**Preparing the ground for attack**:

* Identifying the victim
* Gathering background information

**Closing the interaction, ideally** **without arousing suspicion :**

* Removing all the traces of malware
* Covering tracks

SOCIAL

ENGINEERING

CYCLE

**Obtaining the information over a period of time:**

* Expanding foothold
* Executing the attack

**Deceiving the victim to gain a foothold**:

* Engaging the target
* Spinning a story
* Taking control of the interaction

Social Engineering Attack Life Cycle