This pass thru guidance is being sent to local government users on behalf of Karen Sorady, Acting Chief Information Security Officer

The New York State Office of Information Technology Services (ITS) would like to remind users that malicious actors will use the coronavirus (COVID-19) pandemic to deliver malware, to steal money and/or personal information, or to spy on you through your smartphone's features. We ask that users remain vigilant to COVID-19 related scams.

As a state with one of the highest rates of COVID-19 infections, New York is seeing a significant spike in coronavirus scams. These scams are coming in the form of malicious websites, text messages, phone calls, and phishing emails that are being used to infect user's machines with malware or to defraud the user. Recent examples include:

- Fake coronavirus-based websites, such as corona-virus-map[.]com, coronavirus[.]app, and vaccine-coronavirus[.]com.
- Phishing emails claiming to be from the Centers for Disease Control and Prevention (CDC) and other reputable organizations offering information on the virus in links or attachments.
- Phishing emails asking users to verify their personal and financial information for charitable contributions or to receive coronavirus-related benefits, such as economic stimulus checks, airline carrier refunds, or general financial relief.
- Fake text messages offering information on the virus or resources related to coronavirus relief, such as iPhones, payday loans, or counterfeit virus treatments.
- Illegal robocalls pitching fake treatments or work-at-home schemes.

We recommend that users take the following precautions to protect themselves:

- Use trusted sources, such as legitimate government websites, for up-to-date, fact based information about COVID-19. Check for misspellings within a link - for example, an address that should end with .gov ending in .com or .org instead. (Note, the World Health Organization uses a .int domain.)
- Exercise extreme caution when responding to individual pleas for financial assistance such as those posted on social media, crowd funding websites, or in an email, even if it appears to originate from a trusted source.
- Be cautious of emails or websites that claim to provide information, pictures and/or videos.
- Do not open unsolicited emails or click on the links or attachments in those emails.
- Never reveal personal or financial information in an email or to an untrusted website.
- Hang up on robocalls. Do not press any numbers.

For additional information, please visit https://coronavirus.health.ny.gov/stay-cyber-safe.

If you have questions regarding this email, or need further assistance, please contact the Division of Homeland Security Cyber Incident Response Team at CIRT@DHSES.ny.gov.

As always, thank you for your continued cyber security awareness and vigilance.