AI 犯罪的案例与措施

王曦 2021192010

数学与统计学院

计算机伦理

2023 年 06 月 25 日

1. AI 语音和视频诈骗

AI 语音和视频诈骗

- 2019 年 03 月, 华尔街日报报道: 犯罪分子通过商业化的人工智能语音生成软件, 成功模仿并冒充一家英国能源公司的德国母公司 CEO, 欺骗多位同时和合作伙伴, 一天内多次诈骗并转移资金, 使得该公司损失 220,000 欧元.
- CEO 的说, 当时他正在与他的老板, 即该公司德国母公司的首席执行官通电话, 对方要求他将资金发送给匈牙利供应商, 请求紧急, 要求行政人员在一小时内付款. 英国首席执行官认可了他的老板有轻微的德国口音和在电话中的声音旋律, 使他认为这就是他的老板.
- 未调查到犯罪分子.

AI 语音和视频诈骗

升级版:

- 2023 年, 内蒙古包头警方发布了一起用 AI 实施电信诈骗的典型案例. 福建的郭先生是一家科技公司的法人代表. 今年 4 月, 他的好友通过微信视频联系他, 称自己的朋友在外地竞标, 需 430 万保证金, 想借用郭先生的公司账户走账. 视频聊天 “核实” 身份后, 郭先生在 10 min 内, 先后将 430 万元转到对方的银行账户.
- 事后, 郭先生拨打电话才得知被骗. 骗子通过 AI 换脸和拟声技术, 佯装好友试试诈骗.
- 郭先生说: “当时是给我打了视频的, 我在视频中也确认了面孔和声音, 所以才放松了戒备”.

防范措施

- 打电话和视频都图灵测试? 小心丢了工作.
- 见面交易? 不现实.
- 涉及到资金时多方确认.
- 躺列的好友不亲信, 突然以语音或视频方式联系时应更警惕.

2. AI 换脸诈骗

AI 换脸诈骗

- 2023 年, 常州警方接到报警, 称自己因陷入裸聊陷阱被敲诈 11 万余元. 据了解, 不法分子利用 AI 换脸技术合成不雅视频进行敲诈.
- 2023 年 3 月 17 日, 苏州大学一大学生多次通过恶意 P 图、特效合成的手段在色情网站上传播多位女同学的色情内容.
- 许多色情网站上提供明星的定制化服务, 差别细微.

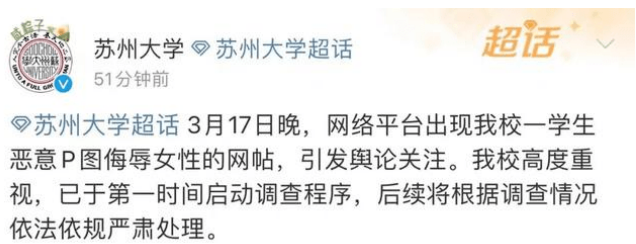

Figure 1: 苏州大学官方微博

Figure 2: 细节对比

AI 换脸诈骗

- AI 换脸为明星进行直播带货. 北京岳成律师事务所高级合伙人岳岫山表示: 换脸直播用于公开传播可能涉嫌侵犯相关明星艺人的肖像权. 若涉及直播带货等商业行为, 会成为加重情节.
- 娱乐性质: b 站上有大量 AI 换脸制作的马保国的鬼畜视频.

Figure 3: b 站上的 AI 换脸制作的马保国的鬼畜视频

防范措施

- 普通人防不胜防.
- 平台加强监管力度, 严格审查直播中是否存在 AI 换脸和拟声的行为.
- 提醒家人不轻信看到的图片和视频.

3. ChatGPT 犯罪

ChatGPT 犯罪

- 2022 年, 有机构通过 ChatGPT 实现了一个完整感染流程, 从创建令人信服的鱼叉式钓鱼电子邮件到运行能够接受英语命令的反向 shell.
- 2022 年 12 月 29 日, 一个名为 “ChatGPT-恶意软件的好处” 的帖子出现在一个流行的地下黑客论坛上. 发帖者透露, 他正使用 ChatGPT 进行实验, 以重新创建他安全研究产出物和常见恶意软件的撰写中描述的恶意软件病毒和技术. 此外, 他还分享了基于 Python 的窃取器的代码和恶意软件的 Java 片段.

ChatGPT 犯罪

- 2022 年年末, 一个名为 “Abusing ChatGPT to create Dark Web Market scripts” 的帖子展示了如何用 ChatGPT 搭建暗网市场, 并发布了一段代码, 该代码使用第三方 API 获取最新的加密货币作为暗网市场支付系统的一部分.
- 2023 年年初, 其他地下论坛有攻击者讨论如何将 ChatGPT 用于欺诈, 其中大部分集中于使用 DALLE2 生成随机艺术, 并在合法的平台上进行销售, 如使用 ChatGPT 为特定主题生成电子书.

防范措施

- 不点击不明连接, 不安装来路不明的软件.
- 不让陌生人接触自己的设备.
- 不连接到不可信任的 Wifi.

Reference

[1] DeepTech 深科技.AI 语音诈骗 173 万！模仿老板声音让科技公司上当，追捕嫌犯犹如大海捞针.
(https://zhuanlan.zhihu.com/p/81132879)

[2] 新华网.“AI 换脸”诈骗防不胜防？要用“法”打败“魔法”！
(http://www.news.cn/legal/2023-05/25/c_1129643944.htm)

[3] 塞讯验证. 担心的事情还是来了——网络犯罪分子开始使用 ChatGPT，AI 犯罪或成新趋势.
(https://www.freebuf.com/news/355374.html)

谢　谢!

Thank you!