2022年9月8日 星期四
责任编辑:张海 编辑:李月
十堰晚报

未履行网络安全义务　侵犯公民个人信息
帮助信息网络犯罪　破坏计算机信息系统罪

我市公安发布十大网络安全典型案例

本周是国家网络安全宣传周,7日,市公安局发布十大网络安全典型案例对社会进行警示,增强网民网络安全意识。

此次公布的案例主要涉及未履行网络安全义务、侵犯公民个人信息、帮助信息网络犯罪、破坏计算机信息系统罪四大类别。

■记者 杨建波 通讯员 唐克俊 实习生 吴鑫云

第一类 未履行网络安全义务

案例一:2021年,我市一车务服务有限公司所有人张某注册备案的网站,在没有使用后,公司一直未对网站备案进行注销,未履行网络安全保护义务,致使网站被植入赌博暗链,造成不良社会影响,违反了网络安全法规定。公安机关根据《中华人民共和国网络安全法》规定,对该公司处以警告,并责令注销其网站。

案例二:2020年,丹江口市公安局民警接上级公安机关线索通报,辖区一医院门户网站存在数据库高危漏洞。接到线索后,网安民警组织技术人员到该医院进行网络安全检查,发现该医院网络安全部门对门户网站数据库敏感字符未屏蔽,导致数据库注入检测时提示错误信息,存在极大网络安全隐患。民警立即要求该医院将网站临时关闭,断网整改。

案例三:2021年,我市一汽配企业网络服务器受到境外黑客攻击,遭遇勒索病毒袭击,该企业多台财务办公用的计算机文件被加密致使无法使用。公安机关在对该企业进行检查后,发现该企业存在网络安全意识淡薄,未制定内部安全管理制度和操作规程,未确定网络安全负责人等问题。该企业未充分履行安全保护义务是导致网络服务器遭受勒索病毒攻击的重要原因。

警方提醒:《网络安全法》第二十一条规定国家实行网络安全等级保护制度。不履行的由有关主管部门责令改正,给予警告;拒不改正或者导致危害网络安全等后果的,处一万元以上十万元以下罚款,对直接负责的主管人员处五千元以上五万元以下罚款。致使违法信息大量传播、用户信息泄露、刑事案件证据灭失,情节严重的,处三年以下有期徒刑、拘役或者管制,并处或者单处罚金。

第二类 侵犯公民个人信息

案例四:2021年,茅箭区公安分局民警发现辖区多个通信营业网点从业人员在帮助客户激活电话卡时,将客户的手机号码及验证码提供给多家短视频、游戏、理财等平台注册账号,每个账号获利6至7元。犯罪嫌疑人到案后,均供述了在帮助客户开通新卡的过程中,趁客户不注意,出卖手机号码及验证码进行牟利的犯罪事实。他们累计出售公民个人信息6000余条,非法获利3万余元。

案例五:2018年,李先生在十堰购置了新房,但房屋钥匙还没拿到,就接到很多装修公司打来的电话。李先生担心个人信息被别有用心的人利用,于是报警。接案后,市公安局网安支队立即着手调查,警方在对一家销售家具的商家进行调查时,该公司负责人交代,公司除拨打到店顾客电话进行回访推销外,还会通过共享交换、购买的方式从房地产、装修、家居等公司的业务员处获得"精准客户"信息。随后,警方找到装修公司负责人及瓷砖、水管业务员等泄露个人信息的"源头",相关人员均被追究相关法律责任。

案例六:2019年,我市公安机关民警发现本地居民高某通过臧某和马某非法查询了多名公民的个人户籍、快递收货地址、车辆档案等信息,后经公安机关顺线追踪,发现相关信息是从外省银行职员、网约车公司职员、计生办工作人员为主要源头的"内鬼"处购买。后民警奔赴多地将相关人员抓获,相关人员最终因涉嫌侵犯公民个人信息罪和因涉嫌非法获取、出售、提供公民个人信息的违法行为被追究刑事责任或行政处罚。

