大成 DENTONS

Intelligence & Strategic Services

Corona Virus Update

Media coverage of COVID-19 appropriately continues to accelerate. At the same time, communication around the global virus status has created an opportunity for fraudsters to take advantage of people's desire to quickly access information. Some potential schemes are as follows:

Counterfeit Products

Criminals will use this opportunity to create counterfeit or defective products that are in high demand, such as safety masks, hand sanitizer, cleaning products, and detection product. Everyone should be aware that when there are supply shortages or crises, criminal organizations will try to sell counterfeit items that at best may be ineffective, or at worst, harmful to use.

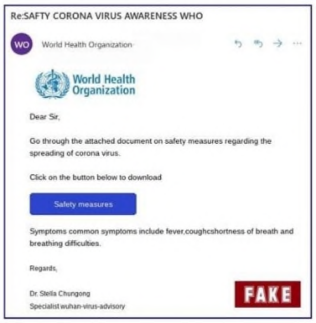
Fake Solicitations

Fraudulent charity schemes may come in many forms such as phishing or and soliciting donations on the phone for victims in different countries. Anytime there is a crisis, fraudulent charity schemes are created to take advantage of both individual and organizational donations.

Phishing

Malicious email related to news about the Coronavirus has started to appear and is predicted to increasingly become a target of phishing attacks. Recently, malicious phishing email claiming to be from the World Health Organization was received prompting recipients to provide their passwords. We have seen messages reporting COVID-19 infection occurrences or claims about future impacts on the global economy. These subject lines are designed to grab attention and get you to click on malicious links.

Here is an example:



Re:SAFTY CORONA VIRUS AWARENESS WHO

World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

Fraudulent Websites

As public desire for information on COVID-19 virus has accelerated, more than 4000 new websites have been created with roughly half of them being malicious in nature. Many of these websites have embedded legitimate mapping software that is used by Johns Hopkins to track the spread of the virus, but combined it with malware. Visiting the websites infects your computer with a program which could ex-filtrate a variety of sensitive data.

When seeking information, use known sources or links. Links to few key, legitimate websites are below.

- WHO - https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen
- CDC - https://www.cdc.gov/coronavirus/2019-ncov/index.html
- Johns Hopkins University Map - https://systems.jhu.edu/
- Canada's public health updates: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19.html
- UK government updates: https://www.gov.uk/government/topical-events/coronavirus-covid-19-uk-government-response
- UK NHS information: https://www.nhs.uk/conditions/coronavirus-covid-19/
- EU public health information: https://ec.europa.eu/health/coronavirus_en
- Australian Department of Health: https://www.health.gov.au/news/health-alerts/novel-coronavirus-2019-ncov-health-alert

Protect your information! We recommend taking extra precautions as more of us transition to remote work.

- Always be wary of messages requesting account verification, confirmation or upgrade, payment or personal information such as your username, passwords, Social Security number, or credit card information.
- Law firms, financial institutions and others are frequently targeted by malicious actors who will attempt to acquire personal information about staff or clients through email and over the phone. Please be aware that these attempts often seem legitimate.
- Carefully review messages to validate the sender / source, and do not click on unknown links or attachments.
- Ask questions, trust your instincts, and if things seem off, don't be afraid to take a message and follow-up later. Attackers will frequently use a sense of urgency to elicit the victim into making a risky decision.
- Ensure that your computer is protected with a strong password and the password is not disclosed to any third parties.
- Documents should not be forwarded to your personal email account. You must not use your personal email account for any work related matters.
- If you have a doubt, contact your IT or security team.

John Koski
Global Chief
Legal Officer

Karl Hopkins
Global Chief
Security Officer