2024

网络安全

为人民 靠人民

2024国家网络安全宣传周

目录

CONTENTS

01

Part One

国家网络宣传周

国家网络宣传周

“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

举行时间

每年9月第三周

第一届举行时间

2014年

2024年国家网络安全宣传周

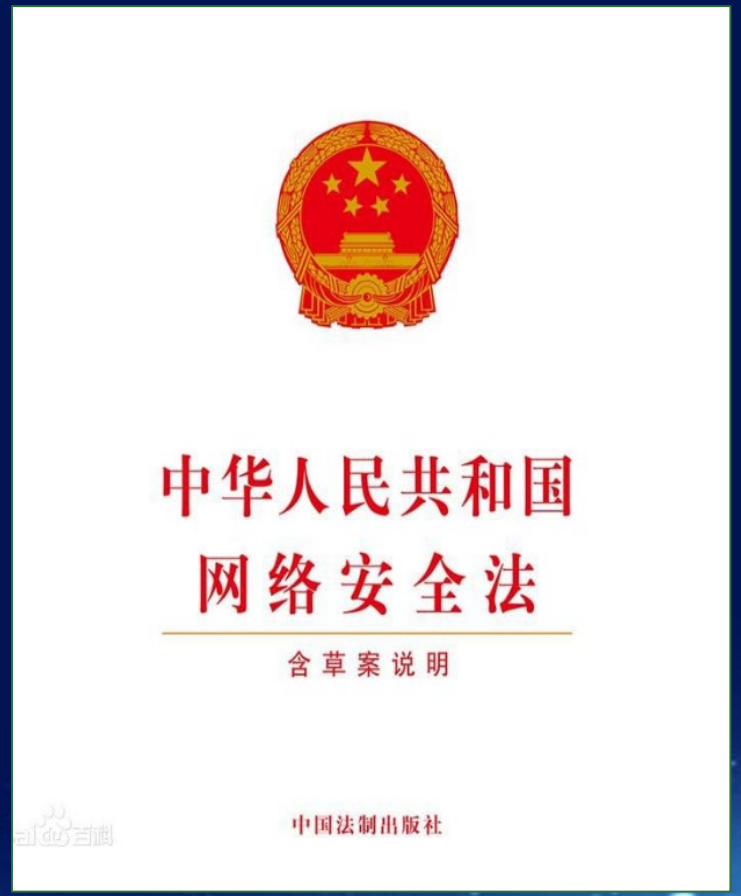
“网络安全为人民，网络安全靠人民”

02

Part Two

国家网络安全法

国家网络安全法



中华人民共和国网络安全法》(以下简称《网络安全法》)是我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,由全国人民代表大会常务委员会于2016年11月7日公布,自2017年6月1日起施行。

国家网络安全法

习总书记指出：

没有网络安全就没有国家安全，没有信息化就没有现代化。《中华人民共和国网络安全法》的出台，顺应了网络空间安全化、法制化的发展趋势，不仅对国内网络空间治理有重要的作用，同时也是国际社会应对网络安全威胁的重要组成部分，更是中国在迈向网络强国道路上至关重要的阶段性成果，它意味着建设网络强国、维护和保障我国国家网络安全的战略任务正在转化为一种可执行可操作的制度性安排。尽管《中华人民共和国网络安全法》只是网络空间安全法律体系的一个组成部分，但它是重要的起点，是依法治国精神的具体体现，是网络空间法制化的里程碑，标志着我国网络空间领域的发展和现代化治理迈出了坚实的一步。

