【公益】

# 大学新生网络信息安全知识教育手册

广东省计算机学会网络空间安全专业委员会

二〇一六年十月

# 编委会

主任：凌捷（广东工业大学）

成员：林帝浣（中山大学）、张昊（工信部第五研究所）、曾海标（中山大学）、罗晓奔（华南理工大学）、梁琦（蓝盾信息安全技术股份有限公司）、柳毅（广东工业大学）

# 序

在硕果累累的金秋时节，同学们带着梦想、怀着憧憬迈进了大学校园，即将开始美好的大学生活。大学不仅是学术殿堂，也是人生修养的大学堂，在这里你们将会学到各种科学知识，建立自己的思维模式和三观，还会感悟到许多人生哲理。编委会祝贺同学们顺利开启人生的新历程！

人类已进入信息社会，信息技术正在改变人们的生产和生活方式，特别是近年来，以云计算、大数据、物联网、移动互联网为代表的新一代信息技术的快速发展，对社会经济各领域正在产生革命性的影响。大学生活已离不开互联网，我们将依赖互联网获取国内外的学术资源和各类资讯，依托互联网进行相互交流，利用互联网开展学术研究，享受互联网提供的各种服务，等等。“互联网+”也成为一种新的经济形态，网络技术的普及应用为人们的生产生活带来了极大的便利，同时也带来了许多安全问题，计算机犯罪、计算机病毒、黑客攻击、

网络诈骗、网络色情、个人敏感信息泄漏、恶意程序和后门等严重威胁着网络的安全；由于网络实名制尚未普及，网络管理和立法普遍滞后，在现实生活与虚拟世界之间出现了道德鸿沟，使得网络领域精神污染泛滥成灾，网络暴力肆意横行；各种不实信息、网络谣言以及淫秽色情信息的传播扩散，给人们的学习、工作和生活带来了诸多烦恼，甚至是损失或危害，对整个网络生态以及社会安定产生了巨大的破坏作用。网络信息安全已经成为现代社会经济发展中，政府、企事业单位和个人必须共同面对的挑战，文明网络行为，净化网络环境，需要我们新一代大学生群体的共同参与；遵守国家网络信息安全法律，努力学习网络信息安全知识，自觉维护网络安全，也是当代大学生的责任和学习生活中重要的一课。

广东省计算机学会网络空间安全专业委员会为配合大学新生入学教育，组织撰写了这本《大学新生网络信息安全知识教育手册》，希望有助于同学们了解网络信息安全的基础知识，掌握网络安全防御的基本常识，提高网络安全的防护意识；有助于营造安全文明和谐的网

