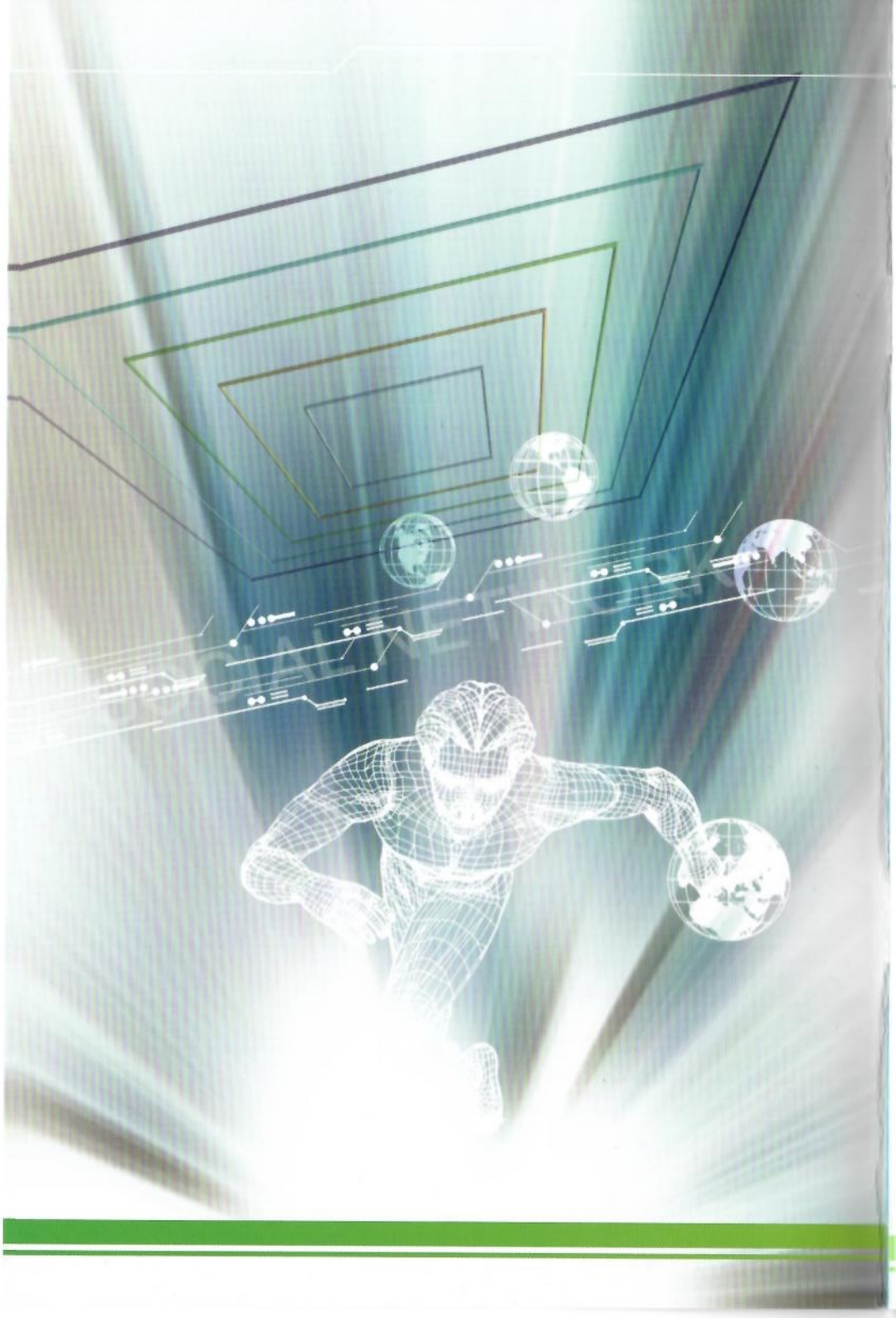
网络安全

知识手册



01 基础知识

一、计算机知识
二、网络安全知识

02 案例

一、【谨防手机木马病毒盗取网上银行账号、密码】
二、【网购小心假卖家骗钱】
三、【兼职“点赞”赚钱不靠谱】
四、【警惕：“招生”中的陷阱】
五、【“扫一扫”，小心陌生的二维码】
六、【警惕“公安机关”的调查电话】
七、【医保卡异常需冻结是骗局】
八、【“幸运观众”大奖莫轻信】
九、【代办信用卡？盗刷储值卡】
十、【网络游戏“代刷”藏木马】
十一、【“猜猜我是谁”诈骗】
十二、【冒充QQ好友进行诈骗】
十三、【假冒单位领导发微信给员工实施诈骗】
十四、【别让爱心变闹心】
十五、【10086短信也有假？】

