Five High-Impact Cyberattacks Healthcare Industry Should Avoid in 2025

Security, administrative, and medical leaders throughout the healthcare industry have grappled with a large number of cyberattacks during the past several years. There are five that are particularly important to detect and prevent in 2025.

AI Cyberattacks

There will be more cyberattacks launched in 2025 that leverage the power of generative artificial intelligence (AI) than ever before. Bad actors will use the technology to launch a barrage of AI-powered phishing emails and text messages (vishing) that are more convincing, harder-to-detect, higher in number, and more automated.

It's no secret organizations all around the world are starting to ramp up AI usage. A CompTIA global survey shows 35 percent of organizations are using AI to improve internal operations while the same percentage are calling upon it to defend against AI-powered cyberthreats and cyberattacks.

In this new year it's crucial healthcare leaders use AI to more quickly detect and prevent cyberattacks, and to automate cybersecurity tasks which will boost productivity and cybersecurity professionals' skill development. AI usage in cybersecurity has become a "must have," not a "nice to have."

Here's a tip: Use generative AI to more quickly and accurately detect these cyberattacks. And take advantage of the productivity benefits of AI automation to streamline cybersecurity tasks. The more you use AI to fight cyberattacks the more likely you are to bolster cybersecurity.

New Types of Phishing Cyberattacks

Cybercriminals will be pivoting this year towards launching new types of phishing attacks. One is called hybrid phishing. In this scenario, a bad actor will send an email to a healthcare professional.

The email will contain a bill from a well-known company saying the professional was charged $1,000 (or some other amount) for a recent purchase that actually never happened. In the email there will be a sentence worded like this: "If you had an issue with this charge, please call this phone number: xxx."

The ploy aims to lure target victims into placing a voice call questioning the bill then tricking them into releasing sensitive information.
Hybrid phishing is becoming more prevalent because including a phone number in a phishing email is more difficult for cyber tools to detect.

Here's a tip: If you get an email indicating you paid for something you're not aware of and there's a phone number included you can call, that's a red flag it's a hybrid phishing

cyberattack. Don’t call the number. Don’t respond to the email and don’t click on any links or attachments.

For your assurance, check on the legitimacy of the person sending the email by visiting the corporate website and see if the phone number matches. There’s a good chance it won’t.

Rise in QR code phishing

The second relatively new type of phishing in 2025 will be QR bar code phishing. This trend came forth in a new Microsoft Digital Defense Report 2024 report.

Cybercriminals are trying to get healthcare employees to scan with their smartphones a malicious QR code. If that happens, the victim will be taken to the bad actor’s fake website where the victim will be asked to type in a password or other sensitive information.

Here's a tip: Don’t share your password or other sensitive information on any website you access through a QR code. To check whether it’s a scam, search on a separate channel for the website to see if it’s authentic. Most likely it won’t be.

Ransomware

For several years ransomware has been one of the most frequently used cyberattack methods against healthcare, and this trend will continue in 2025.

But ransomware tactics are changing. Cybercriminals have been discovering organizations are, generally, less willing to pay ransoms.
As a result, bad actors are shifting more often to data extortion. In this crime the bad actor sends a victim a phishing email and, if successful, steals their data, and threatens to release it publicly if the victim doesn’t pay them not to.

Here's a tip: Be aware that these are double extortion techniques. Cybercriminals threaten to make you pay a ransom and/or release your data to the public. Don’t succumb to this pressure. If you do, it’s only more likely they’ll launch another cyberattack against your organization because you proved once you would pay them.

Deepfakes
Without a doubt, deepfakes will be a major cyberattack type in 2025 throughout healthcare. These are fake videos or audio recordings showing someone doing or saying something that never happened. The aim of a deepfake is to intentionally cause the target victim harm very often by stealing their sensitive personal credentials or coaxing them to click on a link that unleashes malicious software.

The goal is often to disrupt or halt a victims’ computer network from functioning and disrupt several computers and networks across the university.

Importantly, you'll want to be especially vigilant this new year to spot audio deepfakes, which are becoming more widely used because they tend to be more difficult to detect than audio deepfakes.

"Some of the most concerning [deepfake] incidents that we've seen have been audio deepfakes," says Dan Weiner, director of the Brennan Center's Elections & Government Program in an interview with NPR. "Audio, frankly, is easier to clone."

Voice deepfakes are a major growth industry. Decision Market Research finds that from 2024 through 2033 the annual global growth rate for voice deepfakes is projected to be 37.6 percent and will total $79 million this year (34 percent in North America).

Here's a Tip: If you receive a phone call unexpectedly from someone impersonating someone you know asking you take some action urgently, stop. It's probably a voice deepfake. If the person's voice seems in any way odd in tone or not quite how the person sounds or would speak, that's a red flag you're the target of a voice deepfake.

Supply Chain

Cybercriminals will in 2025 be increasing the number of cyberattacks aimed at healthcare supply chain networks. Cybercriminals are finding an abundance of "open doors" within supply chains to go through and steal sensitive information and generate revenues. To establish a foothold, they frequently attack suppliers, which are often smaller in size and resources than large healthcare institutions. Then they go after the larger target which is the bigger organization that has an abundance of sensitive patient data bad actors ultimately want to steal.

Here's a tip: Make sure you do your due diligence on third party suppliers your healthcare institution shares its most sensitive data with. Investigate the cybersecurity controls they have in place, ensuring they have widespread encryption, multifactor authentication, and complex and long password policies.

If you find they're unwilling to share enough information to satisfy the level of security risk you require, it might be best to stop sharing information with that vendor and find one who will be more cooperative.

Looking ahead

There are plenty more types of cyberattacks that are bound to be unleashed against healthcare in 2025. But focusing on the five we've identified here will be time and effort well spent to strengthen your cybersecurity throughout this new year and beyond.

Disclaimer: This is provided to you for education and initial awareness; because this is a rapidly changing field, we cannot assure you that it is complete or that it addresses your specific circumstances. We urge you to remain informed and vigilant.

The opinions expressed in this article do not necessarily reflect the views of TIAA. The opinions are for general information only and are not intended to provide specific recommendations.

730 Third Avenue, New York, NY 10017.

4198467-0127