

近日,网络上一段视频传播很火,视频中男子在扫码使用共享单车时,发现有几辆共享单车的二维码处被贴上新的二维码,将原码完全覆盖,如果不仔细辨认,根本察觉不出来,还好男子心细发现并撕下了假的二维码。

记者梳理发现,针对这段视频,多地网警发出安全提醒,骗子已经盯上了共享单车二维码,一旦扫了假的二维码,很可能钱会被骗走,一定要通过安全渠道下载共享单车应用App,扫码时要留心是否被覆盖,也不要乱扫车身上其他位置的二维码。

事实上,不仅是共享单车,随着扫码支付、扫码下载、扫码开锁等已经遍及人们日常衣食住行的方方面面,利用二维码实施的电信网络诈骗,也以各种形式频频出现,让人防不胜防。



扫码时代当心二维码骗局

制码技术几乎零门槛

利用二维码伪造缴费单

近日,家住河北省石家庄市的刘女士把车停在路边,回来时发现车上贴着一张“罚单”,上面注明为“违章停车单”,并附有一个交罚款的二维码,提示“扫一扫,交罚款”。

看到文字排版、罚单内容、纸张材质等都与之之前收到的违停罚单一致,刘女士并没有疑心,虽然之前的罚单上没有交罚款的二维码,但刘女士心想,这应该是交警推出的便民新举措,便按照“罚单”上的提示扫码缴费。然而,刘女士事后查询发现并没有此次违停记录,才意识到被骗。

利用假罚单行骗的案件已经在多地出现过。记者从石家庄市公安局了解到,这类假罚单在材质、尺寸、抬头、格式等方面,其实都和真罚单有所区别,但当事人往往难以辨认。假罚单上最可疑的就是二维码,扫描二维码后通常会出现微信转账页面。而交警目前并没有提供任何扫描二维码缴罚款渠道。

除了假罚单,不法分子利用二维码还伪造水电费催缴单、商家收款码等,设各种二维码缴费骗局。例如骗子伪造含有二维码的水电费催缴通知,发给手机用户或贴在住户家门口,扫码后出现的是给个人账户的转账界面,不少群众未经核实便落入骗子的圈套。

目前,二维码已被广泛应用于社交媒体、移动支付、产品促销、应用程序下载等方面,但由于制码技术几乎零门槛,不法分子将病毒、木马程序、扣费软件等植入二维码,消费者扫码被盗刷现象时有发生。

每逢节日,网络上就会充斥大量各类活动的二维码。今年春节前,福建莆田开网店的汪女士遇上二维码骗局。一名诈骗分子假冒客户选中汪女士网店的一件商品,在支付时,称当日手机转账已达最高限额,要求通过扫描二维码支付。汪女士达成交易心切,用手机扫了一下对方提供的二维码,并点了下链接。没想到,她等了半天也没等到对方资金到账信息,却收到



资料图片来自网络

自己名下支付宝、余额宝、绑定银行账户等共计18万元资金被人转走的信息。

汪女士报警才得知,不法分子将木马植入二维码,她扫描后手机已经中毒,或者被远程控制,或者个人信息泄露,账户资金即刻被盗刷。

为此,警方提醒,遇到印有二维码的催缴单,无论是水、电、燃气费,还是违章罚款单,只要涉及钱财都要多个心眼,不要扫可疑二维码,不放心的话可以上官方平台查询,查明后再通过官方渠道缴费。

随意扫码暴露个人信息

共享单车上的二维码被掉包,假的缴费通知单上附有假的缴费二维码,只要扫描后认清转账页面不是官方页面,钱财还不会损失,但有的二维码背后则是连环骗局。

据了解,有的二维码扫描后跳转的网页安全性得不到有效保障,有可能在扫码之后跳转到不法分子搭建的钓鱼网站,这些网站会诱导进入的用户填写账号密码、下载恶意脚本等,不仅窃取用户信息,还可能威胁财产安全。

有的二维码是加好友的微信请求,大多为微商,一旦同意加为好友,就会经常收到一些产品广告,或经常被各种推销的朋友圈刷屏。还有些

通过加好友来实施诈骗,比如“微信美女卖茶叶”“美女支教老师”等就是这个套路。

目前比较火热的短视频和直播平台也是二维码诈骗的高发地带,大多数作案手法是扫码充值。粉丝向主播刷礼物需要充值,平台会弹出支付二维码,或用支付宝、微信支付完成充值。不法分子会利用这一环节,声称自己是平台客服或者内部人员以吸引受害人入套,诱导受害人扫码支付,受害人充值的金额直接进入嫌疑人的账号。

今年中秋假期,家住河北省邯郸市的严某带家人到某景点游玩,景点门口有一处活动台,宣传只要扫二维码下载安装某App,再注册成为会员,就能得到该景点的门票优惠券。严某的家人跃跃欲试,可严某思索再三还是心存疑虑,没有让家人下载。回到家后严某上网查询,看到诸多因扫描二维码而泄露隐私、落入诈骗陷阱的案例。

记者从石家庄市公安局获悉,近年来,很多商家都喜欢采取“扫码送礼”的方式吸引粉丝。但是,天下没有免费的午餐,二维码后的公众号、App很可能就是不法分子实施违法犯罪行为的平台,通过一个小礼物就轻易骗取到个人信息,有的用来倒卖,有的则用来在其他平台注册实施不法活动。还有各大社交平台或QQ群发布的一些兼职刷单信息、冒充网

购平台客服人员等,要求扫码支付保证金等,都可能是二维码诈骗。

不要随便扫陌生二维码

为了保证用户资金安全,一些第三方支付公司已对支付二维码进行适当的调整,采取动态二维码支付、禁止二维码截屏操作等相应措施,避免犯罪嫌疑人远程骗取事主付款二维码盗刷事主资金的可能。但是,不少人有不良的扫描习惯,看见二维码就扫,很容易落入不法分子的陷阱。

目前,二维码的生产和流通并没有明确的主体进行统一管理。虽然一些部门开始逐渐意识到二维码存在的巨大安全隐患,但尚缺规范措施,因此很难从源头上打击二维码诈骗。市民一定要做到:加强自我保护,千万不要见码就扫!

警方提醒,在日常扫码支付和扫描其他二维码时,打开二维码付款界面等待出示时,记得遮挡手机屏幕;手机功能允许的情况下,尽量使用指纹、刷脸验证来代替输入支付密码的习惯;用手机扫对方码支付时,要与收款方核对昵称;网上交易时,识别对方二维码须认真阅读提示信息;在手机上安装防病毒安全软件,过滤不安全二维码;不要在不知名的链接中输入身份证、银行卡号、家庭住址等私密信息。

此外,扫码领红包时一定要确认是否是官方活动,不要随意输入自己的身份证号和银行卡号;扫码骑共享单车或者缴纳罚款,要用官方的App进行扫码,要核实信息是否正确再进行付款;街头上的扫码促销免费送礼品不要随意扫码,有可能会套取你的个人信息,严重的会给手机植入木马病毒,导致银行信息密码被盗取;商家要留意自己的静态二维码收款,防止被不法分子替换成他们的二维码。

二维码诈骗看似百变,其实防范起来也是万变不离其宗,不要随便扫陌生人或者非正规商家提供的二维码,如果扫码后需要提供个人信息,一定不要盲目填写,这样骗子也就无计可施了。

据法制日报9月22日报道