Social Engineering

Objectives

- Understand what social engineering is
- Recognize the signs of social engineering
- Learn how to protect yourself and your organization from it

Definition

- My simple definition – “To gain some advantage through human manipulation”
- Typically it’s to obtain confidential information
  - Passwords
  - Financial data
  - Confidential company data
- Other instances it’s far more serious
  - Steal money
  - Install malware

Examples

- Phishing
  - One of the easiest ways to have someone give up their information
  - User receives an email pretending to be someone they aren’t
  - User gives up password because “The IT Help Desk told me my account was going to be shutdown unless I logged in!”
- Phone calls
  - IRS
  - Microsoft
  - Symantec
  - “Your vehicle warranty is about to expire!”
  - “This is card member services. We have a great option to lower your debt”

The security questions…

- Believe it or not, it is not difficult to guess your “secret” questions from an online account
- What’s your first pet
- Where were you born
- What’s your high school mascot
- What is your mothers maiden name
- Add questions it’s better, but not fool proof

Well Known attacks

- From ancient Greece – Trojan Horse
- 2007 attack on the ABN Amro Bank. Got away with $28 million on gems
- 2013 attack on Associated Press twitter account
- Nigerian Price scams – $12.7 billion annually
- Target breach
- Anonymous vs HB Gary Federal

Ways to protect yourself

- Recognize accurate requests for information
  - Chances are there will never be any. You need to call.
- Understand that every link could potentially be dangerous and look closely
- Use two factor authentication when possible in case something happens
- Use a password manager
- It is up to you to ensure you are not the link that broke the chain