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

The InfoGram

Volume 20 — Issue 12 | March 19, 2020

IAFC coronavirus dashboard for fire departments, survey

The International Association of Fire Chiefs (IAFC) created a dedicated COVID-19 Resource Page for Fire Chiefs, which includes the COVID-19 Fire Department Personnel Impact Dashboard (CID) to measure how fire and EMS departments are being affected by the pandemic.

The dashboard tracks personnel exposed, total personnel in quarantine and personnel diagnosed with COVID-19 based on voluntary responses from individual departments in the United States and abroad.

Given the size and scale of this event, there is an opportunity to gather data on how the pandemic is affecting response agencies nationwide, and your department can voluntarily take part by filling out this impact questionnaire.

The IAFC's COVID-19 page also has a recording of the March 16, 2020, webinar "Coronavirus: What Fire Chiefs Need to Know," "Fire Chief's Guide for Coronavirus Planning and Response," and links to other resources including "Information for First Responders on Maintaining Operational Capabilities during a Pandemic" (PDF, 640 KB), from the Department of Homeland Security.

The current situation is very fluid and moving quickly, and it's affecting first responders in unprecedented ways. This is a reminder to keep up-to-date with current guidance, communicate with leadership and public health, and make infection control a priority.

(Source: IAFC)

Reminder of the dangers of mixing chemical cleaners

The Centers for Disease Control and Prevention recommends routine cleaning of surfaces to limit the spread of COVID-19, several agencies are trying to remind people about the dangers of mixing household chemicals.

People are very concerned right now and may not be thinking about the dangers of mixing cleaners. Some departments have shared information on social media listing combinations of chemicals that can either create toxic fumes or be highly corrosive. Departments should consider delivering a public service announcement to the populations they serve reminding them of the following deadly combinations:

- Bleach + vinegar = chlorine gas. This can lead to coughing, breathing problems, burning and watery eyes. Chlorine gas and water also combine to make hydrochloric and nypochlorous acids.
- Bleach + ammonia = chloramine. This can cause shortness of breath and chest pain.
- Bleach + rubbing alcohol = chloroform. This is highly toxic.
- Hydrogen peroxide + vinegar = peracetic/peroxyacetic acid. This can be highly corrosive.

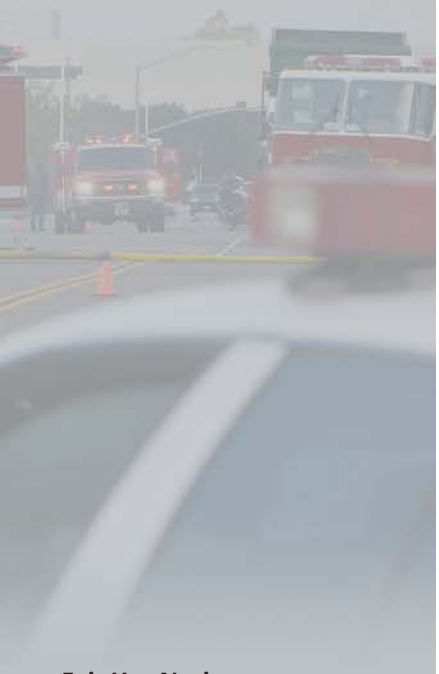
Highlights

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



EMS departments should also keep these symptoms in mind during the current pandemic, as it's possible you may be dispatched out on such a call.

This U.S. Fire Administration (USFA) also offers the infographic "Keep Your Family Safe From Household Chemicals" (PDF, 242 KB). In it, USFA stresses the importance of proper storage and handling of household cleaners, following instructions on labels and never mixing products, and keeping them out of reach from children.

(Source: USFA)

Counter-IED security and resiliency annex for healthcare facilities

The Office for Bombing Prevention (OBP) published the Annex for Healthcare and Public Health Facility Stakeholders (PDF, 3.2 MB) describing actions healthcare facility management and staff can take to understand and improve their ability to perform counter-improvised explosive device (CIED) activities and make critical security decisions.

The annex complements OBP's Security and Resiliency Guide: Counter-IED Concepts, Common Goals, and Available Assistance (SRG C-IED) by tailoring counter-IED guidance and resources to those in the healthcare industry.

To date, OBP has created four other annexes catering to security officials and others working in lodging, outdoor events, sports leagues and venues, and public assembly venues. The annexes all help stakeholders take advantage of available federal resources to build and sustain their preparedness.

