充电宝还能“共享”个人信息？

上海市网信办出手 一家企业遭行政处罚

□记者 季张颖

本报讯 记者从上海市网信办获悉，在国家网信办网络执法与监督局指导下，“亮剑浦江·消费领域个人信息权益保护专项执法行动”近期聚焦租借手机充电器场景中普遍存在的“过度采、强制要、诱导取、违规用”消费者个人信息的违法违规行为开展集中整治。目前，市网信办已对属地一家违法违规情节严重、提供充电设备租借服务的企业予以行政处罚。

根据网民举报线索和前期技术巡查发现，C站充电、电饱饱、火电宝、鲲鲸云电、泡泡充电、豚电充电、喜充共享充电宝等手机充电设备租借服务企业在扫码环节（还未进入租借环节）就强制索要消费者手机号码、微信昵称、头像等个人信息以及存在用户注销账号困难等问题。

市区两级网信部门对相关企业开展约谈指导、普法教育，要求企业按照《个人信息保护法》相关规定，全面落实个人信息处理的“最小必要”原则，个人信息处理规则必须公开、透明，采取有效措施确保个人信息处理活动合法合规。

目前，上海市网信办已指导属地市场占有率较高的一家企业率先完成自查整改，在严格履行个人信息保护各项义务的基础上，率先在行业内推出个人信息收集清单和隐私政策内容提示，并将于近期上线用户账号“自助注销”功能，努力在行业内做个人信息保护的标杆。

此外，上海市网信办已对属地一家违法违规情节严重、提供充电设备租借服务的企业予以行政处罚。针对一批市场使用率高、覆盖面广的非上海属地企业，上海市网信办已将相关违法违规线索上报国家网信办。

上海市网信办相关负责人指出，租借手机充电设备应用范围广、使用频次高、群众感知强。提供扫码充电服务的企业要对照《租借手机充电器场景下所需最小必要个人信息清单》进行自查整改，确保扫码、租借、寻找机柜、支付等各环节全流程合法合规，切实维护消费者个人信息安全。

《清单》明确，扫码环节仅需拍照权限，无需存储、地理位置、手机号码等其他权限或个人信息。寻找机柜环节可通过地图选点等方式为消费者展示特定地点附近可用机柜，精准位置权限基于更好服务可以收集，但不应被强制或频繁索取。支付环节如通过押金支付，则无需手机号码等个人信息；如通过免押金信用支付，则需提供信用账户信息供充电器运营企业核实；如通过他人代付，则无需手机号码等个人信息。

改写电池数据 让故障车“带病上路”

上海警方侦破一起破坏计算机信息系统案

□法治报记者 陈颖婷

为牟取非法利益，不法分子采用技术手段将新能源车健康电池组的数据非法写入故障电池组中，从而绕开后台锁定功能，使故障电池组得以重新充电上路，造成极大道路安全隐患。近期，上海警方紧盯计算机领域新型犯罪，成功侦破一起破坏计算机信息系统、克隆新能源车动力电池的案件，抓获屠某、刘某等4名犯罪嫌疑人，查扣芯片读写器、超级编程器等作案工具，及时消除了道路安全隐患。

新能源车电池组被克隆

今年5月，上海市公安局嘉定分局网安支队在辖区某新能源车企开展工作中，发现近期部分车辆的动力电池数据存在异常。通过企业信息系统，民警发现在同一时间段内，存在同一ID的动力电池在北京、江苏、上海、福建等多地同时出现并使用的情况。

按照国家监管要求，每一块用于新能源汽车的动力电池组，都必须符合国家规定的安全性能标准及安全设计技术要求，并配以唯一的电池ID编号。车辆一旦发生撞击、泡水等情况并达到一定程度时，电池组就会启动后台锁定功能。此时，车辆无法使用高压电，也无法行驶，需要运至维修站检测电池损伤情况，检测或维修合格后才能解锁，以确保车辆行驶安全。

