网络安全

知识手册

目 录

一、安全法律法规解读

1.1 《网络安全法》解读

《中华人民共和国网络安全法》（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。

1.1.1《网络安全法》的基本原则

1）网络空间主权原则。网络空间主权是国家主权在网络空间中的自然延伸和表现，没有网络安全，就没有国家安全。

2）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”。

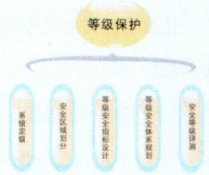
3）共同治理原则。网络空间安全保护需要政府、企业、社会组织、技术社群和公民等网络利益相关者的共同参与。

1.1.2《网络安全法》禁止的网络行为

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，合理的处理方法，向网信、电信、公安等部门举报。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，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。

1.2 《网络安全等级保护制度 2.0》介绍



2019 年 5 月 13 日，网络安全等级保护制度 2.0 标准正式发布，标志着国家网络安全等级保护工作步入新时代（简称“等保 2.0 标准”）。等级保护制度已被打造成新时期国家网络安

全的基本国策和基本制度。应急处置、灾难恢复、通报预警、安全监测、综合考核等重点措施全部纳入等保制度并实施，对重要基础设施、重要系统以及“云、物、移、大、工控”纳入等保监管，将互联网企业纳入等级保护管理。

与 1.0 相比，等保 2.0 标准内涵更加丰富，等级保护对象由原来的“信息系统”改为“等级保护对象（网络和信息系统）”，安全等级保护对象包括基础信息网络（广电网、电信网等）、信息系统（采用传统技术的系统）、云计算平台、大数据平台、移动互联、物联网和工业控制系统等。新版安全要求在原有通用安全要求的基础上新增安全扩展要求，安全扩展要求主要针对云计算、移动互联、物联网和工业控制系统提出了特殊安全要求。

除进行 1.0 时代网络定级及备案审核、等级测评、安全建设整改、自查等规定动作外，还增加了测评活动安全管理、网络服务管理、产品服务采购使用管理、技术维护管理、监测预警和信息通报管理、数据和信息安全保护要求、应急处置要求等内容。

1.3 《公安机关互联网安全监督检查规定》解读

2018 年 11 月 1 日，《公安机关互联网安全监督检查规定》（公安部 151 号令）（以下简称《规定》）正式实施。《规定》的出台，既是公安机关依法履职、提升网络社会管控能力、服务经济社会发展的现实要求，又有助于督促互联网企业全面落实法定义务，防控网络风险，营造清朗稳定安全的网络空间。

1.3.1 检查监督人员

（1）县（区）公安（分）局网安大队即可实施检查。互联网安全监督检查工作由县级以上地方人民政府公安机关网络安全保卫部门组织实施。【《规定》第三条第一款】

（2）由单位的网络管理机构所在地和个人经常居住地公安机关实施。互联网安全监督检查由互联网服务提供者的网络服务运营机构和联网使用单位的网络管理机构所在地公安机关实施。互联网服务提供者为个人的，可由其经常居住地公安机关实施。【《规定》第八条】

1.3.2 监督检查方式

公安机关开展互联网安全监督检查，可以采取现场监督检查或者远程检测的方式进行。【《规定》第十三条】

（1）现场监督检查。公安机关开展互联网安全现场监督检查，可按需要采取以下措施：

1）进入营业场所、机房、工作场所；

2）要求监督检查对象的负责人或者网络安全管理人员对监督检查事项作出说明；

3）查阅、复制与互联网安全监督检查事项相关的信息；

4）查看网络与信息安全保护技术措施运行情况。【《规定》第十五条】

（2）远程检测。公安机关对互联网服务提供者和联网使用单位是否存在网络安全漏洞，可以开展远程检测。【《规定》第十六条第一款】

（3）监督检查可委托第三方。公安机关开展现场监督检查或者远程检测，可以委托具有相应技术能力的网络安全服务机构提供技术支持。【《规定》第十七条第一款】

1.3.3 监督检查对象

（1）四类监督检查对象。公安机关应当根据网络安全防范需要和网络安全风险隐患的具体情况，对下列互联网服务提供者和联网使用单位开展监督检查：

1）提供互联网接入、互联网数据中心、内容分发、域名服务的；

2）提供互联网信息服务的；

3）提供公共上网服务的；

4）提供其他互联网服务的。【《规定》第九条第一款】

（2）三类重点监督检查对象。对第九条第一款规定的服务未满一年的，两年内曾发生过网络安全事件、违法犯罪案件的，或者因未履行法定网络安全义务被公安机关予以行政处罚的，应当开展重点监督检查。【《规定》第九条第二款】

