校园网络安全

5.1 大学生与网络安全

5.1.1 网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行保证网络服务不中断。

从广义上解释，网络安全通常指计算机网络的安全，实际上也可以指计算机通信网络的安全，而计算机网络用于服务资源共享，通信网络是实现资源共享的途径。因此，计算机网络是安全的，则相应的计算机通信网络也必须是安全的，应该能为网络用户实现信息交换与资源共享。只要涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

从狭义上解释，对于网络中的一个运行系统而言，网络安全就是指信息处理和传输的安全。稳定安全地处理、传输信息需要保障计算机硬件系统的安全、可靠运行，操作系统及应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。狭义的网络安全，侧重于网络传输的安全。

5.1.2 网络安全的主要因素

网络安全从其本质上来讲就是网络上的信息安全。因而，网络安全具有网络信息的某些特性，如可用性指可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息，网络环境下拒绝服务，破坏网络和有关系统的正常运行等都属于对可用性的攻击；可审查性指出现安全问题时提供依据与手段进行非授权访问，即对网络设备及信息资源进行非正常使用或越权使用等。

影响网络安全的主要因素有以下几点。

(1) 漏洞。漏洞的存在会造成网络安全出现重要隐患，常见的非法入侵、木马、病毒等都是通过漏洞来攻破网络安全防线的。因此，防堵漏洞是提高系统及网络安全的关键之一。

当前的漏洞问题主要包括两个方面：一是软件系统的漏洞，如操作系统漏洞、IE 漏洞、Office 漏洞等，以及一些应用软件、数据库系统(如 SQL Server)漏洞；二是硬件方面的漏

洞，如防火墙、路由器等网络产品的漏洞。

（2）内部人员操作不规范。在日常故障统计中，工作人员使用不当而造成的问题占绝大多数，例如，有的工作人员在多台机器上使用 U 盘、移动硬盘时，不注意杀毒；有的工作人员在计算机上随意安装软件；还有人安全意识不强，用户口令选择不慎，将自己的账号随意转借他人，甚至与别人共享账号，这些行为会给网络安全带来威胁。

（3）计算机感染病毒。计算机感染病毒以后，轻则系统运行速度明显变慢，频繁宕机，重则文件被删除，硬盘分区表被破坏，甚至硬盘被非法格式化，还可能引发硬件的损坏。主机一旦感染病毒，就会将系统中的防病毒程序关掉，让防病毒防线全部崩溃。

5.1.3　学校网络安全现状

随着目前我国大多数学校都建立了自己的校园网络，网络的普及程度越来越高。网络的建设在使教师和学生能够快速、方便地获取信息的同时，网络产生的安全问题也成为困扰网络发展的重要问题。

通过调查和研究发现，目前我国大多数学校都普遍存在着一定的网络安全问题，主要体现在以下几个方面。

1. 校园网络在硬件方面存在的隐患

校园网络的建设必须要依靠一定的硬件设施，如果硬件存在安全隐患则网络不会畅通。目前我国校园网络在硬件方面存在的隐患主要体现在硬件在设计、研发方面存在着一定的问题，如果核心系统出现问题，其他部分都无法正常使用，这使整个校园网络进入瘫痪状态；一些硬件存在着设计上的安全漏洞，这些漏洞一旦被黑客发现，就很容易受到攻击，整个校园网络的安全就会受到威胁。

2. 校园网络在软件方面存在的问题

对于校园网络来讲，仅仅依靠硬件是无法方便使用的，还需要系统软件或应用软件，供用户方便地使用校园网络，但是校园网络在软件方面也存在一定的问题：主要是网络入侵，一些软件在设计的过程中并没有考虑到加密和访问权限等问题，使得网络上的一些机密和重要的文件能够被非法使用者访问，使得网络容易受到进攻；还有拒绝服务攻击，受到这种攻击以后，计算机网络就无法响应用户的服务请求，网络的功能就形同虚设。

3. 校园网络在管理方面存在的安全隐患

目前校园网络在我国的建设规模越来越大，必须要有专门的管理人员对网络进行管理，从而防止一些网络安全问题的发生，但是目前我国的校园网络在管理方面还存在很多安全问题。主要体现在没有为校园网络安装有效的杀毒软件，虽然我们可以加强网络中的硬件和软件设计，降低网络被攻击的频率，但是防破坏方面的作用有限，不能完全杜绝安全问题的存在；网络管理人员的专业技能有待提高，在网络出现安全问题时应能够及时、有效地解决，避免造成大的损失。

