网络空间安全专业规划教材

总主编◎杨义先　　执行主编◎李小勇

# 网络空间安全导论

## Fundamentals of Cybersecurity

雷敏　李小勇　李祺　苑洁　编著

北京邮电大学出版社
www.buptpress.com

网络空间安全专业规划教材

总主编　杨义先　　执行主编　李小勇

# 网络空间安全导论

雷　敏　李小勇　李　祺　苑　洁　编著



北京邮电大学出版社
www. buptpress. com

## 内 容 简 介

随着云计算、物联网、大数据、人工智能、工业控制网络等技术的快速发展，网络空间安全面临着新的挑战，网络空间作为继陆、海、空、太空之后的“第五维空间”，已经成为各国角逐权力的“新战场”。

本书主要面对网络空间安全的初学者，力图通过轻松简单的讲述方式让读者掌握网络空间安全的基础知识。书中没有复杂的公式推导，叙述简明扼要，通过生动的案例来简化读者对问题的理解过程。全书共分为10章，内容涵盖了物理安全、网络安全、内容安全、数据安全等多个方面。

本书可作为高等学校及各类培训机构网络空间安全相关课程的教材或教学参考书。

**图书在版编目(CIP)数据**

网络空间安全导论 / 雷敏等编著. --北京：北京邮电大学出版社，2018.8
ISBN 978-7-5635-5502-4

Ⅰ. ①网… Ⅱ. ①雷… Ⅲ. ①网络安全－高等学校－教材 Ⅳ. ①TN915.08

中国版本图书馆CIP数据核字（2018）第163044号

**书　　名**：网络空间安全导论
**著作责任者**：雷　敏　李小勇　李　祺　苑　洁　编著
**责任编辑**：徐振华　孙宏颖
**出版发行**：北京邮电大学出版社
**社　　址**：北京市海淀区西土城路10号（邮编：100876）
**发 行 部**：电话：010-62282185　传真：010-62283578
**E-mail**：publish@bupt.edu.cn
**经　　销**：各地新华书店
**印　　刷**：北京玺诚印务有限公司
**开　　本**：787 mm×1 092 mm　1/16
**印　　张**：8
**字　　数**：192千字
**版　　次**：2018年8月第1版　2018年8月第1次印刷

ISBN 978-7-5635-5502-4　　定　价：20.00元

# Prologue 序

Prologue

作为最新的国家一级学科，由于其罕见的特殊性，网络空间安全真可谓是典型的“在游泳中学游泳”。一方面，蜂拥而至的现实人才需求和紧迫的技术挑战，促使我们必须以超常规手段，来启动并建设好该一级学科；另一方面，由于缺乏国内外可资借鉴的经验，也没有足够的时间纠结于众多细节，所以，作为当初“教育部网络空间安全一级学科研究论证工作组”的八位专家之一，我有义务借此机会，向大家介绍一下2014年规划该学科的相关情况，并结合现状，坦诚一些不足，以及改进和完善计划，以使大家有一个宏观了解。

我们所指的网络空间，也就是媒体常说的赛博空间，意指通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间。它已成为继陆、海、空、太空之后的第五空间。网络空间里不仅包括通过网络互联而成的各种计算系统（各种智能终端）、连接端系统的网络、连接网络的互联网和受控系统，也包括其中的硬件、软件乃至产生、处理、传输、存储的各种数据或信息。与其他四个空间不同，网络空间没有明确的、固定的边界，也没有集中的控制权威。

网络空间安全，研究网络空间中的安全威胁和防护问题，即在有敌手对抗的环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施，以及网络和系统本身的威胁和防护机制。网络空间安全不仅包括传统信息安全所涉及的信息保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。

网络空间安全一级学科，下设五个研究方向：网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全。

方向1，网络空间安全基础，为其他方向的研究提供理论、架构和方法学指导；它主要研究网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等内容。

方向2，密码学及应用，为后三个方向（系统安全、网络安全和应用安全）提供密码机制；它主要研究对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护、量子密码与新型密码等内容。

方向3，系统安全，保证网络空间中单元计算系统的安全；它主要研究芯片安全、系统软件安全、可信计算、虚拟化计算平台安全、恶意代码分析与防护、系统硬件和物理环境安全等内容。

