Principles of Influence: Robin Sage Case Study of Social Engineering

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**Principles of Influence: Robin Sage Case Study of Social Engineering**

1. **Robin Sage Profile:**

According to Chapple & Seidl (2023), Thomas Ryan of Provide Security created a fake social networking profile name “Robin Sage”. Thomas used photos lifted from an adult website and created an entire false background as a Cyber Threat Analyst with the Navel Network Warfare Command.

1. **Principles of Social Engineering in Robin Saga:**

There are multiple principles of influence that Thomas uses in “Robin Sage” Profile:

* Principle of liking: Thomas deliberately creates a profile of a young, attractive, and edgy female because much of the security industry is comprised of males. The heavily male-dominated sector allows women to be commodities in more ways than one.
* Principle of Social Proof: By gaining respected connections with the security community, “Robin Sage” quickly attracted the attention of hundreds of other members of the security community.

1. **Potential Targets Reacted to Robin Sage**

There are multiple line staff and senior executives from NSA, DOD, military, Fortune 500, and other sources that make specific contact with Robin Sage about experiments that they work on, job opportunities, gifts, and invitations to speak at security conferences. Robin Sage’s next step could seek to obtain sensitive information and systems within her network and demonstrate a definite risk to cyber security

References

Chapple, M., & Seidl, D. (2023). Chapter 6: The Evolving Threat: From Script Kiddies to Advanced Attackers. In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 103–124). essay, Jones & Bartlett Learning. (1)