网络隐私安全及网络欺诈行为研究分析报告

2018-08-08

前言

2017 年全国数字经济规模达到 27.2 万亿，占 GDP 总量的 32.9%，对 GDP 增长贡献已达到 55%，数字经济成为我国国民经济重要组成部分。中国移动互联网在快速发展的同时，也面临着一些挑战：网民个人隐私泄露、电信网络诈骗等网络安全问题时有发生。因此，预防隐私泄露、打击网络诈骗等非法活动，对保障国民经济健康发展尤为重要。

2018 年 4 月，习近平总书记在全国网络安全和信息化工作会议上指出，要提高网络综合治理能力，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局。要加强互联网行业自律，调动网民积极性，动员各方面力量参与治理。

然而，我国网民在互联网信息保卫战中始终处于弱势地位，网民个体防御能力十分薄弱。因此，网民亟需提高网络安全意识、增强网络安全自我保护能力。

为此，DCCI 互联网数据研究中心联合腾讯社会研究中心针对 Android 端和 iOS 端的手机 APP 进行隐私安全评测，了解移动开发者获取用户手机隐私权限的情况。同时对上半年网络欺诈现象进行研究，分析网络诈骗的最新手段和方法。

本次研究分为两部分，第一部分隐私安全篇，采取 APP 评测的方式，分析常见 Android 手机 APP 和 iOS 手机 APP 的隐私权限获取情况。其中 Android 手机 APP 评测数量为 869 个，评测的隐私权限包括：6 项核心隐私权限（①获取位置信息；②读取手机号；③读取短信记录；④读取彩信记录；⑤读取联系人；⑥读取通话记录）；5 项重要隐私权限(①打开摄像头；②使用话筒录音；③发送短信；④发送彩信；⑤拨打电话)；4 项普通隐私权限（①打开 WiFi 开关；②打开蓝牙开关；③获取设备信息等；④打开数据网络）。iOS 手机 APP 评测数量为 275 个，评测的隐私权限包括：定位服务、通讯录、日历、提醒事项、照片、蓝牙共享、麦克风、语音识别、相机、健康、Homekit、媒体与 APP、运动与健康等共 13 项。

第二部分网络欺诈篇，主要对上半年网络欺诈现象进行详细分析和解读，有助于用户识别网络欺诈信息和行为。数据来自腾讯守护者计划，数据统计周期为 2018 年 1 月 1 日-2018 年 6 月 30 日。部分案例分析得到腾讯安全管理部的支持。

上篇 网络隐私安全篇

一. 移动网络隐私泄露的渠道及风险

截止 2017 年 12 月，中国手机网民规模达 7.53 亿。巨大的用户规模和智能手机上承载的用户信息是一座巨大的金矿。正规的移动开发者可以利用大数据挖掘这些信息更好地为用户服务，而不法分子则可以利用这些信息来发送垃圾短

信、打骚扰电话、窃取手机资费等，还有可能导致进一步的违法犯罪活动，如诈骗勒索等事件的发生。

人们把自己的沟通-社交-娱乐-生活-商务-隐私交给了智能手机及各种 APP，手机早已成为网民的第一终端、成为个人信息中心。如果这些信息没有得到妥善保管和使用，那么用户的隐私、财产、甚至人身安全都有可能遭到侵害。

具体而言，目前通过移动互联网泄露隐私的渠道主要有：①手机 APP；②公共 WiFi；③旧手机；④企业数据。

（一）个别手机 APP 存在隐私泄露风险

手机 APP 各项功能的实现需要调用手机操作系统提供的相应权限。如：导航功能需要调用“获取位置信息”权限，拍照、扫描二维码等功能需要调用“打开摄像头”权限，发送语音功能需要调用“使用话筒录音”权限。因为要实现相应的功能，手机 APP 对以上这些权限的获取是合理的。

然而，不少人应该都有这样的经历，随便注册一个 APP 都会要求读取通讯录等各种权限，即使 APP 的功能用不到这些权限。其实我国《网络安全法》规定：网络运营者采集用户信息时，应遵循合法、正当、必要的原则。但在现实中，一部分移动开发者在申请获取手机权限时采用的是“多多益善”原则，甚至个别移动开发者为追求短期利益，存在售卖用户隐私信息的行为，造成大量用户隐私信息泄露。

后文将详细介绍 Android 端和 iOS 端常见 APP 获取用户隐私权限的情况。

（二）公共 WiFi 钓鱼获取用户隐私信息

随着我国互联网的发展，WiFi 在国内的大小公共场所早已成为标配，商场、饭店、旅馆、咖啡厅、甚至随便一个街边的小饭馆都有免费 WiFi 提供，人们可以方便的接入免费 WiFi 畅游网络。然而，公共场所的 WiFi 并非都是安全的。如果接入不安全的公共 WiFi，用户的隐私信息极有可能被不法分子获取。

通过公共 WiFi 获取用户隐私信息的方式主要有以下三种：

1、恶意架设 WiFi

目前，风险 WiFi 主要有两种类型，一种是不法分子自己架设的，另一种是直接入侵商户提供的 WiFi。当用户连接上风险 WiFi 以后，不法分子可通过多种方式获取用户信息，比如直接抓取数据包、修改 DNS 地址、或者向手机植入木马等等。

常见的是不法分子会在公共场所制造出免费的 WiFi 诱使人们连接。这些 WiFi 的名字常常与周围其他的公共 WiFi 名字类似，以假冒正常的 WiFi，而且这些假冒的 WiFi 大多不需要密码。不法分子通过“域名劫持”可以对用户输入的任何网址进行修改，用户即使输入了正确的网址也会被跳转到“钓鱼网站”。这些钓鱼网站往往伪装成正规银行，购物网站。如果用户在“钓鱼网站”输入用户名和密码进行登录，这些信息就会显示在犯罪分子的电脑上。如果用户在伪装成银行、购物网站的“钓鱼网站”上输入支付密码，后果将不堪设想。

2、流量劫持

流量劫持对不法分子的技术要求较高。不法分子利用公共 WiFi 的漏洞进行攻击，可以任意抓取和修改连接到公共 WiFi 的用户上网信息。如：推送恶意广告、诱导用户进入钓鱼网站等。严重的可以获取用户输入的账号、密码信息，进而造成用户隐私的泄露。

3、通过手机验证码获取用户手机号

这是最为常见的一类免费 WiFi 的服务形式。如果用户想要使用免费 WiFi，一般需要输入手机号获取验证码，这时用户填写的手机号就会被记录下来。

（三）旧手机处理不当，诸多隐私遭盗取

人们的生活越来越离不开手机，人们在手机上进行社交、购物、理财等活动，大量的账户信息和隐私数据被存储在手机上。如果对旧手机处理不当，可能会泄露用户隐私信息，给用户造成损失。

如果旧手机通过二手市场或回收环节落入不法分子手中，通过技术手段对信息加以恢复，手机的原主人的照片、视频等隐私信息可能就会被曝光，短信、通讯录、微信、QQ 的信息会被用来诈骗，银行卡、信用卡或第三方支付被盗刷，邮件里的商业机密被窃取等问题。

（四）企业大数据成黑客攻击主要目标

随着互联网的发展和市场竞争的加剧，用户数据的价值也越来越高。不法分子在利益的驱使下，利用黑客技术非法攻击、盗取企业大量数据，并逐渐形成了一条从数据盗取、售卖、到数据利用的完整产业链条。例如最近的 A 站数据泄

漏事件：黑客攻击并盗取了 A 站近千万用户数据后，这部分数据竟然被明码标价放在暗网上售卖。

发生这种情况的原因，一方面是黑客技术持续提高，在利益的驱使下，不断钻研新的破解方法；另一方面是由于企业网络安全意识薄弱、防范措施不足。

二. Android 端 APP 获取隐私权限情况和越界获取隐私权限情况

（一）用户保护手机隐私信息，须了解掌握相关知识

Android 6.0 操作系统推出以前，Android 系统中虽然有应用通知管理功能，但广受诟病，更为深入的应用权限管理只能依靠第三方 APP 实现。6.0 版本以上的 Android 系统进一步强化了应用权限管理，应用权限管理也成为系统级功能，用户可以方便的自主决定授予 APP 哪些隐私权限，从而更好的保护用户隐私。

但是，即便是否授权 APP 相关权限掌握在用户自己手中，手机隐私泄露风险依然存在。APP 获取隐私权限的用途信息不对称，造成用户始终处于弱势地位，普通用户很难判断 APP 获取相应隐私权限的目的。不法分子依然可以利用 APP 获取不必要的隐私权限，泄露用户隐私信息，给用户造成各种损失。

如今，保护自己手机里的隐私信息，就像开车要看红绿灯、购物要看评论、吃东西要看保质期一样，已经成为人们时刻不能放松的一根弦儿。而这种意识和能力，需要对手机隐私权限知识的了解和掌握。

本次研究选取了 869 个 Android 手机 APP 作为评测对象，对三类隐私权限的获取情况进行分析，这三类隐私权限包括：核心隐私权限、重要隐私权限及普通隐私权限。

