电信诈骗穿上二维码“马甲”

吃饭付账、添加微信好友、下载手机应用等，很多人都习惯拿起手机扫描二维码搞定。然而，在带来便捷的同时，由于制作和传播成本低，二维码也成为一些不法分子实施诈骗的工具。

多地现二维码缴纳罚款骗局

近日，一张印有可缴纳交通罚款二维码的《违法停车告知单》在太原市民的朋友圈中流传。记者看到，这张特别的《违法停车告知单》，无论纸张颜色、抬头、款式还是上面的内容，都与常见的告知单相似，甚至还盖有公章。但特别之处在于，告知单的左下方有一个二维码，可以扫描二维码缴纳交通罚款。

记者扫描二维码后，发现手机页面直接跳转到了转账页面，并且显示“向个人用户‘违章缴费’转账”，金额显示为100元。

“粗一看还真能以假乱真，这要是真的拿手机扫二维码付款，估计钱就进了不法分子的兜兜了。”对此，太原市交警支队相关负责人表示，这是一种新型假冒交通违法罚单类骗局，不法分子通过制作假冒罚单，诱导车主扫描二维码支付“罚款”。

这并非孤例。记者了解到，类似的“诈骗罚单”在北京、长沙、武汉等多地频繁出现。

去年10月18日，武汉市东湖新技术开发区多名群众报案，称车上被贴了《违法停车告知单》。他们用手机扫描《违法停车告知单》上的二维码后，跳转到一个账户，并被要求付款200元。

武汉市公安局交通管理局接到报案后进行核查，确认群众提供的《违法停车告知单》系伪造。民警发现，该告知单漏洞百出，不仅有多个错别字，印章也与公安机关的不同，而告知单左下角的二维码是一个支付宝个人账户。

北京警方也在不久前破获北京市首例伪造“扫二维码违章罚单”诈骗案。据犯罪嫌疑人杨某交代，他在网上看到外地警方发布的“扫二维码缴纳罚款”的诈骗方式，认为可以用这种方式获利。随后，杨某以100元的价格让一名网友伪造了罚单，印上自己的微信转账二维码，打印后在街头张贴。

扫码付款当心被“截和”

二维码是在一维条码的基础上扩展出的一种可读性条码，数据信息储存在图形中。使用扫描设备识别条码的长度和宽度中所记载的二进制数据，即可获取其中所包含的信息。而二维码的技术门槛较低，只要有智能手机，安装一个免费的二维码生成软件，就可以将字符文本生成二维码。同样，只要手机上有微信或其他二维码识读软件，就能任意读取。

记者了解到，目前二维码诈骗形式主要有两种，其中一种是给传统电信诈骗穿上二维码的“马甲”。

据报道，一位重庆市民参加扫二维码赢取商家优惠券的活动，在扫码后，手机中了病毒，300元话费不翼而飞。有专家表示，二维码已成为手机病毒、钓鱼网站传播的新渠道。不法分子只要在网上搜索到任意一款“二维码生成器”，就可以将带有病毒程序的网址链接制作成二维码，用户扫码后，若点击其中的病毒链接，安装染毒程序，就极易导致手机中毒，进而丢失话费甚至泄露个人信息。

二是在二维码广泛应用的移动支付领域，不法分子多采取“无中生有”或“截和”等手段诈骗。

随着支付宝和微信支付的普及，二维码支付已被广为接受。中国互联网络信息中心数据显示，截至2016年6月，我国使用网上支付的用户规模达到4.55亿元，其中手机支付用户迅速增长，达到4.24亿元，半年增长率高达18.7%。

由于二维码在付款过程中应用广泛，一些不法分子制造假冒违章停车罚单、电费催缴通知单等，在上面印制个人收款二维码实行诈骗。

此外，也有一些不法分子将商家收款二维码偷换成自己的，进行“截和”。网上曾传过一个段子，一小偷将数家商店内的二维码偷偷换成了自己的，等到众店主发现时，小偷已默默“收”了70多万元。在不久前，佛山东方广场数家饮食店就接连中招。

见“码”就扫要不得

通信专家项立刚说，二维码其实就是一个入口，是“柳叶刀”还是“凶器”，关键看掌握在谁手中。二维码被不法分子利用之后，由于制作简单，使得诈骗成本变低，但效率却高了，这也是二维码诈骗频繁的一个重要原因。

然而，对二维码的监督却相对薄弱。有业内人士指出，注册一家二维码企业并不需要专业资质，制作二维码没有任何规定，发布二维码也没有任何限制。

对此，警方表示，消费者应提高警惕，在扫码前需确认该二维码是否出自正规的载体，不要见“码”就扫，不随意接收非官方网站的二维码或链接，用于网购的银行卡内不要存入过多的现金。

有专家表示，日常使用的二维码数据存储量较小，木马病毒一般难以直接存储在二维码内，需用户扫码后打开下载。因此，直接扫描二维码不会出现较大安全风险，关键在于对不熟悉的网址或软件一定要谨慎点击。

山西财经大学副教授张华明建议，加大力度打击利用二维码技术传播病毒、盗取手机话费的行为。相关监管部门也应加强在手机应用方面的相关法律法规体系建设，从信誉、认证入手，进一步规范市场发展环境，保护用户的合法权益。

（人民）