Phishing: Tips to Avoid Getting Hooked

According to the Federal Trade Commission, phishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source – an internet service provider, a bank, or a mortgage company, for example. It asks the consumer to provide personal identifying information. Then a scammer uses the information to open new accounts or invade the consumer's existing accounts.

While no one can stop a scammer from sending you phishing emails, there are ways to prepare yourself for the next phishing email that lands in your inbox. To further protect yourself, your coworkers, and your organization, please review the following tips to protect yourself from phishing emails claiming to be from the State of Ohio Board of Pharmacy.

Verify Board of Pharmacy messages on our website. We have created a new page at www.pharmacy.ohio.gov/messages that will become a repository of all mass email notifications that are sent to our licensees. If you receive a suspicious message from someone claiming to represent the Board of Pharmacy, you may verify the message's authenticity by checking our page for the same message.

Be suspicious of any "Board of Pharmacy" message sent outside of our normal business hours. Our hours of business are Monday thru Friday, 8:00 AM until 5:00 PM. Scammers will try to hook you while we are out of the office, hoping to catch you off guard.

Spear phishing schemes look and feel authentic. Creators of these websites and emails spend a lot of time planning their attacks. They attempt to appear legitimate by creating web pages and email accounts that can appear trustworthy without a thorough inspection. Due to the uniqueness of these emails and web pages, they are often fly under the radar of spam filters and other email protections.

Human intelligence is the best defense against phishing attacks. It is critical that we are all trained to thwart phishing attacks. Be sure to take time when reviewing an email that contains any links, attachments, or asks for your information. If you see something, say something. In a recent phishing attack aimed at Ohio pharmacists, numerous recipients quickly reported the message directly to the Board. Due to this early alert, we were able to take swift action and send out a warning to the pharmacy community about the threat, which drastically reduced the number of individuals affected by the attack.

To report a suspected phishing email impersonating the Board or any of its staff, please email us at contact@pharmacy.ohio.gov.

Always inspect URLs by hovering over them with your mouse and reviewing the address before clicking.

Be cautious of shortened URLs. A major strategy being used by attackers is the use of shortened URLs provided by services such as Bitly. These URLs do not reveal the true destination of the link, making it more difficult for vigilant users to verify the domain name of the site.

Review the email address of the sender. Be on the lookout for impersonations of trusted people and brands by looking at the full email address of the sender, not just their name. Anyone can create an email account and set the name to “Ohio Board of Pharmacy”, but attackers cannot create an account that uses our domain. Always ensure that any message you receive from us contains “**@pharmacy.ohio.gov**” in the email address.

For more information on recognizing and avoiding phishing scams, visit:
https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams