

Aerken (Alex) Alikamaer, MSc eHealth; Amama Khairzad, MSc eHealth; Debbie Martino, RN, BScN, CAPM; Kevin Fernandes; Peter Bak, Ph.D.

DESCRIPTION

As cyber threats evolve, healthcare organizations have become increasingly vulnerable to breaches. Humber River Health (HRH) recognized the need for an integrated training approach. The Digital Learning Team (DLT) took on the role to design and maintain a structured cybersecurity awareness program focusing on simulated phishing campaigns following the guidelines from the Local Delivery Groups (LDG) and informative cybersecurity awareness newsletters. This initiative ensures that staff receive ongoing education tailored to real-world threats, such as digital, attachment, and data entry phishing, improving their vigilance against cyber risks. By tracking engagement and results, the program has transformed cybersecurity awareness into a proactive, measurable, and organization-wide responsibility.

OBJECTIVE

To strengthen cybersecurity awareness through phishing simulations and newsletters promoting safe practices and cyber hygiene.

ACTIONS TAKEN

DLT launched quarterly phishing campaigns to evaluate staff awareness and response to suspicious emails, such as lookalike Microsoft, SharePoint, and other email templates. Each campaign followed the LDG guidelines to ensure the data reported to Ministry of Health is accurate and appropriate. The staff who clicked were enrolled in cybersecurity modules that are tailored to the theme of the phishing campaign to enable phished staff to recognize and learn about the real threats. Concurrently, weekly (October 2022 – October 2023) and biweekly (March 2023 – present) newsletters were introduced to share practical cybersecurity tips, highlighted recent phishing trends, and shared prevention strategies.

