RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Coronavirus Opens Doors to Scams

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.

Date: March 17, 2020

Risk Category: Fraud, Scams, Cybersecurity

States: All

Share with:

- ☐ Branch Operations
- ☐ Executive Management
- ☐ IT
- ☐ Marketing
- ☐ Risk Manager

Your feedback matters!

Was this RISK Alert helpful?

Vote Yes | Vote No

Coronavirus Opens Doors to Scams

Risk Mitigation

Credit unions should consider the following loss controls:

- Conduct phishing-themed security training for all staff.
- Warn employees of the Coronavirus-themed phishing scams providing clear instructions to not open attachments or click on links.
- Alert members of this scam and other scams through text alerts, email, and newsletters as well as posting articles on your website.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive risk and compliance resources to assist with your loss control efforts. The Protection Resource Center requires a User ID and password.

- RISK Alert: Coronavirus Outbreak Requires Precautionary Workplace Measures
- RISK Alert: Increased Coronavirus Infections Leads to Preparing Pandemic Response Plans
- The Rise of Social Engineering Fraud Risk Overview

Beazley cyber insurance policyholders can also access other resources at www.beazleybreachsolutions.com (User ID / Password required). Beazley resources include interactive online training on phishing and social engineering. In addition, Beazley policyholders can receive a discount on additional cybersecurity tools and training from KnowBe4 and FireEye.

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for resources & checklists
- Webinars and Education
- RISK Alerts Library
- Report a RISK Alert

The Protection Resource Center requires a User ID and Password.

Facing risk challenges?

Schedule a free personalized discussion with a Risk Consultant to learn more about managing risk.

Interested in learning more about fraud, scams, and other emerging risks?

Contact CUNA Mutual Group's Risk & Compliance Solutions at **800.637.2676** or riskconsultant@cunamutual.com