2022年国家网络安全宣传周

“网络安全为人民，网络安全靠人民”

2022年9月5日- 2022年9月11日

“举”案例说法 —— 这些套路要警惕

01-虚假APP诈骗

李先生神色慌张来到某银行，申请开立银行卡。网点经理上前询问其开卡用途，李先生表示准备向银行申请5万元贷款，支付其在某平台上的贷款保证金。值班经理认为男子的开卡用途可疑，向其进一步了解后得知李先生最近计划开办一家实体店，缺乏启动资金，故下载了一款贷款APP，按操作提示填写个人资料后获批了20万元的贷款。

但贷款在最后放款环节提示放款账号有误，随后自称是该APP客服人员与之联系，要求其缴纳5万元保证金来解冻贷款资金，并出示了“监管部门公函”，强调必须在2小时内缴纳5万元保证金，否则将被控告“恶意套用贷款罪”，接受上门取证调查。被吓懵的李先生赶紧将其卡内的1980元马上转给对方，但因手头资金实在凑不齐5万元，这才想到来银行办理贷款支付该笔保证金。在仔细查看了李先生与对方的聊天记录后，网点经理基本确定这是一起典型的网络安全诈骗案件，随后帮助客户联系公安机关报案。

安全提示

本案例是近年来多地多次发生过的典型网络安全诈骗案例，诈骗分子通过短信、QQ、微信、APP等方式发布可办理高息贷款或信用卡套现等虚假信息，以提前交纳手续费、税款、利息、解冻资金等方式，诱骗受害人汇款，以此骗取钱款。作为普通金融消费者，我们应注意增强防诈警觉意识、提高分辨能力，在正规金融机构的网上、手机渠道办理相关业务，对于来历不明的信息注意拨打官方客服电话和国家反诈中心电话进行确认。

本页内容来源于人民银行《2022年金融网络安全宣传手册》

“举”案例说法 —— 这些套路要警惕

02-“征信修复”骗局

张先生在购买新房办理房贷时，发现自己的征信报告存在多次信用卡逾期记录，导致银行拒贷，陷入困境。此时，两名陌生人士的交谈引起了张先生的注意，其中李某声称在王某的帮助下完成“征信修复”，并成功办理贷款。随即张先生主动加入交谈，并留下王某联系方式。

后经多次联系，王某提出支付2万元即可帮张先生“修复征信”，并要求其先支付40%作为定金。一个月后，王某通知张先生已“征信修复”成功，索要剩余的60%。但当张先生办理房贷再次来到银行时，发现逾期记录并未消除，在银行工作人员的解释下，方知被骗，此时王某已经联系不上。

安全提示

根据《征信业管理条例》有关规定，任何机构和个人都无权擅自修改、删除信用报告上真实、准确的征信信息。每个人作为信息主体，在日常生活中都要注意量入为出、合理借贷、按时还款，避免逾期，保持良好的征信记录。同时，需提高警惕，不要相信“征信修复”广告并远离“征信修复”骗局，避免上当受骗，造成财产损失及个人信息泄漏。

本页内容来源于人民银行《2022年金融网络安全宣传手册》

“举”案例说法 —— 这些套路要警惕

03-虚拟物品骗局

小张是某网络游戏的忠实玩家，在该网络游戏上花费了不少的时间和金钱，游戏账号装备了价值不菲的皮肤。某天小张在游戏论坛中偶然翻到了一条广告，“网络游戏饰品租赁网站，稳定收益无风险，大平台担保...”。

看到很多论坛网友都晒出自己的收益，小张没有多想点开了广告中的网址，并注册了账户。起初，只尝试出租了一套游戏皮肤，很快就有求租的“玩家”主动联系，一周过后小张从网站中成功提现了余额，觉得没有多大风险的他索性把账号中所有皮肤都挂在了网站上，可一连几天过去了却无人问津。