国家网络安全法

网络空间主权原则

《中华人民共和国网络安全法》第1条“立法目的”开宗明义，明确规定要维护我国网络空间主权。网络空间主权是一国国家主权在网络空间中的自然延伸和表现。

网络安全与信息化发展并重原则

既要推进网络基础设施建设和互联互通,鼓励网络技术创新和应用又要建立健全网络安全保障体系,提高网络安全保护能力,做到“双轮驱动、两翼齐飞”。

共同治理原则

网络空间安全保护需要政府、企业、社会组织、技术社群和公民等网络利益相关者的共同参与。

国家网络安全法

看点一：不得出售个人信息

近年来，警方查获曝光的大量案件显示，公民个人信息的泄露、收集、转卖，已经形成了完整的黑色产业链。诈骗分子通过非法手段获取个人信息，包括姓名、电话、 家庭住址等详细信息后，再实施精准诈骗，令人防不胜防。网络安全法规定：网络产品、服务有收集用户信息功能的，其提供者应当向用户明示并取得同意；网络运营者不得泄露其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。网络安全法作为网络领域的基础性法律，聚焦个人信息泄露，不仅明确了网络产品服务提供者、运营者的责任，而且严厉打击出售贩卖个人信息的行为，对于保护个人信息安全，将起到积极作用。

国家网络安全法

看点二：严厉打击网络诈骗

《中华人民共和国网络安全法》针对新型网络诈骗犯罪规定：任何个人和组织不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布与实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。这些规定，不仅对诈骗个人和组织起到震慑作用，更明确了互联网企业不可推卸的责任。

国家网络安全法

看点三：以法律形式明确“实名制”

网络安全法以法律的形式对“网络实名制”做出规定：网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。网络服务提供商要落实主体责任，加强审核把关。

国家网络安全法

看点四：重点保护关键信息基础设施

《中华人民共和国网络安全法》对关键信息基础设施的运行安全进行明确规定，指出国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域的关键信息基础设施实行重点保护。保障这些关键信息系统的安全，不仅仅是保护经济安全，更是保护社会安全、公共安全乃至国家安全。保护国家关键信息基础设施是国际惯例，《中华人民共和国网络安全法》以法律的形式予以明确和强调，非常及时而且必要。

国家网络安全法

看点五：惩治攻击破坏我国关键信息基础设施的境外组织和个人

我国一直是网络攻击的受害国。《中华人民共和国网络安全法》规定，境外的个人或者组织从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该个人或者组织采取冻结财产或者其他必要的制裁措施。《中华人民共和国网络安全法》这一规定，不仅符合国际惯例，而且表明了我们维护国家网络主权的坚强决心。

国家网络安全法

看点六：重大突发事件可采取“网络通信管制”

网络安全法中，对建立网络安全监测预警与应急处置制度进行了规定，明确发生网络安全事件时，有关部门需要采取的措施。特别规定：因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

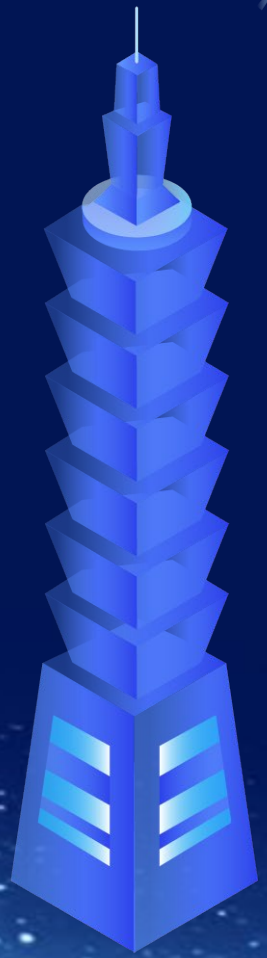
国家网络安全法

《网络安全法》禁止哪些个人和组织的网络行为

不得危害网络安全,不得利用网络从事危害国家安全、荣誉和利益,煽动颠覆国家政权、推翻社会主义制度,煽动分裂国家,破坏国家统一,宣扬恐怖主义、极端主义,宣扬民族仇恨、民族歧视,传播暴力、淫秽色情信息,编造、传播虚假信息扰乱经济秩序和社会秩序,以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