络环境，促进互联网的持续健康发展！手册内容由凌捷统稿审定，手册中漫画主要由林帝浣（小林）提供，手册印刷得到蓝盾信息安全技术股份有限公司的大力支持。

本项目属社会公益活动，手册免费向社会发放。

广东省计算机学会网安专委会

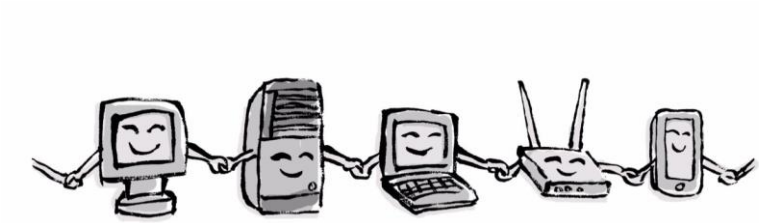
2016 年 10 月

# 目　录

# 1.网络信息安全基础知识

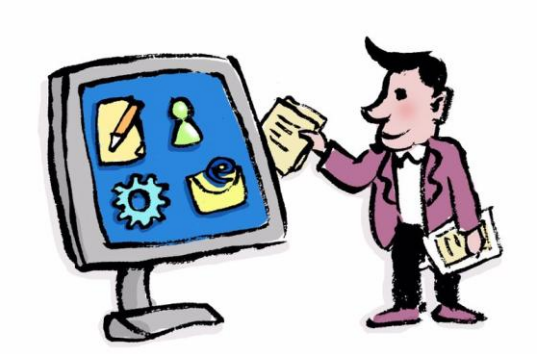
## 1.1 计算机网络

计算机网络是利用通信线路将不同地理位置、具有独立功能的计算机和通信设备连接起来，实现资源共享和信息传递等目的的计算机系统。



主要有局域网（Local Area Network，LAN）、城域网（Metropolitan Area Network，MAN）、广域网（Wide Area Network，WAN）和互联网（Internet）等。

## 1.2 信息系统



信息系统是能进行信息的采集、传输、存储、加工、使用和维护的计算机应用系统。如办公自动化系统、高校教务管理系统、

人事管理系统、火车/飞机订票系统等。

## 1.3 信息安全

信息安全是指保护信息系统中的计算机硬件、软件及数据不因偶然或恶意的原因而遭到破坏、更改、泄露，保障系统连续可靠正常地运行，信息服务不中断。

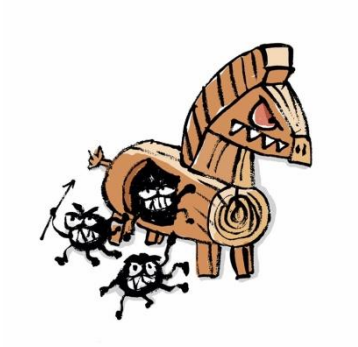

信息安全（狭义）是指保护信息系统的安全，主要目标包括保护信息系统的保密性、完整性和可用性等。

## 1.4 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。计算机病毒具有寄生性、隐蔽性和传染

性等特点。

## 1.5 计算机木马



木马是一种用来非法收集信息或控制另一台计算机的特定程序，通常有客户端和服务器端两部分，植入木马的计算机是服务器端部分。木马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、即时通信等渠道诱导用户下载安装，如果用户打开了此类木马程序，用户的计算机或智能终端等设备便会被植入木马者所控制，造成数据文件被窃取或修改、电子账户资金被盗用等危害。

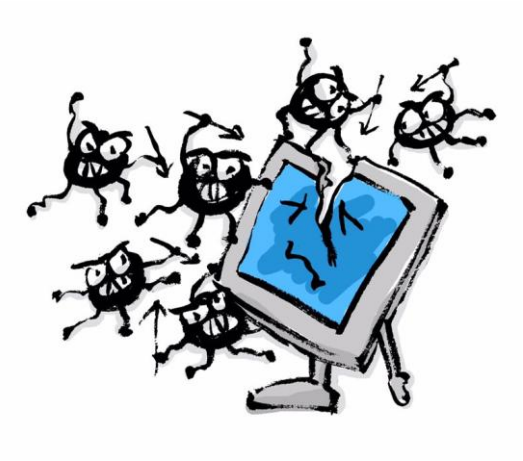
## 1.6 入侵

指对计算机网络或系统的非授权访问行为，通常是恶意的存取信息、处理信息或破坏系统的行为。

## 1.7 黑客

泛指熟悉 IT 技术，热衷于入侵网络或计算机系统窃取数据和信息的人员。

## 1.8 攻击



指利用网络或计算机系统存在的漏洞和安全缺陷对其进行破坏、泄露、更改或使其丧失功能的行为。

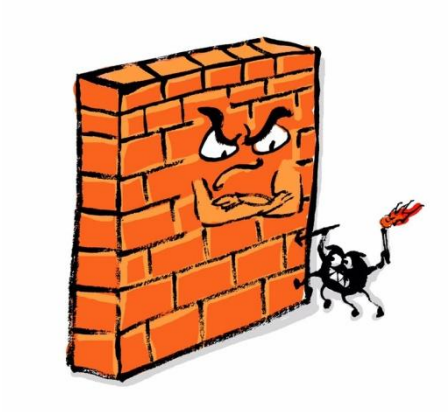
## 1.9 漏洞


指网络或信息系统的硬件、软件、协议的具体实现或安全策略上存在的弱点或缺陷。漏洞可能来自应用软件或操作系统设计时的缺陷或编码时产生的错误，也可能来自业务在交互处理过程中的设计缺陷或不合理的逻辑流程处理。

