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

The InfoGram

Volume 20 — Issue 30 | July 23, 2020

Marijuana grow houses still a threat to firefighters

Despite the legalization of marijuana for different uses in many states, some people are still using illegal grow operations as a money-making scheme. Grows can be either indoor or out. Each pose a significant risk to first responders who may inadvertently stumble into these very dangerous situations during a fire call or other emergency.

Make no mistake: these are deadly situations. An explosion at an illegal grow killed a Fire Department of the City of New York battalion chief and injured 20 others in 2016.

From the outside, grow houses often look like regular homes – sometimes even in affluent neighborhoods. Inside it is a very different story. Many illegal grow houses have dangerously rigged wiring to mask the amount of power used at that location. Also, firefighters should use extreme caution as operators of the grow may use deadly force to stop anyone from entering the building.

Common signs of an illegal grow operation:

- Doors and windows barricaded or sealed from the inside.
- Special sodium or metal halide lighting.
- Sources of CO2, such as from pressurized tanks and propane cylinders.
- Fertilizers and other chemicals.
- Ductwork, wires, pipes, tubes and plastic sheeting are entanglement hazards.

Educating firefighters to recognize the signs of a possible illegal grow house operation helps to protect responders and the public from possibly disastrous consequences.

(Source: Firehouse)

List of online COVID-19-related training available on TRAIN website

The TRAIN Learning Network currently lists over 150 training opportunities related to COVID-19 response. Managed by the Public Health Foundation, TRAIN provides quality training to public health professionals.

The collection offers courses on a number of specific COVID-19 treatment topics such as geriatric care, infection control at nursing homes, complications from diabetes and managing a surge of patients needing dialysis. But it also has offerings on non-treatment issues on response, management and personnel concerns including:

- EMS-, fire service- and 911-related issues (legal, lessons learned, standards of care).
- Hospital Incident Command System (HICS).
- Ethical and moral concerns.
- Contact tracing.

Highlights

Marijuana grow houses still a threat to firefighters

List of online COVID-19-related training available on TRAIN website

COVID-19 Recovery CISA Tabletop Exercise Package (CTEP)

Webinar: Public Health Leadership in Times of Crisis

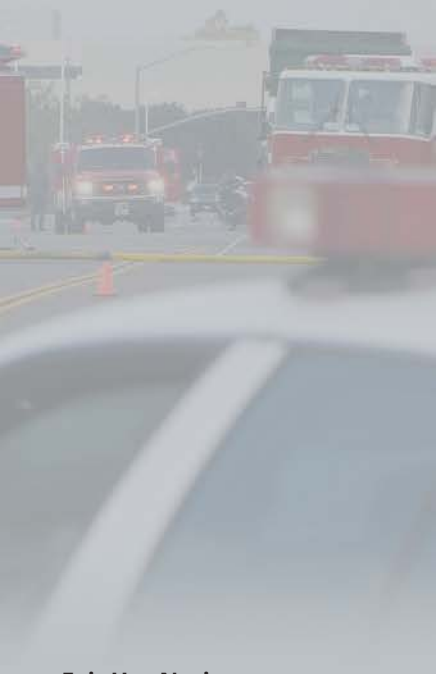
Cyber Threats

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



- Reopening offices.
- Budgetary considerations.

TRAIN offers over 4,600 courses on a variety of topics. Most are free, all require the user sign up for a free account. See the TRAIN catalog for a full list of offerings.

(Source: TRAIN)

COVID-19 Recovery CISA Tabletop Exercise Package (CTEP)

The Cybersecurity and Infrastructure Security Agency (CISA) is pleased to release the COVID-19 Recovery CISA Tabletop Exercise Package (CTEP) to provide critical infrastructure stakeholders and their public safety partners a customizable resource to internally identify and address areas for improvement, threats, issues and concerns affecting their organization.

This exercise package was developed to assess short-term, intermediate and long-term recovery and business continuity plans and address key questions related to organizational recovery from the COVID-19 pandemic. It also provides organizations the opportunity to discuss how ongoing recovery efforts are impacted by concurrent response operations to a potential "second wave" of global pandemic infections.

Stakeholders that use the CTEP can expect improved information sharing, response and recovery capabilities within the collective decision-making process. CTEP focuses on an organization's coordination with federal, state, local, tribal and territorial governments. It is not a test of detailed response procedures, but rather it emphasizes coordination, issue identification and resolution following an incident.

If you have questions about CTEP or supporting documentation, recommendations for improvement, want information on available CTEP products, or are interested in tailored exercises for your specific program, please contact CISA.Exercises@cisa.dhs.gov.

