

聚焦网络安全

弹窗为何成“毒”窗？

——部分网络弹窗违法信息治理难现象调查

新华社记者 覃星星 黄庆刚

观点

当前互联网治理力度持续保持高位。19日,据国家网信办信息,今年三季度,全国网信系统依法查处网上各类违法违规行,累计约谈1211家网站平台,警告954家,暂停更新489家。

但新华社记者调查发现,部分网络弹窗仍在传播色情、赌博、暴力甚至诱导自杀等违法信息,成为增大安全风险、严重影响青少年身心健康的网络“毒疮”,而当前网上仍存在运营发布“毒”弹窗的产业链。

部分网络弹窗成信息“毒”窗

“未成年的妹妹用电脑时,页面上突然就弹出色情照片了。”

南宁市民马嘉嘉的此类经历并不少见。市民吴芳珍一家也被网络“毒”弹窗困扰。

“我们和孩子一起用电脑看视频时,经常会弹出一些不堪入目的色情图片,连我们成年人看了都觉得露骨。”吴芳珍告诉记者,她很担心这对孩子造成不良影响。“更气人的是,这些页面还很难关闭。”

记者发现,使用某知名搜索网站时,有色情游戏弹窗广告不时弹出。记者点击关闭字样后,该页面反被打开,之后即便关闭了弹窗,刷新网页后仍会继续弹出。还有一些网络游戏缓冲时,网页会穿插弹出多个画面露骨的涉黄弹窗。另有大量赌博网站通过弹窗引流推介。

记者还发现,此类弹窗广告往往很难关闭:有的按钮十分隐蔽;有的没有关闭选项;有的设有多个“虚假”关闭按钮,引诱用户点击打开广告页面;还有一些弹窗广告,即使记者将其设置为“对此类广告无兴趣”或“一周内不推送”,仍频频弹出。

此类弹窗广告还可能引发安全风险。此前,江苏一名学生受免费赠送游戏皮肤弹窗信息诱导,被骗5.4万余元。

“毒”弹窗从哪里来?“弹窗广告”有市场

记者发现,有不少商家在网上经营“弹窗广告”业务。“国家虽禁止了部分



运营商弹窗广告,但我们有办法和网络运营商合作。”一家互联网广告公司客服告诉记者,公司经营弹窗广告业务已超过10年,任何信息都能投送,手机App和电脑网页均可显示,价格为6000元100万次曝光或2.5万次点击。

“我们的弹窗覆盖面很广,可以根据登录者搜索或浏览过的内容精准弹窗。”记者根据该客服介绍进行了调查,发现此类商家在接单后会通过技术手段非法搜集并分析网络用户上网行为数据,掌握他们的年龄、性别等重要信息,以此对网络用户进行分类。之后商家会根据广告主要求设置合适的标签用户,在他们上网时进行追踪并有针对性地投放广告,做到“精准定位”,且能实时监控分析投放效果。

记者还被告知,商家有技术“强迫”用户收看或点击弹窗。“我们有些弹窗不设关闭选项,点开后只能关闭网页才会消失。弹窗内容基本不受限制,有色情暴力内容也不会被封。”客服表示此类业务非常受欢迎,“目前公司每月有上百单弹窗业务,我自己每月也有几十单。”

中国信息安全研究院副院长左晓栋、北京师范大学网络法治国际中心高级研究员臧雷等专家表示,弹窗广告“精准投放”行为已涉嫌非法搜集网络用户个人信息,其追踪用户IP投放违法不良信息的行为对未成年人身心健康有重大负面影响。此外,臧雷表示,我国广告法第44条明确规定,在互联网网页面以弹出等形式发布的广告,应当显著标明关闭标志,确保一键关闭。“强迫弹窗”同样涉嫌违法。记者已将调查所获涉嫌违法线索通知当地执法部门。

专家:立法严管、依法重罚 营造清朗网络空间

据全国“扫黄打非”办公室数据,今年上半年,全国共查处网络“扫黄打非”案件1800余起,取缔非法不良网站1.2万余个,处置淫秽色情等有害信息840余万条。但治理“毒”弹窗难度依然不小。

——利益驱动。一位多年从事网络色情案件查处工作的公安民警表示,当前部分网站盈利能力不足,涉黄赌等违法生意“来钱快”,经营违法低俗信息

弹窗是不少网站的主要盈利点。

——处罚乏力。多名基层执法人员均表示,实践中存在违法获利与处罚不相称、处罚乏力的情况。“不法分子往往一个月能获利数万元,有的甚至短时间能赚上百万元,而其面临的处罚却相对较轻。有不少人接受处罚后重操旧业。”

