



线上消费

案例描述:

张女士收到一条显示为“*银行”的短信,称其账户积分即将清零,请及时兑换权益。她点击链接,进入一个与真实银行官网极度相似的页面,并按要求输入了银行卡号、密码及短信验证码。随后,她收到交易通知,账户内的数万元资金已被全部转至一个陌生账户,此时她才意识到遭遇钓鱼诈骗。

注意

钓鱼诈骗

风险提示:

- (1) 警惕诈骗: 兑换积分等业务应通过银行官方APP进行,有问题主动拨打银行官方客服电话或前往网点进行核实。
- (2) 信息保密: 任何索要个人敏感信息的行为都是诈骗,包括姓名、证件号码、手机号、银行卡号、银行卡密码、短信验证码,务必坚守不透露。



移动支付

案例描述:

赵先生在商场门口被“扫码抽奖”的活动吸引。他用手机扫描了一个二维码后,页面提示需下载一个未知来源的APP才能参与。客户下载完成后,手机开始频繁卡顿,当晚便发现其绑定的多张银行卡接连发生了十余笔小额盗刷。



风险提示:

- (1) 扫码谨慎: 坚决不扫描来源不明的二维码,这可能是木马病毒的下载入口。
- (2) 环境安全: 进行移动支付时,避免连接不可信的公共WiFi,以防个人信息被截取。
- (3) 密码管理: 为支付类APP设置复杂的单独密码,避免设置简单数字,并定期修改。



老年人银行支付篇

案例描述:

独居的李大爷接到一个自称是“某银行法务部”的来电,对方准确报出了他的姓名与身份证号,并告知其涉嫌卷入一桩“重大洗钱案”,需立即将全部资金转移到“安全账户”进行核查。惊慌失措的李大爷按对方要求,将个人资金转移到指定账户,直至子女回家才发现资金被骗。



风险提示:

- (1) 识破话术: 所有声称“账户涉案”、“电话转接公检法”、“安全账户”的说辞,都是诈骗的典型特征。
- (2) 家庭联防: 子女晚辈应经常与老人沟通,分享最新诈骗案例,共同建立起一道家庭安全防火墙。
- (3) 积极学习: 老人可参加银行等正规机构反诈类知识宣传,学习最新诈骗套路,避免资金损失。