OUCH!

SANS SECURITY AWARENESS

每月安全意识通讯

让密码简单

概述

你经常听说你的密码是保护你账号的关键（确实是这样），但是鲜有人告诉你一个简单的安全创建和管理你所有密码的方法。下面，我们将介绍三种帮你简化密码、锁定账号和保护未来的方法。

密文

使用疯子般复杂密码的时代已经过了。那些密码很难记，很难输，并且用今天运算超快的电脑，网络攻击者很容易破解。密码的关键在于长，越长越好。这些密码叫作密文——一种用短句或随机词语组成的强密码。这里有两个例子

Time for strong coffee!（喝浓咖啡的时间到了！）
lost-snail-crawl-beach（遗失—蜗牛—爬行—沙滩）

这两个超过 20 个字母的密码都是强密码，很好记，很好输，但是很难破解。你会遇到要求你在密码中加入特殊符号、数字或大写字母的网站或情况，这很正常。但记住，长度才是最重要的。

使用密码管理器吧。

你需要为每个账号创建一个独一无二的密码。如果你的多个账号都使用同一个密码，那么你将自己置于极大的危险之中。网络攻击者所需要做的，仅仅是入侵一个你使用的网站，窃取包括你的密码在内的所有密码，然后用你的密码来冒充你，登录你所有的其它账号。这种事发生得比你意识到的要多得多。不相信？打开 www.haveibeenpwned.com 这个网站来看看你用的哪些网站被入侵了，以及你的密码是否潜在被破解了。那么你该做什么呢？使用密码管理器吧。

这是一种特别的电脑程序，它能将你所有的密码安全存储在一个加密保险库中。你只需要记住一个密码——密码管理器的密码。密码管理器接下来会自动在任何你需要的时候，读取你的密码，为你登录网站。他们还有一些其它功能，诸如储存你安全问题的答案，在你重复是用密码时警告你，作为一个保证你使用强密码的密码生成器等等等等。大多数密码管理器还会将你的密码安全地同步在几乎任何电脑设备上，所以无论你使用什么系统，你都能轻松、安全地访问到你所有的密码。

最后，确保你把密码管理器的密码写在纸上，并将其存放在家中的一个安全位置。有些密码管理器甚至让你打印一份密码管理器恢复包。这样一来，如果你忘记了密码管理器的密码，你还有个备份。或倘若你生病了或遇到突发情况，你的配偶或信赖的家人还能替你找回信息。

两步验证

两步验证（一般叫作“双因素验证”或“多因素验证”）提供一层额外的安全防护。它要求你在登录账号的时候同时拥有密码和一个智能手机生成的或发到你手机的数字码。这个过程确保，即便网络攻击者获得了你的密码，他也无法进入你的账号。两步验证很好设置，并且你通常只需要在你用新电脑设备登录的时候操作一次。只要可以，就开启两步验证，特别是为你的银行、退休、邮箱账号等最重要的账号开启。如果你在使用一款密码管理器，我们强烈建议你用强密码以及两步验证来保护它。

这些方法也许听起来很傻，不过对保护你的工作、名誉和财务未来而言大有裨益。

特邀编辑

Justin Henderson (@SecurityMapper)是 H&A 安全解决方案的联合创始人，同时也是 SANS Institute 的认证讲师，以及 SANS 网络防御和 SIEM 课程的作者。他喜欢所有关于网络防御的东西，并且已经在咨询行业深耕了十五年。

资源

我的密码泄露了吗:	https://haveibeenpwned.com/
两步验证网站:	https://twofactorauth.org/
NIST SP800-63B 数字身份准则:	https://pages.nist.gov/800-63-3/sp800-63b.html
海报: 你是一个目标:	https://www.sans.org/u/OGi