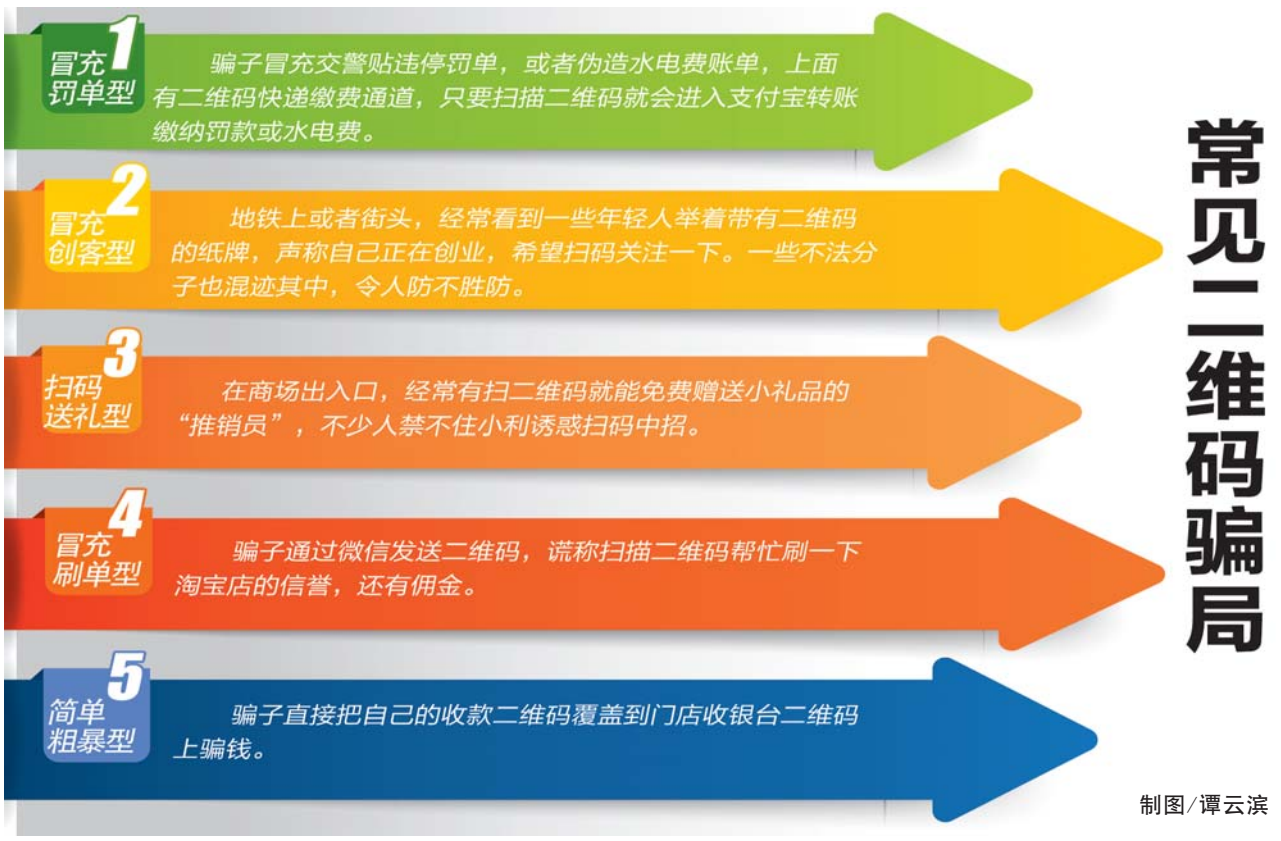
车门上、车厢里、街头电线杆、商店门把手……凡有井水处，皆见二维码。在刚刚结束的全国两会中，一府两院的工作报告都不约而同地采用了附加二维码的方式来做内容增值，从日常生活到政务工作，二维码适用场景越来越多。然而随处可见的二维码自带危险属性，在见码即扫的同时，骗子可能已将黑手探入你的囊中。从今日开始，半岛都市报将连续推出“真真假假二维码”系列报道，看看这些黑白相间、形似迷宫的小小二维码究竟如何发挥大作用，又是如何引你中招的。

