网络安全为人民
网络安全靠人民

2023年国家网络安全宣传周

2023年9月11日- 2023年9月17日

Private and Confidential

一、木马病毒“钓鱼”邮件

不明邮件不打开
警惕病毒和木马

犯罪分子将木马病毒包装成正常邮件中的链接或附件，恶意欺诈受害者。在受害者下载软件或是接收邮件时，将病毒木马植入手机或电脑，破坏或篡改用户数据和个人信息。

典型案例

2023年6月12日，四川省某公司财务人员王先生收到一条关于增值税发票的陌生电子邮件。王先生未察觉到异常，随之在电脑上点击邮件链接、并下载了一个压缩包，解压之后却发现只有一串英文字母，此时，王先生以为只是有人发送了“错误”的发票，便没有将此事放在心上。没想到数天后，王先生的“老板”在微信上发来消息，要求其向某公司账户进行大额资金转账，见对方头像、姓名与自己老板的一模一样，王先生并未对其身份产生怀疑，在没有通过电话进行核实的情况下，先后向对方提供的对公账户转账470余万元，事后才惊觉被骗。

防范指南

1.谨慎点击不明来源邮件的链接

2.使用杀毒软件，定期查杀木马

3.涉及转账业务、敏感信息时要多方求证

二、网络交友陷阱

网络交友别轻信
莫把骗局当爱情

在互联网上，不法分子打着交友名义，通过培养感情获取信任，以此骗取受害者金钱。

典型案例

2020年6月，高某与被害人刘先生通过在一起玩某大型网络枪战游戏而相识，在线上聊天互动过程中，高某编造了虚假身份信息，并隐瞒自己真实的婚姻状态，与刘先生建立“恋爱”关系。2020年7月至2021年6月间，高某以家人看病、同事随礼等虚假理由向刘先生索要钱款，刘先生先后向其转账共计人民币22万余元，高某将绝大部分钱款肆意挥霍于某网络平台上。2023年2月25日，高某被民警抓获归案，到案后向办案机关交代了自己的犯罪事实。

防范指南

1.不轻信通过网络认识的陌生人，对其身份及时核实

2.网络交友若涉及金钱转账、博彩赚钱等行为，应提高警惕、立刻拉黑

3.如果发现被骗，一定要保存好银行流水、对方账号等相关证据，及时报警求助

本页内容来源于市委网信办《2023年国家网络安全宣传周上海地区活动宣传手册》

三、智能网联车安全

车联技术智能化
安全防护需强化

智能网联车是车联网与智能技术的有机结合。随着智能网联车应用范围变广，也面临着远程攻击、恶意控制、隐私保护、数据安全等方面的安全问题。

典型案例

2022年5月6日，一位汽车博主发布了一条视频，该博主在行车记录仪的界面内可以看到同样拥有该品牌汽车的车主用户列表，点击任意一个用户，就能够加载其行车记录仪的画面，这引发了网友关于智能网联车用户隐私泄露的讨论。事后，该汽车品牌做出回应，称该功能属于车队出行、车路协同系统的组成部分，出厂时默认关闭，需用户确认才能开启。事发后第二天，该功能被该汽车品牌关闭。

防范指南

1.购买智能汽车的消费者要注意个人信息的录入与授权

2.涉及智能汽车的企业应该按相关法律保护客户隐私，提升车联网安全防护能力

四、“伪装”共享充电宝

共享充电需谨慎
警惕意识要常有

不法分子恶意投放植入木马病毒的共享充电宝，欺骗受害者用其充电，以盗取个人信息。

典型案例

2020年12月19日，广州市民陈女士租用了商场里不明品牌的共享充电宝，充电大概半个小时之后，就接到某陌生男子电话，对方竟清楚地知道她的银行卡还剩多少贷款没还。对方声称，如果陈女士不马上还贷款的话，会影响她明年的信用额度。该男子要求陈女士按照他的提示把五千元汇至其指定账户。陈女士转账以后，对方便把她拉黑了，陈女士随后马上报警。警方表示，此类“不明”充电宝里很可能安装了一些木马程序，会窃取手机信息。

防范指南

1.使用共享充电宝时，当手机出现是否“信任”提示时，请保持警惕

2.选择正规品牌的共享充电宝，不随意使用无品牌充电宝

3.安装手机安全防护软件，以防御恶意程序攻击

本页内容来源于市委网信办《2023年国家网络安全宣传周上海地区活动宣传手册》

五、虚假二维码陷阱

不扫不明二维码
天上不会掉馅饼

诈骗者通过中奖信息、资源分享等幌子吸引受害者扫描虚假的二维码，从而盗取其敏感数据或金钱。

典型案例

2023年7月，家住上海市民孙女士收到了一个陌生快递，快递盒内有一个手机支架，一份落款为“某宝联盟”的邀请函，和一张带有二维码的刮奖券。孙女士刮开奖券后，发现自己中了10元红包和当季水果。扫描刮奖券上的二维码后，孙女士被所谓的“客服”拉进一个聊天群，领取了红包及水果后，群主开始在群里派发刷单任务。孙女士第一次尝试了充值300元的任务，获利450元；等第二、三笔刷单任务做完，已经充值了7000多元，却迟迟没有收到返利，孙女士才意识到自己被骗。

