ICBC 中国工商银行（亚洲）

AI 代理火热之际 如何做个谨慎投资者

随着人工智能科技的快速发展，AI 工具逐渐普及，最近火热的开源人工智能代理被不少投资者作为智能投资助理，为投资操作带来便利，但其背后潜藏的安全风险同样不容忽视。骗徒及网络攻击者常利用 AI 工具漏洞进行诈骗，用户若疏忽防范，极易导致账户被盗，造成巨额财产损失。为避免成为下一个受害者，保障投资者资金与账户安全，本文将提醒各类使用风险，并提供防范要点，助你远离投资安全隐患。

常见的 AI 代理使用风险

一、授权操作风险

近年来，随着 AI 办公应用工具的功能逐渐强大，部分用户热衷于将办公或个人计算机的操作权限全权授权给 AI 代理，放手任程序自动运行任务以实现全自动化办公。但随着用户量快速增多，任务量日益庞大，近期爆出多项 AI 代理超预期地未经许可便删除用户重要邮件、或删除程序内重要代码、或卸载系统内重要应用的案例，甚至使用客户的投资账户进行交易，造成实际损失。授权 AI 代理的操作风险貌似已不可忽视。

二、密码泄露风险

投资账户授权密码是账户安全的核心屏障，部分用户为图方便，设置简单密码或重复使用同一密码，并授权 AI 代理可随意登陆，在所使用设备未获得充分防护的情况下，极易导致账户密码、IP 地址等隐私信息被网络黑客破解盗取，并擅自进行投资交易、转移资金。用户往往无法及时察觉，最终损失难以挽回。

三、授权 AI 应用于投资的风险

AI 的投资辅助功能仅为数据分析与参考建议，并非专业投资决策。部分用户过度依赖 AI 授权操作，全权交由 AI 代理执行投资买卖、资产配置，忽视市场波动与 AI 算法局限：AI 分析基于历史数据，无法预测未发生的突发市场风险、政策变动；且授权 AI 代理全权操作后，用户丧失人工监控环节，若 AI 代理出现算法偏差、数据错误、或系统崩溃，将直接为投资者带来损失；且自动化执行交易后，责任主体及相关法律责任定存在较大不确定性风险。

四、非法链接与伪冒平台风险

骗徒常伪造 AI 代理官方登录链接、仿冒 APP，以「升级优化」「专属投资通道」为诱饵，引诱用户点击授权、输入账户密码。用户一旦在非法渠道登录，账户信息将直接被骗徒获取。部分伪冒平台还会假借 AI 投资名义，诱导用户授权高风险交易，骗取投资者资金。

AI 代理安全使用贴士

1. **严守授权密码安全**

用户应设置复杂及具有独特的密码、定期进行更换、不与其他平台密码通用及不授权 AI 代理无限制使用个人密码、验证码，可有效降低密码被偷盗之风险。另外，在使用 AI 代理前，建议妥善设置好网络防火墙、防毒软件等网络防护措施，不建议在公共网络、陌生设备登录账户，如有需要登录，登录后应及时退出并清除缓存，杜绝密码被黑客攻击与泄露风险。

2. **理性对待 AI 投资授权**

用户应明确指示 AI 分析结果仅供投资参考，不应授权 AI 代理全权执行投资交易；亦不应盲从大衆使用 AI 代理，而是在使用前，先充分了解其特性、限制、以及能力，并结合市场行情、自身风险承受能力、以及人工分析核实，避免过度依赖 AI 全自动操作而引发亏损。

3. **核实官方渠道信息**

仅通过 AI 代理发行商官方网站、认证应用商店下载登录平台，不点击陌生链接、安装不明来源 APP；遇「授权优惠」「AI 稳赚」等可疑信息，第一时间通过官方客服核实，杜绝上当受骗。

4. **提升数据安全意识**

定期检查账户交易记录，及时发现异常交易；用户应开启账户异常提醒功能。如遇未授权登录或交易，用户应实时联系官方机构并冻结账户；避免招致损失。

5. **杜绝侥幸贪心心理**

切勿轻信「AI 投资稳赚高回报」「授权即享收益」等虚假宣传，所有形式的投资均伴随着风险，无全自动无风险的投资模式，投资者应保持理性，便宜勿贪。

提示:
数码 KEY 睇紧啲，揿 LINK 前要三思！
借卖户口中圈套，助洗黑钱毁前途。
投资涉及风险。

风险披露：

证券交易的风险：投资涉及风险，证券价格有时可能会非常波动，证券价格可升可跌，甚至变成毫无价值。买卖证券未必一定能够赚取利润，反而可能会招致损失。

重要声明

以上风险披露声明不能披露所有涉及的风险，如欲索取完整之风险披露声明，可向本行各分行查询。投资前应先阅读有关产品发售档、财务报表及相关的风险声明，并应就本身的财务状况及需要、投资目标及经验，详细考虑并决定该投资是否切合本身特定的投资需要及承受风险的能力。本行建议您应于进行任何交易或投资前寻求独立的财务及专业意见，方可作出有关投资决定。本文章所载资料并不构成招揽任何人投资于本文所述之任何产品。本文章由中国工商银行(亚洲)有限公司刊发，内容未经证券及期货事务监察委员会审阅。

「本行」或「中国工商银行（亚洲）」乃中国工商银行（亚洲）有限公司之简称。