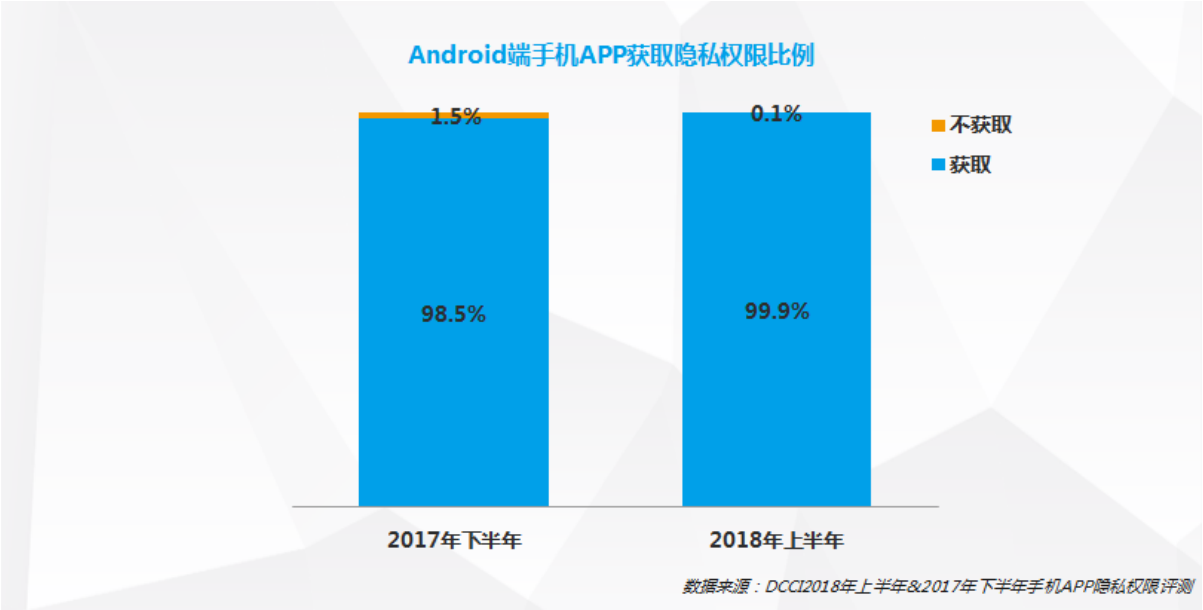
核心隐私权限：访问联系人、获取手机号、读取短信记录、读取彩信记录、读取通话记录及读取位置信息等。这些权限涉及用户敏感信息，一旦被恶意获取，会导致用户的敏感信息外泄，严重时会威胁到用户的财产和生命安全。

重要隐私权限：发送短信、发送彩信、拨打电话、使用话筒录音、打开摄像头等。重要隐私权限主要涉及用户手机功能的使用，一旦被恶意滥用，会造成用户手机业务资源消耗，严重时会产生网络欺诈行为，造成用户财产损失。

普通隐私权限：打开 Wi-Fi、打开蓝牙、打开数据网络及获取设备信息等。普通隐私权限属于低风险隐私权限，但仍存在消耗手机流量资源等风险。

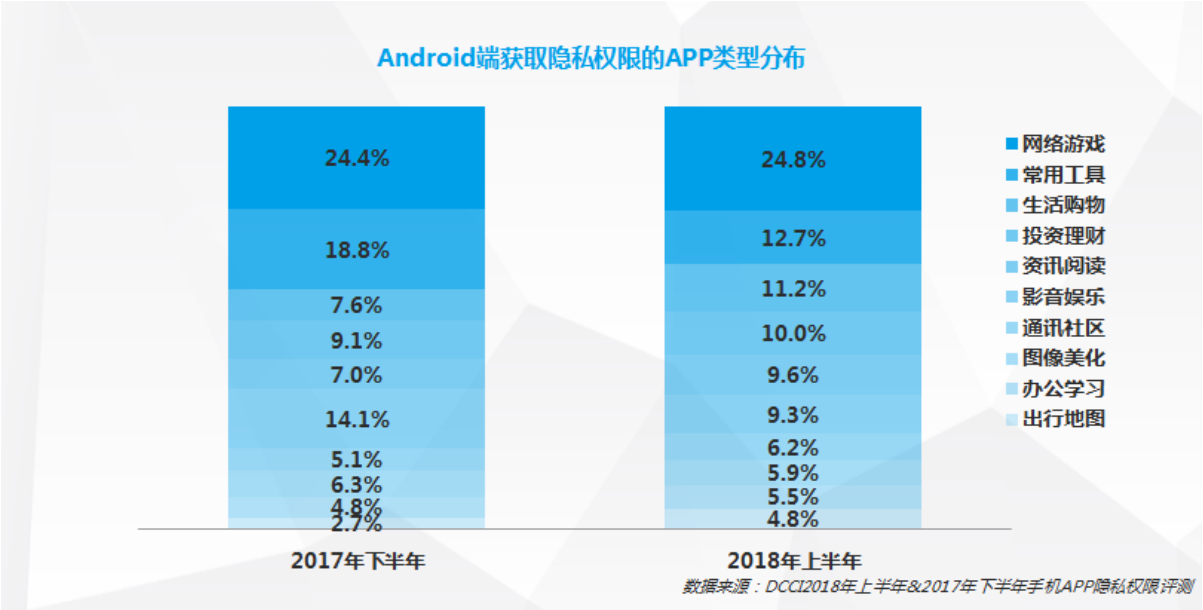
（二）几乎所有 Android 端手机 APP 都会获取隐私权限

评测发现，2018 年上半年 Android 端获取隐私权限的手机 APP 占比相较于 2017 年下半年提高 1.4%，达到 99.9%，未获取隐私权限的手机 APP 仅占 0.1%。几乎所有的 Android 端手机 APP 都会获取隐私权限。



2018 年上半年，在获取隐私权限的 APP 类型分布中，网络游戏和常用工具仍是占比最大的两类应用，分别达到 24.8%和 12.7%。相比 2017 年下半年，网络游戏类 APP 占比进一步提高，常用工具类 APP 占比继续缩小。

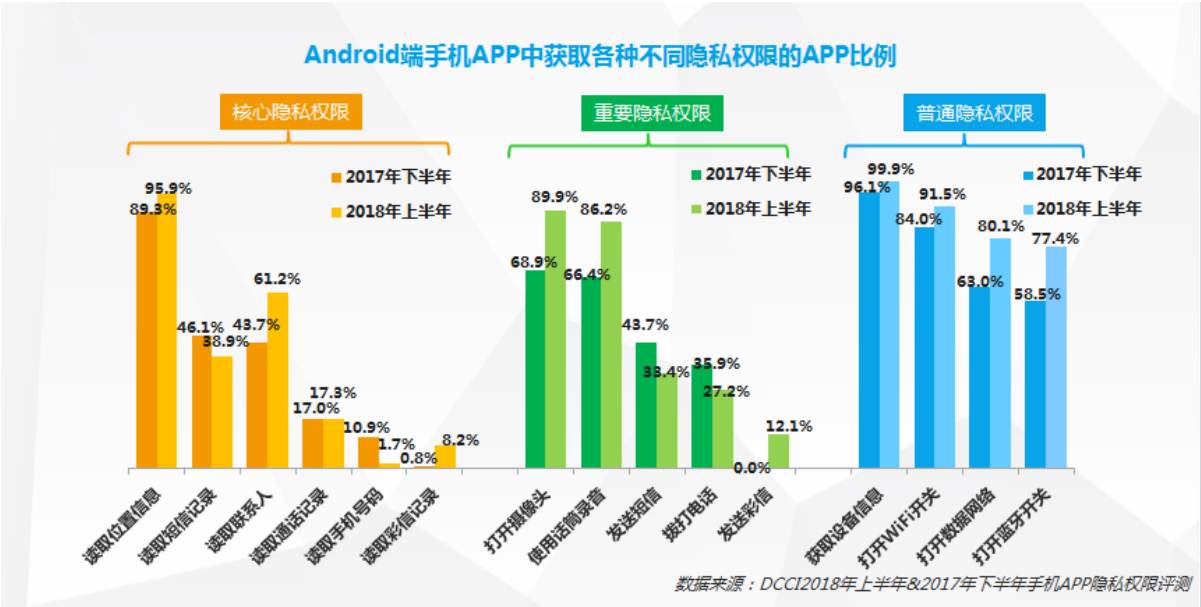
另外，2018 年上半年，生活购物类和投资理财类 APP 占比明显增大，相比 2017 年下半，生活购物类 APP 占比由 7.6%增加到 11.2%，投资理财类 APP 由 9.1%增加到 10%。这一现象与近年移动开发热点向生活购物、投资理财等领域转移有直接关系。



（三）Android 端手机 APP 对三种隐私权限获取比例大幅提高

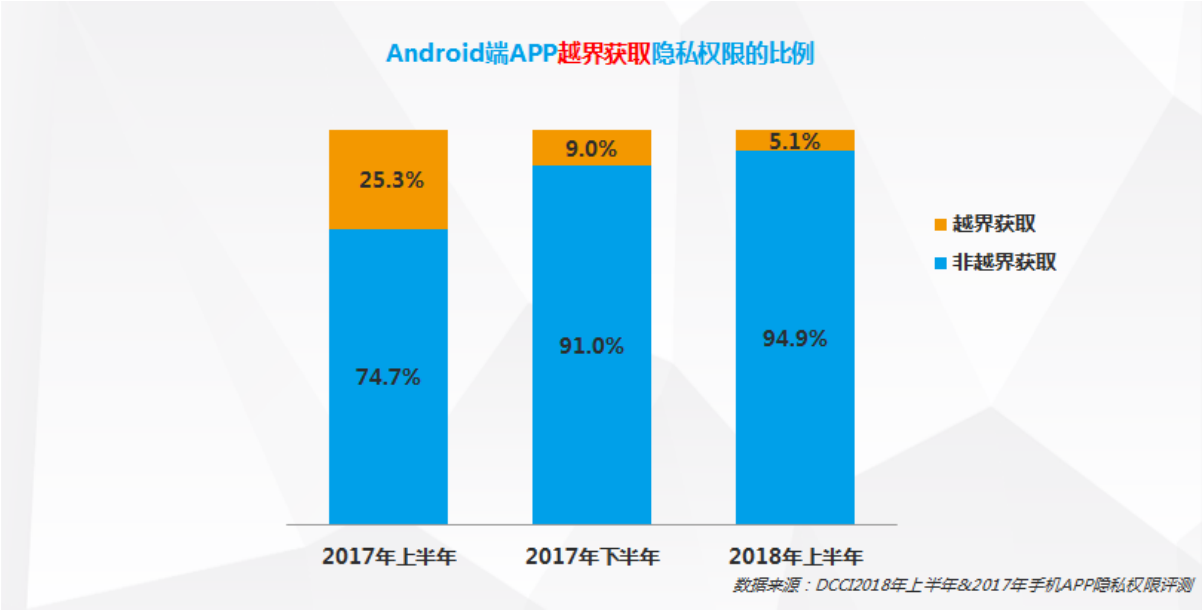
评测发现：Android 端手机 APP 对部分核心隐私权限和重要隐私权限的获取比例大幅提高，它们分别是属于核心隐私权限的“读取联系人”权限，属于重要隐私权限的“打开摄像头”和“使用话筒录音”权限。

相对于 2017 年，获取“读取联系人”权限的 APP 比例由 43.7%增长到 61.2%；获取“打开摄像头”权限的 APP 比例由 68.9%增长到 89.9%；获取“使用话筒录音”权限的 APP 比例由 66.4%增长到 86.2%。

