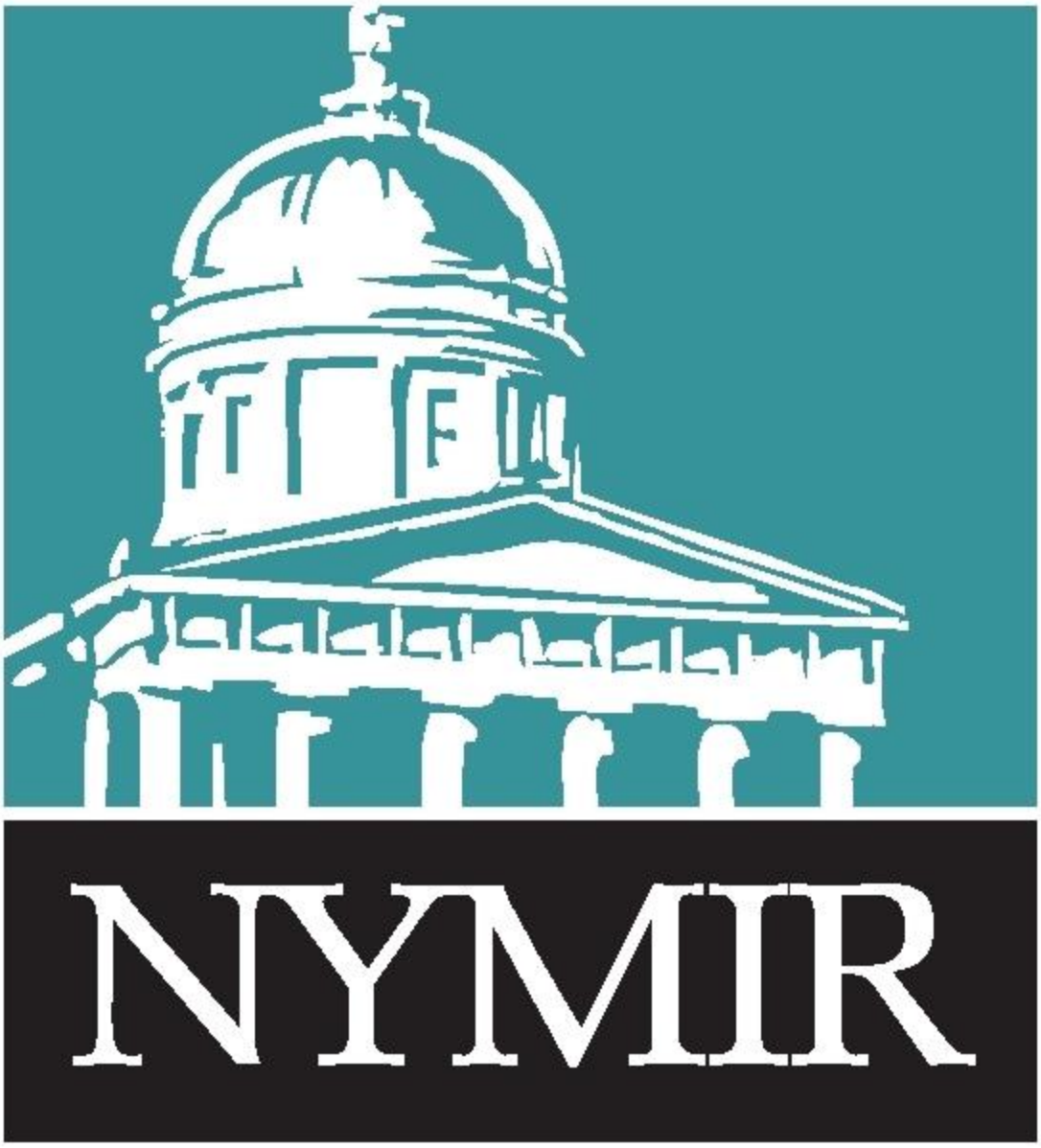
All it takes is one wrong click!

NYMIR WARNING



April 24,2020

Phishing Attempts Continue to Increase with COVID-19

Phishing campaigns are often built around major events and take advantage of breaking news stories. THE COVID-19 pandemic has enforced this fact. Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in an email. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.

Deceptive phishing is popular with cybercriminals, because it's so much easier to trick someone into clicking a malicious link, through what you think is a legitimate email than it is to break through a computer's defenses.

How phishing works

Cyber criminals typically use public sources of information, including social networks like LinkedIn, Facebook and Twitter, to gather background information about the victim's personal and work history, interests and activities.

These pre-phishing attacks uncover names, job titles and email addresses of potential victims, as well as information about their colleagues and the names of key employees in their organizations. This information can then be used to craft a believable email. Targeted attacks, including those carried out by threat actors who gain unauthorized access to a computer network and remain undetected for an extended period of time.

Although many phishing emails are poorly written and clearly fake, cybercriminal groups increasingly use Facebook posts that generate the most likes.

Typically, a victim receives a message that appears to have been sent by a known contact or organization. The attack is carried out either through a malicious file attachment that wreaks havoc on your entire computer system. Their objective is to install malware on your device (which infects the entire computer system of your municipality) or direct the victim to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details to name a few.

How to recognize a phishing email

Successful phishing messages, usually represented as being from a well-known company, are difficult to distinguish from authentic messages. A phishing email can include corporate logos and other identifying graphics and data collected from the company being misrepresented. Malicious links within phishing messages are usually also designed to make it appear as though they go to the masqueraded organization. However, here are top clues that can indicate that a message is a phishing attempt:

- The message uses subdomains, misspelled URLs or typosquatting and otherwise suspicious URLs. (Typosquatting, also called URL hijacking, or a fake URL, which relies on mistakes such as typos made by Internet users when inputting a website address into a web browser.
- The recipient uses a Gmail or other public email address rather than a corporate email address.
- The message is written to invoke fear or a sense of urgency.
- The message includes a request to verify personal information, such as financial details or a password.
- The message is poorly written and has spelling and grammatical errors.