（3）一类特殊监督检查对象。对防范恐怖袭击的重点目标的互联网安全监督检查，按照前款规定的内容执行。【《规定》第十二条第二款】

1.4 其他法律知识

1. 网上的哪些行为会被认定为《刑法》第二百四十六条第一款规定的“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篡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，以“捏造事实诽谤他人”论。

2. 利用信息网络诽谤他人，在什么情形下，应当认定为《刑法》第二百四十六条第一款规定的“情节严重”？

（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。

3. 利用信息网络诽谤他人，在什么情形下，应当认定为《刑法》第二百四十六条第二款规定的“严重危害社会秩序和国家利益”？

（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。

4. 网上何种行为会被认定为寻衅滋事罪？

利用信息网络辱骂、恐吓他人，情节恶劣、破坏社会秩序的，依照刑法第二百九十三条第一款第（二）项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者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，依照刑法第二百九十三条第一款第（四）项的规定，以寻衅滋事罪定罪处罚。

5. 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，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

6. 网上何种行为会被认定为非法经营罪？

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，或者明知是虚假信息，通过信息网络有偿提供发布信息等服务，扰乱市场秩序，属于非法经营行为“情节严重”，依照刑法第二百二十五条第（四）项的规定，以非法经营罪定罪处罚。

7. 非法经营认定的数额标准是多少？

（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”。

8. 明知他人利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪，为其提供资金、场所、技术支持等帮助的，会构成什么性质的犯罪？

以共同犯罪论处。

9. 国家对经营性和非经营性互联网信息服务分别采取什么管理制度？

国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度。未取得许可或者未履行备案手续的，不得从事互联网信息服务。

10. 互联网新闻信息及新闻信息服务包括哪些？

新闻信息是指时政类新闻信息，包括有关政治、经济、军事、外交等社会公共事务的报道、评论，以及有关社会突发事件的报道、评论。互联网新闻信息服务包括通过互联网登载新闻信息、提供时政类电子公告服务和向公众发送时政类通讯信息。

11. 现行《刑法》中，专门规定了哪两个关于计算机犯罪的罪名？

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。

第二百八十六条【破坏计算机信息系统罪】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。

12. 利用计算机或计算机网络实施的犯罪行为在《刑法》中如何定罪？

利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。该条规定的犯罪侵害客体比较广泛，包括公司财产或国家秘密的拥有权等。

二、计算机与网络安全常识

2.1 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。原来发布的软件存在缺陷，发现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。

7. 如何设置 windows 操作系统开机密码？

按照先后顺序，依次使用鼠标点击“开始”菜单中的“控制面板”下的 “用户账户”，选择账户后点击“创建密码”，输入两遍密码后，按“创建密码”按钮即可。

8. 为什么不要打开来历不明的网页、电子邮件链接或附件？

互联网上充斥着各种钓鱼网站、病毒、木马程序。不明来历的网页、电子邮件链接、附件中，很可能隐藏着大量的病毒、木马，一旦打开，这些病毒、木马会自动进入电脑并隐藏在电脑中，会造成文件丢失损坏甚至导致系统瘫痪。

9. 接入移动存储设备（如移动硬盘和 U 盘）前，为什么要进行病毒扫描？

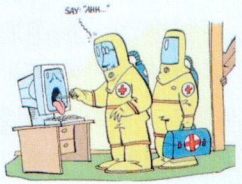
外接存储设备也是信息存储介质，所存的信息很容易带有各种病毒，如果将带有病毒的外接存储介质直接接入电脑，很容易将病毒传播到电脑中。

10. Cookies 会导致怎样的安全隐患？

当用户访问一个网站时，Cookies 将自动储存于用户 IE 内，其中包含用户访问该网站的种种活动、个人资料、浏览习惯、消费习惯，甚至信用记录等。这些信息用户无法看到，当浏览器向此网址的其他主页发出 GET 请求时，此 Cookies 信息也会随之发送过去，这些信息可能被不法分子获得。为保障个人隐私安全，可以在 IE 设置中对 Cookies 的使用做出限制。

2.2 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的文件夹（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．如何防范网络虚假、有害信息？

