



“十四五”职业教育国家规划教材



“十四五”职业教育河南省规划教材

信息技术
(拓展模块)

主 编 丁爱萍 吴教育

信息技术

(拓展模块)

根据教育部发布的高职信息技术课程标准(2021年版)编写

主 编 丁爱萍 吴教育

北京出版集团
北京出版社

北京出版集团
北京出版社

内 容 提 要

本书依据教育部《高等职业教育专科信息技术课程标准（2021年版）》中对拓展模块的要求编写而成。全书共12个单元，主要包括：信息安全、项目管理、机器人流程自动化、程序设计基础、大数据、人工智能、云计算、现代通信技术、物联网、数字媒体、虚拟现实、区块链等。

本书以任务驱动开展教学，方便教师教、学生学。

本书把握时代脉搏，体系新颖、条理清晰、实用性强，适合作为高等职业院校专科信息技术课程教材，也可作为信息技术爱好者自学用书。

图书在版编目（CIP）数据

信息技术：拓展模块 / 丁爱萍，吴教育主编. —
北京：北京出版社，2021.9（2023重印）
ISBN 978-7-200-16643-9

I. ①信… II. ①丁… ②吴… III. ①电子计算机
IV. ①TP3

中国版本图书馆 CIP 数据核字（2021）第 207972 号

信息技术（拓展模块）

XINXI JISHU (TUOZHAN MOKUAI)

主 编：丁爱萍 吴教育

出 版：北京出版集团
北 京 出 版 社

地 址：北京北三环中路6号

邮 编：100120

网 址：www.bph.com.cn

总 发 行：北京出版集团

经 销：新华书店

印 刷：定州启航印刷有限公司

版 印 次：2021年9月第1版 2023年7月修订 2023年7月第2次印刷

成品尺寸：210毫米 × 285毫米

印 张：16

字 数：462千字

书 号：ISBN 978-7-200-16643-9

定 价：49.80元

教材意见建议接收方式：010-58572162 邮箱：jiaocai@bphg.com.cn

如有印装质量问题，由本社负责调换

质量监督电话：010-82685218 010-58572162 010-58572393

单元一 信息安全

任务一	信息安全概述	2
任务二	信息安全防御技术	9
任务三	信息安全应用	14

单元二 项目管理

任务一	项目管理基础知识	25
任务二	项目管理工具应用	32

单元三 机器人流程自动化

任务一	机器人流程自动化基础知识	41
任务二	机器人流程自动化工具应用	45

单元四 程序设计基础

任务一	程序设计基础知识	59
任务二	程序设计语言和工具	61
任务三	程序设计方法和实践	65

单元五 大数据

任务一	大数据基础知识	85
任务二	大数据关键技术	93

单元六 人工智能

任务一	人工智能基础知识	106
任务二	人工智能核心技术	114
任务三	人工智能技术应用	121

单元七 云计算

任务一	云计算基础知识	134
任务二	云计算关键技术	141

单元八 现代通信技术

任务一	现代通信技术基础	148
任务二	5G 技术	153

单元九 物联网

任务一	物联网基础知识	160
任务二	物联网体系结构和关键技术	165
任务三	物联网系统应用	177

单元十 数字媒体

任务一	数字媒体基础知识	190
任务二	数字媒体素材处理技术	195

单元十一 虚拟现实

任务一	虚拟现实技术基础知识	206
任务二	虚拟现实应用开发	215

单元十二 区块链

任务一	区块链基础知识	231
任务二	区块链关键技术	239

单元一 信息安全

问题导入

随着计算机和网络技术的发展和普及，社会的信息化程度越来越高，信息资源也得到更大程度的共享。但随着信息化发展而来的网络信息安全问题也暴露出来，如果不能解决好这个问题，必将阻碍信息化的发展进程。计算机和网络的使用可以为人类造福，也可能给人类带来危害，关键在于使用者采取的道德态度，遵循的行为规范和约束机制。

信息安全是指信息产生、制作、传播、收集、处理、选取等信息使用过程中的信息资源安全。建立信息安全意识，了解信息安全相关技术，掌握常用的信息安全应用，是现代信息社会对高素质技术技能人才的基本要求。

学习要点

1. 建立信息安全意识，能识别常见的网络欺诈行为。
 2. 了解信息安全的基本概念，包括信息安全基本要素、网络安全等级保护等内容。
 3. 了解信息安全相关技术，了解信息安全面临的常见威胁和常用的安全防御技术。
 4. 了解常用网络安全设备的功能和部署方式。
 5. 了解网络信息安全保障的一般思路。
 6. 掌握利用系统安全中心配置防火墙的方法。
 7. 掌握利用系统安全中心配置病毒防护的方法。
 8. 掌握常用的第三方信息安全工具的使用方法，并能解决常见的安全问题。
- 本单元包含信息安全意识、信息安全防御技术、信息安全应用等内容。

任务一 信息安全概述

任务描述

信息安全本身包括的范围很大，大到国家政治军事机密安全，小到防范政府企业机密的泄露、个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，任何一个安全漏洞都可以威胁全局安全。

本任务介绍信息安全的概念、影响因素、等级保护，以及信息道德与相关法规等。

学习目标

1. 了解信息安全的概念和影响因素。
2. 了解信息安全面临的主要威胁。
3. 了解信息安全策略。
4. 了解信息安全等级保护的基本知识。
5. 了解使用计算机和网络应遵守的道德规范。
6. 了解国家对知识产权和软件使用的要求，以及信息安全的相关法律法规。

任务实现

一、信息安全的概念

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续正常地运行，信息服务不中断，最终实现业务连续性。

二、信息安全的影响因素

信息安全的影响因素很多，主要有以下几个方面。

(1) 硬件及物理因素：指系统硬件及环境的安全性，如机房设施、计算机主体、存储系统、辅助设备、数据通信设施以及存储介质的安全性。

(2) 软件因素：指系统软件及环境的安全性，软件的非法删改、复制与窃取都可能造成系统损失、泄密等情况。例如，计算机病毒就是以软件为手段侵入系统造成破坏的。

(3) 人为因素：指人为操作、管理的安全性，包括工作人员的素质和责任心，严密的行政管理制度，完善的法律法规等。防范人为因素方面的安全威胁，即是防范人为主动因素直接对系统安全所造成的威胁。

(4) 数据因素：指数据信息在存储和传递过程中的安全性。数据因素是计算机犯罪的核心途径，也是信息安全的重点。

(5) 其他因素：信息和数据传输通道在传输过程中产生的电磁波辐射，可能被检测或接受，造成信息泄露；同时空间电磁波也可能对系统产生电磁干扰，影响系统的正常运行。此外，一些不可抗力的自然因素，也可能对系统的安全造成威胁。