4. 学生缺乏基本的隐私防护意识

通过对目前学校的网络健康情况调查得知，大学生网络安全意识薄弱，网络安全防范能力不高。大学生社会阅历浅，世界观、人生观、价值观尚未完全正确树立，对网络信息、网络诈骗的识别能力不高。部分学生网络道德、行为失范，存在网上不文明行为；严重者对网

上流传的虚假新闻、宣传资料、反动言论，不加辨识，随意转发、评论、盲目跟帖站队。部分大学生长期使用网络，但缺乏基本的隐私防护意识，个人手机、计算机安全保护措施不到位，网络诈骗防护意识不强，网络求职防范意识薄弱，不法分子利用学生的这些弱点，通过各种渠道和方式向大学生传播各类虚假信息、广告信息、垃圾邮件或者实施网络诈骗、短信诈骗、电话诈骗，甚至有居心叵测之人通过网络交友对大学生实施诈骗等犯罪活动。

综上所述，大学生大多具备使用网络的技能，但网络安全防范意识相对淡薄，抵御网络风险方面的能力不高，对维护网络安全的法律、法规、条例等相关知识储备不足。高校必须高度重视大学生网络安全教育，将此项工作与学校的思想政治教育、心理健康教育、民主法制教育、网络法律法规教育、网络行为规范、校纪校规教育、日常管理与服务等重点工作同部署、同安排，做到齐抓共管、统筹推进，形成常态化的教育模式、教育、引导学生自觉抵制网上有害信息，防止个人网络遭受非法侵入，增强抵御网络诈骗、识骗防骗的能力，切实提高大学生网络安全意识。

5.1.4 网络安全法律法规的意义

《中华人民共和国网络安全法》从 2013 年下半年提上日程，到 2016 年年底颁布，论证、起草、出台，速度非常快，充分说明了出台这部法律的重要性和紧迫性，其意义重大，影响深远。

（1）有助于维护国家安全。“没有网络安全就没有国家安全”，网络空间已成为第五大主权领域空间，互联网已经成为意识形态斗争的最前沿、主战场、主阵地，能否顶得住、打得赢，直接关系国家意识形态安全和政权安全。网络作为经济社会运行神经中枢的金融、能源、电力、通信、交通等领域的关键信息基础设施，一旦遭受攻击，就可能导致交通中断、金融紊乱、电力瘫痪等问题，破坏性极大。《中华人民共和国网络安全法》的主旨，就是要维护、保障网络空间主权和国家安全。

（2）有助于保障网络安全。现在我国已经成为名副其实的网络大国，但并不是网络强国，网络安全工作起点低、起步晚，相关举措滞后，安全形势堪忧。一方面，域外势力加紧实施网络遏制，利用网络进行意识形态渗透；另一方面，我国重要信息系统、工业控制系统的安全风险日益突出，相关重要信息几乎“透明”，存在重大的潜在威胁。《中华人民共和国网络安全法》的出台，对于维护网络运行安全、保障网络信息安全具有基础性、全局性的意义。

（3）有助于维护经济社会健康发展。当前，网络信息与人们的生产生活紧密相连，在推进技术创新、经济发展、文化繁荣、社会进步的同时，也带来比较严重的网络信息安全问题。经济生产、社会生活中的大量数据，大部分通过互联网传播，网络侵权、网络暴力、网络传播淫秽色情信息，网上非法获取、泄露、倒卖个人信息等时常发生，严重危害经济发展、社会稳定，损害百姓切身利益。《中华人民共和国网络安全法》在保护社会公共利益、保护公民合法权益、促进经济社会信息化健康发展方面扮演重要角色。

5.1.5 维护校园网络安全的措施

（1）加强对硬件系统的完善和管理。硬件是组成校园网络的重要部分，加强校园网络的安全建设，就必须要加强和完善对硬件设备的管理。例如，对硬件的研发和设计进行严

格的测试，对于一些明显的设计缺陷要及时提出，从而确保硬件设计的质量；对校园网络进行合理的规划和设计，合理的规划和设计不仅能够节约校园网络的建设成本，而且能够隐藏校园网络内部实现的细节，从而降低校园网络受攻击的概率。

