

捕获仿冒 DeepSeek 手机木马病毒

国家计算机病毒应急处理中心发布防范措施

近日,国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室依托国家计算机病毒协同分析平台在我国境内捕获发现仿冒 DeepSeek 官方 App 的安卓平台手机木马病毒。

用户一旦点击运行仿冒 App,会提示安装所谓的“新版”DeepSeek 应用程序,实际上是包含恶意代码的子安装包,并会诱导用户授予其后台运行和使用无障碍服务的权限。同时,该恶意 App 还包含拦截用户短信、窃取通讯录、窃取手机应用程序列表等侵犯公民个人隐私信息的恶意功能和阻止用户卸载的恶意行为。经分析,该恶意 App 为金融盗窃类手机木马病毒的新变种。

网络犯罪分子很可能将该恶意 App 用于电信网络诈骗活动,诱使用户从非官方渠道安装仿冒 DeepSeek 的手机木马,从而对用户的个人隐私和经济利益构成较大威胁。

除仿冒 DeepSeek 安卓客户端的“DeepSeek.apk”之外,国家计算机病毒协同分析平台还发现了多个文件

名为“DeepSeek.exe”“DeepSeek.msi”和“DeepSeek.dmg”的病毒样本文件,由于 DeepSeek 目前尚未针对 Windows 平台和 MacOS 平台推出官方客户端程序,因此相关文件均为仿冒程序。

由此可见,网络犯罪分子已经将仿冒 DeepSeek 作为传播病毒木马程序的新手法。预计未来一段时间内,包括仿冒 DeepSeek 在内的各种人工智能应用程序的病毒木马将持续增加。

国家计算机病毒应急处理中心发布以下防范措施:

1. 不要从短信、社交媒体软件、网盘等非官方渠道传播的网络链接或二维码下载 App,仅通过 DeepSeek 官方网站或正规手机应用商店下载安装相应 App。
2. 保持手机预装的安全保护功能或第三方手机安全软件处于实时开启状态,并保持手机操作系统和安全软件更新到最新版本。
3. 在手机使用过程中,谨慎处理非用户主动发起的 App 安装请求,一旦发现 App 在安装过程中发起对设备管理器、后台运行和使用

无障碍功能等权限请求,应一律予以拒绝。

4. 如遭遇安装后无法正常卸载的 App 程序,应立即备份手机中的通讯录、短信、照片、聊天记录和文档文件等重要数据,在手机生产售后服务人员或专业人员的指导下对手机进行安全检测和恢复。同时密切关注本人的社交媒体类软件和金融类软件是否具有异常登录信息或异常操作信息,以及亲友是否收到由本人手机号或社交媒体软件发送的异常信息,一旦出现上述相关情况,应及时联系相关软件供应商和亲友说明有关情况。

5. 警惕和防范针对流行 App 软件的电信网络诈骗话术,如“由于 XXX 软件官方网站服务异常,请通过以下链接下载官方应用程序”“由于 XXX 软件更新到最新版本,需要用户重新授予后台运行和无障碍功能权限”等,避免被网络犯罪分子诱导。

6. 对已下载的可疑文件,可访问国家计算机病毒协同分析平台进行上传检测。

据央视新闻 记者 陈庆滨

酒后报假警 被拘留

“喂,110 吗?我举报有人赌博……”近日,本市静海区独流镇一男子拨打 110 报警电话,称某处存在赌博窝点,面对接警员的进一步询问,其无法提供准确点位,便开始大声叫喊,甚至对接警员“口吐芬芳”。

为及时固定违法犯罪线索,静海公安独流派出所迅速赶往男子提供的地点进行核查,但在周围未发现任何违法犯罪行为。通过调查,民警在家中找到报警的张某。原来,张某报警时处于醉酒状态,其报警内容不属实。酒醒后的张某对自己的行为感到十分后悔。他表示在酒精刺激下,没控制住自己的言行。

目前,张某已被依法行政拘留。
本报记者 常健

大货组团超载 全被查

宁河交警不断加大路面巡查管控力度,开展夜间道路交通秩序突击整治,连续查处 6 辆严重超限大货车。

近日晚间,公安宁河分局交警支队潘庄大队针对大货车超载超限,夜间出行等特点,在重点时段重点路段开展集中整治行动,次日凌晨在 112 国道与潮白河左堤路交口,接连查处 6 辆严重超载车辆,经过磅检测,6 辆货车车货总质量均在 92 吨左右,而车辆的最大允许总质量均为 49 吨,超载幅度均达 50% 以上。

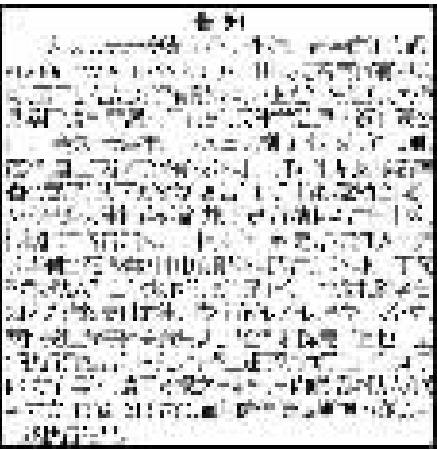
最终,在宁河交通运输部门对上述违法车辆监督卸载、消除违法行为后,交警依法对车辆驾驶人的违法行为予以处罚。下一步,交通运输部门还将根据“一超四罚”原则,按照《公路安全保护条例》和《道路运输条例》的规定,依法对货运车辆、货运车辆驾驶人、运输企业和货运场所经营者实施处罚。

