

**共青团内江师范学院委员会**

**网**

**络**

**安**

**全**

**小**

**常**

**识**

**共青团内江师范学院委员会**

**二○一四年九月十三日**

目录

[一、 网络诈骗案例以及如何防范网络诈骗 3](#_Toc405016081)

[1、利用盗号和网络游戏交易进行诈骗 3](#_Toc405016082)

[、冒充即时通讯好友借钱。 3](#_Toc405016083)

[、网络游戏装备及游戏币交易进行诈骗。 3](#_Toc405016084)

[、交友诈骗。 4](#_Toc405016085)

[2、网络购物诈骗 4](#_Toc405016086)

[、多次汇款 4](#_Toc405016087)

[、假链接、假网页 4](#_Toc405016088)

[、拒绝安全支付法 5](#_Toc405016089)

[、收取订金骗钱法 5](#_Toc405016090)

[、约见汇款 5](#_Toc405016091)

[、以次充好 5](#_Toc405016092)

[3、网上中奖诈骗 5](#_Toc405016093)

[4、“网络钓鱼”诈骗 6](#_Toc405016094)

[5、如何防范网络诈骗 7](#_Toc405016095)

[二、计算机病毒寄生方式分类 9](#_Toc405016096)

[1、引导型病毒 9](#_Toc405016097)

[2、文件型病毒 10](#_Toc405016098)

[3、混合型病毒 10](#_Toc405016099)

[三、拒接服务攻击 10](#_Toc405016100)

[四、计算机加密方式 11](#_Toc405016101)

[1、DES 11](#_Toc405016102)

[2、AES 11](#_Toc405016103)

[3、WPA2 12](#_Toc405016104)

[4、BASE64 12](#_Toc405016105)

[五、第一个计算机病毒 12](#_Toc405016106)

[六、浏览器内核 13](#_Toc405016107)

[1、简介 13](#_Toc405016108)

[2、浏览器内核的分类 14](#_Toc405016109)

[、Webkit(Safari内核，Chrome内核原型，开源) 14](#_Toc405016110)

[、Trident(IE内核) 14](#_Toc405016111)

[、Gecko(Firefox内核) 15](#_Toc405016112)

[、Presto(Presto前内核，已废弃) 16](#_Toc405016113)

[七、NFC 16](#_Toc405016114)

# 网络诈骗案例以及如何防范网络诈骗

当前随着网络的日益飞速发展，网络诈骗犯罪日益严重。网络安全专家提醒网友要学习一定的防范网络诈骗的基本知识，提高防范网络诈骗的基本能力，遇到实际问题，忌盲目，多思考，千万不要被某些假象所迷惑。为了同学们年底学习和生活的安全，我们特别提示大家防范诈骗。为了帮助大家识破一些网络诈骗，我们在此整理了一些常见的诈骗类型（共8类17种手段），供各位朋友们学习参考。

## 1、利用盗号和网络游戏交易进行诈骗

### 、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一定要提高警惕,摸清对方的真实身份.需要您特别当心的是一些冒充熟人的网络视频诈骗，犯罪分子通过盗取图像的方式用“视频”与您聊天，您可千万别上当，遇上这种情况，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，犯罪分子利用某款网络游戏，进行游戏币及装备的买卖，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。

### 、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。

## 2、网络购物诈骗

是指事主在互联网上因购买商品时而发生的诈骗案件。其表现形式有以下6种：

### 、多次汇款

骗子以未收到货款或提出要汇款到一定数目方能将以前款项退还等各种理由迫使事主多次汇款。

### 、假链接、假网页

骗子为事主提供虚假链接或网页，交易往往显示不成功，让事主多次往里汇钱。

### 、拒绝安全支付法

骗子以种种理由拒绝使用网站的第三方安全支付工具，比如谎称“我自己的账户最近出现故障，不能用安全支付收款”或“不使用网易宝，因为要收手续费，可以再给你算便宜一些”等等。

### 、收取订金骗钱法

骗子要求事主先付一定数额的订金或保证金，然后才发货。然后就会利用事主急于拿到货物的迫切心理以种种看似合理的理由，诱使事主追加订金。

### 、约见汇款

网上购买二手车、火车票等诈骗的常见手法，骗子一方面约见事主在某地见面验车或给票，又要求事主的朋友一接到事主电话就马上汇款，骗子利用“来电任意显软件”冒充事主给其朋友打电话让其汇款。