（2）加强对软件系统的管理。软件可以帮助使用者方便地利用网络，所以在加强校园网络建设的过程中，必须要对软件系统进行严格的管理，为此可以做到：在软件的设计和研发过程中，要提高对网络安全问题的重视，增加一些防范技术；对于系统中的文件进行定期的备份，这样在网络受到攻击以后，损坏的文件还可以进行一定程度的补救。

（3）加强学生使用网络的安全意识。一些网络安全问题不仅会使校园网络瘫痪，而且有可能影响用户的计算机，同时用户计算机上的病毒也有可能感染校园网络，所以用户必须要加强自身计算机使用的安全意识，防止病毒的感染和扩散。

（4）制定校园网络安全管理相关的规章制度。制定相关的网络安全管理的规章制度，可以加强校园网络的安全性建设，规章制度的内容主要包括提高管理者的网络安全意识和责任意识，例如，安装一些有效的杀毒软件，对校园网络进行定期的杀毒，而且对于一些重要的用户要定期更换密码，进一步保证校园网络的安全；建立对网络设备管理的规章制度，例如，要做到对机房保持清洁，使得机器在适宜的温度和湿度下工作，对网络设备的运行进行一定的监控，在遇到问题时能够及时报警，争取将损失降到最低。

5.2　常见网络问题及应对

5.2.1　信息泄露

在互联网时代迅速发展的当今，信息的传播与流动速度每日剧增，而在这种情况下个人隐私信息难以得到全面的保护。

其中，个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人身份的各种信息，但不限于自然人的姓名、出生日期、身份证号码、个人生物识别信息、住址、电话号码等。除了这些基本信息以外，还有个人敏感信息、财产信息、健康生理信息、网络身份标识信息、网页浏览记录和行踪轨迹等。

这些信息一旦泄露，可能危害人身和财产安全、导致个人名誉受到损害等。所以在信息时代，我们可以发现自己的个人信息无时无刻不受到来自外界的盗取、泄露。当发现个人信息泄露的情况时，应尽快实施以下解决方案尽可能避免更大的损失。

（1）努力收集证据线索。最好是能收集到一些比较有价值的信息，如电话号码、邮箱地址等。这些信息可能比较零散，但是它能够帮助我们在后续维权的过程中协助警方调查。

（2）及时向有关部门报案。可以向公安部门、互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报。这样一来既可以保护自己的权益，也能够在相关部门备案。

（3）在发现个人信息泄露后，及时修改自己的账号密码，防止自己的账号被人盗取，或者前往如银行、电话营业厅等相关部门申请冻结个人账号，从而在后续过程中大大减少给自己带来的损失。

（4）委托律师进行维权。如果个人重要信息丢失，在知道是如何丢失的或者有很多相关线索的情况下，建议咨询专业的律师寻求解决的方法。

5.2.2 网络成瘾

网络成瘾是指上网者由于长时间地和习惯性地沉浸在网络时空当中，对互联网产生强烈的依赖，以至于达到了痴迷的程度而难以自我解脱的行为状态和心理状态。其中有几种典型的表现形式：网络色情成瘾、网络关系成瘾、网络购物成瘾、网络游戏成瘾等，这些表现大多会影响网民心理健康向不良方向发展。

过度使用互联网将会引发的不良后果，网络上大量的黄色信息、游戏暴力、虚拟恋爱等容易使青少年沉迷其中，对于真实生活的人和事缺少兴趣、情感淡薄、和亲人朋友之间的交流减少，逐渐将自己封闭起来，与社会脱节，程度严重的会影响社会秩序。

改正网瘾的具体办法和正确使用网络的方法如下。

（1）端正对互联网的认识。首先必须认识到计算机或者互联网是一种工具，是人类学习、工作的工具之一，而不是生活的全部。使用计算机及互联网的目的是提高个体生存和发展的质量。

（2）合理安排上网时间，尽可能固定上网时间。正确地使用网络是在有需求时使用或者对自己生活有方便的情况下使用，网络过度使用者主要表现为一种不自主地长期强迫性使用网络的行为。当过度地使用网络对身体造成伤害、对工作、学习和社会交往带来了痛苦，甚至正常的生活交往和社会生活都受到了影响时，应该及时进行矫正。

