## 每周一案 第332期 谨防AI诈骗席卷而来

2023年4月，湖北省某市一名大学生郑某收到同学通过微信跟她借钱的信息。郑某向来谨慎，担心该同学不是本人，没想到同学发来一条语音，声音很像本人，后来同学又给郑某打了一通视频电话，看到对方的脸后，郑某便相信了对方，于是郑某便给其提供的银行卡转了6000元，郑某转完钱后越想越不对劲，觉得该同学表情僵硬，于是拨打该同学的电话，没想到该同学的微信账号被盗了，这才意识到被骗，随后立即报警。后来根据警方初步判断，通话的视频极有可能是诈骗分子通过AI技术“变声”、“换脸”诈骗手段合成而来。

**【案例分析】**

随着不法分子对AI技术的广泛运用，普通人面临着越来越大的信息安全隐患。正常情况下，人们都信奉“眼见为实”，尤其是随着视频通讯的普及，对于通过网络视频“面对面”的交流，大家总是很容易信任的。但在上述诈骗案例中，受害人郑某虽然具有一定的防范意识，但是面对新型的AI诈骗，还是落入了犯罪分子的圈套中。因此了解AI诈骗的套路和防范方法显得尤为重要。AI诈骗的常见手法主要是：

1、AI合成声音诈骗。骗子会通过拨打骚扰电话等方式，录音提取诈骗对象及其重要关系人的声音特征，利用AI技术进行语音合成，使诈骗对象放松警惕，进而用伪造的声音实施诈骗。

2、AI换脸诈骗。人脸效果更易取得对方信任，骗子用AI技术换脸，可以伪装成任何人，骗子会利用AI技术，将他人的脸换成指定人的脸，冒充诈骗对象的亲人、朋友等重要关系人，通过合成视频或照片来“以假乱真”，扰乱诈骗对象的视线进而实施诈骗。

3、AI筛选受骗人群。骗子不是漫无目的地广撒网，而是别有用心地锁定诈骗对象。他们会分析诈骗对象在网络平台发布的个人信息，根据所要实施的骗术利用AI技术对人群进行筛选，从而选出目标对象，制定诈骗计策。

**【保卫处提醒】**

广大师生面对AI诈骗时要牢记：

1、多重验证，确认身份

在涉及钱款时，大家要提高安全意识，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，要格外留意、不要着急汇款，避免上当受骗。

2、保护信息，拒绝诱惑

为避免骗子窃取个人信息实施诈骗，大家应当加强个人信息保护意识，·切勿接听任何陌生人邀请的视频验证或语音聊天，谨防骗子利用AI技术搜集人脸、声音等素材，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。

3、相互提醒，共同预防

做好宣传防范工作。多多提醒、告诫身边的亲人、朋友和同学提高安全意识和应对高科技诈骗的能力，共同预防受骗。