SPAM & Maintenance Plan (TLDR)

March 6, 2025

TLDR (Too Long; Didn't Read)

The newsletters will now include a new section: TLDR (Too Long; Didn’t Read). This will be a short summary of the newsletter, providing key points in a brief format for readers who may not have time to read the full article.

Key points:

- Add SPAM emails to Barracuda SPAM filter to block on your own
- Quarantined phishing emails in Barracuda do not need to be reported to the Help Desk
- To boost cybersecurity on campus, MCC will implement a regular maintenance plan

TLDR END

SPAM

We often receive SPAM (unwanted email) daily. McLennan Community College (MCC) utilizes Barracuda to filter and block SPAM (or phishing) emails. Sometimes, SPAM still gets through. Did you know you are able to block SPAM on your own? For details on how to block, see: IT Hub: Block SPAM article.

Quarantined Phishing Emails

Reporting phishing emails is important to help protect the MCC community from potential harmful content, files, and data leakage. Barracuda is set up to filter incoming/outgoing emails and block suspicious content.

Recently, a phishing email circulated appearing to be from the Chief of Human Resources (HR), Missy Kittner. Some individuals received the email in their inbox and reported the email as phishing to the Help Desk (thank you). Once the email was triggered as phishing, Barracuda began to block the additional emails as ‘Quarantined’.

If a phishing email is quarantined, in Barracuda, you DO NOT need to deliver the email to your inbox to report as phishing to the Help Desk. In this case, Barracuda did its job. The Help Desk will work with the ISS team to purge all the phishing emails from everyone who received this email in their inbox.

Maintenance Plan

MCC will soon implement a regular maintenance schedule for specific applications/systems used at the college. The schedule will be published on the MCC website: Information Systems and Services (ISS) under Maintenance. Why are updates important? As mentioned in a 2023 Cybersecurity Awareness Month Newsletter, software updates are one of the easiest ways to boost cybersecurity.

Developers are constantly looking for clues cybercriminals are trying to break into their systems. To fix these issues and improve security, software companies release routine updates. These are important to protect against potential vulnerabilities and threats, ensure compliance and reduce legal risks, optimize performance, add new features and enhancements, address any bugs or errors, and prevent costly repairs by addressing issues before they escalate.

Revision #1
Created 2 April 2025 13:27:20 by Laura J. Crapps
Updated 2 April 2025 13:32:31 by Laura J. Crapps