## 1.10 后门


指绕过安全性控制而获取对程序或系统访问权的程序方法，是有意留在计算机系统中，供某些特殊使用者通过某种特殊方式控制计算机系统的途径。后门与漏洞的区别在于：漏洞是一种无意行为，而后门是程序员在软件开发过程中有意创建的。

## 1.11 防火墙



是一种将内部网和外部网隔离，保护内部网免受非法用户的侵入的访问控制技术。防火墙可以软件实现，也可以硬件实现。

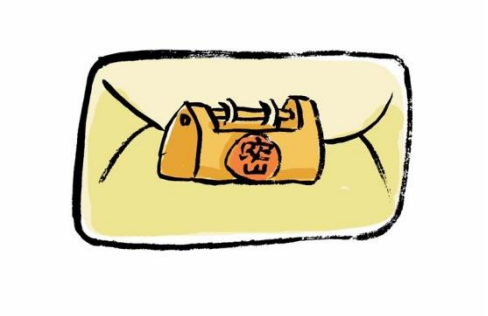
## 1.12 补丁

指针对软件系统在使用过程中暴露的缺陷而发布的修补漏洞的小程序。

## 1.13 密码


一种用于保护数据或信息的技术（符号系统）。密码系统的基本功能是实现信息的机密性服务。

## 1.14 加密



是以某种特殊的算法改变原有信息数据的表现形态，将正常的（可识别的）信息变换为无法识别的信息的过程。加密的目的是使未授权的用户即使获得了加密信息也无法了解信息的内容。

## 1.15 解密

是加密的逆过程。将加密后的信息通过某种算法恢复为可识别的信息，使得授权用户能够了解原有的信息数据。

## 1.16 数字签名

是信息的发送者通过签名算法产生的，用于证明信息发送者发送信息真实性一段数字串。数字签名一般通过密码技术实现，与普通物理签名具有同样法律效力。

## 1.17 数字水印

是一种将标识信息嵌入到数字载体当中，用于确认载体所有者、判断载体是否被篡改或传送秘密信息的技术。嵌入的标识信息也称为数字水印，数字载体包括多媒体、文档、软件等，数字水印嵌入到数字载体时，应不影响原载体的使用价值。

# 2.网络信息安全法律法规

## 2.1《全国人大常委会关于维护互联网安全的决定》

全国人大常委会 2000 年 12 月 28 日通过。该决定共七条，其中有五条共 15 款的内容是对可以追究刑事责任的犯罪行为做出规定。

## 2.2《中华人民共和国刑法修正案（九）》

全国人大常委会 2015 年 10 月 29 日通过。其中在刑法第二百八十六条后增加一条，作为第二百八十六条之一，对网络服务提供者的犯罪行为做出规定；在刑法第二百八十七条后增加二条，作为第二百八十七条之一、第二百八十七条之二，对利用网络实施犯罪的行为做出规定。