方向4，网络安全，保证连接计算机的中间网络自身的安全以及在网络上所传输的信息的安全；它主要研究通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御（攻防与对抗）、端到端的安全通信等内容。

方向5，应用安全，保证网络空间中大型应用系统的安全，也是安全机制在互联网应用或服务领域中的综合应用；它主要研究关键应用系统安全、社会网络安全（包括内容安全）、隐私保护、工控系统与物联网安全、先进计算安全等内容。

从基础知识体系角度看，网络空间安全一级学科主要由五个模块组成：网络空间安全基础、密码学基础、系统安全技术、网络安全技术和应用安全技术。

模块1，网络空间安全基础知识模块，包括：数论、信息论、计算复杂性、操作系统、数据库、计算机组成、计算机网络、程序设计语言、网络空间安全导论、网络空间安全法律法规、网络空间安全管理基础。

模块2，密码学基础理论知识模块，包括：对称密码、公钥密码、量子密码、密码分析技术、安全协议。

模块3，系统安全理论与技术知识模块，包括：芯片安全、物理安全、可靠性技术、访问控制技术、操作系统安全、数据库安全、代码安全与软件漏洞挖掘、恶意代码分析与防御。

模块4，网络安全理论与技术知识模块，包括：通信网络安全、无线通信安全、IPv6安全、防火墙技术、入侵检测与防御、VPN、网络安全协议、网络漏洞检测与防护、网络攻击与防护。

模块5，应用安全理论与技术知识模块，包括：Web安全、数据存储与恢复、垃圾信息识别与过滤、舆情分析及预警、计算机数字取证、信息隐藏、电子政务安全、电子商务安全、云计算安全、物联网安全、大数据安全、隐私保护技术、数字版权保护技术。

其实，从纯学术角度看，网络空间安全一级学科的支撑专业，至少应该平等地包含信息安全专业、信息对抗专业、保密管理专业、网络空间安全专业、网络安全与执法专业等本科专业。但是，由于管理渠道等诸多原因，我

们当初只重点考虑了信息安全专业，所以，就留下了一些遗憾，甚至空白，比如，信息安全心理学、安全控制论、安全系统论等。不过值得庆幸的是，学界现在已经开始着手，填补这些空白。

北京邮电大学在网络空间安全相关学科和专业等方面，在全国高校中一直处于领先水平，从20世纪80年代初至今，已有30余年的全方位积累，而且，一直就特别重视教学规范、课程建设、教材出版、实验培训等基本功。本套系列教材主要是由北京邮电大学的骨干教师们，结合自身特长和教学科研方面的成果，撰写而成。本系列教材暂由《信息安全数学基础》《网络安全》《汇编语言与逆向工程》《软件安全》《网络空间安全导论》《可信计算理论与技术》《网络空间安全治理》《大数据服务与安全隐私技术》《数字内容安全》《量子计算与后量子密码》《移动终端安全》《漏洞分析技术实验教程》《网络安全实验》《网络空间安全基础》《信息安全管理（第3版）》《网络安全法学》《信息隐藏与数字水印》等20余本本科生教材组成。这些教材主要涵盖信息安全专业和网络空间安全专业，今后，一旦时机成熟，我们将组织国内外更多的专家，针对信息对抗专业、保密管理专业、网络安全与执法专业等，出版更多、更好的教材，为网络空间安全一级学科提供更有力的支撑。

**杨义先**

教授、长江学者

国家杰出青年科学基金获得者

北京邮电大学信息安全中心主任

灾备技术国家工程实验室主任

公共大数据国家重点实验室主任

2017年4月，于花溪

# 前言

Foreword

Foreword

没有网络安全，就没有国家安全；没有网络安全人才，就没有网络安全。

为了更多、更快、更好地培养网络安全人才，国务院学位委员会正式批准增设“网络空间安全”一级学科。越来越多的高校申请“网络空间安全一级学科博士点”，并开办网络空间安全和信息安全专业。如今，许多高校都在努力培养网络安全人才，聘请优秀教师，招收优秀学生，建设一流的网络空间安全学院。

