

众所周知，虚拟货币交易的风险很高，其中不仅包括变幻无常的市场行情，诈骗钓鱼现象频出也让投资者们苦不堪言。为了预防这种情况，类似于Bitget、欧意交易所这样的知名交易平台都发布了相应的防钓鱼指南，今天我们就来一起了解一下！



## Bitget防护手册：破解网络钓鱼欺诈

最近，欺诈性 Bitget 网站和应用程序激增，这凸显了提高警惕的必要性。作为 Bitget 社区的一份子，请用这些防护策略武装自己。

1. 面对日益复杂的诈骗手段，在处理突如其来的信息，尤其是要求提供个人或财务信息的通信内容时，一定要谨慎行事。请注意，Bitget 工作人员绝不会询问此类细节。

2. 请务必仔细检查网址，并只信任 Bitget 官方域名：[www.bitget.com](http://www.bitget.com)。

确保应用程序是从 Google Play、苹果商店或我们的官方平台进行下载。访问 Bitget 下载指南获取更多信息。

您也可以通过访问我们的 Bitget 官方验证页面查看邮箱、网站地址或是社交媒体账户是否为官方内容。

3. 警惕下载未知附件，避免在陌生网站上输入个人信息。

4. 在“安全设置”部分设置 Bitget 防钓鱼码。一旦您设置了代码，所有 Bitget 官方邮件中都会包含该代码，以帮助您验证其真实性。

Bitget 应用程序教程：在主页上点击“个人资料”图标，选择“安全设置”，然后前往“防钓鱼码”部分设置代码。

Bitget 网站教程：在 Bitget 主页，选择人形图标下的“安全中心”，在“防钓鱼码”板块设置您的代码。



已经上当受骗了？行动要快！

- 立即行动：在 [www.bitget.com](http://www.bitget.com) 注册新账户，然后立即通过 [support@bitget.com](mailto:support@bitget.com) 联系我们。

- 保护您的资产：尽快将资产从受损账户转移到新账户。
- 切断联系：停止使用被入侵的账户，并尽快删除钓鱼应用程序。

请始终牢记，加密社区的发展离不开集体的警惕。如果有些东西看起来不对劲，那可能真的不太对劲！掌握信息，确保安全！

在与网络威胁的斗争中，Bitget 会始终为社区提供支持。察觉到可疑的内容或阴谋？赶快通过 [support@bitget.com](mailto:support@bitget.com) 与我们联系。让我们一起加固 Bitget 生态系统，保护我们的资产。

看完Bitget上的这些防钓鱼指南之后，大家是不是学到了很多，其实其中有些方法同样适用于欧意交易所这些平台，希望大家可以牢记！