Pavel Volik
A.T. Khar', research supervisor
I.I. Zuyenok, language adviser
SHEI "National Mining University", Dnipropetrovsk

Social Engineering in the Context of Information Security

Nowadays, in the era of computers and internet people start using computers in all spheres of life: from entertainment to conducting of monetary issues that could not be missed by various fraudsters. They have adapted their techniques for computer and internet use and received the great skills in obtaining information remotely. A new science, named social engineering, as a result of using them has been emerged.

Social engineering (SE), in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information.All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware", are exploited in various combinations to create attack techniques.

Let us have a look at an e-mail as a tool of social engineering. For example, one has received a letter from the bank requesting "verification" of information and warning of some dire consequence in case it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN. One doesn`t notice some details that may reveal the fraud and provide the malefactor all s/he needs.

Another great tool of social engineering is a Trojan horse or Trojan. One finds something s/he needs or is interested in (program, video, etc.), and while running/saving/watching its/he installs the malicious software. This method relies on the curiosity or greed of the victim.

The other tool of SE are social networks. They can be used for gathering information on the victim or identity theft. This information can be used for some scrams in future.

But sometimes the fraudster doesn`t need to resort to such tricks. People are willing to give a secret password for a candy bar. According to the research provided by Infosecurity Europe 21% of the participants gave a password and 61% revealed their birth dates and gain chocolate as a prize.

In conclusion, here are corner stones for the success of the social engineering:

- people treat their private information very carelessly;
- people are too curious;
- people are inattentive to details.

If you are aware of these, you have more chances to avoid frauds and take wrong actions.