（1）及时举报疑似谣言信息；

（2）不造谣、不信谣、不传谣；

（3）注意辨别信息的来源和可靠度，通过经第三方可信网站认证的网站获取信息；

（4）注意打着“发财致富”、“普及科学”、传授“新技术”等幌子的信息；

（5）在获得相关信息后，应先去函或去电与当地工商、质检等部门联系，核实情况。

3．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；

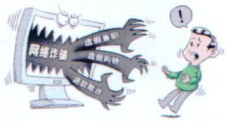
（2）不要轻意点击未经核实的链接；

（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。

4．当前网络诈骗类型及如何预防？

网络诈骗类型可大致概括为四种：



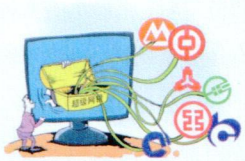
一是利用QQ盗号和网络游戏交易进行诈骗，冒充好友借钱；

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。

5．如何保护网银安全？



网上支付的安全威胁主要表现在以下三个方面：一是密码被破解，很多用户或企业使用的密码都是“弱密码”，且在所有网站上使用相同密码或者有限的几个密码，易遭受攻击者暴力破解；二是病毒、木马攻击，木马会监视浏览器正在访问的网页，获取用户账户、密码信息或者弹出伪造的登录对话框，诱骗用户输入相关密码，然后将窃取的信息发送出去；三是钓鱼平台，攻击者利用欺骗性的电子邮件和伪造的Web站点来进行诈骗，如将自己伪装成知名银行或信用卡公司等可信的品牌，获取用户的银行卡号、口令等信息。

保护网银安全的防范措施如下：

（1）尽量不要在多人共用的计算机（如网吧等）上进行银行业务，发现账号有异常情况，应及时修改交易密码并向银行求助；

（2）核实银行的正确网址，安全登录网上银行，不要随意点击未经核实的陌生链接；

（3）在登录时不选择“记住密码”选项，登录交易系统时尽量使用软键盘输入交易账号及密码，并使用该银行提供的数字证书增强安全性，核对交易信息；

（4）交易完成后要完整保存交易记录；

（5）网上银行交易完成后，应点击“退出”按钮，使用U盾购物时，交易完成后要立即拔下U盾；

（6）对网络单笔消费和网上转账进行金额限制，并为网银开通短信提醒功能，在发生交易异常时及时联系相关客服；

（7）通过正规渠道申请办理银行卡及信用卡；

（8）不要使用存储额较大的储蓄卡或信用额度较大的信用卡开通网上银行；

（9）支付密码最好不要使用姓名、生日、电话号码，也不要使用12345等默认密码或与用户名相同的密码；

（10）注意保护自己银行卡信息资料，不要把相关资料随便留给不熟悉的公司或个人。

6．如何准确访问和识别党政机关、事业单位网站？

按照党政机关、事业单位网站与其实体名称对应、网络身份与实体机构相符的原则，国家专门设立“.政务”和“.公益”中文域名，由工业和信息化部授权中央编办电子政务中心负责注册管理。

（1）通过中文域名访问党政机关、事业单位网站

“.政务”和“.公益”域名是党政机关和事业单位的专用中文域名，其注册、解析均由机构编制部门进行严格审核和管理。通过在浏览器地址栏输入“.政务”和“.公益”中文域名，可准确访问党政机关和事业单位网站。

（2）通过查看网站标识识别党政机关和事业单位网站

网站标识是经机构编制部门核准后统一颁发的电子标识，该标识显示在网站所有页面底部中间显著位置。点击该标识，即可查看到经机构编制部门审核确认的该网站主办单位的名称、机构类型、地址、职能，以及网站名称、域名和标识发放单位、发放时间等信息，以确认该网站是否为党政机关或事业单位网站。网站标识分为党政机关和事业单位两类。

三、常见风险与典型案例

3.1 常见安全风险

3.1.1 网络钓鱼

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。受害者经常遭受显著的经济损失或全部个人信息被窃取并用于犯罪的目的。

3.1.2 木马病毒

特洛伊木马是一种基于远程控制的黑客工具，它通常会伪装成程序包、压缩文件、图片、视频等形式，通过网页、邮件等渠道引诱用户下载安装，如果用户打开了此类木马程序，用

户的电脑或手机等电子设备便会被编写木马程序的不法分子所控制，从而造成信息文件被修改或窃取、电子账户资金被盗用等危害。

3.1.3 社交陷阱

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。

3.1.4 伪基站

“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。

3.1.5 信息泄露

目前某些中小型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。

3.2 经典案例

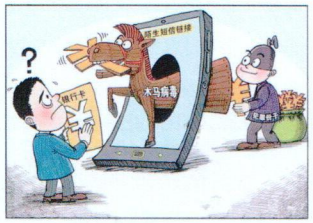
案例 1：远程协助

陈某在一家网店购买一台标价为 3200 元的笔记本电脑，但因操作失误多付了一次款。因退款心切，在客服的要求下，陈某加了对方 QQ，让对方远程操控自己的电脑“帮助退款”，结果被对方分 3 次转走一万余元。