——资源有限。一位地方工信部门负责人透露,当前部分地方监管部门在非法弹窗治理方面投入人力财力有限,导致一些不法分子得以浑水摸鱼、逃避监管。另外,实践中也存在执法标准不清晰、法律法规滞后、移动端监管成本大等难题。

基层文化市场综合行政执法人员建议,应根据违法低俗信息的投放频率、次数等,对相关违法企业依法加大处罚力度。

业内人士建议,应完善相关信息过滤屏蔽技术,构建更高效、开放的监督体系,加强职能部门间信息共享与执法合作。鼓励全社会积极参与网络综合治理,营造更加清朗网络空间和良好网络生态环境。

机构与平台应提高安全验证手段,手机丢失第一时间挂失SIM卡

事件曝光后,大部分涉事的平台和支付机构消除了受害人的贷款记录,并赔付了损失。记者了解到,相关支付机构已着手加强手机丢失防控策略,提升风控水平,适时升级身份验证手段。

针对电信企业存在的漏洞,工业和信息化部日前约谈了此次涉事电信企业相关负责人,并对三家基础电信企业提出要求,对于服务密码重置、解挂等涉及用户身份的敏感环节,在方便用户办理业务的同时要强化安全防护,加强客服人员风险防范意识培训,警惕业务异常办理行为。

中国电信相关人员表示,为进一步防范此类风险,将强化和规范挂失、解挂、呼转等业务的鉴权方式和流程,增加技术核验手段,提高服务人员风险防范意识,对频繁办理业务的行为加强监控,对异常行为进行限制和升级操作授权。

国家金融与发展实验室特聘研究员董希淼表示,非银支付机构及互联网金融公司担负着数以亿计用户的财产安全,有责任不断加强风险防控。针对手机失窃这种情况,金融机构应该考虑得更全面些,不光要“实名认证”更要“实人认证”。

此外,付亮说,相关单位和企业应及时对用户数据进行脱敏处理,按照最小必要原则收集、存储、使用,并注意分级分类保存。

普通民众如果手机被盜或遗失,应如何保护个人信息和财产安全?专家提示:

——第一时间致电手机运营商挂失SIM卡,以免不法分子利用“时间差”窃取个人信息。

——尽快致电银行冻结手机网银,只要办过银行卡的银行都要覆盖到,不要给不法分子留下可乘之机。

——对支付宝、微信等具有金融功能的应用及时支付冻结,且密切关注账户服务和资金变动。

——通知亲朋好友手机遗失,让他们不要轻信相信陌生人打来的电话或发来的信息。

——如果发现异常的资金使用情况,及时拨打110报警电话报案。

400元赌资牵出数十亿元大案 “90后”半年输掉3000余万元

——一起特大跨境网络赌博案件调查

新华社“新华视点”记者 熊丰 韩朝阳

视点

因在某境外赌博网站上非法赌博,“90后”黄某不仅输光家里积蓄,还盗取公司账上资金3000余万元并全部输光。

这只是今年公安机关侦破的一起跨境网络赌博案件露出的“冰山一角”。警方调查发现,仅2019年12月至今年2月,某赌博网站的充值会员数就高达54900人,资金流水达80多亿元。

随着警方深入调查,一百多名犯罪嫌疑人被抓获,案件背后的黑灰产业链条也渐渐清晰。

浮出水面:400元赌资牵出数十亿元大案

今年3月,河南省周口市公安局港区分局接到辖区一名市民举报,称其在某网站上输掉400多元。通过对该平台深入调查,一个涉案金额高达数十亿元的跨境网络赌博犯罪集团逐渐浮出水面。

经侦查,警方发现这是一家将服务器设在境外的违法网络赌博网站,赌博门类众多,网站规模较大。而在背后操纵这些赌博网站的主要犯罪嫌疑人,也藏身境外。

依靠上下游犯罪产业链,该团伙设计了各种赌博花样,利用赌客嗜赌心理,不断垒高投注金额,使其深陷债务漩涡。

为吸引更多赌客,该赌博网站还将活跃度较高的参赌人员拉拢为“网络赌博平台”代理。赌博平台会根据代理人员所拉下线的投注情况,返还千分之一至千分之三不等的佣金;投注越多,代理人员从中获取的佣金越多。