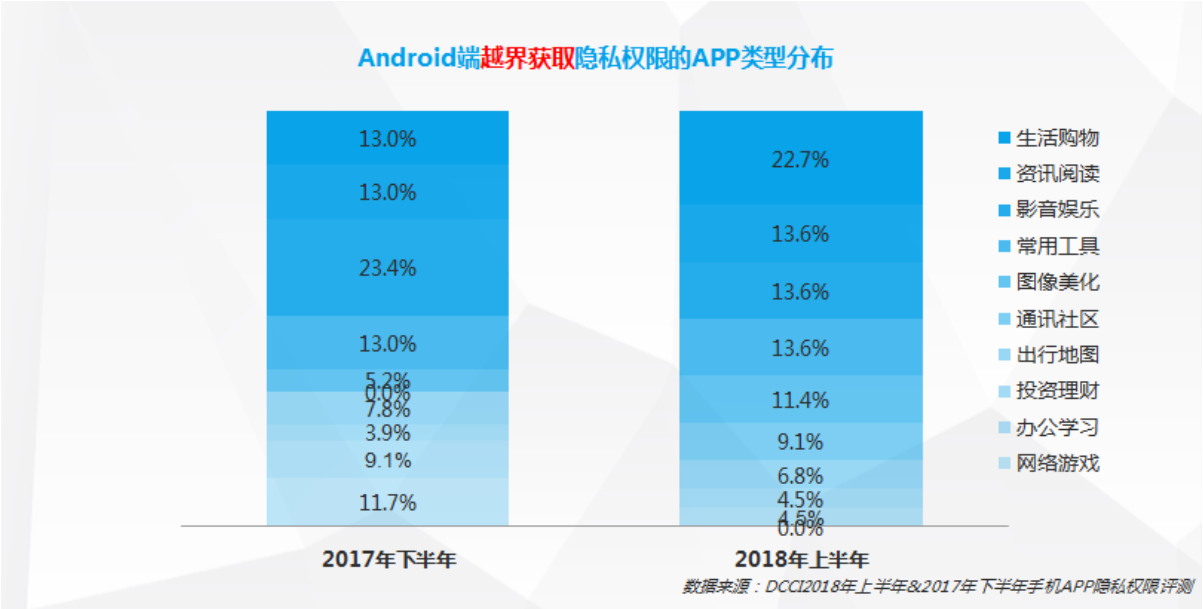


（四）Android 端越界获取隐私权限的 APP 比例进一步下降

与越来越多的 APP 获取隐私权限的趋势形成反差，Android 端越界获取隐私权限的 APP 正在变得越来越少。研究显示：2017 年上半年越界获取隐私权限的 APP 高达 25.3%，2017 年下半年这一比例迅速下降到 9.0%，2018 年上半年越界获取隐私权限的 APP 更是减少到 5.1%。不能不说，2017 年 6 月 1 日正式实施的《网络安全法》促进了移动开发者网络安全意识的提升，越来越多的移动开发者将会在采集用户信息时，遵循合法、正当、必要的原则。



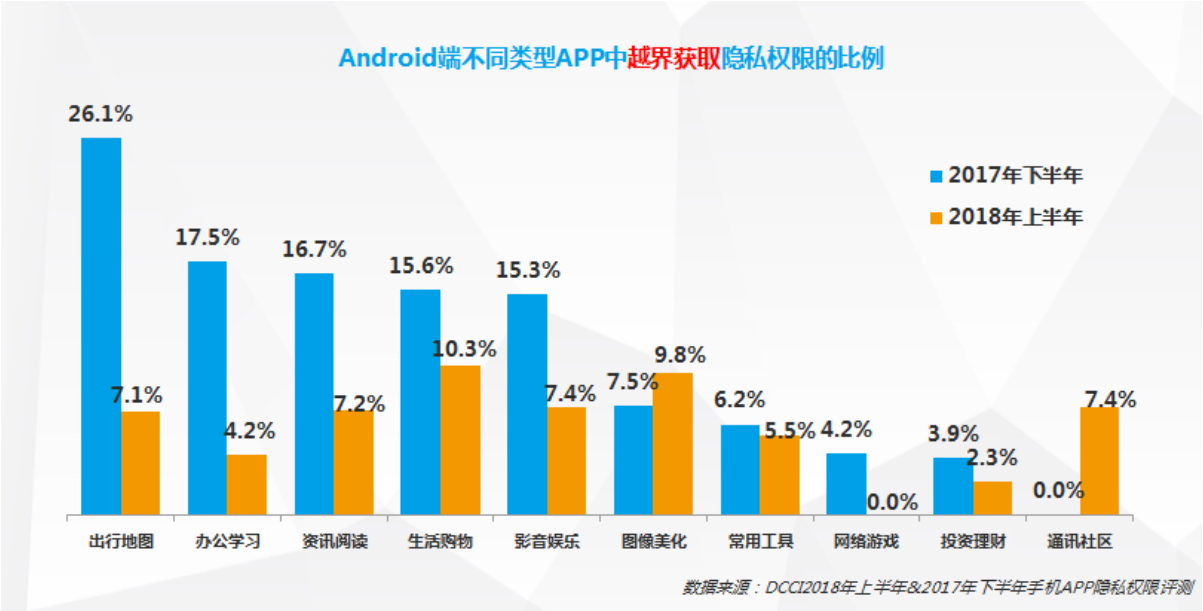
2018 年上半年，在越界获取隐私权限的 Android 端 APP 中，以生活购物类 APP 最多，为 22.7%。资讯阅读、影音娱乐和常用工具类应用并列第二位，均占越界获取隐私权限 APP 总数的 13.6%。



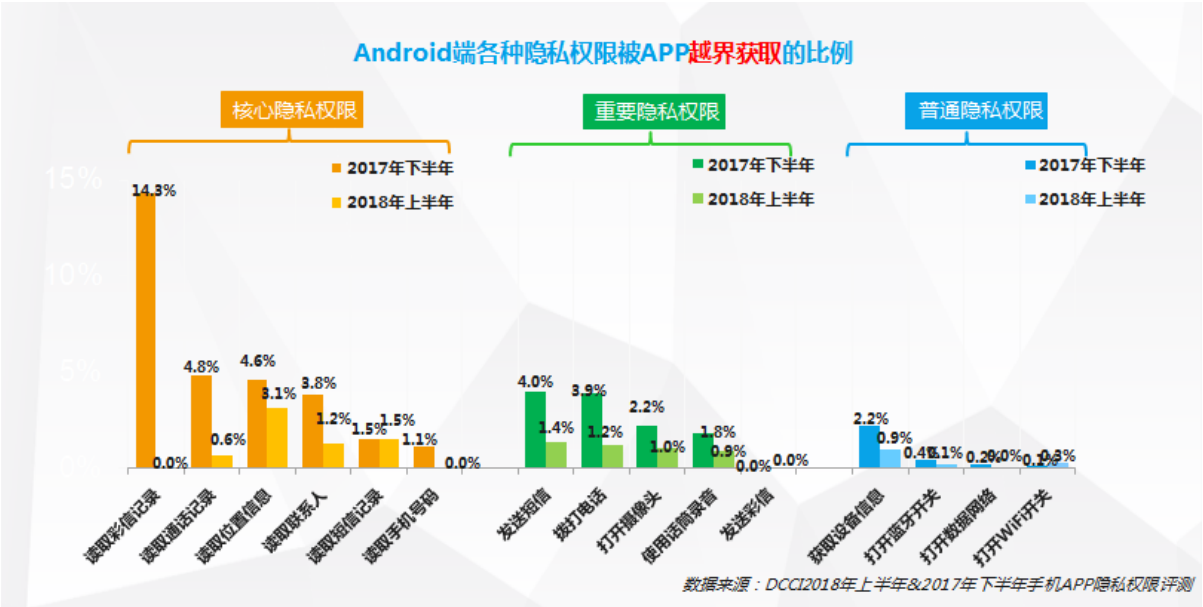
研究发现：深入到不同类型的 APP 来看，多数类别的 APP 越界获取隐私权限的比例明显下降。其中，出行地图类和学习办公类 APP 下降幅度最大：相比 2017 年下半年，2018 年上半年出行地图类 APP 越界获取隐私权限的比例由

26.1%下降到了 7.1%，办公学习类 APP 越界获取隐私权限的比例由 17.5%下降到了 4.2%。

另外，在 2018 年上半年，生活购物类 APP 是越界获取隐私权限问题最为严重的 APP 类别：有 10.3%的生活购物类 APP 存在越界获取隐私权限问题。其次是图像美化类,存在越界获取隐私权限问题的 APP 比例为 9.8%。



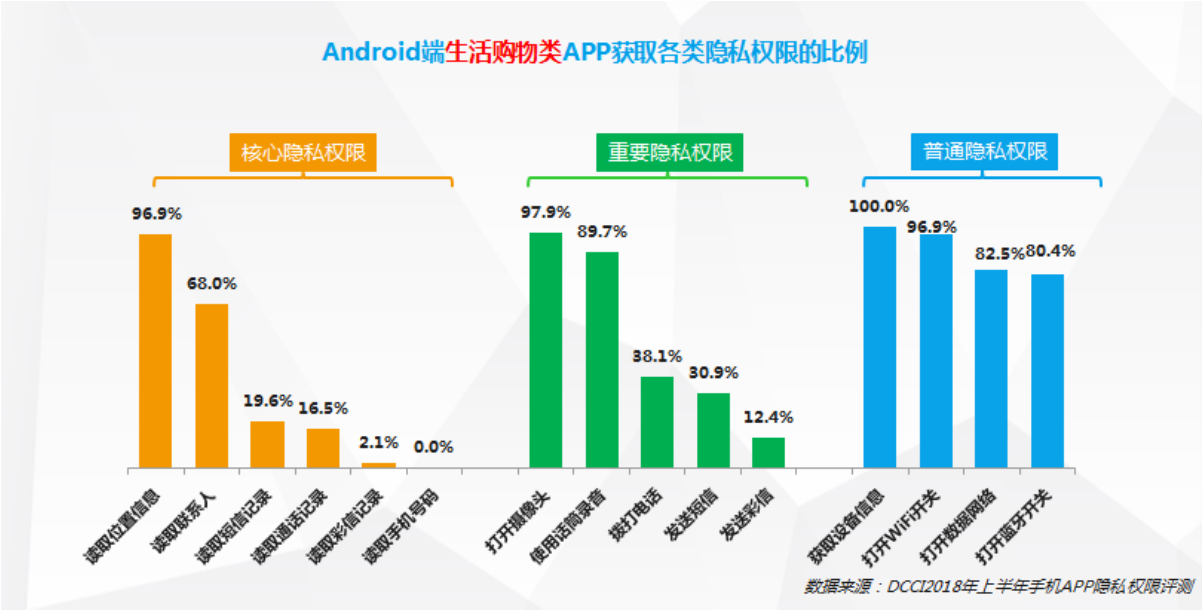
对不同隐私权限被越界获取的情况进行分析发现，2018 年上半年 Android 端各种隐私权限被越界获取的情况均有进一步改善。整体来看，虽然越界获取的隐私权限仍然集中在核心隐私权限与重要隐私权限上，但多数越界获取隐私权限的 APP 比例已降到 3%以下。



