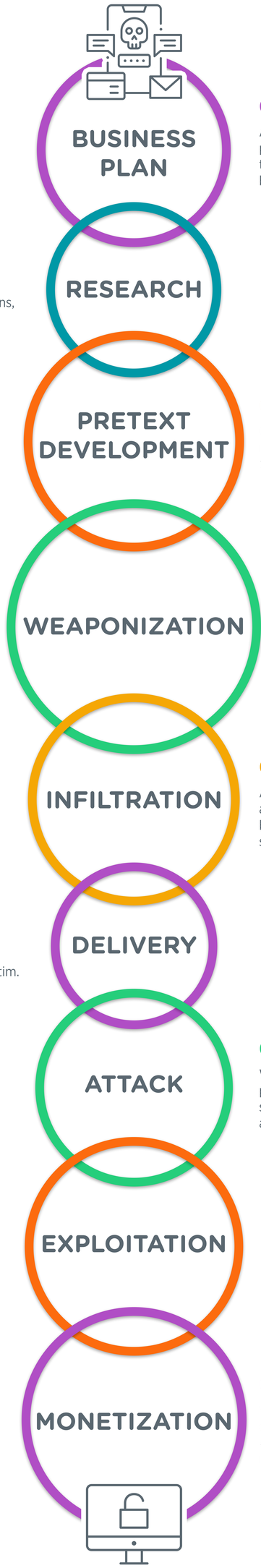
CompTIA

The Process of Social Engineering

Social engineering requires research, development, and flawless execution to work.



01. BUSINESS PLAN

Attackers start by carefully planning specific tactics, techniques and procedures to bring them success.

02. RESEARCH

Then, they conduct detailed data analysis of the victim, including information about behavior patterns, interests and devices.

03. PRETEXT DEVELOPMENT

Choosing the medium and the message are equally important and take up much of the attackers' time.

04. WEAPONIZATION

The most sophisticated social engineering attacks involve creating software to exploit the breach of trust.

05. INFILTRATION

Attackers find ways to get inside an organization and manipulate its business processes and existing security procedures.

06. DELIVERY

The attackers then deliver the weaponized technology to the victim.

07. ATTACK

While the end user is often the party that initiates the attack, sometimes infiltration, delivery and attack all happen at once.

08. EXPLOITATION

Many times, exploitation occurs a considerable amount of time after the delivery and attack.

09. MONETIZATION

Some attackers use stolen credit card data, while more sophisticated attackers pass off assets to networks of third parties.

Turn to CompTIA.org to learn more about cybersecurity and how to stay ahead of bad actors.