03 互联网中，您需要了解的法律知识

一、禁止从事那些危害计算机信息网络安全的活动
二、诽谤
三、寻衅滋事
四、敲诈勒索
五、非法经营
六、危害计算机信息系统安全罪

04 查询、举报常用网址

当今社会，不同年龄、职业、生活环境的人们，几乎都会随时随地接触到计算机网络，它为我们的学校、工作和生活带来了极大的便利。通过计算机网络，学生轻松地学习知识，股民方便地买卖股票；银行职员迅捷地操作业务。

办公室人员大大提高了工作效率；旅行者免去了排队买票的劳顿之苦；还有更多的人通过它了解新闻、搜索查询、通讯联络、聊天游戏……计算机网络使我们的生活变得更加丰富多彩了。

下面，让我们认识计算机的方方面面……

基础知识

一、计算机知识

1、计算机中毒有哪些症状?

（1）经常死机；
（2）文件打不开；
（3）经常报告内存不够；
（4）提示硬盘剩余空间不足；
（5）出现大量来历不明的文件；
（6）数据无端丢失；
（7）系统运行速度变慢；
（8）操作系统自动执行操作。

2、计算机日常使用中遇到的异常情况有哪些?

计算机出现故障可能是由计算机自身硬件故障、软件故障、误操作或病毒引起的，主要包括系统无法启动、系统运行变得缓慢、可执行程序文件大小改变等异常现象。

3、在使用计算机过程中应该采取哪些网络安全防范措施?

（1）安装防火墙和防病毒软件，并经常升级；
（2）注意经常给系统安装补丁，堵塞软件漏洞；
（3）不要上一些不太了解的网站，不要执行从网上下载后未经杀毒处理的软件，不要打开聊天软件传送过来的不明文件等。

4、为什么要定期进行补丁升级?

编写程序不是十全十美，所以软件也免不了会出现BUG，而补丁是专门用于修复这些BUG的。因为原来发布的软件存在缺陷，发现之后另外编制一个小程序使其完善，这种小程序俗称补丁。定期进行补丁升级，升级到最新的安全补丁，可以有效地防止非法入侵。

5、如何防范U盘、移动硬盘泄密

（1）及时查杀木马与病毒；
（2）从正规商家购买可以移动存储介质；
（3）定期备份并加密重要数据；
（4）不要将办公与个人的可移动存储介质混用。

6、如何将网页浏览器配置得更安全?

（1）设置统一、可信的浏览器初始页面；
（2）定期清理浏览器中本地缓存、历史记录以及临时文件内容；
（3）利用病毒防护软件对所有下载资源及时进行恶意代码扫描。

二、网络安全知识

1、如何防范病毒或木马的攻击?

（1）为计算机安装杀毒软件，定期扫描系统、查杀病毒，及时更新病毒库、更新系统补丁；
（2）下载软件时尽量到官方网站或大型软件下载网站，在安装或打开来历不明的软件或文件前先杀毒；
（3）不随意打开不明网页链接，尤其是不良网站的链接，陌生人通过QQ给自己传链接时，尽量不要打开；
（4）使用网络通信工具时不随便接收陌生人的文件，若接收可取消“隐藏已知文件类型扩展名”功能来查看文件类型；
（5）对公共磁盘空间加强权限管理，定期查杀病毒；
（6）打开移动存储器前先用杀毒软件进行检查，可在移动存储器中建立名为autorun.inf的文件（可防U盘病毒启动）；
（7）需要从互联网等公共网络上下载资料转入内网计算机时，用刻录光盘的方式实现转存；
（8）对计算机系统的各个账号要设置口令，及时删除或禁用过期账号；
（9）定期备份，当遭到病毒严重破坏后能迅速修复。

2、如何防范QQ、微博等社交平台账号被盗?