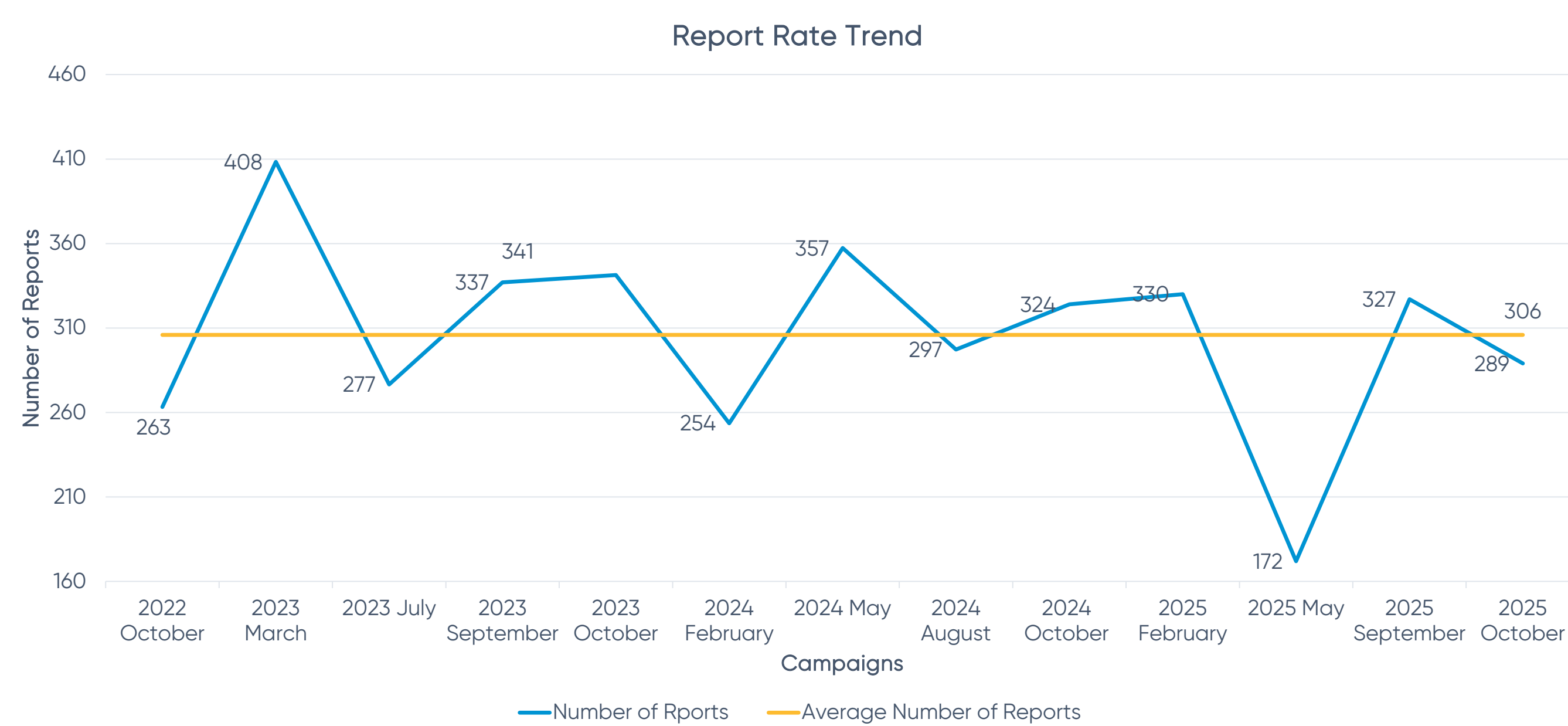


Figure 1. The average report rate from the first phishing campaign (October 2022) to the most recent campaign (October 2025) (Average N=1598)

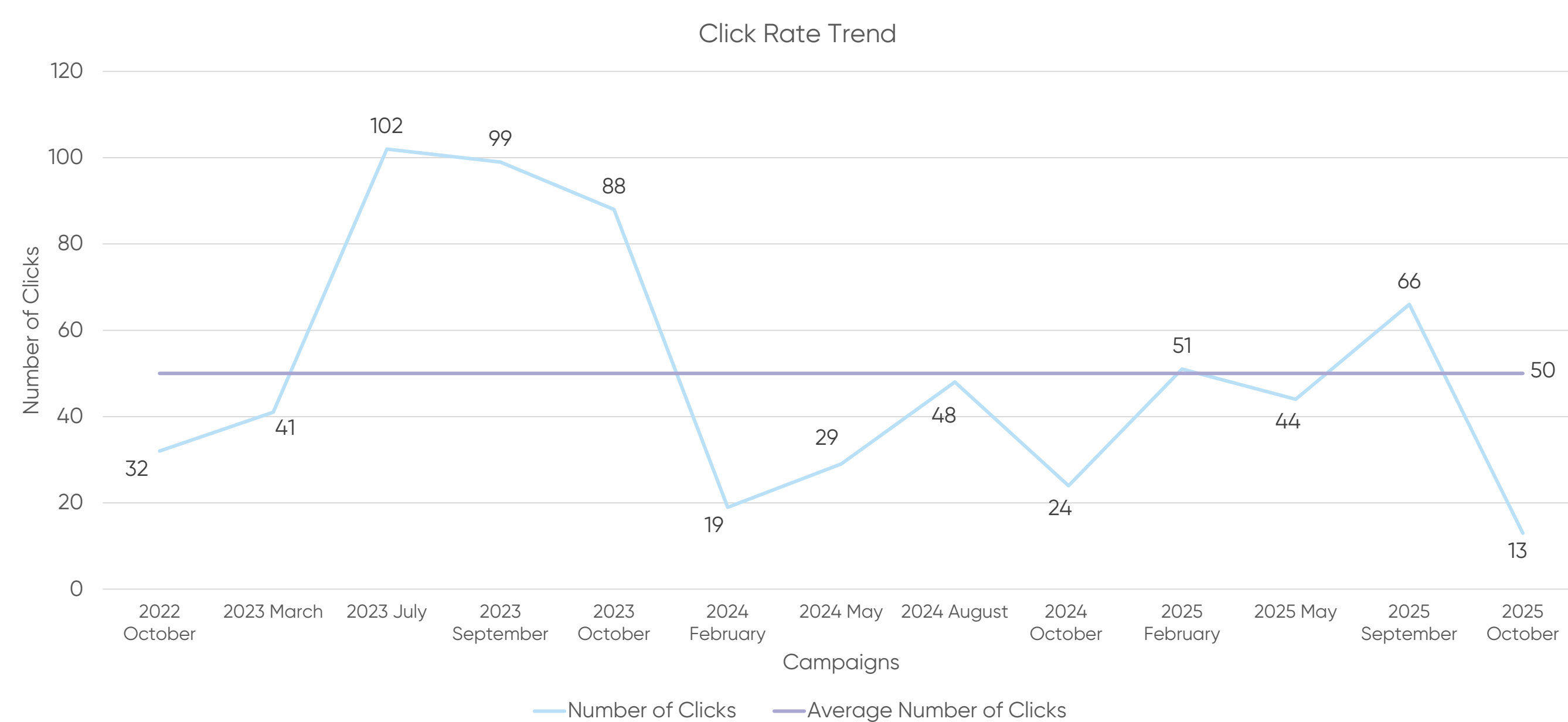


Figure 2. The average click rate from the first phishing campaign (October 2022) to the most recent campaign (October 2025) (Average N=1598)

