Avoiding Scams

Scams are rampant during holidays.

Common types are:

- Phishing
- Social Engineering
- Mobile App Malware
- Bluesnarfing (Hacking your device through a Bluetooth connection)

Be aware of suspicious links sent in e-mails, text messages, e-cards, Facebook pages, etc. Ensure your antivirus software is up to date. Free antivirus software is available to military and DoD employees via the AF Portal.Communications Information

- Shred all documents with personal information
- Don't place specific information in your Out of Office replies
- Break down boxes and don't leave them sitting out by the side of the road (e.g. Free advertisement to burglars about the cool stuff you received for the holidays)
- Change passwords periodically, and don't use obvious phrases or numbers like your birthday
- Don't give personal info over the phone; scammers use the names of legitimate companies to gain information about people
- Don't place gifts in view of windows
- Assume everything you post online is public or can become public

Holiday OPSEC tips

Point of sale—some companies have recently fallen victim to hackers, which compromised multiple credit card numbers; check your statements and activity regularly and report suspicious charges immediately

Package delivery—scam sent via e-mail from a seemingly legit delivery company (such as UPS) with a fake tracking number. There's an attachment with a supposed delivery label to bring to the nearest delivery office to pick up the package. The attachment contains malware/viruses.

ATM Skimming—skimming devices are becoming more popular with criminals; if an ATM looks like it was tampered with, don't use it. And always cover the keypad area when you enter your PIN in case recording devices are pre-positioned.

"Best Deal Ever"—If it seems to good to be true, it probably is. Online shopping scams offer bargain prices on hot ticket items, but never provide a product

Social Media—scammers impersonate friends or hack their accounts to sent out malicious links designed to lure personal information from users

Mobile Apps—many fraudsters target mobile devices; don't download from third party websites, and scan apps for malware prior to use

Fake charitable pleas—emails, phone calls and texts are the tactics of scammers using the names of charities to solicit money or personal information; resist demands for on-the-spot donations and do your research!

Identity theft—keep close tabs on your wallet and consider using magnetic sleeves for your credit cards to protect against electronic eavesdropping

45 SW/IP OPSEC

OPSEC Signature Manager: Christopher Cluckey
321-494-5574

Alt OPSEC Signature Manager: Thomas Lovell
321-494-5570

Holiday OPSEC

Providing you the tools to protect sensitive information

OPSEC & Travel

Critical Information during the holidays

➢ **These are a only a few of the key pieces of information to protect**

1. Your identity
2. Banking information
3. Vacation times
4. Type of gifts
5. You and your family's location
6. Routines/traditions

➢Traveling during the busy holiday season can be stressful; keep your loved ones safe by practicing simple OPSEC tips:

•Don't draw attention to yourself as a military member or government employee by using military-issue or logo bags as luggage or wearing clothing that advertises your affiliation

•Turn off location services on social networking sites, and don't announce every stop along the way

•If possible, have a trusted friend house sit while you're away

•Don't leave valuables in plain sight

•Don't show a change in routine leading up to departure

•Have the post office hold your mail or have a trusted friend pick up your mail while you're away

•Use light timers (some even have a "random" setting)

•Be wary of public/hotel Wi-Fi and sending personal information over unsecure connections

Family Critical Information List

Protect your family and military operations by not disclosing specific details (Who, What, When, Where, Why, and How) related to the following topics:

- Future and ongoing missions or operations
- Deployment activities
- Capabilities of equipment and personnel
- Unit problems or limitations
- Security processes or procedures
- Exercise information
- Special training or equipment
- Rumors, gossip or speculation of operations
- Personal and medical information (SSN, etc)
- Home address and phone numbers
- Financial information
- Names of family members
- Family routines and vacations
- Work and/or school locations of family members
- Computer passwords for personal accounts

Some ways to protect this information include not talking about military information on social networking sites or over cell phones, sharing awareness with other family members outside of the military environment, keeping your personal information safe by using strong passwords, shredding documents and limiting amount of personal information on the Internet.