（1）账户和密码尽量不要相同，定期修改密码，增加密码的复杂度，不要直接用生日、电话号码、证件号码等有关个人信息的数字作为密码；
（2）密码尽量由大小写字母、数字和其他字符混合组成，适当增加密码的长度并经常更换；
（3）不同用途的网络应用，应该设置不同的用户名和密码；
（4）在网吧使用电脑前重启机器，警惕输入账号密码时被人偷看；为防账号被侦听，可先输入部门账号名、部分密码，然后在输入剩下的账号名、密码；
（5）涉及网络交易时，要注意通过电话与交易对象本人确认。

3、如何安全使用电子邮件?

（1）不要随意点击不明邮件中的链接、图片、文件；
（2）使用电子邮件地址作为网站注册的用户名时，应设置与原邮件密码不相同的网址密码；
（3）适当设置找回密码的提示问题；
（4）当收到与个人信息和金钱相关（如中奖、集资等）的邮件时提高警惕。

4、如何保证网络游戏安全?

（1）输入密码时尽量使用软键盘，并防止他人偷窥；
（2）为电脑安装安全防护软件，从正规网站上下载网游插件；
（3）注意核实网游地址；
（4）如发现账号异常，应立即与游戏运营商联系。

5、如何防范社交网站信息泄露?

（1）利用社交网站的安全与隐私设置保护敏感信息；
（2）不要轻意点击未经核实的链接；
（3）在社交网站谨慎发布个人信息；
（4）根据自己对网站的需求进行注册。

6、当前网络诈骗类型及如何预防?

网络诈骗类型如下四种：一是利用QQ盗用网络游戏交易进行诈骗，冒充好友借钱，二是网络购物诈骗，收取订金骗钱，三是网上中奖诈骗，指犯罪分子利用传播软件随意向互联网QQ用户、邮箱用户、网络游戏用户、淘宝用户等发布中奖提示信息；四是“网络钓鱼”诈骗，利用欺骗性的电子邮件和伪造的互联网站进行诈骗活动，获得受骗者财务信息进而窃取资金。

预防网络诈骗的措施

- 不贪便宜；
- 使用比较安全的支付工具；
- 仔细甄别，严加防范；
- 不要在网上购买非正当产品，如毕业证书、考题答案等；
- 不要轻信以各种名义要求你先付款的信息，不要轻易把自己的银行卡借给他人；
- 提高自我保护意识，注意妥善保管自己的个人信息，不要向他人透露本人证件号码、账号、密码等；尽量避免在网吧等公共场所使用网上电子商务服务。

案例

网络可以购票，随时满足您回家探亲、出门旅游的需求；网络可以购物，随时方便您居家生活、衣食住行的需要；网络甚至改变了您固有的生活习惯，它帮助我们节省了在银行里排队转账付款的时间；解决了在招聘会上摩肩接踵投递简历的尴尬……与此同时，网络好像被打开了的潘多拉魔盒，肆意释放出各种“魔鬼”，侵扰着我们的生活，酿制着一出出的闹剧和一场场的骗局……

一、【谨防手机木马病毒盗取网上银行账号、密码】

北京何先生突然收到朋友发来的一条含有链接地址的短信，未曾想到里面却暗藏着一种手机木马病毒。该手机木马病毒一般以您认识的朋友的名义发来短信，通过点开手机短信的方式来盗取用户手机通讯录、网上银行账号密码及拦截快捷支付验证码等信息。一旦用户点开这条短信，便意味着这个病毒将以新的名义，继续向手机通讯录中的每一名联系人传播。

网警艾特提示：凡是收到此类带有网址链接的不明信息，请勿轻易点击，必要时可电话联系发送短信的朋友进行核实，以免个人信息被窃。

二、【网购小心假卖家骗钱】

沈阳徐女士在“某宝网”上购买衣服后，突然收到“卖家”电话，表示其所拍的衣服存在有质量问题，会将所支付的款额全部退还。许女士一开始心有疑虑，但对方对她的个人资料及所拍衣服款式都了如指掌，便信以为真。为配合“卖家”退款，徐女士将银行卡号及解码器动态密码都告诉了对方，最终非但没有收到退款，还被骗损失900多元。

网警艾特提示：网购诈骗花样繁多，请警惕“卖家”二次退换货、款等要求，一定要仔细核实，切勿轻易透露银行卡或其他任何证件号码等个人信息，并且尽量选择第三方支付平台进行交易，谨防被骗。

三、【兼职“点赞”赚钱不靠谱】

很多网友反映，微信上有人以“兼职‘点赞’赚钱”为名诱骗网友进行诈骗。经查，微信中却有某些“金融公司”以招募兼职‘点赞’赚钱的求职者为主要业务，要求兼职员工在入职时缴纳一定费用的入会费后，才可进行“点赞”赚取佣金的工作，但当求职人员缴费成功后，对方便杳无音讯，再也联系不上了。

