NEW YORK CITY POLICE DEPARTMENT

Scams and Fraud Campaigns Exploiting COVID-19 likely to Continue

April 20, 2020

The COVID-19 pandemic has created an environment ripe for fraudulent activity, with threat actors leveraging fears of the virus to perpetrate a variety of malicious and criminal exploitation. Observed scams and fraud have included selling fraudulent personal protective equipment (PPE), hawking fake cures and tests, spreading disinformation, phishing campaigns, and other related scams. The Intelligence Bureau (IB) assesses that this activity will continue, and it will potentially pivot to leverage changing government responses to the pandemic and shifting needs for supplies. Additionally, the IB assesses that cyber-enabled crime will also evolve to prey upon the public's need to remain updated on the stream of ever-changing COVID-19-related information and may shift from COVID-19 themed outbreak to recovery lures.

- Between January 1 and April 15, 2020, the Federal Trade Commission (FTC) has received more than 18,235 reports of scams or fraud related to COVID-19, reportedly costing victims more than $13.44 million.[1]

Law Enforcement and Private Sector Response

Recognizing the breadth of the threat, law enforcement at the federal, state, and local levels, and international partners, are sharing resources and forming partnerships to combat COVID-related criminal activity.

- On April 15, HSI announced a nationwide effort to investigate and combat COVID-19 fraud in partnership with CBP, the FDA, the U.S. Postal Inspection Service, the Secret Service, the IRS, the FBI, and the Five Eyes Law Enforcement Working Group. Multiple federal agencies have released public alerts related to identified scams and fraudulent schemes and products.
- Private sector partners—to include internet providers, social media companies, cybersecurity firms, and financial institutions—are proactively removing malicious websites and accounts and working with law enforcement to detect COVID-19-related attempts to defraud.
- DOJ has encouraged Americans to report COVID-19 related fraud to the National Center for Disaster Fraud (NCDF) and the Attorney General instructed US Attorneys to prioritize the investigation and prosecution of COVID-19-related fraud schemes.

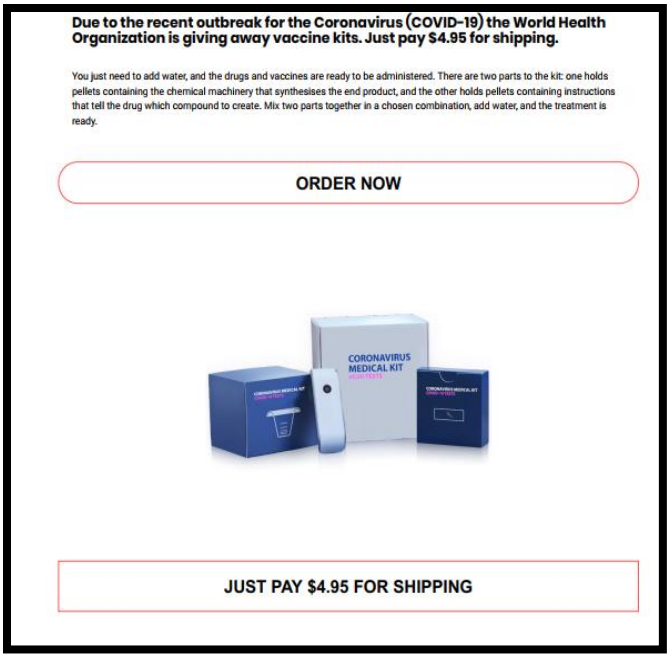
Fraudulent Protective and Testing Equipment

The IB assesses that, as the COVID-19 pandemic extends into the summer and potentially returns in additional waves, malicious actors will continue to sell fake personal protective equipment (PPE) to both individuals and organizations. Scams involving PPE sales target hospitals, health care unions, and government agencies globally. The Federal Bureau of Investigation (FBI) warned that healthcare facilities and professionals may be at an increased risk from fraudulent PPE, as scammers capitalize on fears around the stressed supply chain and the urgent need for protective gear.[2] Furthermore, the growing need for testing equipment and new and updated testing methods presents a vulnerability for fraudulent sales and scams.

- A deal brokered by a California healthcare union that sought to facilitate the sale of 39 million N95 face masks to hospitals in California and New York turned out to be fraudulent. The fraud was detected when

one of the buyers complained it had not received its order of six million masks. Federal authorities are investigating a purported Australia-based broker and a supplier in Kuwait who were communicating with a middleman in Pittsburgh; the middleman was unaware of the scam but stood to potentially make $9 million off the deal.[3]

- Opportunistic actors have also sought to push fake tests and cures for COVID-19, both online and in person.[4] Some vendors on dark web market places are selling blood and saliva of alleged COVID-19 victims.[5] On March 22, the Department of Justice (DOJ) filed a civil complaint against the operators of the website coronavirusmedicalkit.com, which purports to sell World Health Organization vaccine kits. The operators of the site allegedly used victims' credit card information to conduct wire fraud.[6]



