Atitt 密码管理工具 密钥管理系统

目录

[1. 密码 密钥管理工具xlsx记录。。然后加密 1](#_Toc15717)

[1.1. 简单u盘记录存放密钥文件即可。加密最好了。。 1](#_Toc14008)

[1.1.1. 三款密码管理工具lastpass，1password和keepass哪个好... 1](#_Toc21242)

[2. 密码管理器lastpass 1](#_Toc31865)

[2.1. KeePassX 2](#_Toc91)

[2.2. KeePassX 与 LastPass 2](#_Toc16898)

[2.3. 使用1Password： 3](#_Toc27094)

[3. ● 1.2 如何让密码复杂但又不难记 4](#_Toc28148)

[3.1. 浏览器自带的「保存密码」功能 4](#_Toc26879)

[3.2. 免费pwd mng选型KeePass 5](#_Toc13084)

[3.3. Evernote》note(bswd) 6](#_Toc28345)

# 密码 密钥管理工具xlsx记录。。然后加密

Lastpass app

## 简单u盘记录存放密钥文件即可。加密最好了。。

### [三款密码管理工具lastpass，1password和keepass哪个好...](https://www.cnplugins.com/zhuanti/password-manager-compare.html)

[https://www.cnplugins.com › 转体](https://www.cnplugins.com/zhuanti/password-manager-compare.html)

·[翻译此页](https://translate.google.com/translate?hl=en&sl=zh-CN&u=https://www.cnplugins.com/zhuanti/password-manager-compare.html&prev=search&pto=aue)

LastPass的的英文一个优秀的用英语密码管理器状语从句：页面过滤器，采用了强大的加密算法，自动登录/云同步/跨平台/支持多款浏览器的浏览器插件。LastPass的的密码

# 密码管理器lastpass

LastPass主要是一个浏览器扩展，尽管它也具有适用于Windows和Mac OS X的独立应用程序。在上图中，LastPass在脱机类别中标有星号，因为从技术上讲，它是一种在线密码管理系统，但在某些情况下确实可以脱机工作。实际的密码数据库已安全地传输到您的设备并在那里解密（而不是在云中），因此，只要您不通过Web浏览器，Mac应用程序或在移动设备上进行有效的互联网连接，就可以访问该数据库为了获取数据库，已经登录了一次云。

## KeePassX

我终于找到了一个叫做[KeePassX](https://www.keepassx.org/)的免费密码管理器，带有加密工具，可以保护我最重要的个人数据。黑客将不得不跳*了很多*更多关卡，进入我的密码，这是现在比以往更强大，更安全。无论我是在伊斯坦布尔、里约热内卢还是在多伦多的家中，它们也更方便。

KeePassX 是[KeePass](https://keepass.info/)的克隆，我会使用它（它提供更多功能），但它与 Mac 不兼容。另一方面，KeePassX 是一个跨平台程序。你会发现为什么这很重要。

## **KeePassX 与 LastPass**

在选择 KeePassX 之前，我还测试了[LastPass](https://lastpass.com/)，它被许多在线密码管理的市场领导者认为是。它带有更多的花里胡哨，但我出于三个原因决定使用 KeePassX：

LastPass 帐户是免费的，但如果我想将我的密码与我的移动设备同步则不是。为此，我需要高级会员资格，费用为 12 美元/年。便士，我知道，但请继续阅读。以下几点更为重要。

LastPass 是基于云的，并将其客户的密码保存在自己的服务器上，这意味着对公司本身的暴力攻击可能会将我的帐户暴露给黑客（尽管鉴于公司从事在线业务，这种安全漏洞的可能性很小数据保护）。但是，使用 KeePassX，我的密码存储在笔记本电脑的本地数据库中，但我可以选择将其移动、复制或同步到 Google Drive 或 DropBox 等云中，以便从我的 iPhone 访问它。这样，我就不容易受到针对 KeePassX 的安全威胁的攻击。底线是我有一个选择和更多的控制权。如果我确实使用了云，我可以随时从中删除我的数据库。

KeePassX 是一个开源平台，这意味着任何想要质疑或测试其安全性的人都可以检查其代码的完整性。LastPass 不提供这种透明度。相反，它使用专有的加密技术。

尽管如此，LastPass 排在第二位，所以我认为这是一个*不错*的选择。（阅读[本文](https://gizmodo.com/lastpass-vs-keepass-whats-the-best-online-password-m-1452918307)以与 KeePass 进行并排比较。）

## **使用[1Password](https://agilebits.com/onepassword)：**

*“我喜欢 1Password 的旅行，因为它：*

*为我拥有的每个帐户生成一个唯一的密码，我只记得一个来解锁所有帐户。*

*不仅存储密码，还存储各种数据，包括扫描的护照和信用卡。*

*当您进入网站时自动输入您的密码，对于新网站，它会立即创建一个唯一的密码并将其存储。*

*允许在不泄露密码的情况下与他人共享。相反，它会发送一个加密链接。”*

# ● 1.2 如何让密码复杂但又不难记

如此一来，你必然得设计一套自己的密码规则

普遍被大家采用的方法是：**固定密码 + 根据网站来生成额外密码**

Dongtai use nide feoye diaglog zo secry le ..

举个例子，假设阿虚先规定一个固定密码：Axu=666！

建议这个固定密码要包含英文、数字、符号，另外最好是首字母大写，这样能适用于绝大多数网站的密码设置要求

## 浏览器自带的「保存密码」功能

可能部分人觉得浏览器自带的「保存密码」功能就足够了啊

IMG_256

但说实话，单纯用浏览器来记录密码，缺点很多：

1. PC端与手机端用的不是同一个浏览器，那就会很麻烦
2. 不支持对软件、APP自动输入密码
3. 不能记录除了网站以外的密码
4. 无法给密码加上备注
5. ......

用密码管理器除了能解决以上的问题，另外还有个好处是：***你只需要记住密码管理器的一个密码就够了***，其他的密码，全交由密码管理器来记

## 免费pwd mng选型KeePass

付费方案解决起来自然简单，而想必多数人还是更喜欢免费方案的

那在这些工具中，再除掉*免费版有密码数量限制＆设备限制的*，其实就剩下 Bitwarden、KeePass 可以选择了

IMG_256

而本文要推荐的是阿虚一直在用的 KeePass

Keepass 的优点是**开源**，**全平台支持**，**完全免费**，**数据本地加密**，完全不会有那种密码始终是交给别人存放的顾虑，也不用担心别人的服务挂掉

IMG_257

KeePass 还有个最容易被忽略的优势：其加密方式和加密算法，处于密码管理软件的最前沿，至今都没有暴露过任何安全风险（要知道LastPass可是曝出过有严重漏洞的）

但其最大缺点就是工具链比较长，配置略显麻烦，没有详细的教程的话，很多人入不了门

## Evernote》note(bswd)

可以单独选择某个文件夹查询内容，查询密码的。。

很多已经收费了，免费的keepass很难用。。No cloud sync...

So evernote also ok,,bcs already pay money .for that...

Maybe ms auth also a future have bswd mng...