# Personal Security of First Responders in the Digital Age

Terrorists continue to be interested in exploiting publicly available digital information belonging to first responders as well as US government and military personnel. Digital information, including personally identifiable information (PII), can be collected by illicit actors, providing them with potential targeting opportunities for doxing and presenting risks to first responders, including their identity, email and residential addresses, and other PII. First responder awareness on best practices of digital operational security (OPSEC) can increase their own personal safety, as well as that of their organizations.

- In February 2020, two Indonesian ISIS-aligned cyber groups disseminated a poster on their Telegram channels referencing now-deceased ISIS fighter and hacker Junaid Hussain, who directly plotted attacks, inspired potential attack plotters, and disseminated sensitive information including the residential address and personal email account information of a former senior British official.
- In March 2019, authorities arrested a woman in Georgia for conspiring to provide support to ISIS, which carries a maximum sentence of 20 years in prison. In April 2016, the woman joined the ISIS online group United Cyber Caliphate, which disseminated "kill lists" with names, residential addresses, and other PII of members in the US military and State Department.

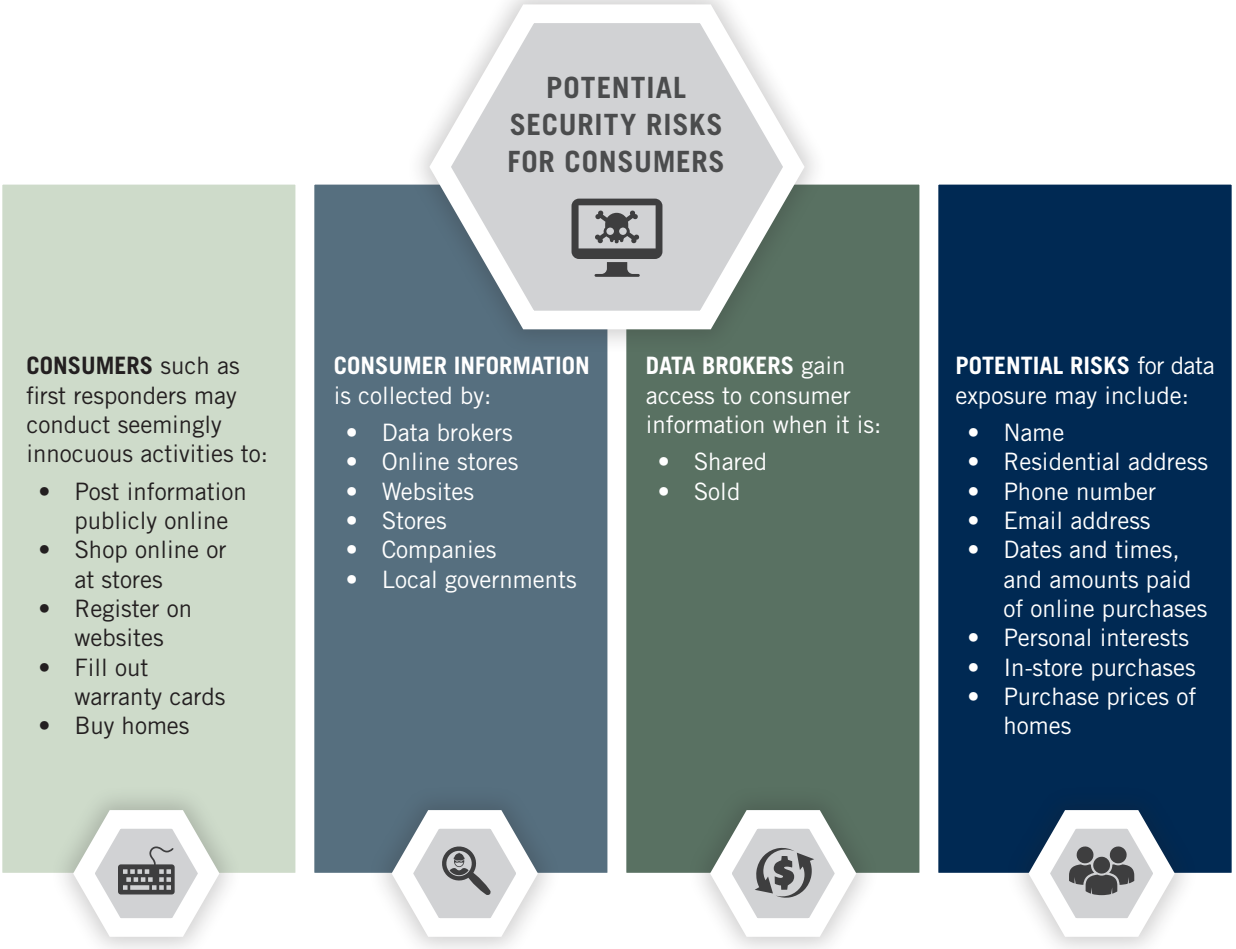
**SCOPE:** This product serves to increase situational awareness among first responders on practicing digital OPSEC to increase personal safety.

