Consumers are scammed by cybercriminals who are taking advantage of their fears about Coronavirus

As the Coronavirus, also known as COVID-19, continues to infect people all over the world, fraudsters are taking advantage of people's fear and ignorance about the virus to sell fraudulent goods and spread phishing emails, messages, and social media postings that target consumers and individuals.

The phishing emails and social media posts promote awareness, preventative suggestions, and false information regarding Coronavirus cases, with some scams requesting donations for victims or offering advice on unproven therapies in order to sell spurious items.

One phishing email scam poses as official World Health Organization Coronavirus material (WHO). The false email, on the other hand, spreads malware that installs the FormBook data-stealing Trojan. According to Bleeping Computer, after being executed, the virus will download an encrypted file from https://drive.google.com, decrypt it, and then inject the malware into the genuine Windows wininit.exe process to avoid detection.

Fake coronavirus-related websites are also being built up, promising natural and pharmaceutical "cures," vaccines, testing kits, face masks, and other products in short supply at extremely low costs. Fake websites steal credit card information and put people's health in jeopardy by selling counterfeit and low-quality medical supplies.

Due to the coronavirus, major eCommerce platforms such as Amazon and eBay, as well as third-party sellers, have been unwittingly offering products that may be damaged, worn, expired, or hazardous, yet are in high demand.

According to Dharmesh Mehta, Amazon's vice president of international customer trust, more than one million products listed by merchants making fraudulent claims about the Coronavirus have been removed. According to Forbes, Mehta revealed his identity in answer to questions from the Congressional Subcommittee on Consumer Protection & Commerce at a hearing on bogus and dangerous products. (1)

According to Jason Glassberg, co-founder of cybersecurity firm Casaba Security, online retailers should be cautious of frauds that may target them using payment apps like Venmo

and Zelle. (2) The "canceled payment scam" occurs when an online criminal purchases goods, pays for them with a payment app and then cancels the payment before it is processed a few days later after the thing has already been dispatched.

Individuals should be careful and wary of online scams and cyber-attacks related to the Coronavirus outbreak, according to the US Cybersecurity and Infrastructure Security Agency (CISA).

"Cybercriminals may send emails containing harmful attachments or links to bogus websites in an attempt to dupe users into disclosing sensitive information or donating to bogus charities or causes." "Handle any email with a COVID-19-related subject line, attachment, or links with caution, and be wary of COVID-19-related social media requests, texts, or phone calls," the agency warns. (3)

Individuals are encouraged to take the following online measures, according to the agency:

- Be aware of email attachments and avoid clicking on links in unsolicited emails. For further information, see Avoiding Social Engineering and Phishing Scams and Using Caution with Email Attachments.

- For up-to-date, fact-based information regarding COVID-19, turn to reliable sources such as authentic government websites.

- Do not send personal or financial information over email, and do not react to requests for such information via email.

- Before making a donation, be sure the charity is legitimate. For additional information, go to the Federal Trade Commission's page on charity scams.

- For more information, see CISA Insights on Risk Management for COVID-19.

(1) forbes.com

(2) finance.yahoo.com

(3) us-cert.gov