本报记者 徐燕 通讯员 焦轩 黄磊

追缴珍贵文物千余件

新华社北京 2 月 17 日电(记者 熊丰)记者 17 日从公安部获悉,2024 年,全国公安机关与文物行政部门密切协作配合,累计侦破盗掘、盗窃、倒卖、损毁等各类文物犯罪案件 940 余起,追缴各类涉案文物 1.6 万件(套)。

一年来,公安机关聚焦盗掘古文化遗址、古墓葬和盗窃、倒卖、故意损毁文物等犯罪,挂牌督办一批大案,重点开展专项打击,追缴一批涉案文物。通过挂牌督办 7 起重大系列盗掘、倒卖文物案件,公安部指挥相关地方公安机关抓获一批犯罪嫌疑人,串并侦破案件 130 余起,追缴涉案文物 4800 余件(套);在打击整治损毁文物违法犯罪专项工作中,立案查处故意、过失损毁文物和故意损毁名胜古迹等犯罪案件 60 余起。公安机关累计追缴一、二、三级珍贵文物 1000 余件(套)。



刻意隐瞒财产 有能力却拒不执行 被传唤后履行义务

法院:构成拒不执行判决罪担刑责

近日,本市蓟州法院依法审结一起拒不执行判决罪案件,被告人张某因故意转移财产、拒不履行法院生效判决确定的义务,被判处有期徒刑八个月,缓刑一年。

2021 年 2 月,蓟州法院判决张某支付原告王某 80 万余元。判决生效后,张某未主动履行义务,法院依法扣划其银行账户存款。然而,张某为

逃避剩余债务,将其名下一处房产出售,并将所得款项另作他用,刻意隐瞒财产交易情况。2022 年 4 月,张某在法院执行局与王某达成和解协议,承诺分期支付剩余款项,但此后仍未履行。直至 2024 年 1 月,张某在公安机关电话传唤后主动到案,并最终履行全部执行义务。

蓟州法院经审理认为,张某对

人民法院的生效判决有能力执行而拒不执行,情节严重,其行为已构成拒不执行判决罪。鉴于张某主动投案并如实供述犯罪事实,自愿认罪认罚,且在案发后全额履行执行义务,法院依法对其从轻处罚,判处有期徒刑八个月,缓刑一年。缓刑考验期内,张某需接受社区矫正。

法官提醒

本案中,张某在明知法院判决生效的情况下,仍通过转移财产、隐瞒收入等方式逃避执行,严重损害司法权威和债权人合法权益。即使其事后履行义务,仍需承担刑事责任。执行生效裁判是公民的法定义务,任何试图隐匿、转移财产或虚假申报的行为均属违法。蓟州法院将持续加大执行力度,严厉打击拒执犯罪,维护法律尊严和胜诉当事人的合法权益。呼吁广大群众自觉履行法律义务,共同维护社会公平正义。如遇执行问题,可通过合法途径向法院申请协助,切勿心存侥幸、触碰法律红线。

本报记者 常健 通讯员 王欣欣

男子谎称自己为高校教师 有“内部消息”

花 44 万能“买”工作? 父子求职被诈骗

只要肯花钱就能“买”到好工作?近日,本市静海法院依法审理一起以“花钱托关系安排工作”为由实施诈骗的刑事案件。

2022 年 3 月至 2023 年 2 月间,男子陈某某谎称自己为天津某大学教师,且有亲友在广西、天津等地有“内部消息”,骗取岳某甲、岳某乙父子的信任,并以给岳某乙介绍天津某大学工作、办理学分及毕业设计、协调刑事案件处理等事项需要钱款为由,陆续骗取岳某甲钱款共计 44 万余元。因未实际办理相关事项,

岳某甲发现被骗后向陈某某索要钱款,陈某某退还其“打点费”7 万余元。

2023 年 9 月至 12 月间,陈某某还谎称可以帮助李某某的女儿介绍天津某集团工作,需要送红包、交押金,以此骗取李某某钱款 5000 元。陈某某将上述骗得款项用于偿还个人债务、日常消费等。

经法院审理判决,陈某某以非法占有为目的,虚构事实,骗取他人钱款,数额巨大,其行为构成诈骗罪,判处其有期徒刑六年六个月,并处罚金

人民币 8 万元。

拒绝所有预付费招聘

近年来,一些不法分子利用学生及家长急于求职的心理,用高薪诱饵、虚假招聘、伪造信息等手段实施就业诈骗,使受害者遭受损失。法官在此提醒大学生群体要牢固树立安全防范意识,通过正规渠道求职应聘,拒绝任何形式的预付费招聘。

本报记者 常健 通讯员 刘丽