



2024年度 网络安全宣传周

网络安全知识宣传手册



宁夏回族自治区人力资源和社会保障厅



个人信息保护

个人信息

是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

敏感个人信息是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。

泄露途径

非法披露



非法买卖



非故意泄露



攻击手机



攻击网站



信息泄露危害

- 1 垃圾短信源源不断；
- 2 骚扰、诈骗电话接二连三；
- 3 垃圾邮件铺天盖地；
- 4 大数据“杀熟”“人肉搜索”等恶意披露特定对象的个人信息事件。

防护建议

- 要优先选择尊重个人信息保护的产品、服务；
- 要审核App要求的权限，并谨慎授权；
- 要在身份证复印件上标注“仅限办理某业务时使用”；
- 要对重要信息进行加密保护；
- 要设置他人对自己所分享信息的访问权限。

防护建议

- 不要随意连接免费Wi-Fi热点；
- 不要随意点击进入短信、邮件中的网站，提交个人敏感信息，
- 不在网上晒车票、证件,以及含有孩子学校、家庭住址个人收入情况的照片。

数据安全



- 个人网购产生的交易记录



- 快递物流信息



- 网约车行车轨迹及服务信息



- 大型互联网平台处理的海量数据信息

- **数据**，是指任何以电子或者其他方式对信息的记录
- **数据处理**，包括数据的收集、存储、使用、加工、传输、提供、公开等。
- **数据安全**，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

数据安全威胁

数据窃取或泄露



黑客攻击、员工窃取、数据安全能力不足、内部违规操作、违规共享等。

数据毁损



违规篡改、破坏、丢失等。

数据非法利用



滥用大数据技术进行分析挖掘，任意共享或发布等。

数据非法出境



赴国外上市的公司，被要求提供审计细节、工作底稿等信息等。

危害重要数据安全的典型案例

- ▶ 2021年3月，李某等人私自在某重要军事基地周边架设气象观测设备，采集并向境外传送敏感气象数据。
- ▶ 2022年6月，西北工业大学遭受美国国家安全局网络攻击，持续窃取该校关键网络设备配置、网管数据、运维数据等核心技术数据。

数据分级

按照《中华人民共和国数据安全法》要求，根据数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，将数据分为一般数据、重要数据、核心数据共三个级别。

怎样加强数据安全保护

数据处理者



备份、加密、访问控制、数据安全应急处置机制、申报网络安全审查

互联网平台运营者



建立与数据相关的平台规则、隐私政策和算法策略披露制度，及时披露制定程序、裁决程序，保障平台规则、隐私政策、算法公平公正

重要数据的处理者



- 明确数据安全负责人，成立数据安全管理机构；
- 制定数据安全培训计划，组织开展全员数据安全教育培训；
- 优先采购安全可信的网络产品和服务、每年开展一次数据安全评估。

电信网络诈骗

电信网络诈骗，是指以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为。

典型骗术

杀猪盘诈骗 甜言蜜语暖心房，卷钱跑路两茫茫

指通过婚恋平台、社交软件等方式寻找潜在受害者，通过聊天发展感情取得信任，然后将受害者引入博彩、理财等诈骗平台进行充值，骗取受害者钱财的骗局。

杀猪盘诈骗 投资理财循正路，刷单兼职是骗术

指刷单诈骗、兼职诈骗，骗子通过发高薪兼职信息吸引受害者参与，再通过套路不断鼓动受害者投钱代刷，最终骗取所有投资钱财的骗术。

刷单返利诈骗

是指诈骗分子通过网络发布虚假兼职信息，具体内容一般为短视频平台点赞关注、手工活代做、电商平台刷人气销量等，之后通过小额返利获取受害人的信任，引诱其做大额充值返利的任务，并承诺本金和返佣一并给予，受害人难以辨识，往往身受其害。

虚假贷款诈骗

是指诈骗分子通过网络平台、电话、短信等方式发布办理贷款的广告信息，后冒充银行、贷款公司工作人员联系受害人，诱使其下载虚假贷款APP，待受害人在APP内贷完款提现时，以解冻金、保证金、验证还款能力等理由进行钱财诈骗。

如何防止电信诈骗

- 1 即使遇到能够说出自己姓名、住址等个人相关信息的电话、短信也不要轻信，需要通过其他渠道核实；
- 2 特别是冒充公检法进行调查、冒充亲朋好友进行转账、冒充淘宝、商家客服进行退款，此类电话基本为诈骗；
- 3 陌生短信、邮件、社交工具中发来的链接不要輕易点击，陌生应用不要随便安装；
- 4 不輕易将个人信息留在不熟悉或不正规的机构、网站中，网银账号、普通社交账号密码要区分，密码定期修改，谨防信息泄露。

防范电信诈骗“三不一要”