三. Android 端典型类型 APP 获取隐私权限说明

（一） 生活购物类 APP

生活购物类 APP 因其自身的特点，需要获取的隐私权限相对比较广泛。大平台、功能全面的生活购物类 APP，不仅有购物、支付功能，还有客服沟通、快递位置查看、好友系统等功能。从本次评测数据来看，生活购物类 APP 主要获取“读取位置信息”、“读取联系人”、“打开摄像头”、“使用话筒录音”等隐私权限。



生活购物类 APP 要求获取必要的隐私权限有其合理性：

读取位置信息：生活购物类 APP 获取用户位置信息，可为用户提供位置附近的服务。如：外卖 APP 需要根据用户位置提供附近的餐饮信息，电商 APP 需要根据位置确定用户所在区域的物流仓库是否有用户需要的商品。

读取联系人：社会化是当前移动互联网发展的趋势，生活购物类 APP 也不例外。部分生活购物类 APP 具有加为好友功能，获取“读取联系人”权限可方便用户在 APP 中添加好友。如：手机淘宝具有添加“淘友”功能。

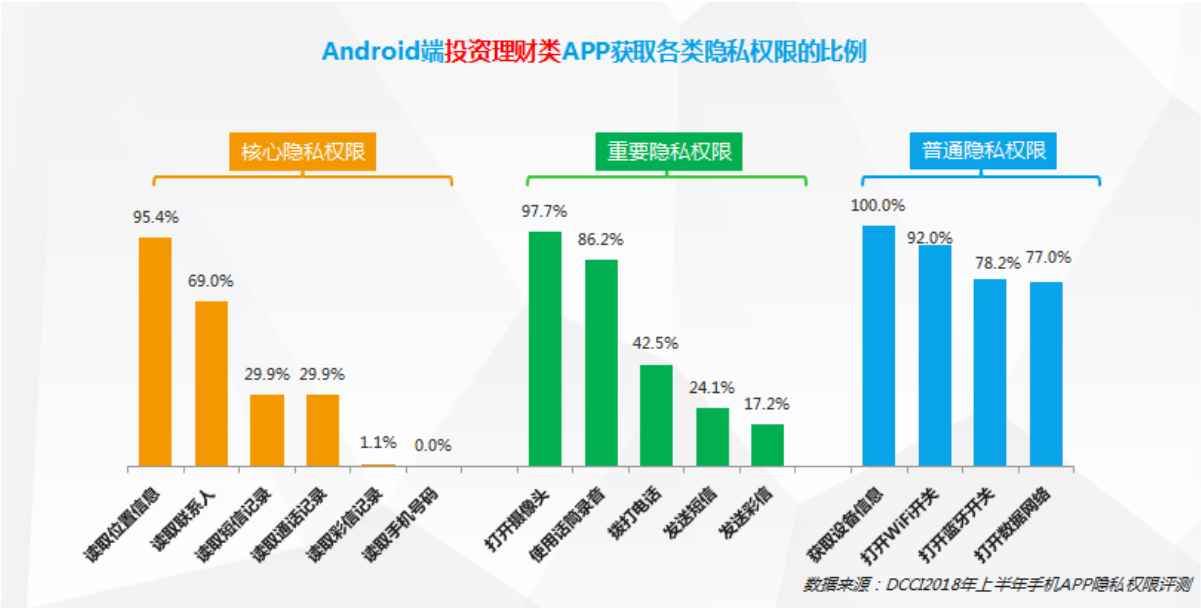
打开摄像头：如今，拍照、扫描二维码等功能都已成为多数 APP 的标配。生活购物类 APP 获取“打开摄像头”权限，可以方便用户随时通过 APP 使用摄像头拍照。生活购物类 APP 的宝贝评价、拍照识别、扫二维码、扫福字等功能都需要使用摄像头。

使用话筒录音：生活购物类 APP 获取“使用话筒录音”权限，最常见的应用场景是发送语音消息给客服，其次语音搜索宝贝等功能也需要调用“使用话筒录音”权限。

（二） 投资理财类 APP

随着人们的生活越来越富裕和投资理财观念的增强，投资理财类 APP 成为近年移动开发的热点领域之一，应用市场上投资理财类 APP 明显增多。

本次对投资理财类 APP 获取隐私权限的情况研究发现，“打开摄像头”、“读取位置信息”、“使用话筒录音”、“读取联系人”是投资理财类 APP 获取最多的四大隐私权限。获取这四大隐私权限的 APP 分别占 97.7%、95.4%、86.2%和 69.0%。



投资理财类 APP 获取各项隐私权限的应用范围如下：

打开摄像头：投资理财类 APP 获取“打开摄像头”权限多用于支付、转账等功能。

读取位置信息：如今，很多投资理财类 APP 除原有的“本职”功能外，还具有生活服务功能，通过获取“读取位置信息”权限，能够自动识别您所在的地区，方便用户使用进行生活缴费、订餐、订票等消费行为。

使用话筒录音：投资理财类 APP 获取该权限后，可实现语音搜索、语音咨询、留言等功能。

读取联系人：投资理财类 APP 获取“读取联系人”，一方面方便用户向联系人分享、推荐“理财产品”，另一方面也是因为部分投资理财类 APP 设有好友功能。

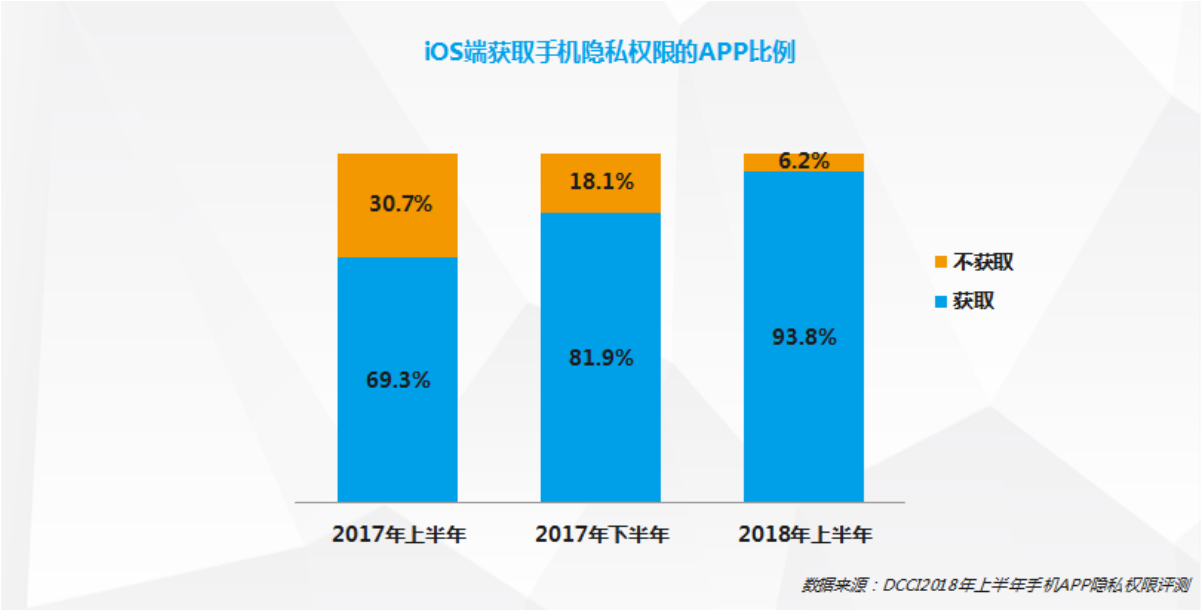
四. iOS 端 APP 获取隐私权限情况

iOS 操作系统一向口碑较好，但也不是绝对安全。在 2017 年 10 月的 GeekPwn 国际安全极客大赛上，一名中国选手现场演示了自己发现的 iOS11 系统最新漏洞。在演示中，用户打开黑客提供的伪装连接后，黑客就能获得 iPhone8 的最高权限，可以盗取用户手机内的隐私信息、在手机上自由安装恶意 APP 等。

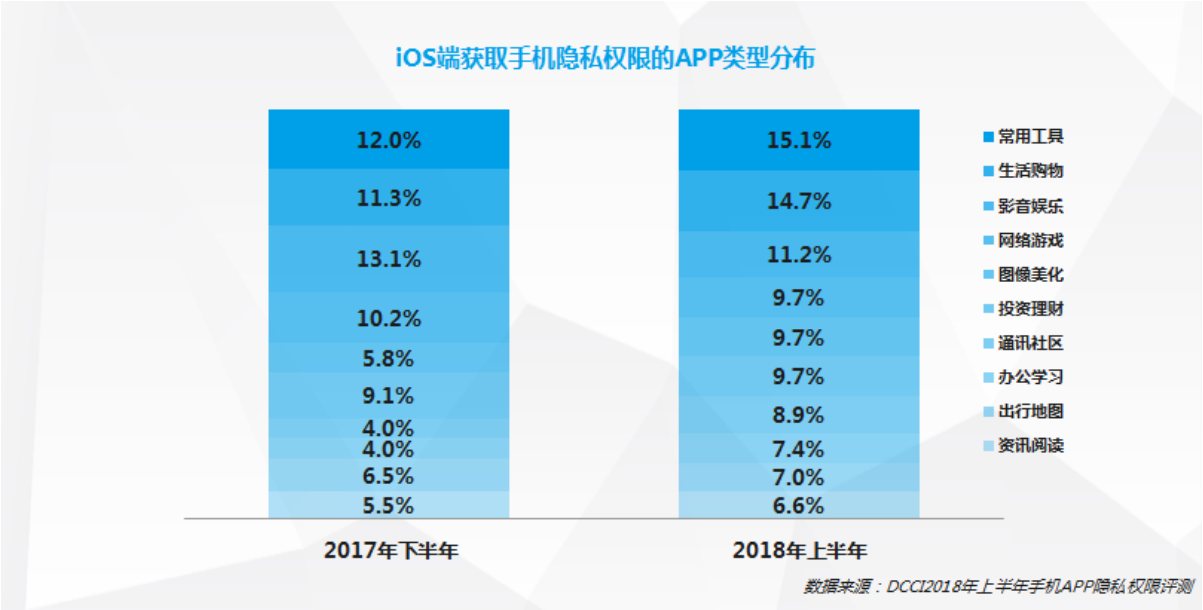
为了确保用户隐私安全，一方面需要苹果公司及时修复发现的系统漏洞，另一方面用户也需要提高安全意识和能力，尽可能的保护自己的隐私，阻止 APP 越界获取不必要的隐私权限。

