A Practical Approach for Combating Social Engineering In Your Enterprise

Albert Lewis
Secure IT Solutions, Inc.

Abstract:

In 2004, Gartner Vice President Rich Mogull stated: "We believe that social engineering is the single greatest security risk in the decade ahead." Yet many organizations still do not understand how to prepare their people for this threat. Sophisticated hardware and software countermeasures are no match for the low-tech social engineer who bypasses these controls to attack unsuspecting users. This session presents a thorough discussion of the psychology behind social engineering (SE), why people are easy prey for the SE hacker, and practical ways to educate users so that they can avoid becoming victims. It will also address social engineering vulnerability testing and the rationale for why this should be included as part of any organization's regular security assessments.

Biography:

Albert Lewis, CISSP-ISSMP, CISM, NSA IAM, IEM, PMP, ITIL
President and COO
Secure IT Solutions, Inc.

Mr. Lewis has 20 years of experience in systems integration, network security operations, and risk management. He has extensive experience in information security program development and currently advises several federal government clients on matters of information security. He helped create the Security Operations Center for the Army National Guard Headquarters in response to 9/11. He has an MS in Information Systems Management from Johns Hopkins University. He is a Certified Information Security Manager (CISM) and a Certified Information Systems Security Professional (CISSP). He is also certified by NSA in their INFOSEC assessment and evaluation methodologies. He has developed and successfully presented at four prior security conferences (NetSec 2006, CSI 2007, and USDA Cyber Security Expo 2007 and 2008). He is a member of the adjunct faculty at Johns Hopkins University where he teaches graduate classes in information security.