发现他人有危害网络安全的行为时,我们应该如何处理

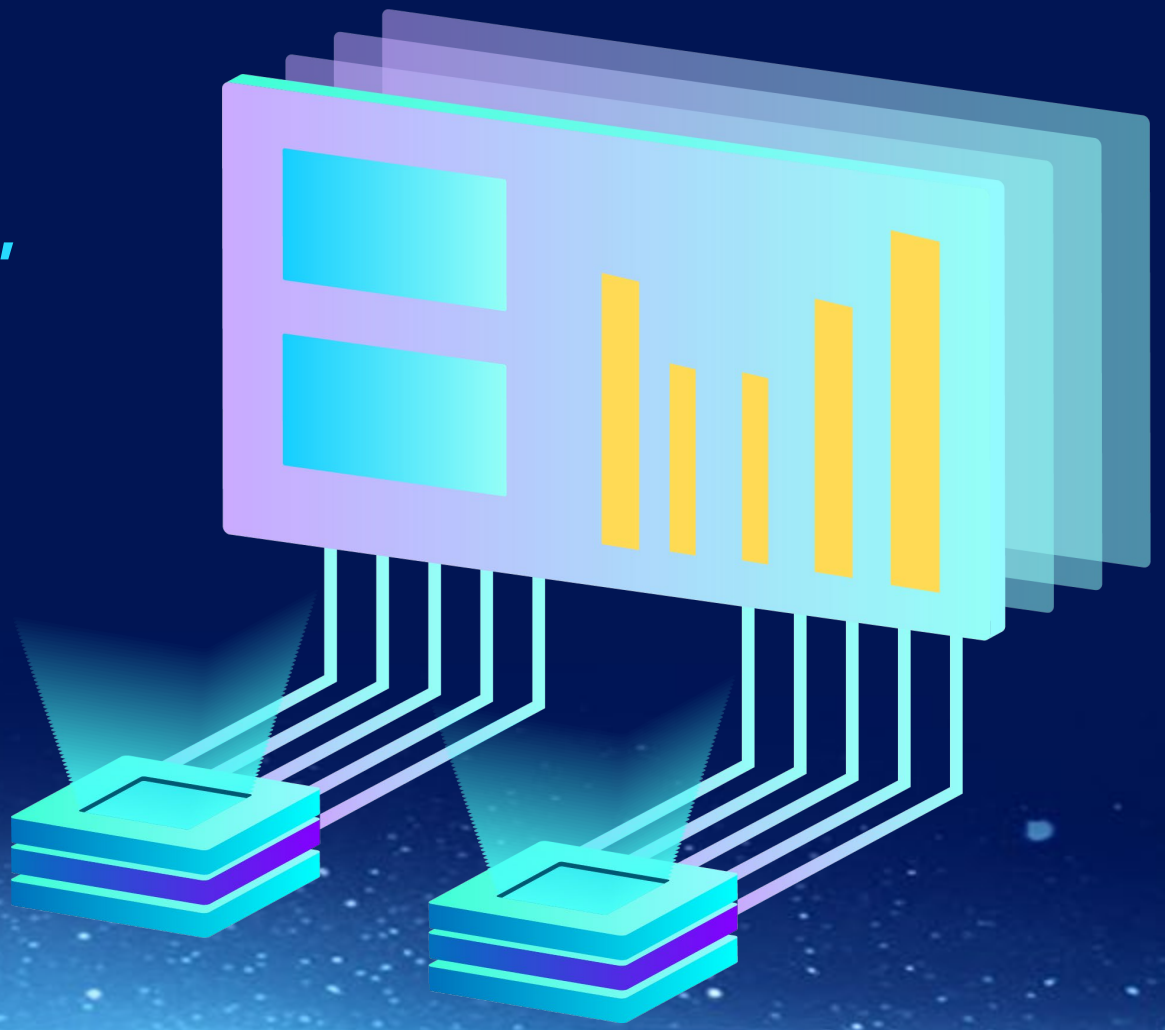
向网信、电信、公安等部门举报。



国家网络安全法

发现网络运营者违反《网络安全法》相关规定，侵犯个人权益的，我们有哪些权利？

有权要求网络运营者删除个人信息，发现网络运营者收集、存储的个人信息有错误的，有权要求网络运营者予以更正。



03

Part Three

网络安全隐患

网络安全隐患

网络诈骗

电脑病毒

隐私泄露

手机病毒

交友诈骗

骚扰电话

手机支付

垃圾短信

网络安全隐患

电信诈骗(又称非接触性诈骗或远程诈骗)是指不法分子以非法占有为目的,利用手机短信、电话、网络电话、互联网等方式,以虚构事实或隐瞒事实真相的方法,骗取受害者财物的行为。

