2019年“普及金融知识万里行”活动宣教内容
支付安全

一、银行卡（账户）安全防范

（一）借记卡种类

现有借记卡从物理结构上来讲，基本上分为三大类：

A.磁条卡:利用磁性载体记录字符与数字信息,磁条卡容易被消磁无法使用且信息容易被复制，安全性较低，社会上层出不穷的盗刷事件，基本都与磁条卡信息被复制有关。

B.芯片卡：也称金融IC卡，以芯片作为介质的银行卡。芯片卡具有安全性高、存储信息大、智能动态验证多项技术优势，截至目前全球尚未出现IC芯片卡被攻破的案例。

C.磁条芯片复合卡：既有磁条又有芯片。当客户使用芯片进行交易时，它的安全性等同于芯片卡，可以有效保障账户资金安全。

2017年5月1日，国内关闭了磁条芯片复合卡的磁条交易功能，综合考虑，为了资金安全，顺应时代趋势，建议及早将磁条卡升级为芯片卡。

（二）银行卡（账户）申请

2016年，中国人民银行研究制定了《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》(银发〔2016〕261号，以下简称《通知》)。《通知》规定：“同一

个人在同一家银行（以法人为单位）只能开立一个I类户,已开立I类户，再新开户的，应当开立II类户或III类户。”

为降低个人资料被盗用风险，建议尽量亲自到营业网点办理银行卡（账户）开立手续，不要委托他人或非法中介机构代办。银行未委托任何中介机构代理银行卡（账户）申请业务。

提供个人身份证件复印件申办银行卡（账户）时，可在复印件上注明使用用途，例如：“谨供申办银行卡（账户）用”，以防身份证件复印件被移作他用。

申请办理银行卡（账户）时，应如实填写个人真实资料，务必留存您本人的手机号码或常用电话号码。手机号码等个人资料发生变更时，务必及时通知银行修改，避免使用过期手机号或与他人共用手机号作为联系方式。

（三）银行卡（账户）保管

请勿随手放置银行卡（账户），公共场合不要将银行卡（账户）放在易丢失、易失窃的地方。同时，银行卡（账户）作为您接触账户资金的工具，仅限本人使用，请勿将您的银行卡（账户）出租、出售、出借给他人使用。

此外，请将您的银行卡（账户）与身份证件分开存放，以免因无法及时办理挂失、补卡等业务而造成不必要的经济损失。

如果银行卡（账户）遗失、被盗或发现被冒用时，请您

及时拨打银行客户服务热线办理银行卡（账户）挂失，并注意留存相关非本人交易证据。

（四）银行卡（账户）信息保护

银行卡（账户）因破损、到期等原因补发新卡时，请将旧的银行卡（账户）的磁条（或芯片）销毁。同时，建议您将不常用的账户撤并，及时到银行网点办理销户等。

由于消费签购单等纸质单据包含卡号等敏感信息，请您务必妥善保管或及时销毁，切勿随意丢弃。

不要将卡号、证件号、姓名、手机号、短信动态验证码、有效期、交易（查询）密码等敏感信息告知他人、中介或在公共电脑上留存上述敏感信息，也不要回复要求提供上述敏感信息的可疑邮件或短信。在任何情况下，银行工作人员都不会直接索取或发送索取短信动态验证码、交易（查询）密码的邮件或短信。如果您收到此类信息，请拨打银行客户服务热线予以核实。

建议您及时开通交易短信提示，定期关注账户资金变动情况，如果发现不明交易，请立即联系银行客户服务热线或至银行营业网点咨询详情。

不要随意在网络留下包含自己银行卡（账户）号、证件号、姓名、手机号等敏感信息的资料，以防信息泄露。

不要随便在街头扫描二维码、填写问卷留下银行卡（账户）号、证件号、姓名、手机号等重要敏感信息。

不要在公共场合随便连接免费 Wi-Fi ,不要在 Wi-Fi 登录页面中输入关于银行卡（账户）号、证件号、姓名、手机号等信息。

（五）银行卡（账户）使用

一旦银行卡（账户）失窃或有异常情况，请尽快与银行联系。如遇资金盗用，请立即向公安机关报案处理。

建议根据自身需要设置和控制银行卡账户资金使用风险，通过电话、网上银行、及营业网点调低 ATM 或 POS 使用限额，如遇有大额交易需求时，可通过柜台或网上银行调高交易限额。

