**github-security-checklist**

GitHub个人和组织帐户的重要安全检查列表。列出被认为是**必填**的项目，**粗体显示**。清单上被认为推荐的项目是斜体的。

## 个人设置

* **设置强密码**：设置密码管理器生成的强随机密码。一个不错的基准是20个混合大小写字母和数字。  
  个人设置→账号→[更改密码](https://github.com/settings/admin)
* **启用2FA**：打开2FA。2FA最强形态是基于硬件的U2F安全密钥。  
  个人设置→安全→[双重认证](https://github.com/settings/two_factor_authentication/configure)
* **备份您的2FA恢复代码**：您应该将恢复代码放在安全的地方，否则您可能会永久锁定在GitHub帐户之外。  
  个人设置→安全→[双重认证](https://github.com/settings/two_factor_authentication/configure)
* **启用漏洞警报**  
  个人设置→通知→[漏洞警报](https://github.com/settings/notifications)（检查“电子邮件”和“网络”）
* **定期审核SSH密钥**：SSH密钥是GitHub帐户用户名/密码身份验证的替代品。临时访问您的帐户的攻击者可以将SSH密钥作为后门添加到您的帐户中。您应该至少每月查看帐户上的密钥列表，并查看上次使用它们的时间。撤销任何不经常使用的东西。  
  个人设置→[SSH和GPG键](https://github.com/settings/keys)
* **安全存储您的SSH密钥**：您只应将与GitHub相关的SSH密钥存储在您认为相当安全的计算机上。避免将 SSH 密钥用于 GitHub 身份验证和其他目的。每个SSH密钥都应该用一个强密码来保护。您应该定期查看帐户上列出的SSH密钥，如果它们不经常使用，请将其吊销。攻击者泄露了您列出的SSH密钥之一，可以访问您的GitHub帐户，而无需进一步的身份验证秘密。  
  个人设置→[SSH和GPG键](https://github.com/settings/keys)
* **添加专用的GPG密钥用于签名提交**：所有用户都应该有一个GPG密钥来加密签名提交。密钥应该安全地存储。  
    
  参考文献：  
  [向GitHub帐户添加新密钥](https://help.github.com/articles/adding-a-new-gpg-key-to-your-github-account/)  
  [高级指南](https://github.com/lfit/itpol/blob/master/protecting-code-integrity.md)  
    
  个人设置→[SSH和GPG键](https://github.com/settings/keys)
* **不要设置回退短信号码**：大多数短信提供商容易受到号码移植攻击。  
  个人设置→安全→[双重认证](https://github.com/settings/two_factor_authentication/configure)
* **仅安装您信任的OAuth应用程序**：仅安装您信任的OAuth应用程序，所需时间最短。删除不再使用的应用程序。您应该查看他们的权限，以确保它们是否合适；OAuth应用程序可以读取或写入帐户数据，包括提交状态、部署、要点、网络钩子、通知等。[此处](https://help.github.com/articles/authorizing-oauth-apps/)提供了可以访问的数据类型的完整列表。Rogue应用程序可以过滤不适当的数据并修改帐户数据。注意：许多应用程序只需要识别您的GitHub帐户，因此只需要只读访问您的电子邮件地址。[更多文档](https://developer.github.com/apps/differences-between-apps/)  
  个人设置→应用程序→[授权OAuth应用程序](https://github.com/settings/applications)
* 使用安全的电子邮件提供商为其主要电子邮件地址：您的主要电子邮件地址可以是帐户恢复/重置过程的一部分，因此此地址是安全的。GMail和ProtonMail等电子邮件提供商提供具有2FA选项的安全服务。为GMail设置增强保护的个人帐户是最好的；考虑为此专用目的创建一个GMail帐户，例如[myname-github@gmail.com](mailto:myname-github@gmail.com)  
  个人设置→[电子邮件](https://github.com/settings/emails)
* 电子邮件地址保密：建议您设置所有电子邮件地址，以更好地防止社会工程。  
  个人设置→[电子邮件](https://github.com/settings/emails)
* 允许通过命令行公开电子邮件：虽然最好避免通过命令行命令公开您的电子邮件，以更好地抵御社会工程，但如果没有允许，您将无法发布公共回购协议的更改。  
  个人设置→[电子邮件](https://github.com/settings/emails)

## 组织设置

* **组织管理员必须限制第三方应用程序的访问**：如果没有此设置，所有由组织成员授权的应用程序都可以访问组织的数据，这可能会允许流氓应用程序访问组织数据，如私人回购协议。  
  组织设置→第三方应用访问
* **组织管理员必须要求成员使用2FA**  
  组织设置→安全性→双重认证
* **将会员资格限制在最低特权**内：组织成员资格由团队组织。项目团队成员获得所需的特定存储库的最低特权。在可能的情况下，应限制对存储库的写入访问权限。  
  人员/团队设置
* **组织管理员必须删除不需要的用户**：管理员应定期审核会员列表，以确保权限合适，并删除不需要的会员。及时撤销对组织的访问应成为组织贡献者退出流程的一部分。  
  人员/团队设置
* 组织管理员应限制默认成员特权：管理员可以设置成员特权以创建、删除、分叉和修改组织存储库；这些特权应仅限于管理员。用户的默认存储库权限应设置为“无”。  
  组织设置→成员权限
* 组织管理员应审核网络钩子：管理员应查看组织网络钩子列表，以寻找可疑的过滤迹象。  
  组织设置→网络钩子
* 来源：https://github.com/kristovatlas/github-security-checklist