GIBBERFISH 快速入门

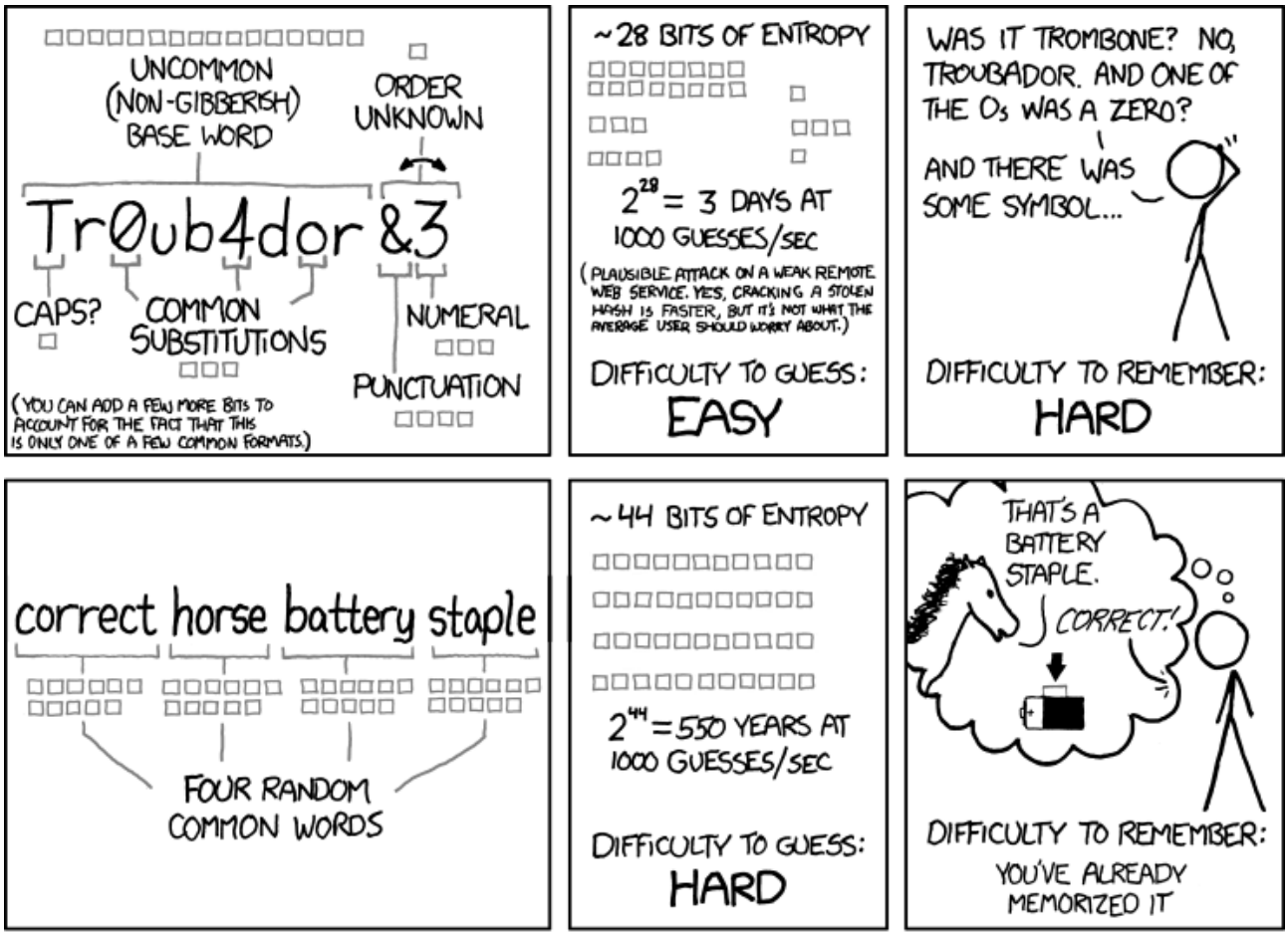
欢迎来到 Gibberfish 我们的重点是你的隐私和安全 但我们需要你是一个平等的参与者。下面是几个建议让你开始。

配置 文件

如果这是你第一次登录 你应该花几分钟填写你的个人资料 而你在那里改变你的密码点击右上角 ⚙ 选择个人编辑你的档案文件。

密码

好的密码对于维护您的数据非常重要。我们 和许多安全专家 建议使用 Diceware 方法创建密码。这是我们认为安全的唯一的密码生成方法。它很容易做 它提供了超强的密码 甚至可以击败最足智多谋的对手。



/Image courtesy xkcd.com.