在研究信息安全问题时，更关注于恶意的犯罪导致的对信息安全的威胁，如信息窃取、信息截

取、信息伪造、信息篡改、拒绝服务攻击、行为否认、非授权访问和传播病毒等。

案例 1-1

超 2 亿国内个人信息在国外暗网论坛兜售

2021 年 1 月，国外安全研究团队 Cyble 发现多个帖子正在出售与中国公民有关的个人数据，经分析来自微博、QQ 等多个社交媒体。本次发现的几个帖子中与中国公民有关的记录总数超过 2 亿。

案例 1-2

可怕的“U 盘小偷”

在某大学期末考试期间，在一门全校公共课的考场上，监考老师发现了多起考试舞弊事件，涉及多个系别。让人吃惊的是，学生舞弊的纸条上有着本次考试的全部试题及标准答案，也就是说试卷泄密了。后来报警调查后发现某系学生利用“U 盘小偷”程序盗走了老师 U 盘上的资料，并传播获得一定的收益。而后该学生被判刑并被开除学籍。

案例 1-3

美国 NASDAQ 事故

1994 年 8 月 1 日，一只松鼠在该证券交易系统网络主计算机的一条电话线附近挖洞，造成电源紧急控制系统损坏，NASDAQ 电子交易系统“日均超过 3 亿股”的股票市场暂停营业近 34 分钟。

三、信息安全的目标

国际标准化组织定义信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。研究信息安全就是为了实现以下目标。

- (1) 真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。
- (2) 保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。
- (3) 完整性：保证数据的一致性，防止数据被非法用户篡改。
- (4) 可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。
- (5) 不可抵赖性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中极其重要。
- (6) 可控制性：对信息的传播及内容具有控制能力。
- (7) 可审查性：对出现的网络安全问题提供调查的依据和手段。

四、信息安全的主要威胁

信息安全威胁主要来自人为因素。常见的信息安全威胁有以下几个方面。

1. 信息泄露

网络中的数据文件或进行网络通信时，如果不采取任何保密措施，数据文件或通信内容就有可能被他人看到，造成信息泄露。如果是未经系统授权而使用网络或计算机资源，这就是非授权访问。或者内部人员安全意识差而造成信息泄露，这是一种内部泄露行为。



信息安全威胁

⇒ 案例 1-4

全国首例利用微信清粉软件获取用户信息案宣判

2021 年 3 月 3 日，江苏南通通州公安对全国首例利用微信清粉软件非法获取微信用户信息进行宣判。被害用户扫描“清粉”二维码是给微信通讯录“瘦身”，不料导致个人信息泄露。8 名被告人则以刷阅读量、售卖微信群聊二维码等方式非法获利 200 多万元。

2. 信息窃取

非法用户通过数据窃听、流量分析等各种手段窃取系统中的信息资源和敏感信息。例如，对通信线路传输的信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄漏截取有用信息等。业务流分析则是通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

⇒ 案例 1-5

央视曝 App 偷听隐私

2021 年 1 月，央视节目中专家用模拟“App 偷听测试程序”发送一个 2 秒的语音，当手松开后，录音仍在继续，并生成一条 120 秒的语音，证实了当测试程序置于前台运行时，偷听是可以实现的。此外经过对比实验，发现在测试程序退至后台或在手机锁屏时，录音依然可持续一段时间。

3. 冒名顶替

通过欺骗通信系统或用户，达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。侵入者通常通过一个合法的用户账号和密码来获得网络服务。

4. 篡改信息

非法用户对合法用户之间的通信信息进行修改，生成伪造数据，再发给接收者。信息篡改是一种严重的主动威胁，其危害程度有时比主动攻击更甚。这种主动威胁可以发生在通信线路上的任何地方，如电缆、微波线路、卫星信道、路由节点、主机或客户计算机系统等。

5. 行为否认

行为否认又称抵赖。在网络中，合法用户在电子商务等交易活动中不能否认其曾经发出的报文。在传统的交易活动中，可以通过用户的亲笔签名或印章来保证合同的有效性。在网络中，要保证发送者对报文的不可抵赖是通过数字签名实现的。

6. 授权侵犯

被授权以某一目的使用某些资源的人，却将此授权用于非授权的目的，也称为内部攻击。

7. 恶意攻击

恶意攻击是当前网络中存在的最大信息安全威胁之一。一般通过“黑客”程序持续扫描指定的网段，查找计算机系统漏洞，从而传播病毒、设置木马，以达到控制对方计算机的目的。当黑客控制很多计算机后，通常会采用拒绝服务和注入漏洞的方式对网络进行攻击。

案例 1-6

西山居旗下逍遥网遭攻击致数据泄露

2021年3月,西山居游戏发公告称,西山居旗下产品屡遭不法分子DDoS攻击、服务器入侵,导致部分用户账号和加密后的非明文密码等信息外泄,官方建议第一时间修改安全等级偏低的短位密码。

五、信息安全策略

信息安全策略是指为保证提供一定级别的安全保护所必须遵守的规则。为了保证信息安全,需要从先进的技术、法律约束、严格的管理和安全教育等着手,制定完善的规则。

1. 先进的技术

先进的信息安全技术是信息安全的根本保证,用户对自身面临威胁的风险性进行评估,然后对所需要的安全服务种类进行确定,通过相应的安全机制,集成先进的安全技术,形成全方位的安全系统。

2. 法律约束

法律法规是信息安全的基石,必须建立与网络安全相关的法律法规,对网络犯罪行为实施约束。《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《中华人民共和国网络安全法》等都是有关信息安全的法律法规。

3. 严格的管理

信息安全管理是提高信息安全的有效手段,对于计算机网络使用机构、企业和事业单位而言,必须建立相应的网络安全管理办法和安全管理系统,加强对内部信息安全管理,建立起合适的安全审计和跟踪体系,提高网络安全意识。

4. 安全教育

要建立网络安全管理系统,在提供技术、制定法律、加强管理的基础上,还应加强安全教育,提高用户的安全意识,对网络攻击与攻击检测、网络安全防范、安全漏洞与安全对策、信息安全保密、系统内部安全防范、病毒防范、数据备份与恢复等有一定的了解,及时发现潜在问题,尽早解决安全隐患。

六、信息安全等级保护

信息安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作,要求不同安全等级的信息系统应具有不同的安全保护能力。

《信息安全等级保护管理办法》规定,国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度,信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

信息系统的安全保护等级分为以下五级,一至五级等级逐级增高。

第一级,信息系统受到破坏后,会对公民、法人和其他组织的合法权益造成损害,但不损害国家安全、社会秩序和公共利益。第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级,信息系统受到破坏后,会对公民、法人和其他组织的合法权益产生严重损害,或者对