在银行卡（账户）使用过程中，您可以通过银行营业网点、ATM、网上银行等随时修改密码。

建议您分别持有银行一类户银行卡（账户）和二类户银行卡（账户），并绑定使用。一类户银行卡（账户）作为主要结算账户，用于大额投资理财等用途，尽量少用于 ATM 取款、POS 消费等生活场景。同时，二类户银行卡（账户）则主要作为日常生活中小额消费、取款等用途使用。

POS 机刷卡时，请不要让银行卡（账户）离开您的视线范围，输入密码时请注意遮蔽键盘。

使用 ATM 时，请留意插卡口是否有改装痕迹，键盘上方是否有摄像头等隐蔽设备；ATM 出现吞卡等故障时，不要轻易离开，可在原地拨打 ATM 屏幕上显示的服务电话或直

接拨打银行客户服务热线咨询，请勿轻信 ATM 周边粘贴的纸质“通知”及“通知”上的电话。

操作 ATM 时，避免被他人转移注意力，调换银行卡（账户）或窥探密码。交易结束后应及时取回银行卡（账户）和现金。

如果您在持卡消费或取现时经常出现不正常的情况，建议您及时联系银行检查银行卡（账户）。

（六）银行卡（账户）被盗用

如发现银行卡(账户)被盗用,应第一时间致电银行客户服务热线，紧急挂失，防止资金损失扩大。同时，就近前往银行网点，出示身份证件及银行卡（账户），确认银行卡（账户）仍由本人持有且交易非本人操作。如遇夜间，可就近前往银行 ATM 机具，错误输入密码锁定银行卡（账户）。客户应及时向公安机关报案，并前往银行网点提交公安机关出具的报案回执、身份证件复印件、银行卡（账户）正反面复印件等，并当场填写否认交易声明。银行在获取上述信息后，将协助客户开展调查，尽最大可能挽回资金损失。

（七）合法合规安全用卡

根据监管有关规定及银行卡（账户）章程和领用协议相关条款，银行卡（账户）仅限本人用，不得出租、出售、出借银行卡（账户）。买卖银行卡（账户）属于违规行为。同时，买卖银行卡（账户）行为过程中可能会伴随着非法持有

大量银行卡（账户）、买卖居民身份证等违法行为，涉嫌违法犯罪。

非法买卖银行卡（账户）具有极高风险。一方面，非法买卖的银行卡（账户）、身份证等可能被用于洗钱、逃税、诈骗、送礼和开店刷信用等行为，扰乱了正常的社会秩序。另一方面，银行卡（账户）内存储了很多个人信息，如果贪图小利出售自己名下的银行卡（账户），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（账户）出现信用问题，还可能导致个人信用受损，甚至承担连带责任。

