise of both rates, especially culminating in the concerning peak in 25W38 where both the Reporting Rate and Click Rate surged significantly. This pattern reveals a fundamental flaw in our phishing awareness program: while we are successfully teaching employees how to *identify* a phishing attempt, the training is failing to instill the crucial behavior of *avoiding* the click in the first place. The result is a workforce at Compumacy that can often spot a phish and report it, but only *after* they have already engaged with the malicious content, thus potentially triggering a breach or compromising our systems before the report can be acted upon.

Group Risk Assessment Analysis



• **Highest-Risk Group Identified:** The Human Resources (HR) department at Compumacy exhibits the highest click rate at approximately 43%. This is significantly higher than other departments, being 16 percentage points higher than Finance (27%), the next highest, and 25 percentage points higher than Sales (18%), which has the lowest click rate. This makes HR our primary area of concern for phishing vulnerability.

• **Effectiveness Comparison:** While departments like Sales (approximately 68%) and IT (approximately 57%) demonstrate strong reporting diligence, HR shows a critically low report rate of only approximately 14%. This is notably lower than all other departments, with Sales reporting approximately 54 percentage points more effectively than HR.

• **Synthesized Findings & Hypothesis:**

• **HR:** The HR department presents a dual vulnerability: the highest click rate combined with the lowest report rate. This indicates a significant susceptibility to phishing attacks and a considerable gap in recognizing and reporting suspicious activity. A plausible hypothesis for this vulnerability is that HR employees may receive a high volume of emails, including many that mimic common HR-related communications (e.g., benefits, payroll, internal announcements), making it difficult to discern legitimate from malicious content. They may also feel less equipped or responsible for identifying and reporting technical security threats compared to other departments.

• **Sales:** The Sales department demonstrates exceptional performance with the lowest click rate and the highest report rate, indicating strong security awareness and proactive reporting habits.

- **IT:** The IT department shows a solid security posture with a low click rate and a high report rate, reflecting good internal security practices.

- **Finance:** The Finance department shows a moderate risk profile, with an average click rate and reasonable reporting, but still indicates an area for potential improvement.

- **Next Steps:** The data clearly indicates that the HR department requires immediate and targeted intervention. This should include enhanced, tailored cybersecurity awareness training focused on common HR-centric phishing lures and clear, easily accessible reporting mechanisms to improve their report rate and overall resilience against phishing attempts.

Key Findings & Conclusion

While Compumacy's employees demonstrate increasing awareness of phishing threats, a critical behavioral gap means they are often identifying these threats only *after* engaging with them, leaving the organization vulnerable. Our KPI analysis reveals a concerning 28% average click-through rate, which severely undermines a commendable 50% average reporting rate, a tension further compounded by the presence of three repeat clickers. This critical paradox is starkly illustrated by the trend analysis culminating in 25W38, where both the Click Rate surged to approximately 27% and the Reporting Rate peaked at 100%. This concurrent rise is definitive proof that Compumacy personnel are increasingly able to report phishes, but often only after having already clicked the malicious link, indicating a severe failure in initial behavioral avoidance. This dangerous behavioral vulnerability is exemplified by our departmental assessment, which identified the Human Resources (HR) department as a primary area of concern with an alarming 43% click rate and a critically low 14% reporting rate, highlighting a profound and immediate risk given their access to highly sensitive employee data.

This data unequivocally points to a fundamental issue for Compumacy: the challenge is not primarily a lack of *knowledge* among our employees, but rather a pervasive disconnect between recognizing a threat and consistently executing the correct *behavior* to avoid it. It is a critical knowledge-action gap. This persistent behavioral vulnerability effectively negates significant investments in security awareness training and robust technological defenses, leaving Compumacy unacceptably exposed to sophisticated phishing attacks and dramatically increasing the risk of data breaches, financial loss, and severe reputational damage.

Actionable Recommendations

Implement Targeted Security Immersion for HR Department

• **Specific Action:** Design and deliver a specialized, hands-on cybersecurity immersion program specifically for Compumacy's Human Resources department. This program must focus on common HR-centric phishing lures (e.g., benefits, payroll, internal announcements), utilize interactive simulations to practice "stop and think" behaviors *before* clicking, and establish clear, easily accessible protocols for reporting suspicious emails *without* engagement. This should include tailored scenarios to counter psychological triggers often found in HR-related phishing, along with dedicated follow-up and progress tracking for the HR team.

• **Justification:** The report unequivocally identifies the Human Resources (HR) department as Compumacy's most critical area of vulnerability, exhibiting an alarming 43% click-through rate and a critically low 14% reporting rate. Given their access to highly sensitive employee data, this represents an immediate and profound business risk that demands urgent, targeted intervention.

Revamp Organization-Wide Security Awareness with "Stop-and-Verify" Protocol

• **Specific Action:** Overhaul Compumacy's general security awareness training to fundamentally shift the focus from merely identifying threats to actively instilling a mandatory "stop-and-verify" behavioral protocol *before* any engagement with suspicious content. This includes:

• Promoting immediate internal verification for suspicious emails (e.g., contacting the sender via a known, alternative channel, *not* replying to the email).

