**COVID-19 (Coronavirus) Related Cyber Scams**

**Phishing**

Mass emails posing as legitimate medical and/or health organizations, some with attachments supposedly containing pertinent information regarding Coronavirus.

* Avoid opening attachments and clicking on links within emails from senders you do not recognize
* Be leery of emails or phone calls requesting account information or requesting you to verify your account

**Social Engineering**

Exploiting the charitable spirit of individuals, seeking donations on legitimate social media websites to fraudulent causes surrounding the Coronavirus.

* Always independently verify a charity’s authenticity
* Visit websites by inputting the domain name yourself

**Non-Delivery Scams**

Criminal actors will demand upfront payment or initial deposits for in-demand medical supplies then abscond with the funds and never complete delivery of the ordered products.

* Use trusted vendors and merchants
* Ignore online offers for vaccinations and home test kits