From: NJCCIC <njccic@cyber.nj.gov>
Sent: Tuesday, May 05, 2020 1:02 PM
To: [redacted]
Subject: NJCCIC Alert | Credential Phishing Campaign Targets NJ Education Sector

NJCCIC
New Jersey Cybersecurity & Communications Integration Cell

NJCCIC Alert

Credential Phishing Campaign Targets NJ Education Sector

TLP: GREEN

May 5, 2020

NJCCIC Education Sector Members,

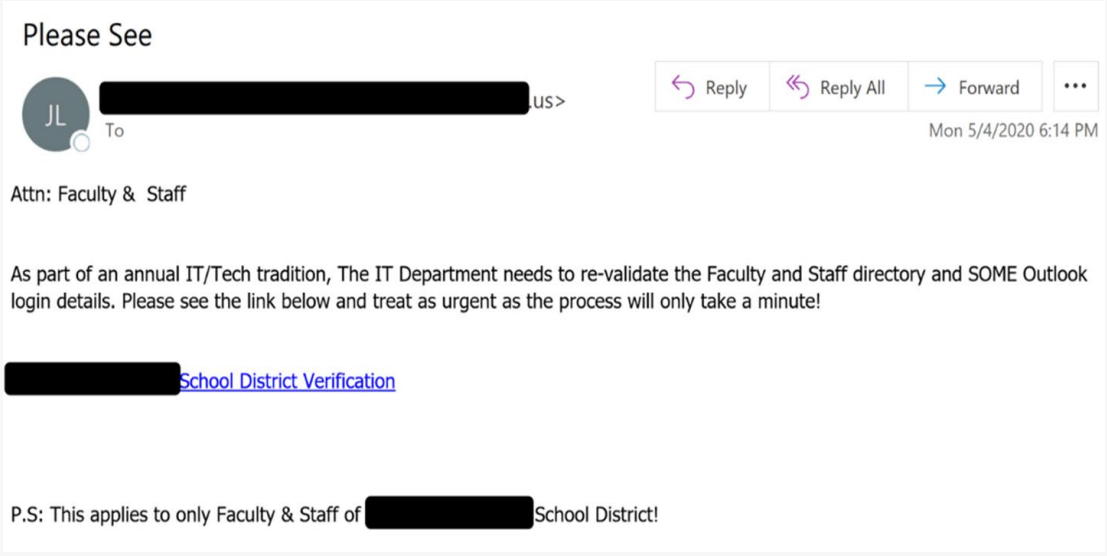
This NJCCIC Alert is being provided to assist agencies and organizations in the protection against cyber threats.

Summary

The NJCCIC has received reports of an ongoing credential phishing campaign in which individuals are impersonated via seemingly-compromised education sector email accounts (those ending in .edu). The emails, which have been sent to multiple New Jersey education sector individuals, contain subject lines that attempt to convey a sense of urgency and invite the recipient to take immediate action by clicking on a link to re-validate Microsoft Outlook login details. If clicked, this link will direct the recipient to a webpage requesting

their Microsoft Outlook login credentials. If the user submits their credentials, they are sent to the threat actors behind the phishing campaign. The NJCCIC suspects that the compromised user credentials are used, in part, to perpetuate this phishing campaign, allowing the emails to be sent from legitimate education sector accounts to decrease suspicion.

Below is an example of a phishing email received by a NJ education sector user. This is meant to serve only as an example, as emails delivered with this or other phishing campaign may include different content.



Recommendations

The NJCCIC recommends educating education sector users about this phishing threat, reminding them never to click on links or open attachments delivered in unexpected or unsolicited emails, and exercise caution with emails from known senders. If you are unsure of an email's legitimacy, contact the sender via a separate means of communication. The NJCCIC recommends only entering account credentials into websites navigated to directly, not via links delivered in emails. Users are advised to run

updated anti-virus/anti-malware programs on all devices and enable multi-factor authentication where available to prevent account compromise as a result of credential theft.

Reporting

The NJCCIC encourages recipients who discover signs of malicious cyber activity to contact the NJCCIC via the cyber incident report form at www.cyber.nj.gov/report.

Please do not hesitate to contact the NJCCIC at njccic@cyber.nj.gov with any questions. Also, for more background on our recent cybersecurity efforts please visit cyber.nj.gov.

The information contained in this product is marked Traffic Light Protocol (TLP): GREEN. The information can be shared with trusted peers and partner organizations within your sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing internet websites, or transmitted over non-secure, external communications channels.

TLP: GREEN

New Jersey Cybersecurity & Communications Integration Cell
24/7 Incident Reporting: 1.866.4.SAFE.NJ
General Inquiries: 1.833.4.NJCCIC

Connect With Us

Forward Notification

This email was sent by:

New Jersey Cybersecurity & Communications Integration Cell