Memorize the four **R**s to protect yourself against malicious profiles:

Recognize
the profile?

Realize
the potential threat

Report
to your security officer

Remove
them from your network

Know the signs

Too good to be true
Offering remote, flexible working; a disproportionately high salary for the role advertised.

Lack of depth/detail
Company lacks any real online presence. The role itself lacks tangible details.

Flattery
Overly focusing on your skills/ experience along with reference to government or 'high-end' candidates.

Urgency
Overly responsive to messages. Attempts to rush you off the website onto another communication method.

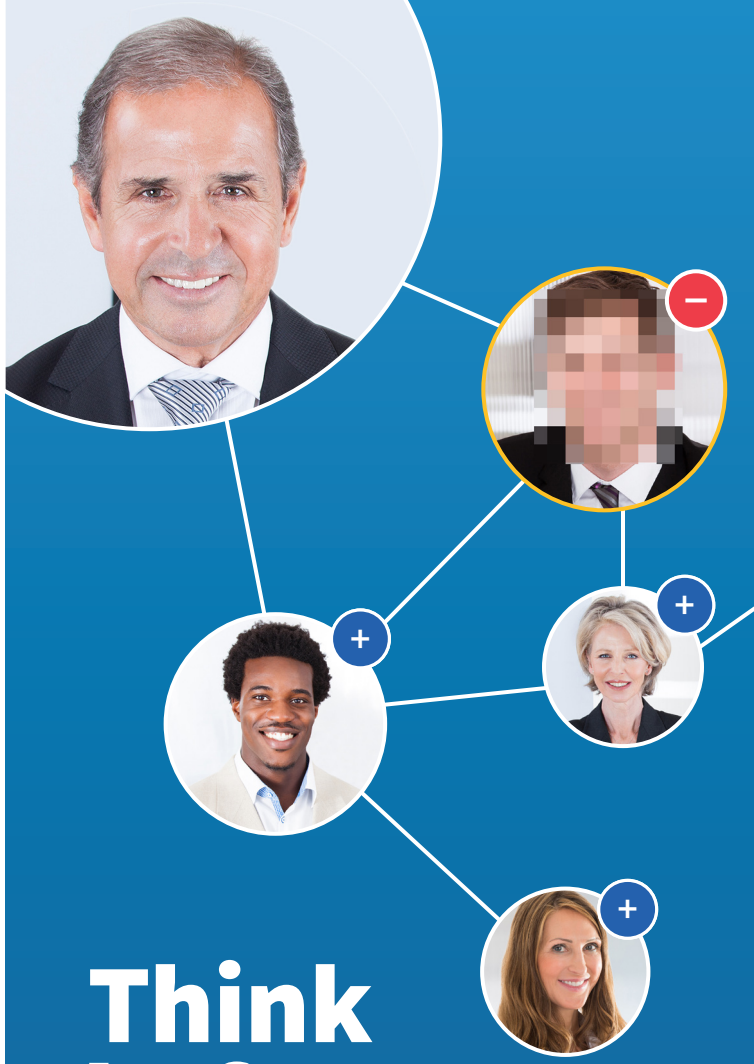
Scarcity
Emphasis on so-called limited, one-off, or exclusive opportunities.

Imbalance
Disproportionate focus on their company rather than validating you as a possible candidate.

What should you do?

- Review your account settings on social and professional networks to control the information that is available publicly, especially relating to security clearances.
- Familiarize yourself with guidance your employer may have provided about posting to social and professional networks.
- Only accept contacts online with people you know or after having verified their identities.
- Report a suspicious contact to **tips.fbi.gov** and your security officer.

FBI.GOV



Think before you link

Online networking guidance

U.S. Department of Justice
Federal Bureau of Investigation

Have you ever encountered someone online who was not who they seemed?

Social and professional networking sites can be a valuable tool for promoting yourself online and enhancing your career prospects, but they can also expose you to unforeseen risks.

“This guidance will help you to protect yourself, your colleagues, and your organization from the harmful impact of malicious profiles online.”

The threat

What’s the problem?

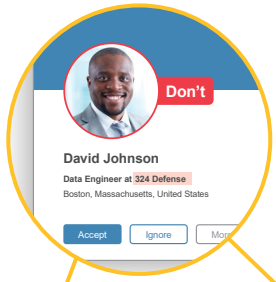
Hostile actors and criminals use social and professional networking sites to target individuals with sensitive accesses.

Why are they doing this?

- Their end goal is to recruit US and Western nationals to provide them with sensitive information.
- Loss of sensitive information could be harmful to you and your organization and pose a national security risk.

Are they targeting you?

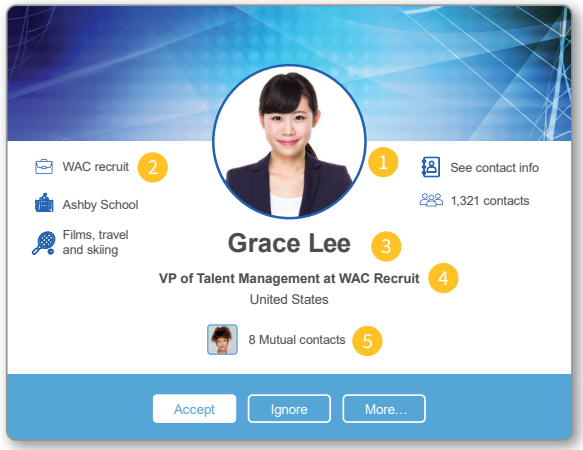
You could be at greater risk of targeting if you publicly disclose your security clearance or that you work for the government or in the private sector with access to classified or sensitive information, technology, or research.



How do they trick you?

- Hostile actors and criminals impersonate employers or recruitment consultants appearing to present a lucrative business or career opportunity.
- They may ask for more details about your role and try to learn about potential sensitive access you might have.
- Their aim is to build a longer-term relationship and manipulate you into giving away sensitive information, knowingly or unknowingly, sometimes in exchange for rewards.
- You may not realize that the information you are sharing is sensitive and may believe the information you are providing is to develop a legitimate business or career opportunity.

What does a malicious profile look like?



1 Profile picture

Picture of attractive individual in business attire.

2 Company affiliation/description

Generic, non-descript consultancy or recruitment company. Reference to defense, government contacts, or ‘state owned’ enterprises.

3 Profile name

Typically this is a common Western first name followed by a non-Western surname.

4 Unrealistic job roles

Senior or high-profile job role with a young profile picture.

5 Mutual contacts

Contacts with mutual friends may have been made to make the profile appear more legitimate. Many people don’t fully check the profiles of new requests.