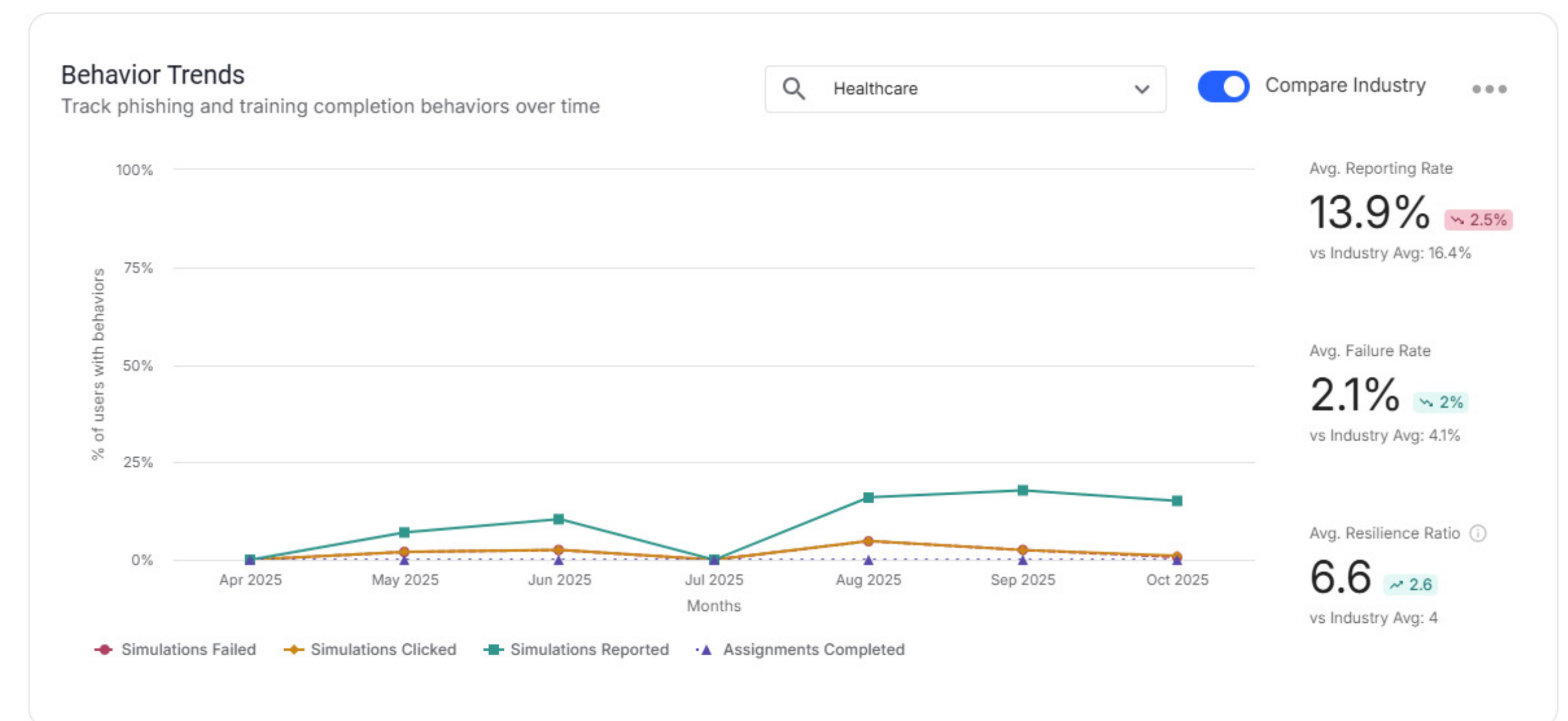


Figure 3. The comparison of HRH's average reporting rate, average Failure rate, and average Resilience Ratio with Industry (Healthcare) average data (As of Oct. 22nd, 2025)

SUMMARY OF RESULTS

Phishing campaign data since October 2022 revealed fluctuations in report and click rates, influenced by the simulation complexity and timing. The average click rate initially increased drastically as more challenging templates were introduced, but demonstrated an overall downward trend, indicating improved user awareness and vigilance. HRH's reporting average is 2.5% lower, average simulation failure rate is 2% lower, and resilience ratio is 2.6% higher than the healthcare industry average. These results demonstrate strong progress, while highlighting opportunities to further improve staff awareness and reporting of suspicious emails.

LESSONS LEARNED

Consistent phishing exercises foster staff awareness. Outcome variability suggests progressive learning, reinforcing the need for diverse, ongoing cybersecurity training strategies.

