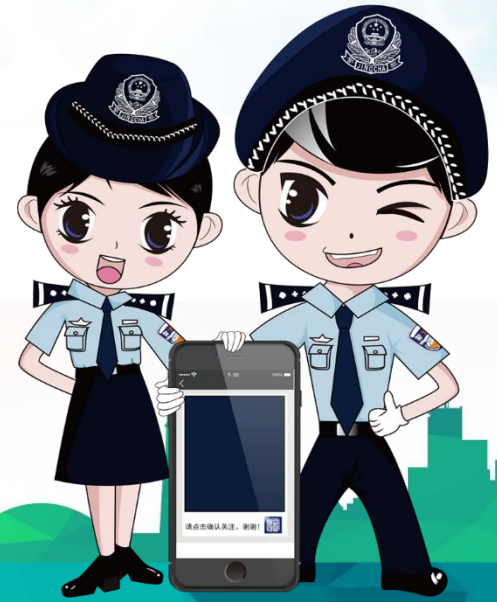
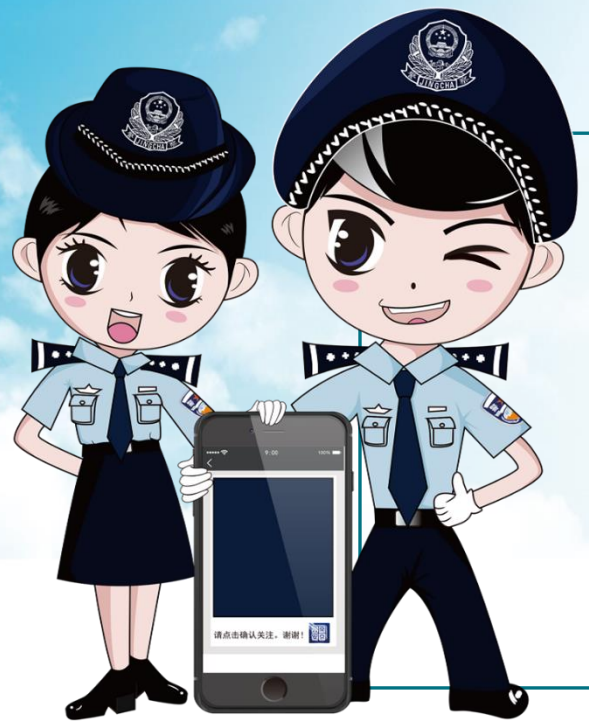
2022年国家网络安全宣传周

网络安全为人民 网络安全靠人民

网络安全

经济贸易学院





前　言

“互联网+”的时代改变了人们的生活习惯和行为模式

——购物交易、社交娱乐、学习工作，

方方面面的需求都可以通过互联网来完成。

我们要如何维护自身的?

目录

第一部分

国家网络宣传周介绍

国家网络宣传周介绍

国家网络安全宣传周

即“中国国家网络安全宣传周”是为了“共建网络安全，共享网络文明”而开展的主题活动，围绕金融、电信、电子政务、电子商务等重点领域和行业网络安全问题，针对社会公众关注的热点问题，举办网络安全体验展等系列主题宣传活动，营造网络安全

人人有责、人人参与的良好氛围。

国家网络宣传周介绍

2022年国家网络安全宣传周于2022年9月5日至11日举行

2022活动主题

“网络安全为人民 网络安全靠人民”

第二部分

电脑上网安全

网上上网的安全

账号密码安全

- 在上网过程中，无论是登录网站、电子邮件或者应用程序等等，帐号和密码是用户最重要的身份信息，因此帐号和密码的安全至关重要，一旦丢失会造成严重后果。在注册和使用的过程中应注意：
- 密码的设定一定要科学严谨，不可过于简单，尽量使用字母和数字相结合，具有一定长度的密码。
- 个人帐号和密码信息不可泄漏给他人。
- 在网吧等公用计算机上使用时切勿开启“记住密码”选项，使用完毕后应安全退出，重新启动电脑。

网上上网的安全

账号密码安全

- 设置浏览器的安全等级。
- 我们常用的浏览器都具有安全等级设置功能，通过合理地设置可以有效过滤一些非法网站的访问限制，从而减少对电脑和个人信息的损害。
- 坚决抵制反动、色情、暴力网站。
- 一方面这些不良信息会影响青少年的身心健康，
- 另一方面很多非法网站会利用浏览器漏洞对用户进行各种攻击。
- 不要随意点击非法链接。
- 下载软件和资料时应选择正规网站或官方网站。

