# Be on High Alert for Spear Phishing Scams

Scammers target specific individuals by connecting the dots of that individual's communication sphere and current circumstances. For example: we have seen that scammers pose themselves as a business function or management to communicate with other employees and/or business colleagues to disclose their personal information, login credentials or trade secrets.

Scammers are targeting nurses by sending them official looking letters from nursing regulatory bodies (NRBs) or other state/federal agencies. These scammers know the business of the NRBs and are connecting with the nurses using messaging like "Your license is suspended or will be revoked unless you connect back with us and transfer funds to fulfill the financial obligation related to this inquiry…"

These scammers also look for nurses who may be vulnerable, such as nurses on probation, sending them fraudulent suspension/revocation notices on forged letterheads (logos swiped on an internet search) and asking the nurse to deposit funds to reverse the sanction or call a phone number in the notice. Scammers are ready for such calls and do their best to get personal information or credit card information. These scammers are not only targeting hospital systems for thousands of dollars, they have also realized that there is a vulnerable population ripe for further exploitation.

**ANYTHING** received needs to be scrutinized — emails, phone calls, text messages — in short, anything regarding personal information or private financial information. An individual should pause and first confirm the legitimacy of the sender. **DO NOT** call the number from Caller ID. **DO NOT** reply to the email or text received. **DO NOT** call the number indicated in the notice. **DO** call the number of the organization or entity once you have researched for yourself and know it to be legitimate; only send email or text messages to an email that you know or to a number you are aware of or have determined is legitimate from your own research.

It is imperative to educate our nurse workforce to be vigilant regarding such scams and to let them know some basics:

1. If you receive a phone call, never give out your personal information during the call. Hang up and then only call a number back that you have determined is legitimate through your research.
2. Never reply to a text message asking for you to call the number provided in the text to discuss your imminent "suspension or revocation of your license."
3. Never reply to an email asking for personal information.
4. Never call a number provided to you in a suspect letter or email.
5. Use your own verified numbers for contacting the NRB.
6. Be vigilant! Do not discard or ignore such communication from scammers, but rather call and/or connect with the NRB to report the scam.

## Resources

1. FBI: Scammers in Disguise Target Health Care Providers with Threats and Phony Investigations
2. Federal Trade Commission Consumer Information: How to Recognize and Avoid Phishing Scams