社会秩序和公共利益造成损害，但不损害国家安全。国家信息安全监管部门对该级信息系统安全等级保护工作进行指导。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行监督、检查。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行强制监督、检查。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行专门监督、检查。

《中华人民共和国网络安全法》规定：“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。”

七、使用计算机应遵守的道德规范

在高度信息化的今天，信息已深入到社会生活的各个方面，信息安全不仅是安全管理人员的责任，同时也需要全社会的共同维护。在享受信息化带来的优质服务的同时，也需要遵守相应的道德规范和法律法规。

国外一些计算机和网络组织制定了一系列规范，比较著名的是美国计算机伦理学会制定的 10 条戒律。这些规范是一个计算机用户在任何情况下都应该遵循的最基本的行为准则。具体内容如下。

- (1) 不应该用计算机去伤害别人。
- (2) 不应该干扰别人的计算机工作。
- (3) 不应该窥探别人的文件。
- (4) 不应该用计算机进行偷窃。
- (5) 不应该用计算机作伪证。
- (6) 不应该使用或复制没有付费的软件。
- (7) 不应该未经许可而使用别人的计算机资源。
- (8) 不应该盗用别人的智力成果。
- (9) 应该考虑所编写程序的社会后果。
- (10) 应该以深思熟虑和慎重的方式来使用计算机。

八、网络社会应遵守的道德规范

我国的信息产业，特别是互联网行业发展迅速，目前我国已拥有世界上人数最多的网民群。在这种情况下，互联网的道德规范建立显得尤其重要。

从 2002 年起，中国互联网协会先后颁布了一系列行业自律规范，主要包括：《中国互联网行业自律公约》《互联网新闻信息服务自律公约》《互联网站禁止传播淫秽、色情等不良信息自律规范》《中国互联网协会公共电子邮件服务规范》《搜索引擎服务商抵制违法和不良信息自律规范》《中国互联网网络版权自律公约》《文明上网自律公约》《抵制恶意软件自律公约》《博客服务自律公约》《中国互联网协会反垃圾短信息自律公约》。

上述的公约规范与人类社会的其他道德规范一样，不仅要理解道德规范的基本原则，更要对这些基本原则深思熟虑，明白哪些应该做，哪些不应该做。

九、国家对知识产权和软件使用的规定

1990 年 9 月，我国颁布了《中华人民共和国著作权法》，把计算机软件列为享有著作权保护的

产品。

1991年6月，国务院发布了《计算机软件保护条例》，规定计算机软件是个人或者团体的智力产品，同专利、著作一样受法律保护。

任何未经授权的使用、复制都是非法的，按规定要受到法律的制裁。人们在使用计算机软件或数据时，应遵照国家有关法律规定，尊重其作品的版权，这是使用计算机的基本道德规范。

十、我国信息安全的相关法律法规

所有的社会行为都需要法律法规来规范和约束。随着网络的发展，我国各项涉及网络信息安全的法律法规也相继出台。

我国现行的信息安全法律体系包括以下四个方面。

1. 一般性法律规定

这类法律法规是指宪法、国家安全法、保守国家秘密法、治安管理处罚法、著作权法、专利法等。这些法律法规并没有专门对网络行为进行规定，但是，它所规范和约束的对象中包括了危害信息网络安全的行为。

2. 规范和惩罚网络犯罪的法律

这类法律包括《中华人民共和国刑法》《全国人大常委会关于维护互联网安全的决定》等。其中，刑法也是一般性法律规定，这里将其独立出来，作为规范和惩罚网络犯罪的法律规定。

3. 直接针对计算机信息网络安全的特别规定

这类法律法规主要有《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际联网管理暂行规定》《计算机信息网络国际联网安全保护管理办法》《中华人民共和国计算机软件保护条例》等。

4. 具体规范信息网络安全技术、信息网络安全管理等方面的规定

这一类法律主要有《商用密码管理条例》《计算机信息系统安全专用产品检测和销售许可证管理办法》《计算机病毒防治管理办法》《计算机信息系统保密管理暂行规定》《计算机信息系统国际联网保密管理规定》《电子出版物管理规定》《金融机构计算机信息系统安全保护工作暂行规定》等。

2016年11月7日，十二届全国人大常委会第二十四次会议表决通过《中华人民共和国网络安全法》，2017年6月1日起正式施行。《网络安全法》是中国网络安全领域的第一部专门法律，是保障网络安全的基本法，这是中国建立严格的网络治理指导方针的一个重要里程碑。《网络安全法》共有七章七十九条，内容十分丰富，具有六大突出亮点。

- (1) 明确了网络空间主权的原则。
- (2) 明确了网络产品和服务提供者的安全义务。
- (3) 明确了网络运营者的安全义务。
- (4) 进一步完善了个人信息保护规则。
- (5) 建立了关键信息基础设施安全保护制度。
- (6) 确立了关键信息基础设施重要数据跨境传输的规则。

《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，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法治利器，是让互联网在法治轨道上健康运行的重要保障。



思考和训练

1. 思考影响信息安全的因素有哪些。
2. 结合你在工作和生活中遇到的问题，谈谈目前信息安全面临的主要威胁有哪些。
3. 为什么要对信息安全分等级进行保护？
4. 你认为使用计算机和网络应遵守哪些道德规范？
5. 上网查询国家对知识产权和软件使用的要求，以及信息安全的相关法律法规。
6. 上网查询影响信息安全的相关案例，对案例进行分析，判断其属于哪类威胁因素，指出产生的危害及处罚建议。
7. 上网查询斯诺登事件（也称“棱镜门”），了解事件背景、事件发展、事件影响，谈谈你的看法。

任务二 信息安全防御技术

任务描述

信息安全防御技术主要用于防止系统漏洞、防止外部黑客入侵、防御病毒破坏、对可疑访问进行有效控制等，同时还包含数据灾难与数据恢复技术，即在计算机发生意外或灾难时，可以使用备份还原及数据恢复技术将丢失的数据找回。

本任务将介绍几种典型的信息安全防御技术。

学习目标

1. 了解信息加密技术的基本知识。
2. 了解认证技术的基本知识。
3. 了解访问控制技术的基本知识。
4. 了解防火墙技术的基本知识。
5. 了解入侵检测技术的基本知识。
6. 了解云安全技术的基本知识。
7. 了解系统容灾技术的基本知识。