据警方介绍,仅2019年12月至今年2月,该网站的充值会员数就高达54900人,资金流水达80多亿元。

收到相关线索后,周口市公安局迅速成立专案组。经过努力,基本掌握了该网络赌博平台的组织架构、运作模式和部分代理的真实身份。一条涉及非法赌博、地下钱庄、银行卡倒卖等黑灰产业链条的跨境网络赌博犯罪脉络渐渐清晰。

3月27日,公安机关组成12个抓捕小组,连夜奔赴广东、湖南、江苏、浙江等15个省份,对犯罪嫌疑人实施集中抓捕,抓获犯罪嫌疑人45人,依法冻结涉案银行卡976张,扣押、冻结涉案资金2000余万元。

转移赌资:高价收购银行卡四件套

在对涉案人员进行抓捕的同时,专案组民警从研判涉案银行卡的资金流和信息流入入手,对调取的1500余张银行卡内近3个月的银行流水进行梳理,初步查清了资金流向。

其中,何某军贩卡团伙受雇于赌博平台,在国内以每套每月1000元的价格,大肆收购银行卡四件套(包括银行卡、U盾、手机卡、身份证复印件)。赌博网站给其每套卡每月3500元。他们将银行卡绑定在手机上,通过ATM机取现,再以将现金交给指定人员或网上银行转账等方式,帮赌博网站转移赌资。2019年7月以来,该团伙共收购银行卡四件套600多套,获利500余万元。

据负责执行抓捕任务的港区分局案件侦办大队大队长陈伟介绍,通过前期研判,警方锁定了福建省晋江市的蔡某。蔡某是本案重要犯罪嫌疑人,仅1月份就有1.7亿元违法资金转移至其银行卡中。专案组民警快速出动实施抓捕,当场缴获大量银行卡、手机、电脑等作案工具,查获大量证据。

截至9月21日,共抓获各类违法犯罪嫌疑人123人,其中代理人员34人,赌徒26人,涉嫌赌卡、洗钱人员61人,提供网络技术服务人员2人。该案还捣毁地下钱庄3个。

输光背后:每场下注都有人在后台操控

随着警方深入调查,掩藏在案件背后的一个个故事,也逐渐浮出水面,令人唏嘘。

半年时间,输掉3000余万元!

“90后”黄某原本是一家大型企业的财务人员,无意中接触到赌博网站,“开始的时候几百几千元地玩,后来断断续续输了几万元,就想投注多一点,哪怕赢个一两把也行。”

最初只是一次赌成百上千元,到后来一次赌上万元甚至数十万元;为了赌资,黄某就跟着了魔似的,到处借钱、贷款、刷信用卡。另一名参赌者郝某,在朋友李某的鼓动下,下载了一款名叫“统一”的手机App。“起初,她叫我跟着群里的投注信息投钱,我投了1000元,结果输了。再充3000元,又打了水漂。”之后,好友李某与所谓的“指导员”又以“保本”等言语诱惑,不断鼓动郝某增加投注。

抵押车辆、借高利贷、网贷……郝某通过各种手段,先后筹集了70余万元,结果全部在该App上输光。

在侦破案件的过程中,郝某所谓的“运气”也露出真相。原来,像郝某这样的赌客在使用该App时,其一切行为都已经被设计好,每场下注都有人在后台操控。

据警方介绍,这类网络赌博网站通常下设运营部、客服部、技术部等部门,各扮演拉人、“导师”、操控赌局等角色。网站先以“充10000送3000”“注册即送现金”等形式诱导人进行在线赌博,之后还会以“充值返现”“保本跟投”等形式持续吸引赌客加大投入。

警方提醒,一定要认清跨境赌博“十赌十输”“十赌十输”的骗人本质和严重危害,不断提高防范意识和能力,自觉抵制赴境外赌博或网上参赌。



“被消费”“被贷款”……

一部手机失窃遭“盗刷”暴露哪些安全漏洞？

新华社“新华视点”记者 吴雨 高亢 张千千

热点

近来,一篇网络文章受广泛关注:一名网友叙述了家人手机遭盗窃后“被消费”“被贷款”的遭遇。文章引发公众对手机失窃可能带来的财产安全问题的担忧。

目前,大部分涉事支付机构已赔付受害人经济损失。工业和信息化部也于日前约谈涉事电信企业相关负责人,并提出对于服务密码重置、解挂等涉及用户身份的敏感环节,要在方便用户办理业务的同时强化安全防护。

“新华视点”记者发现,虽然这是一起偶发事件,但暴露出一系列涉及公民个人信息和财产安全的漏洞。

据了解,案件正在进一步调查中。

手机失窃被不法分子进行多笔消费和贷款

据网民“信息安全老骆驼”称,其家人手机失窃后,不法分子利用电信、金融、支付等机构以及互联网金融平台的安全漏洞,新建账户绑定银行卡,几个小时内,便在线办理了贷款,并进行多笔消费。

不法分子是如何利用手机盗取资金的?

