警惕“PS”合成“艳照”敲诈勒索

□潍坊日报社全媒体记者 王晓萌

手机提示音响起，一条短信跃入眼帘。打开一看，瞬间目瞪口呆，“艳照门”主角竟然是自己！发信人更是嚣张地表示，如果不乖乖交钱，这“艳照”就会发到网上公之于众……近期，各地通过短信方式发送匿名信件PS“艳照”或“不雅视频”的案件高发，潍城公安分局民警对此类诈骗手法进行了分析，提醒广大市民要提高防范，以免掉入不法分子的陷阱。

近日，市民李先生向潍城公安报警称自己收到了一条威胁短信，对方以一张PS处理过的图片，试图对其进行勒索。紧接着，李先生所在的工作单位收到一封匿名信，对方称其受客户委托，对李先生进行跟踪调查，现已经掌握李先生生活不检点的证据，李先生可“拿钱消灾”，否则将把相关照片和视频曝光。

李先生表示，他确实没有拍过这样的视频，但对方发来的图片确系他本人，所以选择报警求助。

民警介绍，在这类案件中，诈骗分子通过PS技术移花接木，通过各种渠道获取受害人的照片，合成“艳照”或“不雅视频”，以信件或发送短信息方式投递给受害人，进而敲诈被害人。

此类诈骗主要有以下特点：一是侵害对象广泛。侵害对象主要针对特定的社会公众人物，如企业家、各行业管理者、公职人员等；二是“不雅”模板统一。不法分子按照固定模板合成制作虚假“不雅视频”或“艳照”，然后通过短信、邮箱、信件等方式精准发送给选定的对象；三是诈骗话术如出一辙。不法分子一般会以恶意骚扰、举报、向身边人散播等手段，威胁敲诈受害人，迫使受害人将钱汇入指定的银行账户。

遇到此类事件应当怎么办呢？警方提醒，凡是收到来路不明的照片、视频，不要有“破财消灾”的念头，要做到不听、不信、不转账；保护个人隐私至关重要。现实生活中，微信朋友圈的一张“人像照片”或一段近距离的人物视频，都有可能被不法分子利用，成为他们的犯罪手段和工具；遇到相似情形的诈骗，注意保存照片、视频、文字等证据，及时拨打110报警。

安全大讲堂

这些办公“黑科技”可能有失泄密风险

科技蓬勃发展的数字时代，网上办公以其时效性和便捷性成为当今社会一种流行的工作方式。诸多线上平台汇集了强大的即时交流、格式转化、文件快传、群组讨论等兼顾社会交流和办公工具属性的“黑科技”功能，成为广大上班族处理日常事务的首选。然而，近年来因使用网上办公程序而导致的失泄密案件屡屡发生，暴露出一系列风险隐患。

云助手泄露涉密文档 “文件传输助手”能够实现文件云端存储，在不同设备终端均可下载使用。一些上班族为图工作便利，将涉密文件违规传输至“文件传输助手”，方便下班后使用个人手机或电脑下载处理。殊不知涉密文件上传网络后，电脑和手机设备自动同步与存储的过程大大增加了境外间谍情报机关通过木马病毒获取相关文件的风险。此外，传输软件公司后台也能轻易获取涉密文件，且无法有效控制知悉范围，极易造成失泄密。

图文识别小程序泄露密件原件 OCR识别技术的成熟给办公工作带来了十足的便利，种类繁多的图文识别小程序能够轻松抓取图片信息中的文字并一键转换文本。部分涉密岗位工作人员为导入密件文字内容，违规将密件使用线上小程序进行拍摄识别。尽管有意遮盖了密件的红头标志和密级，但密件原件的图片上传网络平台后，境外间谍情报机关通过技术手段能够轻松获取软件后台数据，窃取国家秘密。

AI写作泄露涉密内容 近年来，AI写作蓬勃发展，逐渐成为许多办公人士的“笔杆子”，用户只需要输入具体需求，就能一键生成文章。部分涉密人员在起草涉密材料时，为节省工作时间，违规将涉密素材和涉密文件内容输入AI写作小程序生成文章，并认为只是截取文件片段，不至造成泄密。殊不知，AI小程序会自动收集用户输入的信息内容以供自主学习，相关数据易被境外间谍情报机关窃取，造成国家秘密泄露。

