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

May 24, 2013 Release # 216

-- Begin Transmission --

Top 10 Social Engineering Tactics – Final Part

Top 10 Social Engineering Tactics – Final Part

1. Listening to Conversations in Public Places

The best sources of information where social engineers can gather from his target victims are probably at restaurants, coffeehouses and bars. These places are everybody's favorite "hang-outs" when meeting friends, colleagues, relatives, and other people to talk about everything --- personal, business, and other matters while enjoying food and drinks. The social engineer can stalk on his target victim, sit somewhere near him and pretend to be doing something else so that he could not be recognized. He can then listen to the conversations and gather enough information he needs and even interact with his target victims by throwing conversations about common people, events and other topics just to establish rapport and become friends. From there, he can start juicing his victim for relevant information.

These are just a few of the many techniques used by social engineers: majority is for financial gains, revenge, personal interest, intellectual challenge, external pressure, damage containment, and politics.

What can I do?

✓ *Be educated, aware, and a little bit paranoid.* Never give out usernames and passwords. Never tell anyone sensitive information as ID numbers, PIN numbers, server names, system Information, credit card numbers, etc.).

✓ *Be aware of what is being asked over the phone.* Ask for a full and correct spelling of their name, a call back number, and why they need the information. Have them contact the correct information source directly if asked for information managed by someone else. When in doubt, put the caller on hold or tell them you will call them back. This gives you time to log any strange calls and verify if it is ok to give out information.

✓ *Be aware of what is being asked over the internet.* Be aware of what is being asked over the phone. Avoid any requests to enter account information for verification by following a link in the e-mail (this is known as phishing). Never be pressured to comply when someone says "Do you know who I am?" When in doubt, contact information security department or your supervisor.

✓ *Others.* Shred and secure any document that someone can obtain by looking through your trash.

✓ *Always.* When in doubt, ask the person to wait while you verify (a) identity, (b) need to know, and (c) if you are the rightful/authorized source of the information.

Social engineering will always be around. As long as you are willing to have a healthy level of paranoia and good common sense, you do not need to fear them.

…to be continued

-- End of Transmission --

Information Security: It's a Shared Responsibility
REFERENCE(S): http://www.informit.com/
http://www.seasnet.ucla.edu