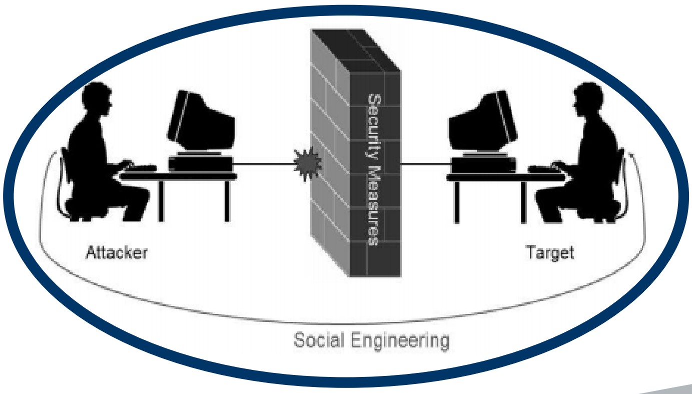
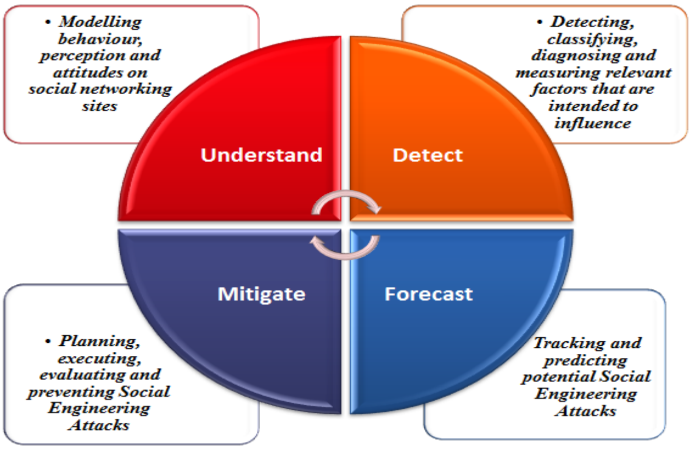
Focus on CSIR services in

Cyber Defence: Social Engineering

Firewalls, intrusion detection and anti-viruses are the most common defence mechanisms for network systems. However, these can be bypassed by manipulating the human vulnerabilities. This is the process of Social Engineering.





- Modelling behaviour, perception and attitudes on social networking sites

- Detecting, classifying, diagnosing and measuring relevant factors that are intended to influence

- Planning, executing, evaluating and preventing Social Engineering Attacks

Tracking and predicting potential Social Engineering Attacks

our future through science

Social Engineering Attack Detection

The CSIR has developed a model which is used to perform early detection of social engineering attacks. This model utilises both psychologically-based principles as well as trust models.

Data Harvesting and Profiling

Many users utilise social networking sites with the purpose to connect with people, share information and create content. Users unknowingly share information that could be used for nefarious purposes against them. A social engineering attack requires data to assist cyber criminals to create a profile to understand the target. The analysis of this data by the attackers is used to get a better understanding of the methods to use to lure the target into performing an attack - for example opening a malicious file that contains embedded malware.

Contact details

Defence Peace Safety and Security

Francois Mouton
FMouton@csir.co.za
012 841 2242

Aubrey Labuschagne
WLabuschagne@csir.co.za
012 841 4536

dpss@csir.co.za