Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 20 — Issue 14 | April 2, 2020

Rumor control, scams, fake vaccines and coronavirus-related malware

Public information officers (PIO) and public officials are struggling to manage the spread of misinformation about COVID-19. The Federal Emergency Management Agency (FEMA) created a webpage to help everyone distinguish between rumors and facts. The site is a trusted source of information the public can refer to if they need answers.

Several other federal agencies created pages to help people identify scams and cyberattacks related to the current pandemic. PIOs should consider listing them in their messaging as another way to protect people in their jurisdictions.

It didn't take long for criminal profiteers to start using COVID-19 for illegal gain. In fact, IBM says coronavirus-themed spam has increased 14,000 percent in 2 weeks.

There are no approved at-home tests nor are there any approved vaccines or drugs to "cure" COVID-19, yet they are being sold online. Several agencies are tackling this misinformation and fraud with websites listing known scams and providing instructions to report them:

- The Federal Trade Commission coronavirus page lists details about known scams and lists information on reporting scams.
- See the Food and Drug Administration's COVID-19 fraud page. It lists instructions for reporting fraudulent products.
- The FBI's page on COVID-19 fraud also has reporting instructions.
- USA.gov has a robust list of what federal agencies are doing to support COVID-19 response that includes a section on scams and fraud.

Hackers are using this as an opportunity to spread malware as well. The Cybersecurity and Infrastructure Security Agency (CISA) offers consumers tips to protect against scams and cyberattacks. StaySafeOnline.org also lists ways consumers can protect themselves from COVID-19 scams.

Cybersecurity experts interested in fighting COVID-19-related cyberattacks should take a look at the related article on page 3 of this week's InfoGram.

(Source: Various)

Minimizing stress during the COVID-19 crisis

First responders' duties are stressful under normal operations, but personnel is now faced with working conditions they may never have imagined seeing.

As PPE and supplies become difficult to find, coworkers get quarantined or become sick, and the reported numbers climb every day, it is very important to make time to destress and take care of your mental (and physical) health.

The International Public Safety Association (IPSA) provides some great suggestions in its blog post "10 tips for emergency responders, healthcare providers for managing stress during the COVID-19 crisis." The simple tips include exercise, spending time with pets, catching up on sleep, taking a break from the news cycle and above all

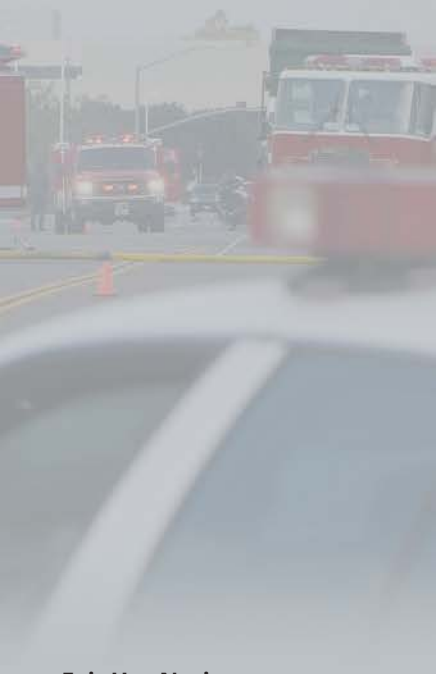
Highlights

U.S. Fire Administration

The U.S. Fire Administration operates the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC).

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.

Subscribe here



else talking about everything that is going on. Talking, either with family, coworkers, friends or a professional therapist is crucial to managing through your stress.

A recent PoliceOne.org article "Protecting the mental health of first responders during a pandemic" notes that while first responders regularly deal with members of the public out of control or panicky, the levels which we now see are well outside the norm. This only adds to the exhaustion and stress.

IPSA also has a set of infographics on stress and mental health care departmental management may consider printing and posting or handing them out to staff. It is especially important for leadership to keep tabs on their staff's stress levels and how they are managing and offer any assistance they can.

(Source: Various)

New tool helps planners weigh which projects are most beneficial

Many communities trying to prepare for disasters have so many infrastructure projects to update that it is difficult for decision makers to identify which to prioritize. Which will be most cost-effective? Which will do the most good?

Researchers at the National Institute for Science and Technology (NIST) developed the Economic Decision Guide Software (EDGe$) tool to give state, local and private sector planners an easy-to-use method of evaluating and comparing different community projects to improve resilience.

EDGe$ calculates the value of investments to include things like benefit-to-cost ratios, internal rates of return and returns on investment (whether a hazardous event occurs or not). By inputting important variables into EDGe$, community planners could reveal key economic insights about potential projects.

