人民银行宁波市中心支行
宁波银监局
宁波保监局
宁波市网信办

电信诈骗银行卡盗刷，个人信息泄露是罪魁祸首

电信诈骗、银行卡盗刷……导致受害者多年积蓄落入不法分子口袋的罪魁祸首之一，就是个人信息泄露！加强消费者信息安全保护的相关立法已经提上议事日程。而作为金融消费者，更要注意妥善保管自己的信息。

个人信息需要妥善保管

身份证上的信息才是“个人信息”吗？其实个人信息的范围要大得多。它包含那些能够进行个人身份辨识的信息，包括：姓名、性别、身份证号码、电话、地址、电子邮箱、银行卡卡号、发卡日期、卡片有效期、指纹、婚姻状况、教育状况、职业等。

如何妥善运用及保护自己的个人信息，避免因个人信息泄露而让诈骗分子有机可乘？

“通过正当途径办卡，不要委托他人或非法中介机构代办信用卡，避免个人资料被盗用。提供个人身份证件复印件申办信用卡时，建议在复印件上注明使用用途，以防止身份证件复印件被移作他用。”监管部门相关人士介绍说，还要警惕向您询问个人信息的电话及电子邮件，银行或公安机关是不会来问银行卡账户信息及密码的。

此外，不要把身份证件、银行卡转借给他人使用，不要轻易向陌生人泄露个人信息，也不要随意在网络留下个人信息。保管好记录着您银行卡账户信息的对账单、签购单、取款凭条等单据，或及时处理、销毁。定期查看对账单，如果发现不明支出，请立即联系发卡银行。

邮寄地址同样是重要的个人信息。因搬家、工作变更等因素需要改账单寄送地址时，或者发现未能及时收到银行对账单时，请立即通知发卡银行。

莫要出售、出租自己的银行卡

出售或者出租个人闲置的银行卡看上去占了小便宜，但把自己的银行卡和个人信息出售给别人，极易被不法分子利用从而诱发违法犯罪。

据了解，在近几年查获的电信诈骗案中，拥有大量的银行卡成为犯罪嫌疑人的一个重要手段。在一些个案中，以各种名义到不同银行开卡，是电信诈骗团伙“外包”出去的一项业务。当有事主受骗往这些银行卡里汇款后，嫌疑人会指挥同伙在最短时间内将汇款全部提取并转移。除了电信诈骗，银行卡买卖的背后还指向洗钱、行贿、受贿、非法所得的财产转移等不法行为。

光大银行宁波分行开展“金融课堂进社区”活动

银行卡内存储了很多个人信息，如果贪图小便宜出售自己的银行卡，有可能被收卡人用来从事非法活动，给自己带来巨大的法律风险，甚至承担刑事责任。一旦所售银行卡出现信用问题，最终都会追溯到核心账户，会导致个人信用受损，甚至承担连带责任。

根据《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》，自2017年1月1日起，出租、出借、出售、购买银行账户（含银行卡）或支付账户的单位和个人，5年内停止其银行账户非柜面业务、支付账户所有业务，3年内不得新开立账户。

■以案说法

冒用他人身份证办卡，违法！

案情回放：6月1日，一男子在宁波市区信用联社江南分社办理借记卡开户。柜员在核实客户信息时发现其身份证照片与本人有一定差异，在将情况反映给运营主管后，询问该男子的家庭地址。因身份证件离手，这个简单的问题难住了该男子，在旁观察的运营主管发现他疑似在查看手机里的身份证照片，“老家地址还需要查看身份证照片，这个身份证不是你的吧？”该男子立即借故快速离开了信用社。

宁波市区信用联社开展金融宣传活动

点评：当前，用他人身份信息进行各种不合法的买卖行为逐年增多，特别是冒用他人身份证办理银行卡，用于洗钱、诈骗等违法犯罪活动。办理银行卡要求实名制是保护客户账户安全的底线措施，我市金融机构从源头切断一切客户疑似利用他人身份证件办理借记卡的违法行为，切实维护消费者合法权益。同时，提醒市民不要听信卖闲置借记卡没有风险的说法，主动办卡卖给他人。

出借账户给他人，有风险！

案情回放：5月3日下午，有三名穿着统一工作服的客户手持光大银行借记卡到光大银行海曙支行柜台要求办理开通令牌版网银业务。经办柜员询问客户开通网银的用途，客户说是单位老板要求他们开通的，给单位资金汇划所用。经办柜员与柜台经理反复劝说提醒存在的风险后，三名客户终于认识到这种做法的不妥，并表示今后不会出借账户给他人使用。

点评：出借账户给他人不但会导致个人信息的泄露、资金上的不安全，而且会对持卡人个人的征信产生影响，更有可能被不法分子利用而负上刑事责任。

常见电信网络诈骗伎俩及防范建议

一、冒充公检法等机关诈骗

以“法院传票、信息泄露、涉及洗钱”等为由，冒充警察、检察官、法官实施诈骗。

防范建议：警方不会通过110电话号码直接拨打用户电话，绝不会通过电话远程做笔录方式办案，更不会要求受访者提供个人的银行卡号、密码等信息。因此，遇到公检法要求提供银行卡号和密码以及将钱转到“安全账户”等情况时，切勿相信。

二、中奖诈骗

通过QQ、短信等方式向用户发送中奖提示信息，并利用在互联网上设置的虚假网站诱导事主误入中奖陷阱，以让事主缴纳税费、公证费、手续费等各种名目实施诈骗。

防范建议：收到类似的可疑短信时，可登录机构官方门户网站或拨打官方热线电话了解相关情况，不要轻易汇款。

三、“猜猜我是谁”诈骗

犯罪分子获取受害者的电话号码和机主姓名后，打电话给受害者，让其“猜猜我是谁”，随后根据受害者的描述冒充熟人身份，并声称要来看望受害者。随后，编造理由向受害者借钱。

防范建议：要注意保存好个人信息，为防止信息泄漏，要慎重在公共场所电脑及QQ、微博、微信等留下自己及朋友的真实信息。如果接到陌生来电，自称是好友时，应多方面核实真假。

四、刷卡消费诈骗

不法分子通过短信提醒手机用户，称该用户银行卡在某地（如商场、酒店）刷卡消费等。在用户回电话后，其同伙冒充银行客服谎称该银行卡可能被复制盗用，利用受害人的恐慌心理，要求其到ATM机上进行加密操作，将受害人卡内的款项转到指定账户。

防范建议：接到此类诈骗短信时，应及时拨打银行的官方查询电话进行核实，不要拨打诈骗短信中提供的咨询电话进行核实。

五、网络虚假投资诈骗

犯罪分子以某某证券公司名义散布虚假个股内幕信息及走势，引导事主在虚假交易平台上理财，骗取事主资金。

防范建议：在选择投资理财时，应确认该平台的所属地、性质、资金流向、过往历史等资料，做足功课后再进行投资。

六、植入木马诈骗

引诱事主点击短信的链接或诱使事主扫描带有木马病毒网站的二维码，进而向事主手机等电子设备植入木马程序，获取事主手机的通讯录、短信、银行卡、支付宝等信息实施诈骗。

防范建议：收到带有链接的短信时应高度警惕，不要随便点击陌生网址，更不要轻易安装可疑的客户端。同时不要见“码”就扫，小心二维码扫描诈骗。

本版撰文 记者 周静 通讯员 曾艳