网警艾特提醒：网络兼职工作多种多样，且门槛较低，寻找兼职工作时需特别谨慎，尤其要警惕那些以先交纳手续费、保证金、抵押款等为名目的兼职工作，以防遭受钱财损失。

四、【警惕“招生”中的陷阱】

每年中考、高考以及硕士研究生入学考试过后，总有一些学生或家长接到自称某校招生办老师或某招生中介机构的电话，被告知家中考生的考试分数比录取分数略低，但由于学校有扩招打算，考生缴纳相关助学费即可被录取。很多家长望子成龙心切，生怕被其他考生捷足先登，错失“大好良机”，便失去了原有的判断能力，最终导致身心、财产受到双重损失。

网警艾特提示：凡是接到所谓的“学校招生办”或“招生中介结构”的电话，并以分数不够为由告知您需缴纳助学费方可录取时，应及时打电话到相关学校或部门核实，以防上当受骗。

五、【“扫一扫”，小心陌生的二维码】

随着网络的不断发展，越来越多的人选择在网络上开店，王先生就在网上经营着一家网店。一天，一个陌生人以买家的身份，在QQ中加王先生为好友，同时发来一张二维码让王先生扫一下以方便日后联系。随后的两天里，王先生突然发现在网上交易时，再也没有收到过银行的提示短信，就连使用支付宝所需要的验证码也没有收到。因为手机捆绑了网银功能，所以不安的王先生急忙赶到银行进行查询，却发现他的银行卡账单上出现了100多次的网上支付记录，累计金额高达9万余元。

网警艾特提示：随着手机的普及，二维码已成为时下流的“名片”，用手机“扫一扫”就能添加微信好友、浏览网页、下载优惠券和手机应用等。但是，这些二维码的背后却可能隐藏着我们难以辨识的病毒。因此，在“扫一扫”之前，应特别提高警惕，不要盲目扫描来源不明的二维码，以免意外泄露个人信息，造成不必要的经济损失。

六、【警惕“公安机关”的调查电话】

近年来不断有市民报警，表示在家中或手机上接到自称“公安机关”的电话，告知其涉嫌洗黑钱、包裹藏毒等案件，要对其银行账户进行监管，并要求涉案人员前往ATM自动柜员机，且在英文界面上办理相关监管手续，结果导致被划走大量现金。

网警艾特提示：遇到冒充公检法类的涉案电话市民无需理会，不要轻信并泄露个人信息，可及时拨打相关部门电话核实对方身份，或直接拨打“110”。

七、【医保卡异常需冻结是骗局】

市民余先生接到录音电话称，他的社保卡和医保卡出现异常需要冻结，并提示他拨打所谓的“检察院”电话进行咨询。“检察院”工作人员在电话中告知余先生，需把银行中的资金尽快转至“安全账户”进行保护。

网警艾特提示：犯罪分子常广泛“撒网”，诱骗不明真相的群众上钩，并对其实施诈骗。在此特别提示，若社保卡真的出现问题，一般情况下，会要求持卡人到相关服务大厅完成办理手续，而不是通过银行转账私下完成。

八、【“幸运观众”大奖莫轻信】

很多网友都在手机中收到过成为某电视台热门栏目“幸运观众”的中奖短信，并要求登录某网站网址领取万元现金大奖及其他电子奖品。不少网友登录短信中提供的网址，并输入身份信息后便会接到一个手机来电，告知领奖须先缴纳一定费用，缴费成功后，对方则会以运费，保险费等为名继续要求汇款，直至最终失去联系。

网警艾特提示：请理性对待各类中奖信息，如确有参与任何节目的有奖环节，可致电相关官方客服咨询具体情况，切勿随意填写个人信息或转账给任何单位、个人。

九、【代办信用卡？盗刷储蓄卡？】

庞先生报案称，去年10月接到自称某金融公司工作人员的电话，表示可办理透支额度为5万元至100万元的信用卡，但同时需要办理一张储蓄卡以监管账户安全，并要求办卡人将相关卡号、联系电话等信息填写在该金融公司网站上进行备案。庞先生办理储蓄卡后存入4万元，在打开电子密码器输入密码后，立即收到银行提示短信，告知其账户内被划走39900元。