网络安全隐患

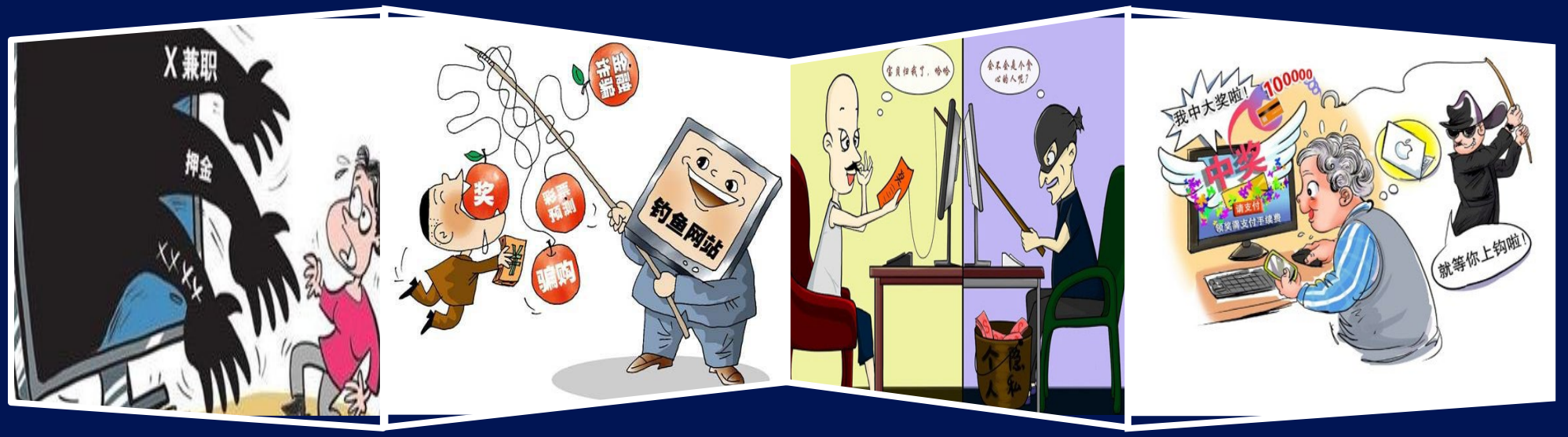
案例一：欢乐购诈骗

李先生手机收到短信，称其获得980元抢购PhoneX的机会。李先生购机后发现，新购手机非常不好用，明显是山寨。

案例二：贫困助学诈骗

某大学新生小徐,先接到自称是教育部门的电话,让她办理助学金的相关手续。随后又接到另一个电话,称有一笔2600元的助学金需尽快领取,并要求她将9900元学费汇入个指定账号,半小时后会返还学费并发放助学金。小徐完成操作后发现对方电话关机,才明白上当受骗了。万分难过的她当天晚上突然晕厥,最终经医院抢救无效去世。

网络安全隐患



网络钓鱼是指不法分子通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件或短信、即时通讯信息等，引诱收信人给出敏感信息（如用户名、口令、帐号 ID 或信用卡详细信息），然后利用这些信息假冒受害者进行欺诈性金融交易，从而获得经济利益。受害者经常遭受重大经济损失或个人信息被窃取并用于犯罪的目的。

网络安全隐患

案例一：钓鱼Wi-Fi诈骗

张女士在一家商场内连接了一个没设密码的Wi-Fi,随后在某网购平台上对商场一件衣服进行比价,由于价格便宜近一半,她毫不犹豫地通过手机支付在该网购平台购买了这件衣服。不久,张女士的手机收到短信提示,其信用卡被盗刷4笔,总金额高达8000多元。

安全提示:

- **谨慎使用免费Wi-Fi。**
- **拒绝来路不明的Wi-Fi,尽量选择正规来源的Wi-Fi。**
- **Wi-Fi连接方式建议设置为手动,或者关闭WiFi自动连接功能。**
- **不要使用破解Wi-Fi密码的软件,谨防被此类软件盗取隐私。**
- **使用公共场所的Wi-F不要输入账号、密码或个人敏感信息。**

