维护资金安全小贴士

防范学生虚假开户实施诈骗

此类诈骗的常用手法有：

不法分子利用当事学生缺乏自我保护意识，不了解银行卡账户被他人使用的风险，通过网络以兼职等幌子，利诱青年学生为他们办理银行卡，然后进行收购，用于电信诈骗、网银诈骗，得手后赃款快速分批提取。

防范此类诈骗需注意如下事项：

银行卡业务风险并不仅限于银行卡资金，持卡人如果出卖个人银行账户，一旦被不法分子利用作为实施诈骗的工具，持卡人将可能面临潜在的法律风险和声誉风险。金融消费者切勿为些许小利，随意出卖自己的银行卡账户。

防范“钓鱼网站”实施银行卡诈骗

此类诈骗的常用手法有：

（1）通过病毒传播“钓鱼网站”信息。不法分子克隆一个与银行网站几乎一模一样的网页，并且使用的登录地址也与银行网站的地址非常接近，然后使用一些病毒程序、垃圾邮件等将假网站地址发送到网银客户的电脑上，或放在搜索网站上诱骗客户登录，以窃取客户卡号、密码等信息。
（2）通过手机短信，冒充银行发送诈骗短信。不法分子利用银行名义向客户发送手机诈骗短信，声称客户中奖或账户被他人盗用等，要求客户尽快登录到短信中指定的网站进行身份验证。
（3）将购物网站作为犯罪平台。不法分子往往以低价引诱被害人进行交易，通过木马病毒等程序获取被害人的账号及密码，随后盗划卡内资金。

防范此类诈骗需注意如下事项：

（1）在网上输入私密信息前，需确认网站地址是否正确；需要登录网上银行或者电子商务网站时，应直接在网址栏填写正确的网站地址，最好不要使用检索页来搜索网站。
（2）对来历不明的短信或电话要提高警惕，不要轻易相信，以免落入诈骗陷阱。如有疑问，可直接向开户银行咨询。
（3）注意防范信用卡交易中的风险，不要贪图小利，要选择较为正规的商店（包括网店）进行交易。

防范ATM盗取银行卡信息

此类诈骗的常用手法有：

不法分子多利用晚上人流稀少的时间段对离行式自助机具安装盗卡装置，或购买ATM配件自行组装山寨机具，并利用盗卡装置盗取银行卡信息。盗卡装置常安装在ATM等自助机具上或自助银行的门禁系统上。盗卡装置在材料质地、颜色、装饰等方面与原机器非常吻合，具有极高的仿真性，且安装极其紧密，不易引起银行清机人员和检查人员的注意。

防范此类诈骗需注意如下事项：

（1）通过自助银行门禁系统时不要输入密码。进入自助银行服务区有时需要在自动门上刷卡（借记卡或信用卡）开门，但不需要密码。持卡人如遇要求输入密码方可进入时，应及时报警。
（2）牢记银行通过网点、网站、媒体、ATM屏幕等正常渠道公布的统一客户服务电话，一旦有吞钞、吞卡等不正常事件发生，不要急于离开自助设备，也不要轻易相信来历不明的电话号码，而应拨打设备所属银行统一客户服务电话寻求帮助。

UOB 大华银行

维护资金安全小贴士

如何区分银行正规短信通知和诈骗短信？

正规的银行短消息当中会明确显示银行卡的消费时间、地点、消费金额以及卡号的尾数几位等明确的信息。而如果是虚假短信的话，由于发送虚假信息的不法分子并不知道持卡人的真正卡号，因此虚假短信中绝对不会包含发生交易的银行卡卡号等信息。此外，银行系统短信使用的是固定的特殊号码，不会使用普通手机号码，更不会经常变更号码。

防范假冒银行以贷款、办理信用卡为名实施诈骗

此类诈骗的常用手法有：

（1）以虚构办理贷款、信用卡业务作为犯罪的前置手段。在此类案件中，不法分子大都先通过网站、当地报纸贷款广告或直接拨打受害人手机等方式，向受害人推荐相关贷款、信用卡业务，并以此为名，要求受害人支付一定数额的手续费。
（2）办理过程不通过银行正规途径。在所谓“办理信用卡”过程中，填写递交申请资料的过程不在相关银行网点内进行，提交的资料也较为简单，仅为个人基本资料及身份证复印件，缺乏常规的收入证明等一系列文件。
（3）使用电讯手段作为犯罪主要手法。不法分子使用电讯任意显号技术手段，使受害人手机上的来电显示号码为相关银行，以取得受害人信任，骗取受害人资金。
（4）不法分子利用真实的银行授信批复加伪造的贷款材料，宣称银行贷款即将到账，使受害人误认为还款来源有保证。

防范此类诈骗需注意如下事项：

（1）不要轻信贷款小广告。金融消费者如需办理贷款业务，请到银行网点和其他经银监会批准的贷款机构申请办理；要时刻提高警惕，不要轻信各类贷款小广告，不要轻信在银行网点以外遇到的所谓“贷款推广人员”或“银行贷款工作人员”，也不要拨打贷款小广告上的联系电话，以免上当受骗。
（2）不要轻信来历不明的电话号码、手机短信和邮件。在任何情况下，银行职员、商店、警方都不会要求金融消费者告知银行账户、卡号、密码或向来历不明的账户转账。如果遇到上述情况，请金融消费者及时通过正规渠道报警，以确保个人账户和资金安全。
（3）不要泄露个人信息。姓名、身份证号、银行账号、银行卡号、密码、信用卡有效期和验证码都是重要的个人信息，是银行卡服务中身份验证的必备信息。只要涉及到这些重要信息，都要提高警惕，不要轻易向任何单位和个人泄露银行账户信息和密码。

防范电汇诈骗

此类诈骗的常用手法有：

（1）不法分子利用非实物交割的特点，以虚拟盘形式虚构交易，先要求客户汇款到香港公司的资金账户后，不法分子又谎称因交易波动，资金全部输光，完成诈骗，客户的投资资金其实早被挪作他用。
（2）不法分子专人陪同办理，且熟悉银行汇款手续，并有意阻挠客户本人与银行工作人员交流情况，所有凭证都是陪同人填写，客户只要现场按密码签字即可，在办理结束后陪同人会借故把所有汇款凭证全部收走。

防范此类诈骗需注意如下事项：

（1）广大金融消费者要提高警惕，不要轻易相信所谓境外投资业务。应牢记：一不给陌生人转账和汇款；二不泄露自己的账号和密码；三不使用他人提供的软件和开启远程协助功能操作网银等。
（2）为防范电汇诈骗、保护客户资金安全，银行柜员对可疑的汇款会询问您：是否认识对方，为何转账给对方，是否转到对方“安全账户”，是否收到过警方防范宣传提示等。您务必配合银行柜员，如实回答问题。

UOB 大华银行