

我行积极参与2019年 "3•15"银行业和保险业 消费者权益保护教育宣传周

"以消费者为中心优化服务"



3•15银行业和保险业消费者权益保护教育宣传周 以消费者为中心优化服务









《信息安全无小事》——案例小漫画



非常感谢您, 姓名 问卷完成了! 年龄 我们将特赠您一份纪念 电话 请留下您的信息. 家庭地址 我们会在这周内 将奖品快递给您! ## 省## 县## 村## 号

市面上经常会碰到各种有奖问卷调查、购物抽奖或申请 免费试用等活动。

这些活动一般要求填写详细的联系方式和家庭住址等个 人信息。



不要轻易向市场调查 人员披露电话号码、 地址、邮件地址等个 人信息,除非您确信它 们会得到正当的使用。

不法分子会将个人信息倒卖给非法机构,各类电话推 销、骚扰电话、电信诈骗蜂拥而至。

在日常生活中,不要贪图小利小惠,慎重参加调查、抽奖 等活动。

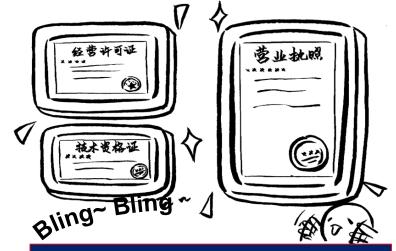




《警惕非法集资》——案例小漫画



不法分子往往承诺高额回报,并给予一定小恩小惠来 诱惑社会公众参与投资。



不法分子大多通过注册合法的公司或企业,编造虚假 项目骗取社会公众投资。



3 消费者往往容易被虚假宣传所影响,加入虚假的投资项目。



待集资达到一定规模后,则秘密转移资金或携款潜逃, 使集资参与者遭受经济损失。

3•15银行业和保险业消费者权益保护教育宣传周 老年人如何防范金融诈骗



1.莫贪便宜, 抵御高收益诱惑

- 不要轻易相信所谓的高息"保险"、高息"理财",不被小礼品打动,不接收"先返息" 之类的诱饵。
- 通过正规渠道购买金融产品,购买保险过程中要尽量做到"三查、两配合",即通过保险公司网站、客户热线或监管部门、行业协会网站查人员、查产品、查单证,配合做好转账缴费、配合做好回访。

2.防止个人和家庭信息外泄

提高警惕

- 注意保护个人信息,不要轻易将个人资料告知他人。
- 请务必妥善保管好自己的个人银行卡及密码,任何情况下都不要轻易向其它人透露账户信息,更不能向不明账户进行转账。
- 根据我国法律规定,公安机关、检察机关、法院在侦查办案中都不会通过电话询问群众家中存款情况以及要求转账等。

3. 警惕金融诈骗风险

- 对来历不明的电话或短信要提高警惕,不要轻信,以免落入诈骗陷阱。如有疑问,可直接拨打开户银行的客户服务电话确认,如遇资金被骗,应及时向公安机关报案。
- 不要轻信街头广告等非正规宣传内容。客户如需办理贷款业务,应通过正规途径,如前 往银行网点和其他经银监会批准的贷款机构。不要轻信在银行网点外遇到的所谓"贷款 推广人员"或"银行贷款工作人员",不要拨打贷款小广告上的联系电话,以免受骗上 当。





《警惕非法集资》——案例小漫画



1 不法分子往往在宣传上一掷千金,聘请明星代言、名 人站台,制造虚假声势,骗取社会公众投资。



不法分子通过在各大广播电视、网络媒体发布广告, 甚至通过网站、微博、论坛等网络平台和QQ、微信等 即时通讯工具,传播虚假信息。



3 消费者往往相信这类造势宣传,陷入以"虚拟货币"、 "金融互助"、"社会捐赠"等为幌子的陷阱。



因 "庞氏骗局"本质,注定了崩盘的命运,最终使得 投资者哭诉无门。





《识别防范非法集资》——案例小漫画



我之前的银行客户经理小李,介绍我个 明星企业,正在向公众募集资金。 年利息固定30%,每个月还额外返息 10%呢!

那你有没有通过银行官方官 网了解过有没有这个所谓的 合作伙伴?



明星企业?你了解这家公司的 性质吗?



你有没有拨打过银行官方客 服热线确认银行真的是担保



当然! 人家公司可有正规营 业执照和金牌牌照呢!

