

BEWARE: EVOLVING PANDEMIC CYBERTHREATS

PHISHING EMAILS EXPLOITING COVID-19 VACCINE ACCESS



Cybercriminals are taking advantage of the limited availability and confusion surrounding the COVID-19 vaccine in an attempt to deceive you. Avoid interacting with any emails containing COVID-related news, offers or requests, since many of these are phishing scams.

Subject: COVID-19 Vaccine Dosage Reservation



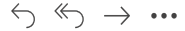
Stoffel, Martha <m.stoffel@cdchelthcare.org>

Thu 3/1/2021 11:43 AM

To: Jane Doe

FAKE E-MAIL ADDRESS:

Incorrect "healthcare" spelling



Reserve Your COVID-19 Vaccine Today!

Hello [[first_name]]

TOO GENERIC / SPAM PERSONALIZATION ERROR

This is a reminder that you are able to reserve your dose of the COVID-19 vaccine through your healthcare portal.

URGENCY

If you are interested, please take the time to fill out the proper information by using the button below:

Reserve Vaccine Here

FAKE LINK:

<http://ccovidd.ccd.gov/covid-vaccines/#reserv>

If you have trouble filling out the required information, please let our patient services team know and someone will be able to assist you.

SUSPICIOUS LINK:

<http://28djjm93.ccovidd.ccd.gov/help>

Thank you,
Martha Stoffel

Customer Outreach Representative

TOO GENERIC / NO CONTACT INFORMATION

LEGEND

- FAKE E-MAIL ADDRESS
- BAIT TACTIC
- TOO GENERIC
- BAD LINKS
- URGENCY
- SYNTAX & GRAMMATICAL ERRORS



TIPS FOR GOOD EMAIL HYGIENE

1

WATCH FOR OVERLY GENERIC CONTENT AND GREETINGS

Cyber criminals will send a large batch of emails. Look for examples like "Dear valued customer."

2

EXAMINE THE ENTIRE FROM EMAIL ADDRESS

The first part of the email address may be legitimate but the last part might be off by letter or may include a number in the usual domain.

3

LOOK FOR URGENCY OR DEMANDING ACTIONS

"You've won! Click here to redeem prize," or "We have your browser history pay now or we are telling your boss."

4

CAREFULLY CHECK ALL LINKS

Mouse over the link and see if the links destination matches where the email implies you will be taken.

5

NOTICE MISSPELLINGS, INCORRECT GRAMMAR, & ODD PHRASING

This might be deliberate attempt to try to bypass spam filters.

6

CHECK FOR SECURE WEBSITES

Any webpage where you enter personal information should have a url with https://. The "s" stands for secure.

7

DON'T CLICK ON ATTACHMENTS RIGHT AWAY

Virus containing attachments might have an intriguing message encouraging you to open them such as "Here is the Schedule I promised."



sales@pcnetinc.com
417-831-1700
2026 E Phelps St.
Springfield, MO 65802