Screenshot of Coronavirusmedicalkit.com from DOJ Complaint

- In mid-March, Europol and Interpol, in conjunction with authorities and financial institutions in Germany, Ireland, the Netherlands, and the UK, foiled a scam to sell what turned out to be nonexistent face masks to health agencies for millions of euros. In an elaborate scheme, threat actors created a malicious website masquerading as legitimate company in Spain and contacted the potential buyers using compromised email addresses from the legitimate company, asking for payment upfront but never delivering the supplies of facemasks. Allowing one sale to fall through, the threat actors created a second malicious website made to look like a Dutch company and began the process again. Over 2 million euros in transactions were made to facilitate the purchase, with a sizeable portion destined for a Nigerian bank account; the transactions were frozen before the money reached the ultimate destination.[7]

- DHS Homeland Security Investigations (HSI) reports 130 investigations nationwide to date, nine arrests, the seizure of over $3 million in illicit proceeds, and over 225 shipments of "mislabeled, fraudulent, unauthorized, or prohibited COVID-19 test kits, treatment kits, homeopathic remedies, purported anti-viral products, and personal protective equipment."[8]

Cyber-Enabled Scams

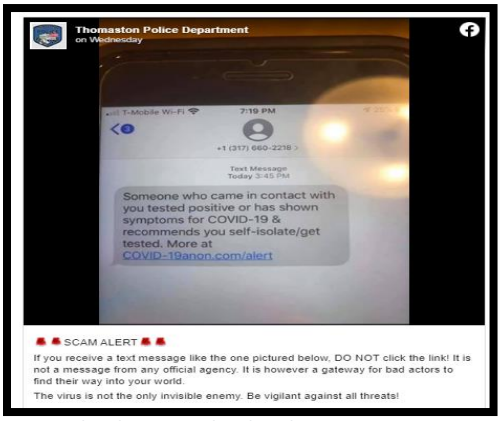
Threat actors around the world have flooded the internet with COVID-19-themed phishing scams in attempts to capitalize on fears of the virus for financial gain, espionage, disinformation campaigns, and other malicious activities. The IB assesses that malicious actors will continue to exploit new developments in the COVID-19 pandemic as fodder for future phishing scams.

- COVID-19-related phishing campaigns include emails impersonating healthcare professionals and organizations such as the CDC, which promise information on COVID-19, then send users to malicious

websites that can steal login credentials and plant malware. The forms of malware employed include ransomware, spyware, and other types that steal or destroy data. In a recent push to curb COVID-related scams, HSI disabled over 11,000 COVID-19 domain names used for these types of cyberattacks and other fraudulent purposes.[9] In March 2020, researchers identified a phishing email campaign in which the attacker pretends to be from the World Health Organization (WHO) and attempts to lure the victim into downloading an attached e- book claiming to contain information on how to protect against the virus; however, the e-book is actually a malicious file that steals the victim's information.[10]

- Exploiting newly-passed federal relief and stimulus packages, some campaigns claim to provide links for individuals to sign up for government assistance, instead stealing personally identifiable information (PII). In some cases, threat actors posing as Department of Treasury employees email potential victims, offering relief checks allegedly issued by the World Bank and the World Health Organization and requesting name, home address, birthday, and other PII. [11]

- Mobile phone phishing threats over text messages, a.k.a. SMShing threats, have also been on the rise, with threat actors using malware-laden links in messages. In some cases, the link directs the victim to malicious websites that prompt them for name, email, passwords for other accounts, and bank account information. On April 15, the Thomaston Police Department in Maine alerted the public to a SMShing scheme in which the fraudster attempts to scare the victim into clicking on a potentially malicious link. The text message has an urgent tone, claiming the recipient was in contact with an individual who had tested positive or had shown symptoms of COVID-19, and pretends to offer more information on self-isolating and testing through an innocuous looking but ultimately malicious link. [12] [13]



Facebook posting by the Thomaston Police Department of a SMShing scam.

- An April 13 alert by the FBI warned of Business Email Compromise (BEC) schemes targeting state agencies and healthcare, in which the fraudster tricks the organization into paying an invoice to the fraudster's account rather than to the legitimate vendor's account.[14] The FBI identified a recent example of BEC in which a financial institution was allegedly emailed by the CEO of a company requesting the date for a transfer of $1 million be moved up and the recipient account be changed due to COVID-19. The perpetrator used an email address that was only one letter off from that of the CEO. Organizations should be wary of such requests and verify the validity of the email address and reach out to a known point of contact via a previously used method of communication.[15]

- COVID-19 related blackmail scams have also been circulating in which the fraudster contacts the victim by email and threatens to infect the victim's family with COVID-19 if s/he does not pay the fraudster money or cryptocurrency.[16] Based on the researched dataset, this type of fraud has had limited success.[17]

