JOINT BASE LANGLEY-EUSTIS OPSEC NEWSLETTER

Good Social Media Practices

Don't give criminals a chance to get your information. Be careful of the personal details, photos and videos you post to your profile on social networks. It's highly recommended that you set privacy settings so that only "friends" can see specifics. Even after establishing privacy settings, don't assume your information will remain private; there's no guarantee. Always use common sense: For example, don't inform potential criminals you're going out of town!

It's a good idea to always operate under the assumption that anything you post online might be stolen by an adversary. Social content shared by JBLE personnel and families is a major target for those looking to impersonate them to gain access to sensitive information, blackmail or intimidate. While there is a definite benefit to using social media to help with support networks, be wary of posting detailed information about support groups. Posting unclassified sensitive information could be just as dangerous as posting classified information.

Operations Security

The primary concern for JBLE personnel using social media is maintaining operations security. Information moves and evolves quickly via social media, which means OPSEC awareness is more important than ever before. Make sure you understand the risks and communicate them to other JBLE personnel. Information about social media awareness is provided in annual computer-based training.

Review all content (photos, videos, links to articles, etc.) for OPSEC violations prior to posting. Remember to take a holistic approach when evaluating whether or not your content violates OPSEC. Don't provide adversaries any advantage by posting classified, controlled unclassified information or sensitive information (for example, troop movements, force size, weapons details, etc.). When compiled, such details can reveal more than intended.

Countermeasures:

- Do not post personally identifiable information.
- Do not allow others to tag you in images they post. Doing so makes you easier to locate and accurately construct your network of friends, relatives and associates.
- Be cautious about the images you post. What is in them may be more revealing than who is in them. Images posted over time may form a complete mosaic of you and your family.
- Do not post your specific location.
- Be cautious when accessing online accounts from public Wi-Fi connections. Someone might have installed software capable of capturing your login credentials and other sensitive information.
- Securely configure your social networking accounts to minimize who can see your information.
- Do not accept friend/follower requests from anyone you do not know; independently verify identities.
- Avoid using third-party applications; if needed, do not allow them to access your social networking accounts, friends list or address books.
- Do not use "check-in". If check-in is enabled, disable it.
- Do not arrange meetings with people you meet online.

Further information related to protective measures while using social media can be found on the 633 ABW OPSEC SharePoint site:

https://langley.eim.acc.af.mil/org/633abw/IG/OPSEC/default.aspx

Additional information:

How Many Pieces of Military Flair are on Yo

ACC Digital Security Tips

Digital Security Command Interest

Threat Awareness Individual Protective I

DET 201 AFOSI/US ARMY CID 3 MP GROUP CORNER

The Air Force Office of Special Investigations along with Army CID 3 MP Group continues to monitor the current threat stream with regard to the Islamic State and recent threats made to DoD members utilizing research from social media websites. In response to queries about information that can be provided to families, I'd like to pass along the information attached and also listed below. All of this information can be shared publicly, and I would encourage wide dissemination to your units. AFOSI Det 201/Army CID 3 MP Group stands ready to provide tailored briefings to individual units upon request, and we will certainly provide updates on the threat via established channels as they are received.

Please do not hesitate to contact AFOSI at 757-764-7971 (main number) or Army CID 3 MP Group at 757-878-4811 or contact us direct at any of the below numbers with any questions or concerns.

Thank you and be safe,

Very Respectfully,

Special Agent Bret Irwin
Commander, AFOSI Det 201
Desk: 757-225-4600
Cell: 757-268-1223

Special Agent Vanessa Neff
Army CID 3 MP Group
Desk: 757-878-4811
Cell: 989-277-8793

SA Irwin's Talking Points for JBLE Personnel and Families

1) Recognize that the social media environment has changed permanently

2) Groups such as the Islamic State will use the information you post to spread fear and alarm, and possibly to plan attacks -- DON'T MAKE IT EASY FOR THEM

3) The best manner in which to protect yourself from becoming a future target is to have a low social media profile

4) Best case scenario: When someone conducts an internet search for your name, the results do not show a military affiliation

5) This is not hiding your service affiliation, but protecting yourself and your families -- only share with verified people

6) Information is power -- don't empower people you don't know by broadcasting details about your life, your family, and your service affiliation

See link for additional information:

http://airforcelive.dodlive.mil/2014/10/securing-your-digital-footprint/

See link and below for information from the Federal Bureau of Investigations:

http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks

See link and below for information from the Computer Crime Investigation Unit US Army Criminal Investigation Command Cyber Crime Prevention Flyer.

http://www.jble.af.mil/shared/media/document/AFD-141217-019.pdf