Social engineering often relies on manipulating human psychology. What are the foundational principles or psychological tactics that social engineers exploit to deceive their targets?

Answer: Social engineering capitalizes on psychological principles such as authority, urgency, and social proof, manipulating targets into divulging confidential information or performing actions that compromise security. Tactics like impersonation, emotional manipulation, and exploiting the natural human tendency to be helpful are commonly used to deceive targets.

Pretexting involves creating a fabricated scenario or pretext to obtain information. How do attackers use pretexting in social engineering campaigns, and can you provide a real-world example of a notable pretexting incident?

Answer: In social engineering campaigns, attackers use pretexting by crafting believable stories or scenarios to gain trust and extract sensitive information from their targets, often posing as authority figures or trusted entities. A notable example is the 2016 incident involving a hacker posing as a tax officer to deceive an employee of the Australian government's Family and Community Services department, resulting in the unauthorized access to personal data of clients.

Every year, new social engineering schemes make headlines. Can you recall a recent major incident involving social engineering that impacted a significant number of people or a notable organization?

Answer: In 2020, a significant social engineering attack targeted Twitter, where attackers manipulated employees to gain access to high-profile accounts, including those of Elon Musk and Barack Obama, to perpetrate a Bitcoin scam. This attack impacted numerous users and highlighted the vulnerability of even major tech companies to sophisticated social engineering tactics.