Steps Used in Typical Digital Attacks

Social Engineering in Organizational Security

Social engineering is a tactic used in cybersecurity attacks that exploits the human element of organizations to bypass security measures. It relies on manipulating individuals into breaking normal security procedures and best practices to gain unauthorized access to systems, data, or physical locations, or to coax individuals into performing actions that are against an organization's interests. Social engineering targets the natural tendency of people to trust.

At its core, social engineering recognizes that it is often easier to exploit human psychology than to defeat complex technical security measures. This method can take many forms, including phishing, spear phishing, pretexting, baiting, tailgating, and quid pro quo, each exploiting different aspects of human behavior and trust.

The human risk in organizational security is significant because even the most technologically secure systems can be compromised through human error or manipulation. Mitigation strategies include education and awareness training, simulated attacks, security policies and procedures, physical security measures, and incident response planning.

Organizations employ several strategies to mitigate the risk of social engineering, including education and awareness training, simulated phishing and social engineering campaigns, security policies and procedures, physical security measures, and incident response planning. The human element remains one of the weakest links in the security chain. By acknowledging and addressing the risk of social engineering, organizations can better protect their assets, data, and reputation.