■本报记者 何易

违法信息发生率全国最低、违法有害网站全国最少、被黑客攻击得逞次数全国最少

上海网络安全管理“三个最”从何而来

违法信息发生率全国最低，违法有害网站全国最少，被黑客攻击得逞次数全国最少。上海网络安全管理领先全国的“三个最”从何而来？

记者昨天从上海市公安局获悉：今年以来，市公安局网安总队对本市黑客攻击破坏、网络侵犯公民个人信息、网络涉枪涉爆、电信网络诈骗等突出网络违法犯罪保持高压严打态势，共侦破网络违法犯罪案件607起，抓获犯罪嫌疑人2017人。其中，侦破黑客攻击破坏案件64起，刑事拘留149人；侦破网络侵犯公民个人信息犯罪案件68起，刑事拘留165人，打掉贩卖公民个人信息团伙40余个，关停网站、栏目7个，处罚网站、网络服务提供商6个，极大震慑了犯罪分子的嚣张气焰。

在惩治犯罪同时，上海在网络安全管理上也铁拳频出：在全国率先开展App软件源头治理；开展网络直播平台专项整治，关停违规直播间1000余个，注销未实名认证的主播1000余名；排查存在漏洞的联网摄像头上万个……

严打网络犯罪
149名网络黑客被刑拘

黑客或内鬼盗取公民个人信息，信息中间商从他们手中获取大量信息并建立数据库，信息使用者从他们手中购买信息用于精准推销，甚至用于诈骗、敲诈勒索等下游犯罪——侵犯公民个人信息犯罪对社会危害性巨大。

今年2月，某金融信息服务有限公司发现其旗下一款App软件被多人利用黑客手段攻击，半天时间内被非法提现1056万元。经查，发现一名嫌疑人利用网络平台漏洞，使用黑客手段进行提现操作实施犯罪。作案得手后，该嫌疑人又通过互联网传授作案方法，致使该漏洞被大量传播利用。至案发，共有422个异常账户使用该方法进行恶意充值，其中269个提现成功。在掌握了嫌疑人的作案手段后，在案发后12小时，上海警方即明确了犯罪嫌疑人，并于3月3日、4日在安徽将赵某、杨某、张某等三名主要犯罪嫌疑人抓获。 截至目前，到案犯罪嫌疑人74人被检察机关批准逮捕，案件仍在进一步侦查中。

据市公安局网安总队副总队长沈与辛介绍，今年以来，上海警方重点围绕人民群众反映强烈的黑客攻击破坏、网络侵犯公民个人信息犯罪开展集中打击，共侦破黑客攻击破坏案件64起，刑事拘留149人；侦破网络侵犯公民个人信息犯罪案件68起，刑事拘留165人。从侦办的相关案件来看，以往黑客攻击动机较多为单纯的“技术炫耀”，而随着网络技术的发展，现在黑客攻击更多地被用于非法获利或不正当竞争。

严惩网络谣言
7×24小时网络巡查执法

随着自媒体技术的发展，部分网民借助微博、微信等即时社交工具的便利，随意编造谣言，扰乱正常社会秩序。为了及早发现谣言苗头、及早澄清事实真相，上海警方开展了7×24小时巡查执法，确保对网络谣言有一起、查一起。

9月5日上午，网上一段“虹桥机场周边高架道路浓烟滚滚”的视频引起网民关注。事实上，这段视频记录的是9月4日沪渝高速邻近的一蔬菜农副产品交易市场发生的火灾，无人受伤。不过，有网民却利用该视频制造谣言“虹桥机场，飞机坠落”。经查，造谣者是一名32岁的企业职工刘某。据其交代，当他看到视频后，为了在网上“出风头”，就在转发视频时随性添加了坠机信息。

上海在网络安全管理上铁拳频出，成效显著。 图/视觉中国

针对网络谣言，上海始终坚持“及时发现、主动应对”的态度，加强各网络管理部门的协调联动，加大对网络谣言和虚假信息查处力度，早发现、早应对、早查处、早宣传，进一步提升网民的守法意识，震慑网上造谣传谣违法行为。 今年以来，先后发现并依法查处编造“上海吴泾电厂发生爆炸”谣言、网上发布“在四行仓库前穿仿制二战日本军服照”、制作“表情包”戏谑“慰安妇”等案件共170余起，依法处理近50人。

