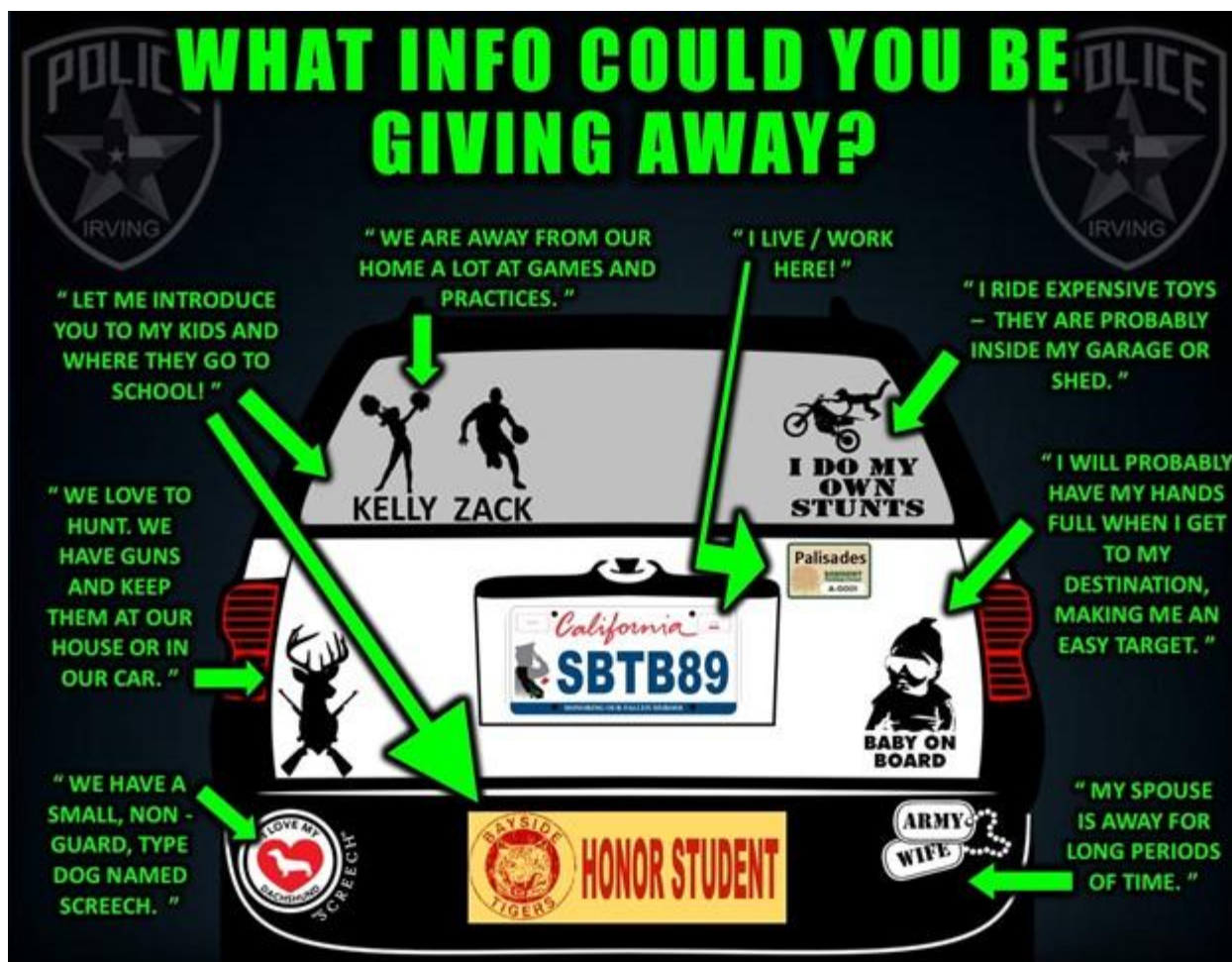


PERSONAL OPSEC

TSgt Sean Lofland, NCO Advisor, SWR-NM-001



Identify your Personal OPSEC.

OPSEC (Operational Security) awareness for military members, government employees, contractors, and Civil Air Patrol members is something you meet when you first step in the door. The information provided at these levels is needed to protect unclassified information about operations and personal information to ensure safe and successful operations and personal safety.

As you read the information provided here, you may find things that are directly applicable to your life and may want to implement immediately. Other things we will discuss here will be, perhaps, less applicable to you, but may be very useful to someone else.

Use what you find useful, and skip that which seem less valuable to you. Don't feel that you have to do everything listed here to add security to your life, or that you somehow create a vulnerability in your life if there is a security recommendation that you choose not to implement. Each person's life is different, and we all have different security needs that may change over time. Security isn't about the number of security measures that you implement, rather it is about understanding the threats that you face in your life, and determining what countermeasures you will implement against those threats.

While I was active duty U.S. Army, we would regularly get OPSEC snippets: just little reminders between recertification trainings. One snippet in particular was being advised not to be ordered. It was on the topic of our personal vehicles. The military has no say whatsoever under regulation on how you present your POV (Personally Owned Vehicle). What they advise us on is don't advertise who or what you are. However, you always get that one new private that buys every sticker in the PX and plasters their eleven-year-old Nissan Sentra with said stickers.

Now since we all are not James Bond, we don't have to worry about being targets of international spies. What we do have to worry about is those elements that would do us and our families harm. Courtesy of the Irving Texas P.D., we have a road map to guide us.

What the informational graphic shows us how we can make ourselves a target. Logically, we understand we need items on our vehicles such as parking passes to do our daily responsibilities. However, the information on our vehicles combined with Social Media can be a bad combination.

Social media sites and apps are great ways to connect and share information including, user profiles, timelines, social media status, friend lists, and message services grant your contacts insights into your day-to-day activities. However, these sites can also provide adversaries with the critical information they need to disrupt your life and harm or harass you, your co-workers or even your family members.

Practicing good personal operations security “POPSEC” (if you will) and using simple countermeasures will minimize the risks that come from using social media and help you protect your critical information. The first step in this process is to identify this critical information.

Identify Critical Information.

Critical information is any information considered sensitive or that could do harm if compromised. Here are some examples:

- Names, photos, and relationships
- Usernames, passwords, computer and networking information
- Operational, security and logistical data
- Mission capabilities or limitations
- Job title, location, salary, grade, and clearance
- Schedules, travel itineraries, and locations
- Credit cards and banking information
- Work or personal addresses and phone numbers
- Interests, hobbies, likes, and dislikes
- Whom you “Tag” in photos.

Apply Countermeasures.

After identifying critical information, analyzing vulnerabilities, and assessing risk, it’s time to apply countermeasures. These countermeasures include practicing good security hygiene: locking down location information, privacy settings, and passwords; and familiarizing yourself with social engineering and misinformation tactics, among other things.

We know everyday people from all walks of life are victims of crime. Some are of opportunity, and some are targeted. Hopefully, this information provided will help you and your family be safe and beat the statistics.

Sources

(n.d.). Retrieved from <https://securityawareness.usalearning.gov/opsec/index.htm>

Et, Al. (2021, August). National Security Agency, Keeping Safe on Social Media. Retrieved from

https://media.defense.gov/2021/Aug/06/2002824387/-1/-1/0/CSI_KEEPING_SAFE_ON_SOCIAL_MEDIA_20210806.PDF

