To: All Staff

From the Department of Commerce (DOC) Office of the CIO.

Avoiding COVID-19 Scams and Phishing Attempts

Coinciding with an increase in telework at the Department and around the nation, our IT staff has seen an increase in scams and phishing attempts that reference the ongoing COVID-19 outbreak. We must all continue to be vigilant to protect our networks from malicious actors.

Scam emails will often claim to be from reliable authorities such as the CDC, HHS, WHO and others. These scams are designed to entice recipients into opening emails containing malicious content, such as attachments or links to web content. Opening these documents or links will likely result in the compromise of the device (computer, phone, tablet) with malicious code designed to steal personal and/or financial information.

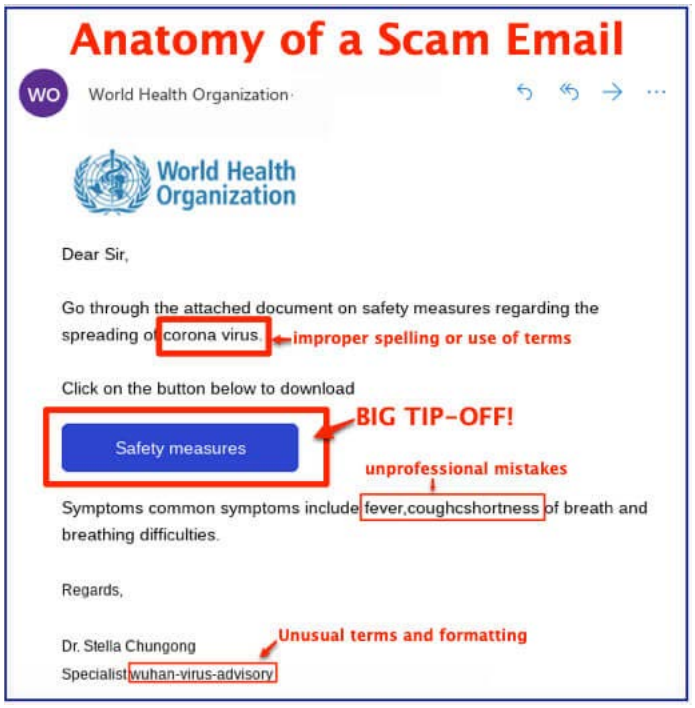
What You Should Be Looking Out For:

Scammers impersonating organizations such as the CDC, HHS, WHO and others, providing purported tips, safety measures, and/or updates on the outbreak. These scammers are leveraging:

- Emails
- SMS (text) messages
- Phone calls

Attached is an example of one phishing campaign that has been reported in the media. It should be noted that organizations such as the WHO will never ask users to log in to verify safety information, send unsolicited emails, email attachments, request that you visit a website, or solicit donations.

Actual Phishing Scam Sample



Another email being circulated delivers an attachment titled, “President discusses budget savings due to coronavirus with Finance Minister.rtf.” The attachment, which contains malicious code, runs silently without the user’s knowledge or permission giving the attacker control over the infected system and its content.

How To Stay Healthy Virtually:

1. Do NOT open any links or attachments from unknown or suspicious senders who claim to be providing you with purported tips, safety measures, and/or updates on the COVID-19 pandemic.
2. Report suspected phishing emails to the applicable Bureau Security Operations Center or to the Enterprise Security Operations Center (ESOC), which can be reached at ESOC@doc.gov or at 202-482-4000.