网警艾特提示：代办高额信用卡与低息无抵押贷款，都存在极高的诈骗风险，在办理时均需填写较为详细的个人信息，切勿按照陌生人的提示填入此类信息，尤其是预留的验证信息。

十、【网络游戏“代刷”藏木马】

曾有网友举报，很多玩家众多的热门网络游戏被不法分子盯上，通过短信、邮件、游戏内系统公告、QQ消息等途径发布“低价刷道具、点券等”虚假信息，诱使玩家上当。随后相关游戏运营商均及时发布辟谣声明，并表示上述“代刷”行为是不法分子利用少数玩家的侥幸心理，发布的含有木马病毒的网页或软件，用以盗取用户电脑账号等信息行骗。

网警艾特提示：网游装备的可交易性易被不法分子利用，游戏的官方运营商不会向任何玩家索要账号、密码及钱财。非官方发布额任何信息和内容，玩家切勿轻听轻信。

十一、【“猜猜我是谁”诈骗】

诈骗分子获取事主的电话号码和机主姓名后，打电话给事主，让其“猜猜我是谁”，随后根据所述冒充熟人的身份，并声称要来看望事主。随后，编造其被“治安拘留”、“交通肇事”等理由。向事主借钱，一些事主没有仔细核实就把钱打入犯罪分子提供的银行卡内造成钱财损失。

网警艾特提示：遇到此类情况，事主应提高警惕，问明事情的详细的情况，或通过其他方式核实机主身份，再作决定。

十二、【冒充QQ好友进行诈骗】

住在某公寓的小唐，QQ上谈出了这么一段话，“跟你商量个事，我有个亲戚向我借5万元钱，我怕以后不好意思催他还，想用你的名义汇过去，钱我会打到你的卡上的。”说话的好友是小唐的高中同学，两人的关系很好，还经常保持联系。虽然，两人关系很好，但小唐还是有些顾虑。为了消除小唐的疑惑，紧接着对方给他发来了一张银行卡的截图，并称会在6个小时以后将钱转到小唐账户上。因为是关系不错的高中同学，也不是用自己的钱转账，小唐思索后便应承下来。结果毫无疑问得小唐不幸中招，一次性被骗5万元。

网警艾特提示：遇到此类情况，头脑中务必多思考，一定要仔细核实对方身份，拨打其常用手机号确认，确认消息是否源自好友或联系人，不要随便向陌生账户转账或汇款，谨慎被骗。

十三、【假冒单位领导发微信给员工实施诈骗】

诈骗分子潜入某家企业内部微信群，长期积累各人员信用，刻意模仿企业领导说话方式后，将自己的微信头像改成该企业领导头像，冒充单位领导给事主加其微信好友。事主信以为真，不便拒绝领导，均会照做。不法分子通过微信向事主发出指示，借口自己在外地出差，洽谈业务急需一笔钱，要事主立刻汇款，并三番五次的通过微信催促事主汇款。由于事主担心影响自己工作前途，便会立即汇款给诈骗分子。

网警艾特提示：千万不要轻易相信网络世界中所谓的“老板”，要严格遵守财务制度，按制度审批，当面确认签字，对于用文字提出转账要求，不能轻易相信对方，要通过电话或其他方式核实。

