交易和账户安全

账户安全对我方很重要，我方已采取了几个措施来保护与贵方 Remitly 账户有关的信息。贵方也可以做一些能保护贵方账户和个人信息的事情。

账户核实流程

贵方的 Remitly 账户需经过核实程序，以保持高水平的安全、信任和保护。

如果贵方是 Remitly 的新客户，且用 Remitly 网站创建 Remitly 新账户，则贵方必须提供某些个人信息并完成电子邮件核实过程。

一旦贵方账户启动并运行，我方将部署各种可使我方能够突出可疑账户活动的手动和自动风险管理程序。其目的是找出任何看似不寻常或与贵方过去使用情况不一致的特性。作为该过程的一部分，我方与行业领先的服务提供商签订合同，以核实个人和财务信息。这些服务永远不会直接联系贵方，也不会把贵方的信息用于成功完成贵方指定交易以外的任何用途。

密码安全

当贵方登录账户时，我方会做一些事来保护贵方账户。首先，贵方无论何时登录 Remitly 账户，都要用安全服务器连接 (https://) 登录。我方使用具有 256 位加密的安全套接层 (SSL)，这是安全服务器保护的行业标准。

贵方账户还受贵方创建的唯一密码保护。贵方不应该用常用词或短语作为密码。相反，贵方的密码应该至少包含八个字符，包括数字和大小写字母。贵方应该对该密码保密。共享密码将降低贵方 Remitly 账户的安全性。

警惕网络诈骗

- 切勿为了领取彩票或中奖奖金，或相信能得到一大笔钱的承诺而付款。
- 切勿因为贵方有信用卡或贷款“担保”而付款。
- 切勿回复贵方不确定是否真实的网络或电话邀请。

- 切勿向贵方不认识的人和贵方无法核实身份的人付款。

如有疑问，可向指定收款人索取有关所要款项之用途及安全性的详细信息。在贵方成功交易之前切勿汇款。

识别钓鱼或假冒电子邮件

有时，贵方可能会收到看似是 Remitly 发来、但实际上不是的电子邮件。此类电子邮件可能会将贵方引向一个看似是 Remitly 网站的网站。该网站甚至可能要求贵方提供账户信息，如贵方的电子邮箱和密码。

这些虚假网站会窃取贵方账户和支付的敏感信息，以实施诈骗。这些虚假电子邮件可能包含能检测密码或敏感数据的潜在病毒或恶意软件。因此，我方建议贵方安装反病毒程序，并随时更新。

以下是防范欺诈性电子邮件的一些要点，谨记：

- 贵方的完整社会保障号码或出生日期
- 贵方的信用卡号、PIN 或信用卡安全代码（包括上述任何一项的“最新信息”）

我方建议贵方切勿打开任何可疑或未知来源的电子邮件附件。电子邮件附件可能包含病毒，当贵方打开附件时，会感染贵方的计算机。如果贵方收到据称发自于 Remitly 并包含附件的可疑电子邮件，我方建议贵方删除电子邮件，且切勿打开附件。

寻找糟糕的语法或排版错误。一些钓鱼电子邮件翻译自其他语言，或者在发送时未经过校对，导致有语法或排版错误。

是来自 Remitly 的邮件吗？虽然钓鱼者会发送伪造的电子邮件，使其看起来就像来自于 Remitly 的一样，但有时贵方可以通过检查返回地址来确定其真实性。如果电子邮件的“发件人”看起来像 "remitly-security@hotmail.com” 或 "remitly-fraud@msn.com”，或者包含另一家互联网服务提供商的名称，则贵方可以确定它不是真的。

真正的 Remitly 网站总是托管在以下域：https://www.remitly.com/

有时，假冒邮件中包含的链接看起来就像真正的 Remitly 地址。贵方可以通过将鼠标悬停在链接上来检查它实际指向的位置--它实际指向的网站将显示在浏览器窗口底部的状态栏中，或者作为弹出窗口显示。

我方永远不会使用在以上所列域之外的域托管的网址。例如，"https://security-payments-remitly.com/. . ." 等变体域，或后面带有 "https://123.456.789.123/remitly.com/. . ." 等目录的 IP 地址（数字串）都不是有效的 Remitly 网站。

此外，有时假冒邮件会设定成：只要贵方点击文本上的任意处，就会被带往欺诈网站。Remitly 永远不会发送此类电子邮件。如果贵方不小心点击了此类电子邮件，并进入了假冒网站，切勿输入任何信息；相反，只需关闭浏览器窗口。

如有疑问，切勿点击电子邮件中的链接。直接前往 https://www.remitly.com/，并在右上角的菜单中点击 **Your Account**（您的账户），查看最近的购买记录，或者检查贵方的账户信息。如果贵方无法访问账户，或者看到任何可疑之处，请立即告知我方。

如果贵方确实从假冒或可疑电子邮件中点击了链接，并输入了贵方的 Remitly 账户信息，贵方应**立即**更新密码。贵方可通过直接前往 https://www.remitly.com/ 并点击 **Account Settings**（账户设置）来更新密码。在下一页，点击 **Change your personal information, e-mail address, or password**（更改您的个人信息、电子邮箱或密码）。

如果贵方将信用卡号提交到了从假冒电子邮件链接到的网站，我方建议贵方采取措施保护贵方的信息。例如，贵方可以想到联系信用卡公司，以将此事告知他们。最后，贵方应从 Remitly 账户中删除那张信用卡，以防止任何人不适当地重新访问贵方的账户。

如果贵方收到已知是假冒电子邮件，或者如果贵方认为自己是钓鱼攻击的受害者，并且担心贵方的 Remitly 账户，请立即通过举报[钓鱼或假冒邮件](/home/contact/)来告知我方。