优秀教材是培养网络空间安全专业人才的关键。但是，写一本优秀教材却是一项十分艰巨的任务。原因有二：其一，网络空间安全的涉及面非常广，包括密码学、数学、计算机、操作系统、通信工程、信息工程、数据库、硬件等多门学科，因此，其知识体系庞杂，难以梳理；其二，网络空间安全的实践性很强，技术发展更新非常快，对环境和师资的要求很高。

“网络空间安全导论”是网络空间安全和信息安全专业的基础课程，通过本书对网络空间安全各知识面的介绍，读者可以掌握网络空间安全的基础知识。本书涉及的知识面较宽，共分为 10 章。

本书在撰写的过程中，参考了国内外的一些资料，在此对资料作者表示感谢!

本书既适合网络空间安全、信息安全等相关专业的学生作为教材和参考资料，也适合网络安全研究人员作为网络空间安全的入门基础读物。随着新技术的不断发展，今后将不断地更新本书内容。

由于作者水平有限，书中难免存在疏漏和不妥之处，欢迎读者批评指正。作者联系方式为 leimin@ bupt. edu. cn。

**编著者**

**2018 年 7 月**

# 目录

Contents

# 第 1 章

# 网络空间安全概述

随着信息化的发展，以互联网为基础的计算、通信等重要信息基础设施在社会生活中发挥着重要作用，但也面临着诸多安全隐患。随着云计算、物联网、大数据、人工智能、工业控制网络等技术的快速发展，网络空间安全面临着新的挑战，网络空间作为继陆、海、空、太空之后的“第五维空间”，已经成为各国角逐权力的“新战场”。

## 1.1 网络空间安全的基本认识

### 1.1.1 网络空间的概念

首先要明确“网络”的内涵与外延。一般认为，网络是由节点和连接边构成的，用来表示多个对象及其相互联系的互联系统。现实中的信息网络，可以抽象地概括为：将各个孤立的“端节点”（信息的生产者和消费者），通过“连接边”（物理或虚拟链路）将之连接在一起，进而实现各端节点间通过“交换节点”进行转发，以实现载荷在端节点之间进行交换。其中“载荷”是网络中数据与信息的表达形式，如电磁信号、光信号、量子信号、网络数据等。由此，网络包含了 4 个基本要素：端节点、连接边、交换节点和载荷。

以我们常用的发送 QQ 消息为例，当用户发送 QQ 消息时，端节点就为用户发送 QQ 消息时所使用的台式计算机、笔记本式计算机、手机或者 iPad 等终端；连接边就是终端设备所连接的网络，可以是家中的 WiFi，也可以是学生宿舍或者单位中的有线网络；交换节点就是腾讯公司的 QQ 服务器和网络中各种用于完成消息发送所需的网络设备；载荷就是 QQ 消息中发送的内容。

该定义反映出“网络”的含义很广泛，不仅互联网符合这一特征，电信网、物联网、传感网、工业控制网、广电网等各类信息网络都符合“网络”的描述，因而本书对网络的讨论就不再仅仅限于互联网。

网络空间可以简单定义为：网络空间是一种人造的电磁空间，其以终端、计算机、网络设备等为载体，人类通过在其上对数据进行计算、通信来实现特定的活动。在这个空间中，人、机、物可以被有机地连接在一起并进行互动，可以产生影响人们生活的各类信息，包括内容信息、商务信息、控制信息等。

为了进一步分析网络空间，需要在直观定义的基础上，进一步地给出学术性和技术性的定义。因此，学术上可以把网络空间定义为：网络空间是人类通过网络角色，依托信息通信技术系统来进行广义信号交互的人造活动空间。网络角色是指产生、传输广义信号的主体，反映的是人类的意志；信息通信技术系统包括互联网、电信网、无线网、移动网、广电网、物联

