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

The InfoGram

Volume 19 — Issue 35 | September 26, 2019

Roadway Safety Teaching Topic Packages available

In the past month at least two struck-by incidents have been reported around the country, resulting in one firefighter death and several injuries. Working roadway incidents is incredibly dangerous, made more so every day by the public's growing use of cellphones while driving.

First responders must have the necessary training to safely manage these incidents. ResponderSafety.com offers 10 free teaching packages for instructors on a variety of road safety and traffic incident management topics such as:

- Setting Up a Traffic Incident Management Area.
- Scene Control.
- Manual Traffic Control.
- Vehicle Fires.
- Termination.

Each package includes lesson plans, pre-class assignments, practical and tabletop exercises, PowerPoint presentations, model SOPs and videos. You can customize these packages to use in one complete training day, quick roll-call trainings, short refreshers or however works best for your department.

ResponderSafety.com also requests feedback on training programs so they may continue to improve them and support roadway safety nationwide. See their website for other training options on roadway safety and traffic incident management.

(Source: ResponderSafety.com)

2020 EMI Virtual Tabletop Exercise Program schedule released

The Emergency Management Institute (EMS) released its 2020 schedule for the Virtual Tabletop Exercise (VTTX) program. A new scenario this year is Family Reunification, scheduled for November. Other scenarios will cover public health emergencies (agriculture, Ebola); active threats (shooter, vehicle as weapon); cybersecurity; and a variety of natural disasters. See the online schedule for a full rundown (PDF, 356 KB).

The VTTX program uses video teleconference to provide a virtual forum to 10-15 communities across the country simultaneously. Each scenario consists of three discussion modules, local discussion with guided questions led by an onside facilitator and back briefs from each location at the completion of each module. The exercises run from 12-4 p.m. Eastern on each day.

VTTX leverages the "whole community" concept, encouraging local governments to collaborate with their greater Emergency Management Community of Practice: non-profit organizations, school administration, local military, businesses and public health agencies. Participating locations usually have between 10-50 participants representing a variety of agencies, organizations and businesses.

To participate, send an email to the Integrated Emergency Management Branch at fema-ems-iemb@fema.dhs.gov or call 301-447-1381, and Doug Kahn at douglas.

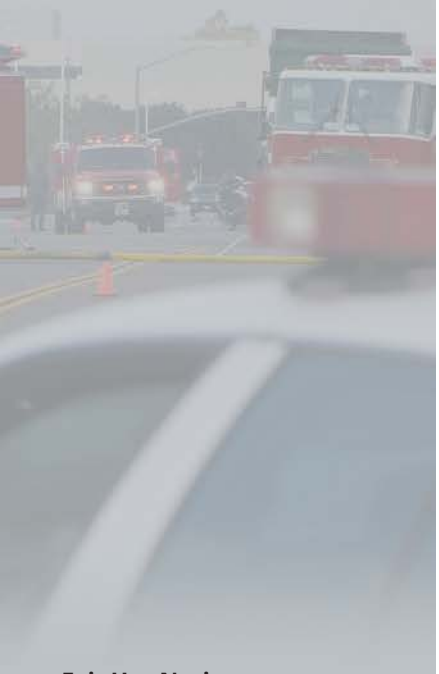
Highlights

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



kahn@fema.dhs.gov or call 301-447-7645. Questions can also be directed to these email addresses and numbers; see the VTTX website for full details.

(Source: EMI)

Office for Bombing Prevention Webinar Series for first responders

The Office for Bombing Prevention (OBP) is holding a webinar series for the Emergency Services Sector. The first webinar will be an overview of OBP, scheduled for Wednesday, October 9, 2019, from 1-2 p.m. Eastern. The first webinar will be an overview of OBP. Future webinars will educate, provide information, and lead the first responder community to available free training and resources.

The OBP works to protect life and critical infrastructure by educating first responders and private sector partners on methods to prevent, protect against, respond to and mitigate improvised explosive device (IED) incidents.

The OBP offers free counter-IED training and awareness products, retail security education through the Bomb-Making Materials Awareness Program (BMAP), information sharing with tools such as TRIPwire, and capability assessments through National Counter-IED Capabilities Assessment Database (NCCAD) and the Multi-Jurisdiction Improvised Explosive Device Security Planning (MJIEDSP) workshops.

Registration is required for this webinar. Connection information will be emailed to participants. The call-in number is 800-685-3601.

(Source: CISA)

October is National Cybersecurity Awareness Month

This year is the 16th National Cybersecurity Awareness Month - yes, 16 years. Despite cybersecurity being the big buzzword only recently, government and industry have been trying for a decade and a half to educate the public on safety online.

