Social engineering exploits networks' weakest point—people

May 12 2016

It requires a lot of effort and expense for computer hackers to program a Trojan virus and infiltrate individual or company computers. They are therefore increasingly relying on psychological strategies to manipulate computer users into voluntarily divulging their login details. These methods are known as "social engineering." For the first time, psychologists at the University of Luxembourg have conducted a large-scale study (involving 1,208 people) to investigate how people are manipulated into sharing their passwords with complete strangers in return for small gifts.

"Social engineering targets the weakest link in the chain, and that is the user," said Dr André Melzer, co-author of the study "Trick with treat - Reciprocity increases the willingness to communicate personal data," which appeared in the most recent edition of the renowned journal *Computers in Human Behavior*. "More specifically, we investigated the psychological principle of reciprocity. When someone does something nice for us, we automatically feel obliged to return the favour. This principle is universal and important for the way we function as a society. However, this internal pressure can also be exploited to achieve certain purposes, such as encouraging someone to divulge a password."

During the experiment, researchers asked randomly selected passers-by about their attitude towards computer security, but also asked them for their password. The interviewers were carrying University of Luxembourg bags, but were otherwise unknown to the respondents. In one condition, participants were given chocolate before being asked for

their password, while in the control group they were only given chocolate after the interview. The research showed that this small gift greatly increased the likelihood of participants giving away their password. If the chocolate was only given out afterwards, 29.8 per cent of participants revealed their passwords. However, if the chocolate was received generally beforehand, a total of 43.5% of the respondents shared their password with the interviewer. The willingness to divulge passwords increased further if the chocolate was offered immediately before the participants were asked to disclose their password. Here, the internal pressure felt by the recipient appeared to be particularly high, with 47.9% giving away their passwords, compared with 39.9% of participants who received their gift at the beginning of the interview.

The study shows how easy it is for people to be manipulated with the help of a simple incentive and the principle of reciprocity. Melzer concluded that "This simulated attack was in no way a sophisticated criminal strategy. Although the consequences of such attacks can be severe for individuals or companies, many people lack awareness of such dangers."

The study was supported and financed by the Luxembourg Ministry of the Economy and the initiative "Security made in Lëtzebuerg."

Provided by University of Luxembourg