网、传感网、工控网、卫星网、数字物理系统、在线社交网络、计算系统、通信系统、控制系统等光、电、磁或数字信息处理设施；广义信号是指基于光、电、声、磁等各类能够用于表达、存储、加工、传输的电磁信号，以及能够与电磁信号进行交互的量子信号、生物信号等信号形态，这些信号通过在信息通信技术系统中进行存储、处理、传输、展示而成为信息；活动是指用户以信息通信技术为手段，对广义信号进行操作并用以表达人类意志的行为，操作包括产生信号、保存数据、修改状态、传输信息、展示内容等，可称为“信息通信技术活动”。在该定义中，网络角色、信息通信技术系统、广义信号和活动共同反映出了网络空间的四要素（虚拟角色、平台、数据、活动），也反映出了虚拟角色的广义性、主体性与主动性，数据的广谱性，平台的广泛性和活动的目的性[1]。

### 1.1.2 网络空间安全的概念

网络空间中的任一信息系统或系统体系自底向上可分为设备层、系统层、数据层和应用层4个层次，每个层次都面临着不同的安全问题，相应地形成了网络空间安全的四层次模型，如表1-1所示。

**表1-1 网络空间安全的四层次模型**

| | |
|---|---|
| 设备层的安全 | 网络空间中信息系统设备所面对的安全问题 |
| 系统层的安全 | 网络空间中信息系统自身所面对的安全问题 |
| 数据层的安全 | 网络空间中处理数据的同时所带来的安全问题 |
| 应用层的安全 | 信息应用的过程中所形成的安全问题 |

网络空间安全涉及在网络空间中电磁设备、信息通信系统、运行数据、系统应用中所存在的安全问题，既要防止、保护包括互联网、各种电信网与通信系统、各种传播系统与广电网、各种计算机系统、各类关键工业设施中的嵌入式处理器和控制器等在内的信息通信技术系统及其所承载的数据免受攻击，也要防止、应对运用或滥用这些信息通信技术系统而波及政治安全、经济安全、文化安全、社会安全、国防安全等情况发生。针对上述风险，需要采取法律、管理、技术、自律等综合手段来进行应对，确保信息通信技术系统及其所承载数据的机密性、可鉴别性、可用性、可控性得到保障[2]。

## 1.2 网络空间安全的发展历程

从信息论角度来看，系统是载体，信息是内涵。网络空间是所有信息系统的集合，是人类生存的信息环境，人在其中与信息相互作用并相互影响。因此，网络空间存在突出的信息安全问题，其核心内涵仍是信息安全。

信息安全是一个广泛而抽象的概念，从不同领域和不同角度对其概念的阐述会有所不同。在中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会发布的GB/T 25069—2010《信息安全技术术语》中，信息安全是指保持、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性和可靠性等性质。信息安全的目标是保证信息上述安全属性得到保持，从而对组织业务运行能力提供支撑。在商业和经济领域，信息安全主要强调的是消减并控制风险，保持业务操作的连续性，并将风险造成的损失和影响降

到最低。对于建立在网络基础之上的现代信息系统，信息安全是指保护信息系统的硬件、软件及相关数据，使信息不因偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。

随着全球社会信息化的深入发展和持续推进，相比物理的现实社会，网络空间中的数字社会在各个领域所占的比重越来越大。数量的增长带来了质量的变化，以数字化、网络化、智能化、互联化、泛在化为特征的网络社会，为信息安全带来了新技术、新环境和新形态，信息安全开始更多地体现在网络安全领域，反映在跨越时空的网络系统和网络空间之中，反映在全球化的互联互通之中。

因此，网络空间安全可以看作是信息安全的高级发展阶段，其发展历程如下。

### 1.2.1　通信保密阶段

通信保密阶段开始于 20 世纪 40 年代，其时代标志是 1949 年香农发表的《保密系统的信息理论》。在这个阶段所面临的主要安全威胁是搭线窃听和密码分析，其主要保护措施是数据加密。该阶段人们关心的只是通信安全，而且关心的对象主要是军方和政府机构。

本阶段需要解决的问题是在远程通信中拒绝非授权用户的访问以及确保通信的真实性，主要方式包括加密、传输保密、发射保密以及通信设备的物理安全。

### 1.2.2　计算机安全阶段

20 世纪 70 年代，网络空间安全的发展从通信保密阶段转变到计算机安全阶段。这一阶段的标志是 1977 年美国国家标准局公布的《国家数据加密标准》和 1985 年美国国防部公布的《可信计算机系统评估准则》。这些标准的提出意味着信息安全问题的研究和应用跨入了一个新的高度。

