Accompanying measures

- Only disclose personal information to authorised persons
- Be careful when opening emails and attachments
- Be careful when using social networks
- Verify your contact via telephone in case you doubt it is genuine

Involve all staff members – otherwise their knowledge or insider information could be exploited.

By involving them at an early stage, you can ensure your personnel’s understanding and acceptance of new safety measures.

Your points of contact in economic security

Do not hesitate to contact us and make an appointment for confidential awareness talks.

For additional information and your local contacts’ communication data, please visit the website

www.wirtschaftsschutz.info

Economic Security

Protecting values in a concerted effort

Obtaining information by social manipulation

Do not hesitate to contact us and make an appointment for confidential awareness talks.

For additional information and your local contacts’ communication data, please visit the website

www.wirtschaftsschutz.info

Imprint
Publisher: BfV (German federal domestic intelligence service) for the community of the domestic intelligence services of the Federation and the federal states
Pictures: © XtravaganT - Fotolia.com
© ViewApart - Fotolia.com
© Nikolai Sorokin - Fotolia.com
DOI: March 2016
**What is "Social Engineering"?**

The term "Social Engineering" refers to a situation where an attacker tries to take advantage of human weaknesses with the purpose of obtaining specific information. The attacker’s intention is to acquire sensitive data through seemingly insignificant information. This extremely efficient method aims at identifying a company’s weak points, the knowledge of which can subsequently be used for attacks.

In this context, characteristics like helpfulness, customer-friendliness, or gratitude, but also pride of one’s work or company, which in principle are positive characteristics, are abused in a manipulative way.

**Case studies**

- During a visit to the restaurant, a staff member lets out confidential information about a current technical development
- A caller who pretends to be a branch manager is given a colleague’s personal information
- An attacker pretends to be a journalist, eliciting important strategic company plans for the future from the board office
- Via social networks, a staff member discloses private information and interests, which are an ideal basis for a conversation leading to an attack
- An outsider calls the help desk, pretending to be a staff member who has forgotten his password. He asks for it to be reset
- An attacker arouses a staff member’s curiosity by cleverly choosing an e-mail subject and sender.

**Regularly sensitise your staff members!**

**Accompanying measures**

- Be sure to hold confidential conversations in a safe environment only. Loss of information can easily occur in locations such as trade fairs, restaurants, public transport and the like
- Do not disclose internal company information to outsiders
- Make sure everyone wears their company/visitor cards openly