国家网络安全宣传周
China Cybersecurity Week

2018 国家网络安全宣传周·金融日

中国人民银行
THE PEOPLE'S BANK OF CHINA

网络安全为人民 | 网络安全靠人民

增强支付环境安全
推进普惠金融发展

主办单位：中国人民银行

国家网络安全宣传周
China Cybersecurity Week

中国人民银行
THE PEOPLE'S BANK OF CHINA

2018 国家网络安全宣传周·金融日

网络安全为人民 | 网络安全靠人民

增强支付环境安全
推进普惠金融发展

主办单位：中国人民银行

防范移动支付诈骗

移动支付诈骗是指用户在使用移动终端进行支付时，不法分子利用黑客技术，终端漏洞或用户疏忽等，盗取用户信息，骗取受害人钱财的行为。

案例九：盗取手机ID诈骗

李先生发现自己的某品牌手机被锁定，随后注册该品牌手机ID的邮箱收到一封勒索邮件，称可以解锁手机但需支付2000元现金。原来，不法分子通过黑客技术，攻破李先生的手机账号并篡改了手机ID密码，再登录更改账户名，最后通过“查找我的手机”远程锁定手机并实施勒索。

案例十：微信支付诈骗

赵先生经营一家化妆品微店，一位微信昵称叫“美美”的网友加了赵先生的微信后，表示想买一瓶眼霜，并用二维码支付。

由于赵先生对二维码支付不熟，在“美美”的指导下，将自己的付款二维码发送给了“美美”，随后他收到银行短信，提示微信绑定的银行卡消费1500元。赵先生遂与“美美”核实，却再也联系不上，此时才明白被骗了。

安全提示：

- 保护好个人信息，尤其是银行卡卡号、支付宝账号和密码等敏感信息；
- 卸载带有支付功能的手机应用时，应先检查是否已解除银行卡绑定；
- 要通过官网或正规应用市场下载安装软件。

防范指纹识别诈骗

指纹识别诈骗是不法分子利用受害人使用指纹解锁和指纹支付过程中的漏洞实施诈骗的行为。

案例十一：盗用指纹诈骗

姜先生的手机解锁和支付需要指纹识别。一日姜先生和朋友在酒吧喝酒，在付费时姜先生使用了指纹支付。随后，其朋友送醉酒的姜先生回家，在姜先生熟睡时，用姜先生的指纹支付向自己转账5200元，并删除了姜先生手机上的转账记录和扣款短信。

安全提示：

- 若手机发生摔碰，应及时检查指纹解锁功能是否正常；
- 在使用指纹验证前，检查指纹触摸键上是否有其他异物；
- 开通指纹支付后，应限额并妥善保管手机，避免被人盗用；
- 尽量避免他人的指纹录入到自己的手机中。

防范网购诈骗

网购诈骗是不法分子利用受害人在网购过程中的疏忽来实施的诈骗。

案例十二：网购退款诈骗

陈女士在某网购平台上购买了一件价格几十元的物品，因对物品不满意申请退款。经沟通，网店同意退款并指导陈女士通过某支付平台办理退款手续，款项很快就退回至陈女士的银行卡，但金额却为1万元。网店的电话紧跟而至，声称由于误操作，错转成了1万元，要求陈女士把钱退回到指定的账户，否则就会报警。幸好陈女士警惕性较高，立即向公安机关报案，未造成资金损失。

经调查，陈女士在通过某支付平台办理退款时，实际上是点开了支付平台的贷款页面并操作成功，而不法分子谎称是其退款操作错误，要求陈女士退回，以此实施诈骗。

安全提示：

- 不点击陌生人发送的链接，不扫描陌生人发送的二维码；
- 网购退款时，要在电商平台的官方网站操作；
- 注意鉴别网址真伪，谨防账号密码被盗；
- 网络购物要留个心眼，千万别贪小便宜上大当。

