

新学期，新征程。今天的杭州银行金融安全课堂从真实案例入手，聊一聊身边的网络诈骗，提醒学生们要保持警惕，避免落入网络诈骗的陷阱，让不法分子无可乘之机



身边的网络诈骗

以支付宝、微信、手机银行等为代表的新型网络支付手段，简便、快捷，特别受到消费者的青睐，但也不可避免地成为不法分子的目标，网络诈骗花样越来越多，学会辨别真伪并防范风险尤为重要。同学们，来看看不法分子是如何挖坑设套的：



案例1

游戏账号买卖：不能说的秘密

起因。 客户来到网点要汇款8000元至女儿银行卡，但说不清资金具体用途。

蹊跷。 营业经理心存疑虑，中学生不应有如此大额的临时用款，马上联系小姑娘。

真相。 原来小姑娘偶然进入的一家网站有收购游戏账号业务，就试着卖出一个闲置游戏账户，居然真的“交易成功”了！但在提现时，网站却提示“卡号输错，账号被冻结”，“热心”的网站客服告知需要充值才能解冻。小姑娘多次充值后银行卡余额不足，客服又出招了--“可以向家长要啊”，并贴心提醒“不能说因为买卖游戏账号，父母肯定不同意的”。小姑娘只好求助妈妈，但担心被责备又不敢告知用途，只是说急需用钱。

劝阻。 营业经理告知这是典型的电信网络诈骗手法，反复劝阻后小姑娘终于醒悟，停止充值并报警，避免了8000元的损失。

案例2

网上兼职：陷阱在后面等着呢

找兼职中招了。 一位小姑娘跑进网点，神情慌张，营业经理连忙迎上询问。原来她刚刚在QQ中添加了一个兼职QQ充值卡推销业务的网友，登陆对方提供的网址并输入手机号码和验证码，然后短信轰炸就开始了！各大网站注册验证短信源源不断，足有几百条。营业经理确定小姑娘的手机中了网站木马病毒！

紧急应对处置。 在安抚小姑娘情绪的同时，为避免客户的银行资金被盗刷盗用，立即指导应对：①马上解绑微信、支付宝等银行卡功能；②查询银行卡交易明细，微信、支付宝、银行卡未有被盗用交易记录；③拨打手机运营商客服沟通短信接收问题。小姑娘终于放心了。

万幸！！！ 小姑娘没有告知对方银行卡号和密码等信息，是资金未受损失的关键！

常见网络诈骗形式

01

网络游戏账号、装备及游戏币交易诈骗

防骗对策： 不要轻信网游中一些“战友”，警惕先付款后交货交易方式。

02
“钓鱼”网站诈骗

防骗对策：确定登录银行官网，保管好网银证书；避免在公用计算机上进行网上交易。

03
网购诈骗

防骗对策：选择正规购物网站，使用网银、支付宝等安全支付工具，拒绝私下交易。

04
群发银行卡透支、消费短信诈骗

防骗对策：收到类似信息应向银行客服咨询，不通过诈骗短信提供的联系电话咨询。永远不要相信有“安全帐户”！



防骗对策

01
保管好账号、密码、验证码和网盾

- 提高密码保护强度，不要用生日、姓名、地址等设置密码。
- 网盾密码泄露了，尽快办理挂失、补办或更改。

请注意

任何情况下银行都不会通过电子邮件、信函、电话或手机短信等方式，要求提供账号、密码、验证码或网上银行网盾。

02 认清网站网址

- 登陆网上银行官方网站，不要通过其他网站链接访问。
- 网上购物时到正规、知名的网站。

03 支付安全意识要提升

- 凡是提到“安全账户”的，都是诈骗。
- 从银行官方网站下载安装网上银行、手机银行安全控件和客户端软件。
- 设置电子支付交易限额。
- 确保计算机系统安全。如设置登录密码、安装防病毒软件和防火墙软件、关闭远程登录功能等。
- 不要轻信接收到的中奖、贷款等短信、电话。
- 避免在公共场所或他人计算机上登录和使用网上银行。

建议下载“国家反诈中心”APP，关注“杭州防诈骗”微信公众号

请同学们切勿因小失大，时刻擦亮眼睛，用金融知识武装自己，多求证、不轻信，远离网络诈骗。

部分资料来源：《大学生金融知识手册》、《浙江银行业保险业金融知识宣传手册(2021版)》