Advisory
New York State Department of Health
October 28, 2020

The New York State Department of Health (NYSDOH) is aware of three (3) ransomware attacks occurring over the last two weeks that have impacted a healthcare system and two of its hospitals, another distinct hospital, a local health department and its county-operated adult care facility. Phishing email has been identified as the source of attack in at least one of these incidents and is suspect in the others. As health care is currently the most targeted sector for phishing attacks, the NYSDOH would like to encourage healthcare organizations to maintain awareness of increasing cyber security threats, including those that come in the form of phishing emails.

While phishing emails can be difficult to identify, awareness and vigilance on the part of all staff in examining emails can greatly reduce the risk that your organization will fall prey to such an attack.

Ongoing staff education is essential. The Department of Health and Human Services (HHS) has compiled excellent webinars, videos and posters that can assist you in building your staff's awareness of this issue, available at: (https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx).

The following common indicators of phishing and general recommendations may help your staff to evaluate email messages before choosing how to proceed:

Common Indicators of phishing email may include the following:

- Email received from an unexpected source.
- Mismatched email sender name and email address.
- Suspicious attachments.
- Poor grammar or punctuation.
- Links that don't look right or that show differently once the mouse is used to hover over the link.

General user recommendations:

- Refrain from accessing personal email (e.g., Gmail, Yahoo) and/or social media. applications from healthcare system.
- Be wary of unsolicited emails, even if the sender appears to be known.
- Use caution with email links and attachments without authenticating with the sender.
- Avoid clicking directly on website links in emails; type the address into your browser.
- Keep browser and virus protection software in most current versions.
- Educate yourself on how to protect yourself from phishing.

Make sure staff are aware of your organization's policies and procedures for dealing with emails they believe are potentially harmful. The attached HHS poster is a quick way to provide important reminders.

We appreciate your continued attention to cyber security best practices.

10 WAYS TO PROTECT YOUR PATIENTS FROM CYBER THREATS

Cyber-attacks are on the rise in the healthcare industry and it is up to all of us to keep our patients safe. Being cyber-prepared is everyone's responsibility, and to get started, check out the below ten best practices to ensure you are keeping your patients safe!

Report suspicious emails. This is the number one way bad actors get access to patient information.

Always ensure to protect your computer, phone and any other connected technology. – Loss of equipment or data is one of the top five cybersecurity threats to the healthcare industry.

Use strong passwords and keep them secure. Weak or default passwords leave your patients' data and safety at risk.

Always ensure you are protecting your patient's data by using encryption and get to know your organization's policies when accessing and transmitting sensitive data.

Always keep your organization informed on the IT assets you possess and purchase, including computers, phones, tablets, and any other devices.

Be sure to keep all of your technology assets up to date by by following your organization's policies on software updates and virus protection software.

Be very careful when accessing your organization's network from a remote location. Hackers frequently intercept open Wi-Fi networks, which could leave your organization's networks at risk.

Practice cyber vigilance by knowing your organization's process for reporting suspicious activity or known cyber-attacks. Timely reporting may potentially lower the impact and damage.

Protect connected medical devices in your organization by ensuring the equipment is up-to-date and all new software patches are verified, tested, and installed promptly.

To best protect your patients, always be in the know of your organization's cybersecurity policies. To learn more contact your cybersecurity professional.

NAME OF CONTACT

EMAIL AND/OR NUMBER

HHS 405(d)
Aligning Health Care
Industry Security Approaches

To learn more about cybersecurity best practices and the 405(d) Program
check out our website at www.phe.gov/405d
or email us at cisa405d@hhs.gov