工作群组泄露涉密信息 许多单位为方便沟通，组建了许多用来通报交流工作事项的“工作群”。部分单位违规在“工作群”中通知、讨论涉密工作事项，甚至将涉及国家秘密和工作秘密的内容以图片、文件等形式在群聊内发布。这些群聊中的涉密信息极易被群成员转载甚至对外公开，无法控制知悉范围。境外间谍情报机关还能通过网络攻击获取重点工作群组的聊天记录，存在极大失泄密隐患。

安全提示

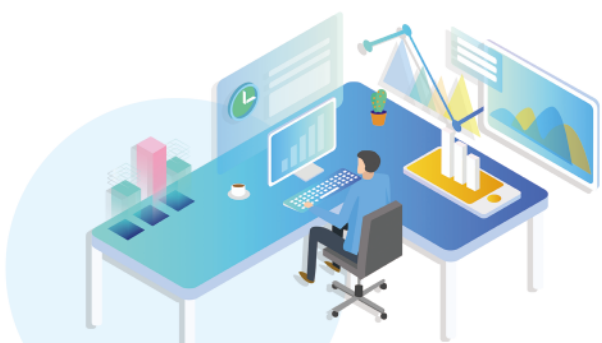
网上办公勿涉密 严禁通过互联网处理涉密信息，使用办公软件时禁止在线上发布、传播涉密信息，不能以方便工作为由将涉密文件线上存储。

小程序使用莫大意 严禁将涉密文件拍摄、摘录后上传互联网，使用文字识别、AI写作等功能时应杜绝输入涉密文件，防止方便了工作却泄露了秘密。

个人设备常自查 从事涉密岗位、有机会接触到涉密内容的工作人员应定期对手机、电脑等私人电子设备开展自查，杜绝用互联网设备处理涉密信息，同时也要及时对涉密计算机开展病毒自检，防止境外间谍情报机关植入病毒窃取数据。

企事业单位重教育 涉密企事业单位要定期开展国家安全宣传与保密警示教育，对内部“工作群”加强监督检查，履行涉密材料处理的日常监督责任，抓好涉密人员日常管理。

据央视新闻客户端



“老师”班级群里收费 小心是“李鬼”

□潍坊日报社全媒体记者 王晓萌

近期，不少家长遭遇“班级群”骗局，骗子通过各种手段混入班级群，迷惑家长和学生骗取钱财。为此，寒亭公安分局民警对此类诈骗进行了解析，提醒家长提高警惕，以防掉入诈骗分子精心布置的陷阱。

民警介绍，在此类诈骗中，不法分子混入班级群的方式有很多。

一是利用部分学生有打游戏的爱好，通过赠送游戏皮肤等方式，诱导学生给其发送班级群二维码；二是有不法分子会直接在QQ内搜索班级群的群聊关键字，即可出现大量公开的群聊信息，申请后便可进入；三是有些学校在家长群的运营安全上较为松懈，班级群微信号、QQ号（老师的微信号、QQ号、手机号）直接写在黑板上或对外公开，给了不法分子可乘之机；四是不法分子通过各种方式获取一些学生的信息后，伪装成学生家长添加班主任QQ或微信，由于学生众多，老师并不会仔细核实，添加成功后，不法分子会要求老师将其拉入班级群；五是不法分子在校园门口逗留，与其他家长闲聊、套近乎，获取相关信息后把自己伪装成学生家长，并向家长索要班级群的二维码，由于很多群聊设置并未开启“群主确认”功能，不法分子可直接扫码进群。

警方表示，不法分子进入班级群后，便可查看该群班主任老师头像、昵称、群备注等信息，然后下载头像、复制昵称，快速创建高仿账号，迷惑性极强。由于老师在上课期间会开启消息免打扰模式或关闭手机，不法分子会挑选老师上课、午休等时间段下手，利用时间差进行诈骗。许多家长见老师发布收费通知，会立即响应，收款率较高。

为了防止不法分子随意进入家长群实施诈骗，警方提醒，无论是QQ群还是微信群，群里的老师要加强对家长群的管理，群管理员可通过设置“加群验证”防止骗子随意进入家长群，家长进群后，需要按要求修改自己的昵称，便于管理；如果有人在家长群中发布收费信息，家长要第一时间联系留存的班主任电话进行核实，也可以通过学校的联系电话或教育机构的官方渠道进行确认。教育费用通常会通过正规渠道收取，不会通过个人账户或非官方平台进行转账；警惕异常要求。如果对方要求额外支付不明费用（如购买电子卡等）或提供个人敏感信息（如身份证号、银行卡信息等），要提高警惕；若遇到可疑情况，要保存聊天记录、转账记录等证据，并立即报警。