> 有营业执照不等于不会犯罪。未经 金融监管部门批准的企业向公众吸 收资金都属于**非法集资**! 金牌牌照有很多,只有银行牌照可



但我每个月都拿到收益的呀! 小李还跟我签订了协议,我 还有收据的。

方吗?

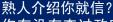


小李推荐的不会有问题的! 这个公司可是银行的合作单 位,都是有银行担保的!

以吸收存款。



我钱都投进去了! 那怎么办?



你有没有查过政府网站,看这家企 业是否是国家批准的上市公司,是 否能发行公司股票、债券等?





你赶紧到就近公安机关进行举报!

庞氏骗局懂不懂?

高回报率不可信!

天上不会掉馅饼!





3•15银行业和保险业消费者权益保护教育宣传周 防范打击非法集资的风险提示



• 承诺高额回报

不法分子为吸引群众上当受骗,往往编造"天上掉馅饼"、"一夜成富翁"的神话,通过暴利引诱,许诺投资者高额回报。

• 编造虚假项目

不法分子大多通过注册合法的公司或企业,打着响应国家产业政策、支持新农村建设、实践"经济学理论"等旗号,经营项目由传统的种植、养殖行业发展到高新技术开发、集资建房、投资入股、售后返租等内容,以订立合同为幌子,编造虚假项目,承诺高额固定收益,骗取社会公众投资。

非法集资 常见手段

• 以虚假宣传造势

不法分子为了骗取社会公众信任,在宣传上往往一掷千金,采取聘请明星代言、在著名报刊上刊登专访文章、雇人广为散发宣传单、进行社会捐赠等方式,加大宣传力度,制造虚假声势,骗取社会公众投资。有的不法分子利用网络虚拟空间将网站设在异地或租用境外服务器设立网站。有的还通过网站、微博、论坛等网络平台和QQ、微信等即时通讯工具,传播虚假信息,骗取社会公众投资。

• 利用亲情诱骗

不法分子往往利用亲戚、朋友、同乡等关系,用高额回报诱惑社会公众参与投资。有些参与传销人员,在传销组织的精神洗脑或人身强制下,为了完成或增加自己的业绩,不惜利用亲情、地缘关系拉拢亲朋、同学或邻居加入。

非法集资风险提示

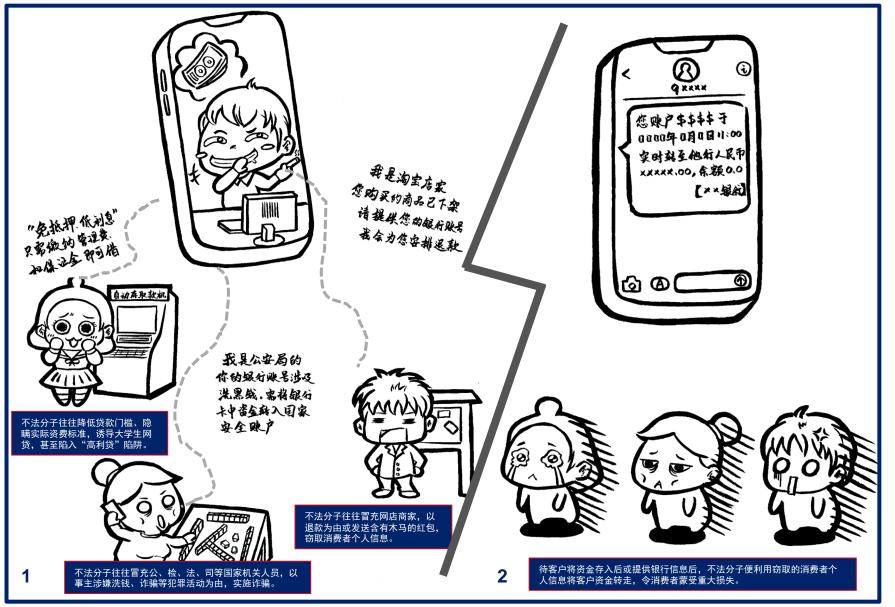


- 非法集资行为不受法律保护,参与非法集资活动受到的损失由参与者自行承担,风险巨大;
- 消费者要提高风险责任意识,对私售理财产品、P2P平台等存在的风险要有清醒的认识, 对手段多样的非法集资行为要提高警惕,谨防受骗,避免"钱袋子"遭受损失。





