The novel coronavirus pandemic presents an opportunity for malicious actors to conduct spearphishing campaigns, financial scams, and disinformation campaigns via social media to collect sensitive information, steal money via fake donation websites, spread false information, and deliver malware to victims.

Several spearphishing campaigns since January have falsely represented various healthcare organizations, including the U.S. Centers for Disease Control and Prevention and the World Health Organization. In many cases, victims receive coronavirus-themed emails requesting the victim to open an attachment or click on a link to obtain details about the coronavirus. Once a victim clicks on the attachment or link, they are directed to a malicious website requesting the victim to enter login credentials.

Law enforcement agencies have observed campaigns wherein victims received hoax emails from what appear to be the CDC requesting donations via Bitcoin to fund an “incident management system” in response to the coronavirus pandemic. Agencies also observed in February a spearphishing campaign targeting Japan-based Internet users with emails that appeared to provide information relating to coronavirus prevention. The emails included malicious Microsoft Office files that upon opening would initiate the download of a sophisticated Trojan known as Emotet.

U.S. officials have released statements advising Russia is likely behind coronavirus disinformation campaigns that are being spread via social media. Reports indicate thousands of Twitter, Facebook, and Instagram accounts have been used to spread false information about the coronavirus pandemic.