• Emphasizing a clear "Report, Don't Click" mantra through all training.

• Utilizing frequent, short, high-quality micro-learning modules and interactive simulations specifically designed to train the *pre-click* decision-making process.

• Implementing a formal policy and mandatory re-training for repeat clickers, as identified in the report.

• **Justification:** The report highlights a critical paradox for Compumacy: while employees demonstrate increasing awareness and a commendable 50% average reporting rate, a pervasive behavioral gap means they often identify threats *after* clicking. The concurrent surge of both Click Rate and Reporting Rate (especially to 100% in 25W38) is definitive proof that current training fails to instill the crucial behavior of *avoiding* the click in the first place, exposing Compumacy despite improved awareness. Addressing the 3 repeat clickers is also critical to mitigate persistent vulnerability.

Conduct Comprehensive Review and Enhancement of Email Security Gateways

- **Specific Action:** Initiate an immediate, comprehensive review of Compumacy's existing email security gateway solutions, endpoint protection, and advanced threat detection systems. Prioritize the implementation or enhancement of technologies that can proactively block sophisticated phishing attempts, malicious attachments, and credential harvesting sites *before* they reach end-users' inboxes, or prevent execution even if a user bypasses behavioral controls and clicks. This includes advanced URL sandboxing, attachment analysis, and AI-driven threat intelligence.

- **Justification:** The report shows that despite awareness efforts, human error persists, evidenced by a concerning 28% average click-through rate, a "catastrophic spike to approximately 27% in 25W38," and an initial 100% click rate in 25W31. These statistics underscore that accidental clicks are an ongoing risk. Robust technical defenses are essential as a critical safety net to prevent data breaches and financial loss when behavioral defenses fail, thereby effectively negating the impact of accidental clicks and supplementing security awareness investments.

Implementing Recommendations with CSword

- We understand that translating security report recommendations into actionable, scalable solutions can often be complex and resource-intensive for organisations like Compumacy. CSword is uniquely positioned to help you bridge these gaps efficiently and effectively.

- **Addressing Recommendation 1: Implement Targeted Security Immersion for HR Department**

  - Our **AI-Powered Training Platform** can immediately create a customised, highly relevant learning path for Compumacy's HR department. This includes specific modules on HR-centric phishing lures, adaptive content that responds to their progress, and “Just-in-Time” micro-lessons delivered immediately after simulated incidents to reinforce "stop and think" behaviors.

  - For deeper engagement, our **Interactive Awareness Sessions** offer live, scenario-based workshops tailored for high-risk groups like HR, allowing them to practice identifying and reporting suspicious content in a controlled environment.

  - **Digital Awareness Deliverables** can be deployed to create customised videos and infographics reinforcing clear reporting protocols without engagement, ensuring consistent messaging across the department.

  - The platform’s **rich analytics** will provide detailed progress tracking and prove the behavioural change within the HR team, offering the data needed for accountability and continuous improvement.

- **Addressing Recommendation 2: Revamp Organization-Wide Security Awareness with "Stop-and-Verify" Protocol**

    - The **AI-Powered Training Platform** is designed to fundamentally shift user behavior. Through personalised learning paths and adaptive content, we can instil Compumacy's "stop-and-verify" protocol across the entire organisation.

    - Our “Just-in-Time” micro-lessons, delivered immediately after failed phishing simulations, are critical for closing the behavioral gap by reinforcing the crucial *pre-click* decision-making process and emphasizing the "Report, Don't Click" mantra.

    - The platform's ability to assign custom learning paths and modules allows us to implement mandatory re-training for repeat clickers, addressing the persistent vulnerability identified in the report with targeted interventions.

    - Complementary **Digital Awareness Deliverables** such as bespoke infographics and short videos can be used to promote the "stop-and-verify" protocol and internal verification methods consistently across all channels at Compumacy.

- **Addressing Recommendation 3: Conduct Comprehensive Review and Enhancement of Email Security Gateways**

    - CSword's **Risk & Security Assessments** provide the baseline and gap analyses necessary for a comprehensive review of Compumacy's existing email security gateways, endpoint protection, and advanced threat detection systems. This quantifies your current posture and feeds data directly into remediation plans.

    - Our **Penetration Testing & Threat Simulation** services can actively identify exploitable weaknesses in your current technical controls, validating their effectiveness against sophisticated phishing, malicious attachments, and credential harvesting attempts *before* attackers do. This provides actionable insights for enhancement.

    - The findings from these assessments and tests feed directly into our **Data-Driven Control Reviews**. Our dashboard and report outputs provide the evidence base to justify technical-control investments and guide tuning efforts, ensuring that accidental clicks are mitigated by robust technical defenses, thereby enhancing your overall security posture and complementing your human awareness investments.

- CSword is uniquely positioned to be Compumacy's long-term partner in building a truly resilient security culture, combining cutting-edge technology with expert services. We invite you to book a tailored demonstration of our AI-Powered Training Platform, or discuss a combined assessment-and-training engagement to proactively address these critical findings.

This report is prepared by Csword for Compumacy

ORIGINAL

★★★

ORIGINAL

★★★

ORIGINAL