部分共享充电宝竟被植入“木马”程序泄露隐私

警惕共享充电宝信息安全“陷阱”

生活中,出门在外遇到手机没电时,一款可租用的共享充电宝可谓“江湖救急”。近两年来,随着消费的变化,曾经被人称为“伪需求”的共享充电宝,如今似乎成了“刚需”。不过,共享充电宝最近陷入了泄露个人隐私的旋涡。

近日,公安部网安局微信公众号推送了一篇题为《警惕身边的共享充电宝陷阱》的文章。该文称,部分共享充电宝不仅可能存在质量隐患,还可能被不法分子植入“木马”程序,导致手机里的通讯录、文本信息甚至照片、视频等隐私数据被泄露。这些充电宝主要来源于三个地方:一是商场里的可租赁移动电源;二是火车站里叫卖的满电充电宝;三是扫码免费送的充电宝。

数据隐私问题突出 相关企业紧急发声

艾媒咨询发布的《2020上半年中国共享充电宝行业发展专题研究报告》显示,2020年中国共享充电宝用户已达2.29亿人。消费者使用共享充电宝致使个人隐私数据泄露现象时有发生。

在公安部网安局微信公众号推送的《警惕身边的共享充电宝陷阱》一文中,警方提示:不要随意购买和扫描来历不明的充电宝,如有需要,请选择正规产品或扫描正规公司的可租赁移动电源。当手机连接充电电源时,提示是否“信任”时,请提高警惕。

目前,我国共享充电宝行业已形成“三电一兽”——街电、来电、小电、怪兽充电的垄断式格局。

当共享充电宝陷入泄露个人隐私旋涡后,2020年12月8日,小电公关负责人刘彬在微信朋友圈回应称:“特地剪了一个充电宝,小电的充电宝只有正负极线路,不涉及数据传输的线路,不会有木马和数据的泄露风险。”

随后,小电发布官方声明称,小电共享充电宝在设计上充分注重对用户隐私数据的保护。在硬件层面,小电充电宝内部线路不含有数据传输线,仅以电源线提供充电功能。在软件层面,小电始终严格遵守《隐私政策》条款,通过多重数据保护技术和管理措施杜绝非法收集用户信息的情况发生。

怪兽充电的工作人员也表示,“我们的数据线是没有数据传输能力的,只能用来充电”“用户的充电订单都会享受隐私保护”,并强调其充电宝查询不到用户手机上的数据、无法读取用户的数据。

企业自律确保合规 行业规范适时出台

大数据时代,如何保障网络安全、数据安全一直是各行各业普遍面临的问题。

据北京师范大学法学院教授刘德良介绍,一些黑色产业利用“木马”等恶意程序,控制用户的终端设备窃取数据,包括手机里面的一些数据信息,之后通过贩卖数据获取非法利益,或直接利用这些数据实施违法犯罪行为,已经形成一条黑色产业链。

值得注意的是,北京市盈科律师事务所高级合伙人韩英伟提出,目前还存在监管部门监管滞后、部分参与者和使用者个人素质待提高、国家法律法规不够完善、准入门槛、准入机制缺失等问题。

最近,共享充电宝行业暴露出来的隐私泄露风险再次将上述问题推上了风口浪尖。

韩英伟建议,共享充电宝相关企业要确保产品合规、安全,始终严格遵守《隐私政策》条款等,杜绝非法收集用户信息的情况发生,设立可疑充电宝检举部门,并设线下检举点,对被检举的充电宝进行检测。在企业内部培养用户隐私绝对至上的企业文化,同时成立监管合规部门,充分了解法律法规。同时,政府应对相关制度进行完善,加强对商家的监管和引导,成立相应的监管部门,加强对隐私保护的普及和推广等。