（3）在现实生活中可以寻找其他的爱好替代网络来分散注意力，如游泳、打球、登山、旅游等户外运动，以充实精神生活。

5.2.3 网恋网婚

网恋网婚是社会网络化发展的产物，随着社会网络化、信息化的深入推进和结婚率走低、离婚率飙升、未婚人群增多等婚恋难题逐渐突出，催生了大量网络交友平台，实现了婚恋由自发向自觉的跨越式发展。

不少犯罪分子利用网恋网婚的虚拟性进行敲诈，使网恋网婚诈骗成为电信诈骗主要犯罪形式之一。每年我国发生网络诈骗案件近几十万起，其中网恋网婚诈骗案几万起，涉嫌多名受害者，这些网恋网婚诈骗案呈现与传销交织、与洗钱勾连、追赃挽损难等新特点。但大量案件仍然反映出多数婚恋网站注册门槛低、非强制实名注册、审核宽松等问题。一些被害人出于对网恋网婚交友平台的信任，轻信犯罪分子提供的网络信息，投入感情后防范意识降低，成为许多“杀猪盘”待宰的“猎物”。

因而学会辨别网络征婚、交友及恋爱诈骗的特点尤其重要，其主要特点有以下几点。

（1）犯罪分子的行骗途径主要是通过网络交友、相亲网站，与受害人进行网络交流，在骗取对方信任、确立交往关系后，选择时机提出借钱周转、家庭遭遇变故等各种理由，骗取钱财后便销声匿迹。

（2）犯罪分子的针对对象主要是有征婚交友意愿的人士。

（3）犯罪分子的征婚信息一般会在各征婚交友网站注册，填报虚假信息，通过家境优

越、有房有车等较佳的经济条件来吸引异性，并在与异性相约见面过程中通过各种手段极力证实其身份的“真实性”，博取受害人的好感。

（4）犯罪分子会极力讨好受害人，获取受害人的初步信任与好感后，以各种方式进一步迷惑、讨好被害人，为最后的诈骗工作做准备。

在征婚网络平台上看见一些比较感兴趣的信息时，一定要及认真核实对方身份，避免上当。

除此之外，还要学会增强自我保护意识，主要有如下几点。

（1）提高自我保护意识，不要随便透露个人信息。因为网络的虚拟性，我们看不到网上的人是否是真诚交友的，同时也无法确认你所“认识”的他是不是现实生活中真实的他。所以在不确定的时候，切记不要透露个人信息。如果不幸遇到坏人和骗子，或是被怀有其他目的与自己接触的人掌握了个人信息，可能会造成很严重的影响或者其他可怕的损失。

（2）保持谨慎的态度，不要轻易与网友见面。如果仅仅在网上相互了解、相互认知之后就考虑见面，却对网络另一端的那个人没有真正的了解，很容易将自己陷入危险的境地。因此，需要保持谨慎，提高警惕，不要轻易与网友见面。

（3）厘清网络与现实的距离，不要与网友有金钱往来。网络上的人良莠不齐，在网络交友时，很难看清这个人是否诚信，是否真实，同时网络是诈骗等案件的高发地。在进行网络交友时，千万不能掉以轻心，轻易答应借钱给对方或发生其他金钱往来。一旦被骗，产生的损失很难追回。

5.2.4　网络不良信息

互联网上的违法信息涉及很多种类，大致包括淫秽、色情、暴力等低俗信息；赌博、犯罪等技能教唆信息；毒品、违禁药品、刀具枪械、监听器、假证件、发票等管制品买卖信息；虚假股票、信用卡、彩票等诈骗信息，以及网络销赃等。

其中最为突出的就是淫秽、色情类低俗信息。互联网低俗之风蔓延，污染社会，违背法律法规和行业规范，对广大网民特别是青少年而言，轻则损害身心健康、导致青少年价值观判断混乱，重则影响青少年心理的健康发展，造成堕落犯罪。据有关调查，在我国许多青少年正在受到网络淫秽、色情及恐怖、暴力等违法和不良信息的伤害。

遇见互联网违法和不良信息，如发现网络上有冒充明星行骗、网络招嫖、跨境网络赌博等犯罪行为，最佳的处理方式就是举报。可以向中共中央网络安全和信息化委员会办公室（国家互联网信息办公室）、不良信息举报中心、12321 网络不良与垃圾信息举报受理中心等地方进行举报。

