支付安全知识宣传材料之二

支付业务安全知识

江苏省支付清算服务协会

银行卡支付安全知识

如何安全使用银行卡

1. 在消费场所刷卡时，眼神不要离开自己的银行卡；

2. 在 ATM 机操作时，注意 ATM 机是否异常，操作完毕后，将凭条取走或撕毁，不要随意丢弃打印单据；

3. 尽快开通银行卡交易短信通知服务；

4. 将传统的磁条银行卡换成 IC 芯片银行卡，以降低被复制的风险；

5. 银行卡密码要及时更换；

6. 银行卡出现异常时，及时在就近的银行网点或自助设备上进行一笔刷卡交易，或留下查询存根，以此证明出事时银行卡就在自己身上；

7. 卡片的信息，包括 16 位卡号、卡片有效期以及卡片背后的 3 位验证码，绝对不能透露；

8. 认真阅读发卡银行提供的银行卡使用说明和安全防范要求，掌握基本的用卡常识；

9. 不要将银行卡与身份证件放在一起，以防同时被盗或丢失后造成严重损失；

10. 不要将卡号告知他人，不要回复要求提供卡号的可疑邮件及短信，也不要在公共场所使用的电脑里留下卡号信息；

11. 认真核对发卡银行按月邮寄的银行卡对账单，如发现不明交易，立即联系发卡银行；

12. 境外消费尽量使用银行卡，少带现金保安全。

银行卡安全使用小贴士

要在领卡后修改初始密码，不要设置易于猜中的密码。

要不定期地更换卡片密码，不要把密码透露给任何人。

要注意妥善保管银行卡片，不要出租转借卡片给他人。

要将卡片与身份证分开放，勿放一起以免被坏人盗用。

要留意刷卡周边可疑情况，不要在不安全终端上交易。

要在输入密码时进行遮挡，不要让交易卡片脱离视线。

要妥善保存私密信息载体，不要随意丢弃各交易凭证。

要及时核对确认交易信息，不要在未核对账单上签名。

要快速挂失丢失被盗卡片，不要耽搁时间致资金损失。

要在资金被盗时立即报案，不要轻信中奖等诈骗信息。

网络支付安全知识

在网络支付过程中，消费者应养成良好支付习惯，加强风险防范，确保网络支付安全。

选择适合自己的安全支付工具

1. 数字证书。电脑或手机上安装数字证书后，即使账户支付密码被盗，也需要在已经安装了数字证书的机器上才能支付，因此数字证书能够保障资金安全；

2. 短信验证码。是用户在支付时，银行或第三方支付机构通过客户绑定的手机，下发短信给客户的一次性随机动态密码；

3. 动态口令。无需与电脑连接的支付安全工具，采用定时变换的一次性随机密码与客户设置的密码相结合；

4.USB Key。连接在电脑 USB 接口上使用的一种支付安全工具，支付时需要插入电脑，才能进行支付。

网络支付安全提示

1. 确保终端安全，保证安全锁完好，及时更新杀毒软件，操作系统补丁。应从官方网站上下载安装银行和第三方支付机构的控件和软件；不轻易点击不明链接或他人发送的链接与文件；尽量不使用公共电脑进行支付交易，必须使用的，先查杀木马或病毒，并开启防火墙保护功能。

2. 查询到自己资金被盗后，及时记录单据号码并立即报警，保存相关网站截图和收到的银行提醒短信作为辅助凭证，及时和银行、第三方支付机构联系解决，冻结账户，防止资金损失扩大。

3. 在支付时注意订单内容，防止订单被替换后继续支付。

4. 使用网络支付时，务必充分使用安全工具或者产品，例如申请数字证书、开通手机动态口令、短信提醒等服务，以提高账户及交易的安全性。如经常进行网上支付，应前往银行办理网银专业版开通手续，在上网终端安装网银数字证书，确保银行账户安全。

5. 妥善保管敏感信息，如身份证、账户、银行卡、手机号等信息，不轻易提供给他人，不轻易在小网站或不知名的网站上预留以上信息。网络支付账号和密码应单独设置，不要和其他网上账户相同；妥善保管支付口令牌等支付安全工具，不要将其交付他人，使用完毕后应及时从电脑上取回，若遗失，尽快到银行办理挂失及补办手续。

6. 密码设置要具有独特性，不应设置一些简易的或者与本人生日、电话号码等关联的密码；短信验证码，动态口令等动态密码不提供给任何他人，任何索取短信验证码的行为都属于诈骗行为。

