

Beware of Scams During COVID-19: Supply Offers from Vendors or Others May Not Be Legitimate

Providers are receiving vendor emails or other contact offering PPE supplies, and some may not be legitimate vendors or businesses. Please beware that some offers are scams and are not credible businesses.

Please always rely on the Centers for Disease Control and Prevention (CDC) guidance for any supplies or related products necessary for your facilities.

[The Federal Trade Commission \(FTC\) has also provided general advice on avoiding scams related to the Coronavirus.](#) This includes:

- Don't click on links from sources you don't know. They could download viruses onto your computer or device.
- Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or experts saying they have information about the virus. For the most up-to-date information about the Coronavirus, visit the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO).
- Ignore online offers for vaccinations. There currently are no vaccines, pills, potions, lotions, lozenges or other prescription or over-the-counter products available to treat or cure Coronavirus disease 2019 (COVID-19) — online or in stores.

Questions to Use to Help Verify True Vendors and Identify Scams

Providers are receiving vendor emails or other contacts offering PPE supplies, and some may not be legitimate vendors or businesses. Below are lists of questions to help safeguard your facility and organization from potential scam and fraudulent vendors.

Ask yourself:

Who is this Company?

1. Why have I never heard of the company before?
2. Where is this company based?
3. Is the price unusually attractive?
4. Why does this vendor have the product when no one else can get it?
5. Do they want you to pay by cash, credit card, or money order?
6. Are they asking personal business information by email?

What Products are they Offering, and is it Too Good to be True?

7. Are they asking or pressuring you to buy now, before supplies are gone?
8. Are they offering something for "Free" if you buy the product?
9. Do they tell you not to worry about a contract?
10. Does it sound too good to be true, during this crisis situation?

Can you verify their information online?

11. Where is the email address from? Legitimate businesses have their own addresses and do not use gmail, yahoo, etc.
12. Does the organization have a website and they cannot be found on Google?
13. Does the URL match the brand name?
14. Does the website use HTTPS or an SSL certificate?
15. The information about their product contains a lot of hype and exaggerations, but few specific details about when, where, why, how much, etc.
16. Does the website content appear to be infused with grammar or spelling errors?
17. Does a whois lookup (<https://www.whois.net/>) on the domain name help prove its ownership?
18. Is the SSL certificate EV or OV validated?
19. How many years has the domain been in use?
20. Does the website have reliable contact details and inbound links?

Ask the company:

21. What is the link to your company website?
22. Send me information about these products, prior to me considering purchasing.
23. Send me your Employee Identification Number (EIN) so that I can look up your company information.
24. Are you listed with the Better Business Bureau (BBB)? Please provide your information there (www.bbb.org).
25. Are you a business partner of AHCA/NCAL? Please provide proof of partnership.