提升安全意识，培养良好习惯

- 经常用于网络支付的银行卡不要存放太多资金，设置每日网络消费、转账限额；
- 签约短信通知服务和盗刷保险服务，可以为资金财产安全保驾护航；
- 不同网络支付账号建议设置不同密码；
- 用于网络支付的电脑或移动终端应安装安全软件，并定期进行扫描；
- 不要点击来历不明的链接，在进行网络支付或退款等操作时应登录正规网站；
- 不要告诉他人网络支付的密码和验证码等关键信息；
- 不要登录非法网站，避免电脑或移动终端被植入木马病毒。

金融知识课堂

之支付安全你、我、他

一、个人银行账户分类管理是什么?

自2016年12月1日起，个人银行账户实行分类管理，分为Ⅰ类、Ⅱ类、Ⅲ类账户，不同类别的账户有不同的功能和权限。个人在银行开立账户，每人在同一家银行只能开立一个Ⅰ类户，如果已经有Ⅰ类账户的，再开户时，则只能是Ⅱ、Ⅲ类账户。

Ⅰ类账户是“钱箱”

个人的工资收入等主要资金来源都存放在该账户中，安全性要求较高，主要用于现金存取、大额转账、大额消费、购买投资理财产品等。

Ⅱ类账户相当于“钱夹”

个人日常刷卡消费、网络购物、网络缴费通过该账户办理，可购买投资理财产品。

Ⅲ类账户就相当于“零钱包”

用于金额较小、频次较高的交易，适用于移动支付。

二、个人账户转账业务的新增规定有哪些?

增加转账方式——自2016年12月1日起，银行和支付机构提供转账服务时，向存款人提供实时到账、普通到账、次日到账等多种转账方式选择，存款人在选择后才能办理业务。

调整转账时间——除向本人同行账户转账外，个人通过ATM（自助柜员机）转账的，发卡银行在受理24小时后办理资金转账。在发卡银行受理后24小时内，个人可以向发卡银行申请撤销转账。受理银行应当在受理结果界面对转账业务办理时间和可撤销规定做出明确提示。

三、什么是小额免密免签?

小额免密免签是中国银联为持卡人提供的一种小额快速支付服务。当持卡人使用具有“闪付”功能的金融IC卡或支持“银联闪付”的移动设备，在指定商户进行一定金额（境内1000元人民币，境外以当地限额为准）内的交易时，只需将银行卡或移动设备靠近POS机等受理终端的“闪付”感应区，即可完成支付。支付过程中，持卡人不会被要求输入密码，也无需签名。

四、开通了小额免密免签功能的银行卡遗失怎么办?

1.与正常的银行卡挂失一样，拨打发卡银行服务热线进行电话挂失或者前往银行柜台办理挂失手续；

2.对于挂失之前72小时内发生的小额免密免签盗刷交易，在挂失后按照发卡银行流程申请赔付；

3.发卡银行在接收到持卡人申请赔付的5个工作日内向中国银联提交补偿申请；

对于审核确认的，中国银联在2个工作日内将资金返还至持卡人账户。

五、如何有效保护自身银行卡信息安全?

1.妥善保管好自己的身份证件、银行卡、网银U盾、手机，不借给他人使用，一旦丢失要立即挂失；

2.开通银行账户变动短信提醒，仔细核对交易业务类型、交易商户和金额是否正确，关注账户变动情况，定期检查账户资金交易明细和余额；

3.不随意丢弃银行卡消费或ATM交易的凭证；

4.不要轻易透露身份证号码、账号、银行卡等信息，不要相信任何索要银行卡密码和验证码的行为；

5.不向银行和支付机构业务流程外的任何渠道提供银行卡密码和验证码，不向任何人发送带有银行卡信息和支付信息的图片。

六、手机丢失怎么办?