任务实现

一、加密技术

信息加密的目的是保护网络中的数据、文件、口令和控制信息，保护网上传输的数据。

1. 加密和解密

密码技术包含两方面内容，即加密和解密。

- (1) 加密就是研究、编写密码系统，把数据和信息转换为不可识别的密文的过程。
- (2) 解密就是研究密码系统的加密途径，恢复数据和信息的本来面目的过程。

加密和解密过程共同组成了加密系统，如图 1-2-1 所示。

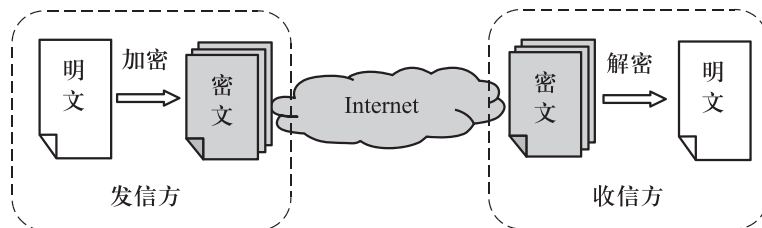


图 1-2-1 加密和解密过程

2. 对称密钥密码体制和非对称密钥密码体制

根据加密和解密过程是否使用相同的密钥，加密算法可分为对称密钥加密算法和非对称密钥加

密算法。

（1）对称密钥加密算法。

在大多数的对称算法中，加密密钥和解密密钥是相同的，所以也称这种加密算法为秘密密钥算法或单密钥算法。它要求发送方和接收方在安全通信之前，商定一个密钥。对称加密技术如图 1-2-2 所示。

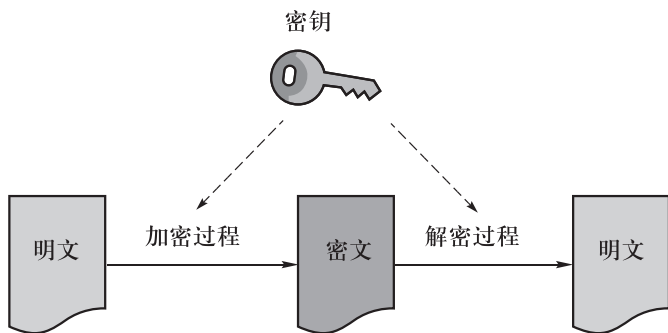


图 1-2-2 对称加密技术

对称算法的安全性依赖于密钥，泄露密钥就意味着任何人都可以对他们发送或接收的消息解密，所以密钥的保密性对通信的安全性至关重要。

（2）非对称密钥加密算法（又称公开密钥加密算法）。

非对称加密算法需要两个密钥：公开密钥和私有密钥。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法称为非对称加密算法，如图 1-2-3 所示。

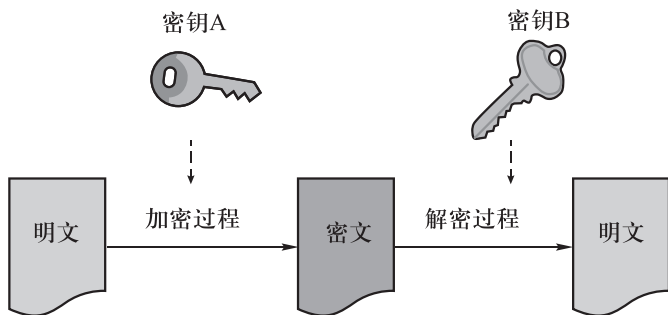


图 1-2-3 非对称加密技术

非对称加密算法比对称加密算法慢数千倍，但在保护通信安全方面，非对称加密算法更具优势。

二、认证技术

认证就是对于证据的辨认、核实、鉴别，以建立某种信任关系。在通信中，要涉及两方面：一方提供证据或标识，另一方对这些证据或标识的有效性进行辨认、核实、鉴别。

1. 数字签名

数字签名是数字世界中的一种信息认证技术，是公开密钥加密技术的一种应用，是根据某种协议来产生一个被签署文件的特征和签署人特征，以保证文件的真实性和有效性的数字技术，同时也可用来核实接收者是否有伪造、篡改行为。

2. 身份验证

身份验证是指通过一定的手段，完成对用户身份的确认。身份验证的方法很多，基本上可分为基于共享密钥的身份验证、基于生物学特征的身份验证、基于公开密钥加密算法的身份验证。不同的身份验证方法，其安全性也各有高低。

数字签名认证技术的基本原理，如图 1-2-4 所示。

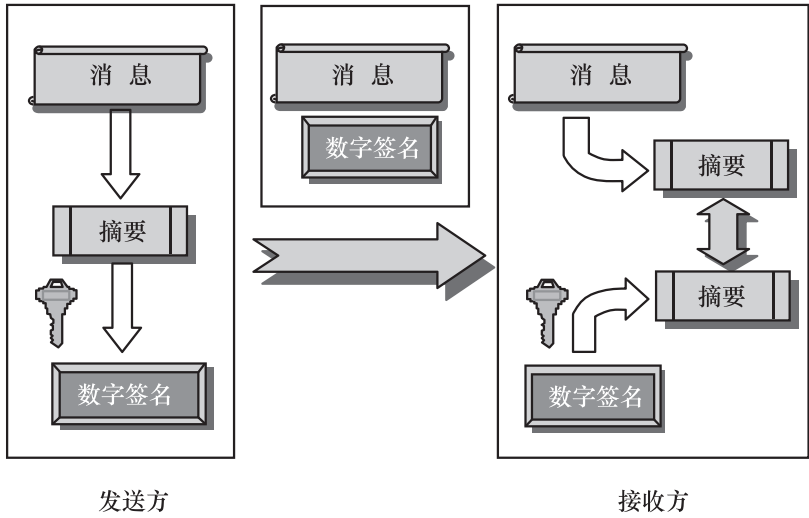


图 1-2-4 数字签名认证技术基本原理

三、访问控制技术

访问控制是对信息系统资源的访问范围及方式进行限制的策略。它是建立在身份认证之上的操作权限控制。

身份认证解决了访问者是否合法，但并非身份合法就什么都可以做，还要根据不同的访问者，规定他们分别可以访问哪些资源，以及对这些可以访问的资源可以用什么方式（读、写、执行、删除等）访问。

访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问，涉及的技术比较广，包括入网访问控制、网络权限控制、目录级安全控制、属性安全控制和服务器安全控制格式等多种手段。

