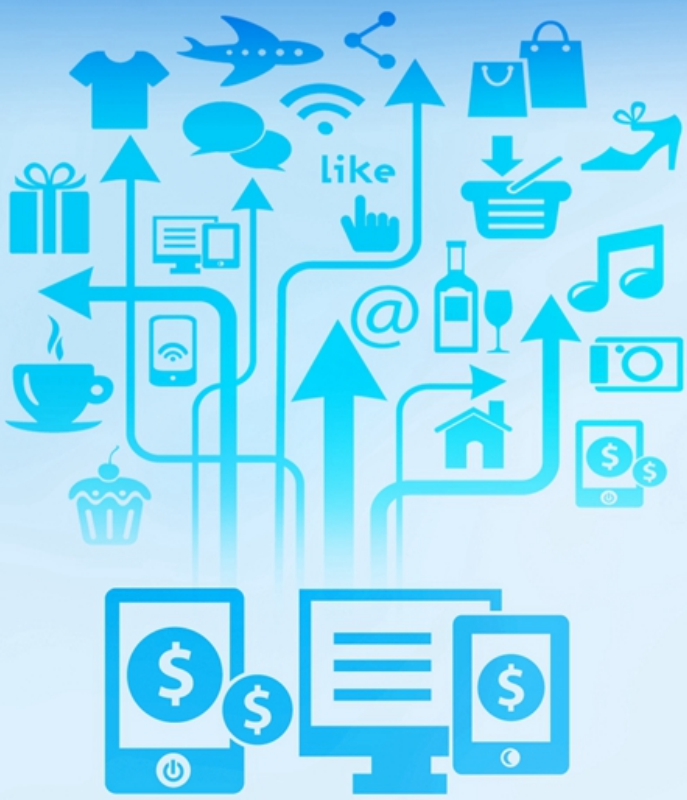

itBank
1234 5678 9012
国家网络安全
宣传周
China Cybersecurity Week
网络安全
一路随行
金融网络安全知识手册
NETWORK SECURITY

安全工具

Security Tools



安全工具相当于给你的账户或者资金上了一道道锁。如果能合理使用网络安全支付工具，能够大大降低网络支付风险，使你的支付更加安全，更有保障。目前，市场上主流的网络安全支付工具主要有下面几类：

一是数字证书。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，保障资金安全。

二是短信验证码。短信验证码是用户在支付时，银行或第三方支付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。

三是动态口令。无需与电脑连接的安全支付工具，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。

四是USB Key。连接在电脑USB接口上使用的一种安全支付工具，支付时需要插入电脑，才能进行支付。

用户可以根据自己的实际情况以及银行或支付机构的建议，选择适合自己的网络安全支付工具。

安全攻略
Security Strategy

一、保管好账号、密码和USB Key（或称Ukey、网盾、U盾等）

- 不要相信任何套取账号、USB Key和密码的行为，也不要轻易向他人透露您的证件号码、账号、密码等。
- 密码应尽量设置为数字、英文大小写字母、和特殊字符的组合，不要用生日、姓名等容易被猜测的内容做密码，并定期修改。
- 如果泄露了USB Key密码，应尽快办理补发或更换业务。

二、认清网站网址

网上购物时请到正规、知名的网上商户进行网上支付，交易时请确认地址栏里的网址是否正确。

三、确保计算机系统安全

- 从银行官方网站下载安装网上银行、手机银行安全控件和客户端软件。
- 设置Windows登录密码，WindowsXP以上系统请打开系统自带的防火墙，关闭远程登录功能。
- 定期下载并安装最新的操作系统和浏览器安全补丁。
- 安装防病毒软件和防火墙软件，并及时升级更新。

四、提升安全意识

- 使用经国家权威机构认证的网银证书，建议同时开通USB Key和短信口令功能。
- 开通短信口令时，务必确认接收短信的手机号码为本人手机号码。
- 不要轻信手机接收到的中奖、贷款等短信、电话和非银行官方网站上的任何信息。

