随着手机银行使用范围不断扩大，逐渐深入到生活的各个场景，如通讯、购物、娱乐等等，也为不法分子带来可乘之机。再加上目前个人信息泄露比较严重，如何安全使用手机银行、保障资金安全十分必要。

【案例回顾】不法分子惯用的诈骗手法

6月25日凌晨，李女士收到一条你尾号为的银行账户于6月24日完成一笔跨境交易，金额为1.9万元，余额为0。的手机短信。随后，一名自称某外汇交易公司职员的男子给李女士打来电话，称李女士于昨天晚上11时30分在该公司网站购买了一款理财产品，因系统故障显示交易失败，但相应的金额已扣除。由于电话里的男子准确地说出了李女士的姓名、银行卡号等信息，李女士便信以为真，忙问如何找回这笔钱。在男子的提示下，李女士在手机上登录了对方提供的网址，并按要求填写了银行账号、转账验证码等相应信息。

在此紧要时刻，李女士接到了来自中国建设银行的网络金融交易核实电话。在建行风控专员的耐心提示下，李女士才意识到自己已经掉进了诈骗分子精心设下的圈套里。建设银行的风控专员立即对李女士的账户进行紧急处理，从而避免了1.9万元的资金损失。

【揭秘惯用手法】

最近一段时间，类似的作案手法非常多，小编总结出几种不法分子惯用的诈骗手法：

1、不法分子使用任意显号网络电话，冒充邮局、电信、公检法等单位工作人员拨打手机用户电话，以邮寄包裹涉毒、有线电视或电话欠费、被他人盗用身份涉嫌犯罪为理由，以没收或保护手机用户银行存款为借口进行威胁恐吓，诱使其汇转资金到指定账户。

2、不法分子通过短信、电话、报纸等发布虚假融资广告，以提供低息贷款、验资等借口，诱骗手机用户使用他们提供的手机号码办理手机银行业务。签约后，通过诈骗获取银行卡账户密码以及手机银行登录密码，迅速盗取资金。

3、不法分子通过伪装成银行、支付类App，并在其中植入手机支付病毒，诱导用户输入银行账号、密码等信息，然后再通过病毒拦截并转发手机支付验证码、支付成功回执短信等，完成资金的窃取。或利用钓鱼信息+手机支付病毒的方式，盗刷用户银行卡。

4、不法分子制作一些抢红包软件投放在网络上，引诱用户下载，或是通过二维码将木马病毒植入用户手机中，以盗取用户信息、截取用户短信、获取验证码等方式，悄悄转移用户财产。

5、不法分子利用伪基站发送含有木马病毒链接的短信，手机用户一旦点击链接就会中毒。该木马病毒能拦截手机短信，并转发至另一个指定手机号码上，使得手机用户的身份、银行卡及短信验证等信息暴露无遗。

五招从容应对诈骗

应对不法分子千变万化的欺诈手法，应牢记以下五点：

1、妥善保护好包括手机号码、身份证信息、银行卡卡号和密码等个人信息。

2、手机用户要从安全的电子市场下载应用程序，不要下载安装来历不明、可能有危险的程序；不要随意点开手机上来历不明的无线网络、链接等，不要扫描来历不明的二维码；不要理睬来历不明的短信或彩信。

3、如遇有人打着银行、公安、司法、税务、海关、银监会等单位的名义，向您索要手机银行登录的用户名、密码、短信验证码等信息，请不要相信，因为在任何情况下，上述单位都不会索要这些信息。

4、为手机安装安全软件，查杀各类手机支付病毒来保证资金安全。

设置手机开机密码，使用数字证书、手机动态口令等安全必备产品。将手机银行、网银、支付宝等涉及资金交易的密码设置为敏感应用访问密码，使用数字+字母等复杂组合并定期修改，不能一套密码走天下。

使用短信动态验证码或银盾等安全必备产品并妥善保管，不能轻易泄露或借与他人使用。

5、一旦发现异常情况，要及时查询，发现资金被盗，在第一时间采取紧急措施。

建议开通账户变动短信、微信等提醒服务，及时关注账户余额变动情况。如有异常及时登陆网银、手机银行对账户进行挂失或拨打官方服务热线，请求工作人员协助对账户进行紧急处理，避免后续资金遭受损失。

如果手机遗失，可迅速使用手机已安装的第三方防护软件，远程销毁手机数据。

??????

????????????????100%????????????????????????

??????????

??5????????