

揭秘 AI 诈骗“四大套路”

语音造假 视频通话都能换张脸

近日,2019年防范治理电信网络诈骗论坛在中国互联网大会期间举行。

论坛内容显示,机器学习、人工智能、大数据等热点技术已被犯罪分子用于实施诈骗。比如,上游黑产利用机器学习、人工智能,突破互联网企业的验证码体系,或是利用人工智能技术恶意注册,获取号码资源,而后提供给犯罪分子实施诈骗。

随着科技的进步,花样翻新的电信网络诈骗令人防不胜防。“技术一直都是双刃剑,我们在享受技术带来便利、新奇的同时,也会面临技术被滥用带来的风险。”中国传媒大学政法学院法律系副主任郑宁说。



诈骗手段不断翻新,四种形式防不胜防

随着技术的更新,诈骗手段也不断翻新,那么 AI 诈骗主要有什么方式呢?

对此,郑宁总结了 4 种 AI 诈骗形式,并详细介绍了其中的原理。

第一种骗术是转发微信语音。骗子盗取微信号后,提出转账要求,多数人会要求对方语音回复。这时,骗子会转发之前的语音,从而获取信任,进而获得钱款。虽然微信语音目前不能转发,但骗子可以通过提取语音文件或者安装增强版微信(一般是基于 xposed 框架的插件),实现转发语音。

“对于这种诈骗形式,群众只需提高警惕,直接电话联系,即可识破骗局。此外,即使要求对方语音回复,也可提出具体的要求,比如要求对方提供身份信息、说明转账原因等,避免骗子利用之前的语音蒙混过关。”郑宁说。

第二种骗术是声音合成。骗子通过骚扰电话等录音来提取某人声音,获取素材后进行声音合成,从而可以用伪造的声音骗过对方。

郑宁说,借助神经网络和机器学习技术,可以达到合成声音的效果。第一个利用神经网络生成人类自然语音的,是 DeepMind 的 WaveNet。WaveNet(波网)是一个用于生成原始音频的深度神经网络由伦敦人工智能公司 DeepMind 的研究人员创建。此技术通过用真实语音记录训练的神经网络直

接模拟波形,能够生成听起来相对真实的类人声音。

据了解,2016年,谷歌在加拿大蒙特利尔大学建立人工智能实验室(MILA),有位美国记者用机器合成的句子和家里人打电话,其家人完全分不清楚真假。

“合成的声音有明显的痕迹,但 WaveNet 可以把合成痕迹明显的机器语音转换成更加流畅自然的语音,与人类声音之间的差异大幅降低,目前在鬼畜视频界做得风生水起。而 Lyrebird 则更进一步,它可以基于音色、音调、音节、停顿等多种特征来定义某个人的声音,然后生成更加拟真的声音。”郑宁说。

第三种骗术是 AI 换脸。视频通话的可信度明显高于语音和电话,但利用 AI 换脸,骗子可以伪装成任何人。

第四种骗术是通过 AI 技术筛选受骗人群。通过分析公众发布在网上的各类信息,骗子会根据所要实施的骗术对人群进行筛选,从而选出目标人群。例如,骗子实施情感诈骗时,可以筛选出经常发布感情信息的人群;实施金融诈骗时,可以筛选出经常搜集投资信息的人群。

对此,中国人民大学法学院教授刘俊海说:“AI 技术用于诈骗已经不是新鲜事,因为任何新技术一旦出现,不法分子就会想到利用它来实施犯罪。”

加强个人信息保护,提高警惕防范诈骗

诈骗手法在不断翻新,那么广大群众该如何防止被骗呢?

郑宁提出了两点建议。第一是验证。提高警惕是防范诈骗的最好方式,在涉及钱款时,群众要提高安全意识,通过电话、视频等方式确认对方是否为本人;在不能确定真实身份时,可将到账时间设定为“2 小时到账”或“24 小时到账”,以预留处理时间。此外,可以选择向对方银行汇款,避免通过微信等社交工具转账。

第二是保护个人信息,

注重隐私保护。社交平台的发展加大了保护个人信息的难度,民众将越多的个人信息暴露在网络上,遭受诈骗的概率越高。实施诈骗需要获取当事人的个人信息,网络共享加上 AI 技术,骗子搜集整理当事人的个人信息更为便捷。因此,为避免骗子借用个人信息实施诈骗,民众应当加强个人信息保护意识,以防止骗子利用 AI 技术掌握大量个人信息,并对人物性格、需求倾向等进行刻画,从而有针对性地实施诈骗。

在刘俊海看来,预防被骗的关键是人们要提高自我保护意识,不要过于轻信网络上的信息,而且不要抱有侥幸心理,时刻记住天上不会掉馅饼,地上却会有陷阱。

“民众要避免占便宜心理,警惕陌生人提供的好处;要谨慎处理金钱交易,无法确认对方身份时,拒绝交易;要保护好网络账号及密码、手机号、身份证、家庭住址、亲属关系等个人敏感信息,不随意提供上述敏感信息。”郑宁说。

充分利用人工智能,提升反诈骗精准度

对于这种利用新技术的诈骗,该如何整治?