十四、【别让爱心变闹心】

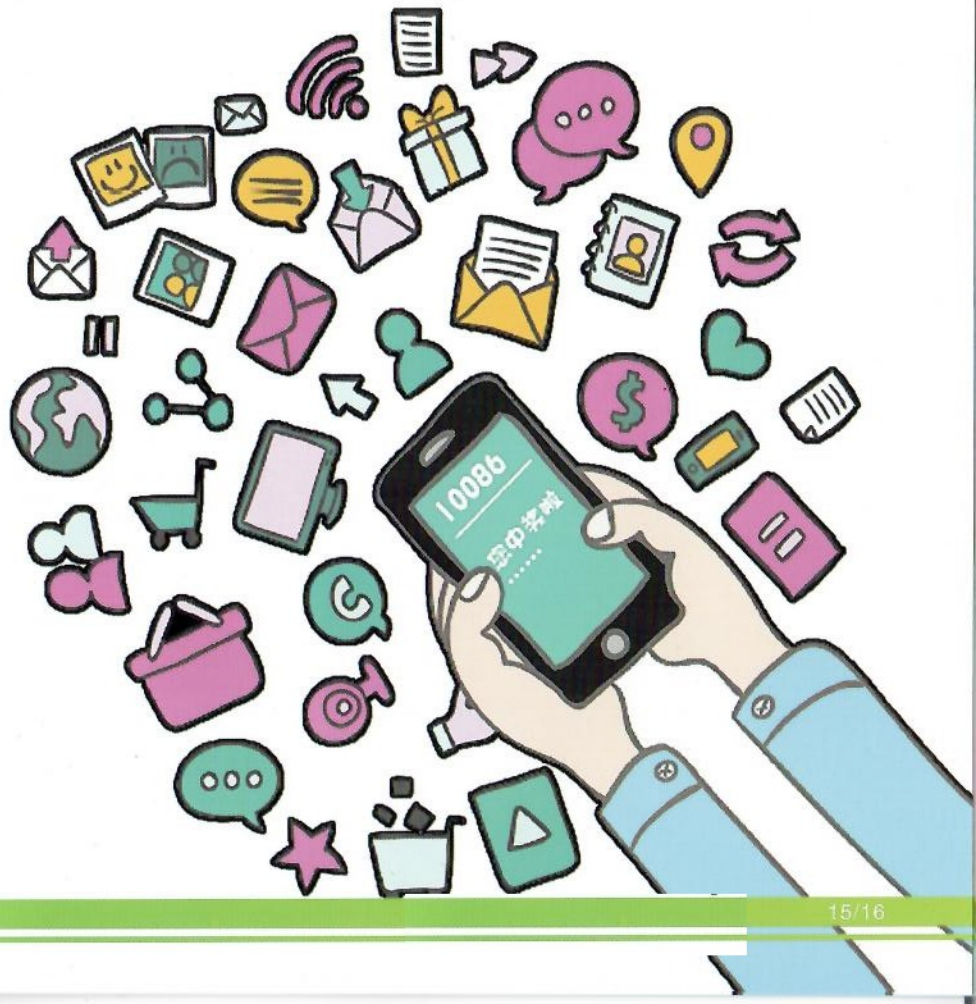
四川汶川地震期间，宋先生收到“四川红十字会”发来的募捐短信，宋先生想到灾区民众真是危难时刻，急需帮助，于是拨打联系电话，询问具体情况。经过对方一番介绍，并听到电话那头传来的孩子哭声时，宋先生消除了疑虑，决定向该银行账号汇款，汇款后当宋先生再次拨打电话咨询情况时，电话变成了关机状态，于是发现被骗。