安全提示：

• 千万不要让陌生人远程操作你的电脑。因为一旦启动远程操控，任何人都可以在异地通过网络控制你的电脑。另外，网购交易需要加 QQ 沟通的，往往是诈骗。

案例 2：钓鱼链接



刘同学收到某银行官方号码“95×××”发来的短信，提示她银行卡积分将于近期到期，建议尽快登录某网站兑换礼品，并附上了网站链接。刘同学完全没有质疑该网址的可靠性，直接通过手机登录，并按照要求输入了个人信息、账号及密码。不久，她就收到银行发来的短信，提示她的银行卡被取现 4000 元。

安全提示：

• 不要轻易点击任何信息发来的链接、获奖等信息，应当搜索官方渠道确认后，再进行操作。

案例 3：校园贷

河南省一名大二学生因赌球而债台高筑，但自身无力偿还而选择轻生。据了解，该学生利用几十名同学的身份信息，先后在名校贷、优分期、趣分期等众多网络平台贷款近百万元并用来赌球。不幸的是，贷款全部输光，他也因此欠下巨债，而父亲一辈子积蓄只有 7 万元。

安全提示：

• 大学生个人要坚决抵制网络赌博行为，要洁身自好，不贪违法钱，拒绝校园贷，培养高尚情操。一旦发现此类网站要及时向公安部门举报，杜绝网络洗钱、赌博的乱象。

案例 4：低价陷阱

2018 年 1 月，某高校徐同学无意中进入一个买卖二手自行车的网址，发现其中一辆名牌车只要 500 元。徐同学心动不已，随即联系网站客服，按照对方要求填写信息并通过网银转账 200 元订金。2 天后，对方告知押车员已将车子运送至收货地址的仓库，要求小徐支付余款 300 元。小徐打款后兴冲冲等着去提车，结果对方又找各种理由要求他再付 500，小徐

这才恍然大悟自己是被骗了。

安全提示：

• 网上购物请选择正规网站，不要轻信虚假网站、QQ、论坛等发布的所谓超低价促销信息。此外，要求通过银行等直接汇款的 9 成以上为诈骗，务必警惕。

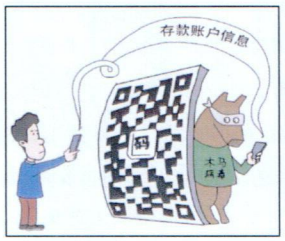
案例 5：兼职“刷信誉”

去年暑期，琳琳在微信群里看到一则兼职赚佣金的广告，一时心动，她加了对方微信，填了“兼职申请表”。随后，被所谓 8% 的佣金所诱惑，在对方的步步引导下，琳琳陆续刷了 120 单游戏充值卡，直到卡里钱刷完。可是琳琳左等右等都没有等到返款到账消息，而对方的微信联系不上了！琳琳这才恍然大悟，钱没赚到，反而被骗了几千块钱。

安全提示：

• 仅通过微信或者电话联系的招聘往往是诈骗，需要你先掏钱的往往更是诈骗。这些需要“刷信誉”的网站实际上都是一些无法退款的虚拟商品交易网站，一旦被骗，投诉无门。

案例 6：扫描二维码送奖品



不法分子利用学生防范心理弱的特点，诱导学生扫二维码，学生在不知情的情况下，登录预设网站自动下载木马病毒，导致个人信息，网银密码等被盗窃。学生小王在某个音乐会的场外因为贪图送的小礼品扫描了陌生的二维码，结果回到家发现自己的支付宝被五次盗刷，总共被盗走 1500 元，等到发现的时候已经晚了。

