网络安全为人民
网络安全靠人民

2024年国家网络安全宣传周

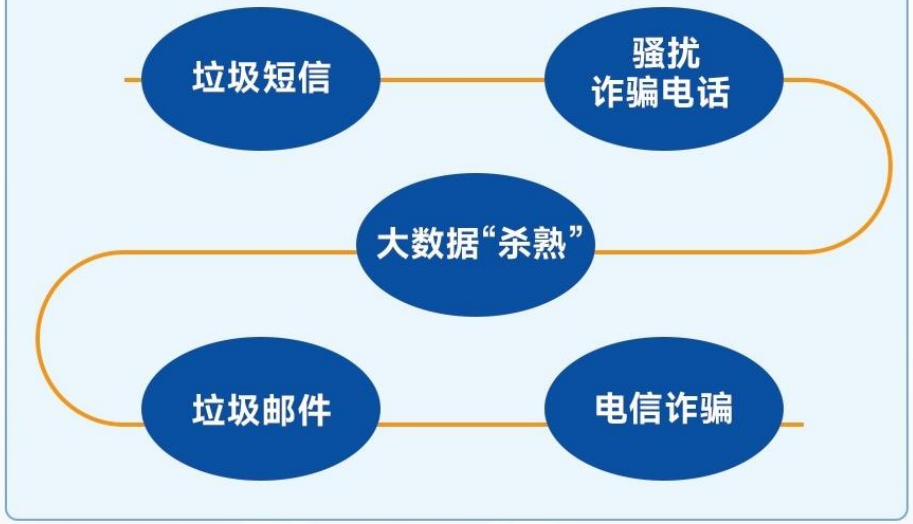
2024年9月9日- 2024年9月15日

个人信息保护

敏感个人信息

敏感个人信息指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

信息泄露危害



信息泄露途径

01 随意处置快递单、车票、购物小票等具有姓名、电话、住址、身份证号、银行卡卡号、消费记录等敏感信息。

02 在使用微信、群聊、贴吧、论坛等的过程中无意间泄露姓名、身份证号、职务、工作单位和住址等真实信息。

03 无意间点击不明来历的钓鱼邮件、链接，下载不明来历的软件从而使得电子设备被恶意攻击最终导致设备内个人信息泄露。

04 黑客等不法分子通过攻击存储有个人敏感信息的数据库，从而导致个人信息泄露。

本页内容来源于中国人民银行《2024年金融网络安全宣传手册》

个人信息保护

个人信息保护小知识

01 网上购物谨防钓鱼网站，尽量到正规的大型网站，仔细检查网站域名是否正确；不轻易接收和安装不明软件，不随便点击聊天中对方所发来的链接；不轻易提交用户名、密码等账户信息。

02 将公私邮箱分开，不轻易泄露邮箱地址；要仔细辨认发件人地址，不轻易点击陌生邮箱发来的邮件；不下载邮件中来历不明的附件；不点击邮件中可疑的或者与目的地址不匹配的链接。

03 妥善保管处置快递单、车票、购物小票等包含个人信息的单据。

04 不轻易添加陌生人的微信，不在微博、微信、论坛、朋友圈等地方轻易透露个人姓名、身份证号、家庭住址等个人信息。

05 不要随意扔弃或出售未经处理包含个人信息的手机、电脑等电子设备。

06 对个人重要信息加强防护，比如要在身份证复印件上标注“仅限办理某业务时使用”。

07 加强账户密码安全性。使用包含数字、字母和符号的复杂密码并定期进行更换。

08 电脑、手机等电子设备应安装安全软件，并定时进行安全扫描，避免因系统漏洞被不法分子利用，导致个人信息泄露。

09 避免在不安全的环境中使用个人信息。如不在公共场合的未加密WiFi下使用存储有个人敏感信息的电子设备，或输入银行账户等重要敏感信息。

本页内容来源于中国人民银行《2024年金融网络安全宣传手册》

电信诈骗案例剖析

冒充银行客服类诈骗

违法人员通过非法手段获取受害人信息，冒充银行客服人员，发送虚假的银行卡查询链接，要求被害人填写个人信息、银行卡卡号及密码并引诱被害人告知银行短信验证码，从而划走资金，导致被害人财产损失。

案 例

在江西打工的王某接到一个电话，显示的是个陌生的个人号码，对方自称是某银行客户经理，告知王某其信用良好，有资格提高其信用卡的透支额度。王某心想信用卡额度高点比较方便，银行打来一些营销电话也正常，还不用去网点，便应允了。按照对方要求，王某将自己在该银行办理的信用卡卡号、有效期、卡背面数字验证码等信息告诉了对方。随后，对方称银行正在审核，需要王某提供动态密码确认，王某信以为真，便提供给了对方，直到资金被划走方知被骗。

安全提示

01

接到陌生电话必须核实对方身份，对于自称工作人员的人，要通过官方渠道进行核实。

02

对于所谓“工作人员”发来的链接或二维码，不点击、不扫描，避免遭受钓鱼网站和木马病毒的侵害。不要轻易泄露自己的身份证号、银行卡号、短信验证码等重要信息。

03

“96110”是反电信网络诈骗专用号码，专门用于对群众的预警劝阻和防范宣传等工作。如遇到此号码打来的电话，务必接听。

本页内容来源于中国人民银行《2024年金融网络安全宣传手册》

电信诈骗案例剖析

“AI换脸”类诈骗

不法分子利用深度学习算法精准地识别视频中的人脸图像，并将人脸特征与目标人脸图像进行匹配、替换、融合，最后通过图像与音频合成的方式生成逼真度较高的虚假换脸视频冒充他人进行诈骗活动。