“信息安全老骆驼”向记者复盘了遭遇“盗刷”的全过程:不法分子取出机主手机卡,将之安装在自己的手机上,通过短信校验的方式,登录了某政务平台App,由此获取了机主的姓名、身份证号、银行卡号等关键个人信息。通过这些关键信息及校验短信,进行服务密码重置,掌握了对手机卡的主动控制权。此后,在支付宝、财付通、苏宁易付宝、京东支付等开立了新账户,绑定机主的银行卡进行消费,并在美团平台申请贷款,造成机主经济损失。

整个过程中,登录政务平台App获

取关键信息、绑定银行卡、贷款消费等操作,都是凭借手机短信验证码顺利通关。

记者了解到,此案之所以产生如此后果的一个重要原因,在于手机遭窃后机主没有第一时间挂失电话卡,令不法分子有了可乘之机。

专家解释,在电话卡未挂失的近2个小时,由于掌握了机主个人关键信息,不法分子通过手机在线服务,对服务密码进行了重置。这相当于掌握了通信业务办理的主动权,能进行远程解除挂失,还可以利用短信验证码登录其他网站和App。

手机失窃被“盗刷”暴露出哪些安全漏洞？

这一网民的遭遇暴露出手机信息安全和支付安全的多个漏洞,引发多方担忧。

——电话卡解除挂失等安全机制有待升级。

据其本人介绍,案发当日,在通过电信客服挂失后不久,他们发现手机卡居然被不法分子解除挂失,仍能使用。双方进行了激烈斗争:挂失、解挂、再挂失、再解挂……来来回回几十次。其间,这张手机卡不断接收消费和贷款的验证码短信。

多位业内人士表示,虽然机主手机被盜后未及时挂失电话卡,让不法分子钻了空子,但电信企业的服务密码重置和解挂失等业务规则是否完善、是否充分考虑了机主手机丢失的可能性,值得探讨。

按照中国电信的业务规则,已挂失账户可以通过拨打客服热线、服务密码鉴权后进行解挂。利用机主挂失前的“空档”,不法分子通过机主姓名、身份证号、短信随机码重置了服务密码,掌握了通信业务办理权,多次诱导电信企业客服人员对其已挂失的电话卡

进行解挂。

电信专家付亮认为,用户反复解除挂失的异常举动,应及时引起电信企业包括客服人员在内的系统的警觉,适当升级安全门槛,而不是依然机械地进行常规操作。

——校验手段普遍不足,风控水平参差不齐。

目前,虽然监管部门对于支付机构开户身份的安全验证有相关规定,但部分机构执行打了折扣。

记者调查发现,不少金融平台和支付机构开立账户或绑定银行卡的流程较为简单,一些机构在授信流程中,只增加了银行短信校验或公安网校验,就顺利放款。在此案中,不法分子通过机主的银行卡号、身份证号、姓名、银行预留手机号等信息,加上短信验证,就在美团平台上办理了贷款业务,并很快将贷款通过新开立的支付账户消费掉了。

业内人士专家表示,为吸引用户,部分金融平台不会在绑卡开户时增加烦琐的校验方式,而是简化开户流程。更有一些小公司,为节省成本而省略步骤,校验的完成度和可靠性难以保障。

与此同时,一些平台和机构风控水平不过硬。从网民“信息安全老骆驼”家人的遭遇来看,同样在凌晨三四点,有的支付系统风控成功识别了异常交易并进行阻断,有的则通过了不法分子的贷款申请,有的支持了不法分子数笔绑卡消费。

——个人敏感信息保护不力。

该案中,不法分子通过短信验证的方式便登录了某政务平台App,获取机主的重要信息如探囊取物一般。

业内人士表示,身份证信息和银行卡信息属于个人敏感信息,一旦遭泄露后果严重。身份验证要强化甄别“确为本人意愿”,如借助人脸识别等方式提高验证门槛。