- **Doxing** is the act of compiling and publicly sharing an individual's personal information without permission. The personal information gathered from social media and other websites can include residential addresses, phone numbers, email addresses, passwords, and other information used to target an individual online and possibly in person.
- **Digital technologies** can include Internet of Things (IoT), personal electronic devices (PED), communication applications, facial recognition software, internet search engines, social-media sites, email, radio-frequency identification (RFID), and maps and global positioning system (GPS).
- **OPSEC** as referenced in this article is the protection of information to deny its exploitation.

**NOTE:** Some states have passed laws amending the Open Public Records Act to protect personal information (email accounts, residential addresses, and phone numbers) of active or retired judges, prosecutors, and law enforcement officers—including family members—from public disclosure and the internet. These laws give individuals the ability to request the removal of such information from the disclosed location (government agency, individual, or business).

## Personal Security of First Responders in the Digital Age *(continued)*

- In February 2018, a woman in Kentucky was sentenced to 90 months in prison for communicating threats. The woman—who was an active member of an invitation-only social media group supporting ISIS—posted a message including a link to a publicly viewable website page calling for the killing of identified US service members and their families. She also posted a series of messages to a group with the full names, dates of birth, and residential addresses of US military members, stating "they make targets on our heads so here are their heads for targets…"
- In June 2018, a woman in Missouri was sentenced to nine years in federal prison using social media to transmit threatening communications on behalf of ISIS. This included two FBI employees and two former members of the US military and their families. The woman admitted to re-tweeting messages in 2015 containing names, residential addresses, photos, and other PII of victims.



## Personal Security of First Responders in the Digital Age *(continued)*

**CONSIDERATIONS:** First responder awareness on their specific information and pattern of life activity—which is gathered through various technologies—is an important component to digital OPSEC. This understanding, combined with training, planning, and practicing safe habits can help decrease first responders' digital footprints. The following are considerations that first responders can employ for digital OPSEC:

### Safe Habits

- Disable facial recognition features, image tagging information, and geolocation data from photos that can be used by companies to recognize individuals and provide information about image rights, administration, and location.
- Avoid first responder affiliations (agencies, employers, and titles) in social media and refrain from tagging other first responders in photos and videos.
- Remove pictures and videos of your home from online listings of real-estate services.
- Eliminate personal use of professional credentials; restrict photocopying and photographing of professional credentials by non-law enforcement entities.
- Use a cross cut shredder when disposing of all documents, including junk mail with personal details (names and residential addresses) to prevent compromise.
- Avoid using public WiFi (coffee shops, eateries, retailers, or airports); if possible, use a virtual private network (VPN) to keep web browsing secure and private.
- Use an identity protection service to monitor unauthorized activity or breach of information (medical records, bank accounts, or credit cards).
- Practice safe cyber habits (beware of phishing attempts, scams, and ransomware) on personal and professional computer systems, including performing safe internet searches, monitoring browsing behavior (opt out of public white pages or use a scrubbing service), encrypting sensitive or personal data, creating strong and non-duplicative passwords for all accounts and devices, frequently changing passwords, and learning how to use password manager tools.
- Conduct frequent searches for personal information (names, relatives, spouses, and children) on search engines and social media in order to remove any social-media tags.
- Delete any social media or online account that is no longer in use.
- Do not respond to requests for PII, or open email links and attachments without verifying the requestor.
- Do not send or store any unencrypted files or documents containing sensitive PII such as social security numbers in emails or cloud-based services.

## Personal Security of First Responders in the Digital Age *(continued)*

- Contact major credit bureaus to freeze credit and reduce the risk of identity theft. If contacting the credit bureau online, ensure that the website is secure when authorizing it.
- When applicable, apply two-factor authentication as a third authentication step after entering a username and password. Consider using an authenticator application instead of short-message service two-factor authentication.
- Properly secure privately-owned PEDs from possible intrusion.

