CHECK MARK SECURITY

Let our experts check your security posture

SOCIAL ENGINEERING DEFENSE TEST

Purpose

Attackers can connect to the internet from anywhere in the world. They can then launch remote social engineering attacks against your organization. Employee contact info is readily available online and can be mass-collected. With this information, social engineers can send phishing emails, vishing calls, or smishing texts to your employees. Remote social engineering is the most common attack method, as it has a high success rate due to its mass targeting.

Remote Social Engineering tests verify if a remote attacker can trick employees into giving confidential information. This could be used to access private data without authorization. Remote social engineering attacks are a common way for attackers to access protected information. So, it's crucial to test employees to ensure they don't fall for a real-world social engineering attack.

Objective

The primary objective of the CheckMark Remote Social Engineering engagement determines whether or not organizational employees are susceptible to social engineering attacks and/or are knowledgeable of company Information Security policies.

Scope

The messages and calls during the Remote Social Engineering test can be sent to any employee with a corporate phone. The client determines the number of employees to be tested and selects the message(s) used in the smishing engagement. During project scoping, the ISA and the client will agree on the list of employees to contact, the message template(s) to use, and the day(s) to send the messages.

Book a meeting at
sales@checkmarksecurity.com

CHECK MARK SECURITY

Let our experts check your security posture

Voice Phishing (Vishing) Threat Landscape 2024:

Contact us for the Threat Landscape
sales@checkmarksecurity.com