此阶段主要在密码算法及其应用和信息系统安全模型及评价两个方面取得了很大的进展。其中，1977 年美国国家标准局采纳了新开发出的分组加密算法；1976 年 Rivest、Shamir 和 Adleman 根据 Diffie、Hellman 在“密码学新方向”的开创性论文中提出的思想，创造了双密钥的公开密钥体制，简称为 RSA 算法；在该阶段还创造了一批用于数据完整性和数字签名的 HASH 算法。

1985 年美国国防部推出了可信计算机系统评价准则，该标准是信息安全领域中的重要创举，为后来英、法、德、荷四国联合提出的包含保密性、完整性和可用性概念的“信息技术安全评价准则”及“信息技术安全评价通用准则”的制定打下了基础。

### 1.2.3　信息安全阶段

20 世纪 90 年代以来，通信和计算机技术相互依存，数字化技术促进了计算机网络发展成为全天候、通全球、个人化、智能化的信息高速公路，国际互联网不断地向社会各个领域扩展，人们关注的对象已经逐步从计算机转向更具本质性的信息本身，信息安全的概念随之产生。

在这一时期，公钥技术得到了长足的发展，著名的 RSA 公开密钥密码算法获得了日益广泛的应用，用于完整性校验的 Hash 函数的研究应用也越来越多。

### 1.2.4　信息保障及网络空间安全阶段

由于针对信息系统的攻击日趋频繁以及电子商务的快速发展，安全的概念发生了以下变化。

① 信息的安全不再局限于信息的保护。人们需要对整个信息和信息系统进行保护和防御，包括保护、检测、反应和恢复能力。

② 信息的安全与应用更加紧密。其相对性、动态性、系统性等特征引起人们的注意，追求适度风险的信息安全成为共识。安全不再是单纯以功能或者机制技术的强度作为评价指标，而是结合了不同主体的应用环境和应用目标的需求，进行合理的计划、组织和实施。

在该阶段，美国国防部提出了信息保障的概念："保护和防御信息及信息系统，确保其可用性、完整性、保密性、可审计性和不可否认性等特性。这些特性包括在信息系统的保护、检测、反应功能中，并提供信息系统的恢复能力。"

信息保障除了强调了信息安全的保障能力外，还提出了要重视系统的入侵检测能力、系统的事件反应能力，以及系统在遭到入侵破坏后的快速恢复能力。它关注信息系统整个生命周期的防御和恢复。

从信息安全各阶段的发展可以看出，随着信息技术本身的发展和信息技术应用的发展，信息安全的外延不断扩大，包含的内容从初期的数据加密到后来的数据恢复、信息纵深防御，直到如今网络空间安全概念的提出。只有把握了信息安全及网络空间安全发展的趋势，才能更好地建立满足现在和未来需求的网络空间安全体系。

## 1.3 网络空间常见安全威胁

### 1.3.1 生活中的网络安全问题

当今社会，不同年龄、职业、生活环境的人们都在使用网络，人们通过网络阅读新闻、查询信息、学习办公、购物娱乐、移动支付等。网络的普及给学习、工作和生活带来了极大的便利的同时，也带来诸多安全问题，网络安全早已和人们的生活密不可分。人们在日常生活中遇到各种网络安全问题，下面列举一些最为常见，而且危害性极大的网络安全问题。

**1. 用户账号设置弱口令**

当用户在使用个人 QQ、微博等时，用于个人用户设置的密码过于简单，也就是常说的口令为弱口令( Weak Password) ，导致用户的个人账号被不法分子盗取。弱口令没有严格和准确的定义，通常认为由常用的数字、字母等组合成的，容易被别人通过简单及平常的思维方式猜测到的或被破解工具破解的口令均为弱口令。常见的弱口令有以下几种。

① 空口令或系统默认的口令，例如，我们申请了一张银行卡，发卡银行给银行卡默认的口令为 666666，如果我们拿到银行卡以后不进行修改，当银行卡丢失或者被盗的时候，极易造成财产损失。