### Education

- Educate family and friends about safe habits and the importance of discretion when posting online.
- Be aware of the potential for illicit actors to post public videos that capture first responder activities online for nefarious purposes.
- Ask your financial institution about opt-out options to avoid the sharing of personal financial information with third parties.

**RESOURCES**

- **Department of Labor Operational Security Program** https://www.dol.gov/agencies/oasam/centers-offices/emergency-management-center/operations-security
- **Essential Privacy Strategies for Law Enforcement (2019)** is a pocket guide for anyone in public safety and contains a list of suggestions to help reduce vulnerabilities of a cyber attack or identity theft. For copies, contact the Statewide Terrorism and Intelligence Center at 877-ILL-STIC (455-7842) or email stic@illinois.gov.
- **FBI Digital Exhaust Opt Out Guide: For Law Enforcement and Their Families** is a how-to guide on recommended practices to reduce Digital Exhaust, particularly in securing a web browser that is a critical component to removing Digital Exhaust. For copies, contact your local Field Office or email kc_digitalexhaust@fbi.gov
- **National Counterintelligence and Security Center** https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials

## Personal Security of First Responders in the Digital Age *(continued)*

| DIGITAL TECHNOLOGY TERMINOLOGY |
|---|
| **Botnet** is a group of compromised computers remotely controlled by an attacker. Botnets can be used to carry out denial-of-service attacks and other malicious online activity. |
| **Client exploitation** refers to penetrating an individual user's device. |
| **Exchangeable image format** is a standard for tagging image files with metadata, or additional information about the image such as the date and timestamp of when an image was taken or altered. Many smartphones and newer digital cameras can include GPS information to "geotag" photos. |
| **GPS** is a satellite-based navigation system (satellites, ground stations and receivers) made up of more than 30 satellites circling Earth. Each GPS satellite transmits a unique signal and orbital parameters that allow GPS devices to decode and compute the precise location of the satellite. GPS receivers use this information and trilateration to calculate exact location of a user (running route and find a phone, residence, business, or area of interest). |
| **Google dorking** is a method of using advanced search terms in search engines that reveals unprotected information on websites that would not normally be available to the public. |
| **IoT** is the connection of devices and the internet. This can include cellphones, coffee makers, washing machines, headphones, lamps, wearable and components of machines (airplane jet engines or oil-rig drill). |
| **Malware** is software designed to enable unauthorized functions on a compromised computer system, which could include key logging, screen capture, audio recording, remote command and control, and persistent access. |
| **Network scanning** is probing a network to identify settings that might make a device vulnerable to exploitation. |
| **PEDs** have the capability to store, record, and transmit text, images, video, or audio data. Examples of PEDs include, but are not limited to: audio devices, cassette players and recorders, cellular telephones, compact disc, laptops, pagers, portable digital assistant, radios, reminder recorders, universal serial bus, and watches with input capability. |
| **Phishing** involves sending fraudulent emails or texts to a broad, generalized group of recipients to trick recipients into installing malware on their computers or divulging sensitive information, such as usernames, passwords, or financial information. |
| **RFID** is a wireless system comprised of tags and readers. The reader is a device with one or more antennas emitting radio waves, which receive signals back from the RFID tag. The tags (active or passive) communicate their identity and other information to nearby readers, using radio waves, and can store a range of information from one serial number to several pages of data. |
| **Ransomware** is a form of malware used by attackers to encrypt a victim's files, followed with ransom demands from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key. |
| **Social engineering** is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. |
| **Social media account hijacking** is the theft of legitimate social media usernames and passwords to gain access to profiles for unauthorized or malicious purposes. |
| **Spear phishing** is a targeted form of phishing that uses emails or texts that appear to originate from trusted or legitimate sources to target a specific individual, organization, or business. |
| **Two-factor authentication** is an additional layer of protection, or authentication step, beyond passwords to ensure online account security. |
| **VPN** is an encrypted connection over the internet from a device to a network, which helps ensure the safe transmittal of sensitive data. It also prevents unauthorized individuals from accessing traffic and allows the user to work remotely. |
| **Watering-hole attacks** target and compromise the computers of specific groups of victims. Malicious actors first compromise and insert malicious code onto websites that members of the targeted group are known to visit and then wait for victims to visit the sites and unknowingly download malware onto their computers. |

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

# PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: NCTC-FBI-DHS (U) First Responder's Toolbox - Personal Security of First Responders in

POOR ☆ ☆ ☆ ☆ ☆ GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT