Need a deeper dive on this topic? **Ask-An-Expert**

COVID-19 Phishing Examples and Guidance

March 17, 2020 | Ask-An-Expert Writeups | Security Awareness, Phishing, Social Engineering |
By Jake Williams, IANS Faculty

The Takeaway

Attackers are using COVID-19 as a phishing lure, including emails designed to look like they come from the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO).

COVID-19 Phishing Attempts Require a Proactive Defense

People generally fall for phishing pretexts that promise:

- A call to action.
- To fill an information void.

COVID-19 offers opportunities for attackers in both approaches. People are desperate for information and are constantly being given updated guidance on how to adapt to remote work and stop the spread of the disease, along with other "helpful tips" to deal with COVID-19. Unfortunately, the onslaught of emails from businesses detailing how they will keep staff and customers safe during COVID-19 has set the stage for users to expect these emails and will likely lead to a higher percentage of users treating them as legitimate.

The best way to protect employees from this specific phishing threat is to:

- Detail when and how you'll communicate COVID-19-related updates and policy guidance.
- Agree on an email template and communication delivery frequency (and then actually stick to it).
- Educate users that attackers will absolutely use COVID-19 as a pretext.
- Show them the examples in this document (see below) so they know what to expect.

Organizations should also educate users with specific advice on differentiating legitimate corporate updates from phishing attempts. Even if users click, once they view the login screen, they should be told to assess with high confidence it was a phish and report it.

Currently, very few vendor emails contain an attachment. Of those that do, most are PDF files, and none that we've seen have any active content (e.g., Office document macros). Also, none were delivered as a compressed attachment (zip, rar, 7Z, etc.).

Specific Phishing Examples

Below, we provide specific examples of COVID-related phishing attempts we've encountered. Many of these phishing attempts are not yet being publicly discussed.

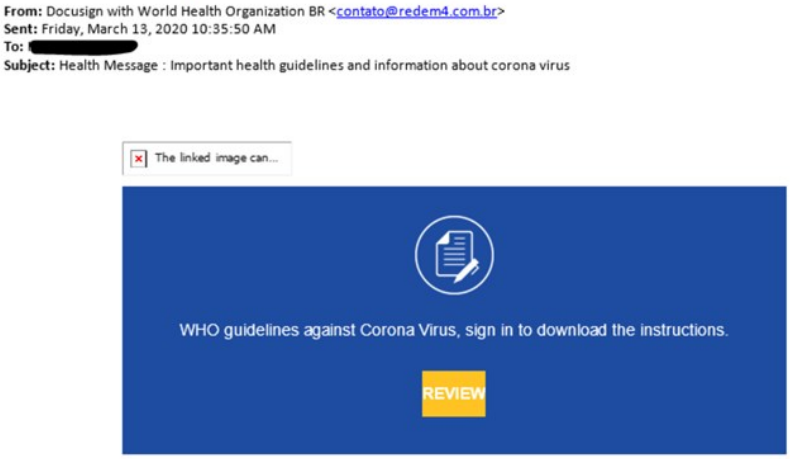
Figure 1 shows a lure that targets foreign visitors by convincing them to provide sensitive information to an attacker-controlled email address.

Figure 1: Phish Targeting Foreign Visitors

Source: IANS, 2020

Figure 2 shows an example of a DocuSign credential-harvesting phish purporting to be from WHO.