- 不要轻信假公安、假警官、假法官、假检察官等以“安全账户”名义要求转账的电话欺诈。

- 避免在公共场所或他人计算机上登录和使用网上银行。退出网上银行或暂时离开电脑时，一定要将USB Key拔出。

- 操作网银时建议不要浏览别的网站，有些网站的恶意代码可能会获取您电脑上的信息。

- 建议对不同的电子支付方式分别设置合理的交易限额，每次交易都请仔细核对交易内容，确认无误后再进行操作。在交易未完成时不要中途离开交易终端，交易完成后应点击退出。

- 定期检查核对网上银行交易记录。可以通过定制银行短信提醒服务和对账邮件，及时获得银行登录、余额变动、账户设置变更等信息提醒。

五、网上银行安全工具组合（安全等级根据★的数量由高到低）
建议客户选择安全等级高的工具组合！

安全工具组合	安全级别
USB Key+短信口令	★★★★★
网银证书+短信口令	★★★★
USB Key	★★★
网银证书	★★
短信口令	★★
普通登录	★

网络安全重在防范，一旦发现被骗，要在第一时间联系银行、支付机构，采取相应应急措施，同时向当地警方报警。

（一）已经在钓鱼网站输入了密码怎么办？

1.如果您还能登录您的账户：请立刻修改您的支付密码和登录密码。同时，进入交易明细查询查看是否有可疑交易。如有，须立刻致电银行或支付机构的客服电话。

2.如果您还输入了银行卡信息：请立刻致电银行申请临时冻结账户或电话挂失（此时您的银行账户只能入账不能出账）。

3.如果您已经不能登录：请立刻致电银行或者支付机构的客服电话，申请对您的账户进行暂时监管。

4.使用最新版的杀毒软件对电脑进行全面扫描，确保钓鱼网站没有挂木马。如果发现有，请在确认电脑安全后再次修改登录与支付密码。

（二）发现账户资金被盗怎么办？

1.要在第一时间修改账户密码，同时转出剩余资金。

2.进入交易管理，查找可疑交易，保留对非授权的资金交易。

3.如果被盗的是银行卡账户的话，请立刻致电银行申请临时冻结账户或电话挂失(此时您的银行账户只能入账不能出账)。

1、什么是金融IC卡？

答：金融IC卡是由商业银行（信用社）或支付机构发行的，采用集成电路技术，遵循国家金融行业标准，具有消费信用、转账结算、现金存取全部或部分金融功能，可以具有其他商业服务和社会管理功能的金融工具。

它具有数据存储容量大，安全性高等特点，可实现非接触式（“闪付”）应用，是基于传统金融支付并可无缝延伸至其他行业小额支付的智能化产品。多应用金融IC卡能够实现政府公共服务管理功能和金融支付功能，可以支持跨行业、跨平台、多功能的应用。

2、如何使用金融IC卡？

答：金融IC卡分为接触式与非接触式（“闪付”）两种。接触式金融IC卡，可通过插入受理终端的读卡槽实现在POS和ATM上使用。如果是非接触式金融IC卡（或称闪付卡），用户可在支持银联“闪付”的非接触式支付终端上轻松一挥便可快速完成支付。一般来说，单笔金额不超过1000元，无需签名和输入密码。

3、相比于传统磁条卡，金融IC卡的优势具体体现在哪里？

答：金融IC卡的优势主要体现在三个方面。一是安全性高。金融IC卡的信息存储在智能芯片中，卡内信息难以复制，加上多重的交易认证流程，可以有效保障持卡人银行账户资金安全。二是快捷便利。金融IC卡除具备磁条卡所有功能外，还可以进行小额快速支付，轻松一挥便可支付，方便快捷。三是一卡多用。金融IC卡可用于社保、交通、医疗、教育等公共领域。

4、为什么说金融IC卡比一般的银行卡安全？

答：传统银行卡磁条技术相对简单，磁条信息易被复制，通过使用磁条信息盗录装置复制银行卡磁道信息就可以伪造磁条银行卡，通过针孔摄像机在自助机终端上偷录持卡人密码就可以盗用磁条银行卡，从而给持卡人和发卡机构造成较大损失。

而采用芯片技术能有效防范这类情况的发生。金融IC卡的芯片实现了硬件升级，完善的密钥体系、脱机认证、联机双向认证等更是保障了卡片的防伪性及交易的安全性。世界各地的实践经验表明，在推广使用采用芯片技术的金融IC卡后，银行卡伪卡案件大幅减少。

