Codify
BY AAPC

Health Information Compliance Alert

Reader Questions: Understand How the NIST Phish Scale Works

Question: We are working on updating our HIPAA Security protocols after doing a risk analysis of our systems. Our IT manager mentioned a Phish Scale. What exactly is that?

Texas Subscriber

Answer: In 2020, the National Institute of Standards and Technology (NIST) developed a Phish Scale to better track spikes in cybercrime via email phishing.

"The Phish Scale uses a rating system that is based on the message content in a phishing email," explains NIST in a release. "This can consist of cues that should tip users off about the legitimacy of the email and the premise of the scenario for the target audience, meaning whichever tactics the email uses would be effective for that audience. These groups can vary widely, including universities, business institutions, hospitals and government agencies," NIST adds.

The Phish Scale collects phishing information across five elements and offers a final score, offering click-rate data that can be incredibly helpful to IT management.

For example: "A low click rate for a particular phishing email can have several causes: The phishing training emails are too easy or do not provide relevant context to the user, or the phishing email is similar to a previous exercise," NIST advises. "Data like this can create a false sense of security if click rates are analyzed on their own without understanding the phishing email's difficulty."

Find out more about the Phish Scale at www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click.