防范指南

1.不贪图小便宜，不扫描来历不明的二维码

2.需扫描二维码付款时，要确认缴费渠道是否正规

3.警惕恶意转账投资、刷单等骗局

六、企业信息泄露

主体责任落实好
数据泄露隐患少

企业因业务需求，收集大量个人信息，但由于自身网络安全系统不完善或是为了获利故意造成的信息泄露。

典型案例

某大型国际信托有限公司项目经理，利用任职便利，采取“撞库”等方式获取某银行个人征信系统用户名和口令，通过其所属国际信托有限公司与该银行之间进行专线互联的终端机，数次非法登陆该用户个人征信系统，查询并下载保存他人征信报告共计100份。

防范指南

1.企业开展数据处理活动时应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取处置措施

2.企业发生数据安全事件时，应当按照规定及时告知用户并向有关主管部门报告

本页内容来源于市委网信办《2023年国家网络安全宣传周上海地区活动宣传手册》

七、网络暴力行为

网络暴力危害大
不评不转不参与

基于互联网，对受害者进行侮辱、诽谤等，并对当事人的隐私权、人身安全权及其正常生活造成威胁或不良影响的行为。

典型案例

2022年，郑同学拿着某高校的研究生录取通知书，希望给正在病床上的爷爷一个惊喜。她将这一幕拍成照片和视频发到社交平台上，照片里的她留着粉色中长发。谈及染头发的初衷，她说希望毕业照上的自己是明媚而鲜艳的，但这一帖子却引发了网友各种谣言，污蔑郑同学从事不正当职业、质疑她学历的真实性，对她进行网络暴力。令人心痛的是，郑同学被网络暴力逼至轻生。

防范指南

1.积极举报网络暴力行为，理智上网

2.不清楚事件原委时，不跟风评论转发，保持互相尊重

3.在遭遇网络暴力时，应保持情绪稳定，收集好证据后可向法院起诉

八、账号密码盗取

密码设置要复杂
不同账号有区分

骗子通过钓鱼网站、木马病毒、密码破解器等不同手段获取受害者密码，受害者密码越简单，风险越大。

典型案例

2020年5月至2021年11月，被告人张某在某社交平台购买了大量的个人邮箱账号及密码，利用这些个人信息，通过某游戏平台扫号器撞库盗取公民的某游戏平台游戏账号和密码，出售其盗取的某游戏平台账号、密码，从中获利。经鉴定，张某出售Steam账号113笔，共计收入人民币30829元。

防范指南

1.密码设置可以增加符号或大小写字母，密码越复杂，安全性越高

2.建议不同平台设置差别化的账号密码，增强账户安全性

本页内容来源于市委网信办《2023年国家网络安全宣传周上海地区活动宣传手册》

九、人工智能AI诈骗

防人工智能诈骗
保个人信息安全

犯罪分子利用人工智能技术合成受害者熟人或亲人的声音、图像或视频，以获取受害者信任，从而诈骗金钱。

典型案例

2023年4月20日中午，郭先生的好友突然通过微信视频联系他，自己的朋友在外地竞标，需要430万保证金，且需要公对公账户过账，想要借郭先生公司的账户走账。基于对好友的信任，以及通过视频聊天、随之轻信对方身份，在走账环节，郭先生在未核实430万是否到账之前，就将钱款转至对方提供的银行账户。之后，郭先生拨打好友电话，才知被骗。骗子通过AI智能换脸和拟声技术，佯装好友对他实施了诈骗。

防范指南

1.不过度公开人脸、指纹等个人生物信息

2.若涉及大额汇款等业务，务必多方面核验对方身份

3.提高安全防范意识，如受骗应及时报警

十、网络购物陷阱

网络购物要谨慎
陌生渠道不转账

骗子通过虚假购物链接、折扣活动、客服售后等不同形式的诈骗手段盗取受害者个人信息或是骗取其金钱。

典型案例

2023年7月2日，王女士的弟媳李女士在某网络平台购物后申请退货，很快便有自称是平台客服人员致电李女士，要求其缴纳保证金后方能退款。李女士因自己的手机软件设置受限，便借用王女士的手机根据“客服”要求下载某会议助手软件，并向“客服”提供王女士的银行卡号、身份证，发送银行卡验证码。很快，王女士的手机收到短信提醒：其在农业银行卡中的30余万元存款已从定期转为活期，看到短信的王女士大惊失色，意识到可能遭遇网购骗局，情急下报警求助。最终在警察帮助下冻结了银行卡。

防范指南

1.不在非官方的平台或链接中填写个人信息

2.警惕不通过官方购物平台、私下联系客户的客服人员

3.谨慎将银行卡、验证码等敏感信息提供给可疑客服人员

本页内容来源于市委网信办《2023年国家网络安全宣传周上海地区活动宣传手册》

Right By You