（一）iOS 端获取隐私权限的 APP 比例继续上升

调查发现，iOS 端获取手机隐私权限的 APP 比例呈上升趋势，2018 年上半年 iOS 端获取手机隐私权限的 APP 比例已达到 93.8%。仅仅时隔一年左右，iOS 端获取手机隐私权限的 APP 比例增加了 24.5%。

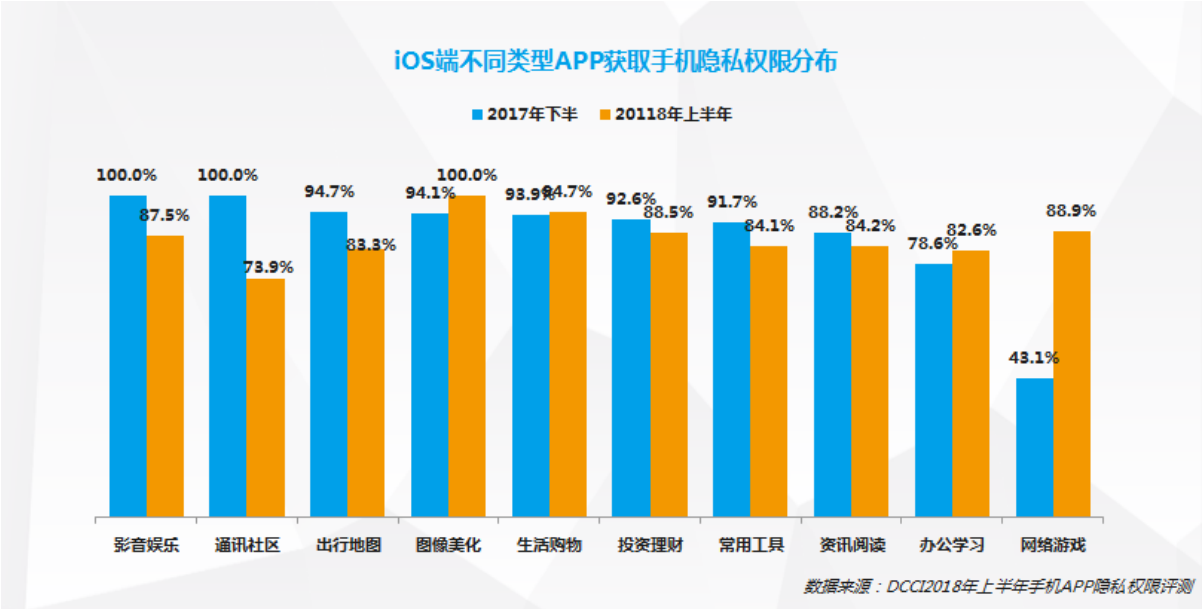


评测发现：在 iOS 端获取手机隐私权限的 APP 中，2018 年上半年常用工具类、生活购物类和影音娱乐类 APP 占比最大，分别占 15.1%、14.7%和 11.2%。



（二）iOS 端网络游戏类 APP 获取隐私权限比例大幅增加

本次针对 iOS 端不同类型 APP 获取隐私权限的情况分析发现：除通讯社区类 APP，其他类型的 APP 获取隐私权限的比例都在 80%以上。其中，图像美化类 APP 获取隐私权限比例最高，达 100%；网络游戏类 APP 获取隐私权限比例增幅最大，由 2017 年下半年的 43.1%增长到 2018 年上半年的 88.9%，增幅达 45.8%；



五. 手机用户隐私安全保护建议

2018 年 5 月 1 日，《信息安全技术个人信息安全规范》正式实施。《安全规范》的正式发布结束了《网络安全法》实施以来个人信息保护原则性规定较多而具体措施欠缺的局面，解答了广大互联网企业的困惑升级，使互联网企业能够更好履行个人信息保护义务。

在企业层面，微信、淘宝、支付宝、滴滴出行、京东商城等五款产品和服务在主动告知提示、允许用户选择的基础上，还为用户提供“一站式”撤回和关闭授权操作。

而用户作为隐私信息的源头和最终受害者，更需要加强网络安全意识和知识，了解隐私保护手段。本报告为用户提供以下手机隐私安全保护措施 ：

（一）手机 APP 使用安全建议

1.下载：尽量选择官方渠道，特别是投资理财、银行类 APP，不要下载来历不明的山寨 APP；

2.授予权限：谨慎授予 APP“发送短信”、“读取短信”、“读取联系人”、“读取位置信息”等权限；

3.流量使用：观察 APP 流量使用情况，对一些使用大量流量且没有告知的 APP，及时检查和删除；

4.自动登录：不要把手机中的 QQ、微信、微博等设置为“自动登录”，密码最好定期更换；

5.退出不彻底：不再使用 APP 时应彻底退出，如果退出不彻底会给后台运行的恶意程序以可乘之机；

6.自启动：某些 APP 即使用户没有打开过，也会自己启动常驻后台，这时最好想办法关闭其自启动功能。如果仍然自启动，则建议卸载。

（二）公共 WiFi 使用安全建议

1、在公共场所尽量不去使用没有密码的免费 WiFi；

2、尽量向服务人员询问商家提供的免费 WiFi 和密码，并认真核对 WiFi 名，避免接入假冒 WiFi；

3、将手机上的 WiFi 设置为手动连接，避免不经意间连入风险 WiFi。

（三）旧手机安全处理建议

旧手机里的信息是如何泄露的？实际上，手机操作系统执行文件删除时，仅是对文件做了一个“删除”标记，但存储的数据本身依然存在，只是处于一个可覆盖的状态。如未进行新的数据操作，最上层的数据很容易被恢复。因为手机存储的数据可反复被覆盖，数据恢复一般只能恢复最上层的数据。如果是最近一次存储的照片、通讯录等，很容易被恢复。所以建议采取以下措施防止旧手机里的信息泄露：

1. 把重要数据备份后，多次存取一些无关紧要的内容或者大型文件（如电影），直至将手机的存储空间全部占满。这样数据即使被不法分子恢复，也只能恢复一些无关紧要的数据;

2.给手机安装一个“文件粉碎机”，进行全盘擦除;

3.将旧手机低价处理或扔掉前，一定要确保手机里的隐私信息已经被妥善处理。

下篇 网络诈骗篇

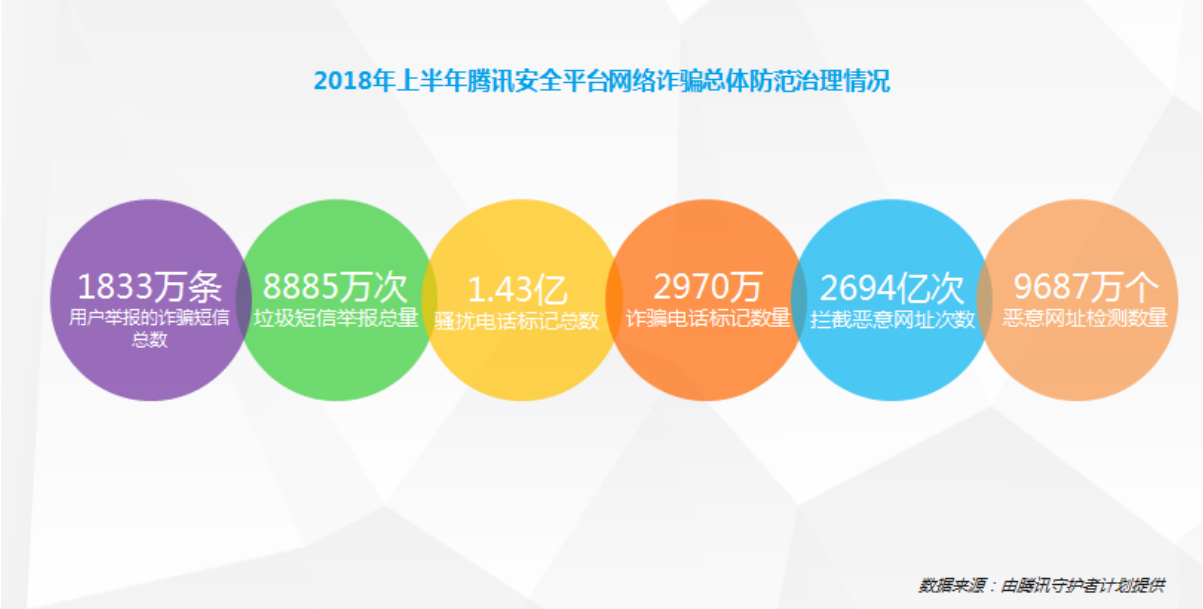
六. 2018 年上半年网络诈骗发生情况分析

（一）2018 年上半年腾讯安全平台网络诈骗总体防范治理情况

基于腾讯守护者计划提供的数据，2018 年上半年腾讯安全实验室共检测到恶意网址数量接近一亿个（9687 万个），拦截恶意网址高达 2694 亿次，相当于每天拦截 15 亿次。

