民生调查

工作群发来“领取补贴”通知？谨慎点！

“本以为是群里同事发的正常补贴通知，谁知填完信息没多久，银行卡就收到了扣款提示，这才反应过来被骗了。”北京某机关单位工作人员张先生说起此前在单位工作群内的遭遇，仍心有余悸。

“2025年综合类补贴申领”“加班补贴申领”“育儿补贴限时申领”……岁末年终，各类补贴政策集中落地。一些诈骗分子打着“政府福利”的旗号，借助木马病毒渗透进入单位办公渠道，冒用领导、同事账号实施精准诈骗。

据悉，目前部分政府机关、企业单位、学校等均已出现相关案例，一些市民因信任同事身份而放松警惕，最终遭受财产损失。

套路1
工作群里混进了假“同事”

张先生在单位办公时，内部办公软件的工作群里弹出一条消息，发送者显示是单位同事，内容附带一则“个人劳动薪资补贴申领”网页链接，还标注“限时申报，逾期作废”。想着是单位内部群里的消息，发送人又是熟悉的同事，张先生未多核实便点击了链接，页面跳转后显示为政务服务相关界面，看起来十分正规。

按照页面提示，张先生填写了姓名、身份证号、手机号及银行卡号，后续页面又要求输入银行卡密码、短信验证码，甚至需要填写账户余额，称“用于核实补贴发放额度”。张先生并未察觉异常，逐一完成了信息填写。

没过多久，张先生的手机便收到扣款短信提醒，累计损失3000余元。直到他联系发送链接的同事核实，才知对方从未发布过该补贴通知，两人这才意识到遭遇了电信诈骗。

无独有偶，北京某研究所工作人员李女士也遭遇了类似骗局。此前，她的工作邮箱收到一封来自同事的邮件，主题为“关于领取2025年劳动补贴的通知”，邮件内附带了申领链接，还备注“经单位核实，该补贴为国家专项福利，符合条件人员均可申领”。

李女士打开链接后，页面显示为“国务院客户政策信息服务平台”相关界面，她随即按照提示填写了个人身份信息及银行卡密码等相关资料。填写完成后，页面提示“补贴将在3个工作日内到账”。结果当天李女士非但没等到补贴，自己银行卡内的4000多元也没了。经警方核查，该邮件链接为钓鱼链接，发送邮件的同事账号已被木马病毒控制，邮件实际由诈骗分子发送。

套路2
这样的“福利”一骗一准儿

除了政府机关、科研单位外，针对企业员工及学校师生的补贴类诈骗也有发生。

某集团员工赵先生的遭遇十分典型。他在公司内部办公软件上收到同事邀请，加入了一个新的工作群，群内成员也都是公司“同事”。进群后，群内有人发布“领取财政补贴”的通知，并称“该补贴为公司专项福利，仅限群内人员申报”。赵先生想着是内部办公软件搭建的群聊，且群内都是同事，便点击链接填写了相关信息，结果账户内7000余元被瞬间盗刷。

学校老师同样未能幸免。北京某中学两名教职工在内部微信群看到“同事”发布的补贴申领通知，部分还附带“我已经领到了，大家赶紧申领”的话术，见“同事”已经申领成功，两人便放松了警惕。最终，一人被骗走1800元，一人被骗走2900元。

记者了解到，除了利用工作群，部分补贴类诈骗还会针对宝妈、学生等特殊群体。市民王女士回忆，“育儿补贴”制度实施方案公布没多久，她就接到自称是办理补贴的工作人员来电，称“孩子出生时没有签署补贴协议，补贴无法通过”，并让她加入一个QQ群“核实身份”。没过几分钟，一自称是政府工作人员的男子向王女士发来语音请求：“我们要确认一下您的身份，请您配合。”该男子一边说，一边催促王女士提供个人信息。

“你工号是多少？具体单位是哪里？”王女士连连追问，但对方支支吾吾。王女士起了疑心，要求对方开视频，“我要看看你是不是官方人员。”话音刚落，男子先是沉默几秒，紧接着爆出粗口：“你是不是存心刁难！”然后狠狠挂断电话。不到1分钟，QQ群也消失不见了。