第三部分

手机上网安全

手机上网安全

手机上网的基本注意事项

- 关闭常用通讯软件中的一些敏感功能。如微信里的附近的人 微信隐私里“允许陌生人查看照片”等。
- 不能随便晒家人及住址照片。长期这样下去，只要经过别人稍加分析汇总，你所晒出来的信息就会成为一套完整的信息，这就暗藏着各种不可预测的风险。
- 不要随便在网上测试相关信息。有的网站搞调查，问你的年龄、爱好、性别等等信息，你若为了一点小利益去做的话，这些信息就可能被人家利用起来，将你的信息逐渐总结，卖给别人盈利或威胁到你。
- 不要随意扔掉或卖掉旧手机。尤其是那些涉密的旧手机，可能出了些毛病你就打算卖掉或扔掉。千万不要这样，一些人就可以恢复你的数据，这其中暗藏着各种危害，你是无法预测到的。

手机上网安全

手机上网的基本注意事项

- 软件安装过程中不要都“允许”。尤其现在使用的智能手机，安装软件过程中，有的软件提示你是否允许安装全部服务，比如获取你的位置，读取你的电话记录等等，这种情况下，要千万小心，不相关的服务不能允许，或者不安装此软件。
- 不要随便接入公共WIFI。公共WIFI中有些是黑客获取你手机信息的一个重要渠道，可能直接盗取你的敏感信息，如卡号、账户密码等。所以，到公众场合后，有免费WIFI也不要随意接入。
- 不要随意发给别人验证码。验证码可以说是保密的一道重要防线，一旦突破了，那么可能就会有很大的后果等着你。

第四部分

网络购物安全防范

网络购物安全防范

购买前要留意商家信誉

确定购买之前，一定要先了解一下卖家的信誉度。卖家的信用评价是一个重要的参考标准。要注意选择合法的网站和商家，一般正规网站都应标注网上销售的经营许可证号和工商机关红盾检验标志。而且，网站应当持有ICP证书，消费者可通过查看网站主页最下方商家的数字证书来验证其“身份”。

不要被低价商品迷惑

特别是名牌产品，因为知名品牌产品除了二手货或次品货，正规渠道进货的名牌是不可能和市场价相差那么远的。

小心商家的文字游戏

当遇到字意模棱两可的介绍时，一定要向卖家询问清楚，以防有些不良卖家玩文字游戏。

网络购物安全防范

最好通过第三方支付

网上购物最好通过安全可靠的第三方交易平台来实现，尽量选择货到付款或交易平台提供的诸如支付宝等带有第三方保障功能的支付方式。同时，使用银行卡进行网络支付时，千万注意不要在网吧电脑等公共设备上使用；最好有专用账户或专用卡作网上支付用，并且卡内不要放太多的现金。如发现问题，及时与银行联系。

邮费太高要小心

购买之前，要跟卖家事先做好沟通，因为地域的关系邮费通常和所标价格不同，以防卖家把商品的价格订得很低，但是邮费却很高。

保存原始证据

对于价格比较高的大宗货品，最好不要在网上购买。如果一定要买的话，则应该向卖家问清来路，并最好要求其开具发票。无论商品价格是否昂贵，消费者都应注意保存和卖家之间的往来邮件、聊天记录，以为日后维权留下证据。

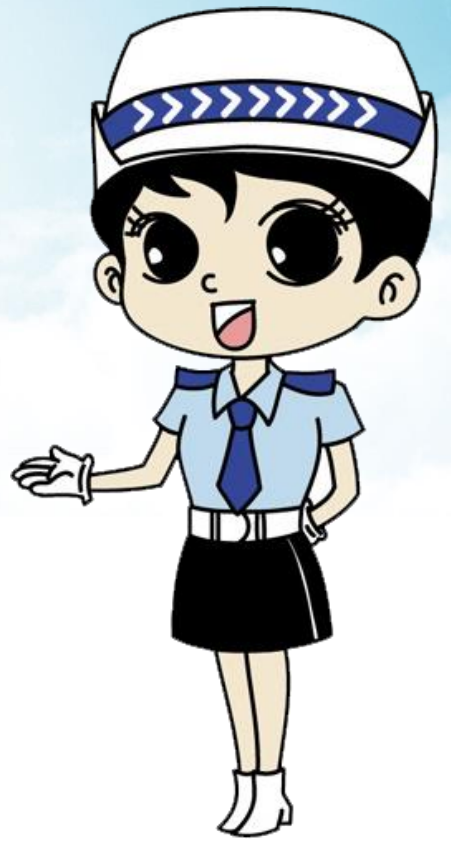
第五部分

常见网络诈骗手法及防范

常见网络诈骗手法及防范

冒充即时通讯好友借钱

骗子使用黑客程序破解用户密码,然后张冠李戴冒名顶替向事主的聊天好友借钱,如果对方没有识别很容易上当.大家如果遇到类似情况最好先与朋友通过打电话等途径取得联系，防止被骗。