5.2.5　计算机病毒

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。计算机病毒具有非授权可执行性、隐蔽性、破坏性、传染性、可触发性。

计算机受到病毒感染后，会表现出如下症状。

（1）运行速度降低。如果发现在运行某个程序时，读取数据的时间比原来长，存文件

或调文件的时间都增加了，很有可能是磁盘剩余空间不足，也有可能是病毒造成的。

（2）经常出现“死机”现象。正常的操作是不会造成死机现象的，即使是初学者，命令输入不对也不会死机。如果机器经常死机，可能是由于系统被病毒感染导致的。

（3）磁盘空间迅速变小。由于病毒程序要进驻内存并且繁殖，因此使内存空间变小。

（4）文件内容和长度有所改变。一个文件存入磁盘后，本来它的长度和其内容都不会改变。但是由于病毒的干扰，会使得文件内容长度改变、文件内容出现乱码、文件内容无法显示或显示后又消失。

（5）外部设备工作异常。因为外部设备受系统的控制，如果机器中有病毒，外部设备在工作时可能会出现一些异常情况。

计算机病毒的传播方式主要包括存储介质、网络、电子邮件等，只有从这些来源断绝接触病毒以及通过计算机软件清扫病毒，防治病毒入侵应做到如下几点。

（1）不使用来历不明的移动存储设备。

（2）不浏览一些格调不高的网站，不阅读来历不明的邮件。

（3）不要随便下载网上的软件，尤其是不要下载来自无名网站的免费软件，因为这些软件无法保证没有被病毒感染。

（4）不要使用盗版软件。

使用新设备和新软件之前要检查如下几点。

（1）安装防病毒软件。及时升级反病毒软件的病毒库，开启病毒实时监控。

（2）一般不要用软盘启动。如果计算机能从硬盘启动，就不要用软盘启动，因为这是造成硬盘引导区感染病毒的主要原因。

（3）重建硬盘分区，减少损失。若硬盘资料已经遭到破坏，不必急着格式化，因为病毒不可能在短时间内将全部硬盘资料破坏，故可利用“灾后重建”程序加以分析和重建。

（4）系统备份。要经常备份系统，防止万一被病毒侵害后系统崩溃。

5.2.6 垃圾邮件

垃圾邮件泛指未经请求而发送的电子邮件，符合以下特征的邮件都属于垃圾邮件的范畴。

（1）来自收件人从未发送过邮件的地址第一次发出的邮件，以及在该邮件未被收件人自定义为正常邮件的情况下随后从同一地址发送给收件人的其他邮件。

（2）来自被拒绝过接收邮件的地址所发给收件人的其他邮件。

（3）来自被收件人列入黑名单的邮件地址的邮件。

（4）内容包含可被反垃圾装置或可被邮件过滤器定义、归类为垃圾邮件的关键字段的邮件。

（5）带虚假、无效邮件头的邮件，带虚假、无效域名的邮件，经过技术处理的不显示任何邮件来源信息的邮件。带欺骗性地址信息的邮件。

（6）未经同意而使用、中继或通过第三方的互联网设备所发送的邮件。

（7）主题行或内容包含错误、误导或虚假信息的邮件。

在日常的生活中，总是能收到各式各样的垃圾邮件，有推销产品的，也有不怀好意的，

有些电子邮件还有可能是带病毒的。当发现自己的邮箱出现垃圾邮件时，可以用以下方法解决问题。

（1）使用邮件过滤系统。这种方法使用普遍但不够精确，大型邮件服务商会提供此类服务。

（2）使用病毒过滤系统。很多垃圾邮件利用了木马病毒，使用杀病毒软件将病毒拒之门外，相关的垃圾邮件也就无机可乘。

（3）保护自己的邮件地址，最好把不同用途的邮件地址分开，不随处暴露自己的邮件地址。

（4）退信。收到可疑的垃圾邮件之后应该怎么做，首先不要打开它，因为很可能含病毒，然后选择退信，这样可能会让有些垃圾邮件服务器端认为你的信箱已经不可用。

（5）注意邮件的注册名。不要设置过于简单，一个远离垃圾邮件的方法是选择合适的用户名。很多人喜欢用自己的名字或者 aaa123 之类的地址，这样很容易被破解。

（6）远离危险区域。据统计，邮件病毒最多的 3 类站点分别是赌博、游戏和成人网站，对于这些网站，要特别注意。

5.3　网络犯罪危机及应对

5.3.1　网络诈骗

网络诈骗是指以非法占有为目的，利用互联网采用虚构事实或者隐瞒真相的方法，骗取数额较大的公私财物的行为。其花样繁多，行骗手法日新月异，常用手段有假冒好友、网络钓鱼、网银升级诈骗等，主要特点有空间虚拟化、行为隐蔽化等。