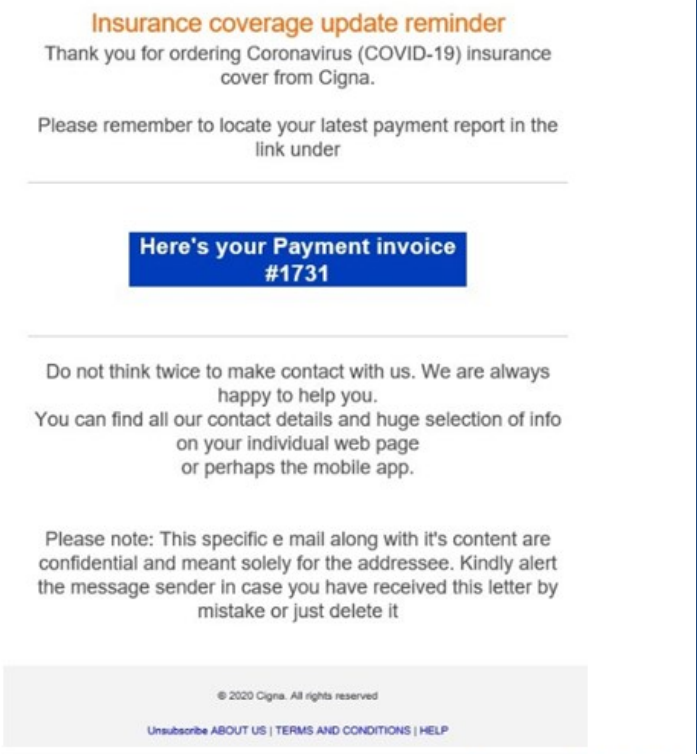
Figure 2: Example of a DocuSign Credential-Harvesting Phish



Source: IANS, 2020

Figure 3 shows an insurance-themed phish targeting Cigna customers. This is particularly effective for attackers because it lets them easily discover the insurance provider for an organization.

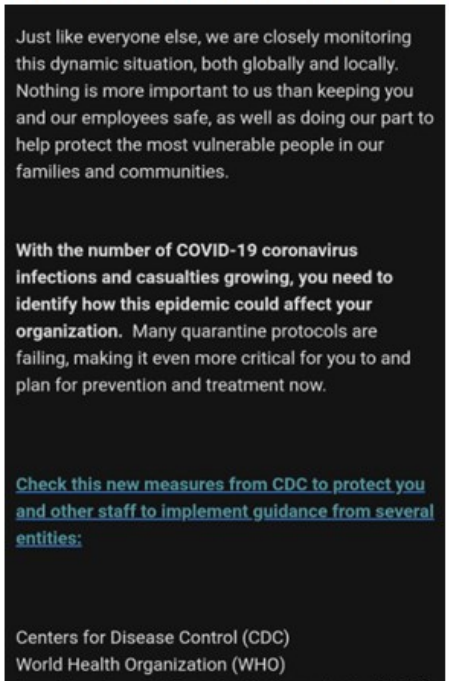
Figure 3: Insurance-Themed Phish



Source: IANS, 2020

Figure 4 shows a phish that has a link to “new measures from the CDC” but also borrows credibility from WHO, the Equal Opportunity Commission (EEOC), the Department of Labor (DOL) and the Occupational Health and Safety Administration (OSHA).

Figure 4: Phish Claiming to Offer New Info from the CDC

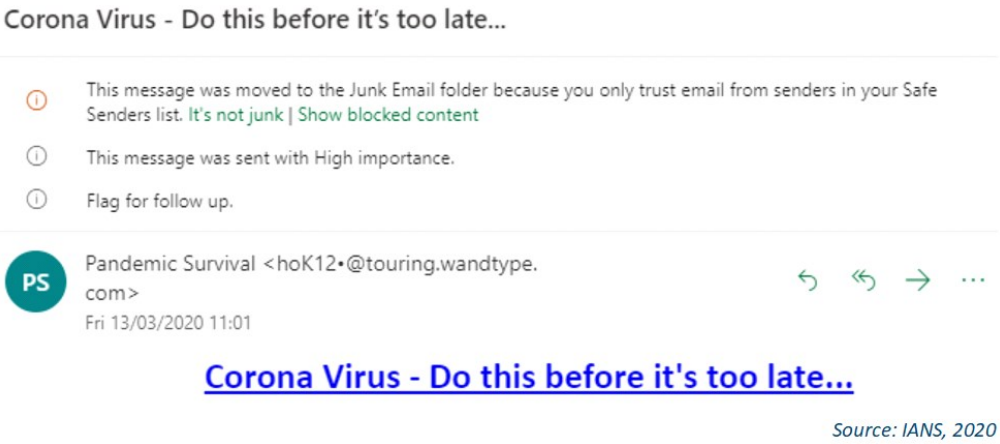


Equal Employment Opportunity Commission (EEOC)
Department of Labor (DOL)
Occupational Health and Safety Administration (OSHA)
State Department
Major medical clinics

Source: IANS, 2020

Figure 5 shows another credential-harvesting phish.

