用户需要了解的十大社会工程攻击手段

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	10 Social Engineering Attacks Your End Users Need to Know About		
原文作者	Steve Zurier	**原文发布日期**	2017 年 10 月 19 日
作者简介	Steve Zurier 拥有 30 多年的新闻和出版经验，主要关注网络和安全技术领域。https://www.darkreading.com/author-bio.asp?author_id=2460		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/attacks-breaches/10-social-engineering-attacks-your-end-users-need-to-know-about--/d/d-id/1330171		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

用户需要了解的十大社会工程攻击手段

Steve Zurier

2017 年 10 月 19 日

“国家网络安全意识月”是探讨被盗密码、网络钓鱼、恶意软件以及普通用户所不知道的一些社会工程攻击的绝佳时机。威瑞森《数据泄露调查报告》显示，去年有 43%的数据泄露与社会工程攻击有关。

PhishMe 首席技术官艾伦·希格比（Aaron Higbee）说：“我们发现了很多社会工程攻击，特别喜欢以寂寞宅男为攻击目标。攻击者向他发送美女裸照，诱骗他发一张自己的裸照，然后威胁说要将其裸照贴到 Facebook，强迫他支付赎金。”

Social-Engineer 首席黑客官克里斯托弗·哈德纳吉（Christopher Hadnagy）补充说，人们应该意识到，电话钓鱼诈骗（vishing）等社会工程攻击变得越来越普遍了。

“犯罪分子在暗网上购买数据，然后打电话给人们说几年前他们欠了几千美元的联邦税。”哈德纳吉说，“即使人们知道国税局（IRS）只会以书面形式通知他们，不会直接打电话，但是很多人还是会上当。”

根据对希格比、PhishMe 首席威胁科学家加里·华纳（Gary Warner）和哈德纳吉的采访，Dark Reading 整理出了十大社会工程攻击手段。

1.电话钓鱼诈骗

最终用户对欺诈邮件已经比较警惕，但是许多人忘记了黑客经常采用低技术的电话诈骗。

在一些电话中，骗子声称是微软技术支持人员，要求用户提供凭证和/或其信用卡号。千万不要上当！记住，微软不会突然打电话询问你的电脑运行情况。国税局也是如此。骗子不停地打电话，若有其事地声称纳税人欠了税款，如 2012 年的 3000 美元欠税。再强调一次，这种事绝对不会发生。国税局不会打电话给你，也不会发电子邮件给你。他们只会以书面形式与纳税人沟通。如果您收到假的微软技术支持电话，请上报给 https://www.microsoft.com/en-us/reportascam/。

2.利用 SEO（搜索引擎优化）诈骗

您是否有需要驱动程序的旧打印机或扫描仪？ 如果有，那您要当心了，因为攻击者花几美元就能使用营销策略将搜索引擎流量引向一个假驱动程序，从而感染您的计算机。

例如，您搜索打印帮助，它可能会把您带到一个看起来像官方驱动程序的网站，而实际上这里只有被恶意软件感染的服务器。他们不必花费大量资金来创建网站并购买关键的互联网搜索术语来引诱不知情的受害者。

3.钓鱼网站也可以是 HTTPS

按照传统的观点，HTTPS 站点上的 SSL 证书意味着网站是安全的。攻击者不希望花大价钱购买有效的 SSL 证书。现在他们可以如愿了，诸如 letencrypt.org 这样的网站免费提供 SSL 证书。

用户不能因为 HTTPS 就认为网站是安全的。对于重要的银行和其它登录页面，用户应该“寻找绿色条”，这意味着该网站不仅使用 HTTPS，而且使用扩展验证 SSL 证书（EV-SSL），攻击者是无法免费获得这种证书的。

4.以假乱真的网站

人们浏览网页，但并不总是仔细看。黑客可以注册一个合法网站的域名，如 PayPal 或 eBay，使他们看起来近 99%的真实。聪明的诈骗者在这些页面中隐藏恶意软件，并且还隐藏肉眼不容易看到的外语字符。

5.从右到左的覆盖

黑客可以使用“从右到左的覆盖”来启动恶意软件。会出现一个如下所示的文件：validate.exe.jpg，基本上是一个正常的 jpg 文件。但实际上，使用 Unicode 进行转换，发现该文件实际上是一个名为 validate.jpg.exe 的可执行文件。然后，用户会在不知不觉中启动恶意软件，感染计算机。

重申一条黄金法则：如果收到了陌生人发来的文件，请勿打开。

6.裸照勒索和色情网站取消订阅诈骗

这些诈骗的目标通常是寂寞男人。骗子发送美女裸照，诱骗受害者发一张自己的裸照。如果目标上当，骗子就会发一条赎金要求，威胁称会将裸照贴在 Facebook 或其它社交媒体上，强迫他们支付赎金。

这些类型的犯罪是低技术的，骗子甚至不必编写代码或建立网站。他们只需要几张美女裸照就行了。在另一起性欺骗中，用户在公司收到一个色情网站的消息，称他们订阅了该网站。要取消订阅，他们需要发送工作邮箱和密码。只要该公司的一名员工上当，骗子就能够入侵公司网络了。

7.低技术勒索软件

正如上文所述，一些攻击者走低技术路线。攻击者向用户发送邮件，声称黑掉了他们的文件和公司账户。当然，这完全是虚张声势，但通常黑客会要求支付价值 300 美元的比特币。

忧心忡忡的用户可能会为求心安而支付赎金。在这种情况下，黑客需要的只是一个电子邮件地址，这样就能赚些快钱了。

8.“文件太大”钓鱼邮件

你有没有遇到过在邮件中添加附件时被告知文件太大的情况？人们已经习惯于通过 Dropbox、Box 或 OneDrive 共享更大的文档和视频了。在这种诈骗中，攻击者向受害者发送一封看起来像来自同事或主管的电子邮件，并告诉他们看一下某个文件。使用这种方法，攻击者可以绕过电子邮件安全保护，诱骗受害者打开热门文件共享站点上托管的恶意软件。

9.获得管理员访问权限

攻击者有许多方法使用“横向运动”来达到目标，但是高权限用户并不总是能够意识到他们被攻击了。

可以通过这种方式获得人力资源数据库或电汇权限。或者，黑客可能需要 IT 服务台的管理员访问权限。因此，攻击者可以访问用户的机器，然后故意破坏某些东西，或者向服务台发送一条消息，称其机器上已禁用了 Word 等应用程序。当帮助台人员登录时，黑客会窃取缓存的管理员凭证，从而访问公司网络。

10.自动化工具

攻击者拥有自动化软件，用于检查密码是否包含字典中的字，因此在密码中使用任何字或名称都会降低安全性。这不是“猜测或不可猜测”的问题--用户应使用没有任何意义、并且不会在任何字典（或电话簿）中找到的字母和数字。