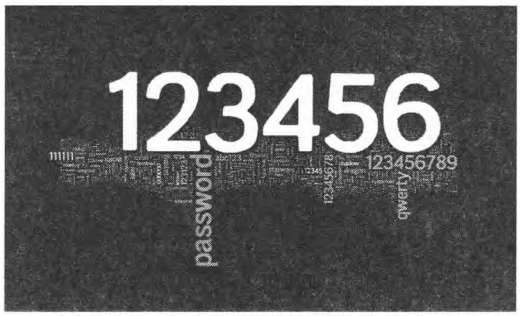
提升安全意识
保护密码安全

文/ASL

电子商务与社交网站的普及，让用户需要注册越来越多的网站账户和密码。简单的密码虽然便于记忆，但是存在着很大的安全隐患。每年SplashData公司都会针对被黑账号进行调查，然后公布“年度最糟糕密码排行榜”，在刚刚过去的2013年，“123456”成功打败“password”，问鼎这个宝座。事实上，不管是网络账户、信用卡还是银行卡，密码都是拦截网络犯罪分子入侵账户的最基本防线，其复杂程度直接影响到用户的数据与信息安全。



这幅文字云图像显示的是人们最常用的密码，其中字体越大其使用率越高

1 密码泄露的影响

可能有人觉得自己又不是名人，又没什么钱，密码泄露没什么危害，但总有你想不到的信息会因此暴露，并产生一系列麻烦。

密码泄露产生的影响有以下几个方面。

账号曝光只是最直接、最浅层次的损害，如果是论坛、SNS账号，可能导致身份被假冒用于发布虚假文章；如果是游戏网站，则游戏装备可能被盗取。而邮箱账号被公开，对某些网络营销者、病毒集团来说，无异于天上掉馅饼，对被泄露者来说，则意味着将收到更多的垃圾邮件、广告邮件，甚至是木马钓鱼邮件。

众所周知，同一厂商的邮箱一般与多个网络服务账号相通，比如新浪邮箱与新浪微博、新浪博客，Gmail与谷歌文档、Google+等，账号和密码都是相同的，如果邮箱和密码被公开，网民的私信、照片、社交网络也随之被曝光，各种“门”可能会不邀而至。

还有不少网民用一个邮箱注册了多家网络服务，甚至通用一个密码，比如用网易邮箱注册团购、淘宝、支付宝等电子商务网站，或者用邮箱接收银行信用卡账单、个人理财、股票交易信息等。由于这些均与银行账户直接关联，账号曝光导致的危害性更高。

危害可能还会波及你的亲友。如果恶意攻击者盗用你的邮箱或者SNS账号，给你的亲朋好友发送假冒欺诈信息，比如临时借钱或者网购东西，他们由于对你的信任，极有可能上当受骗。