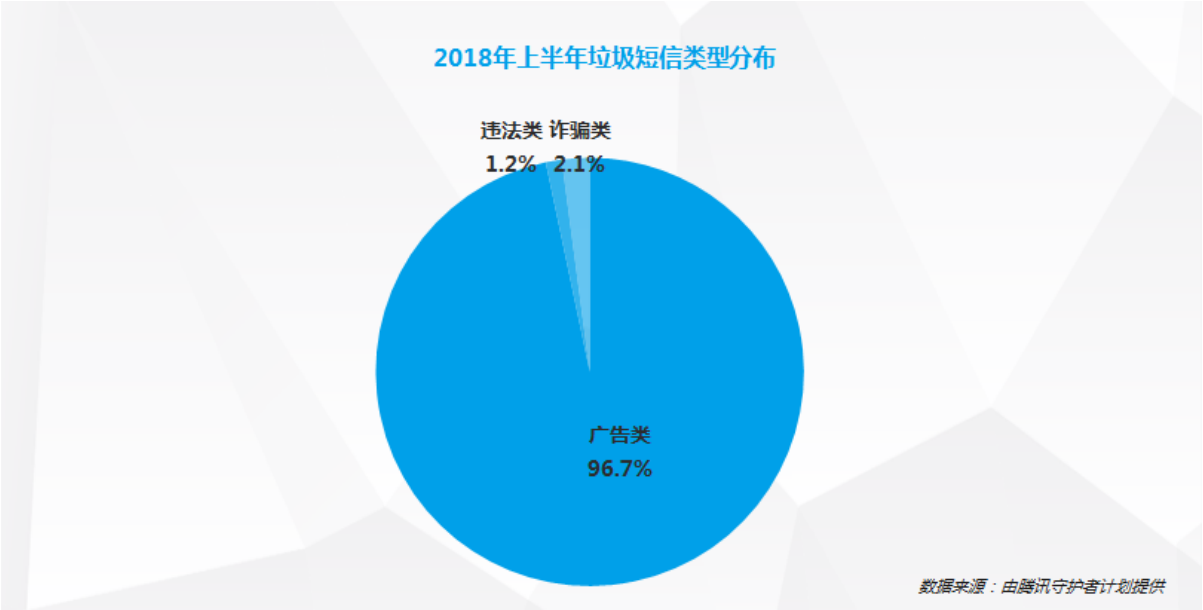
另外，诈骗电话和诈骗短信形势依然严峻。2018 年上半年，腾讯手机管家诈骗电话标记总数为 2970 万个，拦截诈骗短信 1833 万条，相当于每天标记诈骗电话 16 万个，拦截诈骗短信 10 万条。

巨大的标记和拦截数量，展示了腾讯安全实验室保卫网络安全的成果。同时也警示广大网民用户当前网络安全环境仍不容乐观，需要随时警惕诈骗电话、诈骗短信、恶意网站等网络安全风险，避免上当受骗造成不必要的损失。

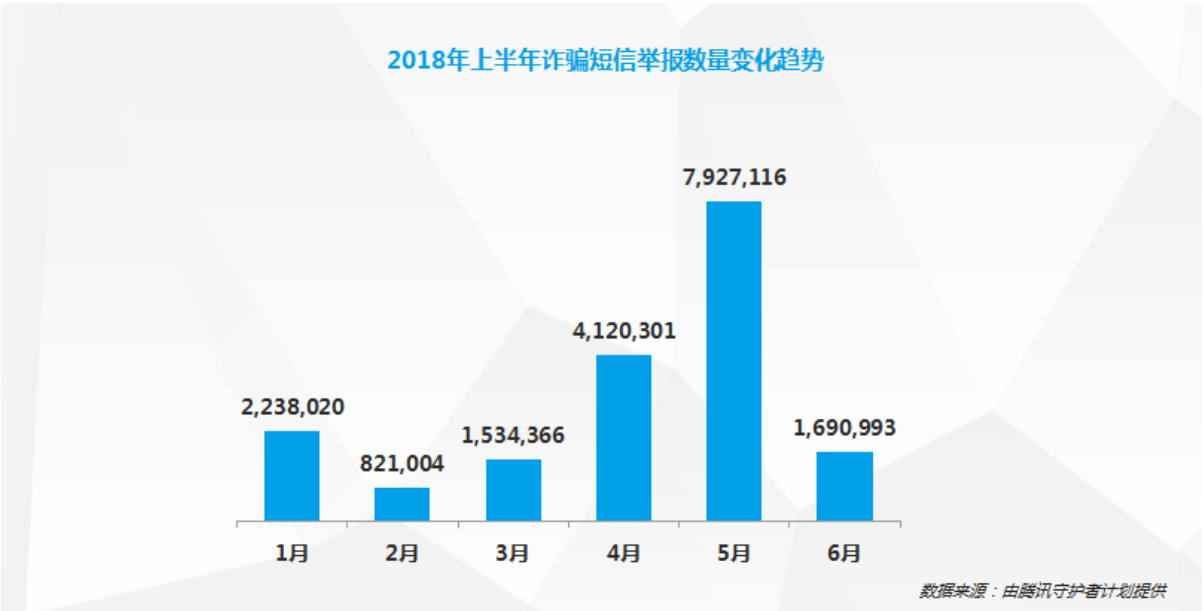


（二）世界杯前夕诈骗短信成倍增长

2018 年上半年数据显示，在腾讯手机管家用户举报的垃圾短信中，广告类占 96.7%，是最多的一种垃圾短信类型。诈骗类和违法类短信占比分别为 2.1%与 1.2%。虽然诈骗类和违法类短信比例很低，但由于其基数巨大仍然值得警惕。

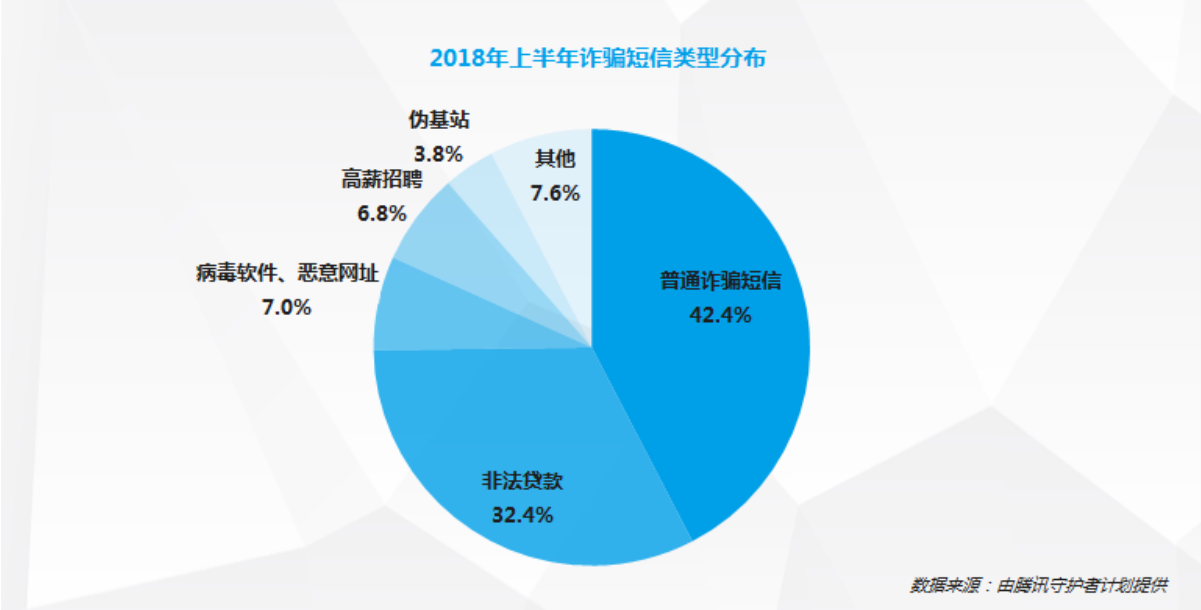


2018 年上半年，每月被举报的诈骗短信多在百万条以上，只有 2 月受春节影响被举报诈骗短信数量较低。其中，3 月-5 月的诈骗短信数量出现成倍增长趋势，并在世界杯前夕的 5 月达到顶峰。5 月份诈骗短信超过 792 万条，是 4 月份诈骗短信数量的近两倍，是 2 月份诈骗短信数量的近 10 倍。



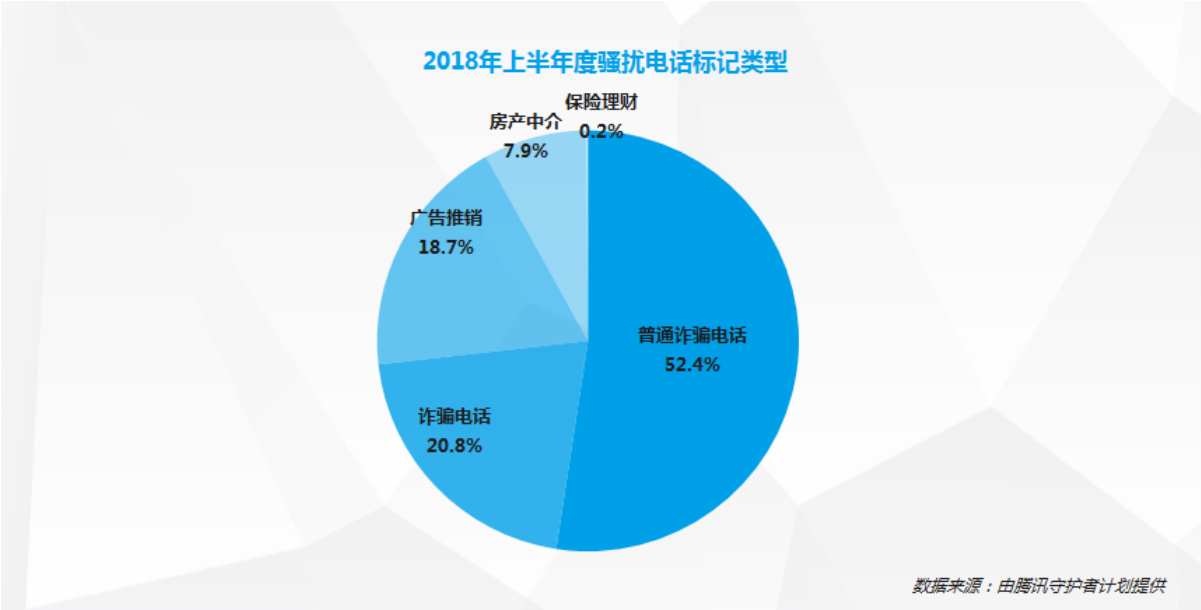
2018 年上半年最常见的诈骗短信类型分别为非法贷款、病毒软件&恶意网址、伪基站、高薪招聘和网购。其中非法贷款短信占 32.4%，即每三条诈骗短信就有一条是“非法贷款”。

