客户通知 – 小心电子网络诈骗

近日香港的电子网络骗案有上升趋势，东亚证券有限公司（「东亚证券」或「本公司」）谨此提醒客户，在收到任何声称代表东亚证券发出的电邮和任何即时电子讯息时（如手机短讯、WhatsApp、微信等），请时刻保持警觉。另外，亦请客户留意以下的提示，慎防受骗:

- 东亚证券不会透过电邮或即时电子讯息，要求客户透露香港身份证号码、账户号码、登入密码、或一次性密码等任何敏感资料。

- 请小心提防任何声称代表本公司，但发出自非正式的渠道，例如一些与本公司官方电邮地址相似的电邮地址。

- 东亚证券不会要求客户跟从或按下任何超连结以进行交易。

若客户对任何收到的信息有怀疑，请立即致电本公司客户服务热线 (星期一至五早上 9 时至下午 5 时（852）3608 8021) 或亲临香港德辅道中 10 号东亚银行大厦 9 楼与我们联络。另外，您亦可以联络香港警务处反诈骗协调中心（Anti-Deception Coordination Centre）：（852）18222，咨询有关反诈骗事宜。

关于更多保安提示，请阅读以下资讯。

保安提示

为确保您的交易及个人资料安全，建议您先阅读以下资讯。

1. 保安提示要点
2. 使用东亚证券电子网络股票买卖服务系统（包括互联网及手机应用程式）
3. 使用自动化电话服务
4. 双重认证
5. 防止诈骗资讯
6. 更多保安资讯

1. 保安提示要点

- 切勿向其他人透露您的东亚证券电子网络股票买卖服务系统（包括互联网及手机应用程式）的使用者号码、密码或一次性密码。
- 切勿打开可疑的电子邮件附件，或点击附于任何电子邮件、短讯、即时通讯讯息、社交媒体平台、二维码、搜索引擎或不可靠来源内的超连结并进入网页及输入敏感资料 – 特别是您的登入资料。如需使用网上服务，应直接于浏览器输入 www.easecurities.com.hk 网址、把网址设为书签或使用东亚证券电子网络股票买卖服务 - 手机应用程式。
- 如您遇到可疑来电、网购卖家、交友邀请、招聘广告、投资网站等，建议您在进行交易前可点击「防骗视伏器」https://cyberdefender.hk/zh-cn/查询相关平台账户名称、收款账户、电话号码、电邮地址、网址等，以评估诈骗及网络安全风险。
- 慎防网络钓鱼诈骗（例如假冒来自政府或金融机构为主题的网络钓鱼诈骗等）、骇客、病毒、间谍软件及其他恶意程式入侵。
- 及时留意本公司发出的短讯/电邮交易提示，并定期透过东亚证券电子网络股票买卖服务系统(包括互联网及手机应用程式）查阅账户交易及结单。若发现可疑情况，应立即通知本公司。
- 使用官方软件并确保您装置上的作业系统及应用程式已装有最新的安全更新，不时更新防毒软件和防间谍软件并定期扫瞄您的装置。
- 请设定一个难以猜破的密码，密码要求为至少八个字元，避免使用容易让人取得的个人资料，如电话号码或出生日期作为密码。该密码应与其他网上服务之密码不同，并定期更改密码。
- 切勿在不同网上或社交媒体的账户使用相同的密码。如您怀疑有人得知您的密码，建议您立即更改密码，如需要可联系本公司寻求帮助。

2. 使用东亚证券电子网络股票买卖服务系统（包括互联网及手机应用程式）

- 登入时需先留意四周环境，切勿让他人得知输入的资料和使用后正确地登出。
- 为确保交易安全，请透过官方应用商店(如: Google Play 或 App Store 应用程式市场)，并切勿在任何已被「越狱破解」或「超级用户权限破解」的装置使用。
- 首次使用网上服务时应立即更改您的密码，然后销毁载有密码之文件。
- 每次登入本公司电子网络股票买卖服务系统（包括互联网及手机应用程式）时，请留意上次登入的日期及时间或「确认讯息」。
- 如您于本公司登记的流动电话号码及/或电邮地址已更改或已失效，请即到本公司、东亚银行任何一间分行或登入东亚证券电子网络股票买卖服务系统 - 互联网更新个人资料。
- 为防止他人未经授权使用，本公司建议您为您的装置设立自动上锁、启用密码锁及启动远端清除等功能。当您的装置有遗失/被盗的情况，建议您登入东亚证券电子网络股票买卖服务系统（包括互联网及手机应用程式）更改您的东亚证券电子网络股票买卖服务系统密码（包括互联网及手机应用程式），并停用您的 i-Token (如适用) 。
- 当发现或怀疑您的账户被他人未经授权使用时，请立即通知本公司。
- 请妥善保管用以登入东亚证券电子网络股票买卖服务系统的电脑及手机。如您的装置能使用生物认证（如指纹或面容辨识），切勿停用任何有助提升生物认证安全性的功能，并不要让任何人在您的装置上登记其生物信息。

