



NFC

手机这个功能 慎用

为了方便快捷支付,很多市民在使用智能手机时都开通了NFC功能。可你是否知道,犯罪分子只需要几步,就能在你眼皮底下盗刷你的钱。近日,多个反诈中心向社会发布预警提醒,警惕骗子利用NFC功能将你的手机变成“提款机”。

什么是NFC功能?

NFC即近距离无线通讯技术。手机和SIM卡同时具备NFC功能,就可通过刷手机完成公共交通、超市餐饮以及其他方面的小额支付。

案例1

通过NFC转账 被骗近10万元

在警方通报的案例中,李先生接到一个自称航空公司客服的电话,对方称其航班因机械故障被取消,并询问是选择改签还是退票。李先生选择改签,对方进一步表示因已为其购买保险,可退还300元到银行卡,但需通过“企业支付”操作。在对方的指引下,李先生使用招商银行卡在抖音平台开通了“放心借”服务,并按照对方要求分两次借款共10万元。随后,对方要求李先生下载名为“NFO-X”的软件,并通过手机NFC功能进行刷卡操作。李先生按指示完成了两笔大额交易,当对方要求进行第三次刷卡时,李先生察觉异常,但已被骗9.8万元。

案例2

手机被远程操控 银行卡钱被转走

罗女士接到陌生来电,对方谎称其已开通“抖音会员直播服务”,如不取消将扣除高额费用。罗女士添加了对方的客服QQ,并下载了两个APP安装包。其中一个会议类软件,另一个则是支付工具。

开启屏幕共享后,罗女士的手机被远程操控,甚至出现自动黑屏的情况。

随后,对方要求罗女士将银行卡贴近手机的NFC识别区域,并指示她不要操作手机。不久后,对方发送“关闭会员成功”的虚假信息后断开联系。罗女士与家人检查后发现,银行卡内的钱已被转走。

诈骗手法分析>>

1.伪装正规身份

以“航班故障”“扣费取消”为由,引起受害者紧张情绪,利用紧迫感降低其警惕性。

2.借助NFC功能实施盗刷

要求受害者通过NFC功能,将银行卡信息与虚假软件绑定,直接读取并转移卡内资金。

3.远程操控制造恐惧感

使用屏幕共享等技术,让受害者误以为对方是正规操作,进一步增加信任度。

4.伪装成功信息转移注意力

骗子发送虚假的“成功取消”消息,让受害者放松警惕,延迟发现资金被盗。

如何防范诈骗>>

1.警惕“客服”来电

接到自称客服的电话,务必核实其真实身份,尤其是涉及改签、退款等敏感信息时。

2.慎用NFC功能

慎用NFC功能,避免随意通过NFC功能进行陌生支付操作,谨防被盗刷。

3.拒绝屏幕共享

任何要求打开屏幕共享或远程协助的操作均应高度警惕,避免泄露个人信息。

4.远离来路不明的APP

此外,对于不明二维码、软件,都应避而远之。不要下载来路不明的APP。

一旦察觉被骗,应立即拨打银行客服电话冻结银行卡,并报警处理!
本报综合