CYBER SECURITY

By Sachin Dedhia
CISA, CEH, ISO 27001 L.A.,
Ethical Hacker & Digital Forensics Expert

Web Conference Security

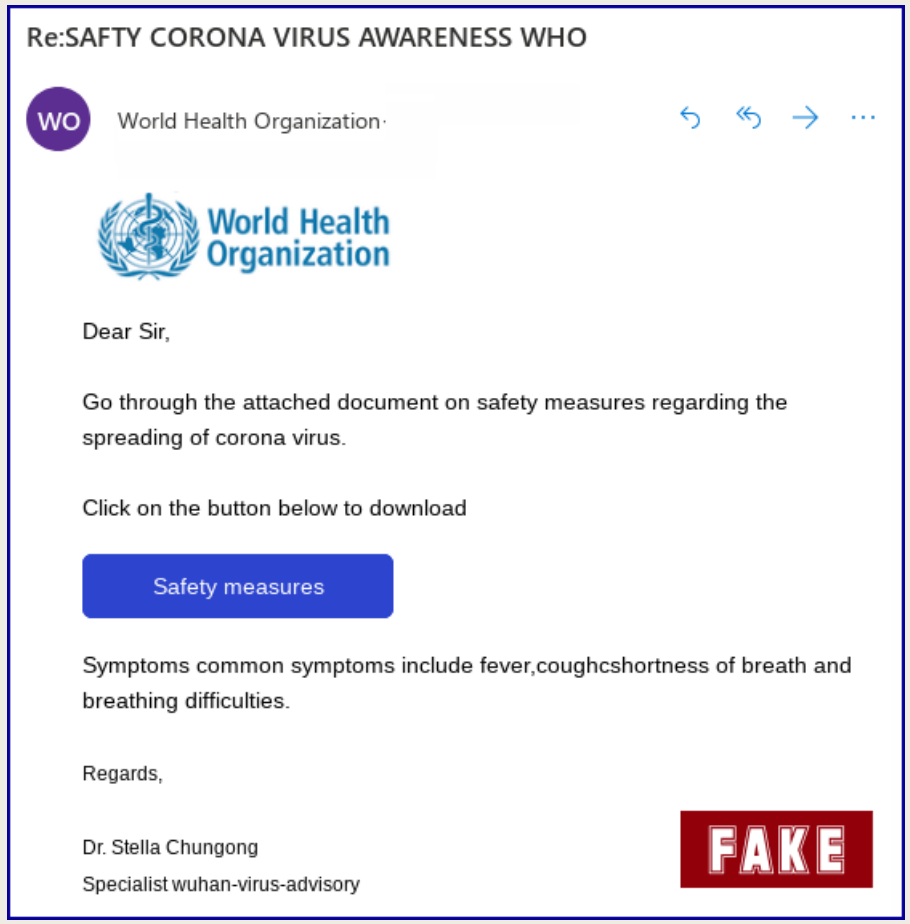
- Few security issues while using web conferencing are:
  - *Attackers joining the meeting if no password to join is required or if they get to know the access code.*
  - *Attacker sending malicious links in chat to extract information.*
  - *Data shared using third parties might be used by attackers to obtain information.*
  - *Vulnerabilities if not patched on time could allow attackers to exploit the target system.*

