针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 社会工程学
- 识别、阻断社会工程学攻击
- 防范未来的攻击

社会工程学

概览

关于网络攻击者，人们常有的一个误区就是认为，他们只只用高端的黑客工具和技术来入侵人们的电脑、账户和移动设备。事实完全不是这样。网络攻击者已经了解到，窃取你信息或入侵你电脑的最简便的方法之一便是和你说话，误导你，仅此而已。本期，我们将了解这种针对人的攻击，即社会工程学攻击，是如何运作的，以及你如何才能保护你自己。

客座编辑

Alissa Torres是一名认证的SANS讲师，专门研究高级计算机取证和事件响应。她的行业经历包括作为时间处理员在前线服役和作为数字取证调查者在一个内部安全小组工作。你可以通过Twitter（@sibertor）找到她。

社会工程学

社工是一种心理攻击，即攻击者通过误导让你做他们想要你做的事。它已经有上千年的历史了，诈骗这个想法并不新奇。然而，网络罪犯已经体会到，在互联网上用这个手段极为有效并且可以针对数百万人。理解社工如何运作的最简单的方法就是看看一个常见的现实世界中的例子。

你接到一个自称是电脑支持公司、你的网络服务提供商或微软客服的人的电话。他解释说他们注意到你的电脑最近行为异常，比如在扫描互联网或者发送垃圾邮件，由此他们相信你的电脑受到了病毒感染，他们现在需要调查此事，并帮助你保护你的电脑。他们然后使用了各种技术术语，让你真相信你的电脑受到了感染。

例如，他们可能会让你检查，看看你的电脑上有没有特定的文件，并且会指导你找到这些文件。当你找到这些文件的时候，电话那头的人会让你相信，这些文件是电脑被感染的一个征兆，但其实这些文件是可以在任何电脑上找到的普通文件。一旦你中了他们的计，他们就会催促你去一个网站买他们的安全软件或让你给他们远程访问权限，从而能让他们“帮”你“修复”你的电脑。然而，

社会工程学

他们卖的软件实际上是恶意程序，如果你买了并且安装了这款软件，不仅他们成功地欺骗了你，感染了你的电脑，而且你还为此给他们付了钱。如果你给了他们远程访问的权限，他们实际上会接管你的电脑，并感染它。

记住，像这样的社工攻击并不限于电话场景，在其它几乎所有的技术场景如邮件、短信、Facebook消息、推文或在线聊天中均可能发生。关键在于要明白要小心什么。

学习如何防范、识别和阻断社会工程学攻击是你能采取的保护自己的最有效的措施之一。

识别、阻断社会工程学攻击

避免社工的最简单的方法就是用常识。如果某件事可疑或者感觉不对，那么它可能就是一场攻击。社工的常见表征包括：

- 某人故意制造极度的紧迫感。如果你感到自己处于快速作出决定的压力之下，那么请小心。
- 某人要他们本没有权限访问或本来就应该知道的信息。
- 某事太好了，不可能是真的。一个常见的例子就是你被告知你彩票中奖了，即便你根本从来都没有买过。

如果你怀疑某人正尝试对你进行社工，那么不要再和他再沟通下去了。如果你们是通过电话交流的，挂掉电话；如果是线上，就断开连接；如果是邮件，就删掉它；如果攻击和工作相关，一定要马上向前台或信息安全部门报告。

防范未来的社会工程学攻击

幸运的是，你能采取一些预防措施来帮助你未来免遭社工攻击。

- **从不告诉别人你的密码** 没有任何组织会联系你，要你的密码。如果某人问你要密码，那么这就是一场攻击。

社会工程学

- **不要分享太多** 攻击者关于你知道的越多，他们就越容易误导你，让你做他们想要你做的事。即便是时常分享关于你自己的一些小细节，也能让他们形成一个你的完整画像。你公开分享的信息——包括社交媒体网站、产品评论和公共论坛、邮件列表——越少，你受到攻击的可能性就越小。

- **核验联系人信息** 有时你的银行、信用卡公司、移动运营商等可能会由于一些正当原因打电话给你。如果你不确定询问你信息的行径是否正当合法，那么问一问这个人的姓名和分机号，然后从一个可信的来源——例如信用卡背面或银行文书、公司网站（确保URL是你自己一字一字输入的）上留下的电话——找到这家公司的电话，这样你向这个号码拨过去，你就能肯定你确实是在和他们而非其他人交流。尽管这看起来很麻烦，但就保护你的身份和个人信息而言这些额外的努力是值得的。

了解更多

订阅OUCH！安全意识月刊，访问OUCH！过往存档，了解更多关于SANS安全意识解决方案的信息，请访问：http://www.securingthehuman.org

相关资源

钓鱼邮件:	http://www.securingthehuman.org/ouch/2013#february2013
安全使用社交网络:	http://www.securingthehuman.org/ouch/2013#march2013
防范诈骗:	http://www.onguardonline.gov/topics/avoid-scams

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻译：成自豪

