

## 账户安全说明

为确保您的交易账户安全，请仔细阅读以下说明，并按照建议操作。

### 1. RedstoneFx 账户安全系统

#### a. 用户名

您登录RedstoneFx的用户名是您注册时使用的手机号码或电子邮箱。请妥善保管您的手机号/邮箱，避免未经授权的访问!

#### b. 标准安全系统-密码登录

当您登录RedstoneFx交易账户时，您需要输入您设置的用户名和密码。请确保您的密码不泄露，以确保您账户资金的安全。

#### c. 额外的安全系统

1) 在注册过程中，您可以选择以下额外的帐户安全类型：电子邮件。

在进行资金操作或更改帐户设置时，我们会发送电子邮件到您在注册过程中提供的电子邮件地址。此电子邮件包含一个独特的代码，以确认所需的交易。在网站的相应栏目输入代码后，交易被确认并执行。

电子邮件的交易确认是一种较低级别的安全保护。如果黑客控制了你的电子邮件账户，他可以进入你的私人区域或将资金转移到其他账户。使用此安全类型时要小心。

如果您收到含有代码的电子邮件，但您没有在个人区域内进行任何操作，请立即删除此电子邮件并报告给技术支持人员。不要向任何人提供机密确认码。

2) 在注册过程中，您可以选择以下额外的账户安全类型：短信。

当您进行资金操作或更改账户设置时，我们将发送短信至您在注册过程中提供的手机号码。此短消息包含确认所需事务的惟一代码。在网站相应栏目输入代码后，交易被确认并执行。

如果您不能访问您的SIM卡，您将无法更改安全类型。

---

## 2. 关于保护电子邮箱的建议

- a. 建议您使用双重身份验证的电子邮件服务。
- b. 建议删除您的电子邮件帐户安全设置中的安全问题或使用随机字符作为答案。安全提示:回答安全问题是入侵电子邮件账户最常见的方法。
- c. 使用安全密码登录你的电子邮件帐户。您的密码不应包含完整的单词, 密码长度应大于10个字符, 应包含数字和大写字母。
- d. 如果您通过网络接口访问相关服务, 请在您的电子邮件帐户设置中禁用SMTP、POP3和IMAP协议。这可以保护您的电子邮件帐户免受恶意攻击。
- e. 不要点击来自陌生人或组织的可疑链接! 如果收到含有链接的邮件, 点击链接后不要输入任何密码。

## 3. 帐户安全保护建议

- a. 不要向第三方泄露登录个人区域的密码, 以避免黑客获取密码。

我们的技术支持人员无法访问您的个人专区, 也没有权利要求您输入密码登录您的个人专区。公司员工只能要求你输入电话密码, 以确认你的身份。为了使第三方能够访问一个特定的帐户(例如, 投资者), 使用该投资者的帐户密码。此密码不允许您更改帐户设置, 也不允许您以自己的名义进行交易或转账。

- b. 不要泄露短信接收到的密码。

我们强烈建议使用一个单独的文件存储在专用的外部媒体(USB闪存盘, CD等)在一个安全的地方, 以保存登录到您的个人区域的密码, 并从您的计算机删除它。

## 4. 如何联络我们

如果您怀疑被欺骗, 请立即通过在线咨询(在线聊天)或电子邮件 [support@redstonefx.com](mailto:support@redstonefx.com) 联系技术支持人员。

根据我们的客户协议, 客户和公司之间可以通过以下方式进行沟通:

- 
- 电子邮件(带有@redstonefx.com域名, 如support@redstone.com)
  - MT4交易平台内部邮件系统
  - 相关电话号码可在公司网站的“联系我们”部分找到
  - 邮件
  - 在线客服

RedstoneFx官方通讯不使用以下方式:ICQ, Yahoo Messenger, Skype等。任何以support@redstonefx.com以外的域名发送的电子邮件都不是我们的正式通信, 即使电子邮件地址包含“Redstone”一词。这些电子邮件地址提供的信息与我们无关。

亲爱的客户, 希望以上建议对您有所帮助。RedstoneFx公司会尽一切可能确保您资金的安全。如果您未能遵守这些安全要求, 您应意识到您将对您的RedstoneFx账户中的资金安全负全部责任。