编者按

刚刚团购了一节健身体验课，就收到健身房的卖卡促销电话；新办了银行卡，很快就会有人来问是否需要贷款……日常生活中，我们的个人信息不知不觉就被泄露，骚扰电话、促销推广接踵而来，让人不胜其扰。

公安机关在办案中发现，当下，犯罪分子侵犯公民个人信息形成了一条产业链，信息获取、信息倒卖、信息使用是关键环节。一些犯罪分子通过植入木马程序、内外人员勾结等多种方式，非法获取公民个人信息，实施违法犯罪活动，严重干扰了公民的日常生活。

谁在贩卖我们的个人信息？

——三起案件揭开侵犯个人信息犯罪的黑灰产业链

张天培

教培机构信息失守——

针对教育培训行业投放木马程序，非法获取内部数据

去年9月，一条关于有人在某教育培训机构电脑内植入恶意软件，导致公司客户资料、用户信息等敏感数据被非法获取的线索浮出水面。该公司内部监控录像显示，员工鲁某某趁公司无人值守，刻意遮挡公司监控探头，将随身带的优盘插入其他员工工作电脑，获取电脑中的数据信息。

经查，这已经不是鲁某某第一次作案。民警意识到，该案应该属于人工投放病毒木马程序案件，而非嫌疑人所供述的单纯为了窥探其他同事隐私，于是第一时间深入排查。鲁某某承认，其频繁跳槽全国各地在线教培机构，主要目的就是在公司电脑内植入木马程序，获取大量公司内部数据。

进一步侦查后，民警发现鲁某某只是犯罪链条中的一环，他的背后还有组织者闫某某、提供木马病毒的专业技术人员等多个环节，犯罪分子分布多地。“此类犯罪链条分为木马制作人员，购买木马程序并分发的组织者，跑腿‘投毒’人员等上、中、下游。”办案民警介绍，本案社会危害性大，涉案团伙人数众多、组织严密，犯罪手段极其隐蔽。

本案中，受害企业全部从事互联网在线教育培训，基本依赖互联网开展业务，但因体量较小，缺乏内部安全管理与网络安全防范专业力量。同时由于销售岗位员工流动性较大，无法及时发现员工电脑异常情况。

据了解，犯罪团伙成员入职受害企业，主要为了投放木马程序，并不为相关企业创造业绩，且全部在闫某某的安排下集中住宿、统一管理，互相之间全部使用匿名聊天工具进行沟通，属于一起典型的非法获取企业内部客户数据、商业数据的恶性涉网犯罪团伙案件。

经审查讯问并结合勘验取证，警方查明该团伙先后对50余家企业进行木马“投毒”。“该案的成功侦破，有效震慑了在线教培行业内从事非法获取、买卖数据的从业人员，有力维护了相关企业的合法利益，保障了公民个人信息安全。”办案民警说。

电商平台“订单解密”——

商户、“解密中介”、快递公司勾连，贩卖个人订单信息

不久前，网民韩某某向公安机关报案称，其在某网购平台店铺内购买茶叶后，手机号多次接到陌生推销电话和境外诈骗电话，同时还收到各类虚假购物信息。接到报警后，公安机关顺线追踪，发现线索背后存在一个组织化、职业化的侵犯公民个人信息的犯罪链条，随即展开深入侦查。

某电商相关负责人介绍，个人信息保护法、数据安全法等法律出台后，为更好保护消费者个人隐私，电商平台和快递企业会在电商商户页面和快递面单上将收件人、手机号、收货地址等字段的中间信息替换为“*”，为订单信息加密。然而在实际操作中，电商平台为满足商户正常业务需求，通常提供少量的“订单解密”额度，但部分商户受利益驱使勾结“解密中介”，对全部“加密订单”进行“解密”。订单导出、订单解密、对单结算，只要简单三步就可以轻松获取被加密保护的客户订单信息。

“电商商户利用订单助手及打单软件将‘加密订单’批量导出，并发送至‘解密中介’。‘解密中介’则勾结快递公司‘内鬼’解密订单信息，并发送至电商商户。随后，电商商户便会按照成功解密的订单数量，向‘解密中介’支付报酬。”办案民警介绍。

