

公安部：

严打侵犯公民个人信息犯罪

记者17日从公安部获悉，针对近日有媒体报道“记者700元就买到同事行踪”等情况，公安部通过组织开展侦查调查工作，现已查明此案是由相关单位内部人员与社会人员相互勾结所为，3名涉案人员已抓捕归案，目前案件正在进一步侦办中。

据介绍，当前随着社会信息化快速发展，侵犯公民个人信息犯罪持续增多。今年以来，公安机关网络安全保卫部门加大了对此类犯罪的打击力度，共侦破此类案件1800余起，抓获犯罪嫌疑人4200余人，查获各类公民

个人信息300余亿条；其中，抓获涉及40余个行业和部门的内部人员390余人、黑客近百人。

从查办案件情况看，犯罪分子获取公民个人信息的方式主要有：一是网络黑客通过技术手段窃取单位或企业存储的公民信息；二是通过招聘、婚介、办理会员、送礼品等需要填写个人信息的渠道获取；三是利用假冒网站链接骗取受害人信息；四是犯罪嫌疑人利用伪基站设备发送虚假链接方式窃取公民信息；五是各行业内部工作人员利用工作便利窃取、出售公民个人信息。同

时，犯罪嫌疑人利用QQ群、百度网盘、黑客论坛等网站平台，使用网络电话、虚假身份等进行联络，通过网银转账或第三方支付平台进行交易、交换公民个人信息。公民个人信息被不法分子窃取后，严重损害了人民群众的合法权益，滋生了电信网络诈骗、敲诈勒索等下游犯罪，社会危害严重，群众反映强烈。

公安部网络安全保卫局有关负责人表示，为了切实保护公民合法权益，维护社会长治久安，公安机关将对侵犯公民个人信息等信息化社会条件下的新型犯罪，持

续保持严打高压态势，进一步震慑违法犯罪分子，并督促拥有公民大数据的相关单位和企业强化安全管理措施，确保公民个人信息安全。公安机关将与相关部门密切配合协作，对涉嫌销售、传播公民个人信息的网店、网络账号、通讯联络号码等开展清理整治工作，净化网络环境，不给违法犯罪留下可乘之机。同时，提醒广大群众切实增强安全防范意识，妥善保管好个人信息。发现侵犯公民个人信息案件线索主动向公安机关举报（举报电话www.cyberpolice.cn）。

据新华社

侵犯公民个人信息犯罪十大典型案例



随着社会信息化快速发展，侵犯公民个人信息犯罪持续增多。今年以来，公安机关网络安全保卫部门加大了对此类犯罪的打击力度，共侦破此类案件1800余起。17日，公安部发布了侵犯公民个人信息犯罪十大典型案例。

案例一、北京顾某等人非法获取计算机系统数据案

2016年6月，北京公安机关网络安全保卫部门破获顾某非法获取计算机系统数据案。经查，自2016年1月起，顾某伙同他人制作用于非法获取某公司账号的软件程序，并在互联网上大肆收购网站身份认证信息，使用软件大量实施“撞库”行为，非法获取该公司账号约10万组，并通过互联网大量出售账号及扫号程序，非法获利10万余元。

案例二、江苏淮安“K8社工库”侵犯公民个人信息案

2016年3月，江苏淮安公安机关网络安全保卫部门成功侦破一起侵犯公民个人信息案，抓获犯罪嫌疑人8名，捣毁国内最大的网络社工库“K8社工库”（www.k8sec.com），查获公民个人信息20亿条。

案例三、四川广元侵犯公民个人信息案

2016年6月，经过1年多的侦查，四川广元公安机关网络安全保卫部门成功侦破一起侵犯公民个人信息犯罪案，抓获犯罪嫌疑人35名，查获四川全省学生信息及家长的公民个人信息1200万条，打掉非法买卖学生信息牟利的犯罪利益链条6个。

案例四、福建泉州“浮云网”侵犯公民个人信息案

2016年8月，福建泉州

公安机关网络安全保卫部门破获“浮云网”侵犯公民个人信息案，抓获犯罪嫌疑人51人，成功打掉买卖公民个人信息的网站“浮云网”，查获公民个人信息2200万余条，打掉了一条非法获取、买卖公民个人信息进而实施网络诈骗犯罪的产业链。