5、金融IC卡产品主要分为哪些类型？

答：各商业银行已陆续推出众多各具特色的金融IC卡产品。按功能分，可分为借记卡、贷记卡、准贷记卡、电子现金等产品；按信息存贮介质分，可分为仅有芯片的金融IC卡和既有芯片又有磁条的双介质卡(业界又称“复合卡”)；按行业应用分，包括市民卡、社保卡、公交卡、大学城一卡通等类型。

6、未来金融IC卡会给人们的生活带来什么改变？

答：金融IC卡具有智能芯片，可集社保、交通、医疗、教育、通讯、购物、娱乐、水电煤缴费等行业应用于一体，实现“一卡多用”，让现在被各类卡片充满的钱包“瘦身”。同时，其非接触式支付功能可广泛应用于超市、便利店、百货、药房、快餐连锁等零售场所和菜市场、停车场、加油站、旅游景点等公共服务领域，轻轻一挥便可支付，提高持卡人生活舒适度和幸福感。

7、如何知道我的金融IC卡是否具有非接功能？这种功能在哪里可以使用？

答：凡是金融IC卡卡面上具有“Quick Pass”标识的卡片就具有非接快速支付功能，也就是即挥即刷、快捷“闪付”的功能，它可以在贴有“Quick Pass”标识的终端上快速刷卡支付。目前全国受理金融IC卡的非接触式支付终端超过100万台，覆盖超市、便利店、百货、药房、快餐连锁等零售场所和菜市场、停车场、加油站、旅游景点等公共服务领域。

8、我该如何办理金融IC卡？

答：您只要携带有效身份证到各大商业银行网点，即可申请办理金融IC卡。办理前可先致电银行客服热线，确保该网点可受理该业务。

常见安全风险
Common Security Risks

一、 网络钓鱼

网络钓鱼是指不法分子通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件或短信、即时通讯信息等，引诱收信人给出敏感信息（如用户名、口令、帐号 ID 或信用卡详细信息），然后利用这些信息假冒受害者进行欺诈性金融交易，从而获得经济利益。受害者经常遭受重大经济损失或个人信息被窃取并用于犯罪的目的。

二、 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编写木马程序的不法分子所控制，从而造成信息文件被修改或窃取、电子账户资金被盗用等危害。

三、 社交陷阱

社交陷阱是指有些不法分子利用社会工程学手段获取持卡人个人信息，并通过一些重要信息盗用持卡人账户资金的网络诈骗方式。例如不要轻信信用卡中心打来的“以提升信用卡额度”为由的诈骗电话。

