

对客户防范仿冒诈骗攻击的建议

一) 防范措施

1. 不要连接滥发电邮等不可信赖来源或电邮所载的 URL 连结或二维码 (QR Code)，以免被看似合法的恶意连结转往恶意网站。
2. 不要登入可疑网站，或连接这类网站提供的连结或二维码 (QR Code)。
3. 不要从搜寻器的结果连接到本公司的网址，应以人手打入 URL 位址或进入之前已加入书签的连结。
4. 开启电邮附件时要提高警觉，常常检查附件的伸展部分，不要打开伸展部分是 ".pif", ".exe", ".bat", ".vbs" 的附件。
5. 避免在设于咖啡室或图书馆等场所的公用终端机或不稳妥终端机，进行网上户口查询或进行交易。
6. 在完成交易后，切记要打印或备存交易记录或确认通知，以供日后查核。
7. 提供敏感的个人或帐户资料时应时刻保持警惕。本公司不会主动以电邮、短讯、电话或语音讯息来电的方式要求客户提供完整的个人或帐户资料、信用卡号码、登入密码及一次性密码。如有疑问，应向本公司查询。
8. 确保电脑採用最新的保安修补程式和病毒识别码，以减低欺诈电邮或网站利用软件漏洞的机会。
9. 确保你的流动装置的应用程式、作业系统和防病毒软件为最新版本。

二) 侦察措施

1. 收到本公司發出的交易成单或月结单后请立即细察，以确定是否有未经授权的交易或帐户活动。
2. 定期登入网上户口，检查帐户状况及上次登入日期，以确定是否有任何可疑活动。

三) 回应措施

1. 如果怀疑已被诈骗（例如你已对仿冒诈骗电邮作出回应或向欺诈网站提供个人或财务资料），应立即更换密码。经查核帐户状况后，立即联络本公司或向警方网络安全及科技罪案调查科报案。
2. 把仿冒诈骗电邮传送给本公司或警方网络安全及科技罪案调查科，以便进行调查。

投诉主任联络方法:

电话: +852 25968230

电邮地址: compliance@chaosinternational.com

通讯地址: 中环花园道 3 号中国工商银行大厦 11 楼 1108-11 室