BEWARE: COVID-19 PHISHING EMAILS

SPREADING FEAR AND PANIC OF INCREASED LOCAL INFECTIONS

Avoid COVID-19 phishing scams by practicing good email hygiene. The CDC recommends you take at least 20 seconds to wash your hands to avoid germs. We recommend you take at least 20 seconds to review each email to avoid falling victim to a phishing scam.

SCHEDULE YOUR FREE cyber security training. Contact us!

2019-nCoV: Coronavirus outbreak in your city (Emergency)

CDC-INFO <cdcchan-00813@cdc-gov.org>

FAKE E-MAIL ADDRESS

Tue 2/4/2020 8:33 AM

To: John Smith

LEGEND
- FAKE E-MAIL ADDRESS
- TOO GENERIC
- BAD LINKS
- URGENCY
- SYNTAX & GRAMATICAL ERRORS

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00813

CHECK BEFORE YOU CLICK!
Hover your cursor over the link to preview the link URL. BEWARE of links that direct you to a login page.

Dear Sir/Madam,

TOO GENERIC

The Centers for Desease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Provence, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

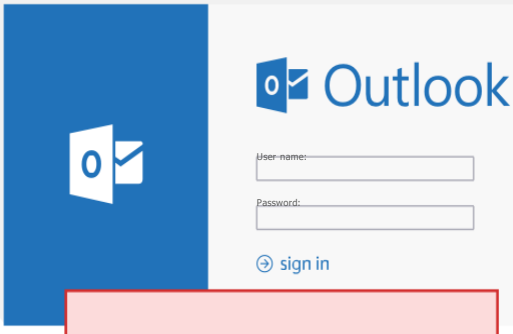
Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html).

You are immediately advised to go through the cases above to avoid potential hazards.

URGENCY

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

POOR GRAMMAR



The fake web page use in the coronavirus phishing campaign looks like an Outlook login window

DATAkloud
SIMPLIFIED TECHNOLOGY SOLUTIONS

SCHEDULE YOUR FREE training

20 SECONDS TO BETTER 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 destination matches where the email implies you will be taken.

5. **NOTICE MISSPELLINGS, INCORRECT GRAMMAR, & ODD PHRASING**
This might be a 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**
Attachments containing viruses might have an intriguing message encouraging you to open them such as “Here is the Schedule I promised.”