SOCIAL ENGINEERING

Social engineering is the art of "hacking the human." If a strong password secures a system, it is a lot faster to trick someone into giving you the password than using a password cracker. It is easy to make fun of the idea of being tricked into revealing your password. However, this sort of mocking is why social engineering is so effective. Social engineering takes advantage of the cognitive biases and social norms that we grew up with and uses those biases and norms to manipulate us.

The Principles of Social Engineering

Like hacking, social engineering has core principles applied in various ways to manipulate a target. While the core principles in hacking exploit the design of our technologies, the principles used in social engineering exploit our cognitive biases and social norms.

Principle 1: Consensus

Consensus, also known as Social Proof, is when a social engineer convinces victims that others have already trusted them. There are many ways to apply consensus to social engineering. Some examples are fake website reviews on social media, forged work orders, using deep fake technology to impersonate someone over the phone in real-time.

Principle 2: Familiarity

Familiarity, also known as Trust, refers to a social engineer using charisma and likeability to get a victim to complete a request. Familiarity is often as simple as striking up a friendly conversation with a victim before making a request. It is often even more effective if the social engineer is, or appears to be, part of the victim's "in-group." For example, striking up a conversation with a security guard about the struggles of the night shift or manipulating an inexperienced receptionist by pretending it is your first day and you forgot your badge.

Principle 3: Urgency

Urgency, also known as Scarcity, refers to a social engineer creating a sense of hurry to put time pressure on a victim. Creating a sense of urgency discourages the victim from thinking critically about the request while also making them feel like they are helping someone in need. Urgency is a time-honored tradition among scammers. One example is emails and robocalls informing you that your warranty is about to expire unless you ACT NOW!

Principle 4: Authority

Authority, or Intimidation, is a high-risk strategy in which a social engineer attempts to intimidate a victim or claim authority over them. While usually more subtle than "Don't you know who I am," Intimidation is not a subtle strategy. It has an elevated risk of the victim reporting the incident rather than complying. More practically, Authority can be combined with Consensus to create the illusion that not only is the social engineer already trusted but that they are trusted by someone with authority over the victim.

Conclusion

Social Engineering is a very effective tool used by ethical and malicious hackers alike. While strong technological security is important, ignoring the human aspect of security creates a severe vulnerability that threat actors can easily exploit. Protecting against social engineering is more than annual training; it requires creating a security culture where people understand their importance and the threats they may face.