网络游戏装备及游戏币交易进行诈骗

常见的诈骗方式一是低价销售游戏装备，在骗取玩家信任后，让玩家通过线下银行汇款的方式，待得到钱款后即食言，不予交易；二是在游戏论坛上发表提供代练，待得到玩家提供的汇款及游戏账号后，代练一两天后连同账号一起侵吞；三是在交易账号时，虽提供了比较详细的资料，待玩家交易结束玩了几天后，账号就被盗了过去，造成经济损失。

常见网络诈骗手法及防范

交友诈骗

犯罪分子利用网站以交友的名义与事主初步建立感情，然后以缺钱等名义让事主为其汇款，最终失去联系。

网上中奖诈骗

是指犯罪分子利用传播软件随意向手机用户、邮箱用户、即时通讯用户等发布中奖提示信息，当用户按照指定的“电话”或“网页”进行咨询查证时，犯罪分子会以中奖缴税等各种理由让用户一次次汇款，直到失去联系。当收到一些来历不明的中奖提示，不管内容有多么逼真诱人，请大家千万不能相信。

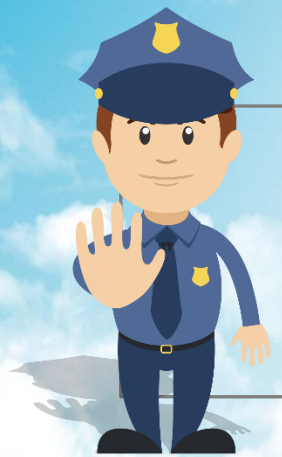
‘钓鱼网站’ 诈骗

是利用欺骗性的电子邮件和伪造的银行、金融机构网站进行诈骗活动，获得受骗者个人帐户信息进而窃取资金。因此，在访问些类邮件和网站时一定要仔细甄别，认真核实，切勿着急操作。

第六部分

日常网络陷阱防范

日常网络陷阱防范



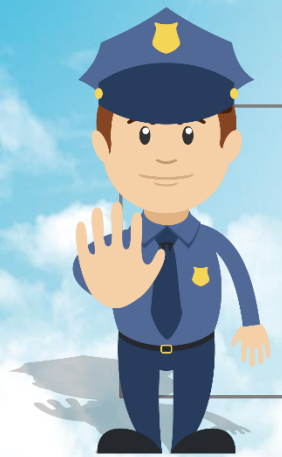
使用手机APP要谨慎

现在恶意APP程序越来越多，各类非官方下载渠道常被恶意应用。手机用户不使用来历不明的APP，使用正规渠道下载,安装时要注意"应用权限"与产品功能是否直接相关.使用防病击软件，为手机安全加上防护网站.

手机越狱和root要慎重

安卓root和苹果越狱会带来便利，可以安装更多软件，实现更多高级功能·但如果安装到恶意APP，可以读写删除手机文件、监听截取手机短信等·建议：非专业人员切勿越狱或root，要在官方市场下载应用。

日常网络陷阱防范



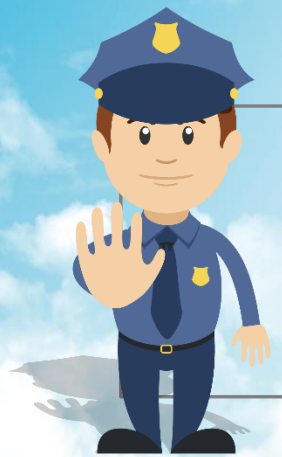
陌生人发微信 红包勿乱点

不法分子将手机病毒伪装成微信红包诱导消费者领取，遇到陌生人发送"红包"不要乱点，很可能带有病毒。建议：如果开红包需要填写个人信息等，肯定是骗局，要第一时间关闭手机网络，修改网银、支付宝等密码，然后通过止规途径删除病毒。

摄像头攻击多留心

家庭摄像头已成黑客攻击对象，很可能导致个人隐私泄露等。建议：不要使用预设密码，重置密码越复杂好，需定期更换，摄像头不要对着较私密空间，浴室、床等应置要尽量躲开，在家时可以关闭摄像头电源或用遮挡物挡住。

