United States Secret Service [INFO]

March 4, 2020

[INFO] Information Only Alert – GIOC Reference #20-004-I
TLP Green

Coronavirus Scams

Criminals are opportunists, and as seen in the past, any major news event becomes an opportunity for groups or individuals with malicious intentions. The Coronavirus is no different. In fact, the Coronavirus is a much more potent opportunity for enterprising criminals because it plays on one of the basest human conditions...fear. Fear can cause normally scrupulous individuals to let their guard down and fall victim to social engineering scams, phishing scams, non-delivery scams, auction fraud scams, etc.

Numerous international sources from Asia, Africa, Australia, and Europe are reporting a rise in Coronavirus scams, and a rise in the number of incidents in the United States is expected. Brief details of the associated Coronavirus scams being encountered are below:

- Phishing Scams
- Social Engineering Scams
- Non-delivery Scams

Phishing scams have become ubiquitous through email communication and commerce. Cyber criminals are exploiting the Coronavirus through the wide distribution of mass emails posing as legitimate organizations such as the Center for Disease Control (CDC) or World Health Organization (WHO). In one particular instance, victims have received an email purporting to be from the WHO with an attachment supposedly containing pertinent information regarding the Coronavirus. This leads to either unsuspecting victims opening the attachment causing various types of malware to infect their system, or prompting the victim to enter their email login credentials to access the information resulting in harvested login credentials. These incidents enable further instances of cyber-enabled financial crime such as Business Email Compromise (BEC), PII theft, ransomware, account takeovers, etc. Another side effect of the Coronavirus is increased teleworking, which furthers the reliance on email for communication adding yet another multiplier to these email fraud schemes. More of these incidents are expected, and increased vigilance regarding email communication is highly encouraged.

Another emerging fraud scheme exploiting the Coronavirus is using social engineering tactics through legitimate social media websites seeking donations for charitable causes related to the virus. Criminals are exploiting the charitable spirit of individuals, seeking donations to fraudulent causes surrounding the Coronavirus. Increased caution should be exercised when donating to causes tied to Coronavirus relief.

A third fraud scheme surrounds non-delivery scams. Essentially, criminal actors are advertising in-demand medical supplies for sale to be used to prevent/protect against the Coronavirus, i.e. medical masks, gloves, disinfectant, etc. The criminal enterprise will demand upfront payments or initial deposits, then abscond with the funds and never complete delivery of the ordered product. Increased caution and vigilance while purchasing these supplies should be exercised.

GLOBAL INVESTIGATIVE OPERATIONS CENTER
WASHINGTON, D.C.

[INFO] - Indicates informational or educational content.