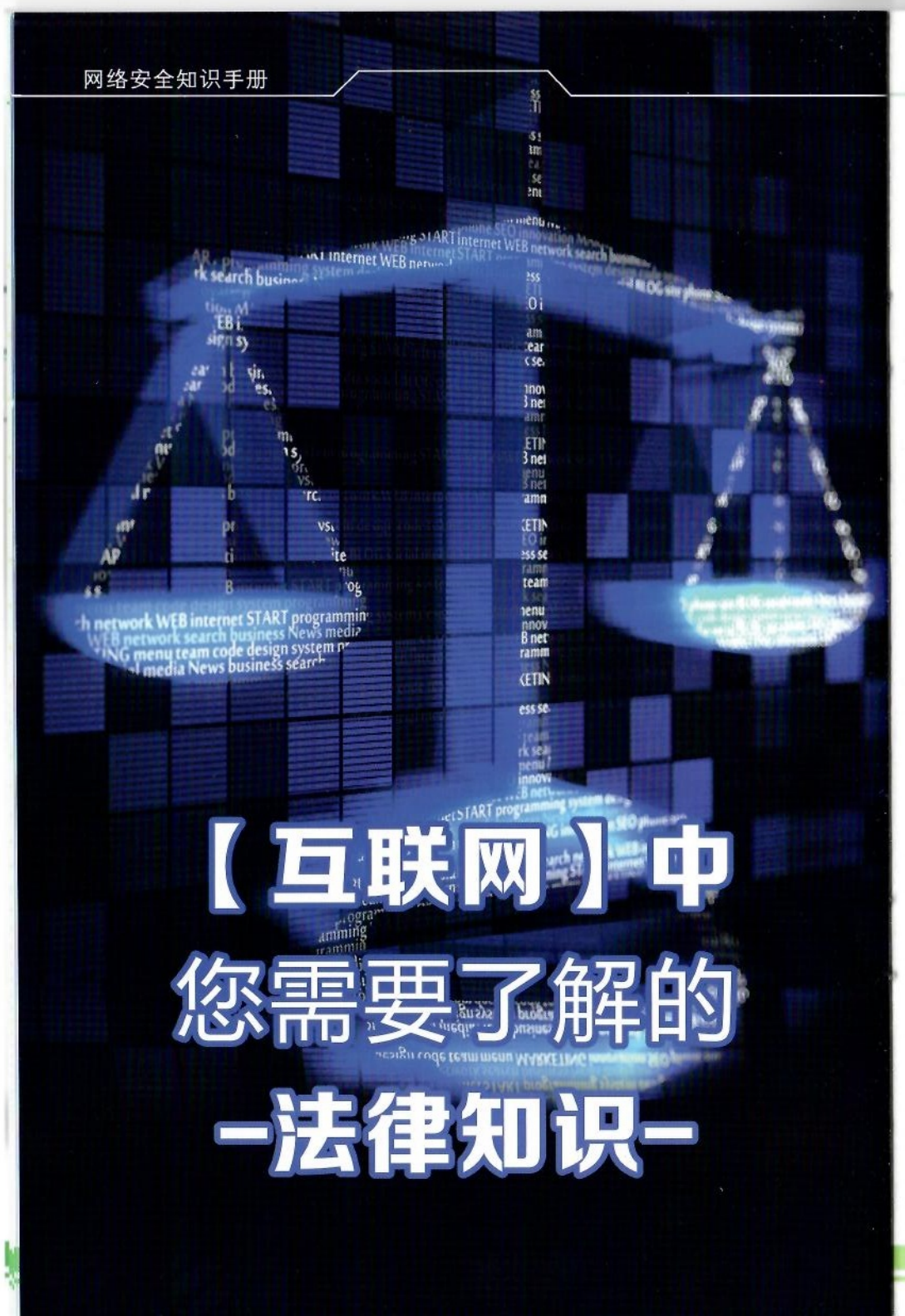
网警艾特提示：在人人都是自媒体的时代里，各类网络、通讯账号鱼龙混杂，不要轻易相信通过手机短信里、电子邮件、即时通信工具接受到的募捐汇款账号或捐款途径。要通过正规部门及正规渠道进行捐款，当重大灾难出现时要特别警惕，发现疑似诈骗信息，请及时联系公安机关，保证自己的爱心不会被“忽悠”成为闹心。

十五、【10086短信也有假?】

市民梁女士收到一天“10086”发送来的短信，短信中写着，只要安装掌上客户端，便可使用移动积分兑换现金。但让梁女士没有想到的是，自己按照短信提示安装客户端后，没过两天银行卡上近1.5万元却被转走了……

网警艾特提示：短信为骗子冒充“10086”所发，内容通常是积分兑换，提示账户不安全。据中国移动官方微博介绍，积分兑换一般是话费、礼品等，绝不会以现金形式、更不会要求用户提供银行账号、身份证号、密码等个人信息。当收到相关短信时，若无法判断真假，应及时拨打运营商客服电话进行确认。





【互联网】中您需要了解的-法律知识-

一、禁止从事哪些危害计算机信息网络安全的活动

《计算机信息网络国际联网安全管理办法》

第五条规定，任何单位和个人不得利用国际互联网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；
（二）煽动颠覆国家政权，推翻社会主义制度的；
（三）煽动分裂国家，破坏国家统一的；
（四）煽动民族仇恨、民族歧视、破坏民族团结的；
（五）捏造或扭曲事实、散布谣言、扰乱社会秩序的；
（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪的；
（七）公然侮辱他人或捏造事实诽谤他人的；
（八）损害国家机关信誉的；
（九）其他违反宪法和法律、行政法规的。

第六条规定，任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或使用计算机信息网络资源的；
（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；
（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；
（四）故意制作、传播计算机病毒等破坏性程序的；
（五）其他危害计算机信息网络安全的。

