
# 笔记本电脑安全防护

# 笔记本电脑安全防护

笔记本——多个身份——盗窃”这个话题好像已经重复了很多次了。不管是谁，饭店的清洁人员还是把笔记本放在车里的知名的审计员（他会在每年检查时想客户重复这些不注意的地方），笔记本和其他物理上不安全的电脑都在大量的丢失或者被窃。丢失笔记本已经不再只是不方便的事情了。最重要的是，这样会导致很多敏感信息处于风险之中。

- **笔记本电脑安全手把手指南之介绍**

## 笔记本安全问题如何发生

你有没有想过人们是如何发现和/或窃取这些不安全笔记本，而其他电脑又是如何攻入这些系统获取敏感信息的呢？我没有采访过任何犯罪人员，但是我斗胆猜测以下他们有自己的工具和技术。不管是多么基础的东西，很多人的笔记本电脑都没简单的密码。电脑工程师都不需要破解代码，而我不会讲这些安全测试技术和这些问题的解决方案。但是那些有密码的电脑呢——那些恶意人士又是如何破入的呢？

- **第一步：笔记本安全问题如何发生**

## 对笔记本电脑的攻击

如果黑客已经进入了笔记本电脑，他们就可以查看存储的密码，进入查看其它的敏感信息——特别是存储在 VPN 客户端的可以提供直接进入网络的信。这类信息可以使用类似于 ElcomSoft Ltd.公司的 Proactive System Password Recovery 等的工具找到。它可以恢复……

❖ 第二步：如何攻击笔记本电脑

## 笔记本电脑安全防护

前文已经解释了所有这些笔记本电脑的攻击技术和工具，你可以关闭系统防止恶意事件的发生。可以创建一个加密的“分区”，它基本上是和正常的磁盘一样的文件。但是我并不特别鼓励这么做。这都要归结于你不信任你的用户每次都会把敏感数据存储在安全的分区上。用户会把资料存储在没有保护的桌面上、邮件应用中以及本地的临时目录下。

❖ 第三步：如何保护笔记本电脑安全

## 笔记本电脑安全总结

笔记本电脑的安全风险是现实中的人遇到的现实问题，而且如果你——和你的管理层——采用可正确的方法就可以避免。以下是可以保护你的笔记本电脑和其他被窃的电脑的安全的一些办法。

❖ 第四步：笔记本电脑安全总结

# 笔记本电脑安全手把手指南之介绍

“笔记本——多个身份——盗窃”这个话题好像已经重复了很多次了。不管是谁，饭店的清洁人员还是把笔记本放在车里的知名的审计员（他会在每年检查时想客户重复这些不注意的地方），笔记本和其他物理上不安全的电脑都在大量的丢失或者被窃。

丢失笔记本已经不再只是不方便的事情了。在现在这种严格管理的社会上，不小心会导致合约被取消、违法事件以及违反行业规则等问题。最重要的是，这样会导致很多敏感信息处于风险之中——商业机密，最重要的是个人生活。根据 ChoicePoint 事件后的数据泄露报表，总共有 31,796,785 的身份问题在电脑丢失和被窃中受到威胁。在 Privacy Rights Clearinghouse 网站上列出了大量的事故，在很多情况下，都不清楚有多少身份处于风险中。

为什么大家不把这个问题大声说出来呢？更重要的是，为什么企业不做些什么呢？你想要做恰当的事情来保护笔记本的安全吗？本系列文章将给你建议！

*（作者：SearchEnterpriseDesktop.com 译者：Tina Guo 来源：TechTarget 中国）*

## 第一步：笔记本安全问题如何发生

你有没有想过人们是如何发现和/或窃取这些不安全笔记本，而其他电脑又是如何攻入这些系统获取敏感信息的呢？我没有采访过任何犯罪人员，但是我斗胆猜测以下他们有自己的工具和技术。不管是多么基础的东西，很多人的笔记本电脑都没简单的密码。电脑工程师都不需要破解代码，而我不会讲这些安全测试技术和这些问题的解决方案。但是那些有密码的电脑呢——那些恶意人士又是如何破入的呢？

接触这个问题的做好方法是从恶意的角度看问题。我并不是提倡或者支持犯罪活动。但是，我确实强烈的相信真正保护系统的唯一方法是从犯罪的角度查看安全问题。当说到笔记本黑客活动的时候，你需要运行一些测试查看你可以用多长时间进入系统和你的网络。

**已经以完全的权限登录了**

电脑系统正在开启的时候就可以被窃取。电量充足的笔记本对这些人来说最方便。不需要中断，然后重新进入—— 他们只需要接受系统并在另外的地方运行，并查看可以收集到什么信息。

