CYBER SECURITY ADVISORY – CORONA PHISHING

March 17, 2020

EXECUTIVE SUMMARY

You are receiving this advisory to make you aware of increased Phishing and malicious activity using the COVID19/ CORONA Pandemic as a lure.

It is strongly recommended that organizations follow email hygiene/ phishing best practices to defend against this increased activity.

HOW DOES THIS INCIDENT AFFECT MY ORGANIZATION?

Phishing and fraudulent emails remain a prominent way in which attackers can gain access and compromise security; malicious parties can try to steal credentials and make victims think the emails come from a trusted party and attempt to convince them to click on malicious links or malicious attachments.

We are aware of phishing scams using the Corona pandemic as a lure and of sophisticated threat actors including multiple state backed APT groups using these phishing emails as well.

WHAT SHOULD I DO?

As soon as possible, forward this notification to your cyber security personnel or IT partners for immediate action.

TECHNICAL DETAILS:

Threat actors are known to be sending alerts that appear to be from the World Health Organization, pose as official communications from University personnel, purport to have information on the spread of Coronavirus, as well as emails that target personnel who are working from home.

In addition to this, we are also aware of recently registered domains "selling" masks and sanitizer, and scams featuring “doctors” pretending to work for the Centers for Disease Control and Prevention (CDC) asking people to download attachments for more information or to donate bitcoin.

We have some indicators of compromise, you can receive these by emailing cyberadvice@ontario.ca , with the subject line “corona ioc”

CYBER SECURITY ADVISORY – CORONA PHISHING
RECOMMENDED ACTION:

The Canadian Anti Fraud Centre provides educational material and guidance on various fraudulent activities including phishing and related scams, more information can be found at the following site: http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/types/phishing-hameconnage/index-eng.htm

We would also recommend reviewing the attached Malware and Security preparedness recommendations document.

FOR FURTHER INFORMATION

If you find any of the indicators of compromise (IOCs) on your networks, have related information or any questions, please contact cyberadvice@ontario.ca

NO WARRANTY
This Cyber Advisory contains third party content and links. CS CoE does not control or maintain third party links and makes no representation or warranty that the link will still work when you click on it or the service or content is useful, appropriate, virus-free or reliable. It is your responsibility to determine whether you want to follow any link or agree to receive or rely on any service or content that is made available to you.

Cyber Security CoE is providing information about a known threat for potential use at the sole discretion of recipients to protect against cyber threats. This notification is provided to help health care organizations enable cyber preparedness and resilience.

DEFINITIONS:
Cyber Security Threats or Incidents are events that may present risk to the security (i.e. confidentiality, availability or integrity) of an organization's information assets, systems and networks.

- Cyber Security THREAT Advice is issued when NO ACTIVE EXPLOITS are observed. Purpose of the advice: to enable organizations to prepare for and mitigate cyber threats.
- Cyber Security INCIDENT Advice is issued when an ACTIVE EXPLOIT is observed. Incident advice is time sensitive to inform partner organizations of an ongoing cyber incident for a timely response and remediation.