金川集团股份有限公司科技与数字化部文件

金集科发〔2025〕23号

关于强化网络安全防范电信诈骗的通知

集团各单位、总部各部室：

近期，集团发生员工点击恶意链接导致的电信诈骗事件。经技术部门溯源分析，攻击者利用远程执行和短链接伪装等手段，诱使职工点击链接进入仿冒网站并在虚假页面输入账号密码等敏感信息，进而窃取个人财物，造成财产损失。为切实保障员工及集团财产安全，现就强化网络安全、防范电信诈骗工作通知如下：

一、提高思想认识，认清诈骗危害

网络电信诈骗犯罪隐蔽性强、作案手段多样，常见形式包括冒充公检法、虚假中奖、冒充领导要求转账、个人所得税退税等。此类诈骗极易导致个人财产损失甚至集团资金被骗。必须提高警

惕，克服麻痹思想，时刻保持清醒头脑，增强防范意识。

二、加强防范措施，筑牢安全防线

保护个人信息：不随意在不可信网站、APP 或社交平台上填写身份证号、银行卡号、验证码、支付密码等敏感信息；收到陌生邮件、链接、二维码，切勿随意点击或扫描，谨防钓鱼网站盗取信息。

加强终端防护：确保办公设备安装集团统一下发的金川终端防护软件，开启实时防护并定期进行全盘查杀。定期通过官方渠道对操作系统、浏览器及办公软件进行更新，修复安全漏洞。避免在公共场所使用免费 Wi-Fi 登录钉钉或处理敏感信息。

谨慎网络交易：网络购物、投资理财等务必选择正规平台，对“高收益、低风险”“先垫付资金后返利”“个人所得税退税”等诱惑性信息保持高度警惕，坚决拒绝参与网络刷单、虚假投资理财等活动。

核实转账信息：涉及资金转账时，无论是集团业务款项支付还是个人资金往来，必须通过电话、视频或当面等多种方式，与相关人员进行二次确认，核实对方身份及转账要求真实性，严禁仅凭短信、微信、钉钉等线上指令进行转账操作。

规范办公流程：严格执行集团资金审批制度，对大额资金支付、异常账户交易等情况，必须按照规定流程进行多级审核；不得将集团财务信息、客户资料等敏感数据随意外传，严防内部信息泄露导致诈骗风险。

三、强化应急处置，降低损失风险

及时止损：若发现疑似诈骗行为或已遭受诈骗，应立即停止一切操作，第一时间联系银行冻结相关账户，防止资金进一步损失。

迅速报案：保留聊天记录、通话录音、转账凭证等相关证据，及时向公安机关报案，并同步向单位管理部门和上级领导报告，以便协助开展后续调查处理工作。

信息通报：集团将及时汇总、通报最新诈骗案例及防范措施，各单位、各部门要积极组织员工学习，提高全员防范能力；若发生诈骗事件，相关单位及部门须配合做好信息收集和案件侦破工作，避免类似事件再次发生。

请各单位、各部门高度重视，压实网络安全主体责任，严格执行集团网络安全相关制度规定，强化全员网络安全意识，开展网络电信诈骗防范知识宣传教育活动，落实网络安全保障措施，确保人人知晓、人人防范，切实增强全员网络安全防护能力与电信诈骗防范水平。

金川集团股份有限公司

党委宣传部

金川集团股份有限公司

科技与数字化部

2025年6月19日

抄送:

金川集团股份有限公司科技与数字化部　　2025 年 6 月 19 日印发