### 、以次充好

用假冒、劣质、低廉的山寨产品冒充名牌商品，事主收货后连呼上当，叫苦不堪。

## 3、网上中奖诈骗

是指犯罪分子利用传播软件随意向邮箱用户、网络游戏用户、即时通讯用户等发布中奖提示信息，当事主按照指定的“电话”或“网页”进行咨询查证时，犯罪分子以中奖缴税等各种理由让事主一次次汇款，直到失去联系事主才发觉被骗。当您登陆聊天或打开邮箱时是否会收到一些来历不明的中奖提示，不管内容有多么逼真诱人，请您千万不能相信，更不要按照所谓的咨询电话或网页进行查证，否则您将一步步陷入骗局之中。

## 4、“网络钓鱼”诈骗

“网络钓鱼”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。作案手法有以下两种：

、发送电子邮件，以虚假信息引诱用户中圈套。不法分子大量发送欺诈性电子邮件，邮件多以中奖、顾问、对账等内容引诱用户在邮件中填入金融账号和密码。

、不法分子通过设立假冒银行网站，当用户输入错误网址后，就会被引入这个假冒网站。一旦用户输入账号、密码，这些信息就有可能被犯罪分子窃取，账户里的存款可能被冒领。此外，犯罪分子通过发送含木马病毒邮件等方式，把病毒程序置入计算机内，一旦客户用这种“中毒”的计算机登录网上银行，其账号和密码也可能被不法分子所窃取，造成资金损失。

## 5、如何防范网络诈骗

面对以上形形色色的网络诈骗手段，作为大学生群体应该如何有效地识别、应对和防范？别着急，网络安全专家给您支招：

当您在网上遇到骗子后，您该怎么做？

、不要主动与对方联系，拨打所谓的咨询电话，这样只能使您一步步上钩。

、不要过分依赖网络，遇到有人借款，要牢记“不决断晚交钱，睡一觉过一天，再找亲人谈一谈”的口诀，比如对方要求你现在把钱给我寄过来，你就记住不决断晚交钱，说等一等，明天再说；第二句话“睡一觉过一天”是说一般睡一觉到第二天早上起来都明白了，当时觉得比较晕，叫忽悠，睡一觉就好了；最后是找同学、室友、亲人谈一谈，大家聊一聊。有这三句话就保了三个险。

、一旦发觉对方可能是骗子，马上停止汇款，不再继续交钱，防止扩大损失。

、马上进行举报，可拨打官网客服电话、当地派出所电话或110报警电话向有关部门进行求证或举报。

**提示：提高警惕，严防上当。**

、不贪便宜。虽然网上东西一般比市面上的东西要便宜，但对价格明显偏低的商品还是要多个心眼，这类商品不是骗局就是以次充好，所以一定要提高警惕，以免受骗上当。

、使用比较安全的网易宝等支付工具。调查显示，网络上80%以上的诈骗是因为没有通过官方支付平台的正常交易流程进行交易。所以在网上购买商品时要仔细查看、不嫌麻烦，首先看看卖家的信用值，再看商品的品质，同时还要货比三家，最后一定要用比较安全的支付方式，而不要怕麻烦采取银行直接汇款的方式。

、仔细甄别，严加防范。克隆网站虽然做得微妙微肖，但若仔细分辨，还是会发现差别的。您一定要注意域名，克隆网页再逼真，与官网的域名也是有差别的，一旦发现域名多了“后缀”或篡改了“字母”，就一定要提高警惕了。特别是那些要求您提供银行卡号与密码的网站更不能大意，一定要仔细分辨，严加防范，避免不必要的损失。

、千万不要在网上购买非正当产品，如手机监听器、毕业证书、考题答案等等，要知道在网上叫卖这些所谓的“商品”，几乎百分百是骗局，千万不要抱着侥幸的心理，更不能参与违法交易。

、凡是以各种名义要求你先付款的信息，请不要轻信，也不要轻易把自己的银行卡借给他人。你的财物一定要在自己的控制之下，不要交给他人，特别是陌生人。遇事要多问几个为什么！

、提高自我保护意识，注意妥善保管自己的私人信息，如本人证件号码、账号、密码等，不向他人透露，并尽量避免在网吧等公共场所使用网上电子商务服务。网络诈骗，正以诡谲多变、防不胜防的态势侵入我们的生活，树立牢固的安全观念，常备警惕之心对没有固定收入的大学生而言尤其重要。

其他应采取的网络安全防范措施还包括：一是安装防火墙和防病毒软件，并经常升级；二是注意经常给系统打补丁，堵塞软件漏洞；三是禁止浏览器运行JavaScript和ActiveX代码；四是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，不要打开即时通讯上传送过来的不明文件等，加强对各类即时通讯病毒的防范和清除措施。

