2020 ISSUE #1

Hot Topics In Risk Management

Every day we hear from our insureds on the Risk Management Hotline, and we will be sharing some of those questions and answers with you.

Our Risk Management Team is here to help you minimize and mitigate professional medical liability risk.

MICA

Coronavirus Scams Targeting Physicians

Q: *I received an email from Centers for Disease Control (CDC) Incident Management System with a link to a list of new coronavirus cases in my city. Is this really from the CDC or is it phishing?*

A: Cybercriminals are capitalizing on the public's fear of Coronavirus Disease 2019 (COVID-19) and hope the public will hastily read official-looking, virus-related emails and click on embedded links to scam sites.

These emails may appear to be from the World Health Organization (WHO), CDC, or the state health department. The "regarding" line may include words such as "emergency," "alert", "act now," and/or "coronavirus. The body may state the organization is coordinating a domestic or international response, advising the reader to review a list of new cases in their city or read about a cure for COVID-19 by clicking on a link. The link may appear to be connected to the CDC or WHO websites, but the link could be directed to a phony webpage, made to look like an actual email service login page (e.g. Gmail or Outlook login pages). The phony login page requests your username and password. Once entered, cybercriminals can access true email service accounts, which might contain other emails with credit card numbers, account numbers, banking information, passwords, etc. The phishing emails may also solicit donations to fund response and relief efforts but allow malware to infect your computer or device.

Beware:

- The sender's email address, links, and websites appear legitimate, such as cdc-gov.org. Be careful to review against the official web address such as cdc.gov or who.int.
- The CDC and WHO do not usually send mass public emails or require login credentials to access public health information. Examine the site carefully before proceeding.
- The sender's name is official and recognizable but just as criminals can make telephone caller identifications look like government agencies or actual people, they can also put most anything in the "from" field.
- The emails often contain spelling and grammatical errors. Read your emails before clicking on links.
- If you enter your username and password before realizing the email is a scam, change your username and password immediately to prevent the criminals from accessing your actual email account.
- Delete emails that appear to be from a suspicious source and go directly to the CDC or WHO websites.

For more information call the MICA Risk Management Hotline 602.808.2137 or email rm_info@mica-insurance.com.