关于避免使用弱密码的安全提示

一、什么是弱密码

弱密码(Weak passwords)即容易破译的密码，多为简单的数字组合、账号相同的数字组合、键盘上的临近键或常见姓名、终端设备出厂配置的通用密码等都属于弱密码范畴。弱密码很容易被他人猜到或破解，所以如果你使用弱密码，就像把家门钥匙放在家门口的垫子下面，这种行为是非常危险的。

二、常见弱密码

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 弱密码 | 序号 | 弱密码 | 序号 | 弱密码 |
| 1 | 123456 | 10 | ILOVEYOU | 19 | 654321 |
| 2 | PASSWORD | 11 | PRINCESS | 20 | !@#$%八&\* |
| 3 | 123456789 | 12 | ADMIN | 21 | CHARLIE |
| 4 | 12345678 | 13 | WELCOME | 22 | AA123456 |
| 5 | 12345 | 14 | 666666 | 23 | DONALD |
| 6 | min | 15 | ABC 123 | 24 | PAS SWORD 1 |
| 7 | 1234567 | 16 | FOOTBALL | 25 | QWERTY123 |
| 8 | SUNSHINE | 17 | 123123 |  |  |
| 9 | QWERTY | 18 | MONKEY |  |  |

三、弱密码的危害

弱密码的危害性比想象中要大得多，对于实体银行卡被盗，弱口令被猜出,户主损失大量的钱财；对于个人电脑或工业主机，弱密码意味着容易成为黑客的肉鸡，成为他们进行不法行为的跳板或僵尸网络的一部分，甚至电脑资料泄露，感染病毒，造成严重损失；信息系统、网站和虚拟机的管理员采用弱密码、默认密码和通用密码，或者长期不进行修改，容易被黑客使用暴力破解软件直接破解本地密码，导致服务器被黑客控制，成为他们进行不法行为的跳板或僵尸网络的一部分，或服务器内部资料泄露，造成群体性危害事件等。

四、常用密码设置原则

1.不使用空密码或系统默认的密码，因为这些密码众所周知，为典型的弱密码。

2.密码长度不小于8位。

3.密码不应该为连续的某个字符（例如：AAAAAAAA）或重复某些字符的组合（例如：tzf.tzf.）。

4.密码应该为以下四类字符的组合，大写字母（A-Z）、小写字母（a-z）、数字（0-9）和特殊字符。每类字符至少包含一个。

5.密码中不应包含本人、父母、子女和配偶的姓名和出生日期、纪念日期、登录名、E-mail地址等等与本人有关的信息，以及字典中的单词。

6.不要长期使用固定密码，应定期或者不定期修改密码。

7.不要在多个场合使用同一个密码，应为不同应用场合设置不同密码，特别是有关财务的网银及网购账户，避免一个账户密码被盗，其他账户密码也被轻易破解。

8.不把密码保存在电脑、U盘、笔记本、书籍等上面。

五、密码设置建议

推荐使用自己喜欢的单词-喜欢的数字排列-网站名称的前三个大写字母或者后三个大写字母，也可以找到一个生僻但又容易记住的短语、句子、歌词、书名或者电影台词都可以摘录，并创建它的缩写形式，其中可包括大写字母、数字和标点符号等。