The metrics from each project, including one where no action is taken, are then laid out side-by-side so they can be easily compared. EDGe$ also factors in benefits that are not related to disasters, such as a project improving commuter traffic flow.

This web-based application can be a very useful tool for planners struggling with the cost-effectiveness of their list of resiliency projects.

(Source: NIST)

Webinar: Cost Recovery for COVID-19 Actions by Fire & EMS Agencies

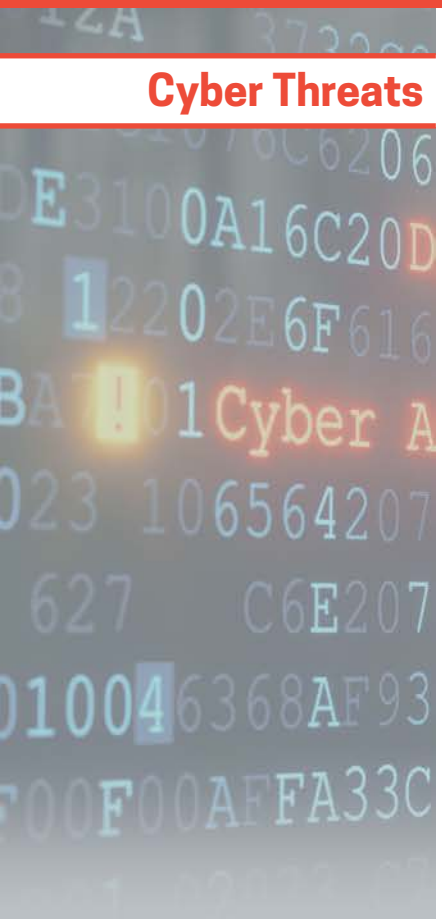
On Monday April 6, 2020, at 4 p.m. Eastern, U.S. Fire Administrator Keith Bryant and Starlene Black, Deputy Section Chief of the Federal Emergency Management Agency's (FEMA) Public Assistance Training Office, will be presenting an overview of cost recovery opportunities for fire and EMS departments using the FEMA Public Assistance Grant Program.

This presentation will be during the International Association of Fire Chiefs (IAFC) COVID-19 Task Force regularly scheduled webinar. There is no cost for this webinar and you do not need to be an IAFC member to participate.

The IAFC weekly COVID-19 webinars are held every Monday at 4 p.m. Eastern. Each is recorded. Past webinar recordings are avialble for viewing through the IAFC website.

(Source: IAFC)

Cyber Threats



Ryuk malware keeps targeting hospitals during the pandemic

The Ryuk Ransomware operators continue to target hospitals even as these organizations are overwhelmed during the Coronavirus pandemic. Of the seven ransomware operators contacted, only two responded that they would no longer target hospitals.

At any time, but even more so now, encrypting a hospital's data not only affects the ability of a doctor to carry out their job but also whether a patient may live or die.

(Source: Bleeping Computer)

COVID-19 Cyber Threat Coalition

The COVID-19 Cyber Threat Coalition is a global community of volunteer cybersecurity analysts who collect and share cyber threat intelligence associated with campaigns exploiting the COVID-19 pandemic. Their resources include blacklists, a Slack Workspace for real-time sharing of indicators of compromise and an Open Threat Exchange Group.

The COVID-19 blacklist is downloadable and contains both vetted (verified suspicious) and unvetted (as-yet unconfirmed suspicious) data sets. Interested parties can volunteer time and information to the coalition.

(Source: COVID-19 Cyber Threat Coalition)

Infrastructure cyberattacks biggest concern for global IT leaders

In a recent survey of more than 3,000 business employees in the United States and Canada, 37 percent said they don't even know what ransomware is, showing a basic lack of knowledge and awareness about this threat.

Further, 32 percent who've already been the victim of a ransomware attack admitted they don't know what ransomware is.

More than a third (35 percent) of respondents said they wouldn't know what to do if their personal information was at risk of being exposed and their company didn't pay the ransom. Some 21 percent of those who've experienced an attack think an organization should never pay the ransom. Only 15 percent of people who've never been hit by ransomware expressed the same opinion.

(Source: Tech Republic)

Cyber webinar: Impact of COVID-19 on the Infosec Industry

The highly-infectious coronavirus, or COVID-19, is spreading across the globe at an alarming rate, significantly impacting a vast array of sectors and verticals. The information security sector is no exception and it has to move quickly and innovatively to help support organizations and employees at this difficult time.

On Thursday, April 9, 2020, at 10 a.m. Eastern, a panel of security experts will discuss various impacts COVID-19 is having on the information security industry, assess the greatest risks currently threatening the security of data and reflect on what the sector must do to address the challenges. Registration is required for this webinar.

(Source: InfoSecurity Magazine)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.