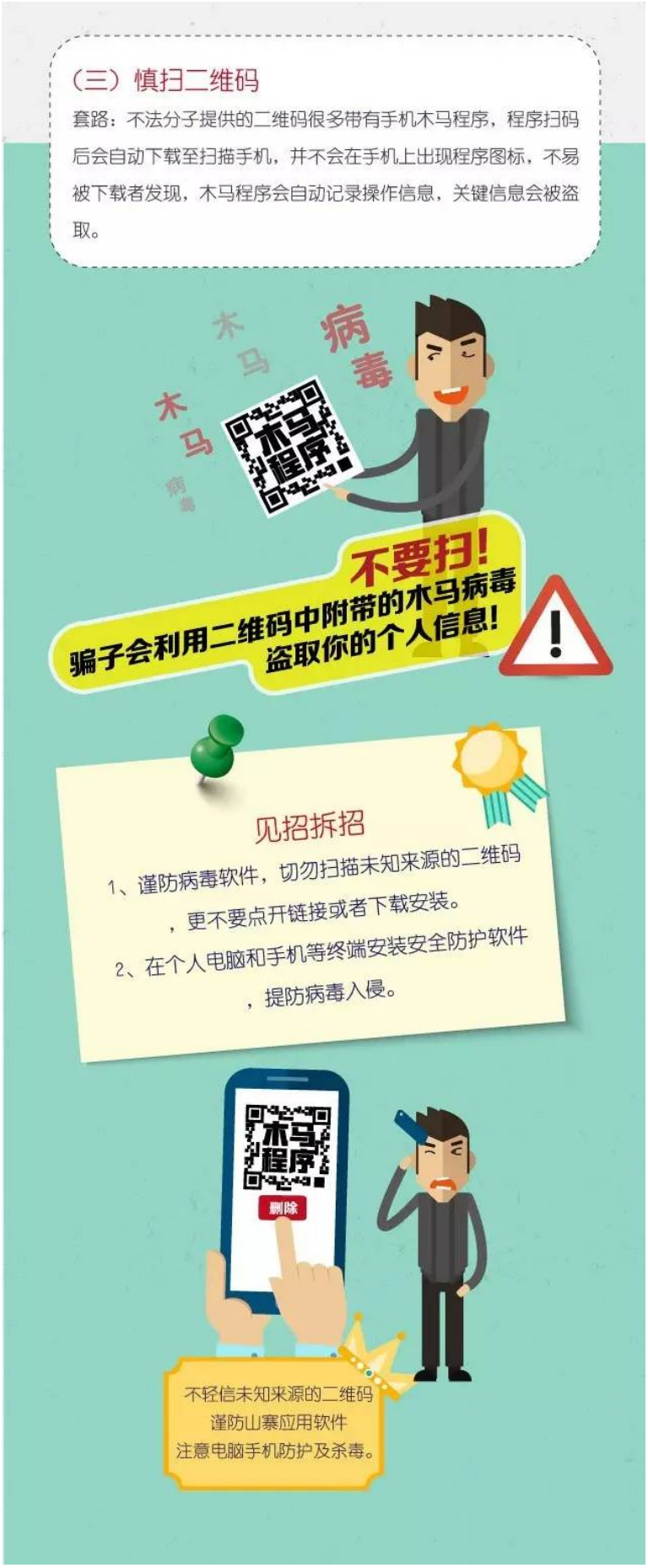

中国银行
BANK OF CHINA
信用卡
Credit Card
诈骗有套路，防骗有招数
安全用卡专题宣传
谨防电信诈骗
（一）“小利小惠”不可信
套路：不法分子假冒银行电话或发送虚假链接，以提升额度、免费赠礼、积分兑换等为诱饵，骗取信任，向客户骗取信用卡卡号、有效期、卡背面数字验证码、短信验证码等重要敏感信息，在掌握相关信息后盗取客户卡片资金。
“您好，这里是**银行，根据您的用卡记录，可以为您提升额度，跟您确认一下您的信用卡信息……”
注意啦！
他正在冒充银行电话骗取你的信息
见招拆招
1、卡片限本人使用，请勿将卡片转借他人。
2、信用卡的重要支付信息切勿告诉他人。银行不会向持卡人索取短信验证码，如有人索要可判定为诈骗，请立即报警。
“您好！您的信用卡可能存在安全风险，请您点击以下链接，提高安全系数，https:safe/955**/AQzx/123”
诈骗电话
删除
小心啦！
诈骗分子会利用短信链接盗取你的信息！