7. 申请网上支付服务时，可根据自己实际使用情况设定资金限额，以避免日后可能带来的经济损失。

8. 交易完成后不论系统提示成功与否，都要查询账户余额和交易明细。要定期查看历史交易明细并定期打印网络支付业务对账单，如发现异常交易或账务差错，应立即与银行或者支付机构联系，避免损失。核对支付信息时注意核对页面显示的“商户名称”、“商品名称”、“数量”和“总金额”等信

息，防止误付和错付。个人资料（联系电话、地址等）如有任何变更，及时通知银行或者支付机构进行修改，或通过客户端自行修改。

手机支付安全知识

应用手机支付注意事项

1. 用本人手机访问手机银行，不要将处于有效登录状态中的手机交给他人使用；

2. 转账、缴费等资金转出类业务按需开通，设定适当的资金限额并登记正确的本人手机号；如手机不慎丢失，尽快联系运营商挂失并补办手机号码；

3. 通过手机自带浏览器或经安全认证的浏览器访问正确的手机银行地址；

4. 尽量使用手机客户端登录，如果需要用浏览器登录，手机浏览器若提示“保存账户及密码信息”，选择不保存；关闭手机浏览器设置中的“保存账户及密码信息”功能，并定期清理浏览器中的缓存、Cookies 和表单等信息；

5. 在公共场合使用手机银行，输入密码时采取遮挡措施，避免他人窥视；

6. 平时最好关闭 Wi-Fi 自动连接，手动使用时，应看清 Wi-Fi 名称，尽量不在不明的 Wi-Fi 上进行网络支付；

7. 在登录手机银行或者支付机构网站时，最好不要直接通过浏览器，而应用银行或者第三方支付机构专门的应用程序；

8. 发现银行卡被盗刷，应及时与银行联系，冻结银行账户，并立即报警。

手机丢失怎么办

为防止手机被盗和丢失后造成资金损失，需做到以下几点：

1. 不要在手机中记录密码等敏感信息；

2. 手机丢失后，及时致电运营商，挂失手机号码；

3. 设置不同的支付密码和登录密码；实现密码保护双保险；

3. 致电银行，冻结手机网银服务；

4. 如手机绑定第三方支付、手机钱包等服务的，拨打服务商户电话进行业务冻结或挂失；

5. 微信、QQ 用户登录 110.qq.com，冻结账号；

6. 修改微博、微信、QQ 等密码。

移动支付安全知识

移动支付最常见的风险类型是信息泄露引起的账户被盗和诈骗，可采用以下手段保障移动支付的安全：

1. 双重身份验证。设置密码和验证码，即便手机被盗，小偷也不会知道账户密码和验证码，所以无从下手；避免“一码走天下”，在不同网站设置不同用户名和密码组合，避免使用连续、重复、生日、身份证号等简易、容易被猜中的密码，使用大小写字母、数字、符号组合的复杂密码，并定期更换。

2. 登录手机银行或支付机构网站时，尽量使用银行或第三方支付机构的手机应用程序，不要从任何非官方应用商店下载安装支付应用，因为它们可能存在盗取用户信息的恶意代码；不要直接通过浏览器进行操作。

3. 加强设备本身的安全性。如果用户手机内置指纹传感器，同时支付应用又支持指纹验证的话，应该开启这项功能；如果不支持，最起码要设置一个额外的锁屏密码。查看手机的隐私设置，确保应用程序访问权限的合理性。

4. 使用额度较小的信用卡或余额较小的借记卡，借记卡余额用完再从其他卡上转入资金，即使遭到盗刷，也可将损失控制在可承受的范围。

5. 使用可信任的网络连接。不要使用公共 WiFi 进行支付，即便用户的支付信息是加密的，也有可能被手段高超的黑客破解，获得支付账户、卡号、密码等信息。

6. 设置账户更改警报。开启支付服务账户改变警告的通知设定，例如改变密码、支付行为、绑定手机终端等，有助于即时了解支付账户的变化，信用卡同样广泛支持消费短信、微信提醒服务。

7. 确定收款人信息。转账时一定要确定收款人信息，不要轻信一些所谓“房东”、“好友”的信息，要在充分确认对方身份后再进行转账。

8. 为转账等交易设置每日每账户交易限额，确保账户支付在一定额度之内。