TURING

Phishing Dark Waters

The Offensive and Defensive Sides of Malicious E-mails

社会工程

防范钓鱼欺诈（卷3）

[美] Christopher Hadnagy Michele Fincher 著 肖诗尧 译

- 著名安全专家教你辨识并防范钓鱼欺诈，避免信息被窃取
- 美国海军陆战队军官、FBI探员/行为学家罗宾·德瑞克作序推荐
- 网络诈骗、电话诈骗横行的今天，人人都需要懂一些可以自我保护的社工方法

中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

TURING

社会工程

防范钓鱼欺诈

（卷3）

[美] Christopher Hadnagy Michele Fincher 著 肖诗尧 译

Phishing Dark Waters

The Offensive and Defensive Sides of Malicious E-mails

人民邮电出版社

北 京

图书在版编目（CIP）数据

社会工程. 卷3, 防范钓鱼欺诈 / (美) 海德纳吉(Christopher Hadnagy), (美) 芬奇(Michele Fincher) 著 ; 肖诗尧译. -- 北京 : 人民邮电出版社, 2016.10
ISBN 978-7-115-43547-7

Ⅰ. ①社… Ⅱ. ①海… ②芬… ③肖… Ⅲ. ①信息安全 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2016)第216678号

内 容 提 要

本书从专业社会工程人员的视角，详细介绍了钓鱼欺诈中所使用的心理学原则和技术工具，帮助读者辨识和防范各种类型和难度级别的钓鱼欺诈。本书包含大量真实案例，全面展示了恶意钓鱼攻击者的各种手段。本书还针对企业如何防范钓鱼攻击并组织开展相关培训提供了切实可行的意见。本书提供了企业和个人面对现实中的社会工程问题和风险的无可替代的解决方案。

本书适合社会工程人员、企业管理人员、IT 部门人员以及任何对信息安全感兴趣的人阅读。

◆ 著　[美] Christopher Hadnagy Michele Fincher
译　肖诗尧
责任编辑　朱　巍
执行编辑　温　雪
责任印制　彭志环

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路11号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：720×960　1/16
印张：12
字数：199千字　2016年 10 月第 1 版
印数：1-4 000册　2016年 10 月河北第 1 次印刷
著作权合同登记号　图字：01-2015-4674 号

定价：49.00元

读者服务热线：(010)51095186转600　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广字第 8052 号

站在巨人的肩上

Standing on Shoulders of Giants

iTuring.cn

版权声明

献词

谨以此书献给那些使得它顺利出版的人。我的妻子阿丽莎，你是我遇见过的最耐心、善良和有智慧的人。我会永远坚持自己的梦想。

米歇尔，多亏平多年前推荐了你。没有你，这一切都不可能实现。

大卫，当我写下这些话时，我都无法相信我们已经走了这么远。谢谢你的支持。

——克里斯托弗·海德纳吉

献给我的丈夫，你是宇宙中最美丽的灵魂，是我整个人生的主宰。

也献给克里斯托弗，谢谢你给我这份工作并且信任我。

——米歇尔·芬奇

序

无论你是否对那些针对主要商业公司、政府部门、电网或者私有银行发起的黑客攻击感到担忧，你都能从更多的信息和个人训练中受益，并以此来保护自己、保护公司、保护你所爱的和所关心的人，避免经济损失、遭遇尴尬或者更糟糕的情况。几乎每一起成功的网络攻击的核心都是人的因素。人的因素使得坏人能找出攻击系统的途径。由于人是每一起成功的安全攻击的核心要素，克里斯托弗（简称克里斯）决心通过教育培训，结合他作为专业社会工程人员（白帽子）和渗透测试者的经验，帮助大型公司以及他遇到的每一个人抵御这些攻击。

