国家网络安全宣传周
China Cybersecurity Week

北京市网络安全公益宣传

2026
北京市国家网络安全宣传周
主题巡展

网络安全为人民
网络安全靠人民

国家网络安全宣传周
China Cybersecurity Week

一个密码走天下？
一泄露，全失守！



多地用户因账号密码复用，
导致社交、购物、支付平台接连被盗

真实案例

张先生习惯在多个平台使用同一套账号密码。一次在某网站注册后，账号信息被泄露，不法分子利用相同密码尝试登录他的社交、购物和支付账户。 最终，张先生的多个账号被他人冒用，部分个人信息泄露，还险些遭遇虚假购物诈骗。

风险拆解

- 多个平台使用同一密码，等于“一处失守，处处失守”。
- 一旦某平台数据泄露，不法分子会尝试登录其他网站。
- 密码过于简单、长期不更换，也会增加被破解风险。

防范提示

1. 不同平台使用不同密码。
2. 重要账号开启多因素身份验证。
3. 避免使用生日、手机号、姓名等容易猜测的信息。
4. 定期更换关键账号密码。
5. 不要在非官方网站输入账号密码。



警示口诀

一钥难守千重关，万密方护一寸安。



国家网络安全宣传周
China Cybersecurity Week

高返利、零风险？天上不会掉馅饼！



受害人被“稳赚投资”诱导，短时间损失数十万元

真实案例

李女士在社交平台看到“内部投资渠道、日收益翻倍、保本稳赚”的广告后，添加了所谓的“投资顾问”。对方先让她小额获利，取得信任后，诱导她加大投入。李女士陆续转账数十万元后，发现平台无法提现，“投资顾问”也销声匿迹。

风险拆解



- 先以“高收益、低风险”吸引目标人群。
- 前期小额返利获取信任。
- 后期诱导大额投入，最终卷款跑路。
- 虚假平台、虚假行情、虚假客服共同制造“真实投资”假象。

防范提示

1.凡是承诺**“稳赚不赔”“高收益零风险”**的，都要高度警惕。
2.不要点击陌生投资链接或下载非官方投资平台。
3.不向个人账户转账投资款。
4.投资前核实平台资质和监管信息。
5.遇到“加急充值、限额提现”等话术，立即停止操作。

警示口诀　虚利浮名皆是幻，静心三思避万难。

国家网络安全宣传周
China Cybersecurity Week

免费 WiFi 随便连？你的数据可能正在被窃取！

用户连接商场免费 WiFi 后，账号密码被窃取

真实案例

王女士在商场购物时，看到一个无密码免费WiFi，名称显示为“商场公共WiFi”。她连接后登录了购物账户和支付账户。不久后，她收到异地登录提醒，部分账户信息疑似泄露。经查，该WiFi实为不法分子搭建的钓鱼网络。

风险拆解



- 陌生公共WiFi可能被命名为“免费WiFi”“酒店WiFi”“商场 WiFi”。
- 攻击者可在同一网络中监听流量。
- 用户登录账号、输入密码、访问涉密信息时，容易被截获。
- 没有加密、没有认证的公共网络风险更高。

防范提示



1. 不随意连接无密码公共 WiFi。
2. 不在公共 WiFi 下登录支付、网银、办公系统。
3. 不使用公共 WiFi 传输敏感信息。
4. 优先使用手机流量或官方认证网络。
5. 发现网络名称异常、信号来源不明，立即断开。



警示口诀

野网无凭藏险诈，谨连慎护守芳华。

国家网络安全宣传周
China Cybersecurity Week

“低价神装私下卖？钱付了，装备却没到！”



游戏玩家被诱导私下交易，损失数千元

真实案例

小赵在游戏中看到有人售卖“绝版装备、低价皮肤、高价回收账号”的信息。对方声称不走平台，直接私下转账更便宜。小赵转账后，对方以“账号冻结”“需要验证金”“系统升级”为由继续索要费用。小赵多次付款后，不仅没有收到装备，还被对方拉黑。

风险拆解

- 不法分子用“低价道具、高价回收、绝版皮肤”吸引玩家。
- 诱导脱离官方平台，进行私下转账。
- 以“验证金、解冻费、手续费”等名义继续骗钱。
- 一旦转账，钱财很难追回。



防范提示

1.网游交易只走官方正规渠道。
2.不相信**“低价绝版装备”“高价回收账号”**。
3.不向陌生个人账户转账。
4.不点击游戏内陌生人发来的链接。
5.遇到**“先转账后发货”**的情况，一律拒绝。