例如，基于角色的访问控制技术，如图 1-2-5 所示。

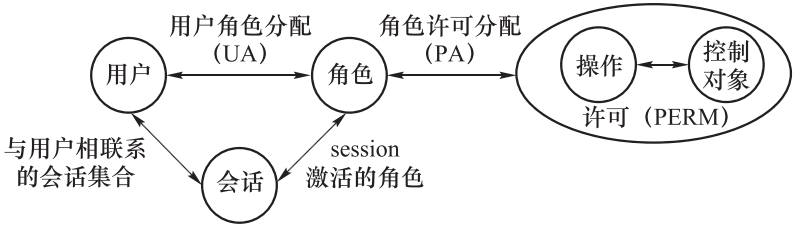


图 1-2-5 基于角色的访问控制技术

四、防火墙技术

防火墙是一种位于内部网络与外部网络之间的网络安全防护系统，如图 1-2-6 所示，可以依照特定的规则允许或限制传输的数据通过，主要用于对内部网和公众访问网进行隔离，使一个网络不受另一个网络的攻击。

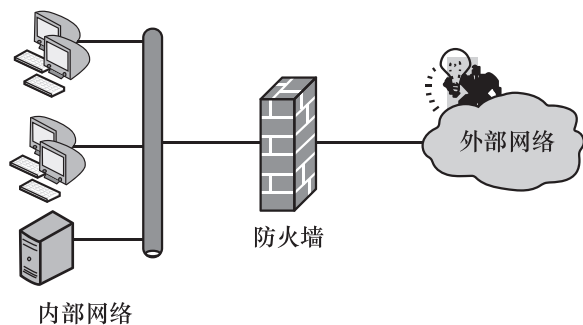


图 1-2-6 防火墙技术

防火墙的主要作用如下。

- (1) 可以限制他人进入内部网络，过滤掉不安全服务和非法用户。
- (2) 防止入侵者接近你的防御设施。
- (3) 限定用户访问特殊站点。
- (4) 为监视 Internet 安全提供方便。

目前防火墙技术已经在计算机网络得到广泛应用。

五、入侵检测

入侵检测系统 (Intrusion Detection System, IDS) 是一种对网络活动进行实时监测的专用系统。该系统处于防火墙之后，是防火墙之后的第二道安全闸门，如图 1-2-7 所示。通过收集和分析网络行为、安全日志、审计数据、其他网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。

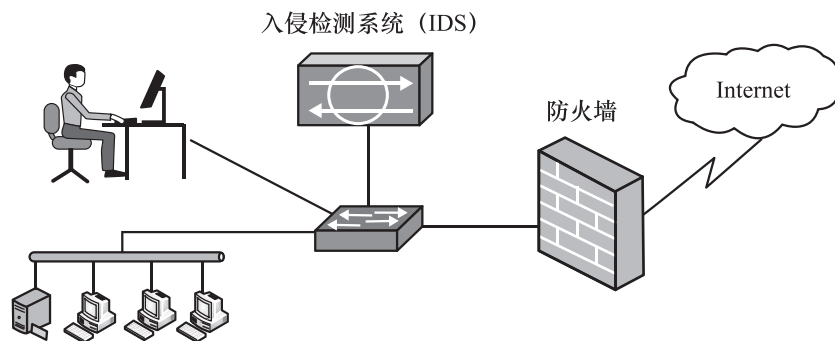


图 1-2-7 入侵检测系统

入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。入侵检测系统能够帮助网络系统快速发现攻击的发生，扩展了系统管理员的安全管理能力。

六、云安全技术

云安全技术是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件异常行为的监测，获取互联网中木马、恶意程序的最新信息，推送到服务器端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。



你要知道的云安全

七、系统容灾

系统容灾主要包括基于数据备份和基于系统容错的系统容灾技术。数据备份是数据保护的最后

屏障，不允许有任何闪失，但离线介质不能保证安全。数据容灾通过 IP 容灾技术来保证数据的安全，它使用两个存储器，在两者之间建立复制关系，一个放在本地，另一个放在异地，本地存储器供本地备份系统使用，异地容灾备份存储器实时复制本地存储器的关键数据。

存储、备份和容灾技术的充分结合，构成了一体化的数据容灾备份存储系统。随着存储网络化时代的发展，传统的功能单一的存储器将越来越让位于一体化的多功能网络存储器。

为了保证信息系统的安全性，除了运用安全防御技术手段外，还必须有管理手段和政策法规支持。管理手段是指确定安全管理等级和安全管理范围，制定网络系统的维护制度和应急措施等。政策法规支持是指借助法律手段强化保护信息系统安全，防范计算机犯罪，维护合法用户的安全，有效打击和惩罚违法行为。



思考和训练

1. 信息加密的目的是什么？对称加密和非对称加密的不同之处是什么？
2. 数字签名在信息传输中有什么作用？
3. 访问控制技术的作用是什么？
4. 什么是防火墙？为什么要设置防火墙？
5. 入侵检测系统在信息安全中有什么作用？
6. 什么是云安全技术？
7. 系统容灾的作用是什么？
8. 上网搜索并学习信息安全防御技术的相关视频、微课、文章等，理解并记录要点，列出不少于 3 项信息安全防御技术的作用和特点。

任务三 信息安全应用

任务描述

随着信息技术的飞速发展，计算机已经成为不同领域、不同职业的重要信息交换媒介。计算机用户要做好安全防范，必须要掌握配置防火墙、防范计算机病毒和黑客攻击、保护计算机安全使用的方法。

本任务将介绍配置防火墙的方法、病毒防护的方法，以及第三方安全工具的使用方法。

学习目标

1. 掌握利用系统安全中心配置防火墙的方法。
2. 了解计算机病毒的概念和特点。
3. 掌握利用系统安全中心配置病毒防护的方法。
4. 了解网络黑客的概念、黑客攻击方式和防范办法。
5. 掌握常用的第三方信息安全工具（360 安全卫士）的使用方法，并能解决常见的安全问题。

任务实现

一、配置防火墙

通过系统安全中心可以配置防火墙，可以较好地实现对计算机系统的信息安全防护。

(1) 打开计算机系统的“控制面板窗口”，单击“Windows Defender 防火墙”项，如图 1-3-1 所示。

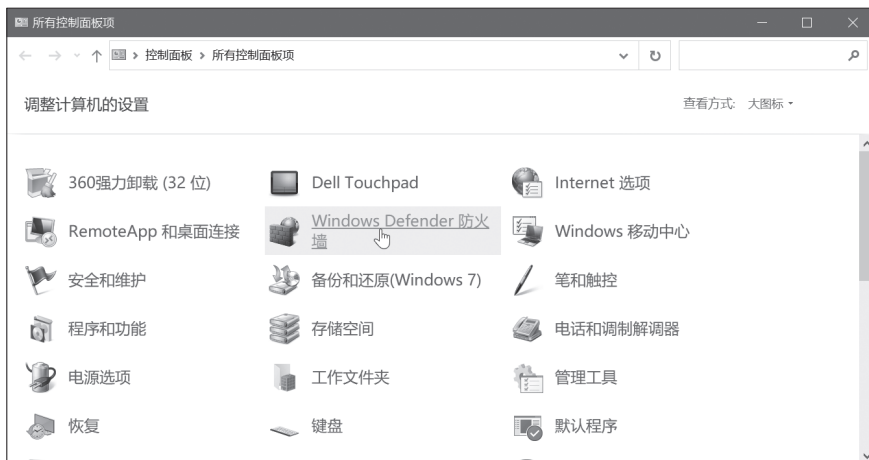


图 1-3-1 “控制面板”窗口

(2) 在弹出的“Windows Defender 防火墙”窗口中，单击左侧的“启用或关闭 Windows Defender 防火墙”项，如图 1-3-2 所示。



