

提高数据安全意识 共同维护网络环境

南京西路街道积极开展 2020 年国家网络安全宣传周活动

□记者 姚沁艺 整理报道

大数据“杀熟”、APP 收集个人信息……在信息时代,你我都会遇到各类防不胜防的网络“陷阱”。那么,居民、白领应当如何辨别种种套路,保护个人信息安全呢?

近期,南京西路街道党工委结合 2020 年国家网络安全宣传周,联合上海报业集团技术运营中心、保障服务部、对外事务部,开展文化共享主题活动“福民讲坛”数据安全治理讲座,帮助大家提高数据安全意识。



提高防范意识 保护信息安全

“没有网络安全就没有国家安全,没有信息化就没有现代化。”9 月 2 日,由天津大学博士、迅达云科技创始人王斌主讲的“福民讲坛”数据安全治理讲座在威海路 755 号举行。王斌从大数据时代的新挑战、数据治理策略、数据安全防范难度、如何应对数据安全保护等方面,深入浅出地讲解群众非常关心的数据安全知识。

王斌博士列举了近年来发生的重大数据安全事故、数据滥用安全事件,通过案例分析讲解维护数据安全性的重要性和紧迫性。他认

为,可以从打通数据“孤岛”、权能分离、保护个人信息、树立“不危害”原则等维度进行数据治理。

数据资产识别梳理难、安全管控难、数据安全建设涉及多部门协作、相关法律未完善、安全意识薄弱……数据安全防不胜防,王斌博士深入剖析其中的难点症结,并提出解决思路。他认为,有必要建立数据安全治理组织架构和全生命周期风险管理机制,整体构建数据安全治理保障体系,分类分级推进数据安全建设。

王斌还建议,居民、白领应当养成良好的上网习惯,老年居民更要提高辨别意识,谨防电信诈骗、拒绝网络谣言。



“福民讲坛”数据安全治理讲座现场

识别金融骗局 提升防护技能

误上钓鱼网站,70 万元瞬间蒸发;网购遇上“客服退款”套路,被骗 130 万元……这些真实的案例,桩桩件件都在告诉我们:居民、白领除了要注意保护个人数据的安全,还应该提高网络金融安全知识。为此,南京西路街道在上海国际集团大厦党群服务

站开展了两场“网络安全 e 讲堂”网络安全主题巡讲活动,分别针对南西街道各个居民区的党员、群众以及辖区楼宇白领,详细解析金融诈骗手段,提高居民、白领网络金融安全意识。

同时,通过巡讲活动,进一步宣传贯彻《网络安全法》,普及网络安全知识,提升网络安全意识和防护技能,营造清朗的网络环境,共同维护国家网络安全。

网 / 络 / 安 / 全 / 小 / 知 / 识

强化风险意识 筑牢安全屏障

如何管好电子钱包?

问

我常常担心自己的电子钱包“支付宝”被盗号,有什么办法可以防止支付宝被盗号滥用?

现在使用支付宝支付、购物的人越来越多,可以说支付宝已经成为名符其实的电子钱包了,那么,我们该如何防止电子钱包里的钱被黑客或小偷偷走呢?其实只要做两方面的保护就可以了。

一方面是保证自己使用支付宝手机不被偷走、不遗失,或遗失了捡到的人也没法盗用支付宝,这方面我们可以通过设置人脸支付、声音锁等多因子认证方式来实现保护;另一方面,可以通过设置支付宝的“暗号”功能,防止支付宝账号不在陌生手机设备上登录以防止账户被盗。

问

我的支付宝每个月都会莫名其妙自动扣掉点钱,这是怎么回事?该怎么处理?

这其实是自动扣款服务在作祟,很多人无意间参与了自动扣款服务,自己却茫然不知。如在打车、外卖、游戏、学习等 APP 的付费过程中,可能一不小心就开启了这样的服务,这样的服务授权了这些 APP 可以自动从支付宝账户中小额扣款而不需要输入密码。假如你正碰到这样的困扰,可以在支付宝的“免密支付”菜单中,将这些不需要的“免密支付/自动扣款服务”项目一起关掉掉。

问

微信转账后被拉黑,如何迅速举报骗子找回血汗钱?

可以在小程序中搜索“腾讯 110”,及时进行举报。需要注意的是,微信转账虽然方便,但转账前一定要反复确认对方身份再进行操作,免得错转后带来不必要的麻烦甚至损失,一定不要随便给陌生人发红包和转账。为了财产安全一定要保护好我们的电子钱包。

如何注意社交安全?

问

有人高价求租我的微信号,我应该出租吗?