OBP developed the newest annex by consulting closely with healthcare entities, by conducting site visits and by facilitating a workshop that focused on the threats that IEDs pose to hospitals across the country.

(Source: OBP)

Webinar: Addressing Trending Topics on Social Media

The Northwest Center for Public Health Practice (NWCPHP) is hosting the webinar "Addressing Trending Topics on Social Media," a timely topic under current circumstances.

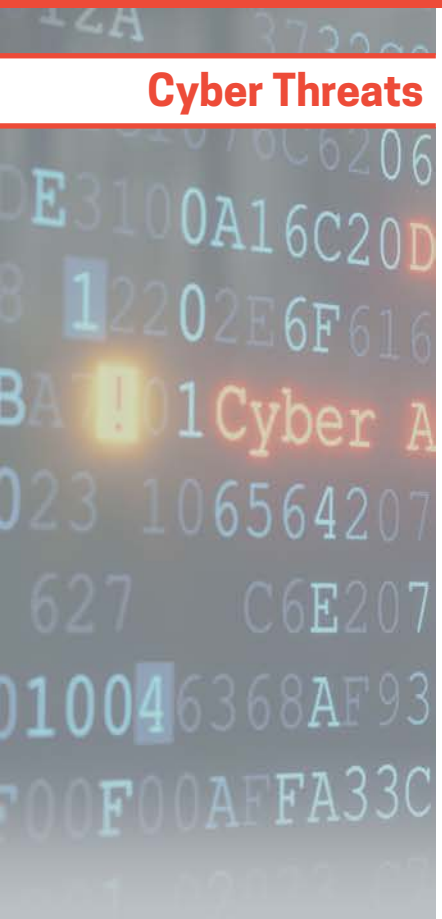
Social media began as a form of personal communication that moved into the business realm without a clear set of rules for how organizations can best use this powerful tool. In the March session of Hot Topics in Practice, a digital media specialist for the Oregon Health Authority shares tips and resources for helping public health professionals better address trending topics on social media.

This 1-hour webinar will feature strategies for connecting directly with key audiences and building micro-influencer campaigns for issues like coronavirus and vaccines. Participants will also learn about practical tools that help small organizations hone their social media persona and establish their reputation as a trusted source.

This webinar is scheduled for Tuesday, March 31, 2020 from 3-4 p.m. Eastern. Registration is required. Be sure to register early, there may be a limit on the number of participants.

(Source: NWCPHP)

Cyber Threats



Cybersecurity becomes top priority for states, local governments

Last month's cyberattack on Louisiana ITI College in Baton Rouge — which followed similar attacks in New Orleans and elsewhere in the state — suggests that hackers have no intention of leaving Louisiana alone.

If that's the case, the state is in good company. More than 110 local and state governments across the country have faced similar problems, as cybersecurity, once a low priority for many jurisdictions, has become a top concern in the last year.

The attack method of choice is ransomware: malicious software that locks up computers and demands payment from its victims to allow them access. While it is not a new phenomenon, it has boomed as some governments, overwhelmed by sophisticated technology, have paid out big sums that have kept the thieves coming.

(Source: Governing)

Seven tips to improve your employees' mobile security

Most organizations support a bring-your-own device (BYOD) protocol in which employees use their personal mobile devices in lieu of corporate-owned ones. But it's a mixed bag: Enterprise-owned devices offer more control over security; however, the business incurs the expense and full liability for them. BYOD puts the burden of buying devices on employees, but it could present a greater risk to the company.

Three security experts share their advice for security managers seeking to improve the security of their employees' mobile devices.

(Source: DarkReading)

Management Checklist for Teleworking Surge During COVID-19

The Healthcare and Public Health Sector released a telework checklist for healthcare enterprise management, although much of it could be adapted to any field, workplace or sector.

The document is a quick reference of important factors to help management make sure operational, information technology and security, patient care and supply chain resilience are factored into any telework surge plan.

(Source: Health Sector Council)

Most ransomware attacks come at night, on weekends

Recent research examined dozens of ransomware incidents from 2017-2019 and found a few common characteristics.

The vast majority of ransomware attacks targeting the enterprise sector occur outside normal working hours, during the night or over the weekend. The reason why attackers are choosing to trigger the ransomware encryption process during the night or weekend is because most companies don't have IT staff working those shifts, and if they do, they are most likely short-handed.

(Source: zdnet)

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.