

## 银行卡安全用卡常识

浦发银行为进一步提升借记卡持卡人服务体验，编写了《上海浦东发展银行借记卡安全用卡指引》，旨在加强对个人信息保护、借记卡用卡安全等方面的支付结算业务知识和法规制度宣传，提高客户风险防范意识，保障资金安全，让客户安全、放心用卡。

### 一、引言

为持卡人提供优质、安全的用卡体验既是我行不断追求的目标，也是浦发借记卡“安全”的品牌承诺。为了帮助您正确使用我行借记卡，避免因外部风险原因造成对账户和资金安全不必要困扰，我们特此编写了《浦发银行借记卡安全用卡指引》。该指引囊括了必要的安全用卡常识与技巧，就常见的欺诈案例分析作案手法并提供了防范建议。通过掌握这些常识和技巧，我们真诚地希望能帮助您更加安心、愉快的享用浦发借记卡及服务。

### 二、卡片安全防范

#### 1、卡片申请

- 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借记卡开卡手续，不要委托他人或非法中介机构代办。我行未委托任何中介机构代理借记卡申请业务。

- 提供个人身份证件复印件申办借记卡时，可在复印件上注明使用用途，例如：“谨供申办浦发借记卡用”，以防身份证件复印件被移作他用。

- 接到自称银行人员的电话向您询问有关借记卡卡号、银行账号及密码等个人账户资料时，要提高警惕。我行工作人员不会向您索要任何密码或短信动态验证码。

- 申请办理借记卡时，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，务必及时通知我行修改，避免使用过期手机号或与他人共用手机号作为联系方式。

## 2、卡片领用

- 如果您从我行网点柜台申领借记卡，请在申领的同时设置六位数的个人安全交易密码；属于他人代理办卡或者批量申领的借记卡，需要您携带本人有效身份证件至我行网点办理卡片激活。若您发现卡片已预先激活或设置密码，请尽快联系我行并办理换卡等业务。

## 3、卡片保管

- 请勿随手放置借记卡，公共场合不要将卡片放在易丢失、易失窃的地方。同时，借记卡作为您接触账户资金的工具，仅限本人使用，请勿将您的借记卡出租、出售、出借给他人使用。

- 此外，请将您的借记卡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。

- 如果卡片遗失、被盗或发现被冒用时，请您及时拨打我行95528客户服务热线办理卡片挂失，并注意留存相关非本人交易证据。

#### 4、卡片信息保护

- 借记卡因破损、到期等原因补发新卡时，请将旧卡片的磁条（或芯片）销毁。同时，建议您将不常用的账户撤并，及时到我行网点办理销户等。

- 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，我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 95528 客户服务热线予以核实。

- 建议您及时开通“及时语”短信提示，定期关注账户资金变动情况，如果发现不明交易，请立即联系我行 95528 客户服务热线或至我行营业网点咨询详情。

- 不要随意在网络留下包含自己借记卡号、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、填写问卷留下借记卡号、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借记卡号、证件号、姓名、手机号等信息。

#### 5、卡片使用

- 一旦卡片失窃或有异常情况，请尽快与我行联系。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。

- 在借记卡使用过程中，您可以通过我行营业网点、ATM、网上银行等随时修改密码。

- 建议您分别持有我行一类户借记卡和二类户借记卡，并绑定使用。一类户借记卡作为主要结算账户，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，另一张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，请不要让卡片离开您的视线范围，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我行 95528 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，调换卡片或窥探密码。交易结束后应及时取回卡片和现金。

- 如果您在持卡消费或取现时经常出现不正常的情况，建议您及时联系我行检查卡片。

## 6、卡片被盗用

- 建议客户第一时间致电我行 95528 客户服务热线，紧急挂失卡片，防范资金损失扩大。同时，就近前往浦发银行网点，出示身份证件及卡片，确认卡片仍由本人持有且交易非本人操作。如遇夜间，可就近前往浦发银行 ATM 机具，错误输入密码锁定卡片。客户应及时向公安机关报案，并前往浦发银行网点提交公安机关出具的报案回执、身份证件复印件、卡片正反面复印件等，并当场填写否认交易声明。我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。

## 7、合法合规安全用卡

- 根据监管有关规定及我行借记卡章程和领用协议相关条款，借记卡仅限本人用，不得出租出售出借借记卡。买卖借记卡属于违规行为。同时，买卖借记卡行为过程中可能会伴随着非法持有大量借记卡、买卖居民身份证等违法行为，涉嫌违法犯罪行为。

- 目前，非法买卖借记卡“来路”和“去向”多种多样。例如，网上买卖借记卡的方式有通过网上商城、商品交易平台、博客等发布相关“广告”信息；网上买卖借记卡的内容有卡片、身份证、网盾、手机卡、开户资料等。不管以什么样的方式进行买卖，这些行为都违法违规。

