Protecting Information Assets
- Week 5 -

Creating a Security Aware Organization
MIS5206 Week 5

• In the News
• Readings
  – Vacca Chapter 16
  – HDFC BANK – case due
  – SANS Assignments 1, 2
• Creating a Security Aware Organization
• Test Taking Tip
• Quiz
In the News

• Discuss items “in the news”
Reading

- Vacca Chapter 16
- Case: HDFC BANK – due today
- SANS Assignments 1, 2
Creating a Security Aware Organization

Because of the importance of defending against social engineering and other information security threats, an ongoing awareness program is vital.
Why is Security Awareness Essential?

• We have a culture of trust that can be taken advantage of with dubious intent

• Most people feel security is not part of their job

• People underestimate the value of information

• Security Technologies give people a false sense of protection from attack
Why is Security Awareness Essential?

- We have a culture of trust that can be taken advantage of with dubious intent
- Most people feel security is not part of their job
- People underestimate the value of information
- Security Technologies give people a false sense of protection from attack
Training Course Content

Social engineering attacks have the same common element: deception

• Verify the identity of the person making an information request

• Verify the person is authorized to receive the information
Basic Security Policies

• Every employee should be instructed in how to devise a difficult-to-guess password

• Every employee should know their responsibility to comply with the policies and the consequences for non-compliance
Security Policy Types

• Security policies related to computer and voice mail passwords

• The procedure for disclosing sensitive information or materials

• Email usage policy, including the safeguards to prevent malicious code attacks including viruses, worms, and Trojan Horses

• Physical security requirements such as wearing a badge
Security Policy Types (continued)

• The responsibility to challenge people on the premises who aren't wearing a badge

• Best security practices of voice mail usage

• How to determine the classification of information and the proper safeguards for protecting sensitive information

• Proper disposal of sensitive documents and computer media that contain, or have at any time in the past contained, confidential materials
Warning Signs of a Social Engineering Attack

• Refusal to give call back number
• Out-of-ordinary request
• Claim of authority
• Stresses urgency
• Threatens negative consequences of non-compliance
• Shows discomfort when questioned
• Name dropping
• Compliments or flattery
• Flirting
Common Social Engineering Strategies

• Posing as a fellow employee
• Posing as an employee of a vendor, partner company, or law enforcement
• Posing as someone in authority
• Posing as a new employee requesting help
• Posing as a vendor or systems manufacturer calling to offer a system patch or update
• Offering help if a problem occurs, then making the problem occur, thereby manipulating the victim to call them for help
• Sending free software or patch for victim to install
Common Social Engineering Strategies (continued)

• Sending a virus or Trojan Horse as an email attachment
• Using a false pop-up window asking user to log in again or sign on with password
• Capturing victim keystrokes with a computer system or program
• Leaving a floppy disk or CD around the workplace with malicious software on it
• Using insider lingo and terminology to gain trust
• Offering a prize for registering at a Web site with username and password
Common Social Engineering Strategies (continued)

• Dropping a document or file at company mail room for intra-office delivery
• Modifying fax machine heading to appear to come from an internal location
• Asking receptionist to receive then forward a fax
• Asking for a file to be transferred to an apparently internal location
• Getting a voice mailbox set up so call backs perceive attacker as internal
• Pretending to be from remote office and asking for email access locally
Why is Security Awareness Essential?

• We have a culture of trust that can be taken advantage of with dubious intent

• Most people feel security is not part of their job

• People underestimate the value of information

• Security Technologies give people a false sense of protection from attack
Test Taking Tip

- If you don’t know the answer ... guess and then move on -

Your score will be higher if you guess and move on even if your guess is wrong

Here’s why:
• Most certification tests do not penalize for wrong answers. That is, they only count the number of correct answers in computing the score
• In a 4 option multiple choice test, guessing at questions to which you do not know the answer is likely to get you an additional right answer ¼ of the time
• Guessing, and then moving on, gives you time to answer the questions that you do know, raising your score
Quiz