② 口令长度小于 8 个字符( 例如: admin、123456) 。

③ 口令为连续的某个字符( 例如: aaaaaa) 或重复某些字符的组合( 例如: abcabc) 。

④ 口令中包含本人、父母、子女和配偶的姓名和出生日期，纪念日期，登录名，E-mail地址，手机号码等与本人有关的信息。此种类型的密码是非常危险的，例如，我们将银行卡密码设置为生日，如银行卡密码为 19790126，当存放银行卡和身份证的钱包丢失的时候，银行卡的密码很容易被猜到，极易造成财产损失。

⑤ 用数字或符号代替某些字母的单词作为口令。

⑥ 长时间不做更改的口令。

产生弱口令的原因应该与个人习惯与意识相关，为了避免忘记密码，使用一个非常容易记住的密码，或是直接采用系统的默认密码等。再者，相关的安全意识不够，没能深刻地意识到口令安全的重要性。

比较常见的弱口令有 123456、000000、666666。随着网络安全技术的发展，目前，大部分网站在设置用户密码的时候都需要使用数字和字母的组合，而且长度必须大于 8 位或者 10 位，因此上面提到的 123456、000000、666666 常见的弱口令基本已经可以避免。

但部分用户在设置账号的密码时，可能会使用账户用户名 + 生日、账户用户名 + 身份证号后 6 位、账户用户名 + 手机号码等作为账号的密码，这些密码极容易被攻击者猜测到，故这些密码不安全。例如，用户张三申请了一个网站的账号，张三的手机号码为 18816881355，张三设置的账号为 zhangsan188，密码为 zhangsan881355，此种类型的密码不安全。表 1-2 是最为常见的 100 个弱口令。

**表 1-2　最为常见的 100 个弱口令**

| 序　号 | 弱口令 | 序　号 | 弱口令 | 序　号 | 弱口令 | 序　号 | 弱口令 |
|---|---|---|---|---|---|---|---|
| 1 | 123456789 | 26 | 0123456789 | 51 | 123456789abc | 76 | 123456q |
| 2 | a123456 | 27 | asd123456 | 52 | z123456 | 77 | 123456aa |
| 3 | 123456 | 28 | aa123456 | 53 | 1234567899 | 78 | 9876543210 |
| 4 | a123456789 | 29 | 135792468 | 54 | aaa123456 | 79 | 110120119 |
| 5 | 1234567890 | 30 | q123456789 | 55 | abcd1234 | 80 | qaz123456 |
| 6 | woaini1314 | 31 | abcd123456 | 56 | www123456 | 81 | qq5201314 |
| 7 | qq123456 | 32 | 12345678900 | 57 | 123456789q | 82 | 123698745 |
| 8 | abc123456 | 33 | woaini520 | 58 | 123abc | 83 | 5201314 |
| 9 | 123456a | 34 | woaini123 | 59 | qwe123 | 84 | 000000000 |
| 10 | 123456789a | 35 | zxcvbnm123 | 60 | w123456789 | 85 | as123456 |
| 11 | 147258369 | 36 | 1111111111111111 | 61 | 7894561230 | 86 | 123123 |
| 12 | zxcvbnm | 37 | w123456 | 62 | 123456qq | 87 | 5841314520 |
| 13 | 987654321 | 38 | aini1314 | 63 | zxc123456 | 88 | z123456789 |
| 14 | 12345678910 | 39 | abc123456789 | 64 | 123456789qq | 89 | 52013145201314 |
| 15 | abc123 | 40 | 111111 | 65 | 1111111111 | 90 | a123123 |
| 16 | qq123456789 | 41 | woaini521 | 66 | 111111111 | 91 | caonima |
| 17 | 123456789. | 42 | qwertyuiop | 67 | 0000000000000000 | 92 | a5201314 |
| 18 | 7708801314520 | 43 | 1314520520 | 68 | 1234567891234567 | 93 | wang123456 |
| 19 | woaini | 44 | 1234567891 | 69 | qazwsxedc | 94 | abcd123 |
| 20 | 5201314520 | 45 | qwe123456 | 70 | qwerty | 95 | 123456789. . |
| 21 | q123456 | 46 | asd123 | 71 | 123456. . | 96 | woaini1314520 |
| 22 | 123456abc | 47 | 000000 | 72 | zxc123 | 97 | 123456asd |
| 23 | 1233211234567 | 48 | 1472583690 | 73 | asdfghjkl | 98 | aa123456789 |
| 24 | 123123123 | 49 | 1357924680 | 74 | 0000000000 | 99 | 741852963 |
| 25 | 123456. | 50 | 789456123 | 75 | 1234554321 | 100 | a12345678 |