图 1-3-2 “Windows Defender 防火墙” 窗口

(3) 在弹出的“自定义设置”窗口中，系统默认防火墙为开启状态，根据需要进行相应设置，如图 1-3-3 所示。

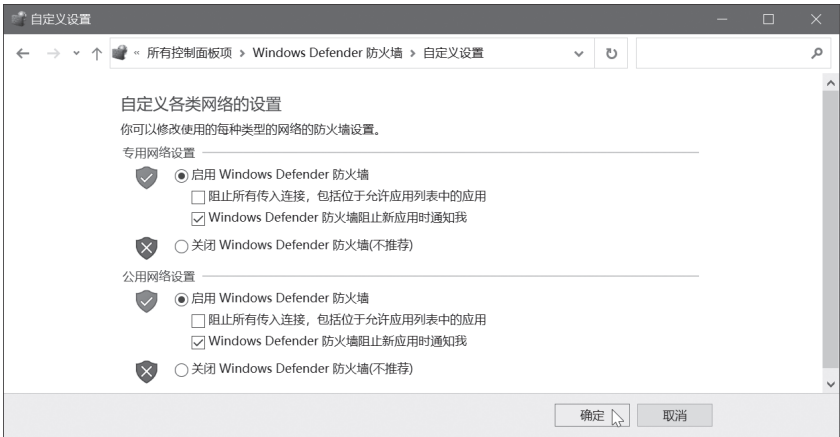


图 1-3-3 “自定义设置” 窗口

- (4) 单击“确定”按钮后，将返回“Windows Defender 防火墙”窗口。
- (5) 如果要恢复系统默认的防火墙设置，可以单击左侧的“还原默认值”项，如图 1-3-4 所示。



图 1-3-4 单击左侧的“还原默认值”项

(6) 在弹出的“还原默认值”窗口中，单击“还原默认值”按钮，在弹出的确认框中单击“是”，如图 1-3-5 所示。



图 1-3-5 “还原默认值”窗口

(7) 在“Windows Defender 防火墙”窗口中，单击“高级设置”项，弹出“高级安全 Windows Defender 防火墙”窗口，如图 1-3-6 所示，在此可以设置系统的入站规则、出站规则、连接安全规则以及监视选项。



图 1-3-6 “高级安全 Windows Defender 防火墙”窗口

二、计算机病毒的概念

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破坏数据、影响计算机使用、并且能够自我复制的一组计算机指令或者程序代码。也就是说，计算机病毒是一种计算机程序，它不仅能破坏计算机系统，而且还能传染到其他计算机系统。

提示

计算机病毒的传播大致分为以下两种。

- (1) 网络传播，包括互联网和局域网。
- (2) 移动介质传播，如 U 盘、移动硬盘、光盘等。

三、计算机病毒的特点

计算机病毒可谓五花八门，但它们有一些公共的特性。

1. 传染性

计算机病毒具有极强的传染性，病毒一旦入侵，就会不断地自我复制，占据磁盘空间，寻找适合其传染的介质，向其他计算机传播，达到破坏数据的目的。



电脑病毒知多少

2. 破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生程度不同的影响。轻者会降低计算机工作效率，重者对数据造成不可挽回的破坏，甚至导致系统崩溃。

3. 潜伏性

某些病毒可长期隐藏在系统中，只有在满足特定条件时才启动其破坏模块。例如，著名的“黑色星期五”病毒会在逢 13 号的星期五发作。

4. 隐蔽性

病毒一般是具有很高编程技巧、短小精悍的程序，通常附在正常程序中或磁盘较隐蔽的地方，也有个别以隐含文件的形式出现，目的是不让用户发现它的存在。

5. 不可预见性

从对病毒的检测方面来讲，病毒还有不可预见性。病毒的制作技术一直在不断地提高，病毒对反病毒软件来说永远是超前的。

四、常见的计算机病毒种类

网络的飞速发展给计算机病毒制造者、传播者提供了快速的传播手段和渠道。常见的病毒有以下几种。

1. 系统病毒

系统病毒一般共有的特性是感染 Windows 操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。

2. 蠕虫病毒

蠕虫病毒的特性是通过网络或者系统漏洞进行传播，大部分蠕虫病毒都有向外发送带毒的邮件、阻塞网络的特性。例如，冲击波病毒，它运行时不停地利用 IP 扫描技术寻找网络上操作系统为 Windows 的计算机，找到后就利用缓冲区漏洞不停地重启，甚至导致系统崩溃。

案例 1-7

网络攻击事件——多个行业感染 incaseformat 病毒

2021 年 1 月 13 日，国内多家安全厂商检测到蠕虫病毒 incaseformat 在国内大范围爆发，涉及政府、医疗、教育、运营商等多个行业，且感染的主机多为财务管理相关应用系统。感染的主机表现为所有非系统分区文件被删除，对用户造成不可挽回的损失。

3. 木马 / 黑客病毒

木马病毒的共有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，而黑客病毒则有一个可视的界面，能对用户的计算机进行远程控制。木马、黑客病毒一般成对出现，木马病毒负责侵入用户的计算机，而黑客病毒通过木马病毒来进行控制。木马病毒的前缀是 Trojan，黑客病毒的前缀一般为 Hack。

4. 宏病毒

宏病毒的共有特性是感染 Office 系列文档，然后通过 Office 通用模板进行传播。例如，著名的梅丽莎病毒，该病毒传播快、制作和变种方便、破坏性大。

提示

防范病毒的方法主要有以下几种。

(1) 给系统打补丁。

很多计算机病毒都是利用操作系统的漏洞进行感染和传播。如果使用 Windows 操作系统，用户可以在系统的正常状况下，登录微软的 Windows 网站进行有选择地更新。在网络连通的状态下，用户可以通过控制面板把系统设置成自动更新。