二、密码安全防范

1.密码设置

设置易于记忆但难以破译的密码。请勿设置简单数字排列的密码或用生日、证件号码、电话号码等作为密码，防止被不法分子试出。

切勿将银行卡（账户）登录密码、取款密码和支付密码与其它网站或网上商户使用的各类注册密码设置相同，避免因其它网站注册密码泄漏而导致银行卡所有密码同时失窃。

若您的银行卡（账户）为单位批量办卡，领用后请及时激活设置密码。

2.密码保管

不要将密码写在或保存在任何可能让他人看到或得到

的地方。不要将密码存放在手机里，更不要写在银行卡（账户）背面。请勿将密码与银行卡（账户）放在一起保管。

密码作为身份识别的最终依据，应当确保只有本人知悉。若怀疑密码发生泄漏风险，请及时通过银行营业网点、ATM、网上银行和电话银行等渠道修改密码。

请不要向任何人透露您的密码。银行、公安机关、司法机关都不会索要您的密码。

建议不定期修改银行卡（账户）密码。特别是密码使用时间较久或境外出行归来的，应及时修改交易密码。

三、ATM 交易安全防范

1.ATM 交易前

刷卡进入自助银行的门禁无需输入密码。

首先保证您自身安全。留意周围环境是否安全。如果有人离您太近，并且举止可疑，请改用其他 ATM 或终止操作。进入 ATM 隔间后应及时上锁。

检查 ATM。如果发现 ATM 上有多余的装置或摄像头，或者插卡口或出钞口有异常情况或有被改造的痕迹，请更换其他 ATM 操作或至银行营业网点办理业务。

若您不会使用 ATM 操作，您可联系银行客户服务热线进行咨询，切记不要按照他人提示的步骤完成取款操作，谨防诈骗。

2.ATM 交易时

专心操作，不要接受陌生人的“善意”帮助或其他人的询问。被他人引开注意力时，应用手捂住插卡口和出钞口，防范欺诈分子将卡、现金等调包。

输入密码时，应尽量快速并用身体遮挡操作手势，以防不法分子窥视。

如果 ATM 出现吞卡或不吐钞故障，不要轻易离开，可在原地拨打 ATM 屏幕上显示的银行服务电话或直接拨打银行客户服务热线 ,请勿轻信 ATM 周边粘贴的纸质“通知”及“通知”上的电话。

3.ATM 交易后

离开 ATM 前，请确认取走您的银行卡(账户) 和现金。

请确认取出的银行卡(账户)是否是您本人的银行卡(账户)。

选择打印 ATM 交易单据后，请勿随手丢弃，应妥善保管或及时销毁单据。

四、POS 交易安全防范

1.POS 交易前

申领到银行卡(账户)时 ,务必在卡背面签名条上签名，并按上述提示，妥善设置并保管密码。

建议您使用 IC 卡。IC 卡又称之为芯片卡，是通过可运算的芯片和存储在其中的密钥，确保终端与银行卡（账户）的交互过程中安全真实，而且能保证联机交易信息的安全，

难以复制，安全性高于磁条卡。

2.POS 交易时

刷卡消费时，切勿让银行卡（账户）离开视线范围，并留意收银员的刷卡次数。

输入密码时，应尽可能用身体或另一只手遮挡操作手势，以防不法分子窥视。

尽量不在不正规场所使用银行卡（账户）。

3.POS 交易后

收银员交回签购单及银行卡（账户）后，您应认真核对签购单上的交易日期、金额等是否正确，银行卡（账户）是否为本人的银行卡（账户），不要在非本人交易或交易信息有误的签购单上签名。

刷卡消费时若发生异常情况，要妥善保管交易单据，如发生卡重复扣款等现象，可凭交易单据及时与银行联系。

及时核对用卡情况，如有疑问，请及时联系银行营业网点或拨打银行客户服务热线进行查询。

签购单因错误需重写时，请您要求收银员将原签购单全部撕毁。

若需当场取消交易，或遇收银员重复操作交易，请您要求收银员当场撤销交易，恢复您的银行卡（账户）账户余额。

五、网络交易安全防范

（一）常见的网络支付方式

1.网上支付：指单位或个人通过电子终端，直接或间接向银行业金融机构发出支付指令、实现货币支付与资金转移的行为。根据支付指令发起渠道可分为网上支付、电话支付、手机支付等。网上支付是由客户通过在商户端选购商品确认订单后点击支付，跳转银行支付页面的一种支付类型。支持信用卡首次支付免签约服务，客户可选择任何一种支付方式进行支付 。包括：银行卡直接支付、网银专业版支付、手机 PUSH 支付、手机 WAP 支付。

