

骗子盗取QQ号借钱 还能模仿号主声音?

相关链接

生成式人工智能技术 实行分类分级监管

近日,国家网信办联合发改委、教育部、科技部、工业和信息化部、公安部等公布《生成式人工智能服务管理暂行办法》(以下简称《办法》),自2023年8月15日起施行。国家互联网信息办公室有关负责人表示,出台《办法》,旨在促进生成式人工智能的健康发展和规范应用,维护国家安全和社会公共利益,保护公民、法人和其他组织的合法权益。

近年来,生成式人工智能技术快速发展,为经济社会发展带来新机遇的同时,也产生了传播虚假信息、侵害个人信息权益、数据安全和偏见歧视等问题,如何统筹生成式人工智能发展和安全引起各方关注。出台《办法》,既是促进生成式人工智能健康发展的重要要求,也是防范生成式人工智能服务风险的现实需要。《办法》提出国家坚持发展和安全并重、促进创新和依法治理相结合的原则,采取有效措施鼓励生成式人工智能创新发展,对生成式人工智能服务实行包容审慎和分类分级监管,明确了提供和使用生成式人工智能服务总体要求等等。

文/记者 吕嘉捷 漫画/刘哲姝

骗子不仅会盗取QQ号骗钱,还会通过模仿号主本人的语音进行诈骗。近日,市民陈先生致电本报市民热线 5589999 讲述了自己儿子的遭遇。他说,儿子小星(化名)刚放暑假就发现自己的QQ号被盗了,骗子用儿子的QQ号向亲朋好友借钱,前后骗走900元。这个骗局本来不新鲜,但是骗子竟然还会发语音给亲朋好友,声音跟儿子本人的很像。陈先生说,难道骗子已经用上了所谓的“AI换音功能”了?

据陈先生反映,7月11日,小星妈妈接到小星舅妈的电话说,小星在QQ上找她借钱,语气跟平时差别很大,她觉得不对劲,赶紧打电话过来核实一下。小星妈妈赶紧问小星,小星表示没这回事,赶紧查看手机,发现QQ果然被盗号,通过翻看聊天记录发现,骗子用自己的QQ号向多个亲朋好友“借”走了共900元,找每个人借的钱也不多,也就是50元、100元。小星赶紧向官方渠道申诉,但钱已经追不回来了。

让陈先生诧异的是,骗子可能是为了“取信于人”,“借”不到钱就给对方发去一段语音,证明自己是本人,而他发送的语音跟儿子的很像。陈先生说,本来一些好友看到是QQ借钱都比较警惕,但是骗子还会发近似的语音,这个迷惑性就



很大了,不少人因此中招。

厦门市打击治理电信网络新型违法犯罪中心的民警告诉记者,小星遭遇的就是冒充好友骗局,骗子先是通过非法渠道获取当事人的身份信息,同时通过一些技术手段盗取QQ号后,就伪装成号主本人向QQ好友借钱,一旦得手立即将钱款转移走。而此次是升级版的冒充好友骗术,更具有迷惑性,骗子会利用一些声音软件模拟当事人的声音,再配合嘈杂的背景噪音蒙混过关,不少人就被骗走了钱财。

至于陈先生所说的“AI换音”,民警分析这种情况可能性不大,一是技术难度较高,二是成本较大,骗子要在短短几个小时内完成难度较高,再加上此次骗取的钱财数目不大,这样做起来得不偿失。

民警也提醒广大市民,遇到好友以任何理由要求转账借钱时,一定要先通过电话、视频、面对面等方式验证对方是否为本人,切勿碍于情面而盲目相信对方,不经核实清楚切勿向陌生账号转账汇款。一旦发现QQ、微信等社交平台账号被盗,一定要第一时间向官方申请追回,并及时修改密码,同时可在朋友圈、QQ空间等予以澄清,以免他人上当受骗。平时也要注意勿点击一些来历不明的链接,以免个人信息被盗取。正值暑期,民警也提醒广大学生、家长等要小心机票、火车票改签、网购退款、兼职刷单、网络交友等各类骗术,有任何疑问都可以拨打96110全国反诈劝阻专线咨询举报,一旦被骗立即拨打110报警。

接到陌生视频电话 上万元没了

警方提醒市民提防利用手机自带通信软件实施的新骗术

警方提醒

陌生人的FaceTime 不要轻信不要接听

厦门警方分析,FaceTime、畅联视频通话可以简单理解为视频电话,不消耗电话费,使用的是流量。跟QQ视频和微信视频只能是好友发起不同,这类手机自带的视频通话功能只需知道当事人的ID邮箱号码即可拨打,允许陌生人发起,因此更容易被用来发起垃圾信息骚扰,这也为骗子联系受害人提供了方便。

厦门警方提醒广大市民群众,陌生人的FaceTime不要接听,如不需要可以设置关闭FaceTime功能。此外,在日常工作生活中,树立正确的消费观念和习惯,办理贷款务必做好前期工作;不轻信自称客服要注销贷款账号的电话,一旦提到“调整利率”“屏幕共享”“转账汇款”等字眼,务必提高警惕,谨慎操作。有任何疑问都可拨打96110全国反诈劝阻专线咨询举报。

警方反映自己通过手机通话软件接到类似的诈骗电话。厦门警方提醒广大市民提防利用手机自带通信软件实施诈骗的新骗术。

7月9日,周先生的华为手机收到陌生账号发来的“FaceTime”视频电话申请。接听后,对方自称是京东金融官方客服,称周先生的京东金融账号利率过高,已经影响到名下所有银行卡的正常使用,需要周先生配合注销相关贷款账号。为了取得周先生的信任,对方还用“人民银行征信中心”邮箱账号给周先生发了一封邮件,内容正是周先生与平台签订的电子协议书。随后,周先生在对方要求下,安装“Zoom”App共享手机屏幕,对方要求周先生申请资金保护,将名下所有银行卡的资金转移至同一张银行卡上,由银行方“监管”,待手续办理成功即可原路退还。周先生便使用手机银行转账至对方指定银行账户共计15587元。转出后,对方称周

先生需要等待半日才能收到信息。隔天,周先生再次联系对方,对方已将周先生拉黑,周先生意识到自己受骗,立即拨打110报警。目前,该案正在进一步侦办中。

据厦门市打击治理电信网络新型违法犯罪中心的民警分析,周先生遭遇的是冒充金融机构客服以“注销贷款账户”为由实施的骗术,此类诈骗分子常伪装成金融机构或金融监管机构工作人员,通过电话恐吓受害人征信已受影响,要求配合下调网贷利率或关闭网贷账号。之后,会伪造虚假征信报告、国家政策文件,借助官方公信力骗取信任。最后,以保护资金为由,让受害人将资金转至其指定的“安全账号”,接着又以需“清空贷款额度”为由诱骗当事人到多个平台贷款,并继续转账至指定“授权账号”扩大“战果”。而此次骗术的新特点是采用FaceTime、华为畅联等进行诈骗。



文/记者 吕嘉捷 通讯员 洪恒亮 漫画/刘哲姝

近日,市民周先生接到一通陌生的“FaceTime”视频通话后,被骗走1万余元。像周先生这样的受害者近期还有不少,许多市民都向