第 2 卷◆第 2 期◆版本 1.0◆2020 年
文章类型:论文 | 刊号(ISSN):2705-0637(P)/2705-0645(O)

# 手机安全及其防范措施

童长卫
中共龙岩市委党校
DOI:10.32629/ems.v2i2.693

[摘　要] 随着科学技术的不断发展,人类已迈入信息时代。智能手机作为信息移动终端,极大方便了人们的工作及生活。但由于手机连接的开放性,黑客利用各种手段入侵用户手机,窃取用户信息甚至盗取用户资金,给手机用户造成极大安全威胁。本文探讨了黑客入侵用户手机的常用手段并提出了防范措施。
[关键词] 手机;安全隐患;防范措施

## 1 手机发展现状及安全防范的必要性

手机做为一种智能移动终端, 已成为人们生活中必不可少的工具,人们利用手机除了进行各种通讯外,还大量利用手机进行购物、资金交易,同时,手机具备独立的操作系统, 用户可在各大软件供应商处获得海量的应用程序。截至 2019 年 6 月,网民规模已达 8.54 亿,网民中使用手机上网人群的占比由 2018 年的 98.6%提升至 99.1%。由于网民数量庞大,绝大多数手机用户并不具备安全防护意识,加之手机具有诸多隐患后门,一旦被恶意程序控制,会严重威胁到个人财产及信息安全。目前手机操作系统主要分为两种:Android(安卓)及 iOS(苹果)系统。在搭载着 Android 系统的手机中,由于自身高度的开放性(Android 系统开放了系统源代码),导致某些包含恶意木马程序的软件被安装到用户的手机上, 用户的全部信息及手机使用行为均会暴露在恶意程序操控者眼中。而 iOS 系统的源代码不对外公布, 仅可使用在苹果公司发布的手机上, 这在很大程度上避免了软件市场的各种乱象。虽然 iOS 系统具有封闭性特征, 但仍旧留有“后门”, 一旦用户主动越狱, 同样会面临 Android 系统的境遇。随着手机商务应用的快速发展,如果手机安全性能得不到解决,势必会给用户造成巨大的财产损失。

## 2 黑客入侵手机的常用手段

### 2.1 通过 wifi

设置一个不加密的 wifi, 诱使手机用户通过该信号连接网络,然后通过专用软件(如抓包软件)窃取你的上网信息,甚至可以通过 wlan 功能直接远程连接你的手机,对手机进行各种操作。

### 2.2 手机充电桩

目前大部分手机的充电接口和数据接口都是同一接口。黑客通过提供虚假的免费充电接口,实际上是接入的黑客电脑的 USB 接口, 再诱导用户开启 USB 调试功能,这样就完全控制这部手机。

### 2.3 诱导安装恶意插件或病毒

通过发送包含链接在内的各种虚假信息或广告,诱导用户打开这些链接,安装恶意插件或病毒。特别是一些黄色网站,利用人们的猎奇心里,诱导用户必须安装 *** 软件才能播放视频或浏览图处, 你在安装这些软件的同时也被安装了恶意插件或病毒。

### 2.4 通过盗取 QQ

许多苹果手机用户都开启了“寻找我的 iphone”功能并使用 qq 邮箱做为手机的登录邮箱, 当 QQ 被盗时, QQ 邮箱一并被盗。盗窃者使用密码重置功能,通过 QQ 邮箱重置 id 密码, 再通过 " 寻找我的 iphone" 远程锁机,最后进行勒索。

## 3 手机安全隐患分析

造成手机的安全隐患的主要原因有以下从几个方面。

### 3.1 监管措施不力

由于智能手机具有高度的开放性, 使得某些恶意软件会利用手机操作系统自身漏洞植入木马程序, 从而窃取用

---

的科学布设。

## 4 总结

激光雷达测绘技术在我国的各个行业都被广泛运用。通过激光雷达测绘技术的准确性,使测绘的数据更加的准确和完善, 使得在工程建设中人们可以有大量的数据作为参考, 因而使得在工程的建设中所运用的数据更加准确,同时还能避免相关资源的浪费状况,同时保障工程建设的质量,为我国现代化建设作出了巨大的贡献。

## [参考文献]

[1]郭新国.工程测绘中激光雷达测绘技术的应用[J].工程技术研究,2020,5(02):38+39.

[2]朱美红.工程测绘中激光雷达测绘技术的应用探析[J].工程建设与设计,2019(16):268+269.

[3]刘子铭.工程测绘中激光雷达测绘技术的应用分析[J].城市建设理论研究(电子版),2019(18):97.