（二）未知电话不盲从
套路：不法分子利用伪基站假冒银行、电信运营商的官方客服号码（如955**）名义向持卡人发送短信或打电话，谎称持卡人的银行卡在某处消费或卡的信息资料被泄漏，诱骗持卡人拨打虚假短信中指定的电话号码，从而进一步通过电话诱骗持卡人进行转账操作。
您的信用卡 15日10时45分成功消费30,000元，如非本人操作，请立即拨打此号码：******
小心啦！
拨打虚假短信中电话，会被诱骗转账哦！
见招拆招
1、对可疑的语音电话或短信不回应；直接致电相关单位或发卡银行客服热线询问。
2、千万不可按照陌生人的“指导”进行ATM或网上银行操作。
电话设置
陌生电话号码加入黑名单
13*********
加入黑名单
提高警惕！
对陌生号码不接不回不信！


（三）远离“黑”中介
套路：不法分子利用持卡人想办理高额卡片心理，收取中介费为持卡人办理信用卡，骗取信息后盗取资金。
“我可以帮你办高额信用卡！”
别信他！
要你交中介费，还会盗取你的个人信息！
见招拆招
1、选择正规银行渠道办理信用卡；
2、注意个人身份材料和隐私保护。
THE BANK
很放心！通过正规渠道办理业务，安全有保障！


网购消费要小心
（一）警惕低价陷阱
套路：不法分子利用受害者好奇心、贪小利等心理特点，通过伪造合法网站、低价秒杀、办理退款等理由发出欺诈邮件，骗取网络用户的个人金融信息，进而实施银行卡诈骗。
低价团购
秒杀
¥10000
停！
骗子正在伪造合法网站，利用虚假信息窃取你的个人信息！
见招拆招
1、切勿点选不明短信或电子邮件中的可疑链接。
2、网上交易时，短信验证码相当于是“一次性密码”，对于任何索要验证码的行为都要警惕。
任何网购退款均无需提供银行卡密码和校验码。
不打开可疑链接
警惕钓鱼网站
不泄露短信验证码
识别加密保护
安装安全防护软件
（二）慎用公共WIFI
套路：不法分子会在公共场所提供一个免费WIFI，持卡人使用后，极易被植入木马病毒，被盗取移动终端内的银行卡信息，除此之外，不法分子会把正规网站的网址绑架到自己的非法网站上，当持卡人使用其WIFI网络并输入正确网址时，会跳到一个高度仿真的假网站，如进行网络支付，就会导致卡片信息泄露。
木马
病毒
是否接入 WIFI
等一下！
不要随便连接未知WiFi，手机会被植入木马病毒！
见招拆招
1、尽量不要打开WIFI自动连接功能，减少连接上“钓鱼”WIFI的风险；
2、切勿在连接公用WIFI时使用一些金融账号或密码。
安全
是否接入 WIFI
确认真正的WIFI
避免自动连接WIFI


（三）慎扫二维码
套路：不法分子提供的二维码很多带有手机木马程序，程序扫码后会自动下载至扫描手机，并不会在手机上出现程序图标，不易被下载者发现，木马程序会自动记录操作信息，关键信息会被盗取。
木马
病毒
木马程序
不要扫！
骗子会利用二维码中附带的木马病毒
盗取你的个人信息！
见招拆招
1、谨防病毒软件，切勿扫描未知来源的二维码，更不要点开链接或者下载安装。
2、在个人电脑和手机等终端安装安全防护软件，提防病毒入侵。
木马程序
删除
不轻信未知来源的二维码
谨防山寨应用软件
注意电脑手机防护及杀毒。