贴心服务暖人心

平顶山联通公司浴“雪”奋战保通信

本报讯 近日，我市出现连续降雪天气，导致部分山区通信基站停电、通信线路中断。为确保人民群众通信畅通，平顶山联通公司组织党员先锋突击队不怕寒冷、迎雪而战，积极奋战在一线，全力做好抢修基站相关工作，用实际行动诠释了初心使命，保障通信畅通。

“拉我一把，我有点儿站不起来了。”在鲁山县熊背乡，一条架设于山间的基站通信线路被滚落的山石砸断，由于光缆接头位置较低，平顶山联通公司网络维护人员只能在零下10摄氏度的室外跪在雪地上弯着腰处理故障，冻得双手僵硬，使得操作更加艰难。当抢修完成时，维护人员却因为近一个小时的“跪姿”难以站立，在同伴搀扶下勉强起身，继续赶赴下一事故处理现场。

在浴“雪”奋战保障通信畅通的同时，平顶山联通公司扎实做好客户暖心服务工作。春节临近，在外求学、务工的老乡们都在陆续返乡，一场精彩纷呈的春晚、一顿阖家团圆的年饭成了这个冬天最温暖的画面。为切实保障返乡客户的用户体验，平顶山联通推出上门服务，从客户线上选购业务到产品交付，用户足不出户即可完成业务办理，无论是宽带装机还是卡品订购，无论是在偏远山区还是在闹市街道，客户的需求，风雪无阻。一个联通人就是一支队伍，截至目前，平顶山联通已受理并上门服务客户1.6万余户，来自平高社区的王阿姨说：“下雪了，路滑得很，联通的人上门服务就是中！”

（邢浩浩 文/图）

▶平顶山联通公司网络维护人员冒雪抢修

智能“骗脸”门槛低，照片也能刷脸……专家认为：

人脸不应该作为重要场景的唯一密码

一位女性手拿一张打印的男性照片挡在自己脸前，对着某品牌人脸识别门禁打卡机打卡，居然成功地被识别为这位男员工——这是中国信息通信研究院云计算与大数据研究所（以下简称信通院云大所）测试团队，在真实场景下进行的一项人脸识别测试。

很多人都觉得人脸识别非常方便，且潜意识里认为人脸信息是唯一的、不可更改的，因此是最安全的，但在互联网安全专家看来，将人脸识别作为唯一且重要的安全密码，是非常危险的，越是重要的应用，例如银行卡、家庭门锁等，用刷脸来做密码，就越发不安全。

人脸识别技术良莠不齐

拿起手机不到一秒钟，就自动解锁；凑近智能门锁，门就自动开了；使用银行APP时抬起手机，就能自动登录……如今，人们已经对生活中随处可见的人脸识别应用习以为常。

信通院云大所相关负责人说，自2021年6月起，该所启动了对可信人脸识别评测，上述以男性照片骗过门禁卡的实验，就是测试项目之一。

其实，人们早就对刷脸技术的安全性产生了担忧。2019年10月，浙江嘉兴上外秀洲外国语学校的同学们在一次课外科学实验中发现，只要用一张打印照片就能代替真人刷脸，骗过小区的丰巢智能柜取出快递件。当时有媒体记者验证后发现确实如此。

“像支付宝或者银行的人脸识别系统，应该是属于技术或安保程度比较高的，但也发生过问题。曾有被告人用别人的人脸信息，轻易绕过支付宝的人脸认证系统，顺利开设了账户，而被告人并不是什么高级黑客。”中国人民大学法学院教授、民商事法律科学研究中心执行主任石佳友说。

“说实话，人脸识别并没有那么准确和安全可靠。”石佳友说，“从纯技术角度看，人脸识别算法的品质本身差异就会非常大；镜头所拍摄照片的质量对匹配的精度也有显著影响。此外，识别度有一个置信度阈值，如果识别度过高，可能会导致更多的漏网，识别度过低，又会误识别一大片，这本身就是一个矛盾。”

