KNOWN ISSUE

Phishing Exploits: False Blackboard Emails

TEACHING LEARNING COMMUNITY | **Faculty Support eLearning**

MATC's IT Department has become aware of phishing scams sending imposter Blackboard emails to MATC faculty and students. The phishing emails are designed to trick you into sharing your MATC network username and password.

If you receive emails similar to the following examples, *do not* reply to the sender and *do not* click on any links provided in the message. ***Do* delete the message**.

EXAMPLE PHISHING EMAILS

> Hello,
>
> We detected something unusual about a recent sign-in to your Blackboard account. For example, you might be signing in from a new location, device or app.
>
> To help keep you safe, we've blocked access to your inbox, contacts list and calendar for that sign-in. Please review your recent activity and we'll help you take correct action. To regain access, you'll need to confirm your identity."
>
> http://uki.blackboard.com/international/globalmaster/TGXUOXWL%&!@#83Access
>
> Thanks,
> Blackboard Administrative.

> *Good Morning,*
>
> *Your school has posted an important information regarding a course for you. You are required to immediately sign in to Blackboard Learn.*
>
> *Click here to sign in to Blackboard Learn*
>
> *Thank you.*
>
> *Blackboard Learn Notifications.*

How to Identify Real Email Notifications Sent by MATC's Blackboard System

- MATC's Blackboard *never* sends email messages that request you to share your login credentials. Emails from MATC's Blackboard *never* require you to log into Blackboard to read announcements. The email messages will contain the announcement content.

- Review the sender's email address and signature. Email sent from MATC's Blackboard system may come from the following addresses: do-not-reply-blackboard@matc.edu; bbsupport@matc.edu; distancelearning@matc.edu; and do-not-reply@learn-prod-5744b9beb8ccb-197933737.us-east-1.elb.amazonaws.com.

- MATC's Blackboard system can be accessed by going to these URL web addresses only: blackboard.matc.edu; mymatc.matc.edu.

- Phishing emails often contain misspelled words, strange phrases, and urgent warnings to prompt you for personal information. These emails often contain disguised web links that connect to malicious websites or programs. By rolling your mouse over a link in the message, you can review the real web address behind the link; the link's real web address will often bear no resemblance to a legitimate website, as shown below.