1. 部分常见诈骗手段

（1）网络购物诈骗。犯罪分子开设虚假购物网站或淘宝店铺，一旦事主下单购买商品，便称系统故障需要重新激活。随后，通过 QQ 发送虚假激活网址实施诈骗。

（2）低价购物诈骗。犯罪分子通过互联网、手机短信发布二手车、二手计算机、海关没收的物品等转让信息，一旦事主与其联系，即以缴纳“定金”“交易税”“手续费”等方式骗取钱财。犯罪分子在微信朋友圈以优惠、打折、海外代购等为诱饵，待买家付款后，又以“商品被海关扣下，要加缴关税”等为由要求加付款项，一旦获取购货款则失去联系。

（3）刷网评信誉诈骗。犯罪分子以开网店需快速刷新交易量、网上好评、信誉度为由，招募网络兼职刷单，承诺在交易后返还购物费用并额外提成，要求受害人在指定的网店高价购买商品或缴纳定金的方式骗取受害人钱款。

（4）招聘诈骗。犯罪分子通过网络、短信或者传统媒体发布虚假招聘信息，进而以缴纳服装费、押金、保证金、定金等名义，让受害人向其提供的账户上汇款。

（5）招商加盟。犯罪分子通过网络或传统媒体发布虚假招商、加盟信息，以高额利润为诱饵，骗取受害人定金、加盟费、货款等费用。

2. 避免进入犯罪分子的圈套，提高防范意识

（1）不要随意拨打网上的电话。有些诈骗网站会留下自己的联系方式，这个时候就一定要提高警惕了，必须先做一个全方位的了解，再考虑进行下一步的操作，万不可自以

为是。

(2) 访问正规的官方网站,注意防范“钓鱼网站”。所谓“钓鱼网站”指不法分子利用各种手段,仿冒真实网站的 URL 地址以及页面内容,或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的 HTML 代码,以此来骗取用户银行或信用卡账号、密码等私人资料。

(3) 在网站购物时,消费者要尽量避免直接汇款给对方,可以采用支付宝等第三方支付平台交易,一旦发现对方是诈骗,应立即通知支付平台冻结货款。即使采用货到付款方式,也要约定先验货再付款,防止不法商家偷梁换柱。此外,一定要在市场上认可度比较高的购物网站上购物,在支付过程中最好选择支付宝、网银等较为安全的支付方式,切记不可现金转账,以免被骗。

(4) 保管好自己的私人信息,不要随便告诉陌生人。注意保管好自己的电子邮箱、QQ 号等相关私人资料,尽量少在网吧或公用计算机上网等。尤其在汇款给别人之前,务必要向朋友或客户核实情况,以免上当受骗。

(5) 账号密码要及时更换。一旦发现自己进入了诈骗圈套,要第一时间去网络官方举报,然后保留好证据,如聊天记录等。若有钱财流失,就要马上到警方报警,一定要做到冷静,更不能试图自己解决,要知道网络诈骗分子的手段不是你能想象得到的。

5.3.2 网购陷阱

随着互联网发展进入高潮,网络购物的优点愈加突出,日益成为一种重要的购物形式。中国网络购物的用户规模不断上升。不少犯罪分子正好看中网络购物的发展,利用网络购物的信息差来盗取他人信息及金钱。目前网购出现的最主要陷阱有以下几种。

1. 退款诈骗

犯罪嫌疑人冒充网站工作人员或者卖家,以退款为由,要求事主按照其要求进行操作,其实是在进一步盗取公民个人信息,进而盗取钱财。购物时应与正规网站上提供的客服人员联系,不要轻易相信陌生电话或者短信,在提供个人信息给陌生人时一定要认真鉴别,小心谨慎。银行卡号及转账的验证码一旦提供给其他人,可能直接造成财产损失。同时,在点击对方发来的网页链接前一定要看清网站域名,使用正确网站域名查看购买货款的情况,防止进入钓鱼网站。