安全提示：

• 面对扫描二维码打折优惠促销等活动，要提高警惕，不要见码就扫，建议在手机上安装防病毒安全软件。

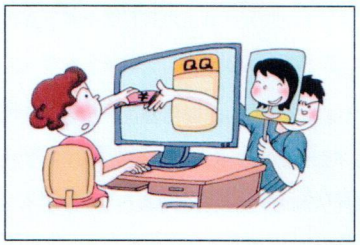
案例 7：办理各种证书诈骗

葛同学用手机上网时，看到一个自称可办理计算机二级合格证书、英语四级合格证书的帖子，其保存对方手机号码并添加微信。当日，葛同学就接到自称办理计算机二级合格证书、英语四级合格证书操作人贾老师打来的电话和发来的微信，对方要求葛同学缴纳 1000 元操作费、3000 元办证费、50 元寄递费、600 元订金。葛同学按对方指示成功缴纳订金后，贾某瞬间将葛同学微信拉黑，此时葛同学拨打贾某电话已处于关机状态。

安全提示：

• 此类案件，嫌疑人主要通过打电话、发短信、网络传播等渠道，以办理各种合格证书为理由，向被害人收取各种手续费、服务费，大学生要警惕这些作案手法，提高警觉性，以正当的途径获取证书与奖励。

案例 8：QQ 上谈钱

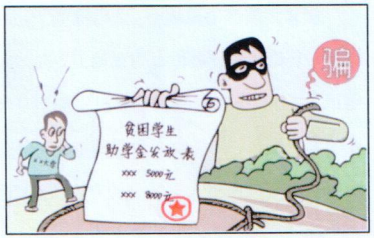


小飞在家上网时，QQ 上一个同学发来信息，说朋友要还自己钱，但自己卡掉了，想先把钱转小飞卡上，然后再由小飞转给他。小飞答应了，对方又说汇钱需要银行卡号、身份证及联系电话，小飞又全部告诉了对方。过了几分钟，小飞手机收到一个验证码，对方称只要告诉他这个验证码，钱就能到账了，小飞没细想就告诉了他。直到收到银行短信通知，小飞才发现自己卡里被消费了 2200 元。

安全提示：

• 无论是给你打钱还是向你借钱，如在网上提出钱财交易请求，即便有视频画面也不要轻信，务必先打电话确认；同时要牢记，手机上收到的验证码，千万不能随意泄漏。

案例 9：贫困助学诈骗



2016 年，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 元学费汇入一个指定账号，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。

安全提示：

• 凡是谈到银行账户信息的，一律挂掉；

• 凡是谈到中奖的，一律挂掉；

• 凡是谈到“电话转接公检法”的，一律挂掉；

• 凡是自称领导、同事要求汇款的，一律不管；

• 凡是告知“家属”出事需要先汇款的，一律不管。

案例 10：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。张先生等了几天，说好的话费却迟迟没有到账，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。

安全提示：

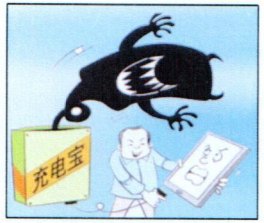
• 发现手机信号突然中断，应提高警惕，因为靠近伪基站时，手机一般会脱网，几秒后才恢复正常；

• 当收到 “中奖、转账”等短信时，一定要提高警惕，不要轻易点击短信中的链接，更不要转账汇款；

• 不要轻信各种积分兑换，正常的积分兑换应通过官方渠道；

• 手机要安装安全防护软件，它们可以有效拦截垃圾短信。

案例 11：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。

案例 12：免费 WiFi 接入、私搭 WiFi 热点

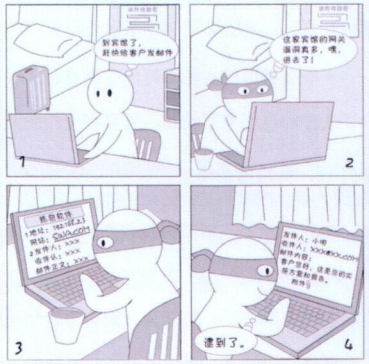
不法分子搭建与常用 WiFi 相同或相近的 WiFi，设置空密码或者相同密码吸引公众连接，然后在 WiFi 路由器上劫持 DNS（域名系统），将用户引入到钓鱼网站获取账号密码，或者在路由器上监听手机流量，获取明文密码。

无线路由器有较多的安全隐患，比如，之前的 WEP 认证能很轻易破解。个人架设无线路由器，如果配备不当会导致蹭网或个人资料泄露，在公司使用可能导致内网被入侵，公司机密、客户资料泄露，后果不堪设想。

