

密码安全

了解如何创建安全的强密码以及如何管理密码

1.什么是强密码？为何要创建强密码？

强密码是整体密码安全的关键。强密码，指不易被猜中或破解的密码。

使用强密码将增强账户安全，防止黑客和其他不法分子未经授权访问您的帐户、窃取您的数据和信息。

但是，强密码也可能很难记住。使用密码管理器来帮助您记录和安全存储您的密码！

2.强密码的特征

对您的密码采用以下最佳实践：

- 长密码最好
 - 目标是至少 12 个字符
- 使用各种字符的组合
 - 大小写字母
 - 数字
 - 符号
- 使用生僻词

切忌使用简单易记的键盘路径或常用词，尤其是“password”、“login”或“qwerty”等词。请务必避免使用包含个人信息的密码，例如您的生日、地址、宠物或家属的名字等。

3.提高密码强度

以下是一些简单的常用密码。请在表格中填写如何提高密码强度的建议。

密码	提高密码强度的建议	您在此采用了哪些最佳实践?
P4ssw0rd		
Fluffy0212		
1234567		
Yankees87 (运动队 + 出生年份)		
Austin2010 (精彩旅行 + 年份)		
Eva23 (孩子的名字 + 毕业年份)		

4.从头开始创建强密码

根据以下建议设置强密码。

A.)使用密码生成器

密码生成器可以生成难以破解的随机密码。唯一的缺点是这些密码往往很难记，因此您应该使用密码管理器来存储这些密码。随机生成密码是一个不错的方式，可以为敏感帐户创建格外安全的密码。

思考题目 — 您想要在哪些地方使用随机生成的密码，请写在此处：

B.)使用密码短句来代替密码

与其使用某个单词，不如选择一个容易记忆的短句。然后，使用短句中每个词的首字母创建一个密码短句，再加上符号和数字，构建您的密码。采用这种方法时，您也可以混合使用数字、符号和短句或名句的唯一拼写。

以下是 [Cybernews.com](https://www.cybernews.com) 上的一些示例。

短句示例：I first went to Disneyland when I was 4 years old and it made me happy（我四岁的时候第一次去迪斯尼乐园，那是一段很开心的经历）

密码示例：I1stw2DLwlw4yrs&immh

NYC Digital Safety

Privacy & Security

短句示例：“One for all and all for one”: The Three Musketeers (“我为人人，人人为我”
：三个火枪手)

密码示例：14A&A413Mu\$keteesr!

思考题目一 您想要在哪些地方使用密码短句，您想到了哪些短句，请写在此处：

C.)混合词典中的词

您也可以从词典中选择一些随机词语，将它们混在一起，再结合字母、数字和符号，共同组成一个安全密码。这里需要注意的一点是，避免只从词典中挑选一个词，因为黑客可以轻易猜到这些词。

思考题目一 您想要在哪些地方使用词典法构建的密码，请写在此处：

4.保护这些密码

考虑下列做法，并讨论您可以在哪些地方增强密码安全。和大家一起头脑风暴，分享您的经验！

NYC Digital Safety

Privacy & Security

- 确保每个帐户都有唯一密码
- 设置多重身份验证
- 使用密码管理器
- 注意您注册帐户的位置
- 最小化数据，留心您要公开的信息
- 警惕网络钓鱼骗局
- 经常更改密码
- 检查不同帐户的隐私设置

您还能想到哪些做法？