TO: ALL MTA EMPLOYEES

In light of the COVID-19 Coronavirus, malicious attackers and hackers are using this situation to send out fake news and links.

DO NOT OPEN OR FORWARD emails with attachments or links from sources that are not known. This includes forwarded emails from trusted people! Sharing information may seem to be helpful to others, but unless it is provided by a known MTA email account, the information must be considered as unreliable (Fake News or a Hoax). In these cases, you must assume that the email contains unsafe attachments or links that can cause harm.

It is a best practice to exercise CAUTION when you receive e-mails with links and attachments to other websites!

DO NOT OPEN any attachments or click on links from unknown sources as they may have misinformation or malicious links that can hijack your device.

REPORT suspicious emails that contain attachments or links to MTA Cybersecurity by using the “Report Phishing” button in your outlook client.

As MTA Cybersecurity discovers these attachments and links, we update our defenses to neutralize threats.

ALWAYS receive your information directly from reputable sources such as the MTA, The Centers for Disease Control (CDC.gov), or news outlets and websites of your choice.

OUR EMPLOYEES AND BUSINESS PARTNERS ARE THE FIRST LINES OF DEFENSE FOR ANY CYBERATTACKS!

Cybersecurity is everyone’s responsibility and the MTA needs you to be vigilant at all times! Please reinforce this with your co-workers and family and encourage everyone to stay healthy and cyber-safe.

Thank you,

Cybersecurity Team

MTA IT Service First