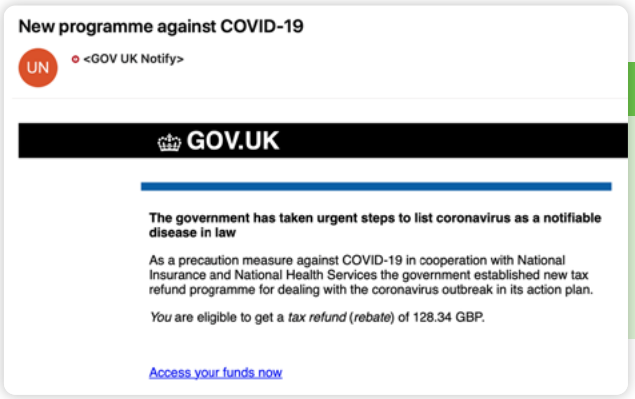
INFOSEC JOHNSON COUNTY KANSAS

Top 9 Coronavirus Phishing Scams

We collected nine coronavirus phishing attack examples to shed light on the top tactics cybercriminals are using so you can prepare your employees for the threats they are facing now and in the foreseeable future.



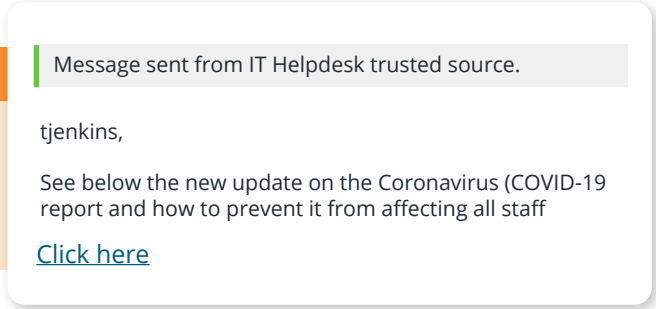
1. Consumer relief package

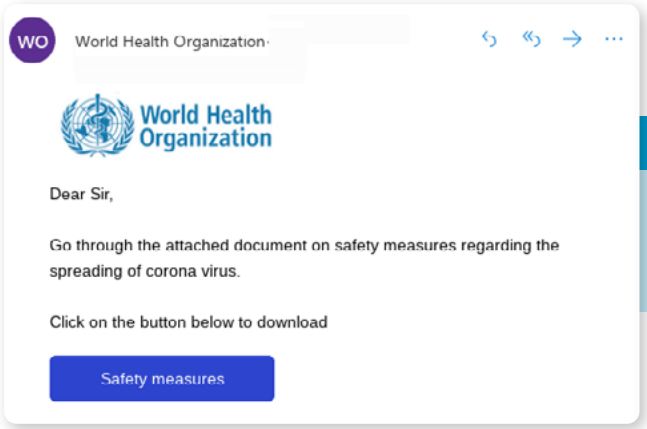
As the economic fallout of the COVID-19 pandemic continues, attackers are leveraging consumer anticipation of tax relief and government-issued economic stimulus plans. These attacks trick victims into dropping their guard and clicking a malicious link.

Similar attacks have been spotted in the United States.

2. Help desk impersonation

At a time when technical support teams are helping employees transition to remote workstations, cybercriminals are impersonating IT help desks to take advantage of their increased visibility and communication.



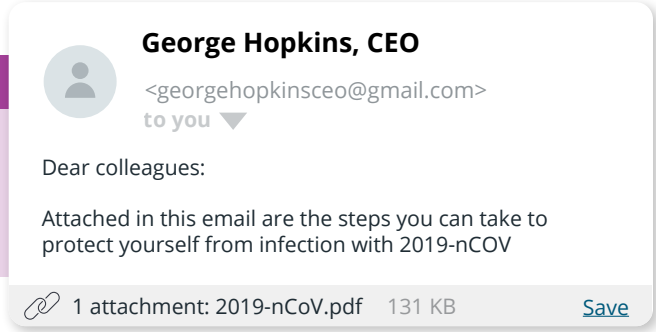


3. Safety measures turned malicious

This phishing attack impersonates a coronavirus specialist from the World Health Organization to trick victims with two malicious options. The email urges the victim to download a malicious file disguised as a safety document.

4. Internal organization alert

This phishing attack takes a corporate approach by impersonating a company's president to deliver an attachment disguised as tips to prevent infection. The attachment is designed to infect an employee's machine with malware.



Centers for Disease Control and Prevention
Flu pandemic warning.

CDC Centers for Disease Control and Prevention

Dear Sir/Madam,

The CDC has updated new cases around your city and is available at:
https://www.cdc.gov/coronovirus/20199-nCOV

5. New cases in your area

This attack preys on the fears of Coronavirus spreading near the victims' location. Disguised as a CDC alert, this phishing email tricks victims into clicking a malicious link by offering an updated list of new cases of the virus documented near them.

6. The donation scam

Like the tried-and-true donation scams used after natural disasters, this phishing attack solicits donations to fight the spread of the coronavirus. The attack imitates a CDC emergency outreach email and asks victims to deposit money into a Bitcoin account.

CDC HELTH emergency coronavirus (2019-nCOV)

Hello sir/ma'am
,
CDC has established a systsem to co-ordinate a public health response to check mate this virus. Fudning is expensive and we plead for your good will donation.

Please find our BitCoin account below for your donation.
Click here

From Dr Li Wei [redacted]
Subject **CORONA-VIRUS AFFECTED COMPANY STAFF** 24/2/20, 5:32 pm
To Recipients [redacted]

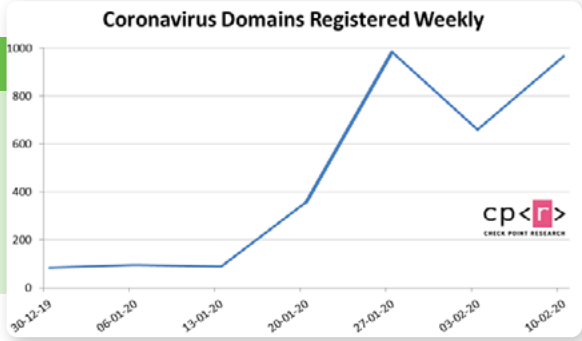
TO WHOM IT MAY CONCERN Find the attached file of victims and predicting victims of corona Virus as at 22/02/2020. This list contains pictures,countries,names and companies affected. Dr Li Wei 26 Shengli St, Jiang'an District, Wuhan, Hubei, China +862782814009 Hubei http://www.zxhospital.com/

7. Information from the source

In this coronavirus phishing attack, the cybercriminal impersonates a doctor from The Central Hospital of Wuhan to play on victims' fears, lend credibility to the email and convince the victim to download a malicious attachment.

8. Coronavirus domains

Along with the phishing tactics above, one of the largest concerns facing cybersecurity researchers is the massive increase in coronavirus-themed domain registrations. Many suspect that these coronavirus-related domains will be used for phishing attempts like those listed above.



!!! Buy coronavirus cure !!!
Click here

9. Fake product scam

Beyond the coronavirus phishing threats listed above, the SEC is warning consumers of investment scams related to products claiming to prevent, detect or cure coronavirus. Future phishing attacks may leverage this same tactic.

Sources: Mimecast, Sophos, MailGuard, Checkpoint