February 2022 ~ Resource #380211

Help Prevent and Manage Pharmacy Scams

Use this checklist to help prevent your pharmacy from becoming the next victim of a pharmacy scam.

Goal	Suggested Approach
Help PREVENT scams	
Adhere to policies and procedures	☐ Stay current and follow policies to maintain security (e.g., "safe words," pin numbers, multifactor authentication). o It can be tempting to skip steps when things are busy (e.g., increased workload with vaccinations, staffing shortages). Scammers are counting on this as their "way in."
Watch for the four "Ps"	☐ Be aware of the four "Ps" that scammers might do:[2] o **PRETEND** to be from a legitimate organization. (e.g., pharmacy inspector, wholesaler, distributor). o say there is a **PROBLEM** (e.g., product recall, payment processing issue). o try to **PRESSURE** you to take quick action (e.g., pay a fine to the pharmacy board "immediately," order a particular product now or it will no longer be available). o request **PAYMENT** in a way that is out of the ordinary (e.g., to a "new" account number, over the phone instead of online).
Be aware of accurate information scammers use	☐ Scammers often have lots of real and accurate information. Here are some examples of things scammer may know, have access to, or share. Do NOT rely solely on this information, even though it sounds legitimate.[1] o caller ID. Scammers have been known to "spoof" phone numbers making it appear that the call is coming from an actual phone number of the organization they are pretending to represent. o address. Scammers often know your pharmacy address and the address of the organization they are pretending to represent. o account numbers. Scammers do their homework, from hacking your computer to "dumpster diving," to find this information before contacting you. o pharmacy national provider identification (NPI) numbers or license numbers. These can easily be found online.
Verify identity	☐ When things seem off, trust your gut. A legitimate organization will be accommodating to verify any information you need. ☐ Ask for key information to verify identity, such as:[1,2] o name o inspector badge number o previous order information (scammers may indicate they can't recall or that they are new to the job) ☐ Resist the pressure to act immediately.[2] Tell the scammer you need to call them back. When calling back:[2] o use the phone number you typically use for this organization or the phone number listed on the organization's website. o do NOT call the phone number on the caller ID or a different number they tell you to use.

Goal	Suggested Approach
Help PREVENT scams, continued	
Protect information	☐ Be cautious about what information you give out. Stop and think before you respond:[1] o Is the information the scammer is asking for something that someone from the organization should know? ☐ For example, someone who truly works for your wholesaler should know the product ID. A scammer may not be familiar with the wholesaler's product ID for a particular drug. The scammer may try to use a national drug code number (NDC) instead (or DIN in Canada).[1] o Is the scammer asking for something that seems inappropriate? ☐ For example, a scammer may call indicating they are performing maintenance on their system and ask you for your user ID and password "just to make sure everything is still working correctly." You should NEVER give out your login information.[3] ☐ Avoid clicking on links or opening email attachments from anyone you don't know. Phishing emails can often look like they are from a company you know and trust.[4] o Look for clues that the email is a scam (e.g., a generic greeting like "hi dear", misspellings or poor grammar).[4] o Links or attachments may give a scammer access to information on the computer.[4] ☐ Use the same philosophy you use to stay compliant with patient privacy (e.g., HIPAA in the US): only give out necessary and appropriate information.
What to do if a scam occurs	
Report the scam	☐ If you are a technician, notify your pharmacist immediately. ☐ Help report the scam to the authorities and corporate. Include as many details as you can, such as: o the date and time the scam occurred. o caller ID information. o name the scammer used. o details of your conversation with the scammer. ☐ What information did the scammer share with you? ☐ What information did the scammer ask you for?
Look for opportunities to reduce future scams	☐ Review what happened with your colleagues. ☐ Identify contributing factors. ☐ Consider if: o there was anything that could have been done differently. o policies or procedures need to be updated to help prevent something like this from happening in the future.

Users of this resource are cautioned to use their own professional judgment and consult any other necessary or appropriate sources prior to making clinical judgments based on the content of this document. Our editors have researched the information with input from experts, government agencies, and national organizations. Information and internet links in this article were current as of the date of publication.

References

1. National Associations of Boards of Pharmacy. Beware of three unique phishing scams impacting pharmacy. January 4, 2022. https://nabp.pharmacy/news/blog/regulatory_news/beware-of-three-unique-phishing-scams-impacting-pharmacy/. (Accessed January 14, 2022).
2. Federal Trade Commission. How to avoid a scam. November 2020. https://www.consumer.ftc.gov/articles/how-avoid-scam. (Accessed January 14, 2022).
3. Minnesota Pharmacists Association. Alert: fraud scams against pharmacies. July 30, 2021. https://www.mpha.org/news/575377/Alert-Fraud-Scams-against-Pharmacies.htm. (Accessed January 18, 2022).
4. Federal Trade Commission. How to recognize and void phishing scams. May 2019. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams. (Accessed January 25, 2022).

Cite this document as follows: **Clinical Resource,** ***Help Prevent and Manage Pharmacy Scams. Pharmacist's Letter/Prescriber's Letter*****. February 2022. [380211]**