What is OPSEC?

Operations Security (OPSEC) is a 5-step process used to deny access to our important information, generally sensitive or critical information concerning our personal or professional lives. Although OPSEC is normally used at work, the same practices can be applied to our personal lives.

Why is it important to learn about OPSEC?

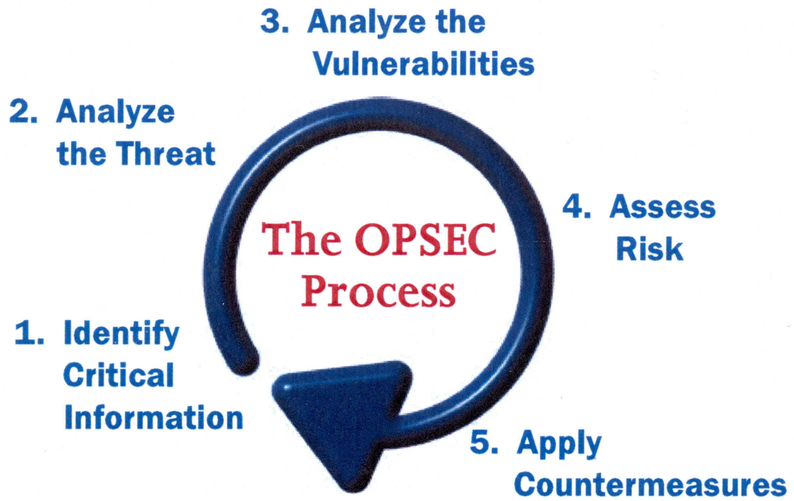
Even when you are not aware, the threat remains. The events of September 11, 2001 proved that there is a demonstrated and known threat. But, most of us thought it could only happen elsewhere - not in America.

In order to protect our families, we should pay careful attention in our daily routines to minimize risk.

OPSEC – Get in the right frame of mind!

The information that is often used against us is not protected; it is information that is openly available to anyone who knows where to look and what to ask:

- Internet chat rooms
- Professional & personal web sites
- Phone books or directories
- Libraries
- Unsolicited phone calls
- Trash cans (work & home)
- Casual conversations in public
- Door-to-door solicitors



1 Identify Your Critical Information

What do you want to protect? Any information that, if compromised, could cause harm to you, your property, or even to your family.

Examples of potential critical information:

- Travel Itineraries
- Home Security Procedures
- Team Rosters
- PIN & Credit Card Numbers
- Social Security Numbers
- Legal Documents

2 Analyze the Threat

So who is the threat? Consider the following threats to determine the level of danger to you & your family:

- Terrorists
- Criminals/Gangs
- Computer Hackers
- Identity Theft Rings
- Sexual Predators

Do your children chat in internet chat rooms? What information do they innocently release: Home address? Phone number? IP Address? Perhaps even the name of the school they attend…

Do your children download programs from web sites that could contain viruses, pop up ads, or spy ware?

Do your children exchange emails or instant messages with strangers?

Do your children email family photos to strangers?

When going on family vacations, do you allow the mail and newspapers to pile up?

Does the message on your answering machine say, "We currently aren't home at this time…"

Take the time and review methods to safeguard sensitive information with family members. Explain why it is unsafe to discuss sensitive information and, if suspicions arise, why it is important to immediately notify a parent or another responsible adult such as a teacher or police officer. This can prevent a potentially dangerous situation from happening to you or a family member.

3 Analyze Vulnerabilities

How is your information vulnerable? Here are examples of vulnerabilities:

- Critical information posted on the Internet or family web page, such as phone numbers, addresses, school districts, children's names, pending vacations
- Discussion of personal information in public areas for others to overhear, such as a spouse going away on business or discussion of personal finances

4 Assess the Risk

Is the risk to your family and home great enough to take preventive action? Often, a small investment can go a long way in providing security.

What is the benefit gained by lowering the risk? Simply put - safety, security, and peace of mind.

Examples to lower risk:

- Install deadbolt locks
- Install alarm system
- Develop safety and security plans
- Keep important documents in a fire-proof safe
- Install fencing & gates
- Install firewall on personal computer system
- Monitor family's computer usage for inappropriate behavior or solicitations for information
- Never give credit card numbers or account information to strangers
- Don't volunteer personal or professional information

5 Develop Countermeasures

What countermeasures can you use to improve your family's safety? Consider the threat when you:

- Use the cell phone or computer
- Use the fax machine
- Use Palm Pilots and other Personal Digital Assistants (PDA)
- Talk to strangers

Examples of countermeasures:

- Shred all documents containing personal information when no longer needed
- Do not share passwords
- Turn off computers when not in use
- Do not display any identification in public places
- Be aware of what you reveal in telephone conversations, particularly on a wireless phone or when in public
- Put children's identification on the inside of backpacks or clothing
- Don't leave property or mail in your vehicle in plain view
- Be wary of unsolicited emails; the message could contain a virus or spy ware

Department of Homeland Security
Office of Security
Phone: (202) 447-5010
E-mail: OfficeofSecurity@dhs.gov

Operations Security for Employees and Their Families

Office of Security
Operations Security (OPSEC) Program

Homeland Security