FACT SHEET
U.S. Army Cyber Command

The Nation's Army in Cyberspace

www.arcyber.army.mil • www.army.mil/armycyber • @ARCYBER

THE FACTS: VIGILANCE

Soldiers and Army civilian employees are often of particular interest to adversaries, intelligence services and others because of their positions and duties and the information, resources or authorities they may possess as a consequence of their Army affiliation. Sometimes even unclassified or seemingly innocuous information can be potentially sensitive or harmful. Whether engaging in activity in person or in the virtual realm, members of the Army team need to be constantly vigilant for attempts to approach them to obtain classified, sensitive or controlled information and to gain military, political, economic, industrial or other advantages.

What are some signs that someone may be attempting to solicit information or advantage?

- Unsolicited correspondence from individuals or entities that you are unfamiliar with
- Undue interest in sensitive information, such as military capabilities, force structures, base locations, manpower, equipment or technology
- Undue interest in an individual's background, access privileges, training or activities

What can I do to help protect myself and the Army?

First of all, never let your guard down. Remember that things and people – particularly in the virtual world – aren't always what they appear to be. Trust your instincts. If something looks, sounds or feels wrong, break off contact and communication.

Be alert for potential insider threats as well. Know that people who appear to be legitimate government or affiliated personnel with authorized access to information or resources may have dangerous agendas and/or exhibit suspicious behavior.

ABOUT US: U.S. Army Cyber Command integrates and conducts cyberspace, electronic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries. As of 7 October 2020

.

Think OPSEC. Do not discuss anything classified or of operational security concern. Even when sharing information with trusted colleagues or partners, remember that your communication can potentially be intercepted by others.

Stay in your lane. The best course of action is to discuss only those things that pertain to your job, role and position – things of which you personally have knowledge or expertise – without disclosing sensitive information. Be cautious to not make or imply any promises or endorsements on behalf of the Army.

You've heard it before: If you see something, say something. Be sure to report any suspicious behavior or concerns to your agency's security or counterintelligence office as soon as possible. You can also make a report via the Army's iSALUTE system online at www.inscom.army.mil/isalute or by calling 1-800-225-5779.

ABOUT US: U.S. Army Cyber Command integrates and conducts cyberspace, electronic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries. As of 7 October 2020

.