防范通讯网络诈骗友情提示

今年以来，经苏州工业园区反通信网络诈骗中心梳理发现，涉企涉商类诈骗损失数额巨大。经梳理，涉企类诈骗类型主要有：

一、QQ（微信）冒充老板诈骗财务

案例：2020年12月7日，苏州天灵路某工程有限公司的财务人员报警称，其在公司上班时QQ上收到一个“股东”发起的群聊，群内有“老板陈某某”。后“老板陈某某”在群内以合同保证金汇款为由，要求财务通过网银转账11万元至指定的银行账号。财务转账后发现被骗。

警方提示：

1、不轻信。不要轻信QQ（群）、微信（群）中涉及公司转账汇款的信息，对公司老板、负责人或其他人员通过网络社交工具要求转账汇款的，要认真识别，提高警惕。

2、不添加。不要轻易通过陌生QQ、微信的好友申请，加所谓的“公司群”。特别是涉及公司老板、负责人名字的QQ、微信，一定要电话或当面核实清楚。

3、慎转账。严格执行相关财务管理制度要求，针对QQ、微信要求的转账汇款，必须经过公司老板、负责人当面或电话核实确认！

4、速报案。一旦发现被骗，第一时间拨打110或96110电话报警。

二、邮箱诈骗

案例：2020年11月3日，工业园区某公司收到冒充供应商的邮件，讨论出货、技术、报关等事宜，骗子同时也冒充其公司的邮箱与真实供应商沟通，设备出货后，骗子要求其公司支付设备中间款项到新的指定账户。该公司财务人员便按其要求三次汇款，后发现被骗，共计损失约200万元。

警方提示：

1、公司企业开展海外业务，对方所用邮箱应添加至常用列表。与对方每次通信都应仔细核对邮箱地址，骗子通常会采用不易分辨的仿冒邮箱名称实施诈骗，如silence@163.com被骗子换成slience@163.com。2、对方提出需要变更收款账户时，务必通过电话、视频等多种方式与之确认。

3、专款设置延迟到帐。

4、定期更换、严格保护邮箱密码，经常查杀电脑病毒。

三、工商登记逾期诈骗

案例：2020年10月5日，高新区某商贸公司企业老板收到短信，谎称其公司、企业工商登记信息已过期（逾期）需要更新，要求点击短信链接，点击链接后跳转到“工商登记网页”，按要求填写银行账户、密码、验证码等信息，后发现其所填写的银行账户内现金被转走25万余元。

警方提示：

1、陌生短信内容不轻信、提供的链接不要点，银行账号密码勿轻易填写。

2、工商注册登记问题，如确有疑问应直接与当地市场监管部门官方客服电话联系询问。

3、银行验证码是资金安全的最后一道防线，不向任何陌生人、网站提供，每次使用时需看清验证码的用途。

四、冒充军警购物诈骗

案例：2020年11月9日，苏州某市装修公司李老板经人介绍，认识1名自称是当地消防大队王参谋的男子，在谈好关于消防训练基地的装修合同后，对方提出需采购一批钢丝床，需要李老板垫付资金。在高额装修项目的诱惑下，李老板向对方提供的钢丝床供应商垫付了13万余元资金，后发现被骗。

警方提示：

1、军警采购需要走报备、招标流程，不存在私下承揽和承诺发包工程，更不会电话或者QQ、微信洽谈项目。

2、勿向陌生商户先行垫资。

五、订餐诈骗

案例：2020年10月19日，吴中区某餐饮店接到要大量订餐的电话，在谈好具体配餐事宜后，对方要求店方提供支付宝收款条形码截图，店方未经考虑便发送了过去，后对方发来一个支付宝二维码并称可以付款了，店方按要求进行了扫

描，并直接点击确认，后发现对方发来的是收款二维码，账户内被扣款2000余元，发现被骗。

警方提示：

1、网络、电话订餐分清“收款码”与“付款码”，手机支付软件上的条形码、二维码和数字编码不要轻易告诉他人。

2、一旦发现受骗，应立即联系支付软件客服冻结账户，并在第一时间报警。

苏州工业园区反通信网络诈骗中心郑重提示：临近年底，上述涉企类电信网络诈骗预计将持续高发，请全市各企业、商户的老板、财务负责人等提高警惕，谨防诈骗。进一步严格企业财务规范，大额转账前要当面、电话核对；提升邮箱安全等级，核对关键信息；短信里的链接不能点，银行卡密码、验证码不能输；飞来好事要当心，网上交易需谨慎；陌生二维码不能扫，收款、付款要分清。