你“清粉”，它“侵”你——

小心中招！微信“清粉”暗藏风险

“系统正在检测删除我的人，勿回”“清粉请见谅。关注公众号可免费检测”……当前，不少微信用户选择用“好友清理服务”控制自己的微信好友人数。新华社记者发现，此类“清粉”服务中暗藏重大风险，可能导致用户微信账户失控、被盗，严重的还可能导致重要个人信息泄露、遭受网络诈骗等。

记者体验：微信账户“中招”了！

广州市民刘先生告诉记者，不久前，为清理微信好友，他尝试使用了“清粉”服务，结果令他至今十分“头痛”。

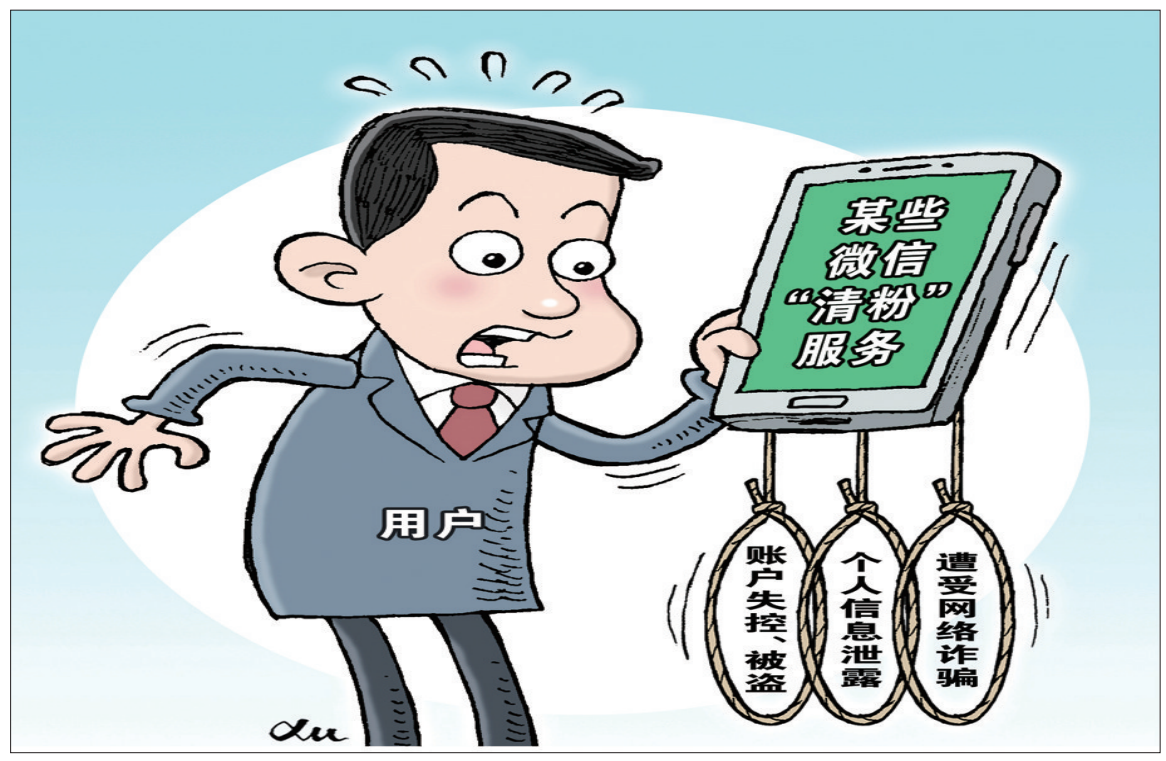
“我的账号自动在朋友圈里所有点赞过的信息下面发布了广告，不断有陌生人侵入我的微信工作群并在其中发布广告。我的部分微信好友也受到骚扰。”据刘先生回忆，这些情况都发生在他按“清粉”服务商家要求，扫描了其发来的二维码之后。

“把我的微信群和朋友圈弄得乌烟瘴气不说，要是有人假冒我找微信好友骗钱那就太危险了。”为避免同事、朋友因此受骗，刘先生不得不逐一在微信上联系大家进行解释。

记者在某知名电商平台搜索发现，有多家网店销售“清粉”服务，单价多为1至3元。据网店数据显示，部分月销量高达10万单。提供此类服务的微信公众号也为数众多，其中部分声称能“0误删0漏删”“无痕清粉”。

记者选择了一家自称提供“绿色清粉”服务的商家交易。商家要求记者将其提供的一个微信号加为好友，并扫描该账号发来的二维码。完成要求后，记者看到“微信即将要通过异地iPad端登录”提示。按商家要求，记者对提示进行了授权确认。随即，记者的微信中开始不断弹出被清除的好友名片，几分钟后，有信息提示清理完成。

然而就在此次“清粉”后不久，记者发现，自己被陌生人直接加为好友后拉入各种广告发布微信群的情况频频发生，微信被迫下线的情况也反复出现。网络安全专家告诉记者，记者的微信账户很可能已经失控。