最后提醒大家，不管是现实诈骗还是网络诈骗，骗子最终的核心或者是共同点都是一个骗字，只要同学们多加强预防心理，多提高一些警惕，多留点心眼，就一定会发现狐狸尾巴。

# 二、计算机病毒寄生方式分类

计算机病毒按其寄生方式大致可分为三类：一是引导型病毒，二是文件型病毒。混合型病毒集引导型和文件型病毒特征于一体。

## 1、引导型病毒

引导型病毒也称磁盘引导型、引导扇区型、磁盘启动型、系统型毒等。引导型病毒就是把自己的病毒程序放在软盘的引导区以及硬盘的主引导记录区或引导扇区，当做正常的引导程序，而将真正的引导程序搬到其他位置。这样，计算机启动时，就会把引导区的病毒程序当作正常的引导程序来运行，使寄生在磁盘引导区的静态病毒进入计算机系统，病毒变成活跃状态（或称病毒被激活），这时病毒可以随时进行感染和破坏。

## 2、文件型病毒

文件型病毒是指所有通过操作系统的文件系统进行感染的病毒。文件型病毒以感染可执行文件（.BAT、.EXE、.COM、.SYS、.DLL、.OVL、.VXD等）的病毒为主，还有一些病毒可以感染高级语言程序的源代码、开发库或编译过程中所生成的中间文件。

## 3、混合型病毒

混合型病毒，也称综合型、复合型病毒，既具有操作系统型病毒的特点，又具有文件型病毒的特点，即这种病毒既可以感染磁盘引导扇区，又可以感染可执行文件，这类病毒的危害性更大。对染有混合型病毒的机器，如果只解除了文件上的病毒，而没有解除硬盘主引导区的病毒，系统引导时又将病毒调入内存，会重新感染文件;如果只解除了主引导区的病毒。而可执行文件上的病毒没有解除，执行带毒的文件时，就会又将硬盘主引导区感染。常常因为杀毒不彻底，而造成“病毒杀不死”的假象。

# 三、拒接服务攻击

拒绝服务攻击即DoS，英文全称是Denial of Service,也就是“拒绝服务”的意思。从网络攻击的各种方法和所产生的破坏情况来看，DoS算是一种很简单又很有效的进攻方式。它的目的就是拒绝你的服务访问，破坏组织的正常运行，最终它会使你的部分网络连接和网络系统失效。DoS的攻击方式有很多种，最基本的DoS攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。

# 四、计算机加密方式

## 1、DES

DES又叫数据加密标准，是1973年5月15日美国国家标准局在联邦记录中公开征集密码体制时出现的。DES在1975年3月17日首次在联邦记录中公布，在经过大量的公开讨论后，1977年2月15日DES被采纳为“非密级”应用的一个标准。最初预期DES作为一个标准只能使用10-15年，然而，事实证明DES要长寿得多。在其被采用后。大约每隔五年被评审一次。DES最后一次评审在1999年1月，在当时，一个DES的替代品,AES开始使用。

## 2、AES

密码学中的高级加密标准，又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来代替原先的DES，已经被多方分析且广为全世界所使用。

## 3、WPA2

WPA2是WI-FI联盟对采用IEEE802.11i安全增强功能产品的认证计划。简单一点理解，WPA2是基于WPA的一种新的加密方式。

“WI-FI联盟”是一家对不同厂商的无线LAN终端产品能够顺利地相互连接进行认证的业界团体，由该团体制定的安全方式是“WAP2004年9月发表的“WAP2”支持“AES”加密方式。除此之外，与过去的WAP相比在功能方面没有太大的区别”。

## 4、BASE64

BASE64是网络上最常见的用于传输9Bit字节代码的编码方式之一。Base64编码可用于在HTTP环境下传递较长的标识信息。

# 五、第一个计算机病毒

全球第一个电脑病毒在1988年11月2日有麻省理工学院(MIT0的学生Robert Tappan Morris撰写，因此病毒也被取名为Morris。

Morris病毒总共仅99行程序代码，施放到当时网络上数小时，就有数以千计的UNIX服务器受到感染。因为他的行为，他成为第一个被1986计算机欺骗和滥用法令起诉的人。他那时宣称他只是想用这个病毒查看互联网到底有多大，原始用意并非用来瘫痪电脑，但程式的循环没有处理好，使得服务器不断执行、复制，最后死机。Morris最后被判了400个小时的社区服务和一万美元的罚款。