2. 钓鱼网站攻击

钓鱼网站的网址通常与真实网址较为接近，页面形式也与真实网站较为相似，不法分子通过病毒等形式将钓鱼网址链接发送给用户，诱骗用户登录个人网银等账号，窃取用户信息，甚至骗取钱财。

例如，中国工商银行的网址是 http://www.icbc.com.cn/，有一些钓鱼网站会将网址设置为 http://www.1cbc.com.cn，网站的内容和 http://www.icbc.com.cn/网站完全相同。通过邮件或者短信的方式将钓鱼网站的链接地址发送给用户，邮件的内容是告知用户“在什么时间在什么地点有一笔中国工商银行的消费，需要用户去核实”，有一些用户可能就会上当受骗，在假的 http://www.1cbc.com.cn 网站输入自己银行卡的卡号和密码，不法分子就可以获取用户的银行卡卡号和密码，从而造成财产损失。

3. 诈骗电话

2016 年 8 月 19 日，山东临沂 18 岁女孩徐玉玉接到了一个诈骗电话，即将进入南京邮电大学英语系就读的她被骗走 9 900 元学费。在与家人去派出所报案回来的路上，女孩心脏骤停，两天后离世。不法分子通过各种渠道获取学生的个人隐私信息，通过诈骗电话通知徐玉玉助学金要发放。因前一天也曾接到教育部门发放助学金的通知，她并未怀疑电话的真伪。按对方要求，她将准备交学费的 9 900 元打入了对方提供的账号。8 月 23 日凌晨，临沂市临沭县即将进入大二学期的山东理工大学学生宋振宁也在遭遇电信诈骗后心脏骤停，不幸离世。

4. WiFi 陷阱攻击

当人们出行的时候，总希望能访问免费的 WiFi，用于发送微信或者 QQ 等即时消息。不法分子在宾馆、饭店、咖啡厅等公共场所搭建免费 WiFi，通过免费的 WiFi 推送各种钓鱼网站，如假冒的淘宝网站，骗取用户使用，盗取用户的用户名和密码信息，并记录其在网上的所有操作记录；或是针对设置了弱口令的家用 WiFi 进行口令破解，实现对家用路由器的远程控制。

形形色色的网络安全事件频发，可见网络安全问题已经渗透到人们的日常生活当中。伴随着迅速发展的信息技术与信息服务不断超越现有的互联网监管体制，网上有害信息传播、病毒入侵、网络诈骗、黑客攻击等日趋严重，网络泄密事件屡有发生，网络犯罪呈现快速上升趋势，严峻的安全形势甚至危及国家安全和社会稳定。

### 1.3.2 我国网络空间安全面临的挑战

当前，我国信息安全环境日趋复杂，网络安全问题对互联网的健康发展带来日益严峻的挑战，网络安全事件的影响力和破坏程度不断扩大。这些问题主要体现在以下几个方面。

① 针对网络信息的破坏行为日益严重，利用网络进行违法犯罪的案件逐年上升。

鉴于互联网具有传播速度快、覆盖面广、隐蔽性强和无国界等特点，传统领域的违法犯罪活动逐渐向互联网渗透，网上违法犯罪案件逐年大幅上升，犯罪类型不断扩展，作案手段不断翻新，危害后果日趋严重。越来越多的高新技术被违法犯罪分子所利用，安全防范的难度越来越大，安全保障的要求越来越高。

② 安全漏洞和安全隐患增多，对信息安全构成严重威胁。

信息安全事件的发生，绝大多数都与利用、误用信息技术自身的缺陷有关，安全漏洞和