本案中，犯罪嫌疑人李某某、陈某等中间商在互联网平台寻找需要解密订单数据的商家客户，嗅到其中“商机”后，一些平台商家动起了歪脑筋。商家将加密订单信息捆绑发送给李某某、陈某等后，又被转手发送给数据解密人员胡某某等人，非法获得订单中的客户个人信息。

“这是一起典型的‘订单解密’型侵犯公民个人信息犯罪案件。”办案民警介绍，本案共抓获犯罪嫌疑人18人，涉案金额高达300余万元。

求职网站虚假招聘——

假冒用人公司诱导下载涉诈APP，骗取倒卖求职者信息

去年6月，某网络招聘平台向公安机关报案：该平台求职者田女士投诉称，平台注册信息为“某科技有限公司第一分公司”的联系人以教如何赚钱为诱饵，对其进行刷单诈骗2400元。“我们经过分析发现，该科技有限公司冒充合法企业，在平台上传虚假的营业执照、办公环境视频，通过发布虚假职位，累计非法获取上百名求职者姓名和手机号。”该网络招聘平台安全部门相关负责人介绍。

求职者一旦将本人简历提供给该科技公司后，犯罪团伙便会于次日添加求职者微信，向其推荐主播打榜工作，并将其引流到某办公APP。引流成功后，诈骗团伙会继续诱导被害人下载涉诈APP，对被害人进行刷单诈骗。公安机关循线深挖，发现了一个从制售假营业执照到倒卖求职个人信息，再到帮助电诈团伙实施精准诈骗的犯罪团伙。

“经查，该团伙已初步形成制售假营业执照、在各大平台违规注册公司、骗取倒卖求职者信息的黑产链条。”办案民警介绍。据查，犯罪团伙一共非法获取近千名求职者的联系方式，涉及的求职人员遍布全国各地。另外，该团伙在7个网络招聘平台上冒用正规企业信息进行注册，致使被冒用的企业无法在平台注册招聘，堵塞求职人员入职相关企业的网上通道，对求职招聘市场秩序造成了严重破坏。

案件侦破后，公安机关将该团伙出售的上千张假工商营业执照信息，通报给多家招聘平台核实注销，及时斩断该黑灰产链条。

近年来，公安机关高度重视公民个人信息保护，始终保持对侵犯公民个人信息犯罪的高压严打态势，深入推进“净网”系列专项行动，仅2024年便侦破相关案件7000余起。

公安机关提醒，个人信息处理者要严格履行法定责任和义务，完善个人信息保护制度规范和技术措施，维护公民个人信息安全；群众要妥善保管、存储和使用个人信息，发现个人信息泄露线索的，及时向公安机关和有关部门投诉举报，保护合法权益。

链接

保护个人信息注意事项

防止个人信息泄露、预防诈骗，山东泰安警方提醒我们从以下5个方面加强防范意识，让不法分子没有可乘之机。

警惕陌生来电

“00”或者“+”开头的多是境外诈骗电话，如果没有境外亲朋很可能就是诈骗电话；400开头的电话一般都是企业号码，只能接听不能呼出；显示未知的电话号码，身份所在地都不显示，这类号码建议直接挂断。

快递单据处理

快递单据、火车票、取款凭条、信用卡账单等往往含有身份证号、手机号等个人信息，随意丢弃容易造成信息泄露，如确需丢弃，可以先用记号笔把含有个人信息的内容涂抹覆盖。

谨慎连接公共WiFi

一些公共场所的WiFi，很可能是不法分子专门搭设的“钓鱼”陷阱，容易泄露自己的个人信息。在使用不常用的公共WiFi时，尽量不要登录网银账号、网购账号。

网银、网购密码定期更换

网银、网购的支付密码最好定期更换，不同账号的密码应当设置不同密码，密码应尽可能加入标点等特殊符号。

不出租、出借身份证、银行卡

向他人出租、出借身份证、银行卡等行为，会为自己带来巨大的法律风险。出借身份证可能会导致他人利用你的个人信息进行不法活动。银行卡包含了你的个人金融信息，如果将这些信息泄露给他人，可能会导致银行卡被盗刷、资金被转移等风险。（王者采访整理）

（来源：人民日报）