虽然上面的漫画解释的概念 Diceware 方法建议一个密码长度为 5 或更多的词 以获得最佳的安全性。

不要使用您在其他任何地方使用的 Gibberfish 登录的密码。

始终为任何服务帐户或设备生成唯一的密码。

双因素身份验证

一旦您更改了密码 我们还强烈鼓励您启用双因素身份验证 2FA。这包括在您的移动设备上安装一个应用程序 它生成了每次登录时必须输入的唯一的 6 位代码。如果有人破解了你的帐号 他们需要知道你的密码并在物理上拥有你的手机。这种组合使您更安全。因为 Gibberfish 是 Nextcloud 生态系统的一部分 所以您可以使用 Nextcloud 2FA 应用程序。这个应用程序支持 FreeOTP 它可以下载在 app 商店的 Android 和 iOS 设备。

钥匙金库

如果您还没有这样做的习惯 那么将您的密码存储在像 KeePass 这样的密钥库中是个好主意。密钥库使您可以轻松地记住所有密码。您将需要使用 Diceware 生成的密码锁来锁定密钥库本身。此外 我们强烈建议您在存储密钥存储库的设备上启用全磁盘加密。

使用此方法可以确保只需要记住一个密码 打开密钥存储库的口令。

数字卫生

良好的数字卫生是一贯使用稳健的安全做法。

通过 强健 我们指的是由受信任的安全专家建立或审核的程序。这些包括但不限于电子前沿基金会卫报项目和 Tor 项目。

我们使用 一致 来强调 任何安全实践的间歇性使用都与不使用一个操作一样糟糕。一旦你制定了一个威胁模型和一个战胜它的策略 你必须在每次从事私人活动时都应用该策略。

威胁

了解您和您的团队将遇到的威胁是建立有用的安全策略的重要步骤。目标是只使用必要的技术来抵御可能的对手。这将防止您的安全机制变得如此繁重 以至于您不再使用它。您的管理员可能已经创建了一个威胁模型 描述您和您的组可能期望的安全挑战。如果您不确定 请与他们联系并询问。

每个用户都必须了解您的组的威胁模型 并始终使用相同的安全做法。

有关威胁模型的详细信息, 请参阅本文所生产的这一优秀底漆。

现有通信

您可能正在将 Gibberfish 添加到与联机活动关联的各种现有帐户和服务中。这些旧帐和服务可能已被泄露。我们建议对涉及您的 Gibberfish 服务器的任何活动存储在那里的内容或与其相关的活动使用新帐户。

我们认识到 这并不总是方便或适合每个用户。在这种情况下 请花时间重新保护您打算用于私人活动的任何帐户或服务。更改您的密码以锁定未授权的用户 他们可能在没有您的知识的情况下获得了访问权限。只要可能 启用双因素授权。检查所有设备 包括电话 的软件更新并安装它们。

TOR

使用 Tor 是保护您的在线隐私的唯一最佳方式。这就是为什么我们使用 Tor 部署您的 Gibberfish 服务器。虽然它具体地提到了洋葱路由器项目 Tor 已经包括了各种各样的免费产品和服务 人们可以用来维护他们的在线活动。我们建议每个人都使用 Tor 浏览器来帮助匿名他们的在线存在

请仔细阅读 Tor 提供的关于在他们的网络上浏览的文档和常见问题。他们对维护你的隐私有重要的建议。重要的是 使用 Tor 浏览器并不保证所有的在线活动都是匿名的。

由于您的安全需要升级 Tor 有其他的免费工具来帮助。评估威胁模型时 您可能希望调查桥头服务器和尾部。桥式服务器允许人们在阻止它的国家访问 Tor。尾部是一个 Linux 操作系统 用通用的程序完成 所有的 USB 棒。它允许极私人计算。

