維基百科
自由的百科全書

社会工程学

社会工程学是指在信息安全方面操纵人的心理，使其采取行动或泄露机密信息。[1]有別於社会科学中的社会工程，這是种以收集信息、欺诈或入侵系统为目的的信任骗局，已發展出各種技術手段，並可能用於犯罪。

概念

以前，社会工程学属社会学，但其影响他人心理的效果引起计算机安全专家注意。[2]它也定义为“影响某人采取可能或可能不符合其最佳利益的行动之任何行为”。[3]与社会科学中的社会工程不同，后者不涉及泄露机密信息的问题。這是种以信息收集、欺诈或系统访问为目的的信任骗局，与传统「骗局」不同，它通常是更复杂的欺诈计划中的许多步骤之一。英美普通法系一般认為这行为侵犯隐私。

社会工程的一例是在大多数须登录的网站使用“忘记密码”功能。不安全的密码恢复系统可用来授予攻击者对用户账户的完全存取权，而原用户将不能再存取账户。

手段和术语

所有社会工程学攻击都建基於使人决断产生认知偏差的基础。[4]这些偏差有时称“人类硬件漏洞”，足以产生众多攻击方式，其中一些包括：

- 假托（pretexting）是一种制造虚假情形，以迫使针对受害人吐露平时不愿泄露的信息的手段。该方法通常预含对特殊情景专用术语的研究，以建立合情合理的假象。
- 调虎离山（diversion theft）[5]
- 线上聊天／电话钓鱼（IVR／interactive voice response／phone phishing）：用另一种身份與聊天者交流，过程中鬆懈对方的警戒心，从而获取想要的信息。
- 下饵（Baiting）[6]：以获取机密信息为目的，“投食”目标，使其放松警惕，并且借他人进一步获取第三人的手段。
- 等价交换（Quid pro quo）[7]：攻击者伪装成公司内部技术人员或者问卷调查人员，要求对方给出密码等关键信息。在2003年信息安全调查中，90%办公室人员答应给出自己的密码以换取调查人员声称提供的一枝廉价钢笔。后续也有调查发现用巧克力和诸如其他一些小诱惑可得到同样结果（未检验得到的密码是否有效）。攻击者也可能伪装成公司技术支持人员，“帮助”解决技术问题，悄悄植入恶意程序或盗取信息。[8]
- 同情心：攻击者伪装成弱者但不限于通过说话声音带哭腔等手段来骗取受害者的同情心，以此来获取想要获取的信息

- 尾随（Tailgating或Piggybacking）：通常是指尾随者利用另一合法受權者的識別機制，通過某些檢查點，進入一個限制區域。

資訊技術演進

雖然社交工程學已流傳多年，但仍一再成功利用，並且不斷演進。各類型的網路犯罪和資安威脅，都會用社交工程學的技巧，尤其是在目標式攻擊中使用的頻率愈來愈高。網路罪犯以往只會用世界盃足球賽或情人節等標題聳動的全球事件或新聞來引誘使用者，現在有其他的犯罪手法往往也搭配使用社交工程學技巧。

可能的常見方式有：

- 釣魚攻擊：是一種企圖從電子通訊中，偽裝成信譽卓著的法人媒體以獲得用戶名、密碼和信用卡資訊等敏感個人資料的犯罪詐騙過程。
- 電腦蠕蟲：不需附在別的程序內，也可以使用者不介入操作的情況下也能自我複製或執行。
- 垃圾郵件：以電子郵件包裝著惡意木馬程式的電子郵件入侵受害者電腦，例如主旨為美國總統大選結果的電子郵件附件卻包含惡意木馬程式。
- 惡意軟體。

特別人物

美国前头号黑客密凯文（Kevin David Mitnick）著有安全著作《反欺骗的艺术》，有人认为是社会工程学大师和开山鼻祖。

参考文献

1. Goodchild, Joan. Social Engineering: The Basics. csoonline. 11 January 2010 [14 January 2010]. （原始内容存档于2013-09-22）.
2. Anderson, Ross J. Security engineering: a guide to building dependable distributed systems 2nd. Indianapolis, IN: Wiley. 2008: 1040 [2013-09-22]. ISBN 978-0-470-06852-6. （原始内容存档于2019-03-12）. Chapter 2, page 17
3. Social Engineering Defined. Security Through Education. [3 October 2021]. （原始内容存档于2018-10-03） （英语）.
4. Jaco, K: "CSEPS Course Workbook" (2004), unit 3, Jaco Security Publishing.
5. Train For Life. Web.archive.org. 2010-01-05 [2012-08-09]. （原始内容存档于2010-01-05）.
6. 存档副本 (PDF). [2012-03-02]. （原始内容 (PDF)存档于2007-10-11）.
7. Leyden, John. Office workers give away passwords. Theregister.co.uk. 2003-04-18 [2012-04-11]. （原始内容存档于2012-05-03）.
8. Passwords revealed by sweet deal. BBC News. 2004-04-20 [2012-04-11]. （原始内容存档于2012-03-27）.

延伸阅读

- Boyington, Gregory. (1990). 'Baa Baa Black Sheep' Published by Gregory Boyington ISBN 0-553-26350-1
- Harley, David. 1998 *Re-Floating the Titanic: Dealing with Social Engineering Attacks (http://smallbluegreenblog.files.wordpress.com/2010/04/eicar98.pdf)（页面存档备份 (https://web.archive.org/web/20160922222220/http://smallbluegreenblog.files.wordpress.com/2010/04/eicar98.pdf)，存于互联网档案馆）* EICAR Conference.
- Laribee, Lena. June 2006 *Development of methodical social engineering taxonomy project (http://faculty.nps.edu/ncrowe/oldstudents/laribeethesis.htm)（页面存档备份 (https://web.archive.org/web/20200111133008/http://faculty.nps.edu/ncrowe/oldstudents/laribeethesis.htm)，存于互联网档案馆）* Master's Thesis, Naval Postgraduate School.
- Leyden, John. 18 April 2003. *Office workers give away passwords for a cheap pen (https://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/)（页面存档备份 (https://web.archive.org/web/20121028225623/https://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/)，存于互联网档案馆）*. The Register. Retrieved 2004-09-09.
- Long, Johnny. (2008). *No Tech Hacking – A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing* Published by Syngress Publishing Inc. ISBN 978-1-59749-215-7
- Mann, Ian. (2008). *Hacking the Human: Social Engineering Techniques and Security Countermeasures* Published by Gower Publishing Ltd. ISBN 0-566-08773-1 or ISBN 978-0-566-08773-8
- Mitnick, Kevin, Kasperavičius, Alexis. (2004). *CSEPS Course Workbook*. Mitnick Security Publishing.
- Mitnick, Kevin, Simon, William L., Wozniak, Steve,. (2002). *The Art of Deception: Controlling the Human Element of Security* Published by Wiley. ISBN 0-471-23712-4 or ISBN 0-7645-4280-X
- Hadnagy, Christopher, (2011) *Social Engineering: The Art of Human Hacking* Published by Wiley. ISBN 0-470-63953-9