警方提醒:广大群众要妥善保管好个人信息,切莫轻易泄密。尤其在互联网上涉及到需注册个人信息时,一定要谨慎。各企业要充分认识保护公民个人信息的重要性,在业务活动中搜集、使用公民个人信息时,应当遵循合法、正当的原则,不可触碰法律底线;对从业人员要加强法律法规教育,坚决杜绝非法倒卖公民个人信息的行为。

第三类 帮助信息网络犯罪

案例七:2022年,我市城区一在校大学生李某将他的微信账号租借他人,并获得一天120元的"租借费"。尝到"甜头"后,李某干脆做起了代理"生意",摇身一变成为"中间商",开始拉"下家"出租微信账号,并从中赚取差价。就这样,李某手里一共管理着10余个微信账号,每天的净收入可达几百元。此后的半个月里,李某管理的10余个微信账号被陆续封号,这时他才意识到问题的严重性,决定收手不再出租微信账号。但最终李某仍被公安机关抓获,涉嫌帮助信息网络犯罪活动罪被追究刑事责任(本报6日曾报道)。

案例八:2021年,张湾公安分局民警在工作中发现一个名为李某的男子涉嫌买卖他人银行卡,在抓获李某后,李某如实交代了买卖他人银行卡的犯罪事实,以及3名出售他银行卡的"下家"。民警随后将另3名犯罪嫌疑人抓获,其中一名嫌疑人小吴年仅18岁,还是一名大一新生。小吴交代其在网上看到有人以每张800元的价格收购银行卡,于是小吴拿着他的身份证,去银行办理了一张银行卡,转手交易后,他获得了对方支付的800元。最终小吴等4人因涉嫌帮助信息网络犯罪被张湾警方依法采取刑事强制措施。

案例九:王某曾在境外一博彩网站工作。回国后通过他人介绍,王某认识了当时在一公司负责支付系统运维工作的技术人员黄某,两人一拍即合,搭建了用于为外汇期货诈骗、赌博网站等非法网站提供资金结算服务的非法结算平台。经过反复测试,该平台正式上线运行,自被公安机关查获通过该平台非法结算的资金高达11亿人民币。王某等三人因帮助信息网络犯罪被提起公诉。

警方提醒:大家切不要因为一时贪念而把身份证、银行卡、U盾及对公账号、手机卡等重要的个人信息出借或出售他人,被出借或出售的银行卡或手机卡通常被不法分子用于诈骗等违法犯罪活动,从而成为网络洗钱犯罪的帮凶。

第四类 破坏计算机信息系统罪

案例十:贵州19岁男子熊某从14岁开始自学网络黑客技术,后在网络上结识了在境外从事网络赌博违法犯罪活动的李某,应李某之邀,熊某出境到菲律宾一赌博公司任职,主要任务是为网络赌博提供技术支持、网站维护及广告推广等。

在菲律宾期间,熊某学到了大量赌博网站推广技术,并窃取拷贝了多种黑客攻击软件工具及木马文件,还结识了从事同样工作的龙某等人。一段时间后,熊某、龙某等人齐聚十堰自立门户,熊某负责攻击、渗透目标网站,拿下网站或服务器的控制权,给受害网站植入木马或链接,使这些网站在被访问时跳转到他们指定的赌博公司广告页面。吴某则负责给他们打下手,短短两周他就攻破了600余个网站,后该团伙被十堰市网警抓获。

警方提醒:计算机已普及,青少年学习网络技术途径众多,黑客犯罪行为人年轻化趋势明显。社会、学校及家庭对青少年教育应当各司其职,加强青少年的政治思想教育、法制教育和责任教育、人格教育和道德教育,提高青少年辨别真假、区分是非的能力,引导青少年正确学习和使用计算机和互联网相关知识,清醒对网上信息进行分析、选择,取其精华,去其糟粕。