

有些二维码,可能是“钱包刺客”

□张珍铮



上周,某地初二学生小涛在班级群里看到一条“帮砍一刀”的链接,想也没想就扫二维码输入了支付密码。他以为只是帮同学省钱,没想到第二天醒来,零花钱账户里少了498元。“我当时根本没多想,就觉得是帮同学忙。”小涛回忆道,“那个页面看起来和平时扫的省钱APP的二维码差不多,也要输入支付密码,没想到遇到了骗子。”那个看似普通的黑白二维码,像一把钥匙,悄悄打开了小涛的钱包。

二维码可能是“钱包刺客”

平常大家扫的二维码,不管是加微信好友,还是买东西,这个二维码其实是一套“计算机语言”。这些“黑白格子”就像密码本,记录着网址、账号等个人安全信息。而骗子利用二维码行骗的常见套路有三种。第一种是偷梁换柱,即把商家的收款码换成自己的,你如果扫了码,支付的钱就进了骗子口袋。就在上个月,某中学旁边的奶茶店就发生过这样的事——有同学付了钱,但商家却没收到,后来发现是商家的收款码被骗子的二维码覆盖了。

骗子的第二种套路是糖衣炮弹,即用“免费皮肤”“现金红包”做诱饵,你如果扫了这样的码就会中病毒,打开这类链接通常会要求你授权各种权限,一旦同意,你的支付账户就危险了。

骗子的第三种套路叫暗度陈仓。骗子的二维码表面看起来和正规的网络链接很像,一旦点了就会跳转到钓鱼网站。这些网站做得和真的几乎一模一样,连图标、颜色都一样,专门骗你输入账号密码。

其实,每次扫码你都在默默塑造自己的数字画像。系统会分析每个人的支付习惯。经常在正规平台消费、按时还款的同学,信用评分会更高;而经常点击可疑链接、频繁大额转账的,会被自动标记为风险用户。

这些数据,可能影响你未来申请助学金、办理信用卡,甚至就业时的背景审查。

扫码支付如何更安全?



- 1、扫码前要三问：
来源可靠吗？优惠合理吗？页面正常吗？
- 2、要有安全设置自查清单，定期检查支付安全设置。
- 3、如发现账户异常，立即冻结账户，截图保存证据，拨打110报警，联系平台客服申请赔付。

制图 王思祺

免密支付 限额不要设置太高

其实,国家早已从法律上为我们准备了“防护装备”。首先,小额免密支付有上限。按照规定,单日累计不能超过1000元。很多同学为了方便,把限额设置得很高,这相当于把家门虚掩着,会带来安全隐患。

其次,个人信息受保护。根据《中华人民共和国消费者权益保护法》,商家不能随便收集个人的消费数据,未经你同意的数据采集都是违法的。比如有些APP要求获取通讯录权限,你完全可以拒绝。

第三,被盗刷赔付有保障。只要能证明不是你自己操作的交易,支付机构必须在3个工作日内完成赔付。去年浙江杭州就有一个典型案例——一名高中生的游戏账号被盗,通过平台申诉通道,两天就追回了全部损失。

扫码前 要先问来源是否可靠

记住下面这三个实用锦囊,让你的零花钱更安全:首先扫码前要先问——来源可靠吗?陌生群发的不明二维码要警惕;优惠合理吗?记住天上不会轻易掉馅饼;页面正常吗?要求额外授权就立即停止扫码。

其次,要有安全设置自查清单。检查支付安全设置,关闭不必要的小额免密支付;每月清理一次授权应用;支付密码独立设置,不与其他账号密码重复;定期查看交易记录。

另外,出了事不慌张,如发现账户异常,立即打开支付APP冻结账户,截图保存所有证据,包括聊天记录、转账截图一个都不能少,拨打110获取报警回执,这是重要的法律凭证,最后联系平台客服申请赔付。

做数字时代的“聪明消费者”

培养金融安全意识,就像给数字钱包筑起一道防护墙。这道墙不仅保护你的零花钱,更守护着你未来的信用资产。

大家可以把《非银行支付机构网络支付业务管理办法》等法规当作数字时代的“交通规则”来了解。扫码前确认对方身份,支付时再三核对收款方信息,每周检查账户的授权应用。这比任何防盗技术都更持久,因为最坚固的安全防线永远是冷静思考的大脑。

(作者为成都市温江区嘉祥外国语学校思政教师)