在下列情况下发现这些和其他 Tor 服务
https://www.torproject.org/projects/projects.html.en

视频呼叫

Nextcloud "聊天" 应用程序允许您在 web 浏览器中创建和加入视频呼叫。为了在移动设备上获得最佳性能, 我们建议您安装并使用 "Nextcloud 聊天" 移动应用程序, 它可从 iTunes、Google 播放和 F 机器人中获得。

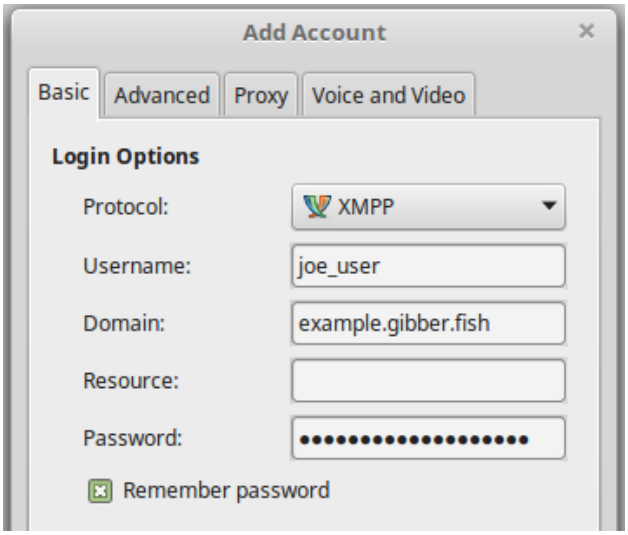
聊天

聊天系统使用标准的 XMPP 协议 它不仅允许您与其他 Gibberfish 用户聊天 还可以与使用 XMPP 服务器的世界上的任何人进行交谈。您的 XMPP 地址为 <your username>@<your gibberfish server>。例如

joe_user@example.gibber.fish

首次登录时 屏幕右侧的聊天名册将为空。从底部的菜单中 您可以添加联系人。只需开始键入 它将自动搜索服务器上的现有用户 也可以键入外部用户的 XMPP 地址。

要在未登录到 Gibberfish 时保持连接 您还可以使用与 XMPP 兼容的客户端 如 Adium 洋泾浜或许多移动应用程序之一 直接连接到服务器。



聊天服务器也可作为端口 5222 上的 Tor 洋葱服务 访问。向管理员询问服务器的 Tor 地址。

但是 在与服务器以外的用户聊天时 除非您和您的联系人使用端到端的加密插件 如 工程机械 否则您无法保证隐私。大多数聊天客户端都支持端对端加密 并具有帮助您理解和启用它的指南。

台式机和移动客户端

Gibberfish 与 Nextcloud 桌面和移动客户端一起工作 允许您自动将文件与服务器同步。默认情况下 此选项被禁用为安全措施。如果希望使用这些客户端 请与管理员联系以更改文件访问规则。如果您决定在本地同步文件 则只有在打开设备的全磁盘加密时才这样做。如果您的设备丢失被盗或被黑客攻击 这将保护您的文件

这是困难的 但可能的 你的数据被截获的资源 而在过境的敌人。因此 我们不建议在不仔细考虑您的威胁模型和安全做法的情况下同步数据。

进一步阅读

有关核心功能的更广泛文档, 请参阅 Nextcloud 用户手册, 它也位于您的 Gibberfish 主文件夹中

https://docs.nextcloud.com/server/13/user_manual/

管理员也应该熟悉管理手册。

https://docs.nextcloud.com/server/13/admin_manual/

最后 我们建议订阅新闻应用程序中的 Gibberfish 博客 以保持最新的重要公告和我们的金丝雀声明。

最后说明

我们希望你喜欢使用 Gibberfish。我们努力使它成为一个安全和易于使用的平台 以及许多独立的贡献者我们已经集成到我们的服务的各种开源项目。特别感谢 Nextcloud 的乡亲们 没有他们我们的平台是不可能的。

我们依靠捐赠来生存。如果你能负担得起 请考虑作出任何金额在 https://gibberfish.org/zh-CN/donate 慈善捐款。我们将不胜感激。谢谢!

出于安全原因 我们只响应您的注册管理员的请求。如果您有与服务相关的问题 请询问您的管理员。