2.快捷支付：是指用户通过电话或者网站等方式订购商品时，不需开通网银，只需提供卡号、手机号码等信息，银行验证客户信息及手机号码正确后，即可完成支付。商户可以选择是否向验证通过的手机号码中发送手机动态口令。目前很多支付工具中用户可以自行设置小额免密额度，使得多频、小额的支付场景更加方便、快捷。

（二）网络欺诈主要风险

1.网络钓鱼是指不法分子通过大量发送冒用来自于银行或其他知名机构的欺诈性垃圾邮件或短信、即时通讯信息等，引诱收信人给出敏感信息（如银行卡号、密码、证件号、手机号、短信验证码等详细信息）的一种攻击方式，然后利用这些信息假冒受害者进行欺诈交易，从而盗用银行卡（账户）账户资金。如不法分子伪冒与银行官方网站非常相似的钓鱼网站，诱使用户输入个人敏感信息。

2.木马病毒是一种基于远程控制的黑客工具，它通常会伪装成程序包、压缩文件、图片、视频等形式，通过网页、邮件等渠道引诱用户下载安装，如果用户打开了此类木马程序，用户的电脑或手机等电子设备便会被不法分子控制，从而造成信息文件被修改或窃取、银行卡（账户）资金被盗用等危害。

3.社交陷阱是指不法分子利用传销、招聘等社会工程学手段，获取用户个人信息，并通过获取的重要信息盗用用户银行卡（账户）账户资金的网络诈骗方式。例如骗子公司在网络上发布招聘信息，利用各种名义收取报名费、介绍费、押金、中介费等不合理收费的欺诈行为。

4.伪基站一般由主机和笔记本电脑组成，不法分子通过伪基站能搜取设备周围一定范围内的手机卡信息，并通过伪装成运营商的基站，冒充任意的手机号码强行向用户手机发送诈骗、广告推销等短信息，通常保护钓鱼链接，诱使客户点击下载病毒。例如用户收到的冒用银行客服热线以“手机银行升级或提升信用卡额度”等为由的诈骗信息。

5.由于部分中小网站安全防护能力较弱，容易遭到黑客攻击，该网站注册用户的用户名和密码便因此泄露。如网站用户设置了与银行卡账户相同的用户名和密码，则极易发生银行卡（账户）账户资金盗用。

（三）网络交易安全防范提示

保护好密码及其他重要身份信息。重点关注密码，勿设置简单易猜测的密码；勿将银行账户密码与互联网邮箱、购物平台、游戏账户等密码全部设置为同一密码；切勿转发短信验证码。

保护好手机和电脑等终端设备。安装杀毒软件，不点击不明链接；在安全的网络环境下使用手机银行和网上银行。

开通账户交易通知功能，及时发现异常情况。

六、移动支付风险防范

条码支付是以条码为信息载体，通过移动终端或商户受理终端直接或间接获取支付要素以完成交易的支付方式。常见的条码包括二维码、条形码等类型。在使用过程中要增强安全意识，做到：

不扫描来源不明的二维码

不轻易将个人二维码信息泄露给他人

不通过二维码支付进行大额交易

加强对手机等智能终端的安全管理

核对帐户名称与商家是否一致，与商家确认帐户名称是否正确后，再进行支付操作。如发现异常立刻停止支付。

七、案例集合

场景 1：ATM 取现案例

案例 1.窥视密码，盗走卡片。客户在 ATM 机取现时，不法分子趁持卡人取款时，窥视密码，然后以询问、故意将

钱丢在地上等手法，引开出卡人注意力，并趁机将预先准备好的卡片插入 ATM 机插卡口，造成卡片退出的假象，催促持卡人取卡离开后，将持卡人的卡片退出盗走。

案例 2.窃取密码，伪造卡片。不法分子在自助银行门禁系统上安装盗录设备及摄像头，待客户刷卡后，盗取磁条信息及密码后，制作伪卡。或者在 ATM 机上安装吞卡装置，或用望远镜窥视安装假密码键盘或在真密码键盘上贴薄膜等手法盗取密码，用微型摄像机偷窃卡号和密码或从持卡人随手丢弃的 ATM 取款凭条上获取相关信息，制作伪卡冒领存款。

