WHAT TO REPORT

- Questionable or suspicious contacts on social media platforms
- Any social media 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
- Request for information, academic solicitation, or 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 reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DCSA
https://www.dcsa.mil

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

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

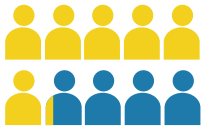
FOREIGN INTELLIGENCE THREATS VIA SOCIAL MEDIA

Defense Counterintelligence and Security Agency

WHAT ARE FOREIGN INTELLIGENCE THREATS VIA SOCIAL MEDIA?

Social media provides foreign intelligence entities (FIEs) vast opportunities to exploit personnel. FIEs attempt to obtain U.S. critical technology, proprietary data, advanced research and development, and other valuable U.S industry information.

WHO IS BEING TARGETED?



62.6%

5.07 billion people use social media, about 62.6% of the global population. Anyone on social media could become a target.*

2.5 hours

The average social media user will spend 2.5 hours on social media every day, amounting to 12 billion hours daily across the globe.*

6.7 platforms

The average social media user will visit 6.7 social media platforms each month.*

HOW ARE YOU BEING TARGETED?

FIEs actively exploit social media. Once posted, information is not private and can not be deleted. Using robust privacy settings provides a layer of protection, but the information still resides on a server.

Social media sites collect information on account owners, which is used to tailor their experience. Depending on the site, information can be sold and analyzed.

FIEs and foreign competitors use social media to conduct collection activities:

- Request friends/professional connections
- Monitor social media accounts
- Elicit information
- Recruit assets

**According to Datareportal.com*

Techniques used to collect on social media are:

- Flattery
- Providing information to get information
- Finding commonality
- Targeting on professional social networking sites
- Obfuscation of true identity
- Résumés containing malware
- Detailed information makes an easy target for adversarial collectors
- Transition from social media to real world using guises: recruiting, speaking engagements, etc

ELICITATION

Elicitation is an effective technique adversaries use to subtly collect information. Elicitation is non-threatening and allows elicitors to easily distort facts and exploit human nature (to be polite, well-informed, appreciated, trusting, etc.).

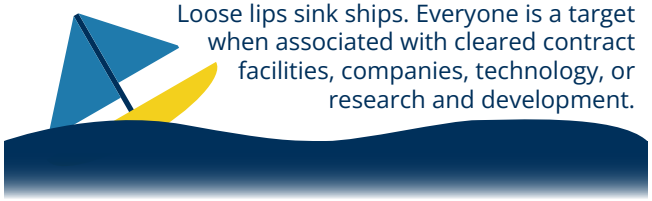
DISINFORMATION

Adversaries spread misleading or false information via social networking service 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. Social media uses algorithms that inadvertently amplify malicious content to users, causing a widespread false narrative. This gives adversarial countries potential influence over current events in the United States.

FAKE PERSONAS ON SNS

- Realistic 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

POPULAR SOCIAL MEDIA SITES*



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

COUNTERMEASURES

- 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 (CUI) on your social media profile
- Be wary of unsolicited messages
- Do not accept connections from unknown sources
- Do not click/download suspicious links or files
- 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 DCSA
- Keep firmware up-to-date

"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