1.挂失手机卡：致电运营商挂失、冻结手机卡，并及时到运营商网点补办；

2.冻结手机银行账户：通过银行客服电话/银行网点/网银渠道冻结或销户；

3.挂失云闪付：拨打银行服务热线或到银行柜台挂失；

4.冻结微信账户：登录http://110.qq.com，通过QQ号或手机号冻结微信；

5.冻结支付宝账户：登录支付宝-安全中心-应急服务。

国家网络安全宣传周

China Cybersecurity Week

网络安全 一路随行

2018年金融网络安全宣传手册

CYBERSECURITY

中国人民银行 THE PEOPLE'S BANK OF CHINA

四川 · 成都

《网络安全法》

这些内容你要懂

《中华人民共和国网络安全法》（以下简称《网络安全法》）是我国第一部全面规范网络空间安全管理方面问题的基础性法律，由全国人民代表大会常务委员会于2016年11月7日公布，自2017年6月1日起施行。

一、《网络安全法》的基本原则是什么？

（一）网络空间主权原则。网络空间主权是国家主权在网络空间中的自然延伸和表现，没有网络安全，就没有国家安全。

（二）网络安全与信息化发展并重原则。既要推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，又要建立健全网络安全保障体系，提高网络安全保护能力，做到“双轮驱动、两翼齐飞”。

（三）共同治理原则。网络空间安全保护需要政府、企业、社会组织、技术社群和公民等网络利益相关者的共同参与。

二、《网络安全法》禁止哪些个人和组织的网络行为？

不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家，破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

三、发现他人有危害网络安全的行为时，我们应该如何处理？

向网信、电信、公安等部门举报。

四、发现网络运营者违反《网络安全法》相关规定，侵犯个人权益的，我们有哪些权利？

有权要求网络运营者删除个人信息，发现网络运营者收集、存储的个人信息有错误的，有权要求网络运营者予以更正。

安全攻略及典型案例

防范电信诈骗

电信诈骗（又称非接触性诈骗或远程诈骗）是指不法分子以非法占有为目的，利用手机短信、电话、网络电话、互联网等方式，以虚构事实或隐瞒事实真相的方法，骗取受害者财物的行为。

案例一：欢乐购诈骗

李先生手机收到短信，称其获得980元抢购iPhone X的机会。李先生购机后发现，新购手机非常不好用，明显是山寨货。

案例二：贫困助学诈骗

某大学新生小徐，先接到自称是教育部门的电话，让她办理助学金的相关手续。随后又接到另一个电话，称有一笔2600元的助学金需尽快领取，并要求她将9900元学费汇入一个指定账号，半小时后会返还学费并发放助学金。小徐完成操作后发现对方电话关机，才明白上当受骗了。万分难过的她当天晚上突然晕厥，最终经医院抢救无效去世。

安全提示：

- 凡是谈到银行账户信息的，一律挂掉；
- 凡是谈到中奖的，一律挂掉；
- 凡是谈到“电话转接公检法”的，一律挂掉；
- 凡是自称领导、同事要求汇款的，一律不管；
- 凡是告知“家属”出事需要先汇款的，一律不管。

警惕伪基站

伪基站是不法分子利用计算机与通讯技术伪装成运营商的假基站。通过冒用他人手机号码强行向用户手机发送诈骗、广告推销等短信息。

案例三：冒充运营商诈骗

张先生收到号码“10000”发来的一条短信，称张先生有大量积分，可以兑换一笔金额不小的话费。张先生随后点击了短信中的链接，进入兑换话费的网页，并按提示输入了自己的银行卡卡号和支付密码。张先生等了几天，说好的话费却迟迟没有到账，反而发现自己的银行卡被转走两万余元。经查张先生是中了伪基站的诈骗圈套。

案例四：冒充银行诈骗

李女士正在玩手机，突然收到一条XX银行发来的银行卡消费积分兑换短信，没有多想就点开了链接，并按提示输入了自己的银行卡卡号和身份证号码，又输入了XX银行短信发来的验证码，没想到短短数十秒后，就收到多条共计转款99998元的短信，李女士这才意识到自己被骗了。