案例 3.造假信息，趁机盗取。不法分子在 ATM 机上安装吞卡装置，ATM 机旁张贴假的银行告示。引诱持卡人拨打告示上的虚假服务电话，并冒充银行工作人员套出持卡人的银行卡密码后，从 ATM 上盗取存款。或者在 ATM 机旁张贴假的银行公告，以“银行程序调试”等为由，要求持卡人将银行卡存款转账到指定账户，盗取卡上存款。

场景 2.POS 消费盗刷案例

案例 1.刷 POS 机送礼品，银行卡遭异地盗刷。“刷一次 POS 机，消费 49.99 元，可获赠一袋大米和一桶豆油！”面对这样的促销宣传，一些市民信以为真，纷纷刷卡领取赠品。某客户信以为真，分别用银行卡刷了一次 POS 机，得到一张凭条，上面显示“划卡消费 49.99 元”，客户获赠了大米和豆

油。然而，一场精心准备好的骗局正悄悄向他们逼近：手机短信一条条响起，显示他们的银行卡在异地被盗刷。

案例 2.技术改造 POS 机，客户信息被窃取。客户王先生收到短信，其银行卡突然被刷了近 30 万元！王先生说：“共收到五条消费短信，第一条 49800 元，第二条 98000 多元，后来三条也都是 4 万多。”银行发来的消费短信显示，王先生的银行卡在一家超市内，在不到五分钟的时间里分五次消费了总计 29 万多元。经警方破案，根据不法分子交代，其通过伪造工商证件等方式从一家网络科技有限公司购买 POS 机，并对这些 POS 机进行技术改装，改装后的 POS 机，不但具有盗取银行卡全部信息的功能，还可以把这些信息同步发送短信到移动设备。改装后的 POS 机，被犯罪嫌疑热以降低手续费等为诱饵，销售给餐饮、足浴店、酒店等商家，在全国布点盗取银行卡信息。

场景 3.密码失窃案例

案例 1.短信诈骗新花样。目前，短信欺诈出现了新花样，“商场消费”的假短信可能变为“中奖”、“退税”等假短信，诱骗持卡人在 ATM 机上进行“银行卡升级”或在网上银行设置“联网报警系统”。

案例 2.钓鱼网站窃信息。不法分子在“网上钓鱼”，设立虚假金融机构网站，储户如果登录该网站操作其银行卡的卡号，密码就会被不法分子窃取。

案例 3.活动链接频盗刷。居民张大爷的手机收到了一条“10086”发来的短信， 当天中午，张大爷收到的“10086”的短信，内容为“尊敬的星级客户，您可享受话费赠送活动，充值 100 元送 100 元，登录充值 http://10086.com.co/m 活动今日截止”。张大爷觉得既然是正规的公司短信不能有假，按照短信内容点击此链接到一网站，再按照网站的要求，依次将电话号码、银行卡号、密码输入网站后，张大爷在家中坐等“充值成功”的短信时 ,结果却收到了银行卡被刷 3000 元的提示短信。 警方已接到此类多次报案，罪犯使用技术手段群发此类信息，只要你一登录对方网站，按照对方要求输入银行卡保密信息，即被犯罪分子乘机盗刷银行卡钱财。

案例 4.网上购物要谨慎，支付信息勿泄露

骗子们通过网络改号软件冒充商户客服，谎称产品有质量问题并声称可以免费退款，要求添加您好友，诱骗您填写个人支付信息，如：短信验证码、信用卡有效期(四位数字)及 CVV2(安全验证码)等支付信息，然后盗刷您的信用卡。

