February 26, 2020

Email Phishing Threats Using Fear of the Coronavirus

As fear of the Coronavirus grows, malicious actors are leveraging that fear to create phishing attacks designed to steal users' credentials, sensitive information or money, or to infect devices with malware. Attackers are sending emails that appear to be from legitimate health organizations or government agencies, including the World Health Organization (WHO) and the Centers for Disease Control (CDC).

Attacks include asking users to review an attached document with instructions on how to protect oneself from the Coronavirus, or to click a link to watch an educational video, or ask a user to provide credentials before accessing information.

Below is one example:

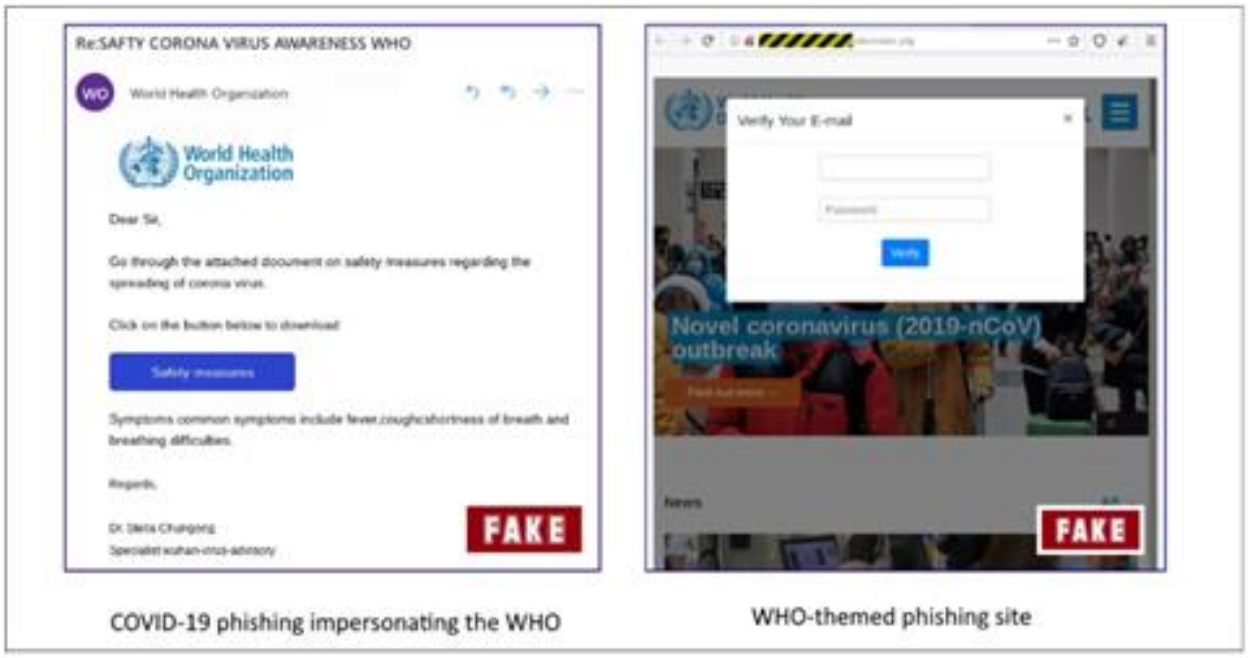

Figure 1: COVID-19 Phishing Email Impersonating the WHO (Source: Bleeping Computer)

Quick Tips:

- **Think twice; don't feel rushed or pressured.** Read emails thoroughly and be wary of communications that ask you to act on your fears.
- **Look at the domain name.** Some attackers modify domains to catch targets off guard. For example, if the correct domain was www.example.com, the phishers may register "examp1e.com" or "example.co". The legitimate domain of the WHO is www.who.int, and the CDC is www.cdc.gov.
- **Always verify.** Verify that the email is from the real sender before engaging. Call or email the sender to confirm it is legitimate. Any email from the WHO would have a sender like *person@who.int*.

Did You Know?

You can safely check where a link goes without clicking:

Desktop (OSx and Windows): Hover your cursor over the link to view the URL.

Mobile Devices (Android, iOS, Windows): Touch and hold the link until a pop-up menu appears.

If you suspect you have received a phishing email at work, report it immediately using the Report Phishing button.