Cybersecurity and the Coronavirus

March 12, 2020

This week, the Department of Homeland Security, U.S. Secret Service issued guidance around coronavirus-related phishing scams. They identified phishing emails “the fraudulent practice of sending emails purporting to be from reputable companies in order to entice individuals to reveal personal information, such as passwords and credit card numbers” as the primary alert to be aware of.

Excerpt from Secret Service Issues COVID-19 (Coronavirus) Phishing Alert:

“Cybercriminals are exploiting the coronavirus through the wide distribution of mass emails posing as legitimate medical and or health organizations,” the guidance reads. “In one particular instance, victims have received an email purporting to be from a medical/health organization that included attachments supposedly containing pertinent information regarding the coronavirus. This led to either unsuspecting victims opening the attachment, causing malware to infect their system, or prompting the victim to enter their email login credentials to access the information resulting in harvested login credentials.”

Read the full page alert here.

We will continue to monitor and update on any further alerts and guidance. If you have any questions, feel free to contact us at info@rightsize-solutions.com