当克里斯和他出色的合著者兼训练伙伴米歇尔·芬奇一起，问我是否愿意为他们最近的一本书作序时，我感到既吃惊又荣幸。我多年前遇见克里斯时，他刚创办自己的公司 Social-Engineer。克里斯曾（并且仍在）主持一系列很棒的播客访谈节目，采访来自人际交互不同领域的专家。在那些日子里，克里斯迅速意识到人是最容易受到攻击的部分，并且技术和它的使用者和维护者一样脆弱。

我很清楚地记得我和克里斯多年前的第一次谈话。我当时就对他在行为学方面渊博的学识和充沛的热情印象深刻。更让我印象深刻的是，他的工作结合了自己在人际关系方面的学识、在安全领域多年的工作经验，以及在大型机构协调和组织培训项目的才能。最后，他的诚意和想要帮助他人的渴望，让我相信他是这个领域了不起的人物。

无需多言，我和克里斯很快就成了朋友。基于帮助他人的共同热情，我们创造了一种克里斯和他的合作伙伴如今成功开展并正在拓展的训练，他的合作伙伴就是空军学校毕业生、行为专家和合著者米歇尔。克里斯开阔了我的眼界，让我了解到我曾经使用多年的、用以获取他人信任的、让我成为海军陆战队军官的技术，以及作为 FBI 探员用来挫败敌人的本领，实际上和恶意攻击者所使用的技术是一样的。通过利用一些建立信任的技术，黑客使得收到恶意邮件的人以为点击恶意链接或者采取某种类似的行动才是最符合他们的利益的。而克里斯正是致力于通过训练来阻止人们采取这种危险行动。

当我帮助别人时，我在生活中的方方面面都会用到从克里斯那里学来的知识。我也会

教授政府和私有企业这些容易由于人的因素而受到攻击的机构一些社会工程学意识。实际上，我常常会把我和克里斯多年前在华盛顿州西雅图市开设第一节社会工程学认证课程时使用的钓鱼邮件拿出来。一周的训练里包含了大量的实践练习，参与者会试着与他们遇到的普通人建立信任并施加影响。克里斯用写字板创建了一封典型的钓鱼邮件，这封邮件他总是在渗透测试中使用，并取得了很大的成功。克里斯解释了他是如何利用这封邮件得到75%的点击率的。那75%的人点击了这封邮件里的链接后，会立刻跳转到一个训练网站，里面展示了一些材料，帮助这些人了解以后应该注意哪些方面。换句话说，学习和教育变成了一种非常积极而非消极的事情。在刚才提到的那封邮件的基础上，我们利用人际关系和信任建立方面的一些技巧对其稍微进行了调整，在不增加邮件长度的前提下增加了3种新的技术。接下来的一周，克里斯告诉我他用那封修改后的邮件取得了100%的点击率。由于训练有素，比起参加克里斯加强型反钓鱼攻击训练前，那家公司已经取得了明显的进步。

我所学到的知识和我的个人经验告诉我：克里斯是这方面的杰出专家。我——和这个世界——都受益于他的热情、知识以及教授别人知识的能力，这样我们就可以生活在一个更安全的世界里。

本书的内容适合所有人阅读，可以用于职业生涯和个人生活的方方面面。克里斯和米歇尔用他们作为专业社会工程人员和渗透测试者的实际经验，阐释了人类点击不该点击的东西这一行为背后的心理学。结合克里斯自嘲式的幽默和米歇尔风趣的点评，本书可以在保护你和你的公司的同时，为你的阅读增添一些乐趣。最后，本书是一本实用手册，告诉你如何经营更安全、红火的企业，同时让个人生活免受恶意攻击者干扰。

通过阅读、记忆和实践本书中的内容，你能够重新审视自我、你的公司以及那些你关心的人。如果我们能够处理好恶意攻击中的首要因素——人的因素，那么这个世界就不会遭受影响数百万人的大范围攻击了。

——罗宾·德瑞克（Robin Dreeke），
美国海军陆战队军官，FBI探员/行为学家，
People Formula（www.peopleformula.com）创始人，
畅销书 *It's Not All About "Me"* 独立作者

