了解新型支付工具，防范支付风险

伴随着支付服务市场的竞争愈发激烈，金融创新日益增长，新型支付方式一方面对经济的发展和日常生活的便利起到了积极的支撑作用，另一方面也带来了风险和问题。今天，小编带您了解各种支付方式，普及如何正确识别和防范风险。

了解新型支付工具

1、第三方支付

常见的第三方支付机构包括支付宝、微信支付、快钱支付等。第三方支付具备一定安全性，支付成本较低，且由于付款人的信用卡信息或账户信息只需告知支付中介，无需告诉收款人，一定程度上减少信息丢失风险。

第三方支付的潜在风险

- 信息暴露给第三方支付平台——付款人的银行卡信息将暴露给第三方支付平台，如果第三方平台的信用度或信息系统安全有限，将可能给付款人带来重大风险。
- 资金寄存风险——第三方支付平台是非金融机构，与银行、证券、保险等金融机构相比资金寄存能力存在差距，资金寄存具有一定风险。
- 网络安全问题——由于第三方支付平台涉及网络问题，可能遭受黑客等袭击。

2、移动支付

移动支付也称手机支付，按支付账户的性质，可以分为银行卡支付、第三方支付账户支付、通信代收费支付三种模式。上文提到的第三方支付主要从支付转账的渠道进行定义，而移动支付则是支付转账的媒介。

移动支付属于电子支付方式的一种，因而具有电子支付的特征，其移动性、及时性、定制化的特点，消除了距离和地域的限制，使得账户交易更加简单方便。目前移动支付主要支付方式有：短信支付、扫码支付、指纹支付、声波支付等。

移动支付潜在风险

- 交易安全问题尚未妥善解决——信息的机密性、完整性、真实性、身份验证、手机的安全性及移动支付各个环节中法律保障尚不健全。
- 资金寄存风险——移动支付中第三方支付平台是非金融机构，与银行、证券、保险等金融机构相比资金寄存能力存在差距，资金寄存具有一定风险。
- 网络安全问题——大量手机支付类病毒、手机漏洞等均给手机用户支付安全造成了严重威胁。

如何防范支付风险

小编在此仅列举几个较为常见的诈骗形式。

1、常见形式

（1）利用网络游戏装备及游戏币交易实施诈骗。

（2）利用网上银行实施诈骗。（比如犯罪分子制作与一些银行官网相似的“钓鱼”网站盗取网银信息）

（3）网购诈骗。

（4）群发银行卡透支、消费短信实施诈骗。（犯罪分子向受害人发送“银行卡刷卡消费”、“信用卡透支”等内容的短信，当接收者打电话询问时，犯罪分子便分别扮演“银行”、“银联”等角色，层层设下圈套，诱骗事主将银行卡内资金转移到“安全账户”。）

2、如何防范风险

（1）保管好账号、密码和网盾

- 请您谨记：任何情况下银行都不会通过电子邮件、信函、电话或手机短信等方式，主动要求您提供账号、密码或网上银行网盾。
- 密码应尽量设置为数字、英文大小写字母的组合，不要用生日、姓名、地址等容易被猜到的内容做密码。
- 如果泄露了网盾密码，应尽快办理挂失、补办或更改业务。

（2）认清网站网址

- 认清网上银行的官方网站，不要通过其他网站链接访问。
- 网上购物时请到正规、知名的网上商户进行网上支付，在进行网上支付交易时，请确认浏览器地址栏里的银行网址是否正确。

（3）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。
- 设置电脑登录密码，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。
- 长时间无人操作电脑时，中断计算机网络连接或关机。

（4）提升安全意识

- 建议同时开通“网盾”和短信口令功能，通过安全保护措施的联合应用提升安全防护等级。
- 开通短信口令时，确认接收短信手机号为本人手机号码。

- 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，如遇有问题，一定拨打该银行全国统一客户服务热线以确认。
- 避免在公共场所或他人计算机上登录和使用网上银行。
- 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，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。

（以上资料取自银监会消保局与中央金融团工委共同设计编写的大学生应知应会金融知识材料）