
Beware phishing attempts in 2020



• [Rachel V. Rose, JD, MBA](#)

January 13, 2020

[Health IT, Pearls, Practice Management](#)

According to the National Institute for Standards and Technology (“NIST”), phishing is defined as “[a] technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.” Often times, phishing attacks, especially those executed through email and unsecure websites, lead to the deployment of ransomware.

In June 2019, the FBI issued a public service announcement entitled [Cyber Actors Exploit ‘Secure’ Websites in Phishing Campaigns](#), which warned the public of websites and “https”. “The presence of “https” and the lock icon are supposed to indicate the web traffic is encrypted and that visitors can share data safely.

Unfortunately, cyber criminals are banking on the public’s trust of “https” and the lock icon. They are more frequently incorporating website certificates—third-party verification that a site is secure—when they send potential victims emails that imitate trustworthy companies or email contacts. These phishing schemes are used to acquire sensitive logins or other information by luring them to a malicious website that looks secure.”

In 2020, phishing continues to be an area of interest—especially in the area of healthcare. And, it’s a worldwide issue. For example, a [Hackensack Meridian Health incident](#) illustrates how a phishing attack led to a ransomware attack. “The organization said it was not aware of any impact to the confidentiality of health information, including patient records, but the attack affected all 17 hospitals and clinics and forced the health system to use paper records as it worked to bring systems back online. The undisclosed sum paid by the New Jersey health system is covered by an insurance plan that helps it cover costs related to cyber-attacks, officials said.”

As the U.S. Department of Health and Human Services (“HHS”) has espoused for years, “the HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware.” These include the following:

- Conducting a risk analysis as part of an organization’s security management process;
- Implementing policies and procedures, as well as adequate training, to detect phishing emails and other forms of malicious software; and
- Requiring access controls to limit the number of individuals, as well as the number of login attempts.

In sum, the continued emphasis of cybercriminals on healthcare organizations should serve as a warning to covered entities, business associates and subcontractors alike. Doing so can assist health systems and physicians’ practices from having to resort to paper charts and a disruption of care, which has the potential to lead to patient deaths.