四、 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。

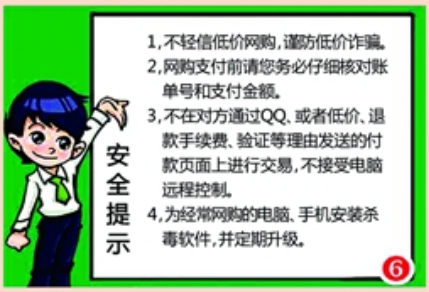
五、 信息泄露

目前某些中小网站的安全防护能力较弱，容易遭到黑客攻击，不少注册用户的用户名和密码便因此泄露。而如果用户的支付账户设置了相同的用户名和密码，则极易发生盗用。

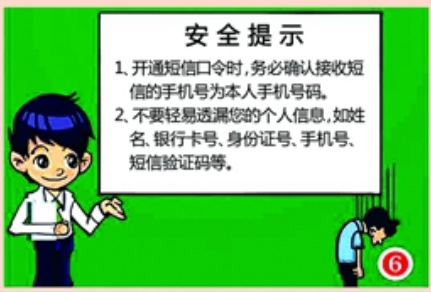
经典案例
Classic Cases

（一）掌上银行短信诈骗篇

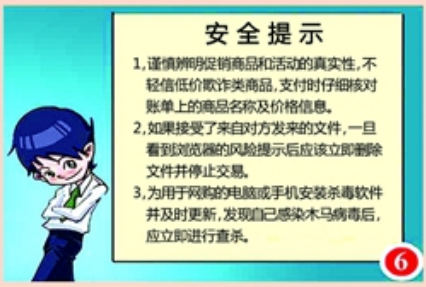
（二）谨防钓鱼网站欺诈篇



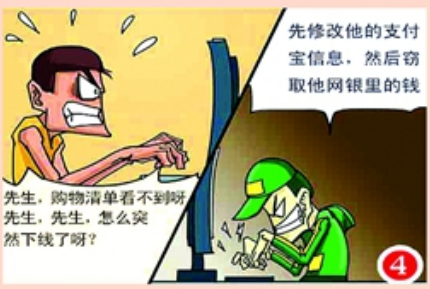
（三）保护个人信息安全篇

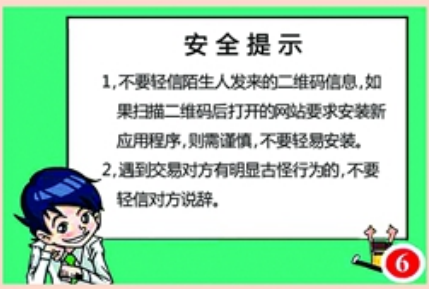


（四）二手交易当心网购木马篇



（五）二维码暗藏木马篇





如何应对智能手机APP使用风险

Security Risks in the APPs

一、从正规渠道谨慎下载APP

请尽量选择从手机软件的官方网站、信誉良好的第三方应用商店等正规渠道下载应用程序。例如iPhone手机建议到苹果官方的APP Store下载，而Android手机可以选择安卓市场、中国移动的应用市场等，否则容易下载“山寨应用软件”导致被盗用个人信息，甚至引起财产损失。

二、 关注APP权限获取问题

用户在安装APP时候，能够清晰地看到APP声明的全部行为和权限，用户也有权利允许或者拒绝APP所要求的权限。所以，用户自身在应用程序安装时应该认真查看应用程序类型及其申请的权限，判断是否有申请不必要的权限，如果有则要谨慎选择是否安装，如果发现可疑，应果断中止安装。

三、 不轻易点击APP弹出广告

在使用移动APP时，不要轻易点击由APP弹出的广告链接，链接可能隐含不安全因素，带来消耗手机流量、泄露个人信息、导致手机中毒、甚至造成财产损失等风险。同时也不要轻易点击任何陌生链接或扫描(下载)来源不明的下载二维码。

四、 定期检查智能手机

除下载安装APP时的小心谨慎外，可安装可靠的移动安全防护软件，并时常为手机“体检”，正规安全防护软件会及时更新病毒库，提升智能手机安全性。

手机银行使用注意事项

Mobile Banking Caution

一、 请您务必从正规的渠道下载手机银行、支付软件，定期更新该类APP的应用。请小心识别虚假网站，不要以非正规链接的形式登录手机银行，若有任何怀疑，请立即致电所使用的银行客户服务热线。

二、 确保您的移动设备安全，建议使用手势密码或口令保护移动设备，并将设备设置为一段时间后自动锁定。切勿尝试破解或修改设备，因为这可能会使设备受到恶意软件的攻击。

三、 如果您使用Wi-Fi联网，请在确保无线网络安全的情况下再连接至您的手机银行站点或应用程序：切勿通过不安全的无线网络发送敏感信息，例如酒店或咖啡厅里的无线网络；如果您要在公共场合下查看银行帐户(如图书馆或咖啡厅)，请注意安全并建议在结束查看后在安全的网络环境下更改密码。

四、 如果APP具备保存密码的选项，建议您不要勾选，每次登录时均重新输入登录密码，同时建议设置较为复杂的登录密码、支付密码等。不要使用生日、电话号码、车牌等容易猜测的密码，同时注意密码的保密，不要将交易过程中的各类密码信息告知他人。

五、 如果您更改了手机号码，请及时通知银行做信息变更。如遇到手机被盗，请及时致电银行挂失银行卡。

六、 在使用交易类、银行类APP进行支付或者转账的过程中保证手机在个人身边，不要在操作过程中远离手机，如确有紧急事项，请结束当前交易并退出APP系统。同时在全部使用完毕后建议结束APP进程，不要继续在后台运行系统。