

Social Engineering in the 21st Century

Attack Techniques and Practical Defense



Presented by Gabriel Serafini, CISSP

Founder / CEO Securanix, LLC

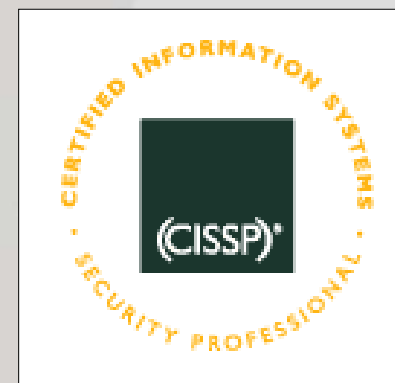
Email: gserafini@securanix.com

© 2003 Securanix, LLC

WWW.SECURANIX.COM

Who am I?

- **Gabriel Serafini - gserafini@securanix.com**
- **Founder / CEO of Securanix, LLC – a local managed security services provider**
- **Certified Information Systems Security Professional (CISSP)**
- **Web developer since 1996**



What is Social Engineering?

Definition:

Social engineering is the art and science of getting people to comply with your wishes for the purpose of gaining unauthorized access, control or disruption of resources.

Typical Targets for Social Engineering

- **Large Corporations**
- **Telephone Companies**
- **Financial Institutions**
- **Hospitals**
- **Government Agencies**
- **Military**

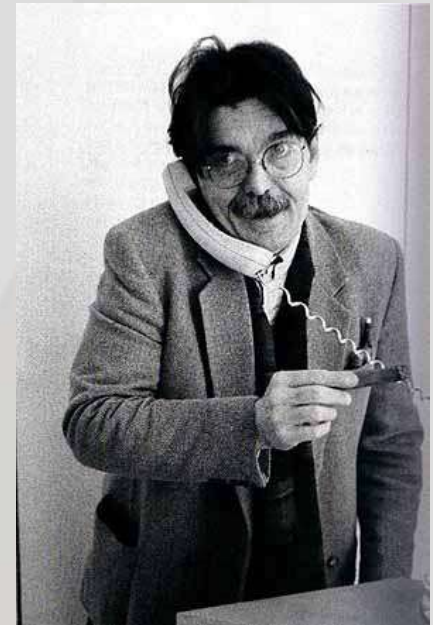


Why Should I Care?

- **Loss of valuable trade secrets**
- **Entire organization can face embarrassment**
- **Loss of competitive advantage**
– **impacts bottom line**
- **Handing over keys to your resources to unauthorized user**

Attack Techniques

- **Telephone Conversation**
- **Help Desk / Customer Service**
- **Dumpster Diving**
- **From the Internet**
- **Persuasion**
- **Reverse Social Engineering**



Telephone Conversation

- **Easy – only equipment required is a telephone**
- **Low risk – no physical presence required**
- **Utilizes natural inclination to trust other people**
- **Can create sense of urgency**

Help Desk / Customer Service

- **They're there to HELP users get information**
- **Often low-paid, little motivation to "Watch out for the Company"**
- **Low emphasis on security**
- **Hard for target to actually verify identity of caller**

Dumpster Diving

- **Can be excellent source of intelligence about organization**
- **Post-it® notes – glowing little nuggets of useful information**
- **Phone books, calendars, memos**
- **Old equipment – hard drives can be recovered**

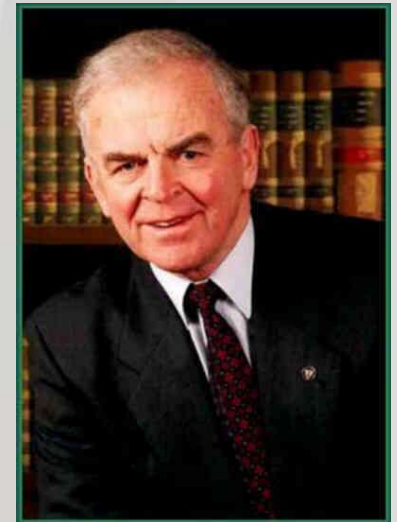
Internet Delivered Attack

- **Fastest-growing area of social engineering**
- **Can be even easier than telephone and more anonymous**
- **Users react in predictable ways**
- **Backdoor programs often emailed as attachments**



Persuasion

- **Psychological element of Social Engineering**
- **Appeals to emotion – empathy, helpfulness, kindness**
- **Impersonation**
- **Authority figure, trusted**
- **Third-party & “newbie” approach used**



Reverse Social Engineering

- **Advertise being the person to call for certain type of problem**
- **Cause problem to happen**
- **Help fix problem, verifying position of trust**
- **Ask for innocuous bit of information – no harm**



Practical Defense Strategies

- **Difficult to eliminate the human inclination to trust others**
- **Organization-wide training and awareness program are the best defense**
- **Enforce Security Policy**
- **Have single point of contact**

Practical Defense Strategies (cont.)

- **Shred all documents prior to disposal, important or not**
- **Use bulk-erase equipment on discarded hard drives**
- **Perform informational audit on publicly available data for sensitive or useful tidbits**

Testing Your Defenses

- **Should test for Social Engineering weaknesses on a regular basis – use the same tactics that attackers might use**
- **Educate workforce, then verify the information is understood**
- **Share results of tests so that all can see the value of compliance**

Summary

- **Defense against Social Engineering is a never-ending battle – training & education most effective tools to defend**
- **Problem won't go away if you simply ignore it**
- **Think like an attacker to defend effectively**

Questions / Answers