安全提示：

- 公共场合连接 WiFi 时请同商家确认好 WiFi 名称；
- 没有密码的公共 WiFi 慎用；
- 使用支付 APP 时，尽量使用运营商的 4G 网络；
- 在办公网络架设无线路由器必须经过公司批准并进行安全安装；
- 认证方式使用安全的 WPA2；
- 建议隐藏 SSID（服务集标识），绑定接入设备的 MAC 地址；
- WiFi 密码必须八位数以上，包含大小写、数字和标点符号，定期修改密码。

案例 13：邮件传输拦截

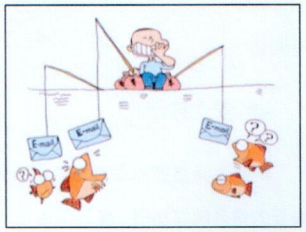


一些宾馆或公共网络的安全性较差，黑客很容易入侵到其网关设备并监控网络流量，如果收发邮件没有加密，黑客抓到这些数据包后很容易还原出邮件正文和附件。

安全提示：

- 收发敏感邮件时要确保传输通道是加密的；
- WEB 邮箱的传输是否加密要看 URL（网页地址）是 HTTP 还是 HTTPS，带 S 说明是加密传输；
- 用邮件客户端的加密设置一般为在发送和接收服务器设置处勾选 SSL。

案例 14：邮件病毒与钓鱼附件



钓鱼邮件种类繁多，利用邮件骗取回复敏感信息是最简单和常见的钓鱼方式。流行的勒索病毒邮件多为英文邮件，主题和正文诱导用户打开附件。这种病毒对文档的加密强度很高，可以说是无法破解，只有付款才能解密文档。

安全提示：

- **望**：看邮件发件人地址、签名等信息，是否是你的熟人，是否是系统邮箱，是否是可疑的地址
- **闻**：多听周围人的看法，骗子不会骗到所有人
- **问**：打电话与相关人员直接确认是最保险的
- **切**：懂一些电脑的技术人员可以查一下发件人的真实 IP 地址、分析一下邮件头内容

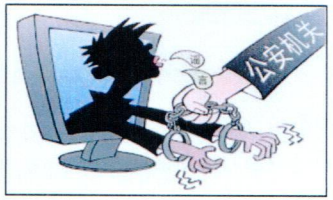
另外

- 必须要装但不要完全相信防病毒软件；

• 确保自己的邮件客户端禁止访问执行文件，可以自己给自己发一个.exe 后缀的文件测试一下；

• 所有类型的文件都可能带病毒，不仅仅是 exe/js/bat 为后缀的可执行文件，非可执行文件的利用难度较高，需要利用相关漏洞。

案例 15：传播虚假信息



2009 年 7 月，雷某在打工期间，经常到网吧上网，为了增加其注册的 QQ 空间的点击量，竟然在自己的空间里撰写了一篇题为“阳春市松柏镇惊现人吃人事件”的帖子，导致该帖子在互联网上被迅速大量传播，至案发时止，共有 148 个转贴，165260 人点击浏览，在社会上造成了极坏的影响，在阳春当地也引起了恐慌，引起了广东省政府和阳春市政府的高度重视，有关部门经过核查，确认雷某的帖子纯属虚构，公安机关将其抓获，随后阳春市法院经审理后对雷某作出判决，被当地法院以故意编造传播虚假信息罪判处二年有期徒刑。

安全提示：

网络不是虚拟而是真实存在的信息交流平台，看似个人、私人的“空间”，却是开放、公开的信息网络场所，任何网络行为都会留下痕迹，雷某任意散播虚假信息的行为，造成了极坏的影响，引起了恐慌，获故意编造传播虚假信息罪。

案例 16：传播淫秽色情内容

2014 年 7 月，成都市公安局网监处在工作中发现，某高校的校园网上一个人的主页非法链接有境外的淫秽色情网站，经查，该网站为成都某大学校园网免费个人主页，建立人系该校 2002 级学生章某，他在网站主页“X-Rate 色情”栏目中提供境外“激情电影下载”、“激情电影与图片”、“电影自动搜索软件”、“色猫网”、“色情综合”、“寻找美女”等淫秽色情链接内容，造成了极坏的影响。案侦民警依法对章某进行了传唤，据章某交待，他利用学校分配给自己的校园网免费个人空间建立了个人主页，并在教育网一论坛上获取了相关境外淫秽色情网站的网址，然后链接在自己的个人主页上，成都市公安局

依据《治安管理处罚条例》，对章某处以治安处罚，受到拘留处罚的章某十分懊悔，他说，当时链接这些淫秽色情网站，只是一时冲动，图好玩，自己根本不知道公安机关现在正在打击淫秽色情网站，更不知道自己做了违法的事。

