



OPSEC IS A WASTE OF TIME

Of course, OPSEC is *not* a waste of time, but when we over-teach OPSEC mechanics and overlook the importance of the "OPSEC mindset", too many people will believe it is. For people who aren't running an OPSEC program, the most important things they need to know are:

Why OPSEC Matters

Bad guys of the world are looking for good targets—If you work anywhere interesting, know something interesting, or just make yourself seem interesting with the information you share (or allow to be shared about you), you can be as much or MORE of a target than people who are famous or "important".

You CAN control risk—The harder you make it for an adversary, the less likely they are to target you and the less likely they are to succeed if they do.

Being "careful" isn't enough—Attack methods evolve. What kept us safe once won't always work as technology and society advance. The only way to really be safe is to stay current about new risks

"Never say anything" isn't an option (and isn't OPSEC)—You must share to be effective, but OPSEC can help you know how much to share and when (and when not to).

The TAO of OPSEC

Some simple rules to help you stay safe are:

There are no guarantees online—What you post might be found by the bad guys; if not now, eventually. Never post something you can't afford for your worst enemy to see.

Assume the worst, always—Do research before acting on received emails/messages or using any device that is used to gather or send information.

Information IS Risk—Don't put yourself at unnecessary risk. Only share when you have to and only WHAT you have to and no more.

Stay aware—You can't prepare for risks you've never imagined. Pay attention to the "new bad" going around and give due consideration to emails from your security people.