严管网络不留死角
上海开发App全部实名

目前全国已有各类App软件1000多万个，远超网站500多万个的数量。由上海App应用市场提供接入的App应用达102万余个，App应用市场公司八家。上海在全国率先探索App软件源头管理，通过App开发者实名制度，确保上海境内制作的所有App软件都通过实名认证，一旦其中有吸费、色情等违法行为存在，马上可以找到责任人。与此同时，对App软件采取定时抽查制度，尤其是重点App和有群众举报的App必查，查出问题全国统一下架。今年以来，上海翰蓝网络科技有限公司的“遮社区”、上海成红网络科技有限公司的“哟趣”两款App因未实名认证且出现淫秽色情信息，被依法处以停机整顿六个月的处罚；上海初生网络科技有限公司“热拉”因未实名认证且未建立安全保护管理制度和安全保护技术措施，被处以停机整顿六个月的行政处罚。

网络直播平台发展迅猛却也良莠不齐，部分直播平台安全管理秩序混乱、涉嫌传播低级庸俗信息，甚至通过色情表演来吸引用户。上海警方不断开展网络直播平台整治，迄今已封停账号4500余个，关停违规直播间1000余个，注销未实名认证的主播1000余个。今年5月，上海公安机关以“网红”何某传播淫秽物品为突破口，辗转重庆捣毁其幕后直播平台“友视”，抓获包括实际经营人在内的5名涉嫌传播淫秽物品的犯罪嫌疑人，侦破了这一利用直播平台实施犯罪的案件。

此外，围绕“吃、住、行、消、乐”等与百姓最贴近的线上生活场景，在本市活跃用户数量多、社会影响力大的重点网站内，上海公安系统设立了网安警务室，以及时掌握各类违法犯罪活动线索，实现对网络违法犯罪的精准打击，并指导网站提高安全防范能力。沈与辛告诉记者， “运用科技手段和法治思维，着力推动网络空间立体化管理，依法保障网络运行安全、信息内容安全，努力提升对城市信息网络安全的感知力和防范力，这是每一个上海网警的职责。”

事先防范、事中堵截、事后拦截

防范电信诈骗，沪上银行各显神通

■本报记者 唐玮婕

电信诈骗手段翻新频繁，令市民防不胜防;犯罪分子得手之后将赃款快速转移，更给案件侦破造成阻碍。银行网点,既是防范电信诈骗的主战场，也是最后一道防线。面对花样百出的诈骗，沪上各大银行将保护客户资金安全放在首要位置，在服务中不断总结经验，围绕如何做好事先防范、事中堵截、事后拦截，构建起各自的电信反欺诈体系。

多措并举
防电信诈骗于未然

以筑起防范电信诈骗最后一道防线为己任，交通银行上海市分行研究并构建了一套包含前、中、后三个阶段的系统防范措施。

为全力配合公安机关做好电信网络新型违法犯罪打击治理工作，交行上海市分行严格执行监管部门要求，对同一客户的个人开卡数量和代理开卡进行限制，通过规范管理，从源头上遏制代开卡、批量开卡等电信网络新型违法犯罪的第一环节，切断不法分子获取犯罪工具的途径。

在做好事先预防的同时，该行充分依托网点阵地宣传防范电信诈骗知识，不仅在全市所有物理网点及自助银行内张贴、摆放统一的警示标语及风险提示牌，还专门制作了警示宣传教育片常年滚动播放，及时提醒客户在提取、转移大额现金时多注意防范电信诈骗。

就在最近，交通银行上海虹口支行成功堵截了一起电信诈骗，在客户即将准备把钱款汇至诈骗分子指定账户之际，银行工作人员两次阻拦、揭露诈骗，成功避免了共计30余万元财产损失。

建设银行上海市分行也始终高度重视日常教育。为了从源头堵截诈骗案件发生，该行普及金融安全知识、下发风险提示，提高员工安全防范意识，强化合规操作，提升全行防诈骗水平，有效防范电信诈骗案件发生；同时，从提高客户安全防范意识入手，组织相关部门业务骨干，联合辖区警方开展社区宣传教育，还通过公示栏、手机短信平台、口头提醒、张贴醒目标示等方法进行安全教育提示，扩大受众面和影响力。

及时堵截
扎紧风险防控篱笆

浦发银行上海分行在日常经营中始终为客户扎紧风险防控的篱笆，仅去年一年就成功堵截各类冒名、假证、伪造等风险事件275起。其中，

沪上各大银行守好最后一道防线构建起电信反欺诈体系。 图/视觉中国

该行对于网络、电信诈骗的堵截效果尤为显著。

伴随网络科技与电子商务的快速发展，各类网上银行、手机银行、自助终端等电子化机具应运而生。这些科技创新在为客户带来更加便捷、高效金融体验的同时，也向银行提出进一步提升交易安全、完善反欺诈手段的新课题。

