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。

案例六

不法分子黄某通过网上购买了ATM的相关配件，自行组装了一台“山寨ATM”，安装在一家烟店旁，并在醒目位置张贴着“24小时自助银行服务”等标志，取款机上也张贴着“VISA”、“银联”等银行卡组织标志。当受害人使用ATM输入密码后，ATM即显示暂时无法提供服务的内容，并将银行卡退出。几天后，受害人发现自己银行卡账户内的资金已被盗取。

Q112. 利用“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。

案例七

不法分子通过短信提醒持卡人密码指令卡即将过期，要尽快登录其提供的假“网站”进行升级，诱使持卡人登录指定网站（该网站是由不法分子建立的、用于套取客户信息的“钓鱼网站”）。一旦持卡人登录该网站进行操作后，持卡人的卡号、密码、身份证件等信息就被不法分子窃取并盗刷，造成资金损失。