“没有盈利也侵权？”徐汇“蓝鲸”现场普法

记者 吴会雄 通讯员 马凯

在第26个世界知识产权日，徐汇公安分局“蓝鲸”护企工作站会同辖区相关游戏公司，在鑫耀光环举办了一场宣传活动，主题为“守护知识产权 护航创新发展”。

民警现场普法

活动紧扣徐汇文创产业高度集聚的区域特点，聚焦群众文化娱乐消费中商标、著作权保护等重点领域，通过发放宣传手册、现场“一对一”法律咨询、趣味问答游戏等丰富形式，吸引了20余家企业及300余名市民群众参与。

“没有盈利，就不算侵权吗？”在趣味问答环节，游戏玩家小徐抽到这样一题：“不以盈利为目的，将游戏中未公开的角色、场景等分享在个人某平台账号中，是否侵权？”他信心满满地回答“不涉及侵权”，却被告知回答错误。“这种行为，即使没有盈利，也涉及民事侵权；如果盈利并达到一定播放量，甚至可能涉嫌刑事犯罪。”经民警现场耐心讲解后，小徐恍然大悟：“这次收获很大，只有尊重知识产权，游戏公司才能为我们玩家做出更多更精良的作品。”活动现场，多家企业的法务负责人也专程前来，就商业秘密保护、侵犯著作权案证据标准、销售假冒注册商标商品案的报案材料等实际问题进行咨询，“蓝鲸”护企工作站民警一一细致解答。

寓教于乐的宣传背后，是徐汇公安对侵犯知识产权犯罪的持续重拳打击。2025年底，徐汇分局环食药侦支队接到辖区游戏公司报案，不法分子通过网络引流推广“泰坦刀塔”“刀塔怀旧”等手游私服，以高额充值优惠吸引玩家充值，非法牟利。经查，该类私服与正版游戏高度相似，涉嫌侵害计算机软件著作权。警方经侦查锁定嫌疑人，2026年3月底在外地抓获李某、黄某浩等4名犯罪嫌疑人，查扣作案工具，并调取私服服务器数据。经查，4人通过私服非法引流充值超300万元，获利近100万元，目前已因涉嫌侵犯著作权罪被依法采取刑事强制措施。

一组数据见证了徐汇公安护企安商的扎实成效：2025年以来，分局已侦破侵犯著作权、销售假冒注册商标的商品等各类知识产权案件30余起，抓获犯罪嫌疑人150余人，有力保护了多个国内外知名企业的合法权益。同时期，徐汇“蓝鲸”护企工作站累计收到各类违法犯罪线索100余条，接受企业法律咨询160余次，深入园区、企业开展涉企风险防范主题宣讲10余场。紧密结合本区文创及人工智能产业高度聚集的新发展趋势，工作站于2025年10月入驻徐汇区知识产权全链条保护中心，与区相关职能部门联动开展值班接待、咨询服务、防范宣讲等各项工作，持续为区域创新生态和营商环境保驾护航。

从街头宣传到一线破案，从企业咨询到全链保护，徐汇公安正以“蓝鲸——警企直联”安商惠企机制为依托，不断织密知识产权刑事保护网，让每一份创新成果在法治阳光下茁壮成长。

警惕医保诈骗新手段

近期，医保诈骗手段不断翻新，已形成从信息盗取、远程操控到资金转移的完整黑产链条，严重威胁参保人财产安全与医保基金安全。“我就按他说的点了几下，输了个密码，二十多万就没了……”年近八旬的杭州张阿姨（化名）直言：“太可怕了，从没遇到过！”张阿姨经历的，正是一起典型的冒充医保工作人员诈骗。

近期，张阿姨接到一通陌生来电，对方自称是医保管理局的工作人员。“告诉我，手头上的职工卡和居民卡，两张保留一张，让我去拱墅区医保局办理并卡业务。我都快八十了，腿脚不方便。她说‘年长者可选择线上服务’，然后把电话转给了一个叫‘小李’的属地工作人员。”

“小李”先让张阿姨报了自己的身份证号、手机号，又主动发来一个办卡网址和软件。“我不太会用智能手机，他就一步步教我点这里、输那个，还问我职工卡是不是绑定了支付宝，绑定了哪些银行卡，让我输入密码。我想着在自己的手机上操作，也没啥风险呐！就按照他说的照做了。”

张阿姨的手机一会儿黑屏，一会儿死机，折腾了一个多小时，搞得老人家有点难为情。“我真的不太会搞，耽误人家那么长时间，小李却特别耐心地教我！”突然，属地派出所的民警敲门到访，告知张阿姨的银行账户正在进行高风险转账，赶快停止！直到这时，老人才反应过来：“并卡业务”就是个圈套，“便民服务”软件也是为了窃取张阿姨银行卡信息的恶意程序。

