Testing Social Engineering

1. Call the receptionist from an outside line when the sales manager is at lunch. Tell her that you're a new salesperson, that you didn't write down the username and password the sales manager gave you last week, and that you need to get a file from the email system for a presentation tomorrow. Does she direct you to the appropriate person or attempt to help you retrieve the file?
2. Call the human resources department from an outside line. Don't give your real name but instead say that you're a vendor who has been working with this company for years. You'd like a copy of the employee phone list to be emailed to you, if possible. Do they agree to send you the list, which would contain information that could be used to try to guess usernames and passwords?
3. Pick a user at random. Call them and identify yourself as someone who works with the company. Tell them that you're supposed to have some new software ready for them by next week and that you need to know their password to finish configuring it. Do they do the right thing?

The best defense against any social engineering attack is education. Make certain that the employees of your company know how to react to the requests presented here. Social engineering works on the premise that people try to help when they are vested in your efforts, such as a co-worker or if you are trying to help them.