警示口诀　网游虚景藏奸计，私转贪利必吃亏。

国家网络安全宣传周 China Cybersecurity Week

一键同意所有权限？你的隐私可能正在被泄露！



用户随意授予 APP 权限，导致位置信息和通讯录泄露

真实案例

陈先生下载了一款便民服务APP，打开后连续点击“一键同意”。该APP申请了位置、通讯录、相机、麦克风等多项权限。不久后，他发现自己常去地点、家人联系方式和日常行程信息被异常读取，还收到针对性营销短信和陌生来电。

风险拆解

- “一键同意”可能包含定位、通讯录、相册、麦克风等敏感权限。
- 权限一旦被滥用，可能导致行踪、关系圈、生活习惯泄露。
- 越权权限还可能被用于精准诈骗、骚扰和数据窃取。

防范提示

1. 不盲目点击“一键同意”。
2. 只授予APP必要权限。
3. 关闭“始终允许”定位等敏感权限。
4. 定期检查手机应用权限设置。



警示口诀

隐私条款藏隐患，一键授权易失安。



国家网络安全宣传周
China Cybersecurity Week

“免费工具、破解软件？安装之后，手机电脑可能失守！”



用户下载破解版工具，导致设备被植入木马

真实案例

刘先生在网上看到一款“免费办公助手、破解版不限功能”的软件介绍。他下载安装后，软件确实打开了，但电脑开始出现弹窗广告、运行变慢。随后，他发现浏览器保存的账号密码、办公文档和桌面文件被异常读取，设备疑似被植入木马程序。

风险拆解

- 钓鱼软件常伪装成工具、游戏、办公软件、视频剪辑软件。
- 破解版、绿色版、免费完整版中可能暗藏木马。
- 安装后可能窃取账号、密码、文件和聊天记录。
- 部分软件还会私自下载恶意程序、弹出广告、篡改设置。



防范提示

1.不下载非官方来源软件。
2.不安装破解版、绿色版、来路不明的工具。
3.不打开陌生网站的下载弹窗。
4.安装软件前查看权限和用户评价。
5.及时更新系统和安全软件。

警示口诀 软件下载要正规，“破解”“盗版”不理会。

国家网络安全宣传周
China Cybersecurity Week

视频里是熟人？声音像本人？AI 换脸也能造假！



不法分子利用AI换脸技术实施精准诈骗

真实案例

周女士接到一个视频通话，画面中是亲友的脸，声音也非常像本人。对方称遇到紧急情况，需要立即借钱周转。周女士正准备转账时，想起最近看到的AI换脸诈骗提醒，于是通过另一个号码再次确认。最终发现，刚才的视频和声音都是AI伪造的。

风险拆解

- AI可以模拟人脸、表情、声音和口型。
- 骗子会利用亲友、同事、领导的影像素材制作虚假视频。
- 通常以“紧急情况”“不便多说”“快转账”施压。

防范提示

1. 遇到紧急转账要求，不能仅凭视频、声音确认身份，必须二次核实。
2. 大额转账前要通过电话、文字或其他共同联系人再次确认。
3. 遇到“紧急、保密、快处理”等话术更要提高警惕。
4. 涉及资金、机密、权限时，务必多渠道确认。





警示口诀

AI幻形千万变・本心审慎破万难。

国家网络安全宣传周
China Cybersecurity Week

“AI 助手真方便？权限、插件、公网部署不能乱！”



企业使用 AI 助手配置不当，导致内部数据泄露

真实案例

某企业员工使用 AI 智能体辅助处理工作，为了提高效率，给 AI 授予了较高权限，并安装了多个第三方插件。由于配置不规范，AI 智能体被恶意指令诱导，开始读取本地文件、聊天记录和内部文档，并将部分敏感数据上传到外部接口，造成信息泄露。

风险拆解

- AI 智能体如果权限过高，可能读取、修改、上传敏感数据。
- 第三方插件可能存在恶意代码或安全漏洞。
- 部署在公网但缺乏保护，容易被攻击者访问和控制。



防范提示

1.不随意授予 AI 最高系统权限。
2.不安装非官方来源的 AI 插件。
3.不将 AI 服务随意暴露在公网。
4.处理涉密信息时谨慎使用自动化 AI。

警示口诀　科学用 AI，安全不踩坑。

国家网络安全宣传周
China Cybersecurity Week

警惕“饭圈”追星诈骗

理性追星，守住个人钱袋子

真实案例

某未成年学生热衷追星，在某平台粉丝群添加冒充偶像的账号。不法分子伪装明星本人，以线上投票打榜为由，发送所谓“投票二维码”，诱导该学生使用家长微信扫码、输入投票编码，实际完成转账，累计被骗10099元。待钱财转出后对方账号失联，受害人才发觉遭遇诈骗。

