Charles H. Greenthal Management Corp.

CHG ALERT

April 14, 2020 Update *(#63)*

To: All Residents & Board Members

From: Charles H. Greenthal Management Corp.

Re: WHO Warns of Scams and Criminals Pretending to be WHO Representatives

The World Health Organization has published a warning to inform people that hackers and cyber scammers are taking advantage of the coronavirus disease (COVID-19) pandemic by sending fraudulent email and WhatsApp messages in an effort to trick users into clicking on malicious links or opening attachments.

These actions can reveal your username and password, which can be used to steal money or sensitive information.

If you are contacted by a person or organization that appears to be WHO, verify their authenticity before responding.

The World Health Organization will never:

- ask for your username or password to access safety information
- email attachments you didn't ask for
- ask you to visit a link outside of www.who.int
- charge money to apply for a job, register for a conference, or reserve a hotel
- conduct lotteries or offer prizes, grants, certificates or funding through email

The only call for donations WHO has issued is the COVID-19 Solidarity Response Fund, which is COVID-19 Solidarity Response Fund. Any other appeal for funding or donations that appears to be from WHO is a scam. Beware that criminals use email, websites, phone calls, text messages, and even fax messages for their scams.

Phishing: malicious emails and messages appearing to be from WHO

The WHO is aware of suspicious email messages attempting to take advantage of the COVID-19 emergency. This fraudulent action is called phishing.

These *"Phishing"* emails appear to be from WHO, and will ask you to:

- give sensitive information, such as usernames or passwords
- click a malicious link
- open a malicious attachment.

Using this method, criminals can install malware or steal sensitive information.

How to prevent phishing:

1. **Check their email address.**
   Make sure the sender has an email address such as 'person@who.int'

   If there is anything other than 'who.int' after the '@' symbol, this sender is not from WHO.
   For example, *WHO does not send email from addresses ending in '@who.com', '@who.org' or '@who-safety.org'.*

2. **Check the link before you click.**
   Make sure the link starts with https://www.who.int. Better still, navigate to the WHO website directly, by typing https://www.who.int into your browser.

3. **Be careful when providing personal information.**
   Always consider why someone wants your information and if it is appropriate. There is no reason someone would need your username & password to access public information.

4. **Do not rush or feel under pressure.**
   Cybercriminals use emergencies such as the coronavirus disease (COVID-19) pandemic to get people to make decisions quickly. Always take time to think about a request for your personal information, and whether the request is appropriate.

5. **If you gave sensitive information, don't panic.**
   If you believe you have given data such as your username or passwords to cybercriminals, immediately change your credentials on each site where you have used them.

6. You can verify if communication is legit by contacting WHO directly. Contact WHO or Report a scam