Cybersecurity Training & Phishing Performance Summary

Reporting Period: September 2024 – September 2025

Summary

Despite extending the deadline for annual cybersecurity training from the original one month to three months, only 77% of employees completed the training on time. The remaining employees only finished after repeated and significant follow-up efforts. This highlights a concerning lack of urgency toward compliance.

The phishing simulation results are equally concerning. With an employee-based phishing rate of 13.3% and an email-based phishing rate of 23.65%, the City's results fall short of industry standards of 16% overall. This level of susceptibility presents a serious risk to the City's cybersecurity posture.

Phishing Simulation Performance

- Phishing Email Rate (by emails sent): 23.65% of simulated phishing emails were clicked.
- Phishing Employee Rate (by unique employees): 13.3% of employees clicked at least one phishing email.

The difference between these statistics is critical:

- The 23.65% represents the percentage of all emails sent that were clicked.
- The 13.3% represents the percentage of employees who fell for a phishing attempt.

Since multiple emails were sent to each user, the email-based rate appears roughly double the employee-based rate.

Cybersecurity Training Performance

- Overall Completion Rate: 99.8% of employees enrolled in Annual Compliance Training completed the course.
- On-Time Completion Rate: 77% completed by the adjusted due date.

It is important to note that the 77% on-time completion rate is inflated by the extended deadline. The original expectation was one month, but the window was increased to three months to accommodate delays. Even with this extended period, nearly one-quarter of employees still failed to meet the deadline without direct intervention and repeated follow-ups.

Recommendations

1. Reinstate a 1-month training deadline to reinforce accountability.
2. Transition to monthly cybersecurity training to strengthen awareness and habits.

3. Secure department head sponsorship to emphasize cybersecurity as a core organizational priority.

Conclusion

The City achieved broad participation in cybersecurity training but demonstrated weak on-time compliance, even after deadline extensions. Phishing results are poor by industry standards and represent an ongoing risk. City leadership should view these outcomes as evidence that stronger accountability, more frequent training, and a reinforced reporting culture are essential for improving the City’s cybersecurity posture.