（文中电诈受害者均为化名）

诈骗分子在网络上发布的补贴信息 图片来源于网络

拆招

索要密码验证码务必警觉

朝阳反诈中心民警王佳告诉记者，办公场景补贴类诈骗有着固定作案流程，诈骗分子借助技术手段突破办公信息安全防线，融合过往诈骗套路升级作案模式层层设套。整个作案链条隐蔽且精准，主要分为三个核心环节：

第一步，植入木马病毒，控制办公账号。

诈骗分子精准锁定政府机关、企业、学校等单位人员，通过邮箱、短信等载体，发送伪装成“会议通知”“内部违规人员名单”“企业报税新格式”等内容的压缩文件，并在文件内植入银狐类木马病毒。

由于这些文件主题贴合日常办公场景，受害者极易放松警惕，即便仅点击文件未成功打开，电脑也可能被植入病毒。随后，电脑会被诈骗分子远程监控，办公账号、通讯信息、企业人员架构、财务流程等各类信息都会被骗子获取。值得警惕的是，银狐类木马病毒隐蔽性极强，常规杀毒软件难以识别，一旦入侵很难及时发现并清除。

第二步，冒用熟人身份，扩散诈骗信息。

诈骗分子控制受害者的办公账号后，会借助该账号进一步渗透办公场景，扩散方式主要分为两种：一种是直接在原有工作群内发布虚假补贴通知，依托群内熟人关系网络降低他人警惕性；另一种是克隆受害者身份，通过相关办公软件邀请同事加入新建的虚假工作群，营造“官方通知”假象。

同时，诈骗分子还会精准把控时间节点，在假期前后、年底加班补贴申领、年初福利发放等关键时段集中作案，利用公众对“领补贴”的关注度实施诈骗。

王佳表示，诈骗分子发布的通知常标注“国家补贴”“劳动薪资补贴”“财政补贴”等字样，部分还附带“限时申报”“名额有限”“逾期作废”，甚至搭配“我已领到”的同事“留言”，制造紧迫感与可信度，诱导受害者尽快操作。

第三步，搭建钓鱼网页，套取信息盗刷。

诈骗分子在虚假补贴通知中附带钓鱼链接，链接跳转的网页会仿冒政务服务平台、企业福利申领平台等官方页面，排版、标识与正规平台高度一致，极具迷惑性。

页面还会逐步引导受害者填写信息，从姓名、身份证号、手机号等基础信息，到银行卡号、银行卡密码、短信验证码等敏感信息，部分页面还会要求填写银行卡账户余额，美其名曰“核实补贴发放额度”，实则是为了明确可盗刷金额，避免因金额超出账户余额导致盗刷失败。一旦受害者填写完整信息并提交，诈骗分子会立即盗刷账户内资金。

提醒

这些格式文件别随意点击

“犯罪分子冒充同事，又潜入工作群，尽管手段极具迷惑性，但是若想不中招，只需记住最重要的一点。”王佳表示，正规渠道发放补贴仅需提供银行卡号，最多要求开户行信息即可，绝不会要求填写银行卡密码、短信验证码，更不会索要银行卡账户余额。因此，市民只要遇到要求填写银行卡密码、短信验证码甚至账户余额的链接，无论页面多么正规、发送人多么熟悉，均为钓鱼链接，坚决不要填写相关信息。

若有市民不慎点击可疑链接、填写敏感信息，发现账户资金异常，需及时拨打110报警，第一时间联系银行冻结账户、申请资金止付，保存聊天记录、转账凭证、链接截图等证据，最大限度挽回损失。

在办公终端使用上，企业也需明确使用规范，禁止内部办公系统与公共社交软件长期并行，减少病毒渗透；员工下班及时关闭电脑，切断诈骗分子夜间远程操控路径，同时安装专业安全防护软件，定期更新病毒库，提升恶意软件拦截能力。

企业管理层面，需建立严格账号管理制度，定期开展安全排查，开启设备锁、二次验证等防护功能；员工对陌生文件，尤其“.exe、.zip、.rar、.bat”格式文件保持警惕，不随意点击下载。

王佳提醒，相关人群日常需强化安全意识，收到薪资补贴、财政补贴等通知，先向单位财务部门或官方机构核实，不点击非官方链接、不扫描陌生二维码、不安装未知软件。唯有筑牢安全防线、保持警惕心态，才能有效规避诈骗风险，守护好个人及单位财产安全。

本版文据北京日报客户端