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

The InfoGram

Volume 20 — Issue 10 | March 5, 2020

Past FEMA PrepTalks speak to current coronavirus emergency

Recent PrepTalks from the Federal Emergency Management Agency (FEMA) hold some key talking points and things to consider with coronavirus planning and management. Take some time to watch these videos, each is 18-25 minutes long.

- "The Next Pandemic: Lessons from History." The presenter focuses on influenza but the lessons are applicable to current events. One example is our reliance on the "just-in-time" economy, which will break down and medical supplies will become scarce. He also discusses avoiding losing community trust.
- "Triage, Ethics, and Operations: Healthcare Emergency Preparedness and Response." Here, the presenter discusses ethical decisions on patient care when resources become limited.
- "Private Sector Resilience: It Is All in the Supply Chain." In terms of suppliers, have you put all your eggs in one basket? What is the potential one event that will disrupt your entire operation? These are the so-called Black Swan events you may not have ever considered.

(Source: FEMA PrepTalks)

Upcoming BMAP administrator trainer, community liaison courses

The Department of Homeland Security Office for Bombing Prevention (OBP) recently graduated 28 state and local participants of the Bomb-Making Materials Awareness Program (BMAP) Administrator Trainer (AT) course, giving them the skills to conduct point-of-sale outreach within the community as well as train Community Liaisons.

During the course, participants gained the knowledge and ability to conduct outreach to public and private sectors. This increases public and private sector awareness and reporting of suspicious purchases of homemade explosives (HME), precursor chemicals and improvised explosive device (IED) components. In addition to the BMAP AT course, participants also completed a one-day Preventive Measures Course.

The final BMAP AT course for 2020 is scheduled for April 19–24. Current BMAP partner communities can contact their BMAP coordinator for assistance with enrolling in the BMAP AT course.

Upcoming on-site BMAP Community Liaison Courses:

- March 17, 2020 El Paso, Texas.
- March 19, 2020 Marfa, Texas.
- April 15, 2020 Fort Meyers, Florida.
- April 28, 2020 Albany, New York.
- May 5, 2020 Ogden, Utah.

Please email OBP@cisa.dhs.gov for more information.

(Source: OBP)

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

Active Shooter Training for Houses of Worship

Federal Emergency Management Agency (FEMA) Region II developed a new toolkit intended to increase preparedness for houses of worship by making exercises easier. The new toolkit contains the materials needed for a house of worship to conduct their own tabletop exercises with little or no previous exercise experience.

The intended audience for this toolkit is safety and security committee members of houses of worship, interfaith preparedness organizations, or local first responder agencies looking to strengthen their ties with the religious institutions in their communities. Registration is required for this free presentation.

FEMA Region II is holding a presentation to introduce the new toolkit on Tuesday, March 10, 2020, from 12-1 p.m. Eastern. It will discuss the toolkit's contents and provide some simple tips for structuring your exercise to maximize your benefit.

(Source: FEMA Region II)

Why you should take the time and dox yourself

Doxing is the revealing of documents and personally identifiable information (PII) online, often with the intent of harassment. First responders and public officials have been victims of doxing in the past several years.

What's more concerning is that information made public can also include the names of family members to include children. Sometimes the information includes things like birthdays and Social Security numbers, making easier for someone to steal your identity.

A recent Slate article suggests doxing yourself; that is, search for your own information online in the same way a doxer would. Then, scrub your online presence to make it more difficult for anyone to abuse the information. Some tips:

- Search different variations of your name, phone numbers, address and any online "handles" you use or used to have. Use different search engines as they may turn up different results.
- Check your social media presence and look at the information publicly available with the eye of someone out to do you or your family harm.
- Take some time to do some reverse image searching of pictures you've put online, such as profile pictures.
- Check Haveibeenpwned.com regularly for data breaches. Many of us have gotten jaded about data breaches because they happen so often, but that doesn't make them any less damaging.
- Look at your information on online data brokers such as AnyWho and Whitepages. These sites collect and sell your private information.
- Avoid using Facebook or Google to log in to other sites as you are giving the third part app access to your social media data. Pay attention to what you are agreeing to when you create accounts on phone apps and online sites.
- Do all of this for all your family members, including your children.

The Slate article goes in to much more detail, lists helpful websites and gives other important tips to keep you and your family safe.

(Source: Slate)

Fair Use Notice:
This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

Disclaimer of Endorsement:
The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.

Cyber Threats

States and feds must help local cybersecurity efforts

Cybersecurity continues to be a major challenge for state and local governments, and the issue will likely grow in importance in the coming year.

They are popular targets. They face a multitude of threats – ransomware, phishing, data breaches – and must be prepared to defend against all of them. And state and local governments are collecting and storing more data than ever before. Securing this information will need to be a top priority.

Unfortunately, many agencies simply aren't up to the task. They don't have the talent, training or resources to respond to the most advanced attacks. Nor is it necessarily reasonable to expect them to.

In many cases, the most effective response to cybersecurity incidents will entail government agencies pooling resources and capabilities.

(Source: GovTech)

Your smartphone has more bacteria than a toilet seat

What's the one item that never leaves your side? It goes into the bathroom with you. You use it in the kitchen. It often touches your face, your desk and, well, just about any other surface within arm's reach.

It's your smartphone, of course. And the tasks listed above are just some of the reasons it's a breeding ground for germs and a cesspool of bacteria.

Fecal matter can be found on one out of every six smartphones, according to a 2011 study done by researchers at the London School of Hygiene and Tropical Medicine.

Think about all the surfaces you touch throughout the day, from subway poles and light switches to remote controls to bathroom doors. All of the bacteria picked up during your day-to-day activities ends up on your daily dialing devices, and odds are, you don't clean them often or well enough.

(Source: Phys.org)

Google, Microsoft giving away conferencing tools for limited time

The ongoing coronavirus outbreak has pushed more companies and organizations to transition to remote work, and now **Google and Microsoft will grant access to their teleconferencing and collaboration tools to make it easier for people to work from home**. These tools are typically only available to enterprise customers. Both companies are only offering free access for a limited time.

(Source: The Verge)

For better cybersecurity, new tool fools hackers into sharing keys

Instead of blocking hackers, **a new cybersecurity defense approach actually welcomes them**. The method, called DEEP-Dig (DEcEPtion DIGging), ushers intruders into a decoy site so the computer can learn from hackers' tactics. The information is then used to train the computer to recognize and stop future attacks.

(Source: Homeland Security News Wire)

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