管理好自己密码的10个技巧 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E7_AE_A1_E7_90_86_E5_A5_BD_E8_c100_460835.htm 密码技术本身有着致命的缺陷，这话本身并没错。但对目前的大多数企业来说，它们却是最好的选择。其实，每个人都可以更有效的管理自己的密码。 密码的安全一直以来都是一个难题，除非将来可以使用类似生物检查的技术来取代它而这是目前工业技术正在努力的方向。在那一天到来之前，我们最好还是着手培养一个安 全文化，从而更有效的管理我们的密码。 1. 一定不要把密码写在纸上 如果有人对这一条感觉不可思议的话，那么只要我们还在谈论密码管理，我们就不得不把这一条作为首要点提出来。 如果你已经告知职员们为什么不能这么做，但是职员依旧写下他们的密码，那么要么是你的系统太复杂，要么就是你对他们的要求太多了。公司必须在安全性和易用性之间保持一 个平衡，因为如果不理解后者，就会很容易破坏前者。 所以必须确认雇员们是否已经接受了正确的密码安全教育，如果你需要修订你的密码政策，请参考下述措施。 2. 必须设置密码 你刚才看到第一条的时候，是不是觉得它太显而易见了？但是如果你看到很多系统只是采用了默认的自带密码，比如“ password ”或者“ changeme ”或者其他类似的单词，而并未 对密码进行修改或设置，你就不会对这一条觉得惊讶了。 3. 尽可能的减少密码 注意在密码数量与可管理性之间维持一个平衡。确认哪个网络系统软件需要最高的优先权。如果职员们必须记住10个密码，分别对应着从最绝密到最垃圾的数据，他们可能根本无法全部记住它们。 谁又能

保证他写下来又丢失了的那个密码不是最绝密的那个呢？ 4. 职员必须定期更改密码 这一条限制了原先同事们之间互相了解的老密码的危害性。同时它也关闭了那些不慎落入不法之徒手中老密码的“ 机会之窗 ”。 至于多久让雇员们更改一次密码，这取决于你如何在安全性和易用性之间保持平衡。如果雇员们被要求每周修改一次密码，他们很容易前后弄混，最后不得不用笔把密码写下来。 实际上修改密码的时间间隔比如90天和30天的对比证明越长期限的密码有效期，越能让人们记住复杂的密码，越能让人们更小心的照管密码。 5. 新密码必须脱胎换骨 更改密码时，切忌直接从老密码变换而来，尤其是那种只改变一个字母的做法。类似RandomW0RD1, RandomW0RD2, RandomW0RD3这样的密码更改，要被人猜出来简直是太容易了。 6.不使用常见单词 密码中不应当使用常见单词，从而可以避免被“ 辞典攻击 ”破解(所谓辞典攻击，就是使用软件自动从辞典中读取所有单词，并逐一测试该单词是否是正确的密码)。姓名、住址 或其他很容易联想到的单词也应当被禁止使用。很多雇员喜欢使用自己的姓名、合作者的姓名或者宠物的名字来做密码，这种情况需要引起足够的重视。 7.密码要够长但不要过长 一个密码起码应当有8位，包含大小写字母和数字。如果密码的长度过长，职员们可能会懒得去记，从而使用一些重复性的字母，或者常见的字符串：比如“ ABCDEFG123456789 ”这 种。 其实，给出一个最低长度和一个合理的上限，反而有助于雇员们发挥创意。一个建议是使用短句要比使用单词效果好。比如mYd0g1sCALLEDf1d0就比"fido"难猜得多了。再重复一 遍，要建立更安全的密码，就不要忽略这一步。 8. 自动强制更改

密码 应该自动的强制性要求职员更改和选择安全密码。不要指望职员们会记住他们上一次更改密码是什么时候，他们过去几年用了哪些密码，以及什么样的词汇不能用于密码之中。这 不是一个信任与否的问题。这是一个历史问题，它告诉我们政策从不依附于选择。 9. 教育职员 确保密码政策被写入雇佣合同，并确保所有的职员了解为何这是必要的。乐观的说，如果其他措施确实有效，可能最认真的人才能达到要求，不要互相透露密码，不要把密码写下 来。这些条款也将阻止服务之间的密码重复特别是企业的内部与外部之间。一个公司的登陆可能比一份报纸的订阅登陆更机密，而后者可以与朋友或家人共享。 10. 放眼未来 最后，注意那些可能取代密码的长期解决方案比如生物检查技术和双因素认证。密码是有缺陷的，而上述推荐的技巧只是设法让密码变得更安全起码现在看起来更安全。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com