- Best practices for using Web Conferencing:-
  - *CERT-In Advisory Notes.pdf*

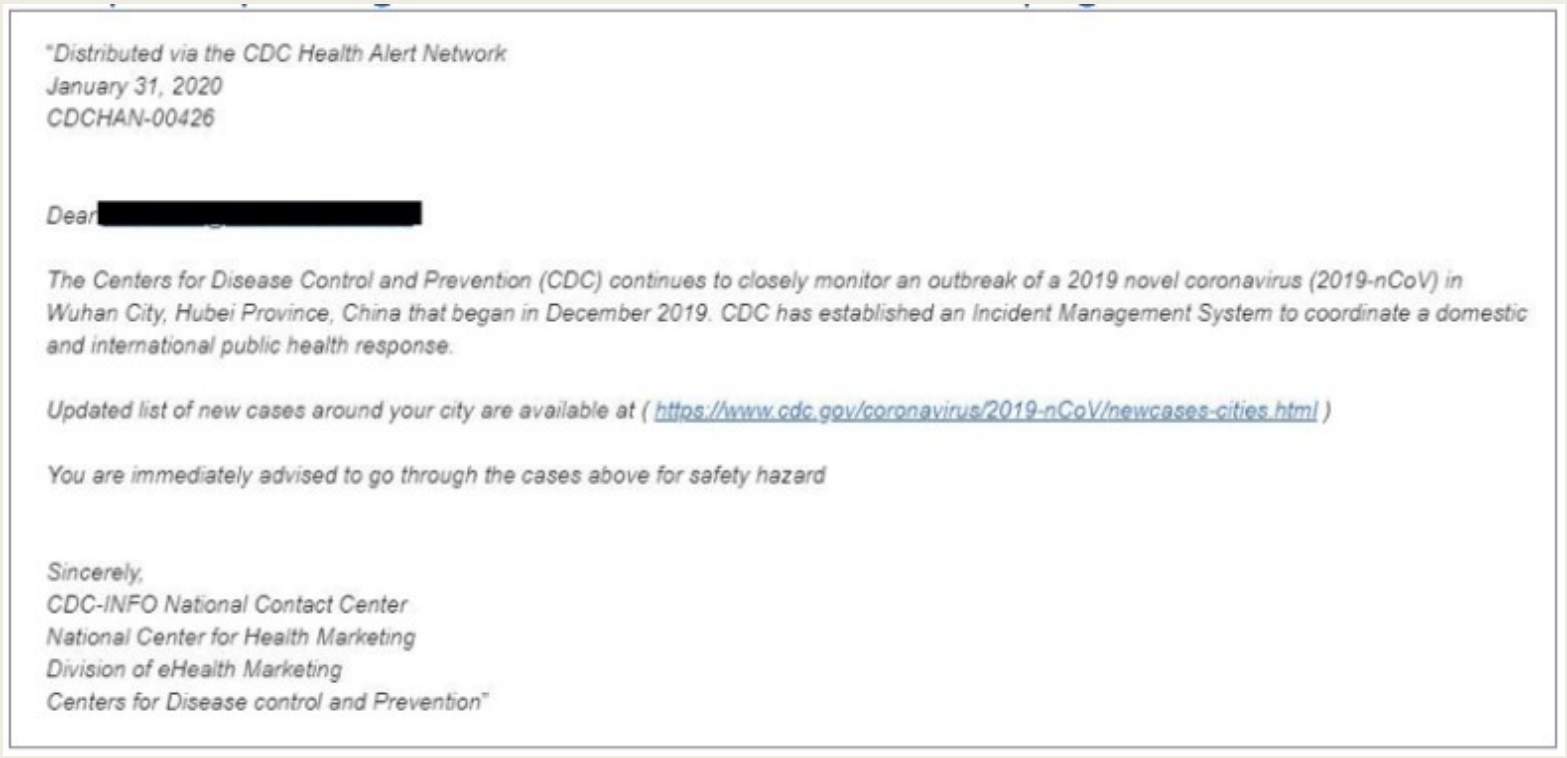
Fake Websites

- coronavirusaware[.]xyz
- corona-virus[.]healthcare survivecoronavirus[.]org
- vaccine-coronavirus[.]com
- coronavirus[.]cc
- bestcoronavirusprotect[.]tk
- coronavirusupdate[.]tk
- coronavirusstatus[.]space
- coronavirus-map[.]com
- blogcoronacl.canalcero[.]digital
- coronavirus[.]zone
- coronavirus-realtime[.]com
- coronavirus[.]app
- bgvfr.coronavirusaware[.]xyz
- Add these websites in the firewall blocklists
- Source : https://twitter.com/DCP_CCC_Delhi

