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. Credit unions should warn employees and members.

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.