(2) 更新或升级杀毒软件和防火墙。

正版的杀毒软件及防火墙都提供了在线升级的功能，用户将病毒库（包括程序）升级到最新，然后进行病毒查杀。

五、配置杀毒软件

(1) 单击 Windows 桌面的“开始”按钮，在“开始”菜单中选择“设置”命令，进入“Windows 设置”界面，如图 1-3-7 所示。



图 1-3-7 “Windows 设置”界面

(2) 单击“更新和安全”项，进入“Windows 更新”窗口，如图 1-3-8 所示。



图 1-3-8 “Windows 更新”窗口

(3) 单击“Windows 安全中心”项，进入“Windows 安全中心”窗口，可以查看和管理设备安全性和运行状况，如图 1-3-9 所示。

(4) 单击“病毒和威胁防护”项，打开“病毒和威胁防护”窗口，单击“打开应用”项，如果已经安装第三方保护软件，系统将打开第三方软件进行实时保护，如图 1-3-10 所示。

(5) 单击“保护更新”项，将对病毒和威胁防护进行更新，以保障获取最新的安全情报。

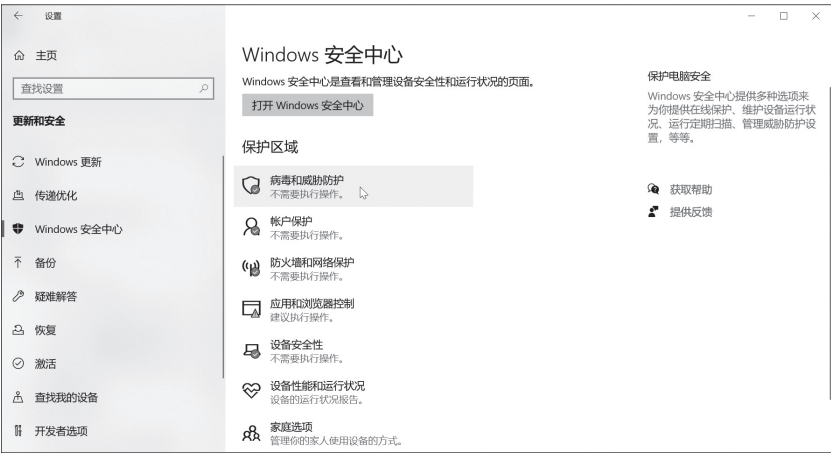


图 1-3-9 “Windows 安全中心” 窗口

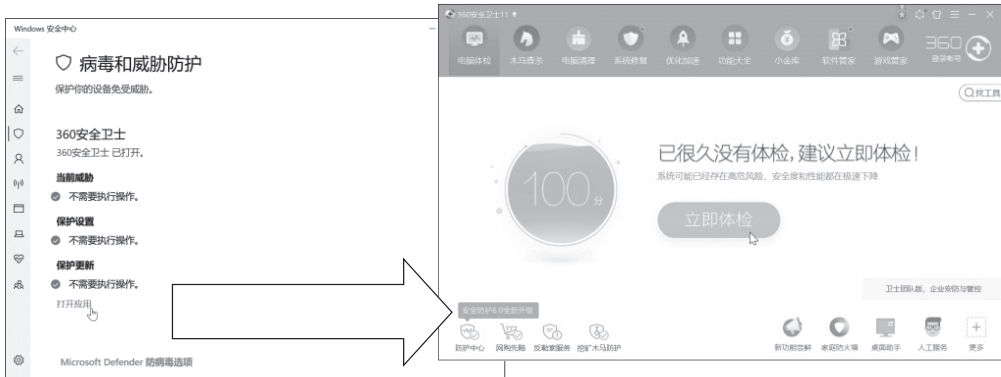


图 1-3-10 “病毒和威胁防护” 窗口

六、网络黑客的概念

黑客 (Hacker)，早期在美国的计算机界是带有褒义的，是对一群智力超群、奉公守法的计算机迷的统称。也就是说，“黑客”原指那些热心于计算机技术、水平高超的计算机专家。

黑客一般都精通各种编程语言和各类操作系统，拥有熟练的计算机技术。事实上，根据黑客的行为，行业内也对黑客的类型进行了细致的划分。

1. 黑帽黑客

在未经许可的情况下，进入对方系统的黑客一般称为黑帽黑客。黑帽黑客对计算机安全或账户安全都具有很大的威胁性，如非法获取支付结算、证券交易、期货交易等网络金融服务的账号、密码等信息。

2. 白帽黑客

调试和分析计算机系统的黑客称为白帽黑客，他们一般有明确的道德规范，其行为以发现和改善计算机安全弱点为主。

但今天，黑客泛指专门利用计算机漏洞搞破坏和恶作剧的人。

七、黑客攻击方式

1. 密码破解

如果不知道密码而随便输入一个，猜中概率很低。但如果连续测试一万个或更多的密码，那么猜中的概率就会非常高，尤其利用计算机自动测试。

例如，假设密码有 8 位，每一位可以是 26 个字母（大小写 52 个）和 10 个数字，每一位的选择就有 62 种，密码的组合可达 62^8 个（约 219 万亿），如果逐个去验证所需时间太长，所以黑客一般会利用密码破解程序尝试破解用户常用的密码，如生日、手机号、门牌号、姓名加数字等。

提示

设置密码要尽量复杂，以便增加破解难度，保障密码安全。

- (1) 密码要尽可能长，不少于 6 位。
- (2) 不用自己的姓名、昵称、出生日期、电话号码等。
- (3) 包含不同类型字符，如数字、大写字母、小写字母、特殊字符等。
- (4) 不同网站设置不同的用户名和密码。

2. IP 嗅探

IP 嗅探也称网络监听。黑客通过改变网卡的操作模式接收流经该计算机的所有信息包，截获其他计算机的数据报文或密码。例如，当用户 A 通过 Telnet 远程登录到用户 B 的机器上以后，黑客就可能通过网络监听软件截获用户 B 的 Telnet 数据包。

案例 1-8

2014 年 3 月，某网站安全支付日志存在漏洞，黑客遍历下载导致大量用户银行卡信息泄露（包含持卡人姓名、身份证号、银行卡号等）。

3. 端口扫描

利用一些端口扫描软件对被攻击的目标计算机进行端口扫描，查看该机器的哪些端口是开放的，然后通过这些开放的端口发送木马程序到目标计算机上，利用木马来控制被攻击的目标。

案例 1-9

2015 年，俄罗斯黑客利用 Twitter 中看似是照片的数据侵入了美国国防系统，入侵了美国政府，并攻陷了美国国防部多台电脑。这些俄罗斯黑客的机器每天检测不同的 Twitter 账户，一旦账户被注册，入侵用户电脑的行为就会被激活。当用户发送推特信息，如网址、数字、信件时，其电脑就会自动转到特定网址，用户信息也会随之被解码。

