

【2024 年国家网络安全宣传周】网络安全为人民， 网络安全靠人民

2024 年是习近平总书记提出网络强国战略目标 10 周年，今年国家网络安全宣传周活动将于 9 月 9 日-9 月 15 日举办，学习网络安全重要法律法规，有效提升网络安全意识和防护技能。今年的国家网络安全宣传周主题是“网络安全为人民，网络安全靠人民”，下面我们来看看国家网络安全教育的相关知识吧！

一、网络安全重要法律法规

（1）《中华人民共和国网络安全法》

《中华人民共和国网络安全法》由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日表决通过，自 2017 年 6 月 1 日起施行。该法是中国第一部全面规范网络空间安全管理方面问题的基础性法律，是中国网络空间法治的重要里程碑。

➤ 关于网络安全

网络安全是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏、非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（2）《中华人民共和国数据安全法》

《中华人民共和国数据安全法》由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于 2021 年 6 月 10 日表决通过，自 2021 年 9 月 1 日起施行。该法作为我国关于数据安全的首部法律，是数据领域的基础性法律，也是国家安全领域的一部重要法律，标志我国在数据安全领域有法可依，为各行业数据安全提供监管依据。

（3）《中华人民共和国个人信息保护法》

《中华人民共和国个人信息保护法》由中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议于 2021 年 8 月 20 日表决通过，自 2021 年 11 月 1 日起施行。在有关法律的基础上，该法进一步细化、完善个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作体制机制。

（4）《关键信息基础设施安全保护条例》

《关键信息基础设施安全保护条例》由国务院于 2021 年 8 月 17 日正式发布，自 2021 年 9 月 1 日起施行。该条例是在《网络安全法》框架下全面规范关键信息基础设施安全保护的基础性法规，是加强网络安全领域立法、完善网络安全保护法律法规体系的重要举措，是依法治理关键信息基础设施的纲领性文件之一，是化解关键信息基础设施安全风险的法律法规重器和重要里程碑。

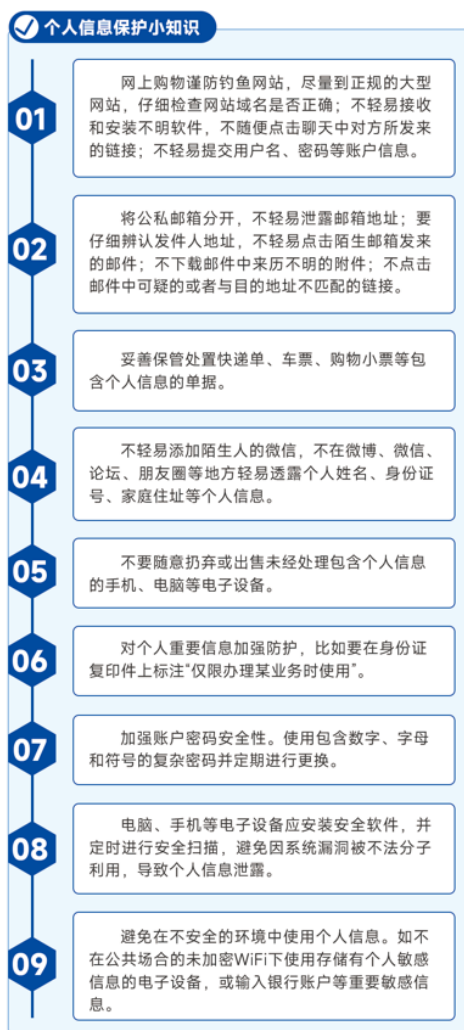
二、 个人信息保护

（1）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。

（2）信息泄露途径

- 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；
- 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；
- 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；
- 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。



三、电信诈骗案例剖析

（1）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。

（2）“AI 换脸”类诈骗

不法分子利用深度学习算法精准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。

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户。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。

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、捏鼻子、捏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。

（3）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

- 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。
- 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”以及无法资质的机构或人员。
- 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、分享含有身份信息照片。

（4）防范电信诈骗小知识

- 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。
- 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。
- 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。
- 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。
- 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。





恒生前海
基金管理
HANG SENG QIANHAI FUND MANAGEMENT



深圳市网络安全宣传周
Shenzhen Cybersecurity Week

2024年9月9日-9月15日

网络安全为人民 网络安全靠人民

2024年深圳市网络安全宣传周



主办单位
市委宣传部、市委网信办、市密码管理局、市教育局、市公安局、
市文化广电旅游体育局、市政务和数据局、市总工会、团市委、
市妇联、市国家安全局、中国人民银行深圳市分行、市通信管理局

基金有风险，投资需谨慎，详情请阅基金法律文件。

文章来源：中国人民银行《2024 年金融网络安全宣传手册》。风险提示：本文仅以投资者教育为目的，不构成任何投资建议。基金有风险，投资需谨慎，详情请阅基金法律文件。