晕，骗子用二维码真能整名堂

木马病毒、钓鱼网站都能“码”里藏，胆大的把商家支付码换成自个的

真真假假二维码



制图/谭云滨

□半岛全媒体记者 **葛欣鹏 景毅** 实习生 **丁世娟**

原本是扫码支付，钱却转给了骗子，本想扫码瞧瞧更丰富的内容，手机却中了病毒。作为移动互联网的入口，二维码已被广泛应用于社交媒体、移动支付、应用程序下载等方面。然而，由于制码技术几乎零门槛，不法分子将木马程序、扣费软件等植入二维码，消费者扫码被盗刷现象时有发生。这个给人带来便捷的小小二维码，似乎成了诈骗分子的帮凶。

骗案多 两年增长5倍

随着科技的发展，移动平台的普及，移动营销好像自然而然地走进了我们的生活，而现在移动营销最直接的工具正是二维码。

扫描衣服上的二维码便可以获知衣服的产地、型号、成分；点一份快餐通过扫描店铺二维码就可以在线转账；即将入驻岛城的ofo共享单车用二维码给每一辆自行车“刻”上身份标记，扫描就可以骑走享受交通便利。

内容获取、交易支付、社交沟通，二维码，从最初仅作为微信的内置功能，如今已发展成覆盖人们衣食住行，链接线上、线下的重要媒介。

这些黑白相间的小方块代表一个个ID数据集，只需要用相应的手机程序对准扫描，就可以获取囊括其中的万千信息。

当见码即扫渐渐变成了习惯，骗子却开始在二维码上找门道，且作案手段不断升级。

据媒体报道，2013年，在青岛开网店的汪女士收到“买家”发来的信息，对方说：“我在微信上看到我朋友发了几件衣服好漂亮哦，款式图片在这个二维码里，麻烦你扫一下，看有没有你家的宝贝。”可是，汪女士扫了一下二维码，支付宝密码被修改了，短短的两个小时之内，汪女士的18万元就落入了犯罪分子的腰包；广州的刘女士在街头看到扫码活动，“充话费扫码赠2G流量”，结果个人信息被曝光，银行卡被刷4000余元；今年2月，有网友爆料，其收到一张落款为“北京市国家水务局”发来的水费缴费通知单，上面显示通过扫二维码的形式可缴纳本月水费，但经网友核实后，却发现此单据为骗局。

今年的3·15晚会报道，专门曝光了有毒二维码。风靡全国的共享单车成为了骗子们的“香饽饽”，用手机扫描此类二维码后，或被要求直接转账，或被要求下载可疑软件，致使资金账户面临被盗刷的风险。

无讼研究院首席研究员李斌，总结了近三年来刑事案件中利用二维码实施的犯罪案件，共计104件276人样本的数据说明，涉二维码犯罪数量指数级增长，2015年比2014年翻了一番，2016年较2015年增加了两倍，是2014年的6倍之多。

从具体案件类型来看，诈骗类案件增速最为迅猛：2016年涉二维码的诈骗类案件占同期全部案件数量的五成。其中侵财类案件占多数，占全部案件数量的62%。

2月17日和2月18日，青岛市公安局官方微信公众号“青岛公安”连续两天发出提醒，市民们在享受扫描二维码带来便利的同时，一定要注意二维码背后隐藏的危险。

低门槛 引来诈骗黑手

这些看似高科技的二维码是如何成为不法分子诈骗工具的呢？

360反诈骗专家刘洋向记者介绍，市面上常见的二维码就是一张能储存信息的拥有特定格式的图形，能够在横向和纵向两个方位同时表达信息，能在有限的面积内表达大量信息。

“制作二维码输入的信息可以分成三类，文本信息，比如名片信息；字符信息，比如网址、电话号码；还有图片信息，甚至还可以包括简短的视频。”刘洋介绍。

这些数据信息是如何编入的呢？刘洋介绍，信息输入后，首先要选择一种信息编码的码制。现在常见的二维码都是以QR（Quick Response）码作为编码的码制。QR码是矩阵式二维码，它是在一个矩形空间内，通过黑、白像素在矩阵中的不同分布，来进行编码的。