日常网络陷阱防范



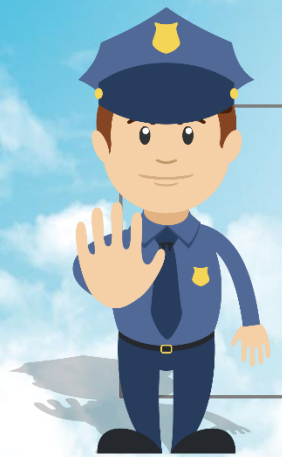
免费打印照片有危害

照片打印成为部分商家"吸粉"利器，目很容易泄露用户信息，比如，扫描二维码可能会让手机感染病毒·建议千万不要见码就扫。

人脸识别也危险

在之前央视315晚会上，人脸识别技术曾被曝出安全隐患，仅凭两部手机、一张随机正面照和一个换脸APP，就能通过3D脸模骗过人脸识别系统。建议：在这技术还没有纯熟之前，慎重使用！

日常网络陷阱防范



智能密码门锁存威胁

技术人员研究发现，现在可以通过之前编写好的破解程序，利用用户注册门锁的手机号码进行破解·建议：最好使用不太常用的手机号码注册，不要把门锁手机号码轻易给不熟悉的人

虚假二维码很可怕

不法分子通过虚假伪装一个网站生成二维码，在受害者扫描二维码时，通过云端软件获取当事人账号、密码等。建议：再重复一遍，干万不要见码就扫

第七部分

防范指南

五 “不”

不轻信

免费了、中奖了、秒杀了、抢红包了、日赚500了…“所有利益诱导性信息都不要轻易理睬；我是领导、我是房东、我是公安、我是老同学、猜猜我是谁 、所有装熟人的都不要轻易相信。

不回拨

客服咨洵、详情请拨、专属通道一一陌生信息中提供的联系方式，都不要轻易致电联系·

不点击

免费领奖、视频相册、工作资料、低价抢购、升级下载、积分兑换．一、、只要是陌生网址，都不要点击。

不透露

手机号码、家庭住址、电子邮箱、亲属联系方式、身份证号、银行卡账号密码、网银登录支付密码、支付宝密码等一切个人以及亲友隐私信息通通不可泄露。

不转账

房补、车补、中奖、退税、银行卡积分兑换现金等不要贪，身份不核实清楚不转账。

核实

核实转账请求

他人要求借钱、打款、线上支付、充值等，所有现金往来一定要当面或电话联系本人确认。

核实转账请求

陌生可疑的短信、电话、QQ、微信、邮件、通知等，只要拿不准情况，都通过线下营业厅、官方网站等官方渠道核实。

养成七个好习惯

① 保护好个人身份址和银行卡信息，保存好不用的复印件、交易流水信息

② 网上银行操作时，最好手工输入银行官方网站

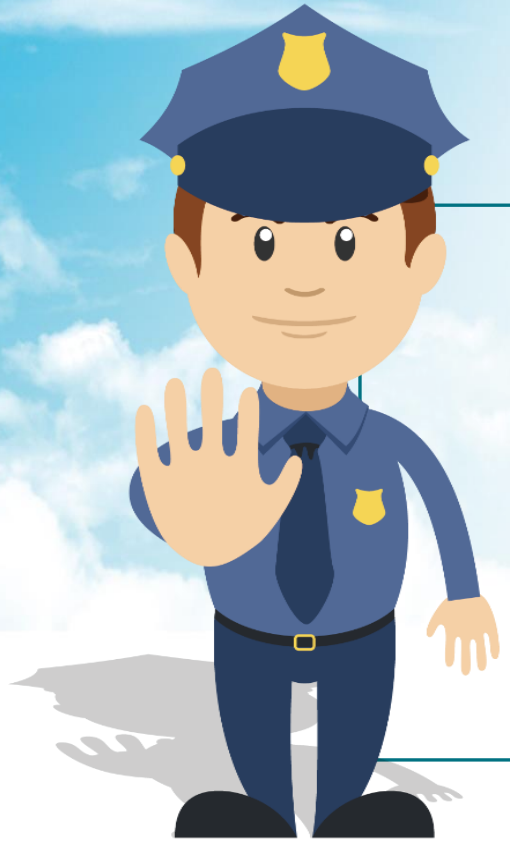
③ 开通账户动账通知短信，发现账户资金异动，立刻冻结或挂失

④ 在取款输入密码时用手遮挡

⑤ 密码要设置地相对复杂、独立，要定期更换

⑥ 进行网上银行、支付账户操作时，不要随意连接不明公共WiFi

⑦ 单独设立小额度银行账户，用于日常网上购物等消费



结束语

网络安全与我们的日常生活息息相关

网络隐患无处不在，在使用过程中同学们一定要提高警惕

树立正确的网络安全观念，加强防范意识，减少不必要的损失。

谢谢您的观看