HAZARD ALERT

Coronavirus Scam Alert

Beware of Criminals Pretending to be the WHO (World Health Organization)

To take advantage of the Cornovirus situation, criminals are disguising themselves as the WHO to steal money or sensitive information. If you are contacted by a person or organization that appears to be from WHO, verify their authenticity before responding.

The World Health Organization Will Never:

- ask you to login to view 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
- ask you to donate directly to emergency response plans or funding appeals.

Beware that criminals use email, websites, phone calls, text messages, and even fax messages for their scams will try to look as convincing as possible to take advantage. You can verify if a communication is legitimate by contacting the WHO directly at https://www.who.int/about/who-we-are/contact-us. Do not click on any links or attachments prior to confirming.

Phishing: Malicious Emails Appearing to be from WHO

Phishing is the fraudulent practice of pretending to be a reputable company in order to induce individuals to give up personal information such as passwords or credit card numbers. Unfortunately, sinister folks are attempting to take advantage of the 2019 Coronavirus situation. The phishing emails reported so far that 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.

Opening any of these communications and clicking on any of the links, the criminals can install malware to track your internet uses and gather this sensitive information even if you did not provide it directly.

How to Prevent Phishing

1. Verify the sender.
   emails from the WHO will have email domains **@who.int** only
2. Check the link before clicking
   Look for the https://www.who.int before the navigation. They recommend going to their website and navigating directly
3. Be careful when providing private information
   there is no reason for the need of personal information to access public information. Ask yourself if them requesting your information is appropriate.
4. Do not feel rushed or pressured
   Cybercriminals use emergencies such as 2019-nCov to get people to make decisions quickly.
5. Report the scam to the WHO.
   https://www.who.int/about/report_scam/en/

If you were caught in the scam, DON'T PANIC.

If you believe you gave data such as usernames and passwords to a cyber criminal, immediately change your credentials on each site where you have used them. Monitor the activity on those sites.

This information was directly sourced from:
https://www.who.int/about/communications/cyber-security

NOTE: Date of last revision and document confirmed current Mar 9, 2020. If you believe this document is out of date, please contact us.

© 1Life Workplace Safety Solutions Ltd. 2020
www.1LifeWSS.com 1-866-223-7374

HAZARD ALERT

RECORD OF HAZARD ALERT	
Company Name:	**Work Location Dept.:**
Talk Given by:	**Date / Time:**

Results of inspection, demonstration or other activity or suggestions during talk:

List of All Employees Who Attended the Safety Talk:	
Name (PRINT)	***Signature***
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	
16.	
17.	
18	
19.	
20.	

Signed: _____ Position Held: _____

© 1Life Workplace Safety Solutions Ltd. 2016

280 Stradbrook Ave, Winnipeg, MB R3L 0J6
1-866-223-7374
www.1LifeWSS.com
info@1Lifewss.com