

扫一扫钱没了,二维码成诈骗“帮凶”

犯罪分子更换商家收款二维码,消费者不注意很可能钱就被转走

日前,南京市民刘先生在扫描摩拜单车二维码时,出现了本不该出现的转账提示,于是向警方报案。当地有些市民也发现,扫描摩拜单车上的二维码后,如果不注意很可能钱就被转走了。

虚假二维码骗局并非孤例。在广东破获的一起二维码诈骗案中,犯罪分子通过扫码盗刷获利90余万元。

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、产品促销、应用程序下载等方面。记者调查发现,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。



监管

建立回溯机制 明确监管主体

郑解介绍,目前,二维码的生产和流通并没有明确的主体进行统一的管理。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,但还没有相关法律法规和具体举措。

“主管部门应该使用技术手段对二维码进行域名解析,通过设立专门的监管平台对二维码进行检测,过滤不良信息。”浙江工业大学计算机科学与技术学院陈铁明教授建议,“可以考虑建立二维码中心数据库,对市面上流通的二维码进行备案登记,将所有二维码数据统一存放在一个中心数据库,实现对二维码生成流通环节的有效追溯。”

“在管理层面上,有关部门应该对二维码的发布内容进行备案审查,对二维码的发布平台进行资质鉴定,对二维码的发布者进行实名登记,形成一整套完善的责任追溯机制。”陈铁明说。

浙江工业大学网络空间安全协会研究人员郑毓波认为,二维码使用企业应该加强相关的防护。据了解,目前微信和支付宝已经在软件里加强了安全监控保护,确保用户扫码安全。支付宝公司近日宣布,从2月20日起,支付宝付款码将专码专用,只用于线下付款。这就避免了一些不法分子利用二维码付款的机制实施转账诈骗。沈杰告诉记者,支付宝已经自带网址检测功能,用于判定扫描的二维码是否存在恶意链接。如果发现安全隐患,系统会发出安全提示,让用户判定是否需要进入跳转界面。

业内专家表示,用户也需要提高扫码安全意识。“不少人不良的扫码习惯,看见二维码就扫,很容易落入不法分子的陷阱。”郑毓波说,应该加大知识普及,让大家了解二维码编码原理和二维码发布机制,不随意扫描来历不明的二维码,保护自己的信息安全。

■据新华社

A “扫一扫”藏陷阱: 虚假二维码覆盖正规码

针对消费者扫码遭诈骗,摩拜单车负责人称,单车上的正规二维码都是用钉子钉在车身上的,车费必须通过APP支付。车身上发现的二维码是后贴上去的,覆盖了原二维码,用户扫描的是不法分子的诈骗二维码。

在广东,佛山公安局禅城分局发现一起数十家店铺的收银柜台均被张贴虚假二维码案件。犯罪嫌疑人更换商家收款二维码,通过植入木马病毒的虚假二维码,获取消费者的手机信息和密码,进行网络盗刷。一共作案320余起,获利90余万元。

记者调查发现,除了用虚假二维码覆盖正规二维码实施诈骗,还有不法分子直接诱导用户扫描带有木马病毒的二维码。比如,浙江就多次发现不法分子以扫码得红包的形式诱导用户,一旦用户扫码后,手机会感染木马病毒,各种信息都被窃取了。

此外,有些不法分子通过拍照、截图、远程控制等方式获取

用户付款二维码,盗刷用户银行卡。浙江台州微商赵女士就是一个受害人。在网络交易过程中,不法分子以自己支付宝余额不足为借口,提出让赵女士将付款码发给自己扫码付款。收到付款码截图后,不法分子随即进行复制,盗刷了赵女士的银行账户。

“付款码相当于银行卡密码,不要轻易发给他人。”专家介绍,不法分子只要获取了,就可以进行复制,获取银行账户和密码。

“现在我都不敢随便扫码了,一不小心就可能被骗。可是现在生活中要用到二维码的地方又这么多,真是让人纠结。”杭州市民陈小姐说。

“以二维码作为入口的新型互联网诈骗案件层出不穷,一些不法分子将手机木马或恶意软件披上二维码的外衣在移动端广泛传播。由于缺乏相关知识,没有防范警惕性,消费者个人很难防范。”浙江省网警总队有关负责人说。