风险拆解

1. 身份伪装：不法分子盗用明星照片，伪造私人交友账号，搭建虚假粉丝福利群。
2. 诱饵引诱：发布充值返利、内部演唱会门票、助力偶像投票等虚假福利信息。
3. 套路欺骗：编造投票编码，将收款二维码伪装成投票工具，诱导扫码转账。
4. 受害群体：主要瞄准辨别能力较弱的未成年人，利用追星心理实施诈骗，造成家庭财产损失。



防范提示

1. 认清常识：明星不会通过私人渠道联系粉丝，更不会索要钱财、要求扫码转账。
2. 理性消费：不在粉丝私域群内购买高价周边、所谓内部演出门票，拒绝充值返利诱惑。
3. 账户看护：家长保管好支付密码、验证码，不让孩子随意使用家长支付账号。
4. 遇险处置：一旦被骗，留存聊天、转账记录，第一时间报警求助。



警示口诀

追星消费要理性，“打榜”“抢票”莫轻信。



国家网络安全宣传周
China Cybersecurity Week

坚决抵制网络谣言



无据信息不扩散，守法上网守底线



真实案例

网民张某在短视频平台看到一则本地突发“爆料”，声称辖区内出现公共安全事故，配有拼接画面和夸张文案。张某未核实信息真伪，认为内容能够博人眼球，随即转发至多个微信群、朋友圈。该不实信息被大量网民跟风转发，快速引发区域性恐慌，严重扰乱社会公共秩序。最终公安机关溯源查处，对造谣源头账号依法处罚，同时对违规转发扩散、造成不良影响的张某作出行政处罚。



风险拆解

1. 虚假爆料引流：不法账号拼接素材、杜撰突发内幕、民生爆料，以“独家消息”“内部实锤”为噱头博取流量。
2. 盲目跟风转发：网民缺乏甄别意识，轻信看似真实的爆料内容，未经核实随意扩散传播谣言。
3. 引发社会恐慌：不实灾情、警情、民生谣言快速扩散，扰乱公众认知，破坏正常社会秩序。
4. 承担法律责任：造谣、传谣均属于违法行为，扩散范围广、造成影响大的，将依法追究行政乃至刑事责任。

防范提示

1. 面对网络爆料、突发消息，坚持先核实、后转发，无官方通报的信息一律不轻信、不传播。
2. 警惕“独家内幕”“未公开实锤”等博眼球内容，此类无权威来源信息大多为杜撰谣言。
3. 自觉抵制网络谣言，不跟风评论、不批量转发、不炒作不实话题，主动劝阻他人传谣行为。
4. 发现网络虚假爆料、造谣信息，及时通过官方平台举报，共同维护清朗网络环境。



警示口诀　网络谣言要明辨，“实锤”“爆料”不轻传。

国家网络安全宣传周 China Cybersecurity Week

警惕网络兼职诈骗

垫资返利全套路，高薪兼职皆陷阱

真实案例

在校学生小李在网络上看到“居家刷单、日结高佣、轻松赚钱”的兼职广告，主动添加客服好友。对方告知只需帮忙刷单冲销量，即可赚取高额抽佣。起初几单小额任务均成功返利。后续对方下发联单、大额任务，以“任务未完成”“资金冻结”为由，要求小李不断垫付资金。小李累计垫付四万余元后，依旧无法提现，对方直接拉黑失联。

风险拆解

1. 低门槛引流：以居家兼职、无需技术、日结高薪为噱头，重点诱骗学生、无业网民。
2. 小额返利套路：前期小额刷单快速返现，降低警惕，骗取受害人信任。
3. 连环套单收割：以联单、超时、系统冻结为借口，强制要求持续垫资刷单。
4. 榨干资金跑路：受害人投入大额资金后，拒绝提现、失联拉黑，造成财产损失。



防范提示

1. 国家明令禁止网络刷单行为，所有刷单兼职均为违规骗局，不存在正规刷单。
2. 任何兼职要求先垫资、交押金、充值解冻的，一律是诈骗。
3. 不轻信高薪轻松兼职广告，不添加陌生兼职客服，不点击陌生链接。
4. 遭遇刷单骗局，立即停止转账，保留聊天、订单、转账记录，及时报警。