一旦他们进入了，任何东西都成了可攻击的对象。很多企业都有这样的政策，任何敏感信息都不能存储在本地硬盘或者移动设备上。正确。我总是看到这样的问题。经常会在个人的电脑上看到各种类型的 Word 处理文档、电子表格文件和其他包含敏感信息的文件。

自己看一下。如果你激活了远程登录并且是本地管理员组的成员，就可以从网络上自己做了。可以在 C:Documents and SettingsAll UsersDesktop and C:Documents and SettingsusernameDesktop 下查看。还可以登录手还在 Outlook 或者其他类型的邮件客户端，查看里面存了什么。用户可能采用邮件作为信息存储库，它就成了敏感信息的金矿。

考虑一下，如果这种数据可以被犯罪分子看到会发生什么呢？所以应该使用简短的屏保时间，要求用户在电脑不适用的时候锁定屏幕，或者在用户离开的时候自动锁定屏幕。

**推断密码**

犯罪分子的下一步可能是简单的推断登录或者屏保密码——有时和 1-2-3 一样简单。在这种情况下，我们假定电脑是开机的，而且用户使用屏保锁了屏幕。很黑可以输入用户的登录 ID（可能显示上次的登录 ID）作为密码，或者在结尾增加 a 1、感叹号或者“pass”。实际上，这很常见。如果屏保密码不起作用，可以简单的重启系统来查看——可能不需要密码就能登录 Windows.

如果重启了，而且提示你需要 BIOS 开机密码，这就是另一层的防御了，但是绕开也没问题。有很多办法重新设置这些密码。

*（作者：SearchEnterpriseDesktop.com 译者：Tina Guo 来源：TechTarget 中国）*

# 第二步：如何攻击笔记本电脑

### 寻找密码

如果黑客已经进入了笔记本电脑，他们就可以查看存储的密码，进入查看其它的敏感信息——特别是存储在 VPN 客户端的可以提供直接进入网络的信。这类信息可以使用类似于 ElcomSoft Ltd.公司的 Proactive System Password Recovery 等的工具找到。它可以恢复登录密码、网络密码、无线加密密钥、拨号/VPN 密码以及其它更多的可以用于攻击的信息。图 1 是 Proactive System Password Recovery 这款工具的界面。


图 1：Proactive System Password Recovery

**破解密码**

如果你已经做了恰当的事情并要求 Windows 使用 Windows 强制的强大密码登录，你可能会想别人还能用别的什么办法攻入呢。不要担心，还是可以实现。只是简单的密码破解，甚至不需要购买工具就可以做到。我曾经用过一个相对较新的攻击叫做 Ophcrack，它使用 rainbow tables 快速破解 Windows 密码。Ophcrack 有一个可启动的“Live CD”版本，可以不用其它方式访问 Windows 系统就可以使用。所以，考虑一下：犯罪分子可以找到/窃取你的系统，使用 Ophcrack 等工具启动，而后，在几分钟内他就可以获得一个或者更多的 Windows 帐户密码。在这之后就全部结束了。可以自己运行 Ophcrack Live CD，看看可以找到什么。