以上观点和想法仅代表笔者个人，不代表FBI。

致谢

2014年，我的生活发生了一些改变，其中一个较好的变化是我的团队在成长。我和米歇尔开始教授新成员一些钓鱼攻击意识方法论，这也让我意识到该再写一本书了。

我们在新闻中看到的网络攻击中大部分都利用了钓鱼攻击，但是人们仍然没有意识到钓鱼攻击是什么，以及应该如何抵御钓鱼攻击。

然而，我的客户见证了员工在面对网络钓鱼邮件时的惊人变化——从80%以上的点击率和少得可怜的汇报率到低于10%的点击率和超过60%的汇报率。随着时间的推移，这些数据仍在朝着好的方向发展。

我最近完成了《社会工程 卷2：解读肢体语言》[①]，并告诉妻子我会暂时停笔休息一段时间。而当我又开始写作时，我变成了个隐士。妻子说我“难对付”。我仍然记得那个场景——我们在公路上开车，我想着可以通过谈论一些近期的安全新闻来激起我写本新书的欲望。于是我开始谈论钓鱼攻击为什么是个大问题，并说我希望能有一本书可以帮助人们解决问题。

在我说完后，我那既聪慧又有惊人洞察力的妻子说：“不，不要现在就开始写另一本书。”我做了每个好男人在这种情况下都会做的事，把责任归咎于我的得力助手米歇尔。

“我和米歇尔认为这是个好主意，另外她会负责主要的写作工作。”

如今摆在这里的就是我们的最终成果——一本细致的关于如何增强企业钓鱼防范意识的书。渗透测试中的审计者常常利用钓鱼攻击来获取远程访问权限，但本书不会谈到渗透测试中使用的钓鱼攻击。本书主要是为了让人们了解他们所在的组织机构会遇到的钓鱼攻击并为此做好准备。

我想感谢很多人，没有他们的话，这本书不可能成功出版。

再一次，感激我的妻子阿丽莎。感谢你的耐心和支持，你总是让我畅所欲言，即使你并不想谈论这个话题。我爱你。

---

① 该书已经由人民邮电出版社出版，书号9787115382467。——编者注

米歇尔，尽管最后我没有让你负责大部分的写作任务，但是如果没有你的支持，这本书也许就不会完成。谢谢你。

卡罗尔，你为这本书付出了很多。我想让你知道你的努力没有被忽视。感谢你的支持。

夏洛特，和你一起工作很开心，很顺利，也很有收获。谢谢你。

大卫，你知道的，当你没有跟我开玩笑、拿我活跃气氛、取笑我、让我尴尬或者用恼人的音乐让我生气的时候，你还是很不错的。谢谢你对本书的贡献。

尼克·菲诺克斯，谢谢你让我借用你的想法。你长期的支持和建议是我继续下去的理由。

平·卢克，七八届 Black Hat 会议前，如果当时你没有花 3 个小时和我谈话并向我推荐米歇尔，帮我调整心态，那么也许就不会有这本书了。

我的队友——阿曼达、迈克、科林、杰西卡和塔玛拉，谢谢你们在我和米歇尔需要抓紧写作的时候支持并帮助我们。

罗宾，真是见鬼了，谁能想到一起工作这么年后我们会是现在这样呢？谢谢你长期的支持、友谊和帮助，也十分感谢你为我的这本书作序。

我忠实的客户、顾客和朋友们同意我使用他们的点子，谢谢你们。

我知道我的前两本书无法让所有人都满意。对于这本书，肯定有人读过之后会喜欢，有人读过之后会反感。如果你发现了错误，或看到了你不喜欢或者不同意的部分，请联系我和米歇尔，给我们一个机会来解释或者更正。

