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

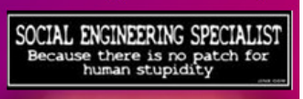
April 19, 2013 Release # 211

-- Begin Transmission --

Top 10 Social Engineering Tactics – Part 1

Top 10 Social Engineering Tactics

If someone you trusted has ever tricked you, you know what it feels like to be socially engineered. This issue will explain both technical and non-technical techniques used by social engineers today to gain trust and manipulate people for their benefit.



The easiest way to get into a computer system is to simply ask permission. At the end of the day, no matter how much encryption and security technology you have implemented, a network is never completely secure. You can never get rid of the weakest link—the human factor. It does not matter how many security solutions have been implemented if the employees give their access to systems to anyone who asks for it.

Who is a Social Engineer?

A social engineer is someone who uses deception, persuasion, and influence to obtain information, or gain access to take certain action. It may also include positive forms of communication with parents, therapists, children, spouse and others.

Social engineering is more than just being a con artist; it is about understanding human psychology and having a methodical way of influencing someone to either give out sensitive information or grant you unauthorized access. In other words, it is not about being a good liar; it is about being an engineer who discovers ways to manipulate people for his advantage.

This article outlines 10 of the most popular techniques used by Social engineers to reach their goals.

10. Social Engineering in Reverse

Reverse social engineering (RSE) has three steps: sabotage, advertising, and assisting. In the first step, a social engineer finds a way to sabotage a network. This can be as complex as launching a network attack against a target website, to as simple as sending an email from a spoofed email address telling users that they are infected with a virus. No matter what technique is employed, the social engineer has either sabotaged the network or given the impression that the network is sabotaged.

Next, the social engineer advertises his or her services as a security consultant. This can be done through many means including sending mailers, dropping business cards, or sending emails that advertise his or her services. At this point, the social engineer has created a problem in the network (sabotage) and is placing himself/herself in a position to help (advertising). The corporation sees the advertisement, contacts the engineer under the false pretence that the social engineer is a legitimate consultant, and allows the social engineer to work on the network. Once in, the social engineer gives the impression of fixing the problem (assisting) but will really do something malicious, such as planting keyloggers (a type of surveillance software that has the capability to record every keystroke on keyboard) or stealing confidential data.

…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.