- 如您有多胞胎或面容相像的兄弟姊妹，或正处于面部特征可能快速发展的青春期，请不要使用面部辨识作认证。
- 切勿透过公共电脑或公共/不知名无线网络登入网上服务。当使用Wi-Fi登入网上服务时，应选用加密的网络，并移除不必要的 Wi-Fi 连线设定。如无须使用请关闭 Wi-Fi、蓝芽、NFC 等无线网络功能。
- 避免透过免费或不可靠的虚拟专用网络(VPN)使用网上服务。如果需要使用远程控制技术来使用网上服务，请利用没有已知漏洞的可靠软件。
- 细阅网站、应用程式和其他软件及程式的安装及/或许可请求。切勿于您的装置上安装或运行来自第三方/来历不明的应用程式，必要时移除任何可疑应用程式。
- 定期检查并更新您的系统浏览器及东亚证券的官方流动应用程式。
- 当使用公共 USB 充电站充电手机或设备时，需留意情况以避免感染恶意软件。
- 请勿在可疑网站或应用程式提交文件（例如身份证扫描档案，银行账单和信件）。

3. 使用自动化电话服务

- 为防止欺诈行为，请将自动化电话服务密码保密。
- 切勿将自动化电话服务密码告知他人(包括本公司职员或警方)。
- 切勿让他人使用您的自动化电话服务密码进行查询/交易。
- 定期更改您的自动化电话服务密码以确保安全。

4. 双重认证

- 为提升网上交易安全，本公司已为相关电子渠道提供双重认证服务。登入时，您需要使用 i-Token[*]或输入本公司发出的一次性短讯交易密码[#]。
- 请妥善保管您的双重认证工具。切勿让您的安全设备（包括已启动 i-Token 或接收一次性短讯交易密码的手机）处于无人看管状态，或让其他人使用或控制该设备。
- 切勿向任何人透露发送至您手机的一次性密码。
- 切勿在任何已被「越狱破解」或「超级用户权限破解」的装置安装使用 i-Token。

[*]客户必须于本公司登记流动电话号码及电邮地址后，才可登记及使用 i-Token。

[#] 即使您已启动香港流动电话服务商提供的「短讯转驳」服务，本公司所发出载有一次性短讯交易密码的流动短讯亦不会被转送至其他电话号码。

5. 防止诈骗资讯

- 若您对任何推广东亚证券产品或服务之代表的身份有怀疑，应立即透过官方渠道致电本公司与职员核实来源。
- 若您早前在开立户口时提供给本公司的身份证明文件已遗失及/或随后已更换，或您怀疑您的个人资料、结单或账户资料可能已被泄露或盗取，应立即通知本公司。
- 慎防伪冒短讯及语音讯息来电。如您对来电者有怀疑，应立即透过官方渠道致电本公司与职员核实。
- 慎防有骗徒伪冒为东亚证券的职员行骗。慎防未经授权股票交易。如发现您的账户有任何可疑或未经授权的交易，应立即透过官方渠道致电本公司与职员查询。
- 回应电邮要求前请先经其他渠道核实电邮发放者身份，提防受骗。
- 慎防一些潜在网络钓鱼攻击的讯号，例如可疑的发件人地址、标题以"警告" 或 "FYI"为题和内容要求您输入个人资料或按下可疑连结、使用通用称呼、用威胁或紧迫性的文字、要求提供敏感资料或指示您打开附件而内容包含不清晰的拼写/语法等，请通过另一 / 官方渠道验证发件人的身份或立即将其删除。
- 在输入一次性短讯交易密码之前，请确定网站是可信任的。
- 采取预防措施以保护您用以进入东亚证券电子网络股票买卖服务系统（手机应用程式）的所有手机，并防止其他人使用该手机。
- 为避免您堕入任何网络诈骗的陷阱，建议您留意香港金融管理局、香港警务处或其他认可机构发出的防骗资料及最新消息。

6. 更多保安资讯

如欲了解更多保安资讯，请按下列连结：

香港警察：

- 预防科技罪案
- 什么是钓鱼攻击
- 什么是网上帐户骑劫?
- 什么是 WhatsApp 户口骑劫?

反诈骗协调中心 - 防骗短片/警示：

- 最新骗案警示
- 「A 股」投资诈骗
- 电话诈骗
- 骗案 - 喜怒哀「落」
- 网络投资骗案
- 「名人效应」投资骗案
- 网上情缘暨投资骗案
- 网上求职骗案
- 网络钓鱼骗案

香港特别行政区政府：

- 网络安全资讯站
- 资讯安全网

香港金融管理局：

- 数码 KEY 睇紧啲，揿 LINK 前要三思! - 信用咭篇
- 数码 KEY 睇紧啲，揿 LINK 前要三思!
- 智醒银行 客户锦囊　网上银行服务
- 智醒银行 客户锦囊　柜员机
- 保护个人数码锁匙
- 智醒消费者 小心骗徒
- 系咪呃紧你？Check 吓「防骗视伏器」

如果您发现任何可疑交易或收到可疑交易通知，请立即致电本行客户服务热线(星期一至五早上 9 时至下午 5 时（852）3608 8021) 或亲临香港德辅道中 10 号东亚银行大厦 9 楼与我们联络。另外，您也可以联络香港警务处反诈骗协调中心（Anti-Deception Coordination Centre）：（852）18222，咨询有关反诈骗事宜。