二、诽谤

（一）网上的那些行为属于“捏造事实诽谤他人”？

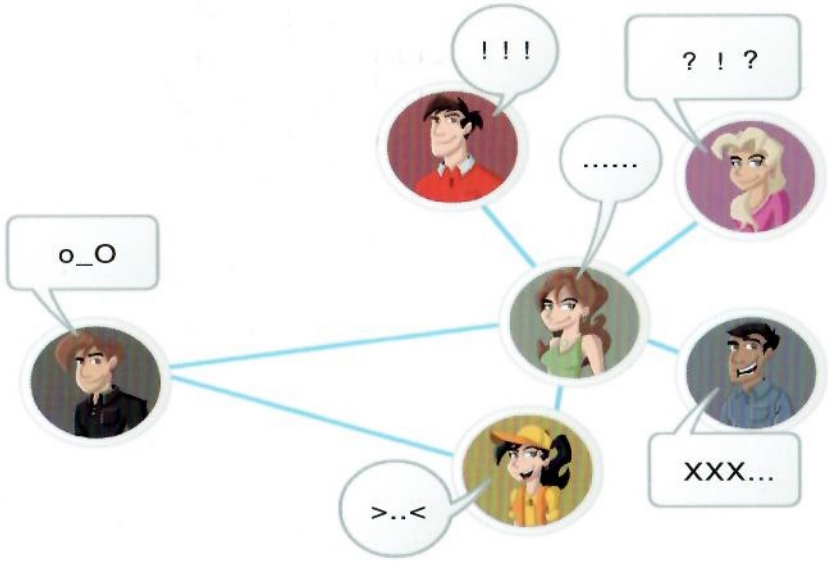
1.捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；
2.将信息网络上涉及他人的原始信息内容改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；
3.明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的。

（二）利用信息网络诽谤他人，在什么情形下，构成诽谤罪（自诉）？

1.同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的；
2.造成被害人或者其近亲属精神失常、自残、自杀等严重后果的；
3.两年内曾因诽谤受过行政处罚，又诽谤他人的；
4.其他情节严重的情形。

（三）利用信息网络诽谤他人，在什么情形下，构成诽谤罪（公诉）？

1.引发群体性事件的;
2.引发公共秩序混乱的;
3.引发民族，宗教冲突的;
4.诽谤多人，造成恶劣社会影响的;
5.损害国家形象，严重危害国家利益的;
6.造成恶劣国际影响的;
7.其他严重危害社会秩序和国家利益的情形;



三、寻衅滋事

网上何种行为构成寻衅滋事罪

利用信息网络辱骂、恐吓他人、情节严重、破坏社会秩序的。

编造虚假信息，或是明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的。

四、敲诈勒索

网上何种行为会被认定为敲诈勒索罪?

以在信息网络上发布、删除等方式处理网络信息为由，威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的。

五、非法经营

（一）网上何种信息处置行为会被认定为非法经营行为?

违反国家规定，以营利为目的，通过信息网络有偿提供删除信息服务，或者明知是虚假消息，通过信息网络有偿提供发布信息等服务，扰乱市场秩序的。

（二）上述行为在什么情形下构成非法经营罪?

1.个人非法经营数额在五万元以上，或者违法所得数额在两万元以上的;
2.单位非法经营数额在十五万元以上，或者违法所得数额在五万元以上的；实施前款规定的行为，数额达到前款规定的数额五倍以上的，应当认定为刑法第二百二十五条规定的“情节特别严重”。

六、危害计算机信息系统安全罪

（一）第二百八十五条【**非法侵入计算机信息系统罪**】违反国家规定，侵入国家事务，国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

【**非法获取计算机信息系统数据、非法控制计算机信息系统罪**】违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

【**提供侵入、非法控制计算机信息系统程序、工具罪**】提供专门用于侵入、非法控制计算机信息系统的程序、工具、或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

（二）第二百八十六条【**破坏计算机系统罪**】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役，后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

查询、举报常用网站

类别	机构名称	网址
服务机构	国家互联网应急中心	http://www.cert.org.cn/
	国家计算机病毒应急处理中心	http://www.antivirus-china.org.cn/
	中国信息安全测评中心	http://www.itsec.gov.cn/
	中国国家信息安全漏洞库	http://www.cnnvd.org.cn/
	工信部ICP/IP地址/域名信息备案管理系统	http://www.miitbeian.gov.cn/
违法和不良信息举报	中国互联网违法和不良信息举报中心	http://net.china.com.cn
	中国互联网协会反垃圾信息中心	http://www.12321.org.cn/
	网络违法犯罪举报网站	http://www.cyberpolice.cn/wfjp
	网络不良与垃圾信息举报受理中心	http://www.12321.cn/
	UNT统一信任网络	http://www.trustutn.org/
	网络社会诚信网	http://www.zx110.org/