## 2.3《中华人民共和国计算机信息系统安全保护条例（2011 年修正）》

国务院于 1994 年 2 月 18 日发布，是我国第一部涉及计算机信息系统安全的行政法规，于 2011 年 1 月 8 日废除同时发布修正版。

## 2.4 《中华人民共和国计算机信息网络国际联网管理暂行规定》

国务院于 1996 年 2 月 1 日发布，于 1997 年 5 月 20 日修正。

## 2.5 《计算机信息网络国际联网安全保护管理办法》

国务院于 1997 年 12 月 11 日国务院批准、公安部于 1997 年 12 月 30 日发布，于 2011 年 1 月 8 日修正。

## 2.6 《互联网信息服务管理办法》

国务院于 2000 年 9 月 25 日发布，对互联网信息服务提供者在制作、复制、发布、传播信息的内容做出规定。

## 2.7 《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》

公安部于 1997 年 12 月 22 日发布，规定（国内外）信息安全专用产品在中国境内进入市场销售前，必须经过公安部门的检测并取得销售许可证。

## 2.8 《通信网络安全防护管理办法》

工业和信息化部于 2010 年 1 月 21 日发布，对电信业务经营者和互联网域名服务提供者管理和运行的公用通信网和互联网的网络安全防护工作做出规定。

# 3.网络信息安全常见漏洞与风险

## 3.1 常见的计算机风险

### （1）操作系统漏洞

由于各种原因，常用的 Windows 操作系统不断被发现存在漏洞，这些漏洞将成为攻击者实施攻击的新途径，危害到整个计算机系统的安全；另外，有些漏洞也可能是系统开发者有意留下用于搜集用户信息或其它目的的。

### （2）遭受黑客攻击


黑客攻击是指通过 Internet 网络进行非法访问、破坏和攻击。

有些黑客出于好奇或炫耀技术，只窥探用户的秘密或隐私，不破坏计算机系统；有些黑客从事恶意攻击和破坏，入侵用户的系统，毁坏重要的数据、非法盗用账号偷窃他人财产或进行网络勒索和诈骗。

**（3）感染病毒或被植入木马和间谍软件**

病毒（蠕虫）可以利用受感染系统的文件传输功能自动进行传播，破坏计算机系统或导致网络流量大幅增加直到网络瘫痪；木马程序可以偷窥用户账号密码和其它个人隐私信息，导致非授权用户能够远程入侵网络系统；间谍软件是一种恶意代码，可以监控系统状态，并将用户数据暗中发送给软件使用者。

**（4）垃圾邮件攻击**

垃圾邮件一般是指未经过用户同意强行发送到用户邮箱中的电子邮件。垃圾邮件发送组织为了大面积散布非法信息，常采

用多台机器同时大量发送的方式攻击邮件服务器，占用了网络带宽和个人邮箱空间，造成邮件服务器拥塞，严重干扰邮件服务器进行正常的邮件递送工作，降低了网络的运行效率。

## 3.2 移动智能终端的风险

### （1）伪基站攻击


伪基站设备一般由笔记本电脑、主机、发射器和天线等组成。伪基站设备运行时，在一定范围内的运营商的手机信号受到干扰和屏蔽，用户手机信号被强制连接到伪基站设备上，伪基站趁机将诈骗短信发送到这部分用户手机上，并且伪基站能把发送号码显示为任意号码。屏蔽运营商的信号一般能持续 10 秒左右，待诈骗短信推送完了，受控范围内用户手机才能重新搜索到运营商信号恢复正常，部分手机则必须关机开机才能重新进入运营商网络。

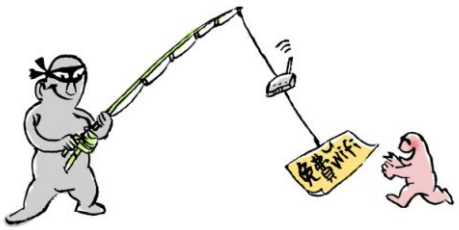
### （2）WWW 欺骗

在网上用户能利用 IE 等浏览器进行各种各样的 WEB 站点的访问，如阅读新闻、搜索信息、咨询产品价格、订阅报纸、电子商务等。然而一般的用户可能想到不会想到正在访问的网页已被黑客篡改过，网页上的信息是虚假的。如黑客将用户要浏览的网页的 URL 改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就能达到欺骗的目的了。