Tips on Identifying COVID-19 Themed Scams and Reporting Resources

- Be wary of suspicious emails and text messages. Verify that these are from a known or valid source, think before clicking on any links, and be aware of suspicious attachments.
    - Suspicious email content may include unexplained urgency, last-minute changes in instructions or information, and changes in typical communication platforms. Verify any changes with a trusted contact prior to acting on suspicious messages.
    - Watch for slight misspellings of domain name URLs in the address or content of email messages. DHS recently highlighted spoofed URLs such as "corona-virus-business-update," "covid19-advisory," or "cov19esupport".
- Ensure your computer is running updated anti-malware software.
- Exercise due diligence before donating to charitable solicitations or purchasing PPE.
- If you receive a scam call, hang up. If the calls persist, report the incident to one of the authorities recommended by the DOJ.
- Additional resources regarding COVID-19-related fraud: FTC: COVID-19 Scams; HHS: COVID-19 Fraud Alerts; CISA: Defending Against COVID-19 Cyber Scams; COVID-19 Exploited by Malicious Cyber Actors

DOJ advises individuals who may be the victim of a scam or attempted fraud involving COVID-19 to:

- Contact the National Center for Disaster Fraud Hotline at 866-720-5721 or via email at disaster@leo.gov
- If it's a cyber scam, submit a complaint through https://www.ic3.gov/default.aspx
- Individuals can also contact their U.S. Attorney's Office, or state or local authorities.

[1] Paul Witt, "COVID-19 scam reports, by the numbers," Federal Trade Commission 15 April 2020, https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers?utm_source=govdelivery

[2]" FBI Warns Health Care Professionals of Increased Potential for Fraudulent Sales of COVID-19-Related Medical Equipment," FBI, 27 March 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-health-care-professionals-of-increased-potential-for-fraudulent-sales-of-covid-19-related-medical-equipment

[3] Bruce Golding, "Feds investigate coronavirus scam over deal for 39 million face masks," NY Post, April 12, 2020, https://nypost.com/2020/04/12/feds-investigate-coronavirus-scam-over-deal-for-39-million-face-masks/

[4] "FBI Warns of Emerging Health Care Fraud Schemes Related to COVID-19 Pandemic," FBI, 13 April 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-emerging-health-care-fraud-schemes-related-to-covid-19-pandemic

[5] David Gilbert, "Scammers Are Selling 'Blood and Saliva From a Coronavirus Survivor' on the Dark Web," Vice, 7 April 2020, https://www.vice.com/en_us/article/m7qdy4/criminals-are-selling-blood-and-saliva-from-a-coronavirus-survivor-on-the-dark-web

[6] "Justice Department Files Its First Enforcement Action Against COVID-19 Fraud," Department of Justice, March 22, 2020, <https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud> (accessed April 12, 2020).

[7] EUROPOL Press Release, "Corona Crimes: Multi Million Face Mask Scam Foiled by Police Across Europe", April 14, 2020, https://www.europol.europa.eu/newsroom/news/corona-crimes-multi-million-face-mask-scam-foiled-police-across-europe

[8] Amanda Lindsley "Homeland Security Investigations to start targeting COVID-19 fraud," WAFB, 15 April 2020, https://www.wafb.com/2020/04/15/homeland-security-investigations-start-targeting-covid-fraud/

[9] Amanda Lindsley "Homeland Security Investigations to start targeting COVID-19 fraud," WAFB, 15 April 2020, https://www.wafb.com/2020/04/15/homeland-security-investigations-start-targeting-covid-fraud/

[10]" Cybercriminals weaponize the World Health Organization name to lure phishing victims" SC Magazine, March 18, 2020, https://www.scmagazine.com/home/email-security/cybercriminals-weaponize-the-world-health-organization-name-to-lure-phishing-victims/

[11] Secret Service Issues COVID-19 (Coronavirus) Phishing Alert, USSS, March 2020, https://www.secretservice.gov/data/press/releases/2020/20-MAR/Secret_Service_Coronavirus_Phishing_Alert.pdf.

[12] "FBI and Secret Service Working Against COVID-19 Threats" FBI and USSS Press Release, April 15, 2020 https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats.

[13]Thomaston Police Department, April 15, 2020, https://www.facebook.com/ThomastonPolice/

[14] "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic," FBI, 13 April 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic

[15] "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic," FBI, 13 April 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic

[16] "COVID-19 has wiped out 33% of cryptocurrency scammers' revenue but that's not the whole story," Chainalysis, https://blog.chainalysis.com/reports/covid-19-cryptocurrency-scams

[17] "COVID-19 has wiped out 33% of cryptocurrency scammers' revenue but that's not the whole story," Chainalysis, https://blog.chainalysis.com/reports /covid-19-cryptocurrency-scams