网络安全隐患

伪基站一般由主机和笔记本电脑组成，不法分子通过伪基站能搜取设备周围一定范围内的手机卡信息，并通过伪装成运营商的基站，冒充任意的手机号码强行向用户手机发送诈骗、广告推销等短信息。

网络安全隐患

案例一：冒充运营商诈骗

张先生收到号码“10000”发来的一条短信,称张先生有大量积分,可以兑换一笔金额不小的话费。张先生随后点击了短信中的链接,进入兑换话费的网页,并按提示输入了自己的银行卡卡号和支付密码。

积分张先生等了几天,说好的话费却迟迟没有到兑换账,反而发现自己的银行卡被转走两万余元。经查张先生是中了伪基站的诈骗圈套。

案例二：冒充银行诈骗

李女士正在玩手机,突然收到一条ＸＸ银行发来的银行卡消费积分兑换短信，没有多想就点开了链接,并按提示输入了自己的银行卡卡号和身份证号码,又输入了ＸＸ银行短信发来的验证码,没想到短短数十秒后,就收到多条共计转款99998元的短信,李女士这才意识到自己被骗了。

网络安全隐患

二维码诈骗是不法分子通过替换商户的收款码、共享单车二维码、罚单二维码等方式更改收款账户，或发布隐藏有木马病毒的二维码，一旦受害人扫码支付，便可轻松获取受害人的钱财。

网络安全隐患

案例一：木马病毒二维码诈骗

倪女士经营一家网店。前不久,一位买家在准备支付时,木希望倪女士通过扫描二维码方式进行结算。倪女士为得到对方“好评”,便用手机扫描了对方发来的二维码，随后出现个链接网址,点击后很久也没显示成功,且手机变慢。倪女士立即用电脑登录支付宝,发现银行卡上的9万元已被转走。

案例二：假冒执法罚单诈骗

张女士发现自己路边停放的车上被贴了罚单,上面还印有快速缴费二维码,张女士随即扫描该二维码并缴纳罚款。事后,经朋友提醒,张女士打电话咨询交管部门,才发现扫描了假的二维码。

网络安全隐患

网购诈骗是不法分子利用受害人在网购过程中的疏忽来实施的诈骗。

网络安全隐患

案例一：网购退款诈骗

陈女士在某网款购平台上购买了件价格几十元的物品,因对物品不满意申请退款。经沟通,网店同意退款并指导陈女士通过某支付平台办理退款手续,款项很快就退回至陈女士的银行卡,但金额却为1万元。网店的电话紧跟而至,声称由于误操作,错转成了1万元，要求陈女士把钱退回到指定的账户,否则就会报警。幸好陈女士警惕性较高,立即向公安机关报案,未造成资金损失。经调查,陈女士在通过某支付平台办理退款时,实际上是点开了支付平台的贷款页面并操作成功,而不法分子谎称是其退款操作错误,要求陈女士退回,以此实施诈骗。

安全提示：

- **不点击陌生人发送的链接,不扫描陌生人发送的二维码;**
- **网购退款时,要在电商平台的官方网站操作;**
- **注意鉴别网址真伪,谨防账号密码被盗**
- **网络购物要留个心眼,千万别贪小便宜上大当。**

网络安全隐患

指纹识别诈骗是不法分子利用受害人使用指纹解锁和指纹支付过程中的漏洞实施诈骗的行为。

网络安全隐患

案例一:盗用指纹诈骗

姜先生的手机解锁和支付需要指纹识别。一日姜先生和朋友在酒吧喝酒,在付费时姜先生使用了指纹支付。随后其朋友送醉酒的姜先生回家,在姜先生熟睡时,用姜先生的指纹支付向自己转账5200元,并删除了姜先生手机上的转账记录和扣款短信。

安全提示:

●若手机发生摔碰,应及时枪查指纹解锁功能是否正常

●在使用指纹验证前,检查指纹触摸键上是否有其他异物;

●开通指纹支付后,应限额并妥善保管手机,避免被人盗用;