户的个人信息。据北京奇虎科技有限公司 360 互联网安全中心发布的《2019 年上半年中国手机安全状况报告》显示,99.99%的安卓手机存在安全漏洞。仅在 2019 年上半年, 该公司即截获安卓平台新增恶意程序样本约 92.0 万个, 拦截钓鱼网站攻击约为 13.8 亿次, 盗版及仿冒软件、网站非法窃取用户信息及财产已成为重点突出问题。第三方软件商店缺乏足够的监管力度,使得某些非正规软件较易将恶意代码植入手机系统中。另外还出现了一些克隆软件,普通用户仅从外表上很难发现问题。这些软件一旦在手机中运行,会调取手机的各种权限,手机用户的使用信息、运动轨迹、账号密码等。还会自动下载捆绑软件,通过所谓的 " 增值服务 " 窃取用户的财产。

3.2 无线网络为黑客与病毒入侵提供了机会

无线网络是智能手机获取外界信息的主要手段,无线网络一般具有较强的私密性。前面讲了黑客常利用免费无加密 WIFI 窃取用户信息。但由于 WIFI 的安全技术协议上的存在漏洞,实际上“全世界的 Wi-Fi 早就不安全了”, 黑客可以利用 KRACK 漏洞攻击对 WPA2 进行破解,其传输的数据存在被嗅探、被篡改的风险。黑客可获取 WIFI 网络中的数据信息,包括微信、交易密码、邮件、等等, 危害巨大。而此漏洞是无线底层安全协议 WAP2 本身的漏洞, 一般的补丁及 WIFI 管家之类的应用层的防御软件、防病毒软件根本无法解决。

3.3 操作系统存在安全漏洞

任何软件都可能存在安全漏洞, 特别是像手机操作系统这样的大型软件,几乎是 100%的存在安全漏洞。几乎每隔一段时间,就会有“*** 手机存在重大安全漏洞,黑客可以...”的新闻。据“美国国家标准技术研究院国家漏洞数据库”公布的官方数据, 在过去二十年里(1999-2019) 微软开发的产品里一共被发现了 6814 个漏洞,位列第一,前五名依次为:Microsoft(6814 个漏洞)、Oracle (6115 个漏洞)、IBM (4679 个漏洞)、Google(4572 个漏洞)、苹果(4512 个漏洞)。尽管各公司不断推出新版本或补丁,已消除发现的安全漏洞,但随着新技术的应用,如指纹认识、人脸识别,又带来新的安全危险。前段,在三星的最新产品 Galaxy S10 系列和三星 Galaxy Note10 系列手机上就发现有指纹识别安全问题。

3.4 防护系统不能应对严峻的防控形势

随着科技的快速发展, 智能手机更新换代的速度极快。由于防护系统无法跟上手机更新的速度,使得手机安全防护始终处于被动地位。手机丢失定位、指纹锁等功能的出现, 在一定程度上缓解了手机安全性能不强的问题,但相应的网络攻击技术也在不断发展,防护系统如不能依据网络攻击做出相应的改变,仅依靠指纹锁、人脸识别等功能,并不能真正保障系统安全。防护系统建设领域中,真正具有较强专业技术的人才较少,不能完全解决愈发严重的手机安全问题。

## 4 手机安全防范措施

4.1 完善各项监管措施

对于智能手机第三方应用软件的安全问题, 监管部门要出台一系列法律法规, 对违反此项规定的软件供应商予以严厉打击。要对各个软件供应商的从业资质及从业范围进行审核,还应加强技术监管力度,每一款上市的应用软件均要进行严格测试, 只有通过检测方可投入到应用市场中。同时要加强宣传力度,使手机用户养成在系统自带的应用市场及各大软件应用市场下载安装应用程序的良好习惯,不给违规软件以可乘之机。

4.2 提高自身安全意识

由于手机在使用过程中极易受到恶意程序威胁,故用户均应将手机安全隐患问题提升到新的高度, 通过提高自身的安全意识,规范使用手机。要通过正规渠道购买手机,选择品牌口碑好的商家,避免使用仿冒手机及二手手机。在下载软件时,应首选手机自带的应用商店,或者选择信誉度较好的第三方应用市场。对于接收到的不明短信,不要轻易点击网页或者短信中的不明链接,更不要主动安装应用市场外的软件。不要随意将手机接入陌生设备中, 避免其他设备读取到手机存储的信息。公共 WiFi 往往由于防护较低,因此应尽量不要接入公共网络中,尤其要避免涉及到金融及个人信息方面的操作。智能手机均具备定位功能,如当前没有相关需要,则应及时关闭 GPS 及蓝牙功能,还要查看软件获取权限的相关情况,对于动机不明的软件坚决予以卸载。对于某些较为重要的数据文件,用户可使用手机自身的加密功能,将相关信息存储于手机的隐藏空间内。在手机使用过程中,会留下诸多痕迹,手机用户要养成及时清理浏览记录、缓存文件的习惯。各种杀毒软件是防范木马病毒的重要保障,应选取信任度高的杀毒软件,并及时更新病毒库,每天均需对手机进行体检。同时, 及时更新手机操作系统及常用软件。

4.3 操作系统供应商应及时优化自身产品

加快国产操作系统的研发, 从根本上掌握安全主动权。开发商应时刻掌握操作系统发展动向,并积极做好市场调查,认真听取广大用户的使用感受及需求。还应加大技术研发力度,及时修正产品缺陷,发布系统补丁,维护系统的良性发展。技术人员应积极研究木马病毒的攻击原理,制定出相应对策,避免造成更大的损失。