我希望你能看到本书背后付出的汗水和心血，你会发现这本书不仅有趣，同时也对你理解、教授和抵御钓鱼攻击有所帮助。

再次感谢你们让我在你们心中停留一小会儿。

——克里斯托弗·海德纳吉，Social-Engineer 公司 CEO 和创始人

尽管没人会为了取乐而读一本关于钓鱼攻击的书，但我还是希望你在这本书中能乐趣和实用性兼得。我写作本书的主要动机不仅是出于对客户的关心，也出于对身边人的关心。我希望他们的生活能够更安全。我的侄女和侄子已经伴随着互联网长大了，想到他们可能在人生真正开始前，就已经成为了网上身份信息窃取的受害者，我感到有些忧虑。因此，这不是一本专门写给安全专家看的书，而是一本写给所有通过网络与

世界相连的人看的书。

正如克里斯托弗所提到的，一本书的写作过程需要得到很多支持。如果我遗漏了谁，那么我提前在这里道歉。要是没有你们的帮助，我可能还在整日为这本书忙碌。

和我丈夫结婚对我写作本书是一大益处。事实证明，他能够一边忍耐冷了的或者烧糊了的晚餐，一边做研究并修改我的书稿。我不知道我们就着比萨（通常是由于晚餐冷了或者烧焦了）进行过多少次“你真的想写那个吗”的讨论。谢谢你，亲爱的。

克里斯托弗，你本可以让其他人帮忙的，而我得到了这个机会，我很感激。

阿曼达、迈克、科林、杰西卡和塔玛拉，你们知道自己有多努力，我也知道。谢谢你们。

Wiley公司的卡罗尔和夏洛特，谢谢你们让我感觉到我的第一次出书经历如此美好。

——米歇尔·芬奇，Social-Engineer公司首席影响官
（Chief Influencing Agent）

引言

这世上没有公平竞争这一回事。要利用一切弱点。

——凯利·卡弗里（Cary Caffrey）

社会工程已经成为大部分 IT 部门关注的重点，尤其是近两年，大部分美国公司也开始关注社会工程。据统计，超过 60%的网络攻击的关键因素或主要因素是“人的因素”。对过去 12 个月里几乎所有的大型攻击事件的分析结果表明，绝大多数攻击都与社会工程有关，涉及网络钓鱼邮件（phishing e-mail）、鱼叉式网络钓鱼（spear phish）或恶意来电（malicious phone call，vishing）。

我已经写过两本书来剖析骗子和社会工程人员的心理、生理和历史沿革。而在写这两本书的同时，我发现了一个最近很火的主题，那就是电子邮件。自从人类发明电子邮件以来，它就被骗子和社会工程人员用来进行信用卡、金钱和信息等方面的欺诈。

在最近的一份报告中，Radicati 集团评估的结果显示，2014 年平均每天有 1914 亿封电子邮件被发送出去，这意味着全年有 69.8 万亿多封电子邮件被发送出去。[①]你能想象这个数字吗？69 861 000 000 000，让人大吃一惊，对吧？但可能更让你吃惊的是，Social-Engineer Infographic 的信息显示，超过 90%的电子邮件都是垃圾邮件。[②]

电子邮件早已成为生活的一部分。我们会在电脑、平板电脑和手机上使用电子邮件。在曾经和我共事过的一些人里，有半数以上告诉我他们每天收到 100 封、150 封甚至 200 封邮件。

2014 年，Radicati 集团宣称全世界有 41 亿个电子邮件地址。根据这一数据我进行了计算，发现平均下来每个人每天都会收到 50 封左右的电子邮件。因为我们知道并不是每个人每天都会收到那么多邮件，所以有人每天会收到 100 封、150 封甚至 250 封邮件也就不足为奇了。

---

① Sara Radicati, PhD, “Email Statistics Report, 2014–2018,” April 2014, http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf.

② Social-Engineer Infographic, April 28, 2014, http://www.social-engineer.org/resources/social-engineering-infographic/.