《防范金融诈骗》——案例小漫画







防范金融诈骗的风险提示



电话诈骗

- 1.虚构子女绑架,利用电话录音(如孩子的哭声)造成家人恐慌,要求家人汇款赎人。
- 2.冒充亲友,以车祸、生病、违法需交纳款项等为由实施诈骗。
- 3.冒充电信局人员,以电话欠费等名义实施诈骗。
- 4.冒充公、检、法、司等国家机关人员,以事主涉嫌洗钱、诈骗等犯罪活动为由,实施诈骗。
- 5. 谎称事主中奖,要求事主缴纳个人所得税、服务费和手续费等实施诈骗。

金融诈骗 常见手段



短信诈骗

- 1.发送短信称事主的银行卡在异地刷卡消费,待事主回电时,不法分子假冒银行工作人员实施 诈骗。
- 2.通过短信发送银行账号及"速汇款"等信息,行骗碰巧要汇款的事主。

网络诈骗

- 1.假借银行名义,通过制作虚假广告、群发短信等方式,以"无抵押、无担保、低息贷款"为 诱饵, 诱使客户与其联系。
- 2.利用QQ向客户发送含有木马的程序包,或诱导客户进入钓鱼网站直接下载此类程序包,在 客户安装该程序包过程中完成木马程序的安装,从而窃取客户网银信息。

大华银行防 范金融诈骗 风险提示



1.请务必妥善保管好自己的个人银行卡及密码,任何情况下都不要轻易向其它人透露账户信息, 更不能向不明账户进行转账。对来历不明的电话或短信要提高警惕,不要轻信,以免落入诈骗 陷阱。如有疑问,可直接拨打开户银行的客户服务电话确认,如遇资金被骗,应及时向公安机 关报案。

2.不要轻信街头广告等非正规宣传内容。客户如需办理贷款业务,应通过正规途径,如前往银 行网点和其他经银监会批准的贷款机构。不要轻信在银行网点外遇到的所谓"贷款推广人员" 或"银行贷款工作人员",不要拨打贷款小广告上的联系电话,以免受骗上当。

3.在网上输入私密信息前,需确认网站地址是否正确;需要登录网上银行或电子商务网站时, 应直接在网址栏填写正确的网站地址,请不要使用检索页来搜索网站,更不应轻易通过他人发 来的网站链接登录相关银行网站,以免误入"钓鱼网站"而遭受损失。

3•15银行业和保险业消费者权益保护教育宣传周注意移动金融安全



1.妥善保管个人信息:

妥善保管好自己的身份证件、银行卡、银行U盾、手机,不要轻易借给他人使用,一旦丢失要立即挂失;不要轻易向外透露身份证件号码、帐号、卡片信息等;不轻易给任何人发送带有银行卡信息和支付信息的图片。

2.设置个性复杂的密码:

妥善设置银行卡和各类支付密码,可采用各种符号穿插排列的方式,不使用同一数字、生日、身份证号码等容易被猜测到的简单密码;不将银行卡密码作为其他网站、APP的密码;为不同银行卡和不同支付账户设置不同复杂度的密码,并定期更换。

3.谨防诈骗短信:

不要轻信要求转账、汇款或提供银行卡号、密码和验证码的短信;收到上述短信时,务必与银行客服进行信息核实;当发现有诈骗行为时,及时向公安机关举报。

4.防范假冒网站:

不登陆不熟悉的网站,进入网站地址时要仔细核对,不随意打开陌生人发来的链接,特别是即时通讯工具 (短信*、*QQ、微信等)上传的信息。

5.警惕虚假"二维码":

陌生人发送的假红包、中奖信息等包含的二维码很有可能植入病毒,会导致账户信息泄露,被不法分子利用盗刷网银、网上支付账户,不要随便扫描来路不明的二维码。

6.谨慎使用公共Wi-Fi:

谨慎使用公共场所的Wi-Fi热点,可以找工作人员确认后连接使用;尽量不用可以直接连接且不需要验证码 或密码的公共Wi-Fi,谨慎使用公共Wi-Fi进行网络购物或网络支付。

7.确保网银终端安全:

不操作网银时,U盾应及时拔出;及时更新电脑、手机以及其他手持终端的安全防护软件,建议开启自动升级功能;为终端安装专业安全软件,防范病毒和恶意程序。

8.防范手机使用风险:

要到官方指定下载APP;手机丢失时,应第一时间致电运营商挂失手机号,将于手机绑定的所有支付业务(如网银、支付宝、微信支付等)一并解绑,通知亲朋好友手机丢失,防止诈骗;旧手机应由专业机构进行回收处理,既环保又安全,切勿交与资质存疑的小商小贩随意处理。

移动安全小 贴士

谢谢