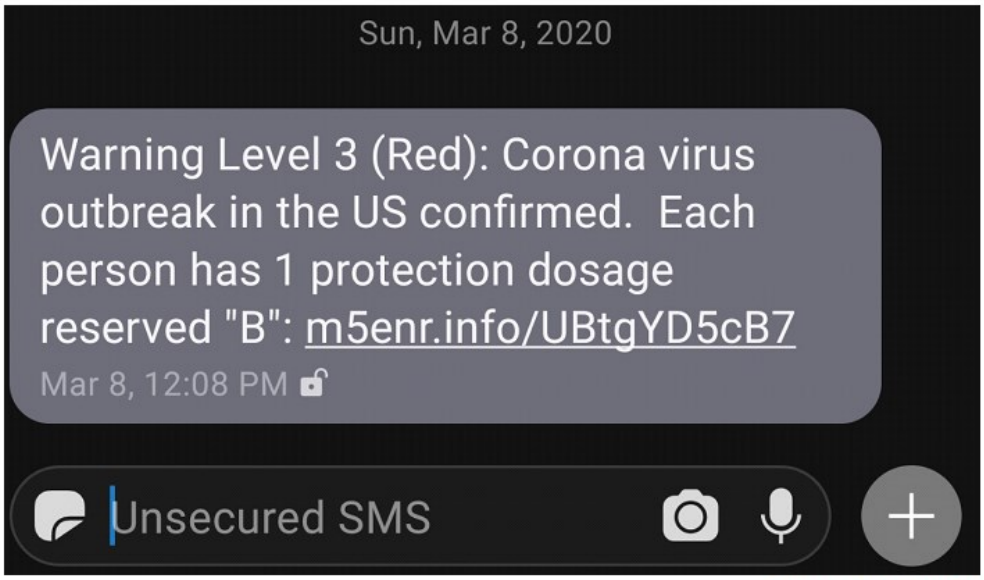
Figure 5: More Credential-Harvesting



Source: IANS, 2020

The following are all SMS-based COVID-19 phishing emails. Figure 6 shows SMS delivery of malware links:

