你的声纹可能被用来诈骗

接到陌生电话，先“沉默三秒”

最近有公安民警提醒，接到陌生来电，如果对方一直不说话，建议最好“沉默三秒”，不要先主动开口。个中缘由为何？原来是诈骗分子通过收集声纹，用AI合成你的声音，再冒充你给亲友打电话实施诈骗。



先开口，风险有多大？

2025年4月，湖北黄石3位老人先后接到家中“亲人”来电，电话那头传来“孙子”的哭声。骗子利用AI拟声技术高度还原声音，编造“孙子”“打伤同学需私了”“要到公安机关赎人”等事由，3位老人共计被骗走6万元。

电话骗子要冒充你，先得“偷”到你的声音。他们常用的手法是：拨通电话后沉默数秒，诱使你先说“喂？”“哪位？”等开头语。短短几个字的语音样本，就可能被AI复刻出你的声纹，进而冒充你实施诈骗。AI拟声技术能高度还原人声的音色并实现实时对话，一般人往往难以辨别真假。

声纹识别，究竟是什么？

声纹，指语音中携带的、能区分不同说话人的声波频谱特征。就像指纹能标识身份一样，声纹也具备独特性和相对稳定性，可以用来识别或确认说话人的身份。

清华大学人工智能研究院听觉智能研究中心主任郑方说，人的声音中蕴含的信息量非常丰富，包括性别、口音、内容、情感等。每个人的声道长度、形状不同，声纹因此具有独特性和唯一性。即便是双胞胎，声纹也各不相同，人耳难辨，AI却能区分。声音会因身体、生理、环境而变化，但声纹具有相对稳定性。

凭借稳定可靠的识别能力，声纹识别不仅可用于身份认证，还可拓展至更多应用场景。目前，声纹识别已广泛应用于公安侦查，可协助公安机关通过电话、网络语音通话识别嫌疑人身份。在金融领域，用户致电客服时，系统可以通过比对声纹快速确认身份，将其作为多层安全验证体系中的一环。

声纹被滥用，普通人该如何防范？

首先，要增强防范意识。接到陌生电话，不要先急着出声回应，静待几秒钟，让对方先发声；对以娱乐应用形式出现的陌生App，不要随意进行语音输入。

其次，接到陌生电话时，如果必须发声，要有意识地变换读音。声纹识别虽可靠，但前提是能采集到稳定的声纹。如果用户主动变换读音，攻击者即便录下或合成声音，由于读音不固定，也无法提取到稳定的声纹特征，这种攻击便无法奏效。

反诈民警提醒，接到自称客服或亲友的可疑来电，应先挂断，再通过官方渠道或家人常用号码回拨核实；难以辨明真伪时，可拨打96110咨询。尤其是来电声音与亲友相似的，更不能省略核实这一步。

相关链接

10家企业获批开展号码保护服务业务试点

日前，记者获悉，工业和信息化部日前批复同意10家企业开展号码保护服务业务试点，并为试点企业核配号码保护服务业务专用700号段码号资源，方便用户识别来电，更好防范治理电信网络诈骗和非应邀商业电子信息。



近年来，为减少用户手机号码在各服务环节泄露风险，各互联网平台企业普遍使用号码保护服务业务，即为用户分配临时号码（通常称为“中间号”或“隐私号”）代替真实号码，与外卖员、快递员、网约车司机等服务人员通信的一种业务。工业和信息化部去年印发《关于开展号码保护服务业务试点的通知》，明确号码保护服务业务参与主体、业务规则与监管要求，并规划15位700号段作为号码保护服务业务专用码号资源。

工业和信息化部信息通信管理局有关负责人介绍，经过企业申报、实地勘验、评估审查、系统建设等准备工作，中电信数智科技有限公司、中移互联网有限公司等10家企业已具备使用700号码开展号码保护服务业务的技术能力与资质条件。试点企业将通过与基础电信企业、互联网平台开展合作，优先在外卖、网约车等高频场景开展探索。

在上述接入场景中，用户可自主选择启用号码保护服务。试点企业的业务开通后，骑手、司机等可通过700开头的中间号与用户进行双向通话，通话过程中相互隐藏真实号码。同时，依托来电显示、接通前语音播报等方式，用户可进一步获悉来电的使用场景、平台主体等信息。

工业和信息化部下一步将在试点探索基础上，积极稳妥、循序渐进推进号码保护服务业务向更多企业、更多场景覆盖。同时加强行业管理和服务，完善相关管理政策，压实相关企业责任，推动号码保护服务业务更好地惠及广大人民群众。

本版稿件
均据新华社

这类诈骗需警惕

冒充车企发布“车辆召回”虚假信息

记者13日从北京市公安局刑侦总队召开的发布会上了解到，今年11月以来，虚假“车辆召回”类诈骗案件多发。诈骗分子冒充各大品牌车企客服，向车主发送虚假召回短信，诱导车主点击信息里的网址或扫二维码，通过“领取”修车补偿进而实施诈骗。

北京市公安局刑侦总队政治处主任李小燕介绍，截至目前，被冒充的车企品牌已有20余家。综合案件分析，诈骗分子多通过“iMessage”、普通短信等渠道向外发送虚假召回通知，信息能够精准显示车主姓名、车牌号，还附带伪造的官方文件、高仿官网链接及二维码。

骗子谎称车辆气囊、转向、制动等零部件存在安全隐患，不及时处置不仅会威胁行车安全，还将取消车辆质保，“逼迫”车主限时联系“客服”，并引导车主选择线上理赔、自主修车的退费模式。

当受害车主联系上“客服”要求退费之后，骗子会以提供的账户没有企业收款功能导致收款失败为由，引导车主通过“刷流水”开通银行卡企业收款功能。等车主彻底相信后，就以“输入转账编码”等为幌子，骗取转账金额。

北京警方提示，正规的车辆召回，不会通过私人手机号、“iMessage”、境外号码发送通知。车主收到召回相关消息，不要直接点开短信内链接，务必通过车企官方客服、官方App、授权4S店等正规途径核实真伪。同时，官方车辆召回只为车主提供免费检修服务，不存在修车补贴、理赔退款等项目。凡是借召回名义，要求“刷流水”、向陌生账户转账的，全部属于诈骗。遇到要求下载会议软件，索要银行卡、验证码，打探银行卡限额等情况，一定要提高警惕。若不慎点击可疑链接、开启过屏幕共享，请第一时间断网，及时联系银行冻结银行卡，守护账户安全。一旦发现被骗，请立刻拨打110报警求助。