RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type: **Awareness** | Watch | Warning

Coronavirus Stimulus Scams Surface Targeting Members

Date: March 31, 2020

Risk Category: Fraud, Scams, Deposit Account Services

States: All

Fraudsters have been quick to deploy scams involving the coronavirus stimulus package that would include direct payments to individuals and married couples filing jointly. Many variations of the scam could impact you.

Details

Fraudsters haven't wasted any time with scams related to the coronavirus. In response to the federal stimulus package, the Better Business Bureau (BBB) reported that fraudsters have deployed a variety of scams involving coronavirus stimulus checks. The BBB Scam Tracker has received several reports of coronavirus scams where individuals are contacted through text messages, social media post /messages, or phone calls.

One version of the scam targets seniors through a Facebook post informing them that they can get a special grant to help pay medical bills. The link within the post takes them to a bogus website claiming to be a government agency called the "U.S. Emergency Grants Federation" where they are asked to provide their Social Security Number under the guise of needing to verify their identity. In other versions, fraudsters claim individuals can get additional money – up to $150,000 in some cases. The victims are asked to pay a "processing fee" to receive a grant.

In North Carolina, there are several reports of a coronavirus scam in which potential victims received phone calls. Fraudsters told the victims they qualified for a $1,000 to $14,000 coronavirus stimulus payment; however, they must first pay a processing fee.

Coronavirus direct payments will likely be in the form of direct deposits or through U.S. Treasury checks. Fraudsters may look to seize this opportunity to create counterfeit U.S. Treasury checks to use in their scams. Knowing when the stimulus checks will be issued, fraudsters could steal U.S. Treasury checks out of the mail and attempt to cash them at a credit union after opening an account. This was a common occurrence in the aftermath of Hurricane Sandy as fraudsters counterfeited and forged U.S. Treasury checks representing the Federal Disaster Assistance checks.

Fraudsters may also attempt to scam you into providing their account number under the pretense of direct depositing the stimulus payment to their account.

Your feedback matters!

Was this RISK Alert helpful?

Vote Yes | Vote No

RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type: **Awareness** | Watch | Warning

Coronavirus Opens Doors to Scams

Date: March 17, 2020

Risk Category: Fraud, Scams, Cybersecurity

States: All

The Coronavirus (COVID-19) has been a windfall for fraudsters as they exploit the global thirst for knowledge on the virus. Fraudsters have launched Coronavirus-themed phishing attacks to deliver malware – typically credential-stealing banking Trojans. The phishing emails purport to be from the Centers for Disease Control (CDC) and the World Health Organization (WHO). Fraudsters have also created fake websites to exploit Johns Hopkins University's interactive Coronavirus dashboard to spread malware.

Details

Fraudsters are exploiting the global thirst for knowledge about the virus by launching Coronavirus-themed phishing attacks to spread credential stealing malware. The emails, which contain an infected attachment or a link to a malicious website, are made to appear like they come from the CDC or the WHO. The WHO posted an article on its website warning users of this scam.

Fraudsters have also exploited Johns Hopkins University's interactive Coronavirus dashboard containing an interactive map that tracks Coronavirus statistics by region. Cybersecurity firms have identified several fake Coronavirus interactive maps that infect user devices with credential-stealing malware. Fraudsters are circulating links to these malicious websites containing Coronavirus maps through social media and phishing emails.

Security blogger Brian Krebs reported several Russian cybercrime forums started selling infection kits that exploits John Hopkins University's interactive Coronavirus dashboard as part of a Java-based malware deployment scheme.

There have also been reports of other Coronavirus-themed phishing campaigns aiming to spread malware, including:

- Coronavirus advice-themed phishing emails purporting to provide advice on how to protect against the virus. The emails might claim to be from medical experts near Wuhan, China where the Coronavirus started.
- Workplace policy-themed phishing emails about Coronavirus targeting an organization's employees. For example, the emails may purport to come from the organization's HR department alerting employees of a new pandemic policy.