UNIVERSITY HOSPITAL
Newark, New Jersey

PHISHING ATTEMPT THREAT!
"NEW UPDATE"

April 24, 2017

Dear UH Employees,

Phishing is a fraudulent process used by spammers to acquire sensitive information from users such as usernames, passwords, and credit card details. Email recipients are often deceived by phishing attempts since messages appear to be sent by legitimate and trustworthy sources.

Today we've learned of a phishing attack at UH that attempts to draw the attention of recipients with the subject line "NEW UPDATE." Here is what the email looks like.

From: "Infante-Rios, Ana" <ainfanterios@paterson.k12.nj.us>
Date: April 23, 2017 at 5:08:10 AM EDT
To: "info@paterson.k12.nj.us" <info@paterson.k12.nj.us>
Subject: NEW UPDATE

Letter to Staff **CLICK HERE** now to Update e-mail

If you receive this, **DO NOT CLICK ON THE LINK.** The link brings you to a site (which should be blocked now) where you are prompted to enter your user name and password and "domain". Doing so would compromise your user name and password.

NOTE: The Information Systems and Technology Department (IST) of University Hospital will never send an email requesting employees to update their account. Nor will they threaten to block their email. Recipients of this message should delete immediately or forward to Spam Prevention at spam@ca.rutgers.edu.

Recipients who responded to the email should contact the IST Helpdesk immediately at 732-743-3200. Our email traffic is filtered, which provides you with protection against dangerous viruses and spam. However, some spam may occasionally get through to your inbox or be diverted to your End User Digest, so please use caution.

Your cooperation continues to assist the Office of Ethics & Compliance (OEC) and Information Systems & Technology (IST) in maintaining a secure environment.

Cyber Criminals are Phishing. Don't Get Caught!