图 2 显示的是 Ophcrack 的 Windows 版本——Live CD 的 Linux 版本本质上和这个是一样的。

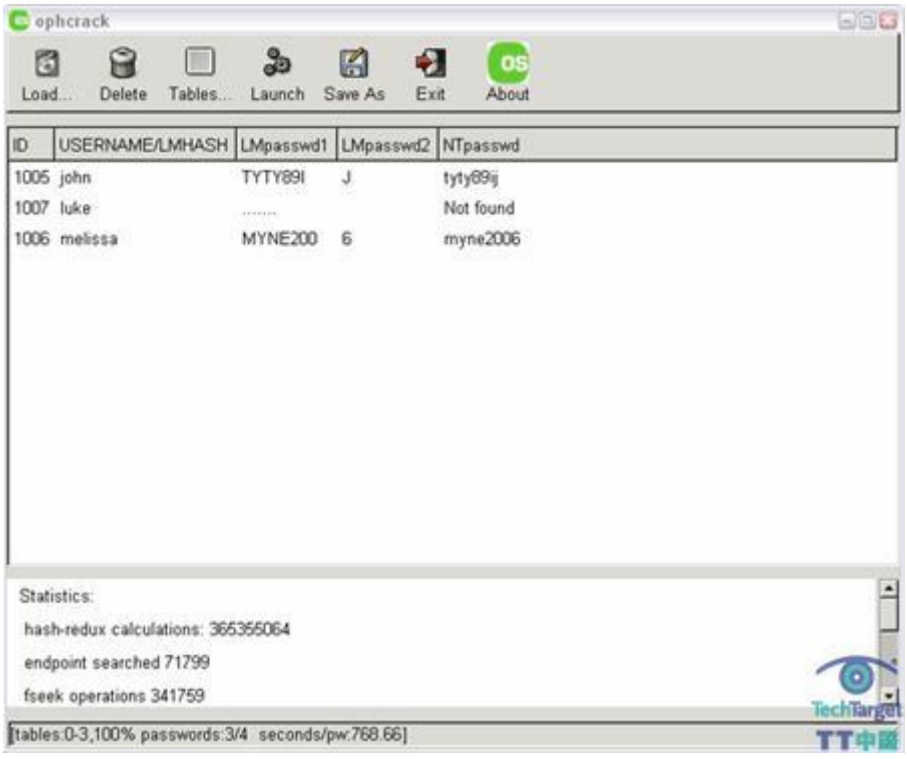

图 2 ： Ophcrack 的 Windows 版本

*(作者：SearchEnterpriseDesktop.com 译者：Tina Guo 来源：TechTarget 中国)*

## 第三步：如何保护笔记本电脑安全

**简单的解决方案**

前文已经解释了所有这些笔记本电脑的攻击技术和工具，你可以关闭系统防止恶意事件的发生。可以创建一个加密的“分区”，它基本上是和正常的磁盘一样的文件。但是我并不特别鼓励这么做。这都要归结于你不信任你的用户每次都会把敏感数据存储在安全的分区上。用户会把资料存储在没有保护的桌面上、邮件应用中以及本地的临时目录下。此外，如何有人可以获得笔记本，并向我之前所描述的那样破解各种 Windows 密码，这些加密的分区使用相同密码的几率你认为有多大呢？以我的经验来看，可能性非常大。

很多人都在笔记本电脑上安装了 LoJack 等笔记本电脑跟踪软件，它可以帮助提供恢复功能。问题是在系统恢复的时候，笔记本上的敏感信息也会受到攻击。很好的解决方案——在安全泄漏时就会有点儿晚了。

真正可以防止信息被攻击的安全解决方案（虽然还不是百分百——没有绝对的）是使用全盘加密技术，例如 PGP Whole Disk Encryption、Voltage Security SecureDisk,和 SecurStar DriveCrypt Plus Pack。他们是独立于系统之外的，他们使用强大的加密技术，有些甚至可以集中管理减少管理员的负担。技术被窃笔记本电脑是开机的，只要整个磁盘是加密的，而且屏幕是锁着的，犯罪分子的唯一选择就是重启系统再次攻入。一旦他这么做了，就会提示他输入密码短语，解锁磁盘。只要加密磁盘的密码短语足够强大，犯罪分子就走到死胡同了。还有，要注意 Windows Vista 中的 BitLocker Drive Encryption，以及 Seagate Momentus 磁盘中的内置加密功能。这些技术也很有前景。

切记这些技术的相关策略——不要只信任用户会作合适的事情——这样可以防止电脑上的敏感信息被攻击。当然，在软件许可证和操作成本上都会产生费用（之前和当中）。

但是这应该相对于丢失信用卡商业权限来说是更好的选择，向政府法规部分解释为什么你被窃的系统没有被保护，或者通知每个信息被攻击的用户。

*（作者：SearchEnterpriseDesktop.com 译者：Tina Guo 来源：TechTarget 中国）*

## 第四步：笔记本电脑安全总结

笔记本电脑的安全风险是现实中的人遇到的现实问题，而且如果你——和你的管理层——采用可正确的方法就可以避免。以下是可以保护你的笔记本电脑和其他被窃的电脑的安全的一些办法：

- 从恶意的角度查看笔记本电脑的漏洞并经常重复。
- 教育你的用户——一次又一次，直到在他们的脑子里生根——而以下这些想法就像“我需要快点买东西——车里的笔记本应该很安全”以及“我要快点儿去卫生间——咖啡店的其它人可以帮我照看东西”都很危险，最后可能给很多人带来麻烦。
- 确保屏幕已经通过 CTRL-ALT-DEL 或者屏保已经锁上了。
- 配置 Windows，在从休眠、待机或者屏保恢复时要求输入密码。
- 最重要的是，使用强大的密码短语进行全盘加密。

你被窃的系统总是可能被售卖，新的软件可能被重装而且不会产生恶意行为。但是，你应该看一下最糟的情况。假设很多信息被存储在不同的位置，而没有全盘加密和合适的密码以及屏幕锁定技术，就没有办法确定所有的资料总是被保护的。这是任何精明的商业人士都不愿意遇到的风险。。

*（作者：SearchEnterpriseDesktop.com 译者：Tina Guo 来源：TechTarget 中国）*