- 1 **不轻信**。不要轻信来历不明的电话和手机短信，不管不法分子使用什么甜言蜜语、花言巧语，都不要輕易相信，要及时挂掉电话，不回复手机短信，不给不法分子进一步布设圈套的机会。
- 2 **不透露**。巩固自己的心理防线，不要因贪小利而受不法分子或违法短信的诱惑。无论什么情况，都不向对方透露自己及家人的身份信息、存款、银行卡等情况。如有疑问，可拨打110求助咨询，或向亲戚、朋友、同事核实。
- 3 **不转账**。学习了解银行卡常识，保证自己银行卡内资金安全，决不向陌生人汇款、转账；公司财务人员和经常有资金往来的人群等，在汇款、转账前，要再三核实对方的账户，不要让不法分子得逞。
- 4 **要及时报案**。万一上当受骗或听到亲戚朋友被骗，请立即向公安机关报案，可直接拨打110，并提供骗子的账号和联系电话等详细情况，以使公安机关开展侦查破案。

AI诈骗

随着AI换脸技术的迅速发展该技术已经展现出广泛的应用潜力，不过AI技术是把“双刃剑”，在给人们生活提供便利的同时，也给不法分子留下了可乘之机。

案例回顾1

某科技公司法人代表张先生10分钟内被骗430万元：案发时，他的好友通过微信视频联系他，称有朋友在外地竞标，需要430万元保证金，想借用张先生公司的账户走账。基于对好友的信任，加上已经视频聊天“核对了身份”，张先生进行了转账。事后，张先生拨打好友电话才得知被骗。

案例回顾2

小王的“大学同学”通过QQ跟她借钱。为了打消小王的顾虑，对方还打来一段四五秒的视频电话，小王见视频中的人确实是“同学”本人，便放心地给对方转了3000元。然而，没过多久“同学”又提出了借钱的请求，就在小王准备第二次转账时，她察觉到了异常，便给对方打了电话，这才发现同学的账号被盗，和自己借钱的并不是同学，马上报警。

AI诈骗是如何实施的？

- 1、骗子通过各种渠道收集受害人及其熟人的信息，如姓名、电话、社交账号、照片、视频等。
- 2、骗子利用AI换脸技术，将自己或他人的面部替换成受害人熟人的面部，并利用AI拟声技术，将自己或他人的声音转变成受害人熟人的声音。
- 3、骗子通过社交软件或电话联系受害人，并以视频方式进行信息确认，让受害人放松警惕。
- 4、骗子以各种理由诱导受害人转账汇款，如借钱、投资、紧急救助等，并催促受害人尽快操作。
- 5、骗子在收到钱款后立即消失，切断与受害人的联系。

AI诈骗常用手法--通过AI技术筛选受骗人群

筛选受骗人群 → 视频通话 → 个人信息

骗子不是漫无目的地全面撒网，而是别有用心地锁定特定对象。他们会根据所要实施的骗术，**通过AI技术对人群进行筛选**，从而选出目标对象。



AI诈骗常用手法--换脸

AI技术换脸 → 视频通话 → 个人信息

骗子首先分析公众发布在网上的各类信息，**用AI技术换脸**，可以伪装成任何人，再通过视频方式进行信息确认，真是防不胜防。

如何防范AI诈骗

看眼睛 → 看嘴巴 → 听声音

多数假脸是使用睁眼照片合成，假脸极少甚至不会眨眼，**缺少眨眼是判断一个视频真假的好方法。**

辨识“深度伪造”换脸视频的方法还包括**语音和嘴唇运动不同步、情绪不符合、模糊的痕迹、画面停顿或变色。**



防范诈骗并不难 不听忽悠不转钱



防范AI诈骗多重验证，确认身份

多次确认 → 转银行账户 → 24小时到账

在涉及到转账交易等行为时，通过电话等形式询问具体信息，**多重验证确认对方是否为本人**。最好向对方的银行账户转账，避免通过微信等社交软件转账，**将转账到账时间设定为“24小时到账”，以预留处理时间。**

防范AI诈骗——保护信息，避免诱惑

保护信息 → 警惕中奖 → 警惕交友

加强个人信息保护意识，谨防各种信息泄露，不管是在互联网上还是社交软件上，**尽量避免过多地暴露自己的信息。**

对于不明平台发来的广告、中奖、交友等链接提高警惕，**不随意填写个人信息，以免被骗子“精准围猎”**

防范AI诈骗——相互提示，共同预防

多提醒 → 关注老年人 → 提高意识

要多多提醒、告诫身边的亲人、朋友提高安全意识和应对高科技诈骗的能力，共同预防受骗。**提醒老年人在接到电话、短信时，要放下电话，再次拨打家人电话确认，不要贸然转账。**

防范AI诈骗—拒绝诱惑，提高警惕

拒绝诱惑 → 不占便宜 → 提高警惕

要学会拒绝诱惑，提高警惕。避免占便宜心理，警惕陌生人无端“献殷勤”。





网络安全为人民

网络安全靠人民