据信通院云大所相关人士介绍，目前市场上人脸识别系统安全防护能力良莠不齐，一些人脸识别技术或产品存在明显的安全漏洞，给消费者的人身财产安全带来了极大的风险。

智能“骗脸”技术门槛低

做过人脸识别录入的用户都知道，被采集者需要通过眨眼、转头、张嘴等动作来配合采集“活体信息”。

“用活化程序，普通人都能够做到让照片摇头、眨眼睛。”清华大学法学院教授劳东燕说，“那种软件技术层级比较低。”

“过去人们常说有图有真相，但在智能换脸术面前，别说图了，连视频都不可信。”奇安信集团行业安全研究中心主任裴智勇博士说，通过人工智能技术，可以将一张普通的静态照片，正面、侧面均可，转化生成一张表情生动的人脸，甚至可以轻松地贴在另一个人的脸上，随着另一个人的动作和表情自动变化。

裴智勇说，以2017年左右的技术水平，已经完全有能力骗过绝大多数人脸识别系统，不过当时能够掌握这种技术的主要是人工智能专家，而随着技术的成熟，各种软件层出不穷，现如今这种“操作”普通人也能轻易做到。

劳东燕认为，虽然所有的个人信息泄露后都有风险，但人脸识别技术有其特殊性。其他的个人信息可能需要结合另外一些个人信息，才能识别到具体的某个人，而人脸本身就具有单一的可识别性，即用人脸信息直接就可以识别到特定的个人，因此风险更大。

“智能换脸的技术门槛比绝大多数人的想象要低得多，”裴智勇说。

人脸信息不符合密码规则

“我个人是非常反对生物特征的人脸识别作为用户的密码，去访问一些重要服务的。”科大讯飞副总裁、大数据研究院院长刘鹏说，“人脸作为密码去访问服务，除非是非常小额的支付，或者是无关紧要的一些登录。从人脸识别的生物特征看，它是违反密码基本原则的。密码的基本原则之一，就是用户可以随时更改，而人脸改不了。”他认为，目前还没有一个兜底的方案，来保证它的安全性。

“人脸识别是一种非常方便的验证方式，随身携带，不易丢失，但从网络安全角度看，人脸识别不适合单独使用或作为唯一的安全验证方式。”裴智勇也持同样的观点。他认为，人脸信息一旦泄露，无法追回更无法“换脸”，这不仅会让犯罪分子钻空子，在各种场合冒用身份，还有可能因此泄露当事人的行为轨迹及更多隐私信息。

“在安全工作者的眼里，人脸、指纹、声纹、虹膜等生物识别技术所识别的生物特征，都是静态的、可复制的信息，本质上和一串复杂的字符口令没什么区别，安全性也不会高到哪儿去，只是可以很方便地随身‘携带’而已。”裴智勇表示，尽管有些公司声称可以识别出真人和照片，那其实也不过是增加了信息复制或模仿的难度而已，并没有从根本上改变生物特征可以被复制且很容易被复制的本质。

人脸信息应用要设置前提

“在远程身份认证的场景下，几乎所有的生物识别技术都不适合单独使用。”裴智勇说，“刷脸虽方便，但并不是哪里都可以用。从纯粹安全工作的视角来看，人脸信息用作身份认证一定要结合应用场景。”

他认为，绑定设备本身既是一种使用场景限定，也是一种辅助验证方法，在刷脸支付、手机验证等远程验证场景下，需要配合手机绑定、短信验证码、大数据验证等辅助手段进行组合验证，如绑定手机支付，用自己的手机刷脸可以，用别人的手机就不行；从使用环境角度看，最好有人值守，如机场、火车站、小区、办公楼等，有保安人工值守或监控值守，可以一定程度上防止有人利用照片、假脸或数字仿真等方法欺骗识别系统；同时，必须要配合必要的网络安全保障措施，如身份管理、数据加密、威胁监测、运营监控等，以防系统被入侵、篡改和泄露。

“配合其他安全措施共同使用，人脸识别完全可能做到既方便又能保障安全。”裴智勇说，“比如刷脸支付，如果用户装有支付APP的手机原先一直在北京活动，某一天刷脸行为突然发生在广西，支付系统就应阻止验证被通过，这就是大数据安全验证模型保障用户账户安全的例子。”（武晓莉）