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。

案例八

不法分子在某购物网站开设黑网店，称可用1元钱“秒杀”50元手机话费，同时在持卡人付款“秒杀”抢购时，向持卡人发送一个假“安全”链接。持卡人谢某在浏览网站过程中，被“秒杀”信息吸引，点击假“安全”链接登录，并按照提示输入了自己的信用卡信息，不法分子通过木马病毒和分析工具盗取了该信用卡账号及密码信息。谢某在提交自己的信用卡信息后，显示交易不成功，不久却收到银行短信，获悉其信用卡被消费人民币7000元。

Q113. 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。

案例九

某日，某银行营业大厅来了两个穿西装的约30岁左右的青年男子，其中一人向柜员要了一份电汇申请书，填好单子后，两人陪同一女士到柜台办理一万美元的电汇业务。因收款人名字特别，而且数日前刚好有另一客户也往这个账户汇过款，也是有人陪同的，故引起了该行柜员的注意。当该行柜员提醒客户因频繁向该账户汇款，可能会出现“账户预警”时，陪同的青年男子根本不让柜员把话说完，一直急切地“表示”知道情况，肯定没有问题，不停催促要求尽快办理电汇业务。该行柜员在排除青年男子的多次干扰后，询问女客户本人是否认识收款人，女客户表示并不知晓收款人，也不知晓这是私人资金账户，于是该行柜员再次试探性地询问女客户是否到境外投资黄金，女客户惊讶地问柜员是如何知道的。由此引起陪同男子的“抗议”，随后两男子匆匆离开了该行营业大厅。