Report on Patient Privacy Volume 22, Number 2. February 10, 2022 Beware Methods That Trip Up Even Strong Multifactor Authentication

By Jane Anderson

Many health care organizations use multifactor authentication (MFA) to help prevent breaches, but one expert said these systems are less secure than most people realize. Therefore, organizations should use MFA but augment it with significant security awareness training that takes into account how the system can be hacked.

"The most secure [MFA] can be hacked at least five different ways," said Roger Grimes, data-driven defense evangelist at security firm KnowBe4 LLC. "Most of them can be hacked probably 10 different ways."

Grimes, who spoke at a recent webinar,[1] said that education of everyone using the system is key: "Educate yourself and your end users to the strengths and the weaknesses of your type of MFA solutions. Make sure they're aware of the different types of attacks against that MFA solution. Just educate them a little bit so they're less likely to be phished."

MFA is used to prevent unauthorized access to websites, applications or systems by requiring users to present two or more pieces of evidence to an authentication mechanism. One of the most common uses is by financial institutions, most of which require users to input a code sent to their phone or email before allowing them to log in to their accounts with their user name and password. MFA also may use biometric evidence—such as a person's fingerprint—in combination with a user name and password. Many vendors who provide advanced systems also use contextual clues, such as looking at whether the log-in attempt is coming from a known device and/or known usual location.