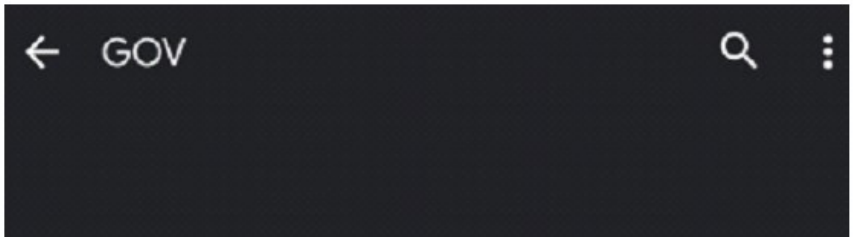
Figure 6: SMS Delivery of Malware Links

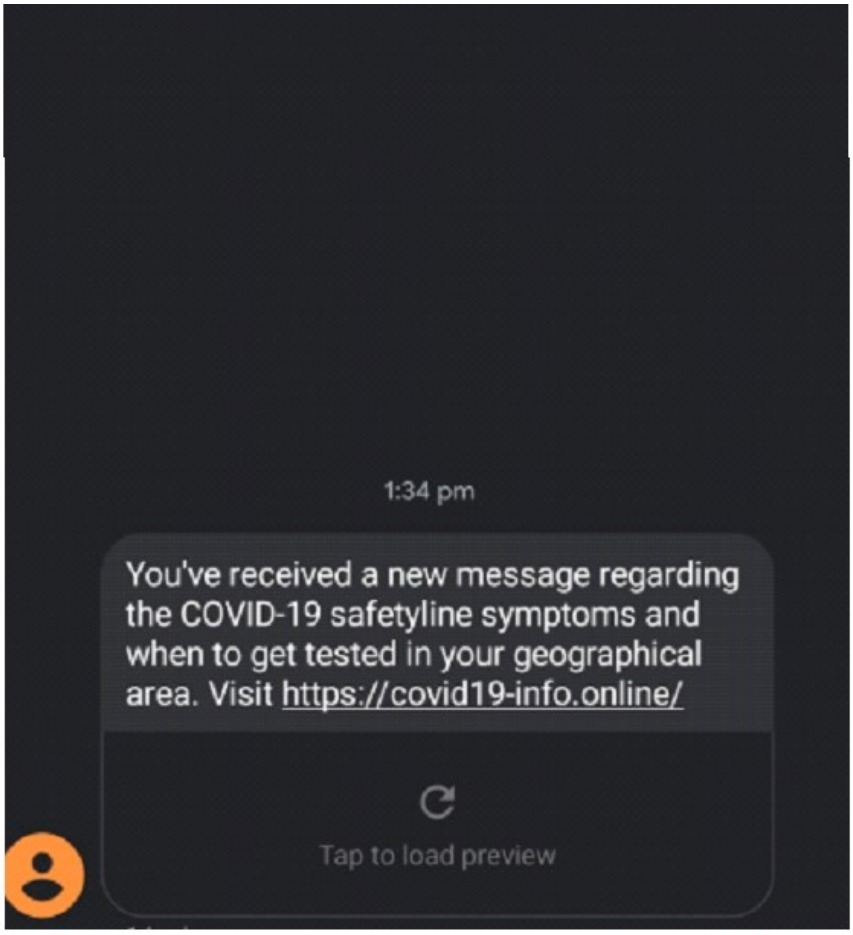


Source: IANS, 2020

Please note the use of sender "GOV" in the SMS delivery in Figure 7.

Figure 7: GOV Used as the Sender





Source: IANS, 2020

The SMS delivery shown in Figure 8 is particularly dangerous and preys on the desire to fill an information void:

Figure 8: Filling an Information Void

All employees will receive (mandatory) paid leave to avoid the spread of the COVID-19 novel coronavirus starting from March 13, 2020.
Offices will resume after 2 weeks of the mandatory closure.
Check the link to see if your company is listed:
http://bit.ly/MandatoryPaidLeave 17:43

Source: IANS, 2020

Potential Phishing Domains

Due to browser warnings for websites not using HTTPS, we are seeing more attackers deploy HTTPS certificates than ever before. This helps them avoid traffic inspection in networks where TLS decryption isn't performed. However, it also works against attackers when certificate transparency logs are inspected. A list of COVID-19-themed domains that have been issued HTTPS certificates can be found here.

Please note, not every domain on the list is malicious. The list merely catalogs the domains containing the words "coronavirus" or "covid," some of which may be legitimate. However, the list can serve as a potential block list for high security environments where confidentiality is valued over availability.

Now Is the Time to Educate

In the weeks ahead, we should continue to expect more COVID-19-related emails. As situations on the ground change (including the possibility of U.S. lockdowns similar to Italy), phishing emails will certainly follow. For example, see these articles from Proofpoint:

- Attackers Expand Coronavirus-Themed Attacks and Prey on Conspiracy Theories
- Coronavirus-themed Attacks Target Global Shipping Concerns
- Emotet Leverages Coronavirus and Greta Thunberg (Again) While Coronavirus Threats Increase

Organizations should engage their workforce immediately to articulate the type and format of authorized communication about COVID-19.

Further Reading

COVID-19 and Infosec: What You Need to Know, March 16, 2020

Phishing Simulation and Training: A Market Overview, Feb. 7, 2020

Phishing Simulations: Know Who to Inform and Why, Dec. 12, 2019

Create an Effective Anti-Phishing Program, Dec. 3, 2019