安全提示：

大学生利用校园网传播淫秽色情内容，居然还不知道自己已经违法的事件，令人震惊。目前，全国打击淫秽色情网站专项行动明确要求，对于建立淫秽网站、网页，提供涉及未成年人淫秽信息、利用青少年教育网络从事淫秽色情活动以及顶风作案、罪行严重的犯罪分子，坚决依法从重打击。

案例 17：购买个人信息

电信诈骗案件频发，浙江宁波一家教育机构因购买上万条学生信息开展电话营销，而被处以罚款 25 万元的行政处罚。该案也成为全省第一起侵犯消费者个人信息的案件。宁波市市场监管局对此做出重罚：海曙区纳思教育科技有限公司因侵犯“消费者个人信息得到保护的权利”，责令当事人改正并罚款 25 万元的行政处罚。

安全提示：

《网络安全法》明确规定，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。

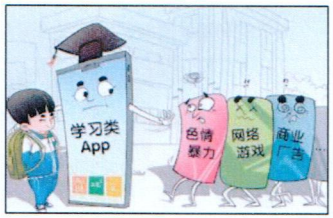
案例 18：黑入高校教务系统篡改成绩

利用高校教务系统 SQL 漏洞取得管理员权限，远程帮助在校学生修改考试成绩并收取酬劳——四川某高校大四毕业生自以为找到了一条生财之路，却因此葬送了自己的前程。近日，崇州市法院审理了该市首例破坏计算机信息系统案，被告人闫某被判处有期徒刑 5 年。

安全提示：

《中华人民共和国刑法》第二百八十六条 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。

案例 19：查处传播有害信息网站和 APP



2019 年 1 月，根据江苏省“扫黄打非”办公室转办线索，昆山“扫黄打非”部门开展查处。经查，2017 年 4 月以来，昆山某公司未获许可开发运营网站和 APP，刊载部分网络小说含有危害社会公德及含有诱发未成年人模仿违反社会公德的内容。目前，“作业神助手”APP 被责令改正违法行为，“红果阅读”网站和 APP 被关停，两公司被处以罚款的行政处罚。

安全提示：

教育 APP 是以教职工、学生、家长为主要用户，以教育、学习为主要应用场景，服务于学校教学与管理、学生学习与生活以及家校互动等方面的 APP。

案例 20：未落实网络安全管理制度

淮南市公安局网安支队经过现场勘验和调查确认淮南某职业技术学院招生信息管理系统因存在越权漏洞，后台登陆密码弱口令，学校未落实网络安全管理制度，未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的 4353 名学生的身份信息泄露。

安全提示：

国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

• 制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

• 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

• 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

• 采取数据分类、重要数据备份和加密等措施；

• 法律、行政法规规定的其他义务。

四、安全攻略及措施

4.1 保管好账号、密码

• 不要相信任何套取账号和密码的行为，也不要轻易向他人透露您的证件号码、账号、密码等；

• 密码应尽量设置为数字、英文大小写字母的组合，不要用生日、姓名等容易被猜测的内容做密码；

• 如果泄露了密码，应尽快办理补发或更换业务。

4.2 认清网站网址

• 网上购物时请到正规、知名的网上商户进行网上支付，交易时请确认地址栏里的网址是否正确。

4.3 确保计算机系统安全

• 从银行官方网站下载安装网上银行、手机银行安全控件和客户端软件；

• 设置 Windows 登录密码，WindowsXP 以上系统请打开系统自带的防火墙，关闭远程登录功能；

• 定期下载并安装最新的操作系统和浏览器安全补丁；

• 安装防病毒软件和防火墙软件，并及时升级更新。

4.4 提升安全意识

• 使用经国家权威机构认证的网银证书，建议同时开通 USB Key 和短信口令功能；

• 开通短信口令时，务必确认接收短信的手机号码为本人手机号码；

• 不要轻信手机接收到的中奖、贷款等短信、电话和非银行官方网站上的任何信息；

• 不要轻信假公安、假警官、假法官、假检察官等以“安全账户”名义要求转账的电话欺诈；

• 避免在公共场所或他人计算机上登录和使用网上银行。退出网上银行或暂时离开电脑时，一定要将 USB Key 拔出；

• 操作网银时建议不要浏览别的网站，有些网站的恶意代码可能会获取您电脑上的信息；

• 建议对不同的电子支付方式分别设置合理的交易限额，每次交易都请仔细核对交易内容，确认无误后再进行操作。在交易未完成时不要中途离开交易终端，交易完成后应点击退出；

