Phishing for Doctors: Phone Phishing Scams on the Rise

By Rana McSpadden, FACMPE

Imagine that you are in the middle of a busy workday, and suddenly you get a call from a DEA agent. He gives his name and badge number, and the caller ID shows a DEA phone number. He discloses various identifiers (such as your or license number) and asks if these are correct. Of course they are, so you confirm "yes." The agent then claims your NPI number has been used to write prescriptions for narcotics across multiple states. He goes further to state there is a warrant out for your arrest unless you cooperate. In shock and confusion, you agree. He asks for your bank account numbers, Social Security Number, and date of birth. You hesitate, thinking something doesn't feel right. At this point, he becomes aggressive and passes the call to his supervising agent. The new agent begins making additional threats of prosecution and imprisonment and claims your DEA registration will be revoked. In fear, you give the agent what he is asking for. Finally, he states you must pay $10,000 in gift cards or bitcoin for fines and penalties, otherwise, the warrant remains active, and you will be arrested.

While this is not an exact scenario, variations of it occur daily in the healthcare community. This is a form of phishing called "vishing" (voice phishing), where scammers impersonate

legitimate individuals or entities to trick victims into disclosing sensitive information. They may impersonate someone from the practice's IT vendor or internet provider to gain access to the EHR, or they can impersonate law enforcement officials or IRS agents to extort money from the victim.

In the above scenario, scammers deployed multiple tactics that gave the scam a level of legitimacy. First, they used the name and credentials of legitimate DEA agents they were able to find online. If anyone were to question this, a quick search would link that name to the DEA. Secondly, the scammers used modern telephone technology, such as Voice over IP (VoIP)[i] to transmit falsified caller ID information to display the phone number of one of the DEA agencies, otherwise known as caller ID spoofing[ii]. Next, they already had the NPI and license number of the provider. The NPI and license numbers are publicly available through sites such as the National Plan and Provider Enumeration System (NPPES) and state license verification websites. Scammers only needed a name to look up the numbers on these sites. This information may also have been involved in one of the many data leaks that have occurred over the past few years. Once sensitive and identifying information is obtained by scammers, it is generally sold through various underground websites and used for fraudulent activity. Finally, the scammers used fear and urgency to pressure the victim into giving them additional sensitive information and extort money. As shown in a recording by the DEA, scammers can be relentless in pressuring their victims into complying with the scam.

To protect yourself from this and other vishing scams, it is important to be suspicious anytime a caller claims to be from a legitimate source and begins asking for sensitive information or making demands.

- If the caller claims to be from one of your vendors, your bank or creditor, law or government officials, hang up and call back using a verifiable number. Verifiable phone numbers can be found on official websites. Do not use the number that shows on the caller ID in case this is a spoofed number.
- Be cautious if the caller is pressuring you for immediate payment, especially if they are demanding bitcoin or gift cards. No law enforcement or government official will ever demand any type of payment over the telephone, especially during an initial contact.
- Use call blocking technology to limit the number of spam and calls that are likely scams. As certain numbers are reported as being fraudulent or spam, this technology can filter these calls from being completed or can label them as being likely scams or spam.

In an October 2024 press release[iii], the DEA reminded healthcare professionals they will never be contacted by phone to request personal information, or to demand money. Any communication from the DEA will be in the form of an official letter or in person. They ask that anyone receiving a call from someone claiming to be from the DEA to report the call to the FBI at www.ic3.gov. They additionally request a report be made to the Federal Trade Commission at reportfraud.ftc.gov.

Another vishing technique recently used by scammers is artificial intelligence (AI)-generated vocal impersonation, also known as vocal cloning. In a December 2024 PSA, the FBI described vocal cloning:

"Criminals can use AI-generated audio to impersonate well-known public figures or personal relations to elicit payments.

- Criminals generate short audio clips containing a loved one's voice to impersonate a close relative in a crisis situation, asking for immediate financial assistance or demanding a ransom.
- Criminals obtain access to bank accounts using AI-generated audio clips of individuals and impersonating them[iv]."

If you are a victim of vishing, or any other phishing scam, in addition to reporting it to the above sites, you may also need to report it to local law enforcement. If financial accounts were compromised, such as bank or credit card accounts, you will also need to notify those financial institutions so they can either monitor the accounts or close and reopen new ones.

In conclusion, protecting yourself from vishing requires a combination of awareness, vigilance, and proactive measures. By staying informed about common vishing tactics and maintaining a cautious approach, you can significantly reduce the risk of falling victim to these scams and safeguard your personal information.

If you have questions about cybersecurity, HIPAA, or how to access to SVMIC resources, call 800-342-2239 or email Contact@svmic.com.

If you experience a cybersecurity or other HIPAA related incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak with the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account here.

[1] Voice over IP (VoIP)- allows users to make voice calls over broadband internet connections.

Federal Communications Commission: https://www.fcc.gov/general/voice-over-internet-protocol-voip#:~:text=Voice%20over%20Internet%20Protocol%20(VoIP)%2C%20is%20a%20technology%20that,(or%20
.

[1] Federal Communications Commission: https://www.fcc.gov/consumers/guides/spoofing

[1] United States Drug Enforcement Administration: https://www.dea.gov/press-releases/2024/10/24/dea-warns-healthcare-workers-impersonation-scam-targeting-doctors-and

[1] FBI PSA on Generative Artificial Intelligence to Facilitate Financial Fraud: https://www.ic3.gov/PSA/2024/PSA241203

[ii] Federal Communications Commission: https://www.fcc.gov/consumers/guides/spoofing

[iii] United States Drug Enforcement Administration: https://www.dea.gov/press-releases/2024/10/24/dea-warns-healthcare-workers-impersonation-scam-targeting-doctors-and

[iv] FBI PSA on Generative Artificial Intelligence to Facilitate Financial Fraud: https://www.ic3.gov/PSA/2024/PSA241203