案例五、山东淄博侵犯公民个人信息案

2016年6月，山东淄博公安机关网络安全保卫部门破获一起侵犯公民个人信息案，抓获犯罪嫌疑人6名，打掉侵犯公民个人信息的犯罪源头2个，查扣公民个人信息近亿条。

案例六、江苏徐州非法获取计算机系统数据案

2016年6月，江苏徐州公安机关网络安全保卫部门破获一起非法获取计算机系统数据案，抓获犯罪嫌疑人8名，摧毁一条以黑客

和快递公司内部员工为泄露源头的倒卖快递信息的黑色产业链，查扣各类快递信息500余万条，犯罪嫌疑人非法获利30余万元。

案例七、湖北宜昌余某某侵犯公民个人信息案

2016年5月，湖北宜昌公安机关网络安全保卫部门破获余某某侵犯公民个人信息案，抓获犯罪嫌疑人10名。经查，该团伙自2015年9月至2016年5月，非法获取并出售股民信息、银行理财信息等公民个人信息1100余万条，非法获利280余万元。

案例八、山东威海董某某侵犯公民个人信息案

2016年6月，山东威海公安机关网络安全保卫部门破获董某某侵犯公民个人信息案，抓获犯罪嫌疑人5名。经查，2名银行工作人员利用职务之便，非法查询公民个人银行账户余额、流水等信息进行出售，非法牟利40余万元。

案例九、内蒙古赤峰李某某侵犯公民个人信息案

2016年6月，内蒙古赤峰公安机关网络安全保卫部门破获李某某侵犯公民个人信息案。经查，该团伙利用“快递单号生成器”等软件筛选快递单号，通过快递公司内部人员查询对应的公民个人信息7万余条，非法获利3万余元。

案例十、湖南怀化侵犯公民个人信息案

2016年5月，湖南怀化公安机关网络安全保卫部门破获一起侵犯公民个人信息案，抓获犯罪嫌疑人5名。经查，该团伙通过在网购买、搜索、下载等方式大量搜集公民个人信息，再通过“撞库”“扫存”等非法软件比对公民网络账户密码，进行出售和“刷单”赢利，非法获利10余万元。 据新华社

惩治个人信息泄露不能停留在口头上

京东信息泄露尚未尘埃落定，国家电网又爆出APP数据泄露。个人信息泄露事件接连发生，再次引发公众担忧。

京东声明称数据泄露缘于三年前的安全漏洞。三年前的安全漏洞为祸至今，直到最近该公司才出面回应，晚了不止一年两年。国家电网虽然否认信息泄露，但大量数据已从相关企业流入淘宝进入黑市。

个人信息安全不是小事，涉事企业恐怕不能以技术漏洞和工作人员麻痹等为借口一推了之。有关部门应该从公众利益出发，加大惩治个人信息泄露工作力度，打消涉事企业的侥幸心理，提高其责任心。否则此类事件接连发生，而涉事企业总是忙于找理由，或作出“自罚一杯”的表态，而不是拿出行动来改正错误。

由于信息泄露，一些人购房之后装修骚扰电话不断、购车之后保险公司马上提供“贴心”服务、生孩子之后被多家母婴服务机构盯上……凡此种种，不仅导致信息骚扰缠身，而且诈骗犯罪案件时有发生。有关调查显示，有的部门和行业甚至出现了交换、贩卖个人信息获利的灰色利益链条。

对此，有关部门不仅要求对技术渠道解决问题，更不能对此类事件频发等闲视之，而要将其纳入社会管理规范和监管视野，长久发力、从严打击。

我国针对个人信息保护目前尚未形成统一的综合法律规范，加上相关部门对一些信息泄露案件查处不力，制裁不到位，没有真正起到惩戒示范作用。为此，应该尽早出台完善有关个人信息保护方面的法律法规，使得处理个人信息泄露问题有法可依。

没有网络安全就没有国家安全。希望有关部门以近期信息泄露事件为契机，就惩治个人信息泄露加紧行动，迈出实质性步伐；同时，要针对具体个案严加追责，遏制不法行为，不能让惩治个人信息泄露停留在口头上。

据新华社