安全提示

01

对不明身份者发来的音视频通话保持警惕，特别是要求提供个人信息或金钱的请求，在转账前要通过电话或当面核实对方身份。

02

通过要求在脸部面前挥手、摁鼻子、摁脸或者询问只有对方知道的问题等方式验证真伪。

03

做好日常信息安全保护，加强对人脸、声纹、指纹等生物特征数据的安全防护。

案 例

李女士忽然收到了自己的老同学“贾某”微信好友申请，她便加了对方的微信，并在对方的要求下转入了QQ聊天。进入QQ聊天之后，这名“贾某”主动发来了视频通话邀请。视频通话虽然只有短短的16秒，但李女士确实看到了所谓老同学的样貌。李女士确信和自己交流的就是老同学“贾某”无疑。

随后这位老同学向李女士索要了银行卡号，接着便声称已经向李女士的账户转了196万元，同时还发来了一张“银行转账记录”截图。在收款未到账的情况下，这位所谓的老同学极力说服李女士先垫付资金。基于对老同学的信任，加上已经视频通话核实了身份，李女士将自己手里的40万元转入了对方提供的一个银行账号。随后李女士感觉到事有蹊跷并拨打了真正的老同学电话，这才发现被骗了，随即便报了警。

本页内容来源于中国人民银行《2024年金融网络安全宣传手册》

电信诈骗案例剖析

征信修复类诈骗

不法分子利用公众急于消除不良信用记录的迫切心理以及对“征信修复”概念的误解，以“征信修复、洗白、铲单、代理、咨询”等名义发布广告，借机收取高额代理费用，通常不良信息修改失败后不予以退款或直接跑路。

案 例

张某因疏忽发生贷款逾期，找银行咨询、沟通，寻求删除不良记录未果后，在网上找到一家所谓“征信修复”的机构，并按要求将1万元定金、一张自己实名办理的手机电话卡和一张银行卡交给这家机构，约定事成之后再付2万元。

一个月后，该机构告诉张某征信逾期已修复成功，要求张某付清全部余款。张某随即将事先承诺的余款转给该机构。当张某查询信用报告后，发现有关信息根本没有修复，于是再次联系该机构讨要说法，才发现对方已“失踪”。无奈之下，张某只能选择报警寻求帮助。

安全提示

01 “征信修复”是完全不存在的概念。所有规范征信业、征信机构的相关法规、文件、制度中，均未提及“征信修复”的概念。

02 金融消费者如果认为征信机构采集、保存、提供的信息存在错误、遗漏的，有权向人民银行征信中心或银行业金融机构提出异议，要求更正。

03 金融消费者应树立依法理性维权意识，直接向金融机构、监管部门公布的官方渠道反映诉求，进行征信异议申请或投诉，或通过法律诉讼等方式依法合理维权。

04 金融消费者应珍爱信用记录，提高信用意识，保持良好的信用记录。

本页内容来源于中国人民银行《2024年金融网络安全宣传手册》

电信诈骗案例剖析

虚假投资理财类诈骗

不法分子制作虚假的网络投资理财平台，通过多种渠道引诱受害人到平台进行投资，刚开始以少数收益吸引受害人投资，在受害人加大投入后通过平台后台控制涨跌，假装钱财全部亏空等手段实施诈骗。

案 例

李某伙同多人搭建“富途”“佰盛”等多个虚拟股票配资平台。平台方统一提供资金账户用于平台出入金，代理方虚构自己系正规券商旗下代理、提供高杠杆配资等事实，隐瞒资金实际不流入股市的真相，组织业务员通过发送虚假盈利图片、谎称有“内幕消息”等方式引诱被害人至平台充值，并扮演“荐股老师”“老师助理”指示、诱导被害人反向操作、频繁交易、购买波动股，造成被害人本金及手续费等损失。

安全提示

01 金融消费者应认清银行理财、基金、信托、期货等均不是存款，高收益意味着高风险，“保本高息”、“专家保证”等均是虚假网络投资理财类诈骗的常见套路，应提高警惕。

02 金融消费者进行投资理财时应首选经金融监管部门批准设立并颁发许可证的金融机构，不轻信通过网络论坛、微信群、QQ群等传播的“小道消息”以及无合法资质的机构或人员。

03 金融消费者要树立科学理性的投资理财观念。对陌生来电、邮件推销等非正规网络途径诱导投资行为保持警惕，不随意点击不明链接或扫描二维码，不轻易授权非官方APP使用协议；拒绝与陌生人共享实时位置、分享含有身份信息的照片。

本页内容来源于中国人民银行《2024年金融网络安全宣传手册》

防范电信诈骗小知识

防范电信诈骗小知识

01

学习反诈知识，增强反诈意识。牢记“三不一多”原则：未知链接不点击、陌生来电不轻信、个人信息不透露、转账汇款多核实。

02

保护好个人信息，不轻易向陌生人透露身份证号码、家庭住址等个人信息。在相关网站输入账号、手机号码等重要信息前要谨慎核实域名真实性。

03

投资理财、网络购物应选择正规渠道，避免在无资质或不合规的平台进行投资；网络购物时应选择官方平台进行交易，避免脱离平台进行交流。

04

主动下载“国家反诈中心APP“，利用APP的预警劝阻、快速举报、远程身份账号验证等功能增强防范能力。

05

遭遇诈骗后应第一时间报警并联系银行对相关银行账户进行冻结，防止损失进一步扩大，积极配合公安机关开展侦查破案和追缴被骗款等工作。

本页内容来源于中国人民银行《2024年金融网络安全宣传手册》

Right By You