

防范伪造网站及诈骗电邮

- 本公司官方网站是 www.bocomgroup.com，请留意浏览器地址栏并提防钓鱼网站。
- 经常检查电子邮件，如收到异常的交易确认电子邮件，请立即向本公司举报。
- 请勿开启来历不明的电子邮件附件或网站链接，以防计算机被入侵盗取数据或落入诈骗陷阱。

保障个人资料的安全

- 阁下应妥善保管各项个人资料，包括身份证明文件、个人密码及其他个人资料，以免被騙徒盗取后冒充阁下身份进行诈骗。
- 若有人通过任何途径向阁下索取个人资料，包括经电话、手机短信、电子邮件等，请提高警觉。
- 在收到日结单后应立即查阅，如发现有任何异常的交易，请立即向本公司举报。

移动设备及个人计算机安全使用

- 经常保持阁下计算机安装最新的操作系统安全更新，建议安装防毒、防间谍及防火墙软件，并定期更新有关软件的版本。阁下可向计算机或软件供货商选取合适的个人防毒、防间谍及防火墙软件。
- 小心保管阁下用作登录本公司网站或手机应用程序的移动设备。
- 使用本公司网上及手机应用程序服务后，请紧记按「注销」键离开。当系统显示确认注销后，关闭浏览器。请勿使用其它方法离开系统。
- 经常保持阁下移动设备升级至最新的操作系统版本及经常进行安全更新。
- 请使用本公司官方网站 (www.bocomgroup.com) 下载交易软件。

安全密码管理

- 建议定期更改阁下的个人密码，如 30 天更改一次。
- 建议阁下选用大、小写的英文字母及数字的组合为个人密码。切勿使用容

易被猜到的密码，例如您的电话号码、出生日期、身份证号码等。

- 请勿向任何人透露或写下您的私人密码。
- 本公司不会以电话或电子邮件向阁下索取密码。

无线网络安全

- 请勿使用公众或共享计算机登录网上服务。
- 当使用公众 Wi-Fi 无线上网时，请小心选用无线网络，以免接入恶意无线网络。
- 请使用 WPA2 或进阶的加密技术来保护阁下的无线网络。
- 请勿使用已被破解（例如 root、越狱）的移动设备登录网站服务。

** 如英文版与中文版有任何不一致或不明确之处，以中文版本为准。