随着人们的生活压力和工作负担加重，以及科技产品的日益普及，骗子和社会工程人员知道电子邮件是渗透进我们的工作和生活的利器。再想想伪造电子邮件账户或合法账户以及愚弄人们让他们做一些不符合他们利益的事是多么容易，就会明白为什么电子邮件很快就成为了恶意攻击的头号媒介。

当我们不在大型会议（比如 DEF CON）上举办社会工程学竞赛，米歇尔也没在和学生斗智斗勇（这是真的，我发誓）的时候，我们会在全世界范围内与一些顶尖的公司一起做安全项目。即使很多公司都知道钓鱼攻击的存在并且有强大的安全措施来防范钓鱼攻击，也还是有人不可避免地成为钓鱼攻击的牺牲品。

写这本书时，我们的脑海中一直在回想着那些经历。我们自问："我们该如何利用这些年和大公司一起工作的经验，帮助每个公司立即行动起来，并做好防范钓鱼攻击的教育培训呢？"

我是一名建筑师了吗

我和米歇尔曾经在一些地方开展过一个项目，这个项目很简单但很强大。它利用那些攻击我们的工具反过来增强我们自己。我们知道这个想法不是我们发明的，毕竟现在有不少公司都在兜售"网络钓鱼"服务给合法组织。这些产品的很多使用者——大公司，过来找我们说："我们已经使用这个工具一年了，但是员工钓鱼攻击的中招率还是很高，我们该怎么办？"

在回答这个问题之前，让我先讲一个故事。我记得我买第一套房子快收房的时候，我和妻子都非常激动，（我们要拥有自己的房子了！）于是我做了所有拥有自己的房子的男人都会做的一件事：买一些工具。我去家得宝（Home Depot）买了一套精致的工具，包括一把拉锯、一把电钻、一把竖锯，还有其他一些五花八门的工具。

把这些工具买回家的第一天，我在地下室的架子上找了一个绝佳的摆放位置，然后就让它们在那儿闲置了一年。然后有一天我突然要锯点东西，我非常激动，因为总算有机会使用这些新工具了！我拿出工具箱，取出圆锯。我把所有的说明书都读了一遍，包括："确定你根据所锯的材料选择了合适的锯齿。"

我看了看锯齿，心想："看起来挺锋利的。"然后我就开始锯板子。起初一切顺利，我的手脚还在，板子也锯开了，圆锯也没毁坏。可是好景不长，几小时后圆锯突然卡住不动了。于是我给圆锯充电，但是没有什么作用。我还拿手摸了一下锯齿，锯齿依旧很锋利。于是我断定是圆锯出了毛病："这锯子肯定有问题。"

然后我请了一个朋友过来帮我解决这个问题，他拿起圆锯看了一下说："你为什么用这种细密的锯齿来锯 2×4[①]的板子？"

我回答道："你说的是什么锯齿？"

我的朋友摇了摇头，然后就锯齿的问题给我上了一课。

为什么我要讲这个丢脸的、缺乏男子气概的故事，而不是直接指出我自己缺乏男子气概？这是为了论证一个观点：拥有工具并不会使你成为一名建筑师！

同样，钓鱼工具和建筑工具没什么区别。仅仅购买工具并不能保证你的安全，也不会让你有能力教导其他人防范钓鱼攻击。

教导人们钓鱼攻击

好了，让我们回到我和米歇尔开展的那个项目上来：我们分析了钓鱼攻击和安全防范意识培训，发现正如很多安全专家所说的那样，这些项目大多都没有用。

当然，这里并不是说安全防范意识毫无作用，我也不会很傻很天真地说我们不需要安全防范意识。但是现有的安全防范意识训练采用的方法和方式的确不奏效。有人曾经在安全防范意识训练中专注地看了 30 分钟或者 60 分钟的 DVD 演示吗？有的话，请举起你的右手。好了，后排坐着的那位朋友，你可以把你的手放下来了。正如我所猜想的，基本上没有人举手。

如果训练中没有互动或者训练时间过长，那么人们就会在训练时开小差。商人显然深谙这一点，他们告诉我们要把网站做得有趣一点、互动性强一点、直奔主题一点，这样人们才会喜欢。教育的过程难道不也该如此吗？

于是我们提出了一个计划，把客户的安全防范意识培训中钓鱼攻击的部分做得更有趣一些、互动性更强一些。当然，最重要的是不要太冗长。这也是有必要写这本书的原因，我们想要在其中回答如下一些问题。

