WHAT TO REPORT

- Questionable or suspicious contacts on social media platforms
- Any SNS persona attempting to elicit information
- Suspected or known fake personas (attempting to obtain specific information pertaining to your profession)
- Suspicious files sent via private message
- Any attempt at click-jacking (concealing hyperlinks beneath legitimate clickable content) or malware unintentionally downloaded
- Request for information, academic solicitation, job offers from adversarial countries
- Unsolicited contacts from unknown individuals

REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM) requires the reporting of suspicious contacts, behaviors, and activities.

If you suspect you or your company has been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks. Reporting allows DCSA to share and address risks with other government and commercial sector partners.

DCSA
https://www.dcsa.mil

DCSA, Counterintelligence Directorate
https://www.dcsa.mil/mc/ci

Center for Development of Security Excellence
https://www.cdse.edu

COUNTERINTELLIGENCE THREAT VIA SOCIAL MEDIA

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

COUNTERINTELLIGENCE THREATS VIA SOCIAL NETWORKING SITES

Social networking sites (SNS) are everywhere in today's society. Worldwide SNS usage provides foreign intelligence entities (FIE) vast opportunities to exploit personnel, cleared or uncleared. The FIE goal is to obtain U.S. critical technology, proprietary data, advanced research and development, and many other aspects of valuable information in U.S. industry.

- 51% = Total world population; 3.96 billion people use social media
- 2.25 = Hours digital consumers spend daily on SNS and social messaging
- 79% = Number of adults in the United States that use at least one SNS
- 8.8 = Number of SNS accounts the average person maintains

Loose lips sink ships. Everyone is a target when associated with cleared contract facilities, companies, technology, research and development, etc.

Our Nation's foreign adversaries actively exploit SNS to serve their own malicious intentions. Once posted, information on SNS is no longer private and can never truly be deleted. The more information posted, the more vulnerable you may become. Using high privacy settings provides a layer of protection, although the information ultimately still resides on a server.

It is well known that SNS collect personal and trending information on account owners, which is used to tailor the individual's experience. Depending on the site, the information can be sold and companies can be hired to analyze user activities.

FIEs and foreign competitors use SNS to conduct collection activities:

- Request friend/ professional connection
- Monitor social media accounts
- Elicit information
- Recruit assets

"Instead of dispatching spies to the U.S. to recruit a single target, it's more efficient to sit behind a computer in China and send out friend requests to thousands of targets using fake profiles."

William Evanina,
Director, NCSC

ELICITATION

Elicitation is an effective technique adversaries use to subtly collect information:

- Nonthreatening
- Ease of distorting facts
- Exploits human nature (to be polite, be well informed, be appreciated, trust others)

METHODS OF OPERATION

Some methods of operation an adversary can use to conduct collection on SNS are techniques such as:

- Flattery
- Provide information to get information
- Find commonality
- High concentration of targeting on professional SNS
- Obfuscation of true identity – easy and cost effective
- Résumés can and have contained malware
- Detailed information makes an easy target for adversarial collectors
- Transition from SNS to real world using guise: recruiting, speaking engagements, etc

Fake personas on SNS:

- Realistic looking online identities
- Purported commonalities such as company, school, research
- Potential connections to colleagues or friends via successful targeting
- Societal norm of an attractive individual
- Linked to the same company but in a different country

Misinformation:

Adversaries can spread misleading or false information via SNS using fake bot accounts and troll farms. A troll farm is an organization whose employees or members attempt to create conflict and disruption in an online community. SNS uses algorithms that could inadvertently amplify the malicious content to users, causing a widespread false narrative. This gives adversarial countries potential influence of current events in the United States.

COUNTERING THE THREAT

- Think before you post
- Limit or exclude personally identifiable information
- Disable geotagging
- Consider a pseudonym
- Create strong passwords; change often
- Never put sensitive proprietary or controlled unclassified information on your SNS profile
- Be wary of unsolicited messages from unknown senders
- Do not accept connections from unknown sources
- Do not click/download anything
- Follow company security and information assurance policies
- Use caution accessing games, quizzes, and applications that access and mine user data
- Assume all posted material can never fully be deleted
- Read the social media site's policy to ensure full understanding of personal data collection
- Report suspicious contacts immediately to the facility security office and the Defense Counterintelligence and Security Agency (DCSA)
- Make frequent updates to SNS configuration