- 非法买卖借记卡具有极高风险。一方面，非法买卖的借记卡、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，借记卡内存储了很多个人信息，如果贪图小利出售自己名下的借记卡，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。一旦所售借记卡出现信用问题，还可能导致个人信用受损，甚至承担连带责任。

- 使用借记卡过程中应注意以下事项。一是妥善保管好自己的身份证、卡片、移动证书 U-Key、SIM 盾等账户存取支付工具，保护好登录账号和密码等个人信息，对于废弃不用的借记卡，应及时办理销户业务，并将卡片磁条和芯片毁损，不随意丢弃。二是不出租、出借、出售个人借记卡、身份证和移动证书 U-Key、SIM 盾等账户存取支付工具，以免造成经济损失，并承担法律责任。三是尽快将手中的磁条卡换成芯片卡，同时对磁条卡进行销户处理。由于芯片卡安全度比磁条更高，复制难度高，目前磁条卡将逐步停发，能够为持卡人提供更高级别的安全保障。四是一旦发现买卖借记卡和身份证的犯罪行为，应及时向公安机关举报，配合公安机关或我行做好调查取证工作，有效打击犯罪分子，自觉维护良好的用卡秩序，保障自己的合法利益。

### **三、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（如 888888）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。

- 切勿将借记卡登录密码、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。

- 若您的借记卡为单位批量办卡，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，更不要写在卡片背面。请勿将密码与卡片放在一起保管。

- 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，请及时通过我行营业网点、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。

- 建议不定期修改借记卡密码。特别是密码使用时间较长或境外出行归来的，应及时修改交易密码。

## **3、密码使用**

- 刷卡进入自助银行的门禁无需输入密码。

- 留意自助银行门禁及 ATM 上是否有多余的装置或摄像头，ATM 密码键盘是否有改装痕迹。

- 输入密码时，应用另一只手或身体挡住操作手势，防止其它人或针孔摄像机偷窥。如果您发觉密码被偷窥，请立即修改密

码或致电我行 95528 客户服务热线办理挂失。

#### **四、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 操作或至我行营业网点办理业务。

- 仔细识别欺诈分子假借“银行”、“公安”名义发布的公告，银行、公安机关均不会要求客户将钱转入指定账户。若发现此类公告请尽快向我行或公安机关举报。

- 警惕借记卡短信诈骗。应谨慎确认可疑手机短信，如有疑问应直接拨打我行 95528 客户服务热线进行查询，请勿拨打短信中的联系电话。

- 若您不会使用 ATM 操作，您可联系我行 95528 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我行 95528 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，请确认取走您的借记卡和现金。
- 请确认取出的卡片是否是您本人的卡片。
- 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。

## **五、POS 交易安全防范**

### **1、POS 交易前**

- 申领到借记卡时，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，确保终端与卡片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，切勿让借记卡离开视线范围，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借记卡。

### **3、POS 交易后**

- 收银员交回签购单及卡片后，您应认真核对签购单上的交易日期、金额等是否正确，卡片是否为本人的卡片，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我行联系。

- 及时核对用卡情况，如有疑问，请及时联系我行营业网点或拨打我行 95528 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，恢复您的借记卡账户余额。

## **六、网络交易安全防范**

### **（一）网络欺诈主要风险**

#### **1、网络钓鱼**

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,从而盗用借记卡账户资金。如不法分子伪装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**

特洛伊木马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、借记卡资金被盗用等危害。

## **3、社交陷阱**

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借记卡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**