(Source: CISA)

Webinar: Public Health Leadership in Times of Crisis

Local, state and tribal public health professionals, leaders and administrators are encouraged to join the webinar Public Health Leadership in Times of Crisis on Wednesday, July 29, 2020, from 4-5 p.m. Eastern to learn about equity-focused leadership during emergencies. Registration is required.

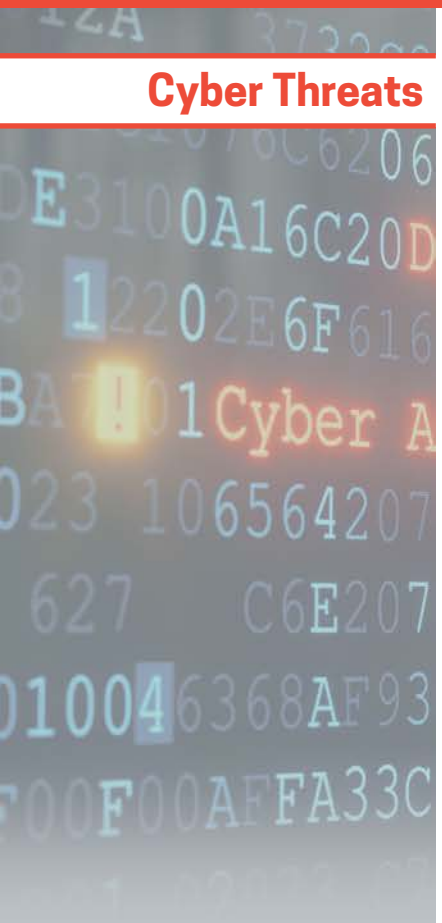
During this free 1-hour webinar, representatives from state and tribal public health will review how Alaska's public health and health care systems are responding to the second wave of COVID-19 cases to distribute resources more equitably and minimize the impacts on small, remote communities.

Officials from the Alaska Department of Health and Social Services and the Alaska Native Tribal Health Consortium will share strategies for partnering and communicating common values within different cultural contexts to collaboratively support health and how the state's American Indian and Alaska Native populations are leading in their own communities and using strategies from past pandemics to survive and thrive.

This webinar is part of the Hot Topics in Practice webinar series from the Northwest Center for Public Health Preparedness.

(Source: NWCPHP)

Cyber Threats



Health Sector Cybersecurity Coordination Center launches website

The Health Sector Cybersecurity Coordination Center's (HC3) is excited to engage with the Healthcare and Public Health (HPH) Sector through its new website www.hhs.gov/hc3. The site offers cybersecurity threat briefs, sector alerts and other products focused on cybersecurity concerns faced by the HPH sector.

The HC3 was created by the Department of Health and Human Services to aid in the protection of vital, healthcare-related controlled information and ensure that cybersecurity information sharing is coordinated across the sector.

HC3's role is to work with the sector's practitioners, organizations and cybersecurity information sharing organizations to understand the threats facing them, learn the patterns and trends used by malicious actors and provide information and approaches on how the sector can better defend itself.

The HC3 hopes its new website will be an asset to the sector and beyond In order to address these threats, to reach a wider audience and to facilitate large scale knowledge sharing.

(Source: HC3)

Iranian hackers accidentally make video of themselves public

When security researchers piece together the blow-by-blow of a state-sponsored hacking operation, they're usually following a thin trail of malicious code samples, network logs and connections to faraway servers. That detective work gets significantly easier when hackers record what they're doing and upload the video to an unprotected server on the open internet. Which is precisely what a group of Iranian hackers may have unwittingly done.

Researchers revealed that they've obtained roughly 5 hours of video appearing to show the screens of hackers working for one of the most active state-sponsored espionage teams linked to the government of Iran. The leaked videos were found among 40 gigabytes of data that the hackers had apparently stolen from victim accounts, including United States and Greek military personnel.

The videos appear to be training demonstrations on how to handle hacked accounts. They show hackers accessing compromised Gmail and Yahoo Mail accounts to download content, as well as exfiltrating other Google-hosted data from victims.

(Source: Wired)

One out of every 142 passwords is "123456"

In one of the biggest password re-use studies of its kind, an analysis of more than one billion leaked credentials has discovered that one out of every 142 passwords is the classic "123456" string.

The study analyzed username and password combinations leaked online after data breaches at various companies. These "data dumps" have been around for more than half a decade, and have been piling up as new companies are getting hacked.

The main discovery was that the 1,000,000,000+ credentials dataset included only 168,919,919 unique passwords, of which more than 7 million were the "123456" string.

(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.