4. 网络钓鱼

就是黑客利用具有欺骗性的电子邮件和伪造的 Web 站点进行网络诈骗活动。诈骗者将自己伪装成网络银行、信用卡公司等，向用户发送类似紧急通知、身份确认等虚假信息，并诱导单击邮件中的超链接进入伪造网页，骗取用户的私人信息。

案例 1-10

针对农信社和城商行的短信钓鱼攻击

2021 年春节期间，全国多地市连续发生通过群发短信方式，以手机银行失效或过期等为由，诱骗客户点击钓鱼网站链接而盗取资金的安全事件。天际友盟检测发现大批钓鱼网站在 2 月 9 日后被注册并陆续投入使用，钓鱼网站域名为农信社、城商行等金融机构客服电话 + 字母，或与金融机构网站相似域名的形式，这些域名多为境外域名注册商注册并托管。

八、网络黑客的防范

黑客攻击会造成不同程度的损失,为了将损失降到最低限度,要了解一些防范网络黑客攻击的方法。

(1) 通过密码、指纹、面部特征或视网膜图案等特征信息来确认用户的真实性,只对确认了的用户给予相应的访问权限。

(2) 屏蔽可疑 IP 地址。这种方式见效最快,一旦网络管理员发现可疑 IP 地址申请,可以通过防火墙屏蔽,这样黑客就无法再连接到服务器上。但这种方法也有一些缺点,例如,很多黑客使用动态 IP 地址,一个 IP 地址被屏蔽,只要更换为其他 IP 地址,就可以继续攻击服务器,而且高级黑客有可能会伪造 IP 地址。

(3) 过滤信息包。通过编写防火墙规则,可以让系统知道什么样的信息包可以进入,什么样的信息包应该放弃。当黑客发送的攻击性信息包经过防火墙时,就会被丢弃掉,从而防止了黑客的进攻。

(4) 关闭不必要的服务和无用端口。系统中安装的软件越多,所提供的服务就越多,而存在的系统漏洞也越多,因此对于不需要的服务可以关闭。计算机进行网络连接必须通过端口,黑客控制用户计算机也必须通过端口,因此对于暂时无用的端口可将其关闭,减少黑客的攻击路径。

(5) 建立完善的访问控制策略。设置入网访问权限、网络共享资源的访问权限、目录安全等级控制、网络端口和节点安全控制、防火墙安全控制等,通过各种安全控制机制的相互配合,最大限度地保护系统。

(6) 经常升级系统版本。任何一个版本的系统发布之后,一旦其中的问题暴露出来,黑客就会蜂拥而至。管理员在维护系统时,可经常浏览著名的安全站点,找到系统的新版本或者补丁程序进行安装,以保证系统中的漏洞在没有被黑客发现之前已经修补上,从而保证服务器的安全。

(7) 安装必要的安全软件。用户还应在计算机中安装并使用必要的防黑客软件、杀毒软件和防火墙。在上网时打开它们,这样即使有黑客进攻,用户的安全也有一定保证。

九、使用 360 安全卫士

360 安全卫士是一款由奇虎公司推出的功能强、效果好、受用户欢迎的免费的安全杀毒软件。360 安全卫士拥有电脑体检、木马查杀、电脑清理、系统修复、优化加速等多种功能。

1. 下载和安装

(1) 登录“360 安全卫士”官方网站可以下载该款软件。

(2) 下载后,双击安装文件,这时系统首先对本机进行安全扫描,片刻后弹出安装向导,确认选中“我同意 360 授权许可协议”项,单击“下一步”按钮。

(3) 在“选择安装目录”中,直接单击“下一步”按钮,也可单击“更改目录”按钮选择其他安装位置。

(4) 经过一段时间的文件复制后,弹出“安装完成”对话框,单击“完成”按钮即安装完成。

(5) 双击桌面上 360 安全卫士的快捷方式,启动该软件。

2. 电脑体检

(1) 在“电脑体检”选项卡中,单击“立即体检”按钮,如图 1-3-11 所示,将自动检测系统中存在的问题。

(2) 单击“一键修复”按钮,将修复大多数问题,操作非常简单,修复完毕后给出检测结果。



图 1-3-11 电脑体检

提示

电脑的健康状况让我们担忧，某网站检测数据：有效检测人数为 2400 多万，其中比较安全的占 8%，一般危险的占 41%，极度危险的占 51%；某安全网站数据：在 400 多万个提交的检测结果中，19% 在黑客暴露程度方面存在风险，12% 在 Windows 系统漏洞方面存在风险，4% 在特洛伊木马检查中存在风险。怎么样，你现在还有安全感吗？是否感到危险就在眼前？因此，电脑体检非常重要。

3. 木马查杀

360 安全卫士的“查杀木马”功能采用云查杀引擎、智能加速技术，比杀毒软件快数倍。在查杀木马的同时，360 安全卫士能自动修复被木马破坏的系统设置，大大简化了用户操作；将可疑文件上传改为并发操作，提高了上传效率和服务器的响应速度。

在“木马查杀”选项卡中，如图 1-3-12 所示，可以选择“快速查杀”“全盘查杀”或“按位置查杀”项，360 安全卫士软件会自动检测系统中有无木马的存在，并进行列举以便用户清除木马病毒。



图 1-3-12 木马查杀

4. 电脑清理

在“电脑清理”选项卡中，如图 1-3-13 所示，单击“全面清理”或“单项清理”项，360 安全卫士将扫描计算机中的各类垃圾、插件、痕迹等，并将扫描结果列出，同时给出建议，单击“一键清理”按钮即可清理。



图 1-3-13 电脑清理

5. 系统修复

在“系统修复”选项卡中，如图 1-3-14 所示，提供了针对 Windows 系统漏洞的软件扫描，能够检测出计算机中存在哪些漏洞、缺少哪些补丁，并且给出修复建议，单击按钮“一键修复”即可修复。



图 1-3-14 系统修复

思考 and 训练

1. 检查自己所用的电脑，启用防火墙设置。
2. 思考计算机病毒的特点，感染计算机病毒的计算机一般会表现为哪些症状？
3. 作为重要部门的工作人员，应当采取什么样的病毒防范措施？
4. 如果病毒防治工具不具备实时监控或计算机用户不使用实时监控功能，会给计算机带来什么样的危害？
5. 在计算机中安装了杀毒软件后是否就万事无忧了？
6. 木马病毒有什么危害？我们应该怎样预防木马病毒？
7. 使用 360 安全卫士清除电脑中的恶意软件和插件。
8. 你经常使用 U 盘、移动硬盘来传送数据吗？检测你的移动设备中是否有病毒，如果有进行查杀。