安全提示：

- 发现手机信号突然中断，应提高警惕，因为靠近伪基站时，手机一般会脱网，几秒后才恢复正常；
- 当收到“中奖”“转账”等短信时，一定要提高警惕，不要轻易点击短信中的链接，更不要转账汇款；
- 不要轻信各种积分兑换，正常的积分兑换应通过官方渠道；
- 手机要安装安全防护软件，它们可以有效拦截垃圾短信。

警惕钓鱼Wi-Fi

钓鱼Wi-Fi是不法分子部署的与免费Wi-Fi相似的假Wi-Fi。当受害人连接钓鱼Wi-Fi后，手机会自动下载木马病毒，不法分子可据此截取手机中的信息，包括银行卡、微信、支付宝、游戏等账号和密码都有可能被记录下来。

案例五：钓鱼Wi-Fi诈骗

张女士在一家商场内连接了一个没设密码的Wi-Fi，随后在某网购平台上对商场一件衣服进行比价，由于价格便宜近一半，她毫不犹豫地通过手机支付在该网购平台购买了这件衣服。不久，张女士的手机收到短信提示，其信用卡被盗刷4笔，总金额高达8000多元。

安全提示：

- 谨慎使用免费Wi-Fi；
- 拒绝来路不明的Wi-Fi，尽量选择正规来源的Wi-Fi；
- Wi-Fi连接方式建议设置为手动，或者关闭Wi-Fi自动连接功能；
- 不要使用破解Wi-Fi密码的软件，谨防被此类软件盗取隐私；
- 使用公共场所的Wi-Fi不要输入账号、密码或个人敏感信息。

防范二维码诈骗

二维码诈骗是不法分子通过替换商户的收款码、共享单车二维码、罚单二维码等方式更改收款账户，或发布隐藏有木马病毒的二维码，一旦受害人扫码支付，便可轻松获取受害人的钱财。

案例六：木马病毒二维码诈骗

倪女士经营一家网店。前不久，一位买家在准备支付时，希望倪女士通过扫描二维码方式进行结算。倪女士为得到对方“好评”，便用手机扫描了对方发来的二维码，随后出现一个链接网址，点击后很久也没显示成功，且手机变慢。倪女士立即用电脑登录支付宝，发现银行卡上的9万元已被转走。

案例七：假冒执法罚单诈骗

张女士发现自己路边停放的车上被贴了罚单，上面还印有快速缴费二维码，张女士随即扫描该二维码并缴纳罚款。事后，经朋友提醒，张女士打电话咨询交管部门，才发现扫描了假的二维码。

安全提示：

- 不要随便扫描未知二维码；
- 扫描后若要求填写个人账户信息的，坚决拒绝；
- 手机安装安全软件，定期对手机进行安全扫描，确保手机使用的安全。

警惕恶意充电宝

病毒充电宝是被不法分子植入木马病毒的充电宝，通常放置在公共场所，一旦受害人连接充电，手机便会自动下载木马病毒，不法分子通过读取受害人通信录、银行卡、支付宝等的信息实施诈骗、勒索等非法活动。

案例八：恶意充电宝诈骗

任女士某次出差途中，手机没电了，恰巧周围没有充电设备，于是借用一名男士的充电宝。次日，任女士接到陌生电话，对方称手里有任女士手机中的所有信息，包括一些重要的客户资料，向任女士索要赎金。经调查，任女士的信息泄露源头是借用他人有病毒的充电宝充电造成的。

安全提示：

- 从正规渠道购买充电宝；
- 尽量不借用陌生人充电宝，以免中了某些不法分子的招；
- 最好使用电源方式给手机充电，谨慎使用公共场所提供的充电设备；
- 手机在连接充电宝后，若出现“信任”选项，不要点击。