此时，内心焦急的小张询问网站的客服人员，其“建议”卖家的皮肤直接寄存在网站的机器人账号中，交易时间更快，也更容易租出去，并再三以“大平台担保”“保证金制度”“理赔案例”等说辞保证账号安全。被利益冲昏头脑的小张将所有的皮肤转到了网站的机器人账户，两周后小张想要提现自己的收益时，发现网站已经不能使用自己的账号登陆，小张共损失了价值数万元的皮肤，等到小张报警后才发现，这些价值不菲的虚拟资产早已经被转移。

安全提示

游戏交易诈骗属于一种新型的网络诈骗方式，其特点是受害者比较集中，而且每位受害者的损失数额相对较大。诈骗团伙往往在较为封闭的游戏论坛和贴吧发布虚假信息，以游戏账号租赁赚钱、游戏装备兑换现金等作诱饵，引诱受害者将游戏中的虚拟物品转移到他们手中。游戏中的虚拟资产转移比常规资产更加容易，虚拟资产的价值也难以认定，受害者的损失相对难以追讨，因此我们应当把游戏仅仅当作一种消遣方式，在游戏中要保持清醒的头脑，理性消费。

本页内容来源于人民银行《2022年金融网络安全宣传手册》

“举”案例说法 —— 这些套路要警惕

UOB

04-围绕“疫情”设骗局

2022年2月，某县公安局网安大队巡查发现，有人利用群众对口罩迫切需求的心理，制作名为“某县防护口罩预约服务”的网页发布至微信朋友圈、微信群，假借预约口罩，非法获取群众的公民个人信息。某县网安部门经过缜密侦查，迅速锁定了犯罪嫌疑人薛某，并于同月将其抓捕归案。经查，薛某共非法获取公民姓名、电话号码、身份证号码、家庭住址等公民个人信息5530条。

安全提示

《中华人民共和国个人信息保护法》规定，任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

若手机收到关于疫情流调的短信，要求点击链接后自行填报个人信息，一定要谨慎判断，最好通过官方渠道进行求证；如未求证，谨慎点击短信链接，防止受骗。

本页内容来源于人民银行《2022年金融网络安全宣传手册》

“举”案例说法 —— 这些套路要警惕

05-“钓鱼广告”骗局

某天刘先生浏览手机时，无意中看见以某商业银行名义投放的打卡送礼品活动广告（广告内二维码实为钓鱼二维码），刘先生扫二维码跳转到伪造的打卡活动网页，并直接下载安装了一款理财软件，刘先生看见软件中实名注册打卡送礼品的活动后非常心动，便填写了姓名、身份证号、手机号等敏感信息，并按活动要求连续2天参与打卡活动，在领取礼品页面又填写了自己的详细收货地址，之后，刘先生便接到了客服的电话，对方以发放礼品需甄别用户真实性为理由，引诱刘先生购买一定金额的理财产品获取礼品，骗取了刘先生5000元。

安全提示

1. 银行等金融机构不会在非官方平台发布签到、抽奖兑礼品等活动信息。
2. 查看网站链接和页面是否为官方渠道。诈骗短信或二维码提供的网页链接可能是假冒手机银行或网上银行网页的钓鱼链接，也可能是病毒木马，不应轻易点击和操作。
3. 任何含可疑二维码、链接、应用程序的广告、短信等消息，不要轻易点击，若无法辨别真实性，应及时联系官方机构求证。
4. 涉及提供个人信息、资金转出时请务必三思，一旦发现受骗，请及时拨打110报警，并保留好相关证据。
5. 请下载“国家反诈中心”APP。“国家反诈中心”APP是公安部联合国家互联网应急中心开发的一个可以智能识别诈骗电话、短信和网址的软件。使用“国家反诈中心”APP可有效防范不断更新、真假难辨的诈骗手段。

本页内容来源于人民银行《2022年金融网络安全宣传手册》

RIGHT BY YOU