一号多“吃”：“清粉”服务背后的利益链条

据信息安全专家徐超介绍，“清粉”的原理是通过应用集群控制软件控制待清理微信账户，令该账户自动向其所有好友群发消息，再由群控软件根据“信息是否能够成功发送接收”来识别其中哪些是“僵尸粉”并删除。

但除清粉外，群控软件还能控制微信账户批量点赞朋友圈内容、群发微信消息、自动同意好友添加并回复等。据微信安全团队介绍，一旦用户同意他人用群控软件“接管”账户，账户就很可能失控。不但会将自己的个人隐私完全暴露给他人，诸如工作、身份、联系方式、社会关系、财务信息等也都可能被他人获得。

记者调查发现，“清粉”服务的背后存在不法利益链条。

有人靠开发此类软件牟利。记者在网上发现，多家网站均可定制清粉软件，且显示已有成功订单。单款清粉软件开发价格在1000元至5000元不等。记者从某电商平台上的一家软件代开发商户处了解到，此类软件的开发成本和技术门槛都不高，代开发并不难。

还有不法分子通过“推荐朋友，免费清粉”“转发到群，赠送礼品”等手段怂恿引诱不明情况的用户将“清粉”链接、二维码等“入口”扩散到自己的微信群、朋友圈中，以此实现“病毒式”传播，扩大“中招”人群范围。

业内人士透露，对“中招”的用户，不法分子有多种“吃”法：先是赚销售清粉服务的钱。徐超告诉记者，不少经营相关业务的店铺月成交量不小，有的商家月销售额过万元。

然后还可以通过控制用户的微信账户，到处散发各种营销广告信息，再赚一笔。业内人士透露，当前互联网平台上部分打着“网络整合营销”“网络人际推广”幌子，散发“小广告”、制造“牛皮癣”的“黑商户”多与此类不法行为相关。

再有就是盗取受害用户个人信息，售卖牟利。网友黄女士反映，今年5月她在使用“清粉”服务后，很快发现微信中有一笔自己并不知情的交易，对方是某网络游戏。继而她发现，在这款从未接触过的网游中，竟有自己的实名注册账号。黄女士怀疑自己的个人信息已被“清粉”软件盗取。

徐超表示，当前“清粉”服务已成为非法数据交易产业链的重要“上游”，通过相关软件攫取的数据通常会在被分类后经由信息“地下市场”交易。记者了解到，不久前杭州互联网法院便审理宣判了利用“清粉”软件盗取个人信息的案件。

● 综合自新华社　　作者：张璇、胡林果、徐骏

微信官方：清粉服务，别用了！

微信团队提供的数据显示，截至2020年6月底，微信共对上百万个明确使用“清粉”软件等外挂的账号，进行了短期或永久限制处理。

“虽然微信官方不断打击，但要根治侵权‘清粉’软件恐怕并不容易。”广州某科技公司技术总监认为，在技术上，不法开发者正不断开发多种框架技术、底层指令与微信安全团队“打游击”；在销售上，部分商家将此类软件包装成“机器人助手”，增大了平台难识难度。

广州大学客座研究员李洋表示，用户个人应提升自身对个人信息与数据权限的安全保护意识，在网络上对陌生人、陌生应用保持应有的警惕，切勿贪小便宜吃大亏。

数字经济智库高级研究员胡麒牧认为，网络平台运营者应进一步强化履行互联网服务提供商安全防护职责的意识，善用人工智能、大数据等技术风控手段保障平台上的“绿色空间”，从源头上杜绝此类风险产生蔓延。

北京师范大学网络法治国际中心高级研究员臧雷提醒，部分“清粉”软件和服务商涉嫌侵犯公民个人信息、电信诈骗等犯罪行为，风险巨大，平台应针对此类服务或内容醒目标识，提示用户“切勿盲目向任何第三方授权，以防隐私泄露”。

“这不是某一家平台单打独斗就能彻底治理的，电商平台也应积极承担共同治理责任，加强对高风险商品商户的甄别与监管。”艾媒咨询CEO张毅说。

微信安全团队提醒用户，不要使用破坏微信软件协议或具有外挂功能的插件及软件。如遇安全风险，可通过微信客户端、腾讯110小程序进行投诉。

进小区、取厕纸都得刷　人脸识别滥用风险需警惕

点完餐看一下摄像头就能完成支付，住酒店刷脸后才能登记，上公厕用厕纸也得刷个脸才能取。随着人工智能的发展，人脸识别技术得到广泛应用，“脸”的应用场景被不断拓宽。

人脸识别技术看似“高大上”，但其存在的个人生物信息被过度采集和滥用的风险也不容忽视。相关专家表示，人脸识别技术不是万能的，收集、处理个人信息应当遵循合法、正当、必要的原则，基于身份验证等需要收集相关信息后也应尽到严格保管的责任和义务。中央网信办等部门近期也表示，针对面部特征等生物特征信息收集使用不规范等重点问题，App专项治理工作组将开展专题研究。

便利支付+身份认证　人脸识别应用场景不断拓展

在屏幕上点餐，选择刷脸支付，人脸比对后，输入手机号码后四位就完成付款。在上海一家商场的肯德基餐厅，记者观察发现，使用自助点餐机点餐的顾客中，选择“刷脸支付”的消费者占到两至三成。

