West Virginia Executive Branch
Privacy Tip

Coronavirus Scare Is the Perfect Cover for Fraudsters

The coronavirus—or COVID-19—has health care experts scrambling, and has caused global concern for health and well-being due to its rapid spread throughout many countries, including the United States.

A scare like this is the perfect opportunity for scammers and fraudsters to prey on well-intentioned people. Unfortunately, during this global health care concern, criminals are using the scare to execute scams and frauds in the name of providing information or products to ward off the risk of contracting COVID-19. It has become so widespread that the Michigan Attorney General recently issued a warning to consumers to be wary and protect themselves against frauds related to coronavirus.

In the warning, the AG explained that fake social media posts and online articles as well as emails with malicious links are being used to obtain personal information from individuals or to obtain credentials or implant malware onto unsuspecting users' computers. In addition, the fake articles might allege that someone in the neighborhood has contracted COVID-19 and ask for monetary donations to support the victim.

Consumers are being warned not to provide any personal information or money through these mechanisms and to be on high alert for these types of fraud. The AG cautions, "Do not fall for these scams. In fact, this is the perfect example of criminals preying on people's fears. Don't give a single piece of personal information to anyone reaching out to you regarding coronavirus."

This tip was shared from the Data Privacy + Cybersecurity Insider blog and is authored by Linn F. Freedman, chair of Robinson+Cole's Data Privacy + Cybersecurity Team.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.