经与车企技术人员深入沟通，民警发现这些相同ID号的车辆之前都因交通事故而被后台锁住了电池组，无法充电和行驶。由此警方分析认为，这些同一ID号电池组内的数据极有可能被人为盗刷篡改，即把一套健康完好的电池组数据写入了多个故障电池组内，从而破解锁定功能。

不法分子的盗刷行为导致被锁定的故障电池可以重新上路行驶，极有可能引发电池短路甚至起火等高危情况，严重危害驾乘人员生命安全，造成极大交通安全隐患，嘉定警方随即抽调警力成立专案组开展攻坚侦查工作。

海量数据“筛”出嫌犯

专案组从电池后台数据库入手，从海量数据中细致梳理克隆电池板从断电锁死到重新上路的时空线索。经过抽丝剥茧的分析，专案组发现有三个互联网自媒体，以汽车电池“解锁”为噱头，发布相关教学视频。经核查，这三个自媒体平台分别对应三个外省市汽车修理企业。同时，经过数据筛选比对，发现涉案车辆均与这三家企业有关联，这些事故车辆的电池解锁极有可能均在这些汽修厂内完成。

由此，屠某等4名犯罪嫌疑人浮出水面。由于三家修理厂之间并没有关联，专案组制订了兵分三路、各个击破的抓捕计划。在进行大量外围调查的基础上，今年6月，警方辗转多地将4名犯罪嫌疑人抓获，并查获了一批用于盗刷电池板的电脑、硬盘、芯片读写器、超级编程器等工具。

解密“作坊式”操作

到案后，犯罪嫌疑人分别供述了自2022年以来，使用工具将多辆正常完好的汽车电池组内的数据读出，后从各种拍卖平台、二手车商收购事故车或故障电池组，再将完好数据写入故障电池组内，完全覆盖故障电池组的原有数据，形成了与母版电池一模一样的克隆电池组，突破后台锁定功能并使得故障电池组可以重新充电上路。之后，嫌疑人再将车辆或电池组倒卖给他人谋取非法利益。

经查，犯罪团伙解锁一块动力电池收取费用在1000至3000元不等，累计获利约5万元。目前，4名犯罪嫌疑人因涉嫌破坏计算机信息系统罪已被嘉定警方依法取保候审，案件正在进一步侦办中。案件侦破后，该车企后台数据显示，全国没有再新增克隆电池组。

印假演唱会门票赚快钱？

徐汇警方破获一起诈骗案

□记者 季张颖 通讯员 马凯

本报讯 近日，徐汇警方在夏季治安打击整治行动中破获一起利用假演唱会门票诈骗案，抓获嫌疑人1名，查获假门票111张，涉案金额7万余元。涉案人员因涉嫌诈骗罪被警方依法刑事拘留。

今年8月14日，徐汇公安分局治安支队经工作发现有人在网络上转发某官方购票平台发售的某歌手世界巡回演唱会——上海站门票照片。经核实，该平台尚未启动相关演唱会的出票售票工作，流转在网络上的票均系假票。徐汇警方立即开展全面核查。

民警于当晚找到信息发布人员张某。经询问，张某称该照片系朋友圈好友所发，自己为满足个人虚荣心进行转发，而本人无相关门票，也并无盈利行为。于是，民警于8月15日找到多名人员，但均系转发他人图片，无盈利情况。

8月15日晚，民警最终找到实体门票持有者蔡某，蔡某又称门票是从好友钱某处购得，一共111张，支付了7万余元。在接受调查时，钱某辩称其手中演唱会门票来自一名就职于某购票平台的朋友，但她神情紧张，始终无法提供该朋友的身份信息。经进一步讯问，钱某终于交代。7月底，好友蔡某向其询问是否有渠道能买到某热门演唱会门票，钱某因急于支付房租，手头周转不开就一口答应了。由于蔡某坚持要看到纸质门票才肯付款，钱某就私下找网上店铺和相关模板，以每张26元的价格制作了100余张票面为1199元和2000元的演唱会假门票，再以每张500-900元不等的价格出售给蔡某。网络上流传的门票照片也是钱某首发的。