众所周知，计算机系统使用二进制（0和1）数来贮存和处理数据，而在二维码中，用黑白矩形表示二进制数据肉眼能看到的黑色表示的是二进制“1”，白色表示二进制的“0”，黑白的排列组合确定了矩阵式二维条码的内容，以便于计算机对二维码符号进行编码和分析。

“现在问题恰恰就出在这QR二维码上。”刘洋介绍，QR码最早源自日本，当时国内没有成熟的拥有自主知识产权的二维码体系，国内市场几乎被QR码占据。而QR码在国内也没有申请专利保护，而是采取免费开放的形式。这就导致了这个看似专业的技术一下变成零门槛，只要会用电脑上网的人都可以通过网络下载二维码生成器，然后将发布的内容粘贴到二维码生成器上，软件随即生成用户所需的二维码。

记者随后在网上搜索“生成二维码”，发现了1300多万条结果，其中包含大量可以直接在线生成二维码的网站。记者随机选择了一个网站，将本报数字报网址输入，点击生成后立即出现一个二维码。用手机自带扫码软件扫一扫，果然可以迅速转到相关网站。不仅如此，记者还可以选择不同的二维码形式，也可以将自主选择的图片logo插入到二维码中间。

刘洋说，如此一来，传统电信诈骗常用的手机木马病毒、钓鱼网站等都可以轻松做成二维码，然后通过各种形式诱骗用户手机扫描。

难溯源 切忌见码就扫

二维码以其独特的大容量、低成本和易制作等诸多优点成为互联网时代链接信息的重要渠道，但同时由于技术门槛过低，二维码目前处在“人人皆可制作、印刷和发布”的状态，由此带来的信息安全风险不容忽视。

据报道，去年12月，青岛科技街一家火锅店的员工发现，收银台前收账用的二维码被人更换了。大家查看监控后发现，一名男子付账时趁前台店员不备，将随身贴着的一张二维码塑料片按在了收银台上；2月，有网友爆料，其收到一张落款为“北京市国家水务局”发来的水费缴费通知单，上面显示通过扫二维码的形式可缴纳本月水费，但经网友核实后，却发现此单据为骗局。

并非所有人都能像上述店员那样警惕。记者从警方获悉，目前，青岛已经出现过通过二维码实施诈骗的案件。

据市刑警支队六大队二中队中队长祝小楠介绍，目前二维码诈骗还是属于比较新型的诈骗手段，由于其与其他电信诈骗手法一样，采取利用互联网远程异地作案的手段，给警方侦破此类案件带来很大困难。

祝小楠介绍，二维码诈骗主要有三种形式，一种是把含有手机木马病毒程序的链接做成二维码，用户一旦扫描，手机就会被植入的病毒木马感染，尤其是安卓系统手机，木马病毒自动在后台暗转后可以隐藏桌面图标，身份证、银行卡号、支付密码等私人信息就会被盗取。另一种是把钓鱼网站做成二维码，用户一旦疏于辨别，将重要支付信息输入钓鱼网站，最终造成财产损失。最后一种就是直接把商家的支付码替换成自己的，顾客扫码支付时把钱直接付给了不法分子。

祝小楠提醒，由于肉眼无法辨别二维码真伪，手机用户在扫码时一定要慎之又慎。“一定要选择官方渠道公布的二维码，在实体店消费刷二维码时，即便是在店内也要询问一下收银员确认该二维码没有问题，公共场合张贴的海报、广告上的二维码尽量不要扫。”

除此之外，祝小楠建议，用户最好为手机快捷支付设置一个单笔以及当日最高支付限额，申请支付口令或数字证书等措施增加支付安全屏障，用于网购的银行卡内也不要存入过多的现金，从而最大限度地减少因误扫“有毒”二维码而造成大量的财产损失。