

Reflective Journal Entry - Week 2

Date: 18JUN2023

Hours Completed: 100 hours

Learning Objectives:

- Learn how social media is related to Operational Security (OPSEC)
- Understand the Importance of Operational Security (OPSEC)

During the last week, I have had the opportunity to learn more about OPSEC and prepare for the brief that I will give during my last week to the candidates before they graduate and go to their respective universities. The brief that I will be giving is about 30 slides and each goes into detail about certain things that are intertwined with OPSEC. One of the most important that I need to emphasize to the candidates is how social media is related to OPSEC. Before I explain what I learned this week about that I needed to understand the importance of Operational Security.

Operational Security also known as OPSEC is a very vital aspect in making sure that confidentiality, integrity, and availability of sensitive/classified information and maintaining overall security. A key point I am going to mention during my brief is geolocation and ship movements. I'm going to go over how candidates and their family members may accidentally disclose the exact location of naval vessels through posts, or stories on social media platforms. This information can be used by the bad guys to track naval deployments, anticipate operational plans, or target certain ships. An example of this I will use is how most will go on their third-class cruise which involves boarding ships and submarines. I will tell them to be careful about posting and only talk about certain things after their cruise is over. This will mitigate any expectations from our adversaries.

Another key point I will make to the candidates is PPI. PPI stands for Personal Identifiable Information. Social media platforms can reveal personal details about Navy personnel, for example, full names, rank, job, and deployment schedules. Candidates need to be aware of what they put in their bio. I avoid putting NROTC in my bio on Instagram to avoid any unnecessary comments from others. It's like putting a target on your head. The main point I will spread to the candidates is that they need to be cautious about sharing sensitive information on social media.

Finally, one of the biggest key points is computer security. If you don't have anything to protect you from any vulnerabilities then you will be an easy target for computer hackers. I will make sure that everyone will have antivirus software, and ensure that a firewall is enabled on their computers. Another thing that most people do is have the same password for their accounts. I will explain the danger of that and how it makes them an easy target because the hacker will have access to all of their accounts. For example, if a hacker finds a password to a

low-security website that you signed up for a couple of months ago, and it's the same password as your email and banking then you just allowed the hacker easy access to your personal information. I am excited to report back next week on how the brief went and how the candidates are turning into fighting machines for the Navy.

End of Report.