重庆市律师协会民事专业委员会主任、重庆中世律师事务所创始合伙人吴启均则认为,从技术保护层面来讲,共享充电宝企业可以采取更多的信息安全防护措施来保障用户的个人信息安全,如制定共享充电宝检测和维护机制,对可能已被拆封、改装或植入恶意程序的共享充电宝及时进行回收并维护等。从企业合规经营层面来讲,共享充电宝运营企业应建立个人信息泄露救济预案机制。若发现保管的用户个人信息发生或者可能发生泄露、毁损、丢失的,应当立即采取补救措施;造成或者可能造成严重后果的,应当立即向准予企业许可或者备案的电信管理机构报告,并积极配合相关部门进行调查处理。

吴启均建议,首先,建立共享充电宝行业标准,对共享充电宝设置特定的行业规范。例如,设置共享充电宝应当不具有数据传输功能等。其次,共享充电宝行业可以建立相应的行业运行规范。例如,在个人信息收集、使用过程中,建立完善的用户个人信息保护机制,通过用户协议或隐私保护政策等明示用户个人信息收集、使用的目的、方式和范围,查询、更正信息的渠道以及拒绝提供信息的后果等,在明确取得用户授权后在其授权范围内对用户个人信息进行采集和使用。

吴启均还建议,政府可以设立企业运营的最基本条件,包括实名制注册使用、服务合同内容、使用费用和押金监管、鼓励为使用者购买责任保险并在事故中先行赔付、明确运营维护内容和从业人员准入要求、对使用者违法违规行为的约束和处理、投诉处理、使用者隐私保护等内容。另外,可以协调政府部门加大对充电宝使用违法违规的执法力度,推动将违规使用,故意损毁、破坏和私自改装等行为纳入信用体系,促进充电宝良好使用“软”环境的建设。

用户增强防范意识 如遇侵权及时止损

面对部分共享充电宝带来的隐私泄露风险,消费者该如何辨别和防范?

韩英伟给出了三点建议:第一,注意商家的虚假标识,不要使用可疑或假冒伪劣产品;第二,查看充电宝的安全标志;第三,使用共享充电宝时,当出现“是否信任此电脑”的弹窗,或出现要求信任等提示时,需要提高警惕。先点击“否”或“拒绝”等,并归还可疑充电宝。

吴启均也建议:消费者在使用共享充电宝前,须仔细阅读用户协议及隐私保护政策,尤其应注意相应责任划分约定及个人信息收集和共享条款,以免后续产生争议。若用户对相应企业的用户协议或隐私政策条款约定存有异议,则需谨慎对个人信息作出授权或使用相关产品。

如果消费者的隐私已经被泄露,怎么办?

对此,吴启均提到,如果消费者在使用共享充电宝时遭遇隐私泄露,首先应该厘清可能的泄露途径,如确定是在使用共享充电宝时泄露的个人信息,那么应当及时采取有效措施固定证据,如手机使用痕迹、可能存在的“木马”等程序、已经泄露的个人隐私信息以及泄露平台。然后立即通知相关平台要求对个人信息予以删除,以降低对个人的不利影响。若因隐私泄露对个人名誉、财产等造成损失,可以要求侵权人予以赔偿。最后,及时向人民法院提起诉讼,要求侵权人停止侵权、赔礼道歉并赔偿损失。若侵权情节严重,构成犯罪的,也可向公安机关检举控告。

韩英伟提出,如果消费者在使用共享充电宝时遇到隐私泄露,可以通过以下途径进行维权:向互联网管理部门、行业管理部门和相关机构进行投诉举报;寻求公安机关的帮助,以减少或挽回损失;向侵犯隐私的违法充电宝公司进行索赔;通过法律手段维护自己的合法权益等。

“日常生活中,消费者在使用共享充电宝时,如果没有意识到相关安全问题,那往往在使用某些共享充电宝时很难发现其隐私数据被窃取,一方面因为“木马”程序都比较隐蔽,另一方面大多数消费者缺乏网络安全技术相关知识,一旦其隐私被泄露,除非遭遇敲诈勒索等,否则很难主动发现自己的隐私被泄露。”刘德良说。

因此,刘德良建议由政府相关部门出面,对提供共享充电宝的企业进行不定时安全检测,如果发现问题,则立即追究责任。

(韩丹东 杨杰)