除了大商场、大超市，部分便利店和街边小店里，刷脸支付设备也得到广泛应用。在上海陕西南路一家便利店，市民洪浩晨在购买一瓶饮料后，也通过刷脸方式完成付款。“从去年开始用刷脸支付就比较多，感觉比二维码方便。”洪浩晨说。

除了消费领域的便利支付，身份认证是人脸识别技术的另一大主战场。在全国机场和火车站的部分通道，乘客将身份证放在相应感应区，面部正视摄像头，每人只需几秒钟就可完成相关信息核验，快速进站。

一些公共服务机构还利用人脸识别技术来打击“黄牛”。复旦大学附属肿瘤医院一半以上的患者来自外省份甚至境外，该院去年就推出“人脸识别+身份绑定”系统，强化早高峰时段热门专家（特需）现场号源的管理。通过人脸识别系统绑定挂号人的身份，使得号贩子失去了现场“投机挂号”的操作空间。

“考虑到家属、亲友代挂号的情况，我们还设定每位患者可以绑定一位代挂号人身份认证信息。”复旦大学附属肿瘤医院门诊办公室主任董枫说。

不仅是医院，记者发现，各地政务类App中，刷脸登录、人脸验证已经广泛使用，如某地公积金App，用户就可通过人脸识别完成验证，线上支取公积金。上海市民胡志国说：“年纪大了，密码经常忘，尤其是登录一些不常用的App时都需要重置密码，刷脸就不存在这个问题。”

进小区、取厕纸都得刷　人脸识别是不是用得太多了？

不可否认，在人工智能成为新基建的背景下，人脸识别技术有其先进性和高效率。但任何先进技术的应用，都有其边界。在一些不必要的场景下，让渡自己的隐私，来换取一张通行证，必然会引起越来越多的反弹。

“现在上班刷脸打卡，工作时刷脸打开手机、笔记本电脑，午饭时刷脸支付，出差住酒店也得刷脸登记，甚至上公厕取厕纸都要刷脸，这张老脸是越刷越多，总感觉不对劲。”有网友如此感慨。

——强制刷脸遭质疑。记者梳理发现，关于公共场合使用人脸识别技术的争议和投诉正在增多。在合肥市“12345政府服务直通车”上，7月份有市民投诉：“繁华逸城”小区更换新物业后，办理门禁卡强制要求采集业主人脸信息。

对此，肥西县政府回复称，该项目的初衷是创建智慧平安小区，系统最终接入公安后台。“考虑老人和儿童人像采集不方便，可以办理门禁卡。”

上海一居民小区近期将小区门禁系统改为人脸识别系统。小区居民王女士说，改造前所有住户均需到物业采集人脸信息，“其实大家对采用人脸识别系统还是认可的，只是不知道个人信息是否会得到很好保护。物业为了让大家放心，出具了一份承诺书，承诺将严格保存收集的相关信息。”

——技术能力参差不齐。丰巢快递柜此前曾试点“刷脸取件”，其后被发现使用打印的取件人照片，也可以轻而易举地刷脸打开快递柜取件。丰巢回应称，“刷脸取件”功能仅为小范围试运营，并将测试版下线。

据悉，人脸识别技术可粗略分为基于2D人脸图像的技术和基于3D人脸图像的技术。通过照片即可完成人脸验证，大概率是采用了技术门槛较低的2D人脸图像认证。中国物流学会特约研究员杨达卿说，快递物流行业涉及消费者个人信息和财产，推广使用新技术时应慎之又慎。

——信息安全存隐忧。“密码泄露了，可以换一个，这脸部信息要是泄露了，可怎么换啊？”不少网友表示。

北京大学法学院教授薛军表示，人脸信息作为生物识别信息，一般来说伴随着人的一生，是不可更改的。这与手机号码之类的个人信息不一样，后者发生泄露，实在不行还可以换一个。但人脸信息发生泄露，不太可能去“换脸”。

● 综合自新华社　　作者：杨有宗、何欣荣、龚雯、王鹏

不宜普遍适用　更不能在商业领域强制使用

人脸识别技术虽然有其优势，但并不能在生活各个领域普遍适用，更不能在部分商业领域强制使用。北京志霖律师事务所律师赵占领认为，收集使用个人信息，需要遵循三个原则，也就是合法、正当、必要原则，但目前缺少判断必要性的标准和依据。“目前收集人的脸部特征信息的商业机构，大多数是基于身份验证的需要。在企业收集这类信息后，能不能妥善保管并按照事先所告知的方式去使用相关信息，这也是大家最为担心的。”

薛军认为，利用人脸信息来快速、精确识别个人主体，对于个人行动轨迹的追踪非常高效，但因此对个人隐私权可能带来的侵害，也非常严重。

中国政法大学传播法研究中心副主任朱巍说，对收集个人生物信息的管理，核心在于对获取方的管理。“现实中遵循的原则应当是能不采集个人生物信息就不采集，而且宜通过立法，进一步明确具备采集资格的主体范围。消费者面对商家，也应当有控制、注销已被采集的生物信息的权利。”