致全市财务人员的一封信

各位企事业单位财务人员：

随着互联网技术飞速发展，电信网络新型违法犯罪也呈多发、高发态势。其中，部分企事业单位的财务人员特别是个体、私营企业财务人员因防范意识相对薄弱，财务管理规定执行不严格，成为诈骗分子的主要目标群体，针对财务人员的精准诈骗时有发生。该类诈骗一旦发生，造成的经济损失相当惊人，动辄几十万甚至达到千万。当前，结合“我为群众办实事”主题活动，茂名市反诈骗中心针对高发电信网络诈骗类型开展针对性滴灌宣传，切实守护群众钱袋子。因此，请你们务必认真阅读此信，增强识骗防骗能力，保护好个人和集体的财产安全。

一、诈骗分子的基本手法和套路

（一）盗取工作号。骗子混入财务人员的QQ群、微信群，通过发送木马软件盗窃群中人员的账号、邮箱、密码等重要信息。

（二）潜入工作群。盗取账号后诈骗分子会借机潜伏在单位、公司内部工作群里偷看聊天记录，了解、熟悉公司的人员组织架构和业务工作流程。

（三）精准实施诈骗。诈骗分子将自己的账号改为与公司老板或领导相同的头像和昵称，冒充公司老板、负责人向财务人员发送转账汇款指令。利用受害人因为敬畏而不敢跟领导核实信息实施诈骗。

二、此类案件真实案例

今年以来，我市发生诈骗财务人员的案件共5宗，诈骗金额共计386.6万元。我们编辑了两宗较为典型的案例供大家学习。

案例一：2021年3月17日9时许，茂名市某建材贸易公司会计陈某芳的QQ邮箱收到一份邮件，邮件是一个QQ昵称为其公司老板王某所发，会计陈某芳误认该QQ账号是老板的QQ，邮件内容是叫事主添加一个QQ群号入公司办公群，事主用自己的QQ号申请加入该群。通过后，该群组有6名成员，群内成员QQ昵称均为该公司员工名字，这群所谓的“同事”在群内谈论客户事宜，后其“老板”在群内发了一个银行凭证回执单文件，并让其打开跟进查询该笔款项是否到账，事主点击打开文件，显示是一个工商银行账号往公司账号汇款46万元，事主通过网银查询该笔款项并未到账，并将情况在该QQ群反馈给“老板”。“老

板”告知该款项因执行“T+1”汇款方式次日到账，随即“老板”称有一笔14.8万元急款需要汇款给客户，事主操作完成14.8万转款后向“老板”反馈；接着“老板”又让其将余款27.8万元转到另一建设银行账号，事主随即转款27.8万元。最后，事主电话询问老板王某，遂知被骗，共损失42.6万元。

案例二：2021年3月24日上午9时许，化州市某劳务公司财务陈某霞接到一个陌生电话，对方自称其是中国银行工作人员，负责公司对公账户年审业务，叫事主准备年审材料，并添加一个QQ名为“李经理”的人，“李经理”把事主的QQ拉到一个QQ群，群里有陈某霞公司的经理“苏某”，后“李经理”主动退群，苏某在QQ群上说因正在开会不方便接听电话，叫事主联系“周总”，并交代“周总”已于昨天和公司谈好合作项目，到时要将合同保证金转给“周总”公司，还发了一个电话号码给事主联系。事主联系“周总”后，“周总”提出立即打合同款。不一会，公司经理“苏某”就在群上发信息说已收到198万合同款，并给事主发了一张电子收款单截图，并叫事主立即从公司账户支付80万元到对方收款账户，事主立即汇款，后经询问经理苏某，发现被骗。

三、防范方法

（一）不轻易相信QQ、微信等即时通讯消息，要严格执行财务制度，转账汇款操作前，务必当面核实或电话联系单位、公司负责人，确认身份和转账汇款事由，对对方提供的陌生账号尤其是私人账号更应该提高警惕。

（二）定期对工作电脑和手机进行杀毒、不定期更换密码。尤其是财务人员使用的电脑应安装必要的防护杀毒软件，不要胡乱点击陌生的链接、网页。

（三）加强防骗知识的学习，提高防范意识，注重做好日常通信中的保密工作。在日常工作、生活联系中，应当避免使用邮件、QQ、微信等网络通信工具传送单位、公司重要资料信息，避免信息泄露。再次提醒大家时刻保持警惕之心，因为如果被骗，损失的不只是单位、公司的财产，更有可能构成玩忽职守罪，葬送自己的前程。

（四）一旦被骗，立即拨打110或反诈专线96110，早一点发现，早一步报警，就能多一点增加止付挽损的可能。

茂名市反诈骗中心

2021年4月9日