Social Engineering in the Business World:

Battling the Art of Deception

Media BUZZ

July 9, 2009

Possibility Room, National Library Board Singapore

What is social engineering?

- A collection of techniques for information gathering or computer system access
- Uses manipulation and deception to obtain important and often confidential information from people
- In most cases, victims never come face-face with their attacker

The Realm of Social Engineering

- Basically, hackers make use of the human tendency to trust
- According to Kevin Mitnick, “You could spend a fortune purchasing technology and services… and your network infrastructure could still remain vulnerable to old-fashioned manipulation.”

The Realm of Social Engineering

Social engineering attack vectors:

- **Phishing**
  The act of acquiring personal/sensitive information by masquerading as a trustworthy entity in an electronic communication.
- **Link Manipulation**
  Designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization.

The Realm of Social Engineering

- **Website spoofing and forgery**
  Java script commands are used to alter an address bar
- The rise of cross-site scripting
- **Pop-up windows**
- **Passwords**
- **The Posers & Impersonators**
- **Trojan Horses & Other Malicious Malware**

The Realm of Social Engineering

- **Spam**
  In May 2009, the global ratio of spam in email traffic from new and previously unknown bad sources was 90.4%, an increase of 5.1% since April 2009 (Source: Symantec's MessageLabs May 2009 Intelligence Report)
- **Vishing**
  The practice of leveraging VoIP technology for financial rewards

The Realm of Social Engineering

- **Social Networks**
  With the level of interest in social networking gaining traction in the business world, social networking sites are increasingly on the radar of cybercriminals.
- Personal data is more easily available and accessible.
- Beware of impersonators
- Risk that social engineers gain confidential company information or are able to hack your company network

The Realm of Social Engineering

The Need for In-Depth Defence

- One of the greatest dangers of social engineering is that a single successful victim can provide enough information to trigger an attack that will affect an entire organization.
- Therefore, it is crucial to create a security aware culture within the organization itself.
- Provide regular/ongoing security awareness training for employees/

The Realm of Social Engineering

Conclusion

- Bear in mind that the risks of social engineering are significant
- While you cannot prevent social engineering completely, you can put reasonable controls and processes in place
- Remember that technology can only do so much

The Realm of Social Engineering

Thank you!

Shanti Anne Morais
MediaBUZZ Pte Ltd
shanti@mediabuzz.com.sg