

Social engineering (computer security)

From Wikipedia, the free encyclopedia

For a similar concept in a different discipline see Social engineering (political science).

Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that “users are the weak link” in security and this principle is what makes social engineering possible.

Contents

- 1 Examples of social engineering
- 2 Social engineering in popular culture
- 3 See also
- 4 References
- 5 External links

Examples of social engineering

A contemporary example of a social engineering attack is the use of e-mail attachments that contain malicious payloads (that, for instance, use the victim's machine to send massive quantities of spam). After earlier malicious e-mails led software vendors to disable automatic execution of attachments, users now have to explicitly activate attachments for this to occur. Many users, however, will blindly click on any attachments they receive, thus allowing the attack to work.

Perhaps the simplest, but a still effective attack is tricking a user into thinking one is an administrator and requesting a password for various purposes. Users of Internet systems frequently receive messages that request password or credit card information in order to "set up their account" or "reactivate settings" or some other benign operation in what are called phishing attacks. Users of these systems must be warned early and frequently not to divulge sensitive information, passwords or otherwise, to people claiming to be administrators. In reality, administrators of computer systems rarely, if ever, need to know the user's password to perform administrative tasks. However, even this might not be necessary — in an Infosecurity survey, 90% of office workers gave away their password in exchange for a cheap pen. [1] (<http://www.theregister.co.uk/content/55/30324.html>)

Social engineering also applies to the act of face-to-face manipulation to gain physical access to computer systems.

Training users about security policies and ensuring that they are followed is the primary defense against social engineering.

One of the most famous social engineers in recent history is Kevin Mitnick.

Social engineering in popular culture

- The film *Hackers* used a form of social engineering, where the main character accessed a TV networks control system by phoning the security guard for a modem number, posing as an important executive. Although the film is not highly accurate, the particular method demonstrates the power of Social engineering.

See also

- Pretexting
- Phishing
- Confidence trick

References

- John Leyden, April 18, 2003. *Office workers give away passwords for a cheap pen* (http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/) . The Register. Retrieved 2004-09-09.
- Kevin D. Mitnick, William L. Simon, Steve Wozniak. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, 2002. ISBN 0471237124.
- SirRoss, January 20, 2005. *A Guide to Social Engineering, Volume 1* (<http://www.astalavista.com/index.php?section=directory&cmd=detail&id=3487>) *A Guide to Social Engineering, Volume 2* (<http://www.astalavista.com/index.php?section=directory&cmd=detail&id=3488>) . Astalavista.

External links

- Social Engineering Fundamentals (<http://www.securityfocus.com/infocus/1527>)
- Social Engineering: A complete Article (<http://www.cissponline.com/name-News-article-sid-2.html>)

Retrieved from "http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29"

Categories: Security exploits

-
- This page was last modified 18:07, 15 May 2006.
 - All text is available under the terms of the GNU Free Documentation License (see **Copyrights** for details).
Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc.