SOCIAL ENGINEERING

Social Engineering is one of the biggest threats to information security. It is so successful due to the fact that it targets the weakest point in your organization – your employees!

Accume Partners has developed proven tactics to locate and isolate potential weaknesses in social engineering awareness, as well as provide the proper guidance and expertise to help strengthen those areas of concern.

Our Social Engineering services include:

- Phone Impersonations
- Email Phishing Attacks
- Baiting Attacks
- Physical Social Engineering
- Social Engineering Awareness Training

PHONE IMPERSONATIONS

Phone impersonations are intended to obtain sensitive information by way of misrepresenting a caller. The goal is to attempt to trick people into revealing information that could compromise a targeted system's security or release confidential information over the telephone.

EMAIL PHISHING ATTACKS

Phishing is the most successful form of social engineering utilizing email to entice unsuspecting recipients to either click on a link to a malicious website or provide some form of credentials.

BAITING ATTACKS

Baiting is when an attacker leaves malware infected media in an open location. The attacker gives it a legitimate-looking label to pique interest and waits for the victim to use the device and execute the files on it. Upon inserting the media into a computer to see the contents and executing one of the files, the user would unknowingly install malware onto their computer, likely giving an attacker unrestricted access to it.

PHYSICAL SOCIAL ENGINEERING

Physical social engineering is a technique of obtaining physical access to sensitive areas through physical interaction with employees. The aim is to bypass the physical security measures implemented at a given location to gain access to restricted areas, such as phone closets, data centers and record rooms. Once inside the restricted area, an attacker will attempt to gain access to computers, networking equipment or sensitive files and documents.

SOCIAL ENGINEERING AWARENESS TRAINING

Social engineering awareness training provides organizations information on social engineering tactics, to include phone Impersonation, physical impersonation, phishing and baiting, and the countermeasures that can be used to thwart these types of activities. Topics include detection, prevention and methods to help maintain awareness.

TO LEARN MORE, PLEASE CONTACT:
Michael Barrack, Managing Director
702.461.8682 or **mbarrack@accumepartners.com**