上述的影响大都涉及到基于账号盗取的隐私暴利。

黑客一般能按以下步骤进行利用：

1）从账号信息中找到关联的邮箱，破解邮箱的密码。

2）搜刮邮箱里面的重要信件和资料，如网游账号信息、公司资料、个人照片等。

3）通过社会工程学搜索，确认哪些邮箱与重要的人物、公司有关联，可以用来做商业犯罪或者发布病毒等。

4）没太大用处的邮箱可以用来广发垃圾邮件和病毒，也可以用来注册大量垃圾账号，广泛用于论坛刷帖等等。

5）黑客把所有密码编成字典，以后盗号可以更快了。

6）隐私信息都可以用于社会工程学攻击，用于制作钓鱼邮件。

以上步骤除了能榨取用户账户内的有限财富外，用户本身的隐私和数据也具有很大的利用价值。

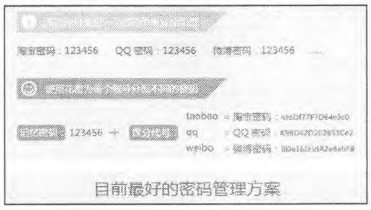
2 密码设置安全原则

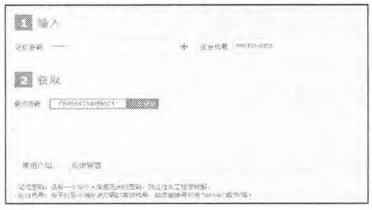
基本原则

首要第一条便是密码不要设定为带有生日、电话号码、QQ或邮箱等与个人信息有明显联系的数据，否则你的密码即使不能入选“年度最糟糕密码排行榜”，也会被犯罪分子轻易联想到；第二，尽量为不同网站设置不同密码；第三，妥善保存密码并定期修改。不要将密码信息保存在电脑、手机中，这些设备一旦丢失，里面的密码也将失守；第四，不要将密码信息轻易透露给他人，特别是通过即时通讯工具、邮箱等。

低关联性

有些人设置的密码确实复杂，但是有可能存在的一种情况就是使用同一个密码，这种情况不在少数，即使是有些是搞安全的也会存在这样的情况，这样存在一种风险，就是一旦有一个密码被盗了，其他所有的全部完了。有的密码虽然不一样，但是规律却很明显，这样也是跟用同一个密码区别不大。





注册邮箱

保护好自己的邮箱。很多时候注册都需要填写邮箱进行验证。如果在多个地方注册使用同一个邮箱，一旦我们的邮箱被破解，那么我们其他网站密码被破解的可能性就会变大。所以，这里的建议是注册多个邮箱，或者单个网站对单个邮箱，对于不常去的且不重要的，可以单独注册一个这样的邮箱。特别重要的，可以注册一个重要的邮箱，也可以根据自己的情况去申请几个邮箱，作为某一类或某一种情况的专用。

密码强度

将自己现有的网络账户进行分类整理，密码根据账户的重要程度去进行设置。可以分为三个等级：弱、中、强。

弱：一般表示非常容易记的，不用去背的。例如123456这样的密码。中：一般为字母+数字，其中有的密码是由名字和生日进行组合而成的，或者某些单词+数字，这种与上一种要复杂一些，位数要多一些。高：大小写字母+数字+特殊符号。比较复杂，不容易记忆。

当然除了字符以外，密码的长度也是其中的一个标准。安全的建议是8位以上复杂密码和中等密码，这样在破解的过程中耗费的时间要长很多。

你也可以通过微软官方的密码检查器来检查自己的密码强度（http://t.cn/8FN0fyj）。

3 密码的保护

设置复杂的密码只是为了防止被别人破解，但是获取密码的方式不止一种破解方式，如果想要做到安全，需要了解相关的安全知识。

获取密码的方式可以通过网络钓鱼、键盘记录方式、嗅探、暴力破解，社会工程学、读取内存实现。窃取文件（读取配置文件），密码的保护的话也是从这些方面入手防御。

对于钓鱼和键盘记录，我们要提高警惕，不要随意打开一些网址（要注意看好网址）以及别人发来的文件等（除了exe外，还要小心doc、xls、pdf这类常用文件），需要确认后打开查看。

嗅探的话，做好arp方面的防御；暴力破解，就是加强自己的密码强度，设置复杂的密码。

社会工程学，不要轻易告诉别人你的密码，并且说要密码的邮件或者网站，都不要相信，别人说因为某某原因需要提供密码的时候也不要给。

对于配置文件方面，要加强程序的安全、服务器的安全性，防止配置文件被别人查看。做好文件系统的权限设置。

希望使更多人了解，使用较弱的密码会带来什么样的风险，希望有更多人可以采取简单的措施来保护自己，包括使用更强的密码，以及在不同网站使用不同密码。

虽说没有人期望你是一个安全专家，但希望你能保持警惕。

万方数据

提升安全意识保护密码安全

万方数据 WANFANG DATA 文献链接

作者： ASL
作者单位：
刊名： 电脑迷
英文刊名： PC Fan
年，卷(期)： 2014(6)

本文链接：http://d.g.wanfangdata.com.cn/Periodical_dnm201406020.aspx