郑宁提出了 4 条监控整治建议:第一,即时通信、网络社交等平台企业应当加强账户管理,防止他人盗用用户账号及密码;建立风险提示制度,出现账号异常登录等情况时,对用户进行风险提示。第二,利用以大数据分析和智能预警算法为基础的 AI 技术进行反网络诈骗。在工信部等部门的主导下,利用大数据优势,将相关数据通过反诈骗机制进行共享,进而提高反诈骗的精准度。第三,建立专

门人工智能安全机构,制定人工智能标准,对 AI 技术进行管理和监督,监督 AI 技术在不同领域内的应用。第四,采取措施保证人工智能系统使用的数据被合理限制、管理和控制,以此来保护隐私权,在保护数据安全的情况下,不禁止利用 AI 技术造福公众。

刘俊海也提出了自己的建议。他希望监管部门和司法机关要善于驾驭 AI 技术,并且关注群众反映最突出的问题。

科技的发展虽然会给人们的生活水平带来便

利,但同时也会出现许多问题,那么应当如何减少科技发展所带来的安全隐患?

郑宁表示,科技发展与百姓生活是相辅相成的,科技发展使百姓生活质量有了极大的提高,因此应当大力促进科技发展。但也要认识到科技的两面性。科技发展的同时会产生一些负面影响,应当清楚认识并接受这一点,从而更加理性地看待科技发展,这有助于采取积极措施应对科技发展的负面影响。⑫ 2

(据新华社)

《南都晨报》系国家新闻出版广电总局批准、公开发行的都市报,国内统一刊号:CN41-0104。凡在本报刊登的遗失声明、公告等信息均具有法律效力。

遗失声明、增删资及注销公告

招聘求职、房屋出售出租……

找

南都晨报

分类广告

△《南都晨报》全国统一刊号,刊发遗失声明、公告等具有法律效力

△报社公众号、微信平台同步播发,影响大、效果好、收费低

△刊登广告方便、快捷,一个微信(19837709171)即可

做分类广告,就微信19837709171

分类广告部电话:63505002

遗失声明

●阳光财产保险股份有限公司南阳中心支公司交强险保单(代码:AB0507A32015A(豫),单证号:1702176、102177、1702180)遗失,声明作废。

●南阳万众文化传媒有限公司(统一社会信用代码91411303MA4638WX16)法人章、公章、财务章遗失,声明作废。

诚聘

南都晨报分类广告诚聘兼职业务员 20 名,不限年龄、性别、学历,人脉广即可。

咨询电话:19837709171

声明

南阳市绿城园林绿化有限公司(注册号:411302000042184)经股东会研究决定,拟向登记机关申请注销登记。公司已成立清算组,对公司进行清算。请债权人自本公告发布之日起 45 日内向本公司清算组申报债权,逾期视为自行放弃。特此公告。

诚聘

YOUR 高定礼服店是唐河首家集婚纱礼服租赁、出售,婚礼跟妆兼具婚庆一条龙服务于一体的高端私人订制专业团队。现诚聘高级销售顾问 10 名,高级化妆师 10 名。工资面议,有销售经验者优先录用。

联系电话:18317839931、15303777122

售房

人民路南头有一单元房出售,六楼顶层,121 平方米,经典三室两厅,大市房产证,出路好、价格优、可按揭。

联系电话:13503906183

出租

南阳市工业路天工牡丹园北院,三室二厅二卫出租。有太阳能热水器、空调、洗衣机各一部,带整体厨房,三张床。

联系电话:15839987345

苗木销售

唐河乐苑农场大量供应软籽石榴树、软籽石榴树苗、苹果树、桃树、梨树、冬枣树、枇杷树、山楂树、树莓、柿子树等果树,大叶女贞、小叶女贞、凌霄、花石榴、蔷薇、海棠、楸树、梓树等苗木。

联系电话(微信):13782172996