

OPSEC

Think before you act. It is important to be able to identify and understand the value of your critical information. It is your duty to make sure you maintain good OPSEC practices, especially online. Hackers, spies, terrorists, and criminals are all threats looking for any opportunity to obtain your work and personal information.

What can I do about it?

There are many things you could do to apply OPSEC in your everyday activities. Examples include: shredding sensitive paperwork, such as alert rosters or technical manuals; reporting suspicious activities on or near the facility to your Facility Security Officer; or not wearing your security badge outside the facility.

You should also follow OPSEC practices in your personal online activity. Check your privacy settings often and do not allow strangers to see your personal information. Be cautious of suspicious emails or links and be sure to NEVER post sensitive information on social media.

Contact your FSO for further guidance or clarification on OPSEC.



CDSE

Center for Development
of Security Excellence