B 制码技术几乎零门槛 骗子可轻易制“毒码”

业内人士介绍,二维码就是一张能存储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。个人名片、网址、付款和收款信息等都可以通过二维码图案展现出来。

据了解,目前我国广泛使用的二维码为源于日本的快速响应码(QR码),QR码没有在国内申请专利,采取了免费开放的市场策略。“这也意味着谁都可以通过网络下载二维码生成器。只需要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。”杭州某网络安全公司工程师郑解说。

记者在网搜索“二维码生成器”,发现了205万多个搜索结果,大部分

的二维码生成软件可以直接在线使用。记者在首页选定了某一在线二维码生成平台,输入文字、图片、邮箱、网址后,瞬间就转换成了二维码。

“二维码的制作生成没有任何门槛。一些不法分子将病毒、木马程序、扣费软件等的下载地址编入二维码,用户一旦扫描,手机就会被植入的病毒木马感染,身份证、银行卡号、支付密码等私人信息就会被窃取。”阿里安全部资深品牌经理沈杰说。

“任何人都可以制作二维码,而且生成的二维码没有办法溯源,也没有相关的管理机构提供认证,这给警方侦破二维码诈骗案带来了很大困难。”浙江省网警总队工程师介绍。

开启 2017 年新征程 奥克斯温情感染亿万用户

2016年,空调领军企业奥克斯一路奔跑,创造了“电商销量双双第一、内销出货增长率第一、外销出货增长率第一、全年互联网电商占比第一”四项傲人的战绩。在大步向前的同时,奥克斯仍坚持贯彻感情路线,2017年春节前后,在机场、高铁站等地方投放了“有家的地方就有奥克斯”的形象广告,并联合本来生活网在全国范围内发送上万份新年大礼包,充分展示奥克斯的品牌实力和用户关爱。

温情传递 有家的地方就有奥克斯
在鸡年春节到来之际,奥克斯还

启动了“奥克斯陪你回家”活动,踏上高铁列车,为归乡的游子提前送上新年的祝福和“年货大礼包”。

据悉,1月9日活动当天,在北京南-南京南以及南京南-宁波的高铁上,奥克斯工作人员带着暖心年货及对返乡游子的温暖祝福,踏上了这趟承载游子返乡的高铁列车,将精心准备的年货送给每位乘客。而由奥克斯空调联合本来生活网推出的互动抽奖H5,上线24小时便引发近10万网友争相参与,



上万份年货大礼包一天内被抢空。
跨界新领域 打造有温度的营销策略
奥克斯温暖举动不仅如此,2016

年,奥克斯更是首次跨界影视圈,出品了暖心微电影《树洞的秘密》,唤醒人们内心的爱和关爱,唤醒忙碌中的人们用心去关爱自己的人。

为回馈消费者的支持,奥克斯更携手电影《决战食神》推出了“奥克斯空调食神争霸赛”的互动H5,免费送出2017张《决战食神》电影票。

温暖不止步 2017奥克斯闪耀世界
站在2017年家电行业的新起点上,奥克斯已率先亮相世界中心的舞

台。

2017年,奥克斯将继续以“传递温暖”为营销策略的主题,以切实“关怀消费者”的营销理念,继续打造堪称经典的走心营销,让每次营销活动不仅是品牌推广,更是设身处地的关爱大众。

在消费者心中站稳真诚、暖心企业的位置,赢得消费者信任,从而为奥克斯创造更强大的品牌号召力,力争在2020年实现“千亿市值、千亿规模、百亿利润”的战略目标,实现千亿梦想。

“两会”热点主题迎“黄金时刻” 工银瑞信主题基金业绩闪耀

两会临近,热点主题投资提前引爆,相关概念股不断走强。医疗改革作为历届两会的关注

焦点,亦或成为今年两会最大的热点之一。据银河证券数据,今年以来截至

2月21日,工银瑞信前沿医疗股票基金和工银瑞信医疗保健行业股票基金包揽了医药行业股票基金的冠

军和亚军。除此之外,工银瑞信作为行业主题基金全面布局的“领先者”,旗下

产品短、中、长表现均可圈可点,其中4只行业主题基金今年以来回报位居于同类前十。