**（3）手机病毒（木马）攻击**

手机病毒（木马）可利用发送短信、收发电子邮件、浏览网站、下载铃声等方式进行传播，容易导致用户手机自动关机、死机、手机个人资料被删、泄露手机个人信息、自动拨打电话、自动向外发送短信邮件等并进行恶意扣费，甚至会损毁 SIM 卡、手机芯片等硬件，还可能被远程监听，具有很大危害。

**（4）无密码 WiFi 攻击**




手机连接过无密码的公共 WiFi 后，一方面是攻击者可以很容易监听在同一个网段内所有的广播流量，可以截获各种手机用户名、密码、上网记录、设备信息、聊天记录及邮件内容；另一方面是攻击者可以伪造 WiFi，利用手机会自动搜索自动连接以前连接过的所有 WiFi 的功能，欺骗用户登录伪造的同名 WiFi。

## 3.3 网络支付的风险

**（1）恶意二维码**

恶意二维码是嵌入了病毒或木马链接的二维码，扫描二维码的过程就是点击链接的过程。扫描了恶意二维码，手机将被植入木马病毒，或者登录到假冒的钓鱼网站。恶意二维码正在成为网络诈骗的一个新手段，手机用户不要轻易扫描宣传广告中的二维

码，要在官方工作人员的指导下扫描，或通过官方网站下载 APP、关注公众号。

**（2）网络钓鱼攻击**

攻击者通过发送欺骗性电子邮件或短信，建立假冒网上银行、网上证券网站，引诱受骗者上网主动泄露个人隐私信息，如用户名、信用卡号、银行卡账户、身份证号、密码等内容，多数受害者通常事后才能发现遭受攻击。

**（3）网银木马攻击**

是一种专门攻击网银支付的特种木马，可通过下载工具、浏览器和购物软件加载。攻击者利用第三方支付 HTTP 网页与网银的衔接认证的缺陷，能够有选择地劫持中马用户的支付页面，篡改网购收款人的账号信息，在不知不觉中转移大量财产，可以危害绝大多数网络银行与第三方支付的衔接环节，攻击成功率高。

# 4.网络信息安全防护策略

## 4.1 计算机安全防护策略

### （1）计算机及应用系统要设置登录口令

计算机要设置开机口令，重要的应用系统要设置登录口令；口令长度一般不少于 8 位，除非系统限制，尽可能用字母、数字和下划线混合编制口令；不要以容易猜测的个人信息（如姓名、生日、手机号、计算机用户名）、学校名称等作为口令；口令使用一段时间后要更换。

开机口令设置方法：打开计算机的“控制面板”，进入“用户帐户”，选择“创建密码”或“更改密码”功能。

### （2）计算机要安装杀毒软件

计算机应安装主流的杀毒软件，并且至少一周更新一次；对杀毒软件要进行更新设置，可选择每天检查更新，确保软件的病毒查杀能力。

杀毒软件安装方法：在杀毒软件厂家的官网下载并安装，建议使用 360 安全卫士等免费的杀毒软件套装。

### （3）计算机要及时更新操作系统补丁

Windows 等操作系统开发商一般每月都会发布最新的补丁程序用以修复新发现的操作系统漏洞，漏洞类型主要分为高危漏洞和功能性漏洞两种，对高危漏洞的补丁必须安装，功能性漏洞的补丁可选择性进行安装，避免造成系统资源的浪费。要定期进行

补丁升级更新，升级到最新的安全补丁，可以提高计算机的防御能力。

补丁更新方法：打开计算机的“控制面板”，进入“Windows Update”，选择“检查更新”功能；或者通过 360 安全卫士自动检测更新。

**（4）防止通过 U 盘的病毒感染**

如果将带有木马或病毒的 U 盘接入计算机，很可能会将木马或病毒传播到计算机中。要使用杀毒软件或查杀木马软件及时对接入到计算机的U盘进行检测，并关闭计算机U盘自动播放功能；在 U 盘处于工作状态时不要拔出 U 盘，避免造成数据丢失。

