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

The InfoGram

Volume 19 — Issue 9 | March 28, 2019

Social Media Officer Safety video training series

The Bureau of Justice Assistance VALOR for Blue program just released a new eLearning course giving law enforcement officers tools to help them protect their digital footprint.

Online connectivity has inroads into almost every aspect of our lives, both personal and professional. The amount and type of personal information you share, and how openly you share it, can put you and your family at risk. It is especially important law enforcement personnel protect themselves by limiting their digital footprint.

The "Social Media Officer Safety Video Series" covers three core topics:

- Foundational information on how personally identifiable information, or PII, is discovered on the internet.
- Relevant law enforcement examples of how PII has been found and used against law enforcement officers.
- Best practices for sanitizing your online presence to protect your digital footprint.

The training is free through the eLearning portal, but users must create a free account. To access this video and to see all the VALOR for Blue training available, visit the eLearning portal.

For more resources on cybersecurity for law enforcement officers, see the International Association of Chiefs of Police Law Enforcement Cyber Center.

(Source: VALOR for Blue)

Fire as a weapon

The Department of Homeland Security (DHS) recently released the two-page Action Guide "Fire as a Weapon: Security Awareness for Soft Targets and Crowded Places" (PDF, 870 Kb). It is part of the "Securing Soft Targets and Crowded Spaces" information collection.

The document details a few incidents of foreign and domestic use of weaponized fire in the past 2 years. Examples range from simple acts of arson with terrorist or extremist motives to more complex attacks such as launched Improvised Incendiary Devices.

Some potential indicators include theft of large or heavy-duty vehicles, purchase of hazardous materials, suspicious questioning about things like egress methods or water supply, and social media messaging that promotes fire as a weapon. None of these things should be taken individually as indicators.

DHS suggests access controls for security planning purposes to include:

- Employing monitoring, surveillance and inspection requirements.
- Defining a perimeter and identifying locations needing special access controls.
- Maintaining an inventory of all flammable or combustible materials.

Highlights

U.S. Fire Administration

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

- Inspecting packages, bags, or briefcases for everyone entering the premises.

This document is unclassified and can be shared with private sector partners who may encounter some of the potential indicators listed. Examples of private sector partners include industrial sites with chemical precursors, venues or other facilities hosting large numbers of people, transportation hubs, vehicle or truck rental companies, and schools or universities.

(Source: DHS)

HHS stands up new healthcare/public health cybersecurity center

Facilities in the Healthcare and Public Health (HPH) Sector are prime targets for cybercriminals. Between the medical community's specialized, life-saving work and the amount and type of information they handle, the costs associated with a cyberattack or breach at a healthcare facility or public health office are very high.

In recent months, hospitals have had to turn patients away, cancel elective surgeries and pay bitcoin ransom to unlock crucial systems. Attacks against healthcare are increasing and facilities struggle to keep up with the evolving threat.

The Department of Health and Human Services (HHS) recently formed the Health Sector Cybersecurity Coordination Center (HC3) to help the Healthcare and Public Health Sector defend against cyberattack. HC3 enhances cybersecurity resilience through timely and actionable cybersecurity intelligence (PDF, 162 Kb) geared toward health organizations.

Currently, HC3 disseminates its cybersecurity information via third party mechanisms such as the "Healthcare and Public Health Sector Highlights." Those interested in subscribing to this newsletter can do so by contacting CIP@hhs.gov.

To request more information about HC3, contact HC3@hhs.gov.

(Source: HHS)

Webinar: Educate and Train Your Cybersecurity Workforce

FedVTE is a free online, on-demand cybersecurity training system for government personnel, contractors and veterans. The course catalog contains more than 800 hours of training on topics such as cybersecurity, surveillance, risk management and malware analysis.

Join the Cybersecurity and Infrastructure Security Agency's (CISA) on Thursday, April 4, 2019, at 1:00 p.m. Eastern for an overview of the FedVTE program's free cybersecurity training, education and workforce programs. No registration is required.

FedVTE is part of the National Initiative for Cybersecurity Careers and Studies (NICCS), offering a total of over 3,000 cybersecurity-related online and in-person courses. Other training options include courses offered in the NICCS catalog and the program training veterans in cybersecurity careers.

(Source: CICCS)

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI office and also the State or Major Urban Area Fusion Center.

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201,** or by email at **nicc@dhs.gov.**

The U.S. Fire Administration maintains 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.