Technology has become such a big impact in our daily lives that one cyber misstep can wreak havoc, and the reliance on such technology becomes stronger year after year. It is up to each of us to protect ourselves, help protect our workplaces and ensure cybercriminals don't have easy access to our information and assets.

This year, they are focusing on three things you can do to protect Information Technology (IT):

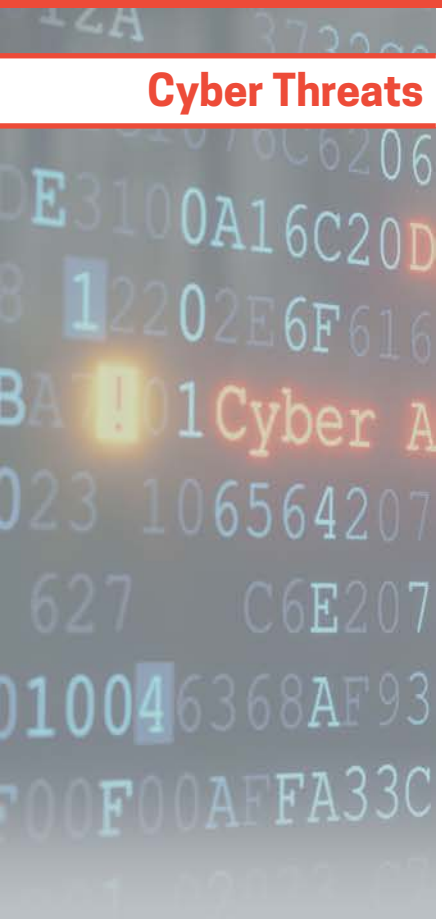
- Own IT. Never Click and Tell: staying safe on social media, Update Privacy Settings, Keep Tabs on Your Apps: best practices for device applications.
- Secure IT. Shake Up Your Passphrase Protocol: create strong, unique passphrases; Double Your Login Protection: turn on multi-factor authentication; Play Hard To Get With Strangers: how to spot and avoid phishing.
- Protect IT. If You Connect, You Must Protect: updating your security software, web browser and operating systems; Stay Protected While Connected: Wi-Fi safety; If You Collect It, Protect It: keep customer/consumer data and information safe.

For more information, see the National Cybersecurity Awareness Month website and the Cybersecurity and Infrastructure Security Agency.

State, local, tribal and territorial governments should consider joining the Multi State Information Sharing and Analysis Center (MS-ISAC). This free membership offers a large number of resources including incident response services, a 24/7 call center, cybersecurity tabletop exercises and a host of resources.

(Source: NCSAM)

Cyber Threats



Vulnerability actively exploited to track, spy on mobile phone owners

Simjacker extracts the location information of mobile phone users from vulnerable operators, retrieved using malicious SMS messages. The location information of thousands of devices was obtained over time without the knowledge or consent of the targeted mobile phone users.

Based on previous intelligence, **it is likely that these attacks originated from a surveillance company which works with governments**, to track and monitor individuals; bypassing existing signaling protection.

(Source: HelpNetSecurity)

U.S. Cyber Command shares 11 new malware samples

U.S. Cyber Command has released 11 malware samples to the malware aggregation tool and repository, VirusTotal. The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review U.S. Cyber Command's VirusTotal page to view the samples. CISA also recommends users and administrators review the CISA Tip on Protecting Against Malicious Code for best practices on protecting systems and networks against malware.

(Source: CISA)

5G requires a cybersecurity reset

With so much attention focused on the potential of 5G to revolutionize internet communications powering smart cities, autonomous vehicles and advanced manufacturing, **more attention must be focused on its cybersecurity before insecure products and services become de facto standards**.

Once the 5G infrastructure is installed, the massive numbers of small-cell antennas deployed throughout urban areas will become targets of attack, as will the devices connected to them. Additionally, advances will be software based, making the network particularly susceptible to cyber risk.

The nature of the network "requires a similarly redefined cyber strategy," and both industry and government must step up and work on forging a new relationship.

(Source: Government Computer News)

Industry challenged to find way to detect, prevent "Deepfakes"

Facebook, Microsoft and a number of universities have joined forces to sponsor a contest promoting research and development to combat deepfakes, or videos altered through artificial intelligence (AI) to mislead viewers.

Deepfake techniques use AI in such a way that **videos of real people are altered so they appear to do and say things that are not real** to present a distorted version of reality. While this technology currently exists and is rapidly advancing, industry doesn't yet have a data set or benchmark for how to detect when it's being used.

Deepfakes created quite a stir recently thanks to a viral video of actor Bill Hader impersonating Tom Cruise and Seth Rogen, in which Hader's face was altered to look like Cruise and Rogen.

(Source: ThreatPost)

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.