

REMINDER: Emailed to a group account. Do NOT reply using email group account.
For comments or inquiries email infosec@pjlhuillier.com.



April 26, 2013 Release # 212

-- Begin Transmission --

Top 10 Social Engineering Tactics – Part 2

Top 10 Social Engineering Tactics – Part 2

9. Piggyback Rides

It's surprising to know that piggybacking is still one of the most effective ways to an organization. With piggybacking, a social engineer appears as a legitimate employee and walks into a secure building by following behind someone who has access.

A classic example is a social engineer showing up at the front door of a secure facility on a rainy day, carrying a heavy box. As an employee walks up, the social engineer takes advantage of human kindness by saying, "Would you mind opening the door for me? I can't reach my badge to open the door while carrying this box." Because people generally want to help others, the employee will open the door granting access to the social engineer.



8. Techie Talk

Many penetration testers and malicious hackers do social engineering by pretending to be a technical support or IT helpdesk personnel because this position is closest to the users.

Here is an example of what that phone call may look like:

Social Engineer: "Hello. This is Andrew from the help desk. Hey listen, we've been noticing that some passwords have leaked out, and we are calling around to make sure that people are changing their passwords. We think your password may have been compromised, so if you don't mind, I'd like to walk you through changing it."



User: "Sure."

Social Engineer: "Great! First, I want you to hold down the Control button, the Alt button, and the Delete button at the same time. That will bring up a new screen that has several buttons. Once this appears, click on the Change Password button. Now it's important that you type in a secure password that contains a good mixture of uppercase and lowercase letters as well as numbers so that it is difficult for an attacker to hack into your computer. What password are you going to use?"



User: "Hmm...let me think. How about clh123!!? Is that secure?"

Social Engineer: "Absolutely. Go ahead and type in the new password and press OK. I really appreciate you taking the time to do this to keep your computer secure."



The social engineer was able to use his knowledge of technology to convince a user to give out a password.

...to be continued

-- End of Transmission --

Information Security: It's a Shared Responsibility
REFERENCE(S): <http://www.informit.com/>

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.