- ❑ 钓鱼攻击有多严重？
- ❑ 心理学原则在钓鱼攻击中起到了怎样的作用？
- ❑ 钓鱼攻击真的可以在安全防范意识训练中成为一个成功的部分吗？
- ❑ 如果说可以，那么公司应该如何开展这一训练呢？

---

① 指未处理过的木材的尺寸。——译者注

❑ 任何规模的公司都能进行钓鱼攻击的培训吗？

我们列了一下关于钓鱼攻击的书的提纲，对我们的项目进行了定义，并对我们的流程进行了规范。我们考虑了很久是否要把这本书向公众发行。毕竟，研究这些方法花费了很多年。在看到这一项目对客户的巨大帮助之后，我们决定写这本书。乍一看，这似乎是一本大多数人都没什么兴趣的书，至少在 2014 年不断出事以前是这样的。2014 年，钓鱼攻击在真实的黑客攻击中一次又一次地占据了头条，每天的攻击中都使用了钓鱼攻击，钓鱼攻击服务的提供者每个月都层出不穷，全世界的公司都开始跻身于轰轰烈烈的反钓鱼培训之中。

本书主要内容

我和米歇尔希望本书可以帮助你进行自我保护，以及帮助公司防御恶意钓鱼攻击者。本书会带你踏上我们准备写这本书时所走过的路。

第 1 章介绍基础知识。这一章解释了钓鱼攻击是什么，以及为什么要使用钓鱼攻击。我们列举了很多最近发生的有效的钓鱼攻击的例子。

第 2 章探究了钓鱼攻击的原理。为什么钓鱼攻击有效？它们背后蕴含了怎样的心理学原则？

第 3 章只关注一个方面——影响，解释了影响原则是如何被恶意钓鱼攻击者利用的。

第 4 章讨论保护。前三章已经涵盖了钓鱼攻击的基础知识，所以是时候讨论该如何自保了。我们分别对普通人和专业人士提出了建议，同时也分析了我们所听说过的最糟糕的建议。

第 5 章介绍了公司如何开展钓鱼攻击项目以帮助员工提高安全意识。

但是你如何把这些内容融入到公司政策里？我懂，我懂，政策这个词在这些书里看上去似乎没有探讨的必要。但是我们不得不讨论它，简短而重要的第 6 章就是讨论这一主题的。

如果不介绍市面上一些重要的钓鱼攻击软件的话，那么这本书就是不完整的。第 7 章会介绍这些工具，同时告诉你如何运用它们来进行钓鱼攻击。

第 8 章对本书中所有的原则和讨论进行了总结，并对钓鱼攻击训练的一些原则进行了讨论。

本书排版约定

为了帮助你理解书中内容，本书采用了一些排版约定。

- 专业术语和重要的词汇用楷体表示。

说明/警告/提示　表示注释、建议、提示、诀窍或者当前讨论内容的边注。

总结

本书的主旨是剖析钓鱼攻击是什么、为什么它会起作用，以及它背后的原理是什么。我们想要把钓鱼攻击所有的漏洞都揭示出来，这样你就能了解如何抵御钓鱼攻击。

在我的上一本书《社会工程　卷 2：解读肢体语言》中，我讲了一个剑术大师朋友的故事。他通过学习关于剑术的一切知识——如何用剑以及剑术的原理——来掌握剑术，然后找来了最好的陪练来帮他学习如何运用剑术。这个故事在这里也同样适用。当你学会辨认钓鱼攻击，熟悉钓鱼攻击工具，知道如何选择好搭档以后，也可以通过创建钓鱼攻击项目来提高你的技术水平，同时帮助你的同事、家人和朋友抵御钓鱼攻击。

在深入学习之前，我们需要了解一些基本问题，例如“什么是钓鱼攻击”以及“钓鱼攻击有哪些例子”。

一起来寻找这些问题的答案吧。

目　录