PRESS RELEASE

United States Secret Service
Department of Homeland Security

March 9, 2020
CMR 04-20

Secret Service Issues COVID-19 (Coronavirus) Phishing Alert

WASHINGTON - Criminals are opportunists, and as seen in the past, any major news event can become an opportunity for groups or individuals with malicious intentions. The Coronavirus is no different. In fact, the Coronavirus is a prime opportunity for enterprising criminals because it plays on one of the basic 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, and auction fraud scams.

The United States Secret Service is proactively taking steps to alert the public about the types of email scams associated with the Coronavirus. The Secret Service's Global Investigative Operations Center (GIOC) reports the subsequent email scams:

"Phishing" is 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. Phishing scams have become ubiquitous through email communication and ecommerce. Cyber criminals are exploiting the Coronavirus through the wide distribution of mass emails posing as legitimate medical and or health organizations. 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 lead 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. This type of incident enables further occurrences of cyber enabled financial crimes such as Business Email Compromise (BEC), PII theft, ransomware and account takeovers. 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 charitable organizations.

A third fraud scheme surrounds non-delivery scams. Essentially, criminal actors advertise as an in-demand medical supply company that sells medical supplies that can be used to prevent/protect against the Coronavirus. The criminal enterprise will demand upfront payment or initial deposits then abscond with the funds and never complete delivery of the ordered products.

Quick Tips:

- **Phishing Emails / Social Engineering** – Avoid opening attachments and clicking on links within emails from senders you do not recognize. These attachments can contain malicious content, such as ransomware, that can infect your device and steal your information. Be leery of emails or phone calls requesting account information or requesting you to verify your account. Legitimate businesses will never call you or email you directly for this information.
- Always independently verify any requested information originates from a legitimate source.
- Visit websites by inputting the domain name yourself. Business use encryption, Secure Socket Layer (SSL). Certificate "errors" can be a warning sign that something is not right with the website.

The United States Secret Service will continue leading the charge to combat cyber-enabled financial crimes. To learn more about the Secret Service's Investigative Mission please visit us at: www.SecretService.gov

For questions concerning this release, please contact the U.S. Secret Service Office of Communication and Media Relations at 202-406-5708.