Morris现在 是MIT计算机科学和人工智能实验室的一名专家。他专注于计算机网络体系。

Morris是第一个在网络上流传的病毒；最早发现病毒的记录，则是1982年Xerox旗下Xerox Palo Alto实验中心两位研究人员John Shoch和Jon Hupp，发现1个有缺陷的程序，会自动复制、传送到不同的服务器里，但这个病毒只在Xerox的实验中心里流窜，没有感染其他电脑。

# 六、浏览器内核

## 1、简介

浏览器最重要或者说核心的部分是“Rendering Engine”,可大概译为“解释引擎”，不过我们一般习惯将只称为“浏览器内核”。负责对网页语法的解释（如标准通用标记语言下的一个应用HTML、JavaScript）并渲染（显示）网页。所以，通常所谓的浏览器内核也就是浏览器所采用的渲染引擎，渲染引擎决定了浏览器如何显示网页的内容以及也卖弄的格式信息。不同浏览器内核对网页编写语法的解释也有不同，因此同一网页在不同的内核浏览器里的渲染（显示）效果也可能不同，这也是网页编写者需要在不同内核的浏览器中测试网页显示效果的原因。

## 2、浏览器内核的分类

### 、Webkit(Safari内核，Chrome内核原型，开源)

Webkit:它是苹果公司自己的内核，也是苹果的Safari浏览器使用的内核。Google Chrome、360极速浏览器以及收购浏览器高速模式也使用Webkit作为内核。

苹果在Safari中采用Webkit核心，并与2005年将Webkit公开作为开源软件。谷歌采用苹果的Webkit核心打造Chrome浏览器

### 、Trident(IE内核)

该内核程序在1997年的IE4中首次被采用，是微软在Mosaic代码的基础之上修改而来的，并沿用到IE11。Trident实际上是一款开放的内核，其接口内核设计的相当成熟，因此才有徐东采用IE额你好而非IE浏览器涌现。此外，未来方便也有很多人之间简称其为IE内核。

由于早期IE浏览器的“垄断性”，使得Trident内核长期一家独大，微软很长时间都并没有更新Trident内核，这导致了两个后果—一是Trident内核曾经几乎与w3c脱节（2005），二是Trident内核大量BUG等安全问题没有得到及时解决，然后加上一些致力于开源的开发者和一些学者们公开自已任务IE浏览器不安全的观点，也有很多用户转向了其他浏览器，Firefox和opera就是这个时候兴起的。非Trident内核浏览器的时常占有率大幅提高也致许多网页开发人员开始注意网页标准和非IE浏览器的浏览效果问题。其中部分浏览器的新版本是“双核”甚至是“多核”，其中一个内核是Trident，然后再增加一个其他内核。国内的厂商一般把其他内核叫做“高速浏览模式”，而Trident则是“兼容浏览模式”，用户可以来回切换。

### 、Gecko(Firefox内核)

Gecko:Netscape6开始采用的内核，后来的Mozilla FireFox(火狐浏览器)也采用了该内核，Gecko的特点是代码完全公开，因此，其可开发程度很高，全世界的程序员都可以为其编写代码，增加功能。因此这是个开源的内核，因此受很多人青睐，Gecko内核的浏览器很多，这也是Gecko内核虽然年轻但是市场占有率能够迅速提高的重要原因。

Gecko引擎的由来跟IE不无关系，前面说过IE没有使用W3C的标准，这导致了微软内部一些开发人员的不满；他们与当时已经停止更新的Netscape的一些员工一起创办了Mozilla,以当时的Mosaic内核为基础重新编写内核，于是开发出了Gecko。不过事实上，Gecko内核的浏览器仍然还是Firefox（火狐）用户最多，所以有时也有时也会被称为Firefox内核。

### 、Presto(Presto前内核，已废弃)

Presto：Opera12.16及更早版本曾经采用的内核，现已经体质开发并废弃，该内核在2003年的Opera7中首次被使用，该款引擎的特点是渲染速度的化达到了极致，然而代价是牺牲了网页的兼容性，Opera现已改用Chrome的最小内核Blink

# 七、NFC



NFC(近场通信），又称近距离无线通信，是一种短距离的高频无线通信技术，允许电子设备之间进行非接触式点对点数据传输交换数据。与目前使用较多的蓝牙技术相比，NFC使用更加方便，成本更低，能耗更低，建立连接的速度也更快，只需0.1秒钟。但是NFC的使用距离比蓝牙要短得多，有的只有10CM，传输速率也比蓝牙低许多。