目前，钱某因涉嫌诈骗罪已被警方依法刑事拘留。该案中部分假票的回收以及印票网店的追查工作仍在进一步开展中。

1.2万余台电商电脑被植入木马病毒

上海警方抓获犯罪嫌疑人30名，涉案非法所得达100余万元

□法治报记者 陈颖婷

互联网经济下，网购已经成为市民的消费习惯，电商网店也由此存储了大量客户信息。为了获取不法利益，犯罪分子冒充客户以购买商品、服务为名添加电商客服微信，然后以需要定制商品为由向客服发送带有木马病毒的文件，诱骗客服在电脑端下载浏览，悄然植入木马后大肆窃取公民信息。日前，上海警方经过缜密侦查，成功捣毁一个专门在各大电商平台商家电脑植入木马、实施窃取公民信息等违法犯罪行为的犯罪团伙，抓获犯罪嫌疑人30名，涉案非法所得达100余万元。

平台电商电脑屡屡“中毒”

今年6月初，上海市公安局闵行分局接本市一家知名电商平台报案，称入驻平台的多家电商反映客服电脑疑似“中毒”，即派员到现场调查核实。经技术检测，涉事电商平台运行正常，未发现系统故障或人为破坏，但在多家电商客服的电脑内，警方都找到了隐蔽且自动运行的木马程序，能够窃取电脑数据并自动发送诈骗信息。

经过全面梳理排查，警方发现该电商平台内不少电商的电脑均被植入了木马，涉及导航、文印、购物、家装、中介等不同行业，彼此之间并无实质关联。在对涉事电商进行了大量走访调查后，警方总结出一个普遍现象，即这些电商的客服均在日常经营中遇到过声称要定制商品的客户，且该客户都会发送一个压缩文件，并以各种理由要求客服解压浏览。

曾女士是一家婚庆跟拍网店的客服，她告诉民警，近期有一位客户自称有大量订单，为了做成这笔大生意，两人添加了微信，对方将订单需求放在一个压缩包里，要求曾女士解压这个文件后要逐一点击每个文件，以便明确具体需求。曾女士照做后，电脑就开始出现故障，但她并没有在意，直至民警联系上她。经鉴定，曾女士点击的文件中的一张照片就是木马程序，而这款木马程序会自动搜索、收集电脑内储存的公民信息并自动上传至境外服务器。

植入木马的陌生来客现形

闵行警方成立了多个部门组成的专案组，展开深入侦查。

专案组很快锁定了以陆某某为首的犯罪团伙，其中，陆某某为总代理，林某某、锁某为一级代理，分别发展下线团伙成员，形成了一个多层级、松散型的犯罪团伙。陆某某从境外接收任务及木马文件后，通过即时聊天工具联系并安排团伙成员冒充客户使用话术，以购买商品、服务为名添加电商客服微信，然后以需要定制商品为由向客服发送带有木马病毒的文件，诱骗客服在电脑端下载浏览，从而植入木马，收集信息。

抓捕幕后犯罪团伙

7月16日至18日，专案组组织警力分赴全国4省7市，将团伙30名犯罪嫌疑人一网打尽，当场查获手机、笔记本电脑、硬盘等作案工具，初步查证该团伙非法获利100余万元。

经查，该犯罪团伙自5月开始，按照境外诈骗集团要求，以一台电脑种植木马80至120元的价格招揽团伙成员，并以代理的方式层层转包，底层人员则在各大电商平台联系商家客服、诱骗植入木马。截至案发，该团伙已在国内1.2万余台电商电脑种植木马，受害商家涉及全国多地。

目前，犯罪嫌疑人陆某某、林某某、锁某三人因涉嫌非法控制计算机信息系统罪已被检察机关依法批准逮捕，徐某某等27名犯罪嫌疑人因涉嫌非法控制计算机信息系统罪已被闵行警方依法采取刑事强制措施，案件正在进一步侦办中。

根据上述犯罪手法和木马特点，警方已经对具备采集公民个人信息资质的电商企业发出预警提示，要求相关企业对数据安全防护工作开展集中检查，督促各商家落实防护措施，全力筑牢数据安全“防火墙”。