MIDDLESEX-LONDON HEALTH UNIT

REPORT NO. 06-22FFC

TO: Chair and Members of the Finance and Facilities Committee

FROM: Emily Williams, Chief Executive Officer

DATE: 2022 April 7

CYBER SECURITY TRAINING

Recommendation

That the Finance & Facilities Committee recommend to the Board of Health to receive Report No. 06-22FFC, re: Cyber Security Training for information.

Key Points

- In early 2022 the MLHU Information Technology team offered two Cyber Security training sessions to all MLHU staff, as well as conducted two Cyber Security tests.
- Training sessions include three-to-four-minute videos on varying Cyber Security subjects with a short questionnaire at the end. The first training session was selected to counter the real time threats that have been seen with increased frequency at MLHU in recent months. Starting with "Introduction to Phishing" and then "CEO Scams", training sessions were provided to all staff with a completion rate of 32% on the first training and currently 22% on the second. Both sessions remain open and can still be actioned by staff.
- The Cyberthreat tests come in varying degrees of difficulty and the first test was ranked at medium difficulty. It showed a higher-than-expected result of 24% (258) of staff using the link and 17% (189) providing their credentials to the fake site. The second test, being a lower degree of difficulty, showed an expected result of 12% (131) following the link and 2% (25) providing credentials. Training sessions were offered after the first test was completed and prior to the second test being administered.

Background

This report provides an update on the status of the MLHU Cyber Security Training and Testing efforts. In 2021 a gap in the Cyber Protection was noted and a Cyber training/testing option was selected to counter this challenge. An initial test was completed to determine the overall level of Cyber awareness at the health unit, comprised of a fake email tailored to the environment, with various ways of having staff click an item, provide data, or give username/password. The test was ranked at medium difficulty and demonstrated a concerning result with 24% (258) of staff clicking on the link and 17% (189) providing their credentials to the fake site. Following this baseline result, Cyber training was introduced as highly recommended but voluntary for staff. It was followed with repeat testing which, although ranked at a lower level of difficulty, produced improved results with 12% (131) following the link and 2% (25) providing credentials.

Next Steps

Currently the IT team is in the early stages of Cyber training/testing at MLHU. Staff education is a key defense against Cyber-attacks, and the IT team will continue to send out monthly training and tests to MLHU staff that cover various threats. Given the importance of this training, as well as the dependence on it to ensure ongoing Cybersecurity insurance coverage for the health unit, the IT team will be recommending to Senior Leadership that four key modules of the training become mandatory for all staff, with the training spread throughout the year.

This report was prepared by the Manager of Information Technology, Healthy Organization Division.

EWilliams

Emily Williams, BScN, RN, MBA, CHE
Chief Executive Officer