随着我国经济社会的快速发展，人们对美好生活的向往、对快速致富的追求越来越迫切，加之消费观念的转变，使得部分用户更容易成为不法分子实施贷款诈骗的对象。用户收到贷款类的短信时一定要提高警惕，切勿上当受骗，并及时举报。

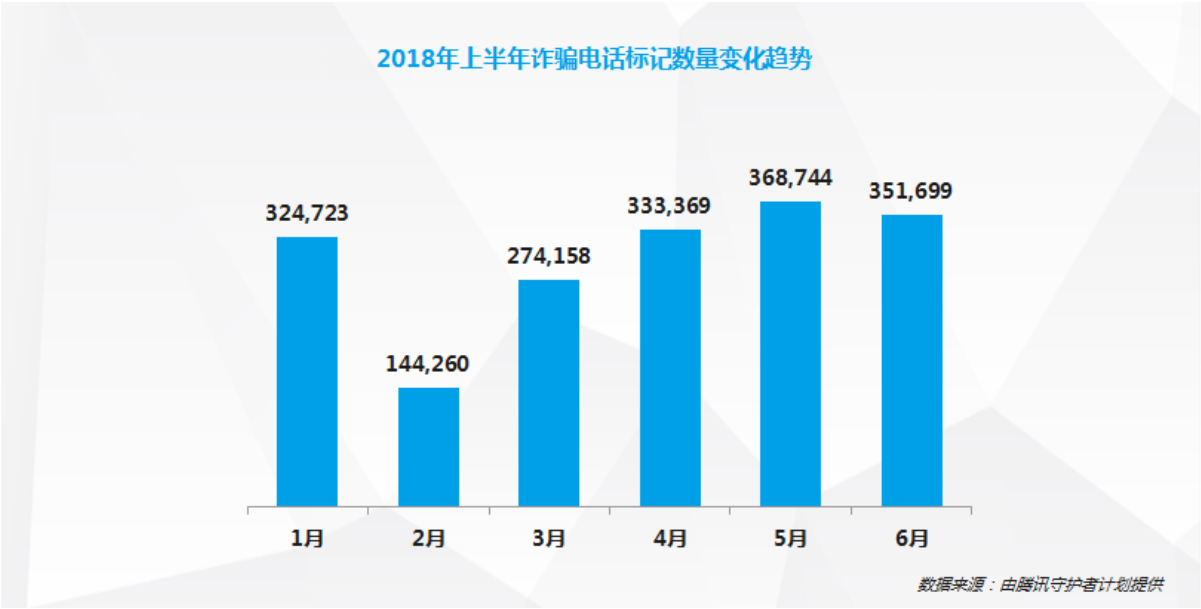


（三）上半年诈骗电话呈增长趋势

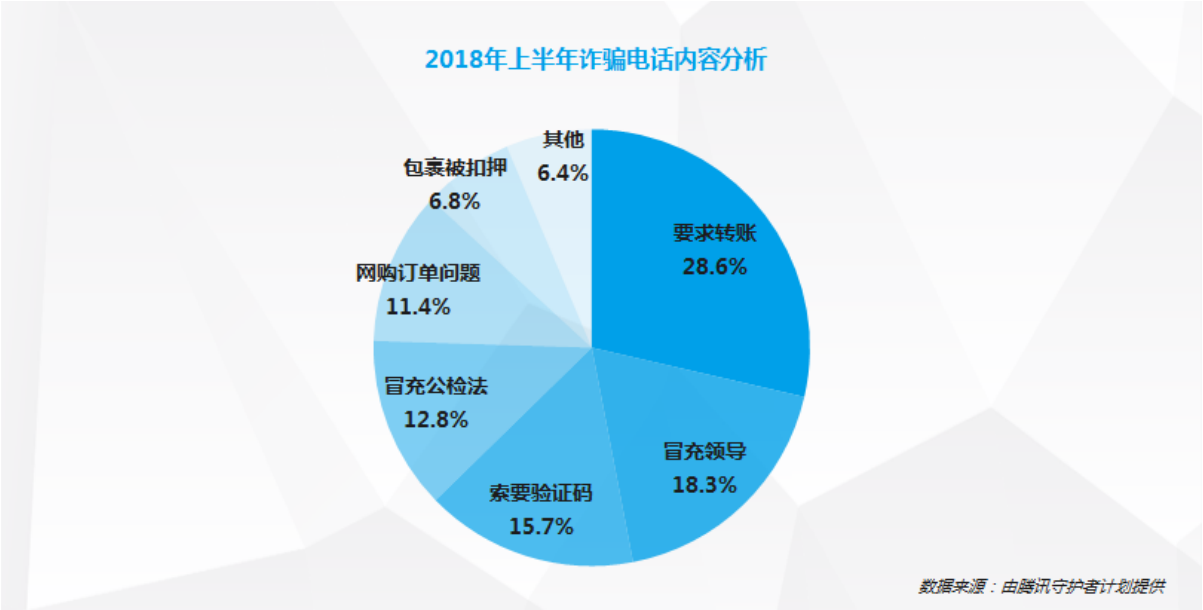
2018 年上半年，在腾讯手机管家用户标记的骚扰电话中，诈骗类电话是第二大骚扰电话类型，20.8%的骚扰电话是诈骗类电话，即五个骚扰电话里就有一个是诈骗电话。由于诈骗电话骗术相当高明且极具蛊惑性和煽动性，当用户接到不明电话时，一定要多加小心，确认诈骗电话及时报警。



2018 年上半年，诈骗电话与诈骗短信同样呈现出增长趋势，并在 5 月到达高峰。5 月份诈骗电话数量超过 36 万，是 2 月份的 2.5 倍。

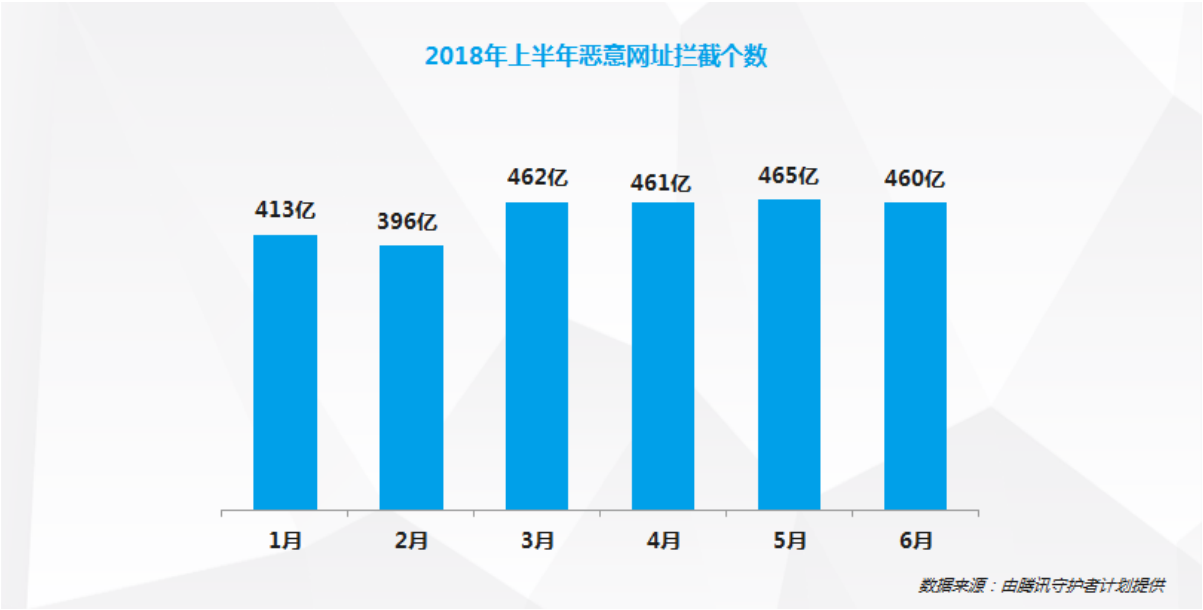


诈骗电话形式花样百出，令人防不胜防。通过对 2018 年上半年诈骗电话内容分析发现，有 28.6%的诈骗电话会以各种听上去合理的理由要求用户转账；有 18.3%是冒充领导；有 15.7%是索要验证码；有 12.8%冒充公检法，编造用户违法信息让用户缴纳罚款。此外还有 11.4%的诈骗电话称用户网购订单有问题，6.8%的诈骗电话会声称用户快递包裹被扣。

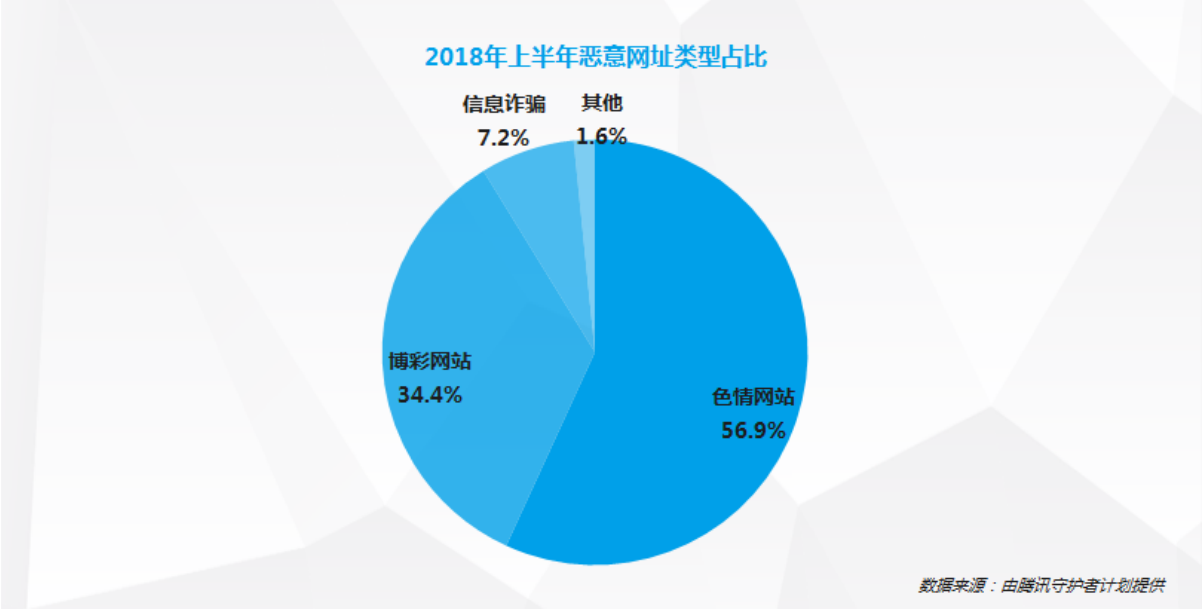


（四）每三个恶意网站就有一个是博彩网站

腾讯安全实验室对恶意网址的拦截数据显示：从 2018 年 3 月开始，拦截恶意网址数量明显增加，随后的 4 月-6 月拦截恶意网址数量保持稳定。5 月份拦截恶意网址数量最高，达 465 亿个。



