

Security Management Partners

Social Engineering Assessment



SECURITY MANAGEMENT
PARTNERS

People are your weakest link, not technology.

Security awareness is more important than ever. Your employees must understand the importance of their role in protecting the business. Social engineering tests validate the strength of your training and policies, the comprehension and compliance of staff, and the viability of physical controls.

Real Information Security from the Independent Experts

Companies Lose *Hundreds of Millions* of Dollars Each Year From Social Engineering Attacks.

Social Engineering uses non-technical or low technology means of exploitation, such as lies, impersonation, tricks and invented scenarios to achieve unauthorized access, potentially breaching a valued system and the information that resides on that system.

What is The Goal of a Social Engineering Assessment?

It is NOT to confirm the level of Security Management Partners' trickery, but to examine and validate your organization's current training and security posture by testing employee comprehension and compliance with existing policies, controls and procedures.

Common Social Engineering Tests

Physical—Physical security is a combination of people, processes, procedures, and equipment to protect resources. SMP works with clients to create a physical social engineering testing plan that makes sense. The assessment can be passive, such as looking for passwords out in the open and observing physical controls. Security Management Partners can also actively attempt to breach physical security, gain physical access to the premises, obtain records, realize network access, remove equipment, and more.

Phone Calls—With client-approved scripts, SMP Consultants phone designated personnel in a series of calls, attempting to manipulate employees into performing actions or divulging confidential data such as passwords, usernames, and other useful information that would allow an intruder access to a system and acquire protected information.

Phishing Emails—With each client, Security Management Partners crafts a phishing-style e-mail intended to trick recipients into clicking on a link within a bogus e-mail, either by spoofing the organization's email address (i.e. from sender `smpone.net` instead of `smpone.com`) or by creating an external phishing message (i.e. 'You have received a greeting card'). Emails are sent to multiple individuals in a number of corporate locations identified by the client.

CONTACT SMP

391 Totten Pond Road Suite 201 Waltham, MA 02451

Phone: 781-890-7671 Fax: 781-890-1454

www.smpone.com