4.4 建立起完善的手机防护系统

智能手机的安全问题需各方紧密合作共同完成,从手机开发商、网络提供商、应用开发商直至手机使用者,同时,还需要法律、法规的保障,各环节缺一不可。只有建立立体综合的防护体系才能从根本上解决手机面临的安全威胁,从而实现手机信息安全保障。

文章类型:论文 | 刊号(ISSN):2705-0637(P)/2705-0645(O)

# 试论个人信息网络侵权的民法规制

李婧一
河北省唐山市润新公证处
DOI:10.32629/ems.v2i2.694

[摘　要] 随着经济和科学水平的不断提升,现代互联网技术被广泛应用到人们的生活中。给人们带来极大的便利同时,也给人们的个人信息安全带来非常大的挑战。在这样的背景下,个人信息网络侵权、维权处理工作成为了相关部门的重点关注对象,也是法律层级上重点控制内容。本篇文章对个人信息网络侵权进行详细的分析和研究,深度探究个人信息网络侵权民法规制完善的实践策略,给相关人员提供理论上的建议。
[关键词] 个人信息网络侵权;民法规制;实践策略

网络侵权就是指在互联网的大环境下进行的侵权行为。网络侵权是进行知识侵权的其中一个形式,与传统意义上的侵权行为本质上不存在差异。行为人利用互联网资源共享特点,侵害他人的财产和人身权利,被称为网络侵权。对于个人信息网络侵权问题的治理,在全世界范围内都受到了同样的高度重视。在 2008 年的 5 月到 11 月份,我国相关部门联合开展网络市场监管专项行动,打击网络犯罪、网络虚假宣传、网络侵犯他人个人信息的行为。

## 1 个人信息网络侵权民法规制的现状

### 1.1 立法规制角度

从当前发展形式来看, 我国政府的相关部分已经对个人信息网络侵权行为作出了相应探究和措施, 并且取得了一定阶段的成效。但是,随着网络信息时代大环境的不断冲击,个人信息网络侵权形式复杂多变,不好掌控,控制难度系数非常大。所以,个人信息网络侵权法律规制的工作进行过程中存在落差和滞后。我国在《刑法修正案》中有明确规定, 相关单位的工作人员不能向他人出售或者提供公民的个人信息,如果违反,需要遵从情节的严重程度,依法进行刑事追责[1]。

### 1.2 民事侵权角度

从民事侵权角度出发分析泄露个人信息的行为,由于现如今个人信息网络侵权事件层出不穷, 没有完善的保护措施,只能够依照个人信息网络侵权的现实情况,根据现有的立法资源进行整合,才能初步突破,逐步的供给侵权势力经验, 进一步开展个人信息网络侵权法律保护工作。在现阶段的发展过程中,我国并没有完善具体的、针对个人信息网络侵权的相关法律法规, 只是出台了一系列对个人信息泄露进行适当限定的保护措施。只有制定具体法律措施,不断完善已有政策,我国国民个人信息在网络中才能够得到安全的保障。因此,在信息飞速发展的鼎盛时期, 要制定系统化的个人信息网络侵权民法规制,不断更新处理策略,确保个人信息网络侵权得到妥善的处理。

## 2 个人信息网络侵权的相关责任和适应前提

### 2.1 个人信息网络侵权的行为和责任

通常情况下, 侵权行为分成了一般侵权行为和特殊侵权行为。一般侵权行为适用于过错责任,特殊侵权行为用于严格责任。立法方式的不同影响着二者的区分标准。概括式的一般法律规定适合一般侵权行为,列举式的特殊法律规定适合特殊侵权行为。不过,社会还在持续的发展中,网络信息化世界也依旧复杂多变,还会在演变中出现全新的侵权行为种类。特殊的侵权行为在法律的文件、效率等方面都进行了特殊的规定条例,但是不代表这些方面在一般侵权行为中运用不到。因此,侵权行为和侵权责任并没有确定的相对应关系。一般侵权行为的归类责任事因是过错,特殊侵权行为包括过错,更重要的是除过错以外进行的无过错行为, 但责任的本身性质就已经

## 5 结语

信息安全总是相对的,绝对的安全是不存在的。智能手机已成为人们生活及工作中必不可少的工具, 手机的使用过程不可避免的存在或多或少的安全隐患。首先要从技术上解决问题, 其次要从法律法规、从管理上下功夫,最后手机的使用者也要增强自身风险意识,构筑手机信息安全的最后一道防线。

[参考文献]

[1]王晓妮,韩建刚.信息时代智能手机安全隐患及防范措施研究[J].信息与电脑:理论版,2018,(14):216+218.

[2]祝毅博.浅谈个人手机信息安全技术防范与保护措施[J].中国战略新兴产业,2018,(034):131.

[3]李宇斐.手机 App 个人信息安全风险与防范[J].保密科学技术,2019(8):49+52.