针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 概览
- 五个关键步骤

保证安全的五个步骤

概览

随着技术在我们生活中重要性的增加，它也在变得愈发复杂。想想技术更新的速度，你会发现有时很难与安全建议保持同步，感觉就好像总是有新的指南告诉你该做什么，不该做什么。然而，尽管如何保障安全在细节上随着时间推移而变化，一些最基本的东西仍然能帮助你保护自己。无论你使用什么技术，在什么地方使用它们，我们都推荐你采取如下五个关键步骤。

客座编辑

Lenny Zeltser供职于NCR Corp，专注保障客户IT操作安全，并在SANS Institute教授恶意软件对抗课程。他活跃于Twitter（@lennyzeltser）上，并且有一个安全博客（blog.zeltser.com）。

五个关键步骤

下面每个步骤都只是一个简单的概述。了解详情，请参考本刊底部的“相关资源”部分 。

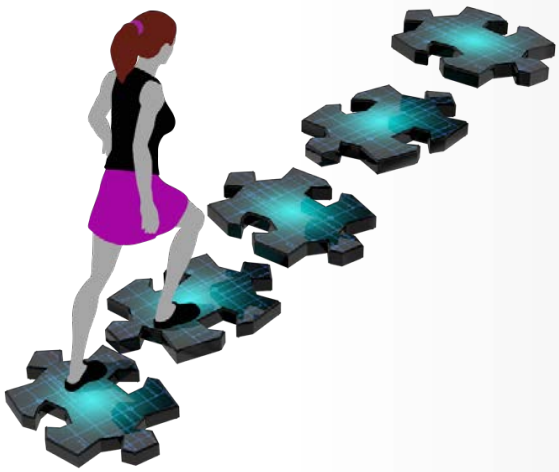
1. **你**：首先而且最重要的是，记住，单凭技术，是保护不了你的。攻击者已经认识到，绕过多数安全技术最简单的方法就是攻击你。如果他们想要你的密码或者信用卡，那么对他们而言最简单的方法就是骗你给他们这些信息。例如，他们可以假装是微软的技术支持，并且声称你的电脑受到了感染，而事实上他们其实是想要你给他们电脑访问权的网络罪犯；又或者，他们也许会向你发一封邮件，说你的包裹无法送达，要你点击一个链接，确认你的地址，而事实上他们是想要你访问一个恶意网站，以便让他们能入侵你的电脑。对这种技俩要保持怀疑，通过常识你能识破、阻止绝大多数的攻击。

2. **更新**：　确保你的电脑、移动设备、应用和其它任何连接到网络上的东西使用的软件都是最新的。网络最烦时刻都在寻找你所使用的技术中的漏洞。当他们发现这些弱点后，他们就会用特

© The SANS Institute 2014

保证安全的五个步骤

别的程序来利用这些漏洞，并且入侵你，包括你的网络、电脑和移动设备，无论你使用的是什么技术。同时，那些创造你当前使用的技术的公司也在加班加点让它保持更新，一旦有漏洞被曝出来，他们就会制作、发布补丁。通过升级电脑和移动设备，你就能减少已知漏洞数，使他人更难入侵你。为了保持最新，你最好在任何可行的时候都启用自动更新。这一法则适用于几乎所有的与网络相连的设备，包括网络电视、婴儿监视器、家庭路由器、游戏机，有朝一日包括你的汽车也说不定。如果你电脑的操作系统、移动设备或者你在使用的其它技术不再受到支持，并且将不会得到任何更新的话，我们建议你获取一个有支持的新版本。



采取这五个关键步骤，你就能在利用最新技术的同时有效保护你自己。

3. **密码**：保护你自己的下一个步骤就是针对你的每个设备、网上账户和程序使用一个独一无二的强密码。这里的关键词是“强”和“独一无二”。强密码指的是不能被轻易猜到和被暴力破解的密码。与其使用一个词，不如使用由多个词以及一些符号和数字组成的一个长密文；而“独一无二”则意味着每个设备和每个网上账户的密码都不一样。这样一来，如果一个密码被破解了，其它账户和设备仍然安全。怎么，记不住所有这些独一无二的强密码？不要担心，我们也记不住，这也是为什么我们推荐你使用智能手机和电脑上用来加密存储所有密码的特殊程序，它就是密码管理器。最后，如果你的账户支持两步校验，我们十分建议你启用它，因为它也是账户的有力保护之一。

4. **加密**：我们建议的第三个措施就是使用加密。加密确保只有你或者你信任的人才能访问你的信息。数据在两个地方可以被加密：静态数据或动态数据。静态数据加密的意思是在数据被作

© The SANS Institute 2014

保证安全的五个步骤

为文件存储在你的硬盘或者U盘上时加密，大多数操作系统都能支持全盘加密等自动加密的功能，我们十分建议你只要有可能，就启用这个特性；动态数据加密的意思是加密电脑或设备间传输的数据，比如加密你登录网上银行时传输的数据。判断浏览网页时加密是否被启用的一个简单方法就是看你访问的网址是否以“https:”开头，并且开头旁边是否有个锁形标志。

5. **备份**：有些时候，无论你多么小心，你的某个设备或者账户还是有可能被侵入。如果这真的发生了的话，确保你的电脑或者移动设备不被恶意软件侵扰的唯一方法往往是全盘擦除重装。攻击者甚至还有可能阻止你访问个人文件、照片以及其它储存在被入侵系统上的信息。这样的话，你就只能从备份中回复你的所有个人信息。确保你按时备份你的重要信息，并且检查其有效性。大多数操作系统和移动设备都支持自动备份。

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
保护你的平板电脑:	http://www.securingthehuman.org/ouch/2013#december2013
强密码:	http://www.securingthehuman.org/ouch/2013#may2013
密码管理器:	http://www.securingthehuman.org/ouch/2013#october2013
两步校验:	http://www.securingthehuman.org/ouch/2013#august2013
加密:	http://www.securingthehuman.org/ouch/2014#august2014
个人备份和恢复:	http://www.securingthehuman.org/ouch/2013#september2013

OUCH！由SANS Securing The Human出版，根据 " 知识共享许可协议4.0（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。

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

© The SANS Institute 2014