2. 重拍诈骗

网上购物一定要多加小心,接到自称是卖家的陌生电话,要通过购物网站的正规渠道向卖家求证,谨慎鉴别;陌生链接不要轻易打开,避免泄露自己的支付信息,造成财产损失。

另外,有些骗子会以网购返利为借口,要求事主提供收款的姓名、身份证号、银行卡号和手机号,随后骗子称事主身份信息核对有问题,让事主扫描二维码,进而盗刷银行卡。

3. 开设虚假网店诈骗

犯罪嫌疑人利用购物网站平台为依托,提供虚假物品诱使市民购买,其本质为诈骗行为。提醒市民在选择商家时一定要选择有信誉且有认证的正规商家,切勿贪图便宜。

4. 盗刷信用卡

日常生活中要注意保护个人隐私,不在不熟悉的网站随意输入银行账号、密码等信息,

不在不正规的网站购物，也不要在自己不熟悉的境外网站购物和留下信用卡信息，以防给犯罪分子留下可乘之机。

5. 冒充客服诈骗卖家

卖家也要提高警惕，小心被骗。淘宝卖家遇到客服人员要求缴纳保证金时要谨慎，要先确定客服的真实性，并通过正规渠道咨询官方客服人员。不要轻信陌生人，不与陌生人进行私下交易，正规的网站工作人员不会让卖家将钱款打进个人账户。

6. 虚假打折机票诈骗

凡是要求提供身份证号、信用卡号及后三位 CVV 码、信用卡有效期等信息的购物类、旅游类网站，需要格外警惕，认清正规官方网站，远离诈骗钓鱼网站，谨防信用卡信息泄露造成个人财物的损失。不要轻信网上的超低价折扣机票信息，购买机票应到正规的订票网站订购，订购成功后应打官方服务电话进行核实。在上网过程中，注意保护好自己的个人信息，特别是在网银支付时，尽量采取使用 U 盾等可靠性更高的验证手段，避免个人信息泄露。

7. 经常查杀手机木马病毒

嫌疑人将手机木马植入事主手机，利用木马获取事主账户和密码，拦截事主短信，盗取事主钱财。植入手机木马的形式多种多样，嫌疑人会将木马程序标识换成公众并不会产生怀疑的提示标志，如显示“QQ 更新”“系统更新”等图标，诱骗事主点击下载。使用手机客户端时，不要轻易点击弹出的链接，一定要通过正规、可靠的手机应用市场或官网下载和更新客户端。对于网上的二维码，也一定要慎扫，防止手机被植入恶意程序。

8. 邮件钓鱼诈骗

网络上不乏各种形式进行钓鱼诈骗的手段，利用邮件进行钓鱼是一种新型网络骗局，骗子恶意模仿支付宝提醒付款邮件信息内容，用户如果不仔细看发件人地址，上当的可能性非常大。在收到类似邮件时，一定要认真鉴别发件人地址，并通过正规途径与客服进行确认。

9. 超低价诈骗

购买二手商品需注意，天上不会掉馅饼。消费者应该根据商品的市场价格对比卖家出售价格，勿以低价作为选购二手商品的首要标准。尽量选择支持消费者保障服务的商品，谨慎购买超低价商品。坚持正确的购物流程，未收到货前不要确认付款，不提倡使用即时到账的付款方式。

防骗必须养成好习惯，用电商平台提供的正规渠道跟卖家进行沟通，并保存好聊天记录；不轻易向陌生人透露银行卡账号和密码。如果被骗要及时到公安机关报案。

5.3.3　传销陷阱

传销是指组织者或者经营者发展人员，通过对被发展人员以其直接或者间接发展的人员数量或者销售业绩为依据计算和给付报酬，或者要求被发展人员以交纳一定费用为条件取得加入资格等方式牟取非法利益，扰乱经济秩序，影响社会稳定的行为，及非法牟取利益的行为。传销的危害性在于扰乱社会经济秩序，影响社会安定团结；引发社会刑事案件上升、家破人亡等社会骚乱。