



Fort Bliss Antiterrorism/ Force Protection Program

Risks of Social Media Use

Social Engineering Attacks Awareness

In social engineering, the attackers use human interaction (social skills) to obtain or compromise information about an organization or its network / computer systems. By asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the organization and rely on the information from the first source to add to his or her credibility.

How to Avoid Being a Victim.

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company or IT helpdesk.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

***If you are approached through your workstation,
report to IT personnel immediately.***

For more information, go to <https://www.bliss.army.mil/iWATCH/>