八、安全小贴士集合

1. 保障 ATM 操作安全，四要点

（1）在 ATM 上查询、取款时，要留意周边环境，谨防密码被偷窥；

（2）选择打印 ATM 交易单据后，要妥善保管或及时处理、销毁，不要将其随手丢弃；

（3）操作 ATM 出现机器吞卡或不吐钞时，要原地直接拨打银行客户服务热线进行求助；

（4）要认真识别银行公告，千万不要相信要求客户将钱转到指定账户的公告。

2.保证刷卡消费安全，五步走

（1）要在正规商户进行交易，刷卡消费时请勿让银行卡离开自己视线范围，要留意收银员的刷卡次数，避免误刷多刷；

（2）在刷卡消费输入密码时，应尽可能用身体或另一只手遮挡操作手势；

（3）签署签购单时，要仔细核对是否是本人的卡号、日期和金额，如发现有误，应要求收银员当面撕毁凭证并取消交易；

（4）交易完成时，要确认收银员交还的是否是自己的银行卡，并保存好签购单，以便日后与对账单核对；

（5）开通短信提醒服务，及时掌握账户动态信息，当账户发生异常变化后，要及时联系发卡银行查询交易，一旦发现被盗刷，应及时申请冻结账户和挂失卡片，避免损失扩大。

3.保证网上支付安全，七应该

（1）网上交易前应确认网址是否正确，要选择信誉好、运营时间长的网站进行银行卡网上支付业务；

（2）完成网上交易后，应及时退出，避免发生后续风险交易；

（3）在进行境外网上交易时，应通过安全途径，开通相关认证服务；

（4）应避免通过公用 WIFI 进行支付，不在网吧等公共场所进行网上交易，以免泄露账号及密码等信息；

（5）应注意不要扫描来源不明的二维码、登录不明网站，避免被不法分子植入木马病毒。

（6）办理网络购物、网络退货、退款时，应认清官方渠道，切勿轻信不明身份的电话、网络聊天工具或其它形式提供的非正规的网络链接；

（7）收到可疑手机短信时，应谨慎确认，如有疑问应直接拨打银行客户服务热线查询。

4.发现信用卡被盗刷，四应对

（1）一旦发现的信用卡被盗刷，请立即致电发卡银行官方客服电话报告异常交易，及时冻结账户或挂失卡片。

（2）立即在就近的 ATM 或 POS 上进行一笔刷卡交易，证明卡片在您身上未丢失，如果卡片已经冻结或挂失，刷卡不会成功，通过 ATM 机交易时卡片可能会被吞卡，此情况为正常现象，请按 ATM 机所属银行的相关规定进行后续处理即可，无需惊慌。

（3）立即向当地公安部门报案，积极配合公安机关开

展调查，联系发卡银行办理异议交易申请及相关手续等。

（4）如您的网银、电话银行、手机银行等设置的密码与被盗刷卡片密码相同，建议您尽快修改用户名和密码等，以防其它账户被盗。

5.安全用卡 12 条

（1）芯片卡（金融 IC 卡）的安全性远高于磁条卡，因此首先建议您尽快将手中磁条卡升级为金融 IC 卡。

（2）开通短信、微信提醒功能，可以第一时间发现账户收支详情。

（3）使用卡片前，要在卡背面签好姓名，防止错拿与被不法分子调换

（4）不得出售借记卡，也不要将卡片转借他人或将密码告知他人。

（5）刷卡消费时，不要让卡片离开视线范围，使用密码交易时防止被他人偷窥。

（6）不要设置较为简单的密码，如 112233、123456 等，更不要将密码存在手机中或卡背面，也不要将第三方密码作为借记卡密码。

（7）不要使用公共 wifi 接入手机银行、网上银行等，使用完网银及时退出。

（8）警惕钓鱼网站，对于有奖链接、不熟悉网友的链接等不明网址不要轻易登录。

（9）取款存条不要随手丢弃，以防被不法分子获取个人相关信息。

（10）不贪小便宜，警惕街边以及小摊刷卡。

（11）刷卡消费后，一定要核实刷卡记录上的刷卡信息与 POS 单上的商户信息是否相符。

（12）如发现银行卡被盗刷，应第一时间报警，并与银行或第三方支付平台进行联系，及时冻结资金，最大限度保证资金安全。