警示口诀

网络兼职要注意，“刷单”“抽佣”不实际。

国家网络安全宣传周
China Cybersecurity Week

警惕扫码点餐隐私泄露



隐私授权不轻给，严防泄露保权益

真实案例

市民张某在外就餐时，商家要求必须扫码关注公众号、授权手机号、允许获取位置信息，才能解锁点餐功能。张某被迫授权个人信息后，后续长期收到大量商家营销短信、垃圾广告。经查，该餐饮店违规收集、外泄顾客手机号等个人信息，批量流转给营销黑产，数百名顾客隐私遭到泄露，频繁遭遇骚扰推销。

风险拆解

1. 强制授权牟利：部分商家借点餐便利，强制要求关注公众号、绑定手机号、授权隐私权限，违规收集非必要个人信息。
2. 信息泄露倒卖：违规采集的顾客手机号、消费轨迹、就餐记录被打包售卖，流入黑灰产渠道。
3. 高频骚扰扰民：隐私泄露后，持续接收垃圾短信、营销电话、商业广告，严重影响日常生活。
4. 衍生诈骗风险：消费信息、出行轨迹被掌握，易被不法分子精准锁定，诱发诈骗风险。



防范提示

1. 扫码点餐只需基础点餐权限，坚决拒绝强制关注、强制授权手机号、位置信息等多余要求。
2. 遇到商家强制授权隐私方可点餐的行为，可当场拒绝，并向市场监管、网信部门投诉举报。
3. 点餐结束后及时取消关注、关闭授权，关闭小程序自动获取信息权限。
4. 不随意允许陌生商户获取个人隐私，杜绝非必要个人信息采集，守住隐私安全底线。



警示口诀　扫码点餐要便利，“关注”“强制”不合理。

国家网络安全宣传周
China Cybersecurity Week

警惕冒充公检法诈骗

调查执法有规范，线上办案是诈骗

真实案例

市民刘某接到陌生来电，对方自称公安民警，准确报出刘某身份证、住址等信息，谎称其名下账户涉嫌洗钱涉案，需要配合线上核查办案。对方发送虚假通缉、涉案文书，以资金核查、账户洗白为由，诱导刘某将名下全部存款转入所谓“安全核查账户”。刘某心生恐惧、未敢核实，先后转账32万元，事后联系当地派出所，才得知遭遇冒充公检法精准诈骗。

风险拆解

1.精准恐吓施压：不法分子掌握受害人隐私信息，冒充公检法人员，捏造洗钱、涉案、违法等罪名制造恐慌。

2. 伪造官方材料：发送虚假警官证、立案文书、通缉令，伪造办案流程，提升骗局可信度。

3. 隔离外界求证：要求全程保密、不得告知家人朋友，切断受害人求助核实渠道。

4. 诱导资金转移：以账户核查、验资洗白为由，诱导转账至虚假安全账户，完成全额诈骗。



防范提示

1.公检法机关绝不会电话办案、线上核查，更不会要求群众转账验资、资金洗白。

2. 接到涉案核查类恐吓电话，保持冷静，不恐慌、不转账，第一时间报警求助。

3. 不轻信陌生来电、不点开陌生涉案文书链接，遇到涉法涉诉问题通过官方渠道咨询。



警示口诀

法治常识要加强,“涉案”“核查”不慌张。



国家网络安全宣传周
China Cybersecurity Week

守护智能家居安全



智能家居可能隐藏个人信息泄露风险

真实案例

市民李某家中安装智能摄像头、智能门锁等智能家居设备，长期使用初始默认密码。不法分子通过扫描网络漏洞，破解设备后台权限，非法远程入侵智能摄像头，持续偷窥家中生活画面、录制视频，窃取家庭隐私。受害人长期不知情，直至设备出现异常弹窗、频繁离线才察觉，个人私密影像已被非法留存，隐私遭到严重泄露。



风险拆解

1. 弱密码漏洞：智能设备沿用出厂默认密码、简单密码，极易被黑客批量破解、暴力入侵。
2. 远程非法监控：攻击者私自远程操控摄像头、智能音箱，偷拍、偷录居家画面与对话。
3. 隐私数据外泄：家庭生活影像、居住环境、家人作息等私密信息被窃取、泄露甚至非法传播。
4. 衍生安全隐患：摸清居家作息后，极易诱发入室盗窃、精准骚扰等线下安全风险。



防范提示

1. 新购智能家居设备第一时间修改初始密码，设置复杂独立密码，杜绝通用弱密码。
2. 关闭设备陌生远程访问权限，定期查看登录记录，及时下线非本人登录设备。
3. 卧室、浴室等私密区域不安装智能监控设备，避免隐私暴露。
4. 定期更新设备固件系统，修补安全漏洞，闲置设备及时断电、关闭联网功能。



警示口诀　智能家居要警惕，“远程”“监控”不保密。