●尽量避免他人的指纹录入到自己的手机中。

网络安全隐患

病毒充电宝是被不法分子植入木马病毒的充电宝,通常放置在公共场所,一旦受害人连接充电,手机便会自动下载木马病毒,不法分子通过读取受害人通信录、银行卡、支付宝等的信息实施诈骗、勒索等非法活动。

网络安全隐患

案例一：恶意充电宝诈骗

任女士某次出差途中,手机没电了,恰巧周围没有充电设备,于是借用一名男士的充电宝。次日,任女士接到陌生电话,对方称手里有任女士手机中的所有信息,包括一些重要的客户资料,向任女士索要赎金。经调查,任女士的信息泄露源头是借用他人有病毒的充电宝充电造成的。

安全提示：

- **从正规渠道购买充电宝。**
- **尽量不借用陌生人充电宝,以免中了某些不法分子的招。**
- **最好使用电源方式给手机充电,谨慎使用公共场所提供的充电设备。**
- **手机在连接充电宝后,若出现“信任”选项,不要点击。**

网络安全隐患

移动支付诈骗是指用户在使用移动终端进行支付时,不法分子利用黑客技术,终端漏洞或用户疏忽等,盗取用户信息,骗取受害人钱财的行为。

网络安全隐患

案例一：盗取手机ID诈骗

李先生发现自己的某品牌手机被锁定,随后注册该品牌手机ID的邮箱收到一封勒索邮件,称可以解锁手机但需支付2000元现金。原来，不法分子通过黑客技术，攻破李先生的手机转过来2000元。账号并篡改了手机ID密码,再登录更改账户名,最后通过“查找我的手机”远程锁定手机并实施勒索。

案例二：微信支付诈骗

赵先生经营一家化妆品微店,一位微信昵称叫“美美”的网友加了赵先生的微信后,表示想买一瓶眼霜,并用二维码支付。由于赵先生对二维码支付不熟,在“美美”的指导下，将自己的付款二维码发送给了“美美”,随后他收到银行短信,提示微信绑定的银行卡消费1500元。赵先生遂与“美美”核实,却再也联系不上,此时才明白被骗了。

安全提示：

- **保护好个人信息,尤其是银行卡卡号、支付宝账号和密码等敏感信息。**
- **卸载带有支付功能的手机应用时,应先检查是否已解除银行卡绑定。**
- **要通过官网或正规应用市场下载安装软件。**

网络安全隐患

目前某些中小网站的安全防护能力较弱，容易遭到黑客攻击，不少注册用户的用户名和密码便因此泄露。而如果用户的支付账户设置了相同的用户名和密码，则极易发生盗用。

网络安全隐患

社交陷阱是指有些不法分子利用社会工程学手段获取持卡人个人信息，并通过一些重要信息盗用持卡人账户资金的网络诈骗方式。例如不要轻信信用卡中心打来的“以提升信用卡额度”为由的诈骗电话。

04

Part Four

安全上网建议

安全上网建议

安全软件

密码安全

时刻戒备

保持更新

洁身自好

安全上网建议

1. 经常用于网络支付的银行卡不要存放太多资金,设置每日网络消费、转账限额。

2. 签约短信通知服务和盗刷保险服务,可以为资金财产安全保驾护航。

3. 用于网络支付的电脑或移动终端应安装安全软件,并定期进行扫描。

安全上网建议

4 不要点击来历不明的链接,在进行网络支付或退款等操作时应登录正规网站。

5 不要登录非法网站,避免电脑或移动终端被植入木马病毒。

6 不同网络支付账号建议设置不同密码。

7 不要告诉他人网络支付的密码和验证码等关键信息。

安全上网建议

01 **挂失手机卡：**

致电运营商挂失、冻结手机卡,并及时到运营商网点补办。

02 **冻结手机银行账户：**

通过银行客服电话银行网点/网银果道冻结或销户。

03 **挂失云闪付：**

拨打银行服务热线或到银行柜台挂失。

04 **冻结微信账户：**

登录http://110.qg.com通过QQ号或手机号冻结微信。

05 **冻结支付宝账户：**

登录支付宝—安全中心-应急服务。

2024

网络安全

为人民 靠人民

2024国家网络安全宣传周