https://www.who.int/about/communications/cyber-security



CDC alerts Fake Emails



"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

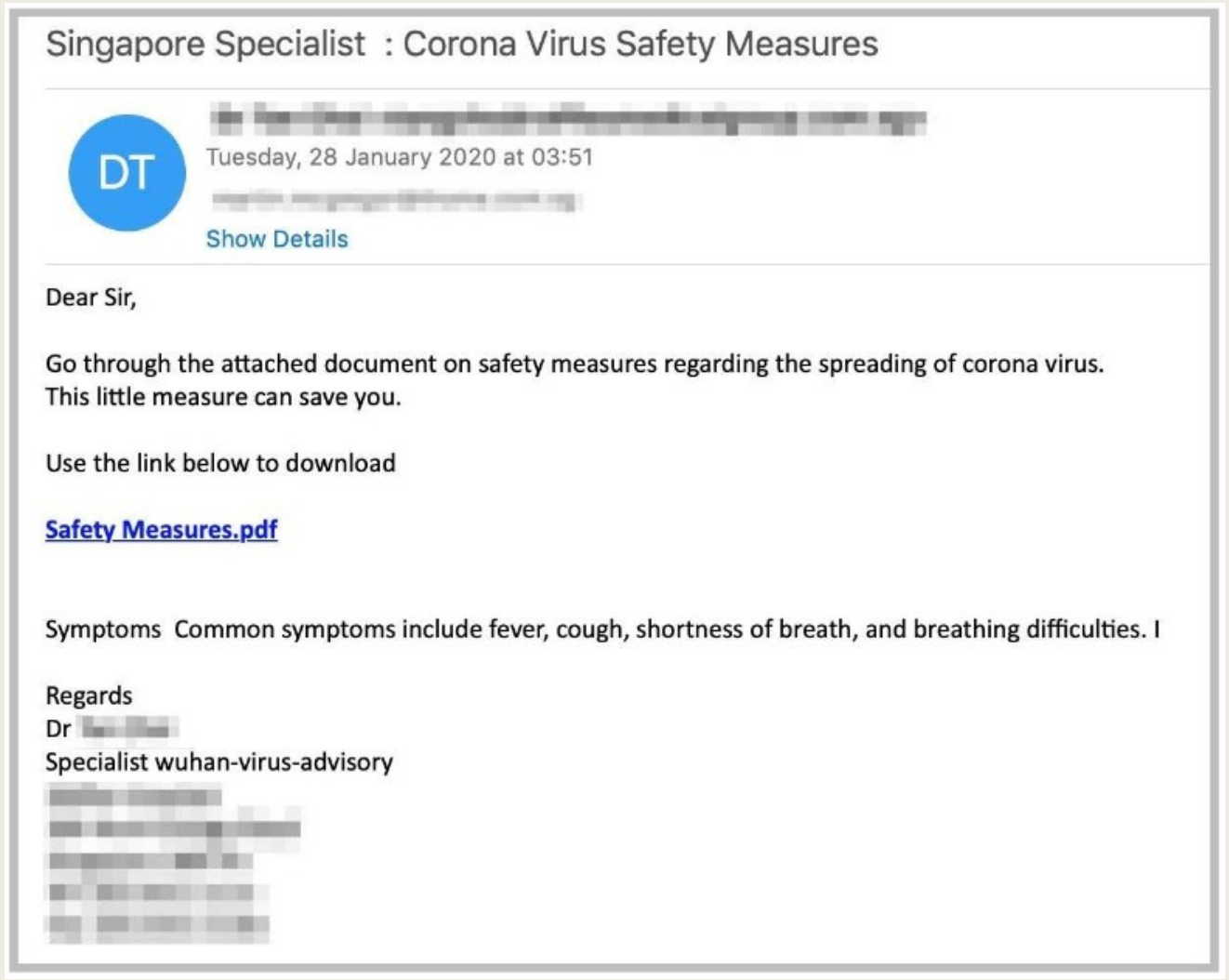
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health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

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

Health advice Fake emails.



Singapore Specialist : Corona Virus Safety Measures

DT

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Work Place Policy Fake emails

All,

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before **[[current_date_1]]**.

If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

Regards,
Human Resources

Safety tips

- **Beware of online requests for personal information.** A coronavirus-themed email that seeks personal information like your Social Security number or login information is a phishing scam. Legitimate government agencies won't ask for that information. Never respond to the email with your personal data.
- **Check the email address or link.** You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses. Delete the email.
- **Watch for spelling and grammatical mistakes.** If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email. Delete it.
- **Look for generic greetings.** Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.
- **Avoid emails that insist you act now.** Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete the message.
- www.Virustotal.com

Zoom Security Advisery.pdf

ZOOM Meeting

1. **PASSWORD PROTECT YOUR MEETINGS**

If you want to set up a password at the individual meeting level, head straight over to the "Settings" tab and enable "Require a password when scheduling new meetings", which will ensure a password will be generated when a meeting is scheduled. All participants require the password to join the meeting.

2. **AUTHENTICATE USERS**

When creating a new event, you should choose to only allow signed-in users to participate.

3. **JOIN BEFORE HOST**

Do not allow others to join a meeting before you, as the host, have arrived. You can enforce this setting for a group under "Account Settings."

4. **LOCK DOWN YOUR MEETING**

"lock" your meeting as soon as every expected participant has arrived.

5. **TURN OFF PARTICIPANT SCREEN SHARING**

6. **USE A RANDOMLY-GENERATED ID**

7. **USE WAITING ROOMS**

Identify Fake News

Websites to help identify fake news.

https://www.boomlive.in/fake-news

https://www.altnews.in/

https://check4spam.com/

https://www.factchecker.in/

https://smhoaxslayer.com/

https://tineye.com/

https://www.invid-project.eu/tools-and-services/invid-verification-plugin/

https://weverify.eu

Work from home policy

- https://resources.workable.com/remote-work-policy
- https://resources.workable.com/work-from-home-company-policy#