## 4.2 互联网安全防护策略

**（1）浏览器安全设置**

互联网上充满着各种钓鱼网站、病毒、木马程序，打开来历不明的网页、电子邮件链接、附件可能导致木马或病毒自动进入计算机，造成文件丢失、损坏甚至计算机系统瘫痪。

当前主流的浏览器有微软的 IE 浏览器、谷歌的 Chrome 浏览器、360 安全浏览器和火狐 Firefox 浏览器等等，不同的浏览器产品对恶意网址拦截的功能差别较大，大家可以比较后选择安装。

修改安全设置的方法（以 IE 浏览器为例）：打开 IE 浏览器，点击“工具/设置”后，在下拉菜单“Internet 选项”中，选择“安全”，可对“Internet”或“本地 Intranet”区域的安全级别进行自定义设置，一般选择“中-高”，如果选择级别太高，会对浏览网页产生一些影

响。

**（2）Cookie 安全限制**

Cookie 是一个数据包，当用户浏览一个网站后会生成这样一个数据包，包含了发布 Cookie 的网站名、用户访问该网站的种种活动、个人资料、浏览习惯、消费习惯等数据。它的作用是能够让你在下一次访问时不需要重新输入用户名和口令。Cookie 本身是安全的，它既可以存储在个人计算机上，也可在一次浏览会话中创建、使用并删除。Cookie 的安全问题是个人信息容易被别人以不为人觉察的方式收集、存储和利用。

安全防范策略：

- ✧ 在浏览器中对 Cookie 的使用做出限制，并定期删除浏览器中的 Cookie。清除 Cookies 有利于保护自己的隐私不被跟踪。

限制使用 Cookie 的方法：单击“工具/Internet 选项”->“隐私”->“设置”菜单中，调整 Cookie 的安全级别。多数的网站论坛站点需要使用 Cookie 信息，一般选择“中高”或者“高”的安全级别。最高安全级是“阻止所有 Cookie”；如果只是为了禁止个别网站的 Cookie，可以单击“编辑”按钮，将要屏蔽的网站添加到列表中。

清除 Cookie 的方法：点击浏览器上方的“工具/Internet 选项”->“常规”菜单，点击“删除浏览的历史记录”，选择删除“Cookie”。

**（3）公共场所上网安全**

在公共场所如酒店、网吧、图书馆、咖啡厅、机场、地铁站等地方，使用公用计算机上网登录邮箱、网上购物时，很容易遭

受网络攻击，导致账户口令被泄露，带来经济损失。

**安全防范策略：**

- ✧ 不要轻易使用公共场所提供的计算机登录邮箱和进行网上购物，在使用时尽量使用 Https 协议登录网站和邮箱；
- ✧ 在上网时不要选择“记住用户名和密码”；
- ✧ 互联网浏览器后，应清空历史记录和缓存内容。

## 4. 3 无线网络安全防护策略

**（1）WiFi 上网的安全**

WiFi是一种允许电子设备连接到一个无线局域网的传输技术，遵循IEEE802.11标准。目前使用WiFi无线网络存在重大的安全隐患，一方面是公共场所的无密码WiFi热点，很可能就是钓鱼陷阱；另一方面是网民家里的无线路由器如果设置不合理，很可能被恶意攻击者轻松攻破，攻击者除了免费享用网络带宽外，还可以登录无线路由器的管理后台，这样网民在家里通过WiFi连接无线网，进行微信、QQ、甚至网银登录，很可能在毫不知情的情况下，面临个人敏感信息遭盗取风险，甚至遭受直接的经济损失。