自去年12月央行发布支付结算新规后，从银行堵截电信诈骗的形式上可以发现，犯罪分子更多采用迂回战术，不过最终目标还是直指储户银行卡里的资金。浦发银行千汇苑社区支行就在营业过程中成功堵截了一起这样的电信诈骗：当天，市民秦女士前来开通手机银行，在业务办理期间，不停查看手机信息；这一异常行为引起了柜面工作人员的注意，当向客户进行风险揭示时，秦女士表现得更为紧张；在被反复询问开通手机银行的目的和用途时，秦女士含糊其辞，而在“手机银行密码等必须保管好，不要告诉别人，如果告诉别人了，您的银行资产就有风险隐患”风险提示过后，秦女士更为犹豫；柜员随即请大堂经理协同向秦女士进行电信诈骗的风险防范提示。

在银行工作人员不断提示下，秦女士这才说出了原委：前一天她接到一个电话，声称她涉及洗钱犯罪，要求她前往银行开通手机银行，并要求她对此保密，手机银行开通之后会再联系她。在得知此情况后，浦发银行的工作人员立即劝其拨打110报警，公安人员也迅速前来网点，登记了诈骗电话，并向秦女士列举各种电信诈骗手法。秦女士猛然醒悟，对于银行工作人员的火眼金睛及警方的及时介入感激万分。

有效拦截
避免客户资金损失

记者从工商银行上海分行获悉，截至2016年年末，上海地区通过工商银行自主研发的外部欺诈风险信息系统已成功预警堵截近700笔电信诈骗汇款，为客户避免资金损失超过3400万元。

工商银行运用大数据技术于2013年在国内外同业中率先研发推出了“外部欺诈风险信息系统”，实现了对外部欺诈风险的实时精准预警和有效拦截干预。该系统收录来自行内、金融同业以及司法行政部门提供的各类风险客户和账户信息，建立起外部欺诈风险数据库，并与全行相关业务系统对接应用，形成集信息采集、风险预警、监测分析和主动控制为一体的全方位外部欺诈风险管控平台，系统实现日均筛查集团各类业务交易1000余万笔，平均每分钟筛查7000余笔。工商银行还完成了外部欺诈风险信息系统对涉案账户的全渠道布控，对所有通过网点、网上银行、电话银行、手机银行和自助终端等渠道进行的转账汇款交易进行即时筛查，及时向客户进行风险提示，对电信诈骗犯罪实时自动预警，从源头上降低电信诈骗得逞概率。

为增强社会公众对电信诈骗的防范能力，工商银行还于去年推出国内首款防电信诈骗公益软件——“工银融安e信”（公益版）。用户只需要通过手机下载并登录工商银行“融e联”App，即可在“发现”栏目中找到“融安e信”，并免费使用该软件，在办理转账汇款前对收款账号进行安全性查询。截至2016年年末，“工银融安e信”（公益版）点击量已超过548万次。

据介绍，在严格执行“四问一告知”“四核实”“七步法”等提示措施的基础上，交通银行上海市分行正不断提高技防手段，将防范重心由“宣传提示”向“预警拦截”转变。目前，一套由人民银行、公安机关、电信部门、工商管理部门、银行和支付机构共同建立的电信网络新型违法犯罪交易风险事件管理平台已正式上线，通过功能的持续完善，未来将可实现在网上银行、手机银行、ATM等多渠道拦截向可疑账户转账汇款。

为进一步提高电信诈骗案件事后拦截成功率，提升反欺诈工作效率，交通银行上海市分行将在交通银行总行推出的“总对总”网络查控平台基础上，加强与上海市公安反欺诈中心合作，提升公安对涉案账户的查询、止付、冻结操作效率。

电信诈骗『魔高一尺』 运营商服务『道高一丈』

■本报记者 朱伟

从2003年电信诈骗“初现江湖”至今,不法分子的诈骗手段伴随通讯习惯、金融支付手段的改变不断翻新“进化”:从1.0版的短信诈骗,到2.0版本利用网页种木马,随后是3.0版利用任意显电话,再到网页和电话混合型4.0版,移动端诈骗5.0版,最后发展到如今与网络投资等相关的6.0版。