【诈骗套路解析】

1. 冒充官方诱导“屏幕共享”。骗子冒充医保局工作人员，谎称你医保卡“涉嫌骗保”“信息异常”“需注销多张卡”，诱导你下载远程控制软件并开启屏幕共享，从而实时窥屏获取短信验证码、银行卡密码等关键信息，实施盗刷。

2. 伪造“补贴领取”钓鱼短信。发送“城乡医疗补助金已到账”“就医补贴失效”等短信，附带虚假链接，诱导点击后进入仿冒医保网站，填写社保卡号、身份证、银行卡信息，进而盗取资金。

3. 连环骗局：医保+公检法双重恐吓。先以“异地医保报销”吸引注意，再转接“公安民警”，谎称你卷入重大案件，需缴纳“保证金”或“资金审查”，如湖北一位老人险些被骗走4万元养老钱。

警方提醒 >>>

1. 医保部门绝不会通过电话要求注销医保卡或修改信息。任何要求下载陌生软件、开启屏幕共享的，均为诈骗；2. 医保部门发送的服务短信，不会附加任何网址、链接，也不会要求点击链接输入个人信息、银行卡密码或验证码；3. 切勿点击来历不明的链接或接听可疑电话。切记不可透露个人金融账户及身份信息，更不要按其提示操作；4. 请提高警惕，保护好个人信息和财产安全。如发现被骗，请立即拨打110报警；5. 若有任何疑问，应直接拨打参保地医保窗口电话进行咨询。（来源：湖州网警）

警惕这十种行为，全都涉嫌违法犯罪（上）

近年来，电信网络诈骗出现新动向，境外诈骗团伙大肆在境内拉拢、诱骗人员充当“工具人”，协助实施诈骗犯罪。不少年轻人，尤其是在校学生，因辨别能力不足、防范意识薄弱，不慎落入圈套，涉嫌帮助信息网络犯罪活动罪、掩饰隐瞒犯罪所得罪被依法刑事拘留，还有多人受到行政处罚、联合惩戒，甚至被学校开除，令人痛心惋惜。

为切实提高大家的风险识别和防范能力，现将常见的十种帮信行为整理发布。

一、出租、出借、出售“两卡”

非法买卖、出租、出借电话卡账户、银行支付账户和互联网账号等，并以此户牟利的行为。

警方提示 >>>

“两卡”是指个人手机卡和银行卡。任何人不得非法买卖、出租、出借“两卡”。除此之外，对公账户、物联网卡、流量卡和支付宝、微信等网络平台账号同样不能出租、出借和出售，一旦被用于非法活动，极有可能触犯帮信罪、掩隐罪、妨害信用卡管理罪和诈骗罪，面临刑事处罚和惩戒。

二、发放涉黄小卡片

诈骗分子雇佣地推人员，印刷张贴带有二维码的涉黄小广告，引诱受害人下载涉诈APP实施诈骗的行为。

警方提示 >>>

现在的涉黄小卡片不再是曾经的招嫖小卡片了，而是新型刷单诈骗的引流手段。诈骗分子以“做任务就可以免费同城约炮”为幌子，诱骗受害者垫资刷单，给受害者造成巨大的财产损失。张贴涉黄小卡片是违法行为，如果造成受害人重大损失，可能构成犯罪，将受到法律严惩。

三、安装“VOIP”“GOIP”

非法购买、使用Goip、Voip等虚拟拨号设备，为境外诈骗分子搭设通话转接通道的行为。

警方提示 >>>

“GOIP”和“VOIP”分别是利用手机号码和固话号码进行虚拟拨号的诈骗设备。其实二者大同小异，都是基于IP的语音传输转换给不法分子的境外来电披上一层外衣。GOIP是利用手机卡接入电话网络，来电显示的就是手机号码；VOIP是利用固定电话线路接入电话网络，来电显示的就是固话号码。注意：非法安装GOIP和VOIP都是违法犯罪行为。

四、“手机口”诈骗

通过同时打开两部手机扬声器，一部手机通过网络软件接通诈骗分子；另一部机拨打指定电话，帮助诈骗分子完成电话转接的行为。

警方提示 >>>

除了使用语音软件，也有使用数据线将两台手机的音频口联通起来实现语音中转的情形，故称之为“手机口”诈骗。“手机口”的目的，是为了将高风险的境外来电，通过语音中转，在受害人手机来电显示为境内来电，从而提高诈骗的成功率。

五、“跑分”洗钱

使用自己或他人银行账户、第三方支付账户，为诈骗分子提供非法资金转移的“跑分”洗钱行为。

警方提示 >>>

很多“跑分”项目都是打着游戏代充值、走账等“兼职”的幌子推广，不少年轻人特别是在校学生参与其中，触犯法律获刑，断送了学业和前程。天上不会掉馅饼，动动手指就赚钱的“兼职”工作，可能会付出自由的代价，一定要小心。

（未完待续）

（来源：青城反诈）