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

The InfoGram

Volume 20 — Issue 15 | April 10, 2020

DHS releases COVID-19 resource guide for law enforcement

The need for local response to COVID-19 required changes to standard procedures and tactics in order to safeguard the health of responding personnel. In many cases, responding law enforcement agencies were not prepared for the necessary operational changes during a wide-spread pandemic.

The Department of Homeland Security (DHS) just released "COVID-19 Exposure and Risk Mitigation Best Practices for Law Enforcement," a resource guide to assist departments with the many different facets of response during the COVID-19 pandemic. It links to guidance, training and tools available from state and federal agencies. Much of the information contained in the guide is useful for other first responders.

Information is broken down into four sections:

- Exposure Levels and Risk Assesment.
- Personal Protective Equipment for Law Enforcement.
- Mitigating Risk Through Altered Tactics and Procedures.
- Exposure Guidance and Decision-Making Tools.

It is important to note this is a fluid situation; much of the guidance is likely to change and be updated.

(Source: DHS Office for State and Local Law Enforcement)

Downloadable tool helps hospitals, responders optimize PPE use

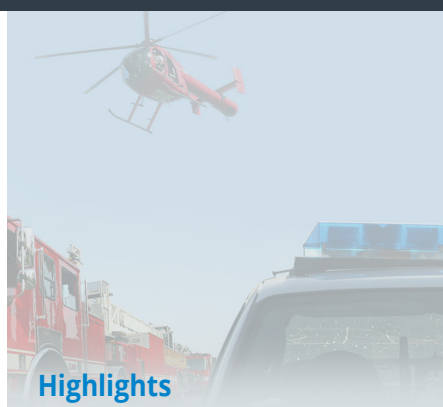
PPE distribution is an ongoing concern during the current COVID-19 pandemic. Hospitals, first responders and other workers on the front lines are facing a serious supply and demand issue, which is even more concerning when you factor in that experts say we still have not yet seen the peak of this crisis.

The Centers for Disease Control and Prevention (CDC) recently released the Personal Protective Equipment Burn Rate Calculator to help you plan and optimize the use of PPE during COVID-19 response. While this Microsoft Excel spreadsheet-based model was developed with healthcare facilities in mind, it is available to any agency using PPE as part of their response.

With this tool, you can estimate your "burn rate" for PPE including gowns, gloves, surgical masks, respirators, face shields and anything else you might be using. You can then base new orders on estimated future needs.

The spreadsheet has three separate sheets: instructions, the calculator and automatically generated graphs based on the information you put into the calculator. System specifications and instructions for downloading the spreadsheet are also listed on the CDC's webpage.

(Source: CDC)



Highlights

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

FBI guidance on securing video-teleconferencing against hijacking

As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected during the COVID-19 crisis, reports of VTC hijacking (also called "Zoom-bombing") are emerging nationwide. The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language.

FBI recommends following steps to mitigate teleconference hijacking threats:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a teleconference or classroom through an unrestricted website or a publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. In Zoom, change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications.
- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

If you were a victim of a teleconference hijacking, or any cyber-crime for that matter, the FBI requests you report it to the FBI's Internet Crime Complaint Center. If you receive a specific threat during a teleconference, please report it at tips.fbi.gov.

(Source: FBI)

Webinar: Fire as a Weapon

Join IPSA on Wednesday, April 15, 2020, from 1-2 p.m. for the webinar "Fire as a Weapon." Registration is required.

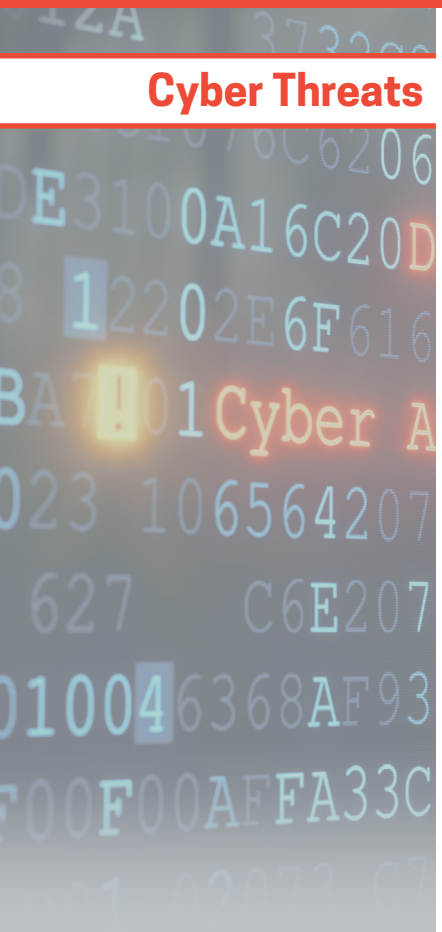
Fires happen regularly in our communities, but during the response and size-up many first responders don't consider the fireground may be a crime scene. However, fire is an easy, cheap and effective tool to commit crimes.

This webinar will provide first responders with an initial exposure to the use of fire to destroy property, inflict casualties or instill fear. First responders need to be aware of the current trends and utilization methods of fire as a weapon, as officer safety may depend on it.

This topic ties in with this year's Arson Awareness Week theme "First Responders: Fire Investigations, Arson Laws and You!" The U.S. Fire Administration offers resources to combat arson in your community. Watch for more on Arson Awareness Week in an upcoming issue of the InfoGram.

(Source: IPSA)

Cyber Threats



Use of legacy VPN systems overloads systems, attracts hackers

Virtual Private Networks (VPNs) have always been the technology backbone of remote work. Previously, they were sufficient as only a few million people globally were working remotely. Before the sudden necessity a large percentage of people to work from home, most workers treated VPNs as a dependable, yet occasional solution for remote access.

Now, with the sudden surge of workforces implementing different VPNs, cracks are starting to emerge: these solutions were not built to scale to support millions of users nationally or globally. In the United States alone, there is a 53 percent increase in usage of VPNs. This is due to the number of state governments mandating a work-from-home policy, and is creating an unprecedented stress test on VPNs.

This rapid global transformation has forced the largest amount of people to work remotely in history. With millions of people connecting to their corporate networks from their homes, network infrastructure is being taxed like never before, creating new issues of internet overload and skyrocketing VPN usage.

(Source: Beta News)

Hackers scanning for vulnerable VPN networks

The number of cyberattackers attempting to exploit the coronavirus outbreak for their own gain continues to rise as both cyber-criminal groups and nation-state-backed hacking operations attempt to take advantage of the COVID-19 pandemic.

A joint advisory published by the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency warns about the continued threat posed by coronavirus-themed scams, phishing attacks, malware operations and ransomware campaigns against both individuals and organizations.

The NCSC and DHS also issue warning about how cyber criminals are trying to take advantage of the sudden rise in remote working to conduct attacks, noting that there's been a rise in attackers scanning for vulnerabilities in remote-working tools and software.

(Source: zdnet)

It's too easy for people to send fake texts from official-looking sources

With email, there are ways to verify the legitimacy of the sender, but SMS texting doesn't have any such checks and cybercriminals have already taken advantage of this weakness with their COVID-19 scams.

Earlier this week, someone sent a scam message telling United Kingdom citizens all residents had been given £258 to help them during the pandemic.

The United Kingdom is not alone in this vulnerability. The same goes for any other nation using SMS for mass alerts. If you do receive a COVID-19 message appearing to come from your government, it might be best to avoid clicking on any links within.

(Source: Forbes)

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.