在上海,电信、移动、联通三大运营商持续推动防范打击工作向纵深开展,目前已形成涵盖电话用户实名登记、重点业务管理、诈骗电话拦截、伪基站打击等工作的综合防范治理格局,通讯信息诈骗治理取得显著成效,受到用户普遍好评。

“400”电话原则上只能接听不得拨出

在上海电信营业厅，记者注意到员工业务手册中的一条新规定:严格执行新增业务“一季度一证一卡”,用户不能一次性购买同一家运营商两张及以上移动语音号卡。这一举措,彻底杜绝了“一人多卡”情况的出现,断了不法之徒的后路。

为防范通讯诈骗,三大运营商都加大了源头堵截力度。记者从上海电信获悉,上海电信重点加强中小渠道的管理,要求所有业务网店100%配备二代身份证读卡器、100%拍照设备、100%业务办理及身份证信息系统校验,且规定购买号卡必须当场实名登记并激活,非身份证证件办理入网,营业员必须引导用户到1–3级自营厅办理。与此同时,上海电信还要求各分局将“业务销量异常、受理时间异常、实名渠道异常、用户信息异常、人证合一不符”等场景纳入日常稽核工作,及时发现风险、预防问题发生。

曾几何时,400打头的骚扰电话是通讯信息诈骗的重灾区，上海电信在防范通讯信息诈骗中，将规范语音中继、400业务、一号通和企业总机业务作为重点,严格按集团公司要求进行业务受理。对于400外显(400号码作为主叫外呼,原则上400只能被叫),须通过集团审批同意后才允许实施,并暂停新增用户。目前，上海电信已完成重点业务语音中继、400业务全量存量用户签署使用承诺函,对于业务使用用途、外呼时段、呼叫频次等方面予以严格约束。新规实施以来,仅今年第一季度就关停三家语音中继客户,共计2500个号码。

各种防骚扰服务屏蔽垃圾电话

防止通讯信息诈骗,除了源头堵截,三大运营商还主动出击,实现对现网络诈骗信息的传播进行有效管控。

上海联通于2015年12月开通防骚扰提醒服务，这是上海联通提供的一种公益性质的基础提醒服务，直接在运营商侧实现。用户只要编辑短信“KT”至10655587,马上就能免费开通防骚扰提醒服务，运营商自动就可以帮用户屏蔽垃圾诈骗电话,从源头掐断诈骗信息。

如何让用户在遭遇欺诈或骚扰之后能够及时发现、如何让用户免受“呼死你”等诈骗新手段的骚扰,真正保护用户合法权益,已成为上海移动防范打击电信诈骗的关注焦点之一。为此,上海移动进一步强化手段支撑,通过技术手段优化和改造,向用户免费提供“0000”退订屏蔽、用户终端侧安全提示、“呼死你”防护等多项安全服务,2017年上半年,已累计处理“0000”退订屏蔽请求19万条、发送提醒彩印1975万条、累计拦截“呼死你”电话527万次。

大数据锁定诈骗电话拦截异常呼叫

面对日趋严峻的网络安全形势,政府与企业需要联手,通过产业链合作对抗黑色产业链。在这一背景下,包括大数据分析在内的一系列新技术的成功应用,为运营商打击通讯信息诈骗提供了可靠的技术保障。

2015年下半年,上海移动试点建设了公司诈骗电话智能分析平台。以事中劝阻为切入点,基于实时采集信令数据建立大数据分析模型,通过分析诈骗电话的行为模式快速锁定被深度“洗脑”用户,并在此基础上与执法部门合作,有针对性地开展事中劝阻工作,以期成功防范既遂诈骗案件。上海移动与公安等执法部门协同,大数据反诈骗手段启用至今,已合计成功劝阻受骗用户3200余名,准确率达94%以上。根据公安提供数据,2016年5–7月冒充公检法号码诈骗案件同比下降47.2%,案值同比下降34.9%。

在上海电信,相关部门目前已建成1–4期防欺诈系统,对于异常呼叫及时进行拦截,同时认真落实工信部、12321、公安、10000号等多渠道通报及举报的核查工作,对接公安反欺诈中心,接应黑名单关停,将被通报、举报、涉案号码作为样本,通过最先进的大数据技术分析,主动定位符合诈骗、骚扰、电话推销等特征的异常呼叫,并形成诈骗骚扰电话的“黑名单”和“灰名单”。截至目前,上海电信已清理22万黑名单号码,对于“灰名单”,则通过电信的闪信业务在用户接听期间实施提醒。截至目前,上海电信共发送提醒闪信超500万条。