• 定期检查核对网上银行交易记录。可以通过定制银行短信提醒服务和对账邮件，及时获得银行登录、余额变动、账户设置变更等信息提醒。

五、知识问答

5.1 如何防范 QQ、微博等账号被盗？

- 账户和密码尽量不要相同，定期修改密码；
- 密码增加复杂度，尽量由大小写字母、数字和其他字符混合组成；
- 不同用途的网络应用，应该设置不同的用户名和密码；
- 防止网吧账号被侦听，可先输部分账户名、部分密码，再输剩余账户名、密码；
- 涉及网络交易时，要注意通过电话与交易对象本人确认。

5.2 如何防范病毒或木马的攻击？

- 为电脑安装杀毒软件，定期扫描系统，查杀病毒；及时更新木马库，更新系统补丁；
- 下载软件时尽量到软件相应的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；
- 请勿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；
- 使用网络通信工具时不随意接收陌生人的文件。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；
- 对公共磁盘空间加强权限管理，定期查杀病毒；

- 需要从互联网等公共网络上下载资料转入内网计算机或涉密计算机时，用刻录光盘的方式实现转存；
- 定期备份，当遭到病毒严重破坏后能迅速修复。

5.3 如何安全使用电子邮件？

- 不要随意点击来历不明邮件中的链接、图片、文件；
- 使用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密码；
- 当收到与个人信息、金钱相关的邮件时要提高警惕；
- 适当设置找回密码的提示问题。

5.4 如何防范钓鱼网站？

- 通过查询网站备案信息等方式核实网站资质真伪；
- 警惕中奖、修改网银密码的通知，不轻易点击陌生链接；
- 不在网吧等多人共用的电脑上进行金融业务操作。

5.5 如何防范假冒网站？

- 直接输入所要登录网站的网址，不通过其他链接进入；
- 登录网站后留意核对所登录的网址与官方公布的网址是否相符；
- 登录官方发布的相关网站辨识真伪；
- 安装防护软件，及时更新补丁；
- 收到邮件、短信、电话等要求到指定网页修改密码时务必警惕。

5.6 如何保护网银安全？

- 核实银行正确网址，安全登录网站银行；
- 登录时不选择 “记住密码” 选项；
- 交易完成后要完整保存交易记录；
- 网银交易完成后点击“退出”按钮，使用完 U 盾立即取下；
- 对网络单笔消费和网上转账进行金额限制，开通网银短信提醒；

- 不要使用存储额较大储蓄卡或信用额度较大信用卡开通网银；
- 支付密码最好不用生日、姓名拼音、电话号码等。

5.7 如何保障无线上网安全？

- 请勿见到免费 WiFi 就用，而是要用可靠的 WiFi 接入点；关闭自己手机和平板电脑等设备的无线网络自动连接功能，仅在需要的时候开启；
- 警惕公共场所免费的无线信号为不法分子设置的钓鱼陷阱，尤其是一些和公共场所内已开放的同名的 WiFi 信号；
- 在公共场所使用陌生的无线网络时，尽量不要进行与资金有关的银行转账以及支付宝支付；
- 修改无线路由器默认管理员用户名密码，将家中的无线路由器的密码设置的复杂一些，并采用强密码，最好应是字母、数字的组合；
- 启用 WPA/WEP 加密，修改默认 SSID，关闭 SSID 广播，启用 MAC 地址过滤；
- 无人使用时关闭无线路由器电源。

5.8 如何安全使用智能手机？

- 不要轻易打开陌生人通过手机发送的链接和文件；
- 为手机设置访问密码是保护手机安全的第一道防线，以防智能手机一旦丢失时，犯罪分子可能会获得其中有的重要信息如通讯录、文件等等并加以利用；
- 为手机设置锁屏密码，并将手机随身携带；
- 在某些应用程序中关闭地理定位功能，如 QQ、微信；并仅在需要时开启蓝牙；
- 禁用 WiFi 自动连接到网络功能，例如使用公共 WiFi 有可能被盗用资料；
- 下载手机应用软件要到权威的网站，安装时谨慎选择与程序不相关的权限；
- 不要试图破解自己的手机，以此来保证应用程序的安全性；
- 安装安全防护软件，并经常扫描手机系统；
- 经常为手机数据做备份；
- 请勿见码就刷，谨防市面上的“扫码有礼”营销业务。

六、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/
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/wfjb/
	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/