来核实对方身份。

在鄢晓玲看来，现在的骗子也是“精准行骗”。他们会根据所要实施的骗术，通过 AI 技术筛选目标人群，在短时间内生产出定制化的诈骗脚本，实施精准诈骗。比如情感诈骗的骗子会筛选经常发布感情类信息的人群，金融诈骗的骗子会筛选经常搜索投资理财信息的人群。

“骗子都是聪明人。他们很会拿捏受害人的心理，比方说利用人的虚荣心，利用中国人爱面子、不好意思拒绝，或者利用一些人爱贪便宜、爱猎奇猎艳的心理，都很容易陷入裸聊杀猪盘等诈骗圈套中。”鄢晓玲说，这么多年来的反欺诈、违法违规内容鉴别工作，让她更加感慨现在的 AI 骗局，很容易通过骗子事先详细的“功课”，做到定制专门的骗局脚本，获取受害人的信任，让人防不胜防。

在 AI 诈骗面前，专家通常会根据画面的频域信息、质量、生物特性、物理特性等维度来鉴别真伪。对于普通人而言，可能需要更加谨慎地使用所有会让你自拍、录音的软件，也需要谨慎使用所有能访问你的摄像头、麦克风，甚至是相册的软件。

两位业内专家都表示，对于容易上当受骗或者对智能手机使用不那么熟悉的老人，帮助他们下载国家反诈中心 App 是一个很管用的选择。此外，尽量不要在微信、支付宝内绑定银行卡，只存少量的零钱，尽量不要开通网上支付业务。

萧子豪认为，AI 诈骗是在传统诈骗的基础上运用了人工智能技术，并不意味着传统诈骗手段不再存在或不再有效，只不过是增加了诈骗的复杂性和识破诈骗的难度。相比传统诈骗，AI 诈骗利用了“眼见为实”常识，降低了受害者的警惕性，也导致这类诈骗很难防范。

“对于普通人而言，如果说你发现诈骗的内容有违常理和常规的时候，不要第一时间相信，尤其是涉及个人财产的时候，就需要提高警惕。因为哪怕没有 AI，电信诈骗还是会存在！”鄢晓玲说，普通人很可能无法区别到底是不是 AI 在诈骗，但“事出反常必有妖”的铁律在任何时代都成立。遇事保持足够的清醒和质疑非常重要。

> 上海是个时时刻刻在变化的城市，**改变是唯一不变的东西。**

用魔法打败魔法

除了诈骗以外，AI 技术还被用来增加流量，非法获取收入。此前就有骗子将自己的脸 AI 换成某明星，开直播引导粉丝刷礼物，或者将自家主播 AI 换脸成杨幂、迪丽热巴进行带货。

纵观 AIGC 生成的海量内容，可能导致的违法乱纪情况，包括但不限于：误导性和虚假信息、不当或违法内容、深度伪造的内容、恶意利用的安全事件、伦理道德、歧视性内容和隐私泄露。

鄢晓玲说，自己所在的团队从 2012 年就开始与腾讯合作，进行反欺诈和反违法违规内容的模型识别工作。后来又开始与抖音、微博、快手、京东等大厂商合作。

“坦白来说，作为普通人，虽然说我自己很了解 AI 生成的一些原理和背景，但如果你随便拿一些东西来让我识别它到底是出自于 AI 还是出自我们人类生产，肉眼上，我是很难去识别的。但这并不是说我们就只能坐以待毙了。”鄢晓玲表示，用技术来判断是可以实现的，算法在一定程度上是能够去识别哪些是 AI 生成的，哪些不是。

但要让算法具备这样的能力，需要大量的标注和训练。你要告诉它这些内容是 AI 生成的，这些内容是人类生成的，然后再通过一部分人工去验证 AI 识别的准确性，通过

左图：有些商家将自己的主播 AI 换脸成杨幂、迪丽热巴等明星进行带货。