针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 密文
- 安全使用密文
- 相关资源

密文

背景

每天你基本上都会用到密码，无论是查邮件、网银购物还是访问智能手机。但同时，它也是你的致命弱点之一。一旦某人知道了你的密码，他们就能窃取你的身份，转移你的存款或是访问你的个人信息。强密码对保护你自身而言相当必要。本期，我们将了解如何创建易记的强密码——密文。

客座编辑

Guy Bruneau是IPSS Inc.的一位高级安全顾问、一名SANS讲师和ISC处理员Guy拥有SANS GSE认证，并且完成了SANS网络守护者项目。你可以在Twitter（**@GuyBruneau**）上关注他或者在**handlers.sans.org/gbruneau**了解他的动态。

密文

当前我们正面临严峻挑战，网络攻击者已经研发出了相当复杂的方法来猜解或“暴破”密码，并且他们的手段越来越先进。这意味着，如果你的密码很弱很好猜，那么他们就能破解它。保护自己的一个重要手段就是使用强密码。密码的位数越长，就越强越难猜。然而不管有多长，要记住复杂的密码都不是一件容易的事。因此我们建议你使用密文——由简单的短语或句子构成，好记但难猜。比如这个例子：

Where is king Julian?

这个密文之所以如此强，并不单单是因为它长度为21，还因为它用了大写字母和符号（记住，空格和标点都是符号）。如果把字母换成数字或标点，比如用“@”代替“a”或者用数字“0”代替字母“o”，这个密文还可以更强。如果网站或程序限制了密码长度，那么就用允许长度范围内的最长密码。

密文

安全使用密文

在使用密文的方式上你也必须留意。如果不法分子能够轻易窃取或复制它，使用密文也是无济于事的。

使用密文是保护你身份和信息的最有效的方法之一。

1. 针对不同账户、设备使用不同密文。例如，工作账户和诸如网银、Facebook、YouTube、Twitter等个人账户就不要使用相同的密码。这样一来，如果一个被入侵，其它的账户仍然是安全的。如果你密文太多记不住（这很常见），那么你可以考虑使用密码管理器——专门用来帮你安全存储密码的程序。这样，你只需要记住你的电脑密码和密码管理器密码就够了。

2. 不要跟任何人谈及你的密文或者你创建密文的策略，包括同事。记住，密文属于秘密，一旦其他人知道了，它就不再安全。如果你不小心将密文告诉了别人或者认为你的密文已经被破解被盗，那么一定要马上对其进行变更。

3. 同密码一样，要避免使用容易猜想到的或者常见的密文，例如“Four score and seven years ago”（来自林肯葛底斯堡演说，译者注）就不是一个好密文，因为它太常见了，大家都知道。

4. 不要使用酒店、图书馆等地方的公共电脑登录工作或银行账户，因为任何人都可以使用公共电脑，它们可能已经感染了键盘监听的恶意代码。只在可信的电脑或移动设备上登录你的工作、银行账户。

5. 对要求你回答私人问题的网站要格外小心。这些问题用于密码找回。问题在于，这类问题的答案常常可在网上甚至是你自己的Facebook主页找到。确保你回答的问题的答案都不是公开的，或者干脆就是自己编的。密码管理器在这方面同样能帮你储存额外的信息。

密文

6. 许多网上账户提供双因素校验功能，它也被称作两步校验。使用它的时候，你需要不止一个密码来登录，比如还要求你输入发送给你手机的校验码。这一手段的安全性比单纯使用密文要高得多。只要有这些安全选项，就启用它们。

7. 移动设备经常要PIN码来解锁。记住，PIN码和其它密码别无二致。PIN码越长越安全。许多移动设备还让你使用密文。

8. 最后，如果你不再使用某个账户，那么一定要关闭、删除或者禁用它。

公共电脑

不要使用酒店大厅、图书馆或网吧里的公共电脑，你完全不知道在你之前有多少人用过它们，他们可能或无意或有意地让其感染了病毒。无论何时，都尽量使用你能控制和信任的设备用于线上活动。如果你必须要使用公共电脑，那么不要使用需要你登录或输入密码的任何服务。

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

《两步校验》：	http://www.securingthehuman.org/ouch/2013#august2013
《密码管理器》：	http://www.securingthehuman.org/ouch/2013#october2013
《社会工程学》：	http://www.securingthehuman.org/ouch/2014#november2014
常用安全术语:	http://www.securingthehuman.org/resources/security-terms

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