其实这是犯罪分子最新的套路。租用微信号往往为了实现两种目的。

第一种目的是用于网络黑产的恶意注册。由于近两年微信平台加大了对不法微信账号惩处,封停了一大批原来违规使用的微信号,这就使得不法分子必须找到新的可用账号,才能继续他们的违法违规活动。而所谓“租号”,就是黑产组织想出来的一种解决办法。

另一种目的就是用于诈骗。这些犯罪分子美其名曰是“短期租借”微信号,实际上就是变相盗号,通过哄骗用户自己交出账号、密码,再理所当然地将这些账号挪作他用。

由于普通用户的实名账号拥有支付功能,而且一般没有异常交易记录,因此很容易被不法团伙盯上,用来拆分、“洗白”他们手上的赃款,逃避监管部门和警方的监控、追踪。而一旦用户出租的微信被卷入“洗钱”风波,他们的账号也将不再“清白”。

总而言之,出租微信本质上是网络黑灰产业为了借普通用户身份实施违法犯罪、逃避监管追踪而布设的陷阱,不仅可能导致个人账户被盗、被封,还有极大的概率会危及他人乃至整个网络空间。

问

听说身份证可能会被别人绑定微信支付是怎么回事?

虽然绑定微信支付不等同于绑定银行卡,仅进行了身份认证的微信号,也只有 1000 元的微信支付额度。但是,一旦对方用我们身份信息认证的微信从事违法活动,后果将不堪设想。所以,我们需要定期查询自己名下的微信号,看看其中是否存在陌生的微信号。可以打开微信,依次点击“我”-“设置”-“通用”-“辅助功能”菜单中进行设置。

问

为什么总有陌生人加我微信?

由于微信已经成为人们日常生活中最主要的社交软件,因此,很多骗子就盯上了这一平台,通过添加陌生人成为好友,就成为成功诈骗的第一步,他们会想方设法地添加微信,模拟一个帅哥或美女的头像,或假冒熟人,一旦用户通过好友验证,他们就会开启诈骗套路。一般会有以下几种目的:

第一种是加一个好友,多一个看朋友圈的,里面全是微商,有枣没枣乱打一杆;第二种是酝酿一段时间后,骗人买东西,茶叶、酒、保健品等,价格高,却不能告他诈骗;第三种是炫耀他的赚钱方式,诱导人去买贵金属、原油期货、各种投资,都是看起来利润超高的,实际上连本金都拿不回来;第四种是假装搞暧昧、谈恋爱,然后骗人发红包、买包包的杀猪盘;第五种是潜伏在人们的朋友圈,分析当事人的照片和行为,再找机会对当事人进行恐吓、勒索。警惕添加你的陌生人,可以通过限制微信号的添加模式,来防止陌生人骚扰你。尽量只通过出示二维码来添加好友,以保证你的微信中都是经过你认可的熟人。

如何识别网络套路?

问

假冒 APP 是怎么回事?

随着智能手机的普及和移动互联网的发展,手机 APP 的功能越来越多,这让一些不法分子嗅到了“商机”,推出各种假冒手机 APP,“浑水摸鱼”获取不当利益。不法分子将假冒 APP 下载短链接置入短信中,诱使用户点击下载,之后通过收取工本费、解冻费、保证金、担保金等方式实施诈骗。

除了假冒 APP,还有高仿 APP 问题,一些高仿 APP 仿冒各种“官方 APP”,甚至还能处于一些手机应用商店的搜索第一位,高仿 APP 通过应用内的大量广告赚取广告费,甚至通过应用盗刷用户银行卡,泄露用户个人信息,利用用户个人信息贷款等。

虽然假冒 APP 诈骗不断衍生新花样,但是其核心依然是通过提前收费骗取钱财。对此,用户一定要记住:一是下载 APP 时一定要选择正规官方渠道;二是不通过各种推荐链接安装 APP,要安装,只通过正规 APP 商店搜索该 APP;三是安装手机安全软件,定期给手机杀毒。

问

有时候发现手机信号从 4G 变成 2G,没法上网了但还能收到短信是怎么回事?

假如你发现手机的信号从 4G 变成 2G,那么要警惕,你可能正在遭受到“短信嗅探”攻击。

“短信嗅探”攻击的原理是,犯罪分子利用“伪基站”,强制周围的手机从 4G 网络跌落到 2G 网络,在 2G 状态下,由于加密方式太过简单,不法分子就是利用漏洞截获 2G 网络中传送的短信。

因此,如果自己的手机信号原因不明地从 4G 降到 2G,特别是在深夜发生,有可能就是手机受到了攻击,请马上启动飞行模式。此外,睡觉前,可将手机关机或设置为飞行模式,防止被短信嗅探设备探测。如果早上起来,看到半夜收到奇怪的验证码短信,一定要想到可能是遇到短信嗅探攻击,迅速查询账户资金,有异常情况火速冻结银行卡,保留短信内容并报警。

(市网信办)

