农历春节将至，各种银行卡盗刷、短信欺诈案件频发。百姓如何保护好自己的钱袋子，平安过年？业内人士指出，首先，居民应该保护好个人信息，不要向他人泄露个人信息及交易密码。其次，如果遭遇欺诈事件，应第一时间去警察局报警备案，并向银行挂失卡片。此外，如果发生被盗刷事件，第一时间更改密码及相关重要信息，同时要警惕再次被盗刷风险。

春节前夕金融诈骗频发

“回顾2015年，我遭遇两次网络欺诈，名下银行借记卡余额被不法分子转入个人名下外汇账户。不法分子两次均是截取了我的短信验证码，通过网银给我开立了个人外汇账户，并将账户余额转入外汇账户，进行购汇。随后假装是银行工作人员试图骗取我的手机验证码，进行网上转账。”一位在外资银行工作的市民李先生对京华时报记者表示。

李先生感叹称：“还好只是在换汇时损失了点手续费和汇率差价，但我的个人信息肯定泄露了。”

在金融街工作的殷女士近日注销了自己的信用卡。她表示，因为身边有朋友遭遇信用卡盗刷，也频繁接到信用卡发卡行的风险提示。“估计是在单位附近的餐饮店就餐时造成盗刷的。建议信用卡消费付款时不离开视线。我宁可先注销这张信用卡，再重新办一张新卡，以免发生和同事一样的信用卡被盗刷情况。”

客户损失金额大幅增长

类似金融诈骗案例时有发生。例如，持卡人在未收到动态交易密码的情况下银行卡账户发生网上支付；有些持卡人因对“超级网银”等网上银行产品功能不了解而被盗刷；还有在银行卡丢失或被盗后，盗刷人在挂失止付前持真实银行卡到柜台或通过ATM机、POS机交易。

以信用卡为例，中国银行业协会近期发布的《中国信用卡产业发展蓝皮书（2014）》显示，伪卡、虚假申请、互联网欺诈、失窃卡、账户盗用是信用卡最突出的五大欺诈类型，其中互联网欺诈呈现快速增长态势，2014年欺诈损失金额为2245.4万元，比上年增长59.1%。信用卡网络欺诈盛行，致使客户损失金额呈大幅增长态势，这已成为危害百姓生活、影响经济发展、扰乱社会安定的一大顽疾。

建议保管好个人信息

一位银行业反欺诈人士对京华时报记者表示，“按照以往经验，春节前夕是金融欺诈案件高发阶段。从盗刷方式来看，主要的是盗取他人银行卡信息后伪造卡片，并使用盗取的银行卡密码通过ATM机或POS机取现或转账。盗用他人银行卡信息进行网上转账情况也呈现上升趋势。”

业内人士表示，首先，持卡人一定要保管好个人银行卡及银行卡信息。银行卡不能转借他人使用，不向他人泄漏个人账号密码。如果遭遇非本人交易的银行提示短信，第一时间联系银行卡客服中心，确认该笔交易是否已经发生，同时请客服中心立即冻结银行卡。如果真的发生被盗刷事件，第一时间向警方报案。如果被转移金额找回，第一时间注销旧卡，并修改其他卡片关键信息。

□典型欺诈案例

伪基站发布钓鱼网址

有些消费者近期收到信用卡积分即将清零短信，短信内容中附带链接。有持卡人登录短信中显示的网站地址，在网站中输入了卡号、交易密码、登录密码、动态密码等，卡内资金被转走。

银行反欺诈部门人士指出，不要轻易相信来路不明的来电、短信，可直接拨打银行官方客服或到银行网点咨询。

冒充电商客服“退款”

不法分子冒充一些电商客服致电有退货退款需求的消费者，甚至将消费者近期退款订单内容及个人信息全部告知本人，表示因为退款引发其他错误扣款，可以由银行客服取消。骗取需要客户提供信用卡卡号、有效期等信息进行“取消错误扣款操作”，随后用获得的持卡人信息进行转账，盗取资金。

专家建议，首先，尽量选择风控能力较强的电商平台进行消费。其次，要避免在公共场所登录网银，接到陌生电话不要轻易相信，更不要按照对方的指示进行密码操作。再者，遭遇类似情况应第一时间向警方报案，并更改涉及网站以及银行卡关键信息。

个人资金被转入名下其他账户

这类案例就是文中李先生所遭遇的情况。消费者收到银行提示短信称，账户进行了网上银行交易，购买了外汇。随后，接到自称外汇公司人员的电话，表示可以取消交易，退还资金，进而诱导持卡人ATM机上输入银行卡的六位密码。

专家表示，购买外汇的钱如果没有支付密码是无法转出去的，也就是说钱还在银行的系统里面，只是没显示在余额里面。遭遇类似情况，应第一时间挂失卡片并报警。