**无密码WiFi的安全防范策略：**

- ✧ 尽量不使用公共场所提供的无密码的WiFi无线网络；
- ✧ 不要在无密码WiFi网络环境下进行与资金有关的银行转账与支付等操作。

**家庭WiFi的安全防范策略：**

- ✧ 路由器管理后台的登录账号、密码，不要使用默认的admin，启用时更改为字母加数字的高强度密码；

- ✧ WiFi设置要选择WPA/WPA2加密认证方式；
- ✧ WiFi密码要使用相对复杂的密码，可提高黑客破解的难度。

**（2）手机等智能终端的安全**

智能手机和平板电脑等移动智能终端已融入了我们的生活，大家也越来越依赖智能手机。但手机支付漏洞、手机远程定位、手机信息泄露等安全问题屡见不鲜。智能手机强大的上网功能和部分用户不安全的上网习惯，给了手机病毒、木马乘虚而入的机会，短信彩信、邮件等也是手机病毒传播感染的重要途径。

**安全防范策略：**

- ✧ 设置手机锁屏密码，以防手机遗失时，被不法之徒轻易获得通讯录、文件等重要信息；
- ✧ 不要轻易点击打开别人在 QQ、微信、短信、邮件中发来的链接地址；
- ✧ 平时关闭手机的自动搜索无线网络功能，仅在需要时开启；
- ✧ 在手机的 QQ、微信等应用程序中关闭地理定位功能；
- ✧ 经常为智能手机做数据备份。
- ✧ 在正规的通信运营商处维修手机，防止手机被植入病毒木马程序。

## 4.4 网上银行安全防护策略

**（1）网上支付的安全**

随着电子商务的发展，社会公众对小额、快捷、便民的小微

支付服务需求日益增长，网络支付服务得到了快速发展，相关问题和风险也不断显现。由于客户在网上银行及其它支付机构不需要提供任何印鉴，仅凭 USB Key 或手机支付密码就可以办理支付业务，伴随着日益频繁的支付活动，个人支付信息泄露风险大大增加，消费者面临更大的资金被盗和欺诈风险。

**安全防范策略：**

- ✧ 妥善保管好相应的网上银行认证信息；
- ✧ 不要在网吧等不安全的公共场所使用网上银行交易系统执行支付操作；
- ✧ 不要轻易相信陌生的电话或者短信、邮件，避免个人信息泄漏；
- ✧ 静态口令应牢记脑中，动态口令要谨慎保管，支付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、姓名等容易被猜中的内容做密码；
- ✧ 建议对不同的电子支付方式分别设置合理的交易限额，在交易未完成时不要中途离开交易终端；
- ✧ 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。

**（2）钓鱼网站的防范**

钓鱼网站通常伪装成为银行网站，骗取访问者提交的账号和密码信息。它一般通过电子邮件传播，通过邮件中一个经过伪装的链接将收件人导向钓鱼网站。钓鱼网站的页面与真实银行网站界面几乎完全一致，要求访问者提交账号和密码。钓鱼网站结构一般都只有一个或几个页面，其 URL 和真实网站有细微差别。

**安全防范策略：**

- ✧ 查看网站身份信息，可通过中国互联网络信息中心（CNNIC）运行的国家最高目录数据库中的“可信网站”子数据库，可以甄别网站的真实身份；
- ✧ 查询网站备案，可通过 ICP 备案可以查询到网站的基本情况和网站拥有者的情况，没有合法备案的非经营性网站或没有取得 ICP 许可证的经营性网站，都是非法的网站。
- ✧ 认真核对网站域名，钓鱼网站和真实网站有细微区别，有疑问时要仔细辨别其不同之处，比如在域名方面，钓鱼网站通常将英文字母 I 被替换为数字 1。
- ✧ 查看网站的安全证书，大型的电子商务网站都应用了可信证书类产品，其网址都是“Https”打头的，对不是“Https”开头的电商网站要特别谨慎。
- ✧ 网上购物时请到信誉好、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；
- ✧ 不要随便点击手机接收到的中奖、贷款等短信和非银行官方网站上的链接信息。