The New York State Intelligence Center Cyber Analysis Unit (NYSIC CAU) has become aware of the following information. NYSIC-CAU will continue to provide updates as necessary.

Overview: The New York State Intelligence Center Cyber Analysis Unit is aware of two separate incidents occurring in late 2018 and the first half of 2019 whereby numerous employees of local governments (county, city, town, etc.) within New York State received a phishing email. The email in question which appeared to come from the "Help Desk" requested employees click on a link provided to update email account information. The link in fact contained a credential harvester; when the victim provided their information the malicious actor used the credentials to take control of victims' payroll accounts. Thus, diverting payroll deposits to the malicious actors bank accounts. A credential harvester is a fake web application designed to mimic official business wherein malicious actors collect usernames and passwords from victims.

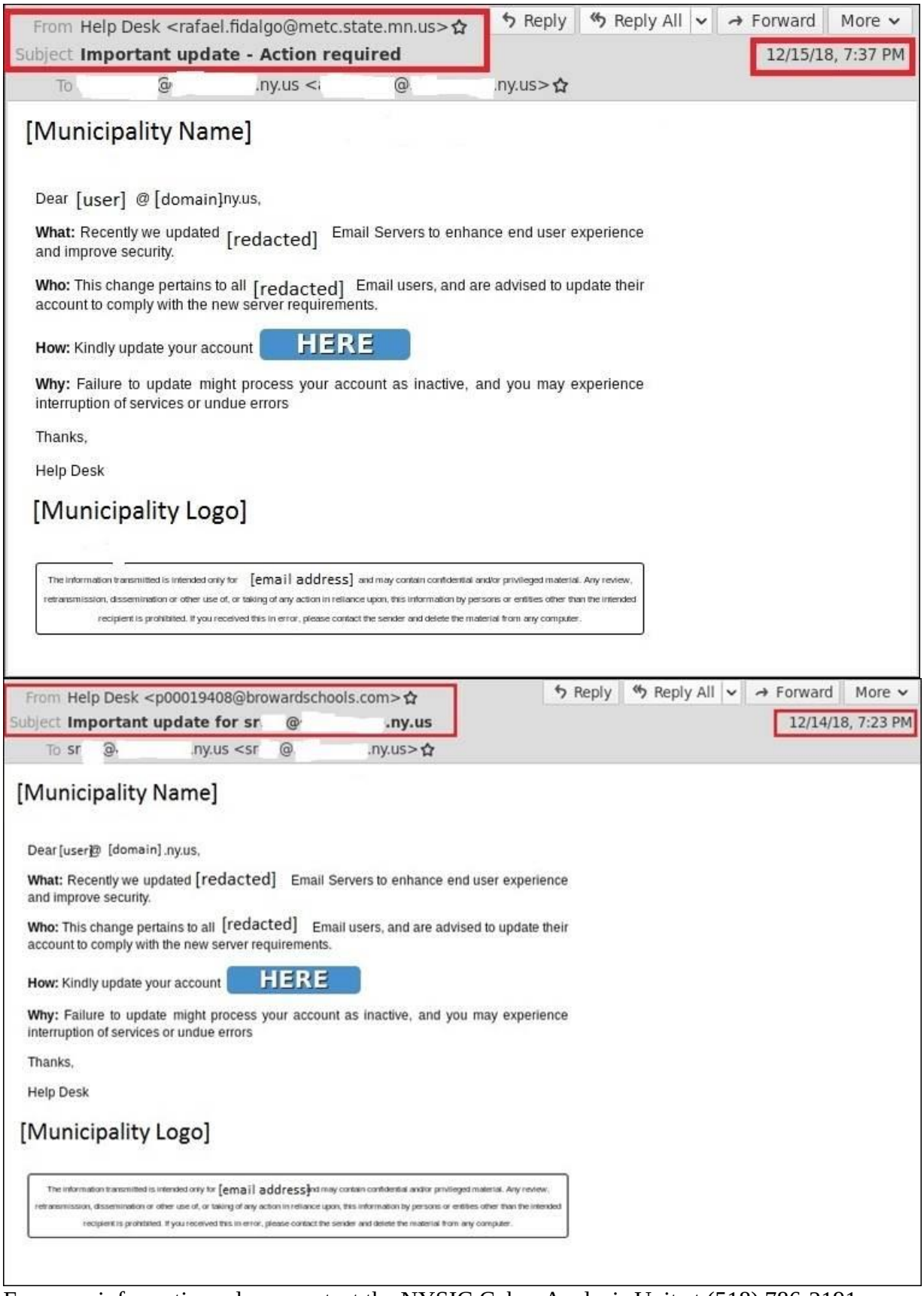
A review of the emails show they contain a similar format, wording, and appear to be from an official source. The emails contained the following subject lines, "Important update – Action required" or "Important update for [employee/victim email address]". The emails explained a supposed system upgrade which would require the victim to login utilizing the provided link detailed in a large box colored blue with white letters and spelling out the word HERE (See below imagery). The email goes on to note that a non-response would result in accounts to become inactive. The email is signed to purportedly represent a government entity's help desk while utilizing the appropriate branding from that agency. The bottom of the email body contains official instructions detailing proper usage and handling.

NYSIC-CAU recommends sharing this situational report as part of any information assurance training.

Analyst Note: The following indicators should be utilized to identify the possibility of a phishing campaign:

- The From: line of one of the emails appears to be from a different state as the recipient yet claims to be from a local municipality.
- The From: line of one of the emails is from a domain indicative of a school district while claiming to be from a local municipality.
- The To: line shows the recipients full email address rather than name which indicates the email may be from outside the network.
- Email date and time stamp are outside of typical business hours.
- Email is addressed "Dear (entire email address of recipient)".
- The link in the email to update ones information when hovered over clearly shows a website link to Outlook Web Access (OWA) which is a remote way to access email outside a network

Below are images of the emails along with suspicious indicators highlighted:



For more information, please contact the NYSIC Cyber Analysis Unit at (518) 786-2191 or CAU@nysic.ny.gov.