**案例一**

某网站声称可通过其办理多家银行信用卡，客户只需填写个人基本资料并提交身份证复印件就可申请，申请前收取200元工本费，卡片办出后按额度收取2%手续费。客户周某在该网站递交申请并支付手续费后，该网站以相关银行某支行电话号码致电周某，告知已申请成功。随后周某又支付一笔手续费，但未收到信用卡。周某便致电相关银行询问，银行查询后发现系统里并无其申请信息，周某方知上当受骗。

**案例二**

某客户在报纸上看到一则关于无抵押贷款业务的广告，根据广告信息联系了对方。不法分子要求其填写了一份“贷款表格”，并提供了“某银行电话号码”让其联系。由于电话联系某银行未果，不法分子向客户介绍了“该银行的某支行负责信贷部门的陈经理”，“陈经理”告知贷款已获批，但要客户提供其在任何一家银行的30万元资金证明。客户向“陈经理”提供了其在其他银行开立的银行卡号和密码后，两小时内账户内的资金（30万元人民币）就被人支取。后经证实，该银行从未办理无抵押贷款业务，客户提供的“贷款表格”系伪造，该银行亦无所谓“陈经理”。

**案例三**

不法分子沈某与受害人孙某签订借款合同，承诺以其名下公司向某银行申请贷款作为还款保证，并支付利息48万元。为骗取孙某信任，沈某出示该银行贷款授信批复，还伙同他人伪造贷款材料收据和指示放款的承诺书，使孙某信以为真，出借1100万元，造成巨额资金损失。

## Q110. 调包客户银行卡实施诈骗

此类诈骗的常用手法有：

（1）犯罪分子制造事端，分散持卡人注意，再由同伙趁机掉包银行卡；

（2）犯罪分子故意靠近持卡人，在持卡人输入密码时在一旁偷窥。

防范此类诈骗需注意如下事项：

持卡人在使用ATM时，要随时注意周围情况。如遇有人故意以各种理由靠近，或制造事端分散自己的注意力时，应要求其与自己保持一定的距离，在输入密码、刷卡消费等过程中注意用身体遮挡键盘。若中途有被干扰的情况，持卡人在完成所有操作环节后，应仔细核对取回的银行卡，确认没有被人趁乱掉包。此外，不要随意放置银行卡和身份证件（最好分开存放），不要随意丢弃刷卡签购单和对账单，以防不法分子拾遗、窃取或破解这些重要的个人信息，假冒持卡人身份盗用资金。

**案例四**

犯罪分子团伙作案，在持卡人到ATM自动取款机取款时，偷窥持卡人密码，并故意在附近制造事端，分散持卡人注意力。同时使用消磁处理过的废银行卡，趁机将持卡人的银行卡掉包，再用窃得的银行卡进行冒领。该犯罪团伙在短短四天内，共作案10多次，成功调包银行卡2张，盗取银行卡内资金2.65万元。

## Q111. 利用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）凡是发现ATM机器外壳和电子显示屏上没有银行名称和银行标识的、使用过程中出现可疑迹象的ATM机具，应立即拨打相关银行客户服务电话进行确认，必要时立即向公安机关报警。

（2）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。

（3）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。

（4）牢记发卡银行的统一客户服务电话，并尽量开通账户变动短信提醒服务，第一时间了解自己账户金额变动情况。一旦怀疑自己的银行卡信息或资金被盗用，应立刻联系发卡银行查询账户余额、办理止付或将卡内资金转移到属于自己的其他账户中。

**案例五**

某银行发现一台离行式ATM上被安装了盗卡装置。盗卡装置分为两个部分：一部分为针孔摄像头，安装在屏幕上方，用于拍摄用卡人密码输入情况；另一部分安装在插卡口或门禁系统的刷卡槽上，用于盗取银行卡磁条信息。幸好该行迅速采取各种防范措施，未发生客户资金被盗取等后果。