2018 年上半年，恶意网址类型以色情网站占比最大，占比高达 56.9%；其次是博彩网站，占比达 34.4%，即每 3 个恶意网址就有一个是博彩网站。博彩网站历来是恶意网站的重要类型。2018 年上半年博彩网站占比较大，四年一度的世界杯无疑是重要刺激因素。



七. 网络诈骗常见类型汇总

（一）代办大额信用卡

以代办大额信用卡的方式种植木马。犯罪分子声称可以办理大额度信用卡，将木马链接伪装成信用卡申请协议等文件，诱骗收信人点击安装。

（二）冒充银行客服

冒充银行客服以积分兑换、电子密码器失效等方式种植木马。犯罪分子通过技术手段伪装成银行客服如：95588、95533 等，向不特定多数人发送短信，以提醒客户积分兑换、电子密码器到期等方式，诱惑收信人点击木马网址。

（三）冒充购物返礼

以购物返礼、降价促销等方式种植木马。犯罪分子通过假冒京东、淘宝等商家进行购物返礼、积分兑换或者谎称自己有某某物品，因资金周转等原因降价甩卖等方式，诱惑收信人点击木马网址。

（四）冒充通知交通违法

以通知交通违法的方式种植木马。犯罪分子以提醒收信人交通违法并提供违法照片链接的方式，诱惑收信人点击木马网址。

（五）冒充移动客服

冒充移动客服 10086 以积分兑换、感恩回馈、话费余额不足等方式种植木马。犯罪分子通过技术手段伪装成移动客服 10086 向不特定多数人发送短信，以通知客户积分兑换、感恩回馈、话费打折等方式，诱惑收信人点击木马网址。

（六）发诱惑力照片

利用彩信种植木马。犯罪分子往往发送一张图像较小或者比较有诱惑力的照片，手机持有人点击查看后会自动跳转至含有木马病毒的网址。

（七）冒充同学好友

冒充同学、好友、同事以聚会照片、整理的资料、帮忙查看合同等方式种植木马。犯罪分子往往以熟人之间日常聊天的语气，称“整理了同学聚会的照

片”、“发点东西留念”、“推荐个很不错的网站”或者“帮忙审看一下合同/资料”等方式，诱惑收信人点击木马网址。

（八）爆料恐吓

以爆料、恐吓等方式种植木马。犯罪分子往往以威胁恐吓的语气，声称“你老公/老婆有外遇了”、“瞧你做的好事”或者“你朋友的手机中木马了，有照片”等，诱惑收信人点击木马网址链接。例如：“某某某我是某某某，你们在外面搞的事都发在网上去了，你自己看看，网址 XXXXX”。

（九）冒充学校老师

冒充学校或教师以学生查看成绩、平时表现等方式种植木马。犯罪分子冒充学校教师，以提供给学生家长查询孩子成绩、平时表现的网址的方式，诱惑收信人点击木马网址。

（十）冒充第三者

言语刺激收信人的方式种植木马。犯罪分子在通过非法渠道获取手机机主的信息后，声称与机主的老公/老婆真心相爱，有照片为证，诱惑收信人点击木马网址。

八. 上半年典型网络诈骗案例说明

（一）“高考后”诈骗

诈骗手法 1：“高考补助金”诈骗

骗子冒充教育局、财政局等政府部门工作人员，通过电话报出考生姓名、学校等信息，通知考生领取“高考补助金”，诱骗考生或家长进行转账诈骗。

诈骗手法 2：“黑客改分”诈骗

骗子自称黑客可为成绩不理想的高考生修改高考成绩。骗子通过发送带有考生姓名、学校、高考分数等信息的短信打消考生或家长的疑虑，并告知如需修改分数可通过添加 QQ 或微信详谈。在进一步详谈中，骗子为了进一步获取考生或家长的信任还会发送各科成绩截图。然后一步步骗取考生或家长的“成绩修改费”。

诈骗手法 3：“保送”诈骗

骗子谎称可以保送上名牌大学、军校：不法分子以高仿的证件，以高校自主招生、定向招生等名义，称其有内部指标、机动指标等诈骗考生钱财；还有不法分子采取伪造军校招生公文、公章等手段获得考生或家长信任，同时还会声称军校为特殊院校，不会经过统一的招录途径录取考生。

诈骗手法 4：伪造录取通知书诈骗

不法分子通过发送短信、发放通知书的方式，要求家长或考生先缴纳一部分费用，借机实施诈骗。

诈骗手法 5：短信链接植入病毒诱骗点击

骗子模仿“校讯通”、“高考直通车”等向考生及家长发送带有链接的“服务短信”，一旦点击链接进入，手机立刻被植入木马病毒，进而窃取绑定的银行卡账户、密码等资料，转走钱财。由于植入木马病毒，手机转账后，银行回执短信被截留，使得被害者很难发现钱款被盗取。

（二）“世界杯”网络诈骗

诈骗手法 1：赌球、竞猜诈骗

很多人热衷足球，四年等一回的世界杯更是不容错过。看球、熬夜、喝啤酒、吃小龙虾相信是很多球迷的标准行为，而赌球也是其中一项重要的世界杯活动。

世界杯期间赌球诈骗频发，骗子号称能“100%预测足球”、“100%操作足球”，一步步引导用户上钩，欺骗钱财。一般的骗局很容易会被识破，但是为什么这个骗局会一直存在而且一直会有人相信呢？其实骗局的真相很简单：

1、小组赛的赛制分赢、平、负三种情况，骗子也会把诈骗对象分为 A/B/C 三组，假如骗子掌握了 100 万个手机号码或用户邮箱，则会分成每组 33 万的形式，然后向 A/B/C 三组用户发送不同的预测结果，其中必有一组是准确的。

2、猜错的那些用户全部舍弃，再将剩余的 33 万分成每组 11 万，然后依次类推。

3、那些一直在预测成功小组中的用户就会越来越相信背后的神秘人物，开始上钩，而此时骗子则放出竞猜的渠道和巨额的奖金诱惑，在触手可得的奖金面前很多人都会放下心里防备，转账付款。

诈骗手法 2：获奖诈骗

发送虚假的获奖信息是世界杯网络诈骗的主要方式之一。不法分子伪装成官方合作伙伴邮件告知收件人在世界杯活动中获得大奖。此类邮件通常包含 PDF、WORD 附件，邮件通常要求获奖者填写详细的个人资料，如姓名、身份证号、电话号码、家庭住址等。有的邮件甚至会要求收件人支付部分手续费或者邮费进行诈骗。

诈骗手法 3：钓鱼网站&恶意 APP 诈骗

不法分子假借“世界杯直播”、“世界杯赛事”的名义，常制作自称是世界杯官方合作伙伴的钓鱼网站或恶意 APP 来窃取受害者的隐私信息，甚至银行和其他帐户凭证。世界杯期间钓鱼网站&恶意 APP 常包含以下几类：

1.仿冒正规博彩网站网站&APP；

2.仿冒 FIFA 官方的购票网站；

2.仿冒航空公司提供廉价机票；

3.仿冒世界杯官方纪念品商店；

（三）荐股诈骗

诈骗手法 1：玩概率

骗子从互联网等渠道购买公众个人信息，再对目标人群进行分组，推送次日某只个股“大涨”信息，通过广撒网和博取大涨概率来获得受骗用户，骗取会员费。

诈骗手法 2：炒软件

以各种噱头向特定群体推销各类“荐股神器”软件，诱骗用户购买软件或在软件中进行充值，骗取用户钱财。

诈骗手法 3：假平台

犯罪团伙搭建假冒的股票交易平台，雇请推广团伙多渠道推广，利用荐股类专业话术，以高盈利做诱饵，诱骗用户投入资金。犯罪团伙则在后台实时操纵行情，伪造交易记录，诈骗用户大量资金。

九. 用户网络诈骗预防安全手册

骗子行骗的过程都有两个阶段：一是博得信任；二是骗取对方财物。对于骗子和受害用户来说，第一阶段都是最重要的，也是骗子行为表现得最为突出的阶段。虽然行骗手段多种多样，但只要我们树立较强的反诈骗意识，克服内心的一些不良心理，保持应有的清醒做到“三思而后行，三查而后行”，在绝大多数情况下是可以避免上当受骗的。

十个凡是：

1、凡是问你银行卡号和让你转账的都是骗子；

2、凡是自称公检法工作人员要求核查账户、转账汇款的都是骗子；

3、凡是找工作找兼职让你先掏钱的都是骗子；

4、凡是退票改签要去 ATM 操作的都是骗子；

5、凡是声称免费退款换货的陌生电话和网址都是骗子；

6、凡是接到 170、171、147 号段牵涉到钱的都是骗子；

7、凡是说你中奖要求先交保证金的都是骗子；

8、凡是购买游戏装备要你先汇款的都是骗子；

9、凡是补贴、补助要求去 ATM 操作的都是骗子；

10、凡是 QQ、微信上要求借钱、汇款、充话费的务必电话确认；

五个一律：

1、接电话，不管你是谁，只要一谈到银行卡，一律挂掉；

2、只要一谈到中奖了，一律挂掉；

3、只要一谈到是公检法税务或领导干部的，一律挂掉；

4、所有短信，但凡让你点击链接的，一律删掉；

5、微信不认识的人发来的链接，一律不点。