

# OUCH!

## 本期导读

- 概览
- 为什么你被当成目标
- 保护你自己

## 是的，你就是一个目标

### 概览

许多人有一个共同的误解，就是他们不是网络犯罪的目标：他们或者他们的电脑没有任何价值。没有什么能比这更大错特错了。如果你有电脑、便携设备、网上账号、电邮地址、信用卡，或者参与到其它类型的在线活动中，在网络罪犯眼中，你就是值钱的。在本刊中，我们将解释你为什么会成为目标，你是如何受到攻击的，以及为了保护你自己你所能做的。

### 客座编辑

Eric Conrad是Backshore Communications的主席和CTO，还是《CISSP学习指南（第二版）》《第十一个小时CISSP（第二版）》的首席作者。他在SANS还与他人合著了“持续监控和安全操作（SEC511）”六日课程。

### 为什么你被当成目标

诸如诈骗、身份窃取、勒索等犯罪从文明产生的那天起就一直存在，它们是我们日常生活的一部分。罪犯的目标总是一样的：尽可能赚钱，越多越好，越容易越好，风险越小越好。传统意义上，这并不容易，因为罪犯一般受地区因素局限，要想实施就得和潜在受害者发物理上的接触。这不仅限制了罪犯的下手群体范围，还让其承担了巨大的风险。然而，随着互联网和网络技术的兴起，犯罪发生了翻天覆地的变化。现在，网络罪犯能够轻易以极小或者为零的成本以及低风险，对几乎世界范围内的任何人实施目标性打击。除此之外，网络罪犯还变得高度有组织和高效率，这使得他们的攻击比以往都更有效。

最终，网络罪犯们知道，他们窃取的信用卡越多，他们侵入的银行账户就越多，或者说，他们破解的密码越多，他们能赚的钱就越多。他们真的就是在试图侵入连接上互联网的所有人——包括你。入侵世界上数以百万的人听起来像是一个巨大的工程，但事实上出奇简单，因为自动化工具帮他们把事儿都做好了。比如，他们可能会创建一个含有数百万电邮地址的数据库，然后用自动化工具来向每一个邮箱发送钓鱼信息。发送邮件几乎完全不花罪犯一分一厘：她们仅仅使用其它的被入侵的电脑——甚至或许是你

## 是的，你就是一个目标

的——来干所有这些粗活。这也是另外一个能证明为什么你的设备拥有价值的例子——至少他们能用你的设备来入侵或者损害他人。最终，这些罪犯并不知道谁最后会上钩，但是他们知道他们发送的钓鱼邮件越多，最后上钩的人就越多。或许罪犯会扫描互联网上的任何一台电脑（还是使用入侵控制的电脑来做扫描），寻找任何他们能够入侵的电脑或设备。记住，你不会因为你很特别就被排除在外。恰好相反，这些个罪犯把所有能作为目标的人都作为目标，这些目标恰好包括你。

### 保护你自己

当网络罪犯试图入侵世界上的人们的时候，他们一般都是用相对简单的方法。幸运的是，采取一些同样简单的措施，你就能在保护自己的道路上迈出一大步。以下是我们建议的一些措施：

- **你自己**：归根到底，你是抵抗任何网络攻击的第一线。许多攻击都以一个网络罪犯试图欺骗或愚弄你——比如欺骗你打开一个带毒的文件或者愚弄你让你在通话时泄露自己的密码——开始。常识是你的最佳防御：如果某个东西有点奇怪、可疑或者太好了以至于不可能是真的，那么它最有可能就是一次攻击。
- **更新**：确保你用的每一台电脑、每一部设备都全面更新并且打上了所有的最新补丁。这不仅对你的操作系统具有重要意义，对你用的每一个程序、插件也是一样。总是更新你的系统和程序能帮助你保护你免受最常见的攻击。
- **密码**：针对你的每个账号使用一个强健的唯一的密码。这样一来，当你使用的一个网站被入侵并且网站上的所有密码（包括你的）都被破解了的话，你的其它账号还是安全的。另外，保证



你或许还未意识到，你的设备和信息对世界上的网络罪犯而言具有巨大价值。

## 是的，你就是一个目标

你所有的不同的设备都被一个强健而唯一的密码、PIN码或者其它类型的锁定机制保护。我们建议你使用一款密码管理器来安全地储存你的不同密码。

- **信用卡：**经常检查你的财务帐单，我们建议至少一周一次（一月一次不够）。一旦你在信用卡上看见任何未经授权的交易，就及时告知你的发卡行。如果你的银行让你开启异常大额交易邮件或者短信提醒，就使用这项功能，以更快地收到可疑活动的通知。
- **你的网络：**通过设置强健的管理员密码来保护你的家庭网络Wi-Fi接入点，并且保证任何想连接你Wi-Fi网络的人都需要密码。另外，保证你知晓你家庭网络内的所有设备，并且那些设备都是最新的。
- **社会化媒体：**你在网上发布的信息越多，你的风险就越大。你发布的任何信息不仅能让网络罪犯更容易地以你为目标展开愚弄或欺诈活动，而且事实上还可能给你贴上一个“有价值的目标”的身份标签。

## 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

- OUCH! 《密码管理器》：<http://www.securingthehuman.org/ouch/2013#october2013>
- OUCH! 《保护你的家庭网络》：<http://www.securingthehuman.org/ouch/2014#january2014>
- OUCH! 《钓鱼式攻击》：<http://www.securingthehuman.org/ouch/2013#february2013>
- 海报“你是一个目标”：<http://www.securingthehuman.org/resources/posters>

OUCH! 由SANS Securing The Human出版，根据“[知识共享许可协议3.0（署名-非商业使用-禁止演绎）](#)”发行。你可以在不对其进行修改的前提下，自由传播这份新闻简报或在你的安全意识课程中使用它。了解翻译或更多信息，请联系：[ouch@securingthehuman.org](mailto:ouch@securingthehuman.org)。

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

翻译：成自豪