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、网站信息泄露

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，则极易发生借记卡账户资金盗用。

### （二）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。

## 七、电信诈骗安全防范

近年来，借记卡诈骗出现了一些新的常用手法，主要包括以下几种：

**手法一：假银行短信。**以银行或银联名义，发送借记卡商场消费或借记卡账户信息泄露等虚假短信，诱骗持卡人拨打短信中的电话号码后，假扮银行工作人员，以“账户升级”等理由，诱骗持卡人通过 ATM 或网上银行将存款转至某银行卡账户。

**手法二：假退款电话。**以政府机关、电力公司、电信等单位名义，编造退还税款、水电费、电话费等理由，直接打电话或者

通过录音电话，诱骗持卡人通过 ATM 转账，将钱划到其他账户上。

**手法三：假销售短信。**以出售廉价商品或违禁物品为由，诱骗持卡人汇款至某银行卡账户，并谎称未收到汇款，要求持卡人再次汇款，骗子始终不露面。

**手法四：假中奖短信。**以中奖为由，骗取身份信息、借记卡账户信息及密码，然后利用上述信息登录网上银行，以转账方式盗取持卡人的存款。

**手法五：假招工短信。**例如以高薪招聘为由，骗持卡人将报名费汇至某银行卡账户，并谎称未收到汇款，要求持卡人再次汇钱。骗子始终不露面。

**手法六：网银转账陷阱。**编造各种借口，骗持卡人开立网上银行账户并存款，然后通过网上银行转账方式将持卡人借记卡资金盗走。

为了防范此类陷阱，持卡人应掌握“四不”防范技巧，以保护借记卡资金安全：

**一、不相信。**政府机关、银行或公共事业单位通常不会直接与持卡人电话交谈涉及费用的问题，更不会直接“遥控指导”持卡人去 ATM 等没有银行工作人员在场的地方进行转账。接到这样的电话，应不予理睬。

**二、不回应。**对可疑的语音电话或短信不要回应，应直接致电相关公共事业单位或我行客户服务热线询问，以避免上当受骗。

**三、不泄露。**注意保护身份资料、账户信息，而且任何情况

下，也不要泄露借记卡密码。同时，密码作为银行卡的防护线，只有持卡人有权知道。任何人，包括银行工作人员，均无权询问密码。

**四、不转账。**为了银行卡资金安全，万万不可按照陌生人的“指导”进行 ATM 或网上银行操作，以免被骗。持卡人在进行不熟悉的 ATM 转账或网上银行业务时，应由熟悉此类业务的熟人进行指导。

此外，若持卡人发现已经被诈骗，应及时向当地公安机关报案，并配合公安机关做好调查、取证工作。

## **八、常见欺诈案例分析**

### **案例一：吞卡+假提示**

**欺诈手法：**欺诈分子在 ATM 插卡口处安装吞卡装置盗卡，并在 ATM 旁张贴假的银行告示，诱骗持卡人向冒充银行工作人员的欺诈分子说出借记卡密码后，从 ATM 上盗取存款。

**防范技巧：**遇到 ATM 故障，应待在原地拨打 ATM 屏幕上显示的银行服务电话，或拨打我行 95528 客服热线及时与我行取得联系。对 ATM 旁张贴的通知上的服务电话要谨慎识别。请谨记银行工作人员决不会向您询问密码。

### **案例二：侧录+窥号**

**欺诈过程：**欺诈分子在 ATM 插卡口处安装吞卡装置，在持卡人背后或在远处用望远镜窥视密码。等持卡人离开后，欺诈分子取出借记卡，用密码取款。

防范技巧：使用 ATM 取款时要防范可疑的人，如有陌生人靠近，请提高警惕，防止欺诈分子偷窥密码。

### **案例三：吞卡+假门禁或假键盘窃号**

欺诈过程：欺诈分子在 ATM 插卡口安装吞卡装置盗卡，在 ATM 键盘上贴假 ATM 键盘或安装假门禁，以电子方式窃取持卡人密码后，盗取存款。

防范技巧：在使用 ATM 时，要对易被改装的部位如：入卡口、出钞口、键盘及隐蔽探头等进行检查。当卡被吞以后，应在原地等候并立即拨打我行 95528 客户服务热线请求帮助。请谨记门禁不需输入密码。

### **案例四：侧录+伪卡复制**

欺诈过程：欺诈分子应聘餐厅服务员，并在客户结账时偷偷侧录磁条信息，之后复制伪卡并通过 ATM 完成取款盗刷。

防范技巧：刷卡消费时不要将借记卡交给他人操作，输入密码时应注意遮蔽。

### **案例五：伪基站+钓鱼链接+病毒**

欺诈过程：欺诈分子通过伪基站假冒通讯运营商、银行、学校等发送短信，在短信中嵌入钓鱼链接，通过积分换现金、信用卡提额、考试成绩等内容诱使客户点击，从而在客户手机中安装比病毒软件，获取客户信息以及发送至该手机的短信验证码等敏感信息。而后登陆客户网上银行或手机银行，盗取资金。

防范技巧：不点击短信中的链接，安装手机杀毒软件。

### **案例六：信息泄露+电话诈骗**

欺诈过程：欺诈分子从非法途径获取客户信息，例如购物、机票、冒充公检法等信息，利用社会工程学手段结合场景对客户进行诈骗，诱使客户主动将资金汇入欺诈分子账户或将用于转账的短信验证码主动告知欺诈分子。

防范技巧：联系官方客服了解详细情况，所有退款或购买操作均通过官方渠道进行。切勿相信所谓“安全账户”。

### **案例七：信息泄露+手机卡被停用**

欺诈过程：欺诈分子从非法途径获取客户信息，冒充客户通过运营商置换原手机 sim 卡，导致客户手机无法正常使用，从而获取到银行发送至客户的短信验证码，通过电子渠道操作客户银行账户，盗取资金。

防范技巧：保护好个人信息，开通微信等通知方式，及时发现账户异常。

## **九、挂失服务指南**

• 如果您的借记卡遗失、被盗或被冒用，请立即联系我行办理挂失，及时冻结账户，避免欺诈损失。我行持卡人可拨打 95528 客户服务热线办理口头挂失，并随后持有效身份证件到就近任一网点办理书面挂失手续。

• 浦发银行客户服务热线：95528