



上海城建职业学院  
Shanghai Urban Construction Vocational College

# 网络安全意识培训

---

图文信息中心



# 目录

- Contents
- 安全上网基础课
- 安全办公提高班
- 法律法规必修班



# 01

## 安全上网基础课

安全软件务必装，自家大门要看好  
定期体检打补丁，提前免疫不得病  
密码设置强度高，验证短信不外泄  
使用U盘先杀毒，危险文件入沙箱  
陌生来电不轻信，不明链接不要点  
删除资料能恢复，二手交易猫腻多

# 安全软件务必装，自家大门要看好



## 安全软件

现代安全软件是电脑，手机的必备软件，一般包含以下几大功能：

- 防病毒，防木马
- 反钓鱼，反诈骗
- 打补丁，修系统
- 垃圾清理，系统加速
- 软件管理，权限管理

一般来说，只要经常用安全软件给电脑、手机做体检，多数安全问题都能“一键”解决。

### 特别提示：

有些会“卖萌”的病毒或者是网络骗子会谎称安全软件有“误报”，建议你暂时关闭安全软件。千万不能信啊！

# 定期体检打补丁，提前免疫不得病

## 打补丁：

打补丁是为了修漏洞。系统不打补丁，就像家里不关门窗，很容易被入侵。存在漏洞的系统，安全软件也很难有效防护。



2003年8月，冲击波病毒利用微软已经修复的漏洞发起攻击，一周之内感染了全球约80%的电脑。



2007年1月，熊猫烧香病毒利用Windows漏洞肆虐全国，这是最为臭名昭著的一款“国产”病毒。



2017年5月，WannaCry勒索蠕虫利用漏洞永恒之蓝发起攻击，30个小时内就使100多个国家的大量机构陷入瘫痪。



## 打补丁工具

# 密码设置强度高，验证短信不外泄



## 密码的四项基本原则

密码是所有帐号安全的基本保障，设置密码一般需遵守以下原则：

- 15位以上
- 数字+字母+特殊符号
- 定期修改（建议180天）
- 支付、社交、邮箱等核心帐号单独设密码

## 动脑时间

你能在2分钟内记住下面三个密码吗？哪一个密码最安全？你知道怎样构造一个又长又好记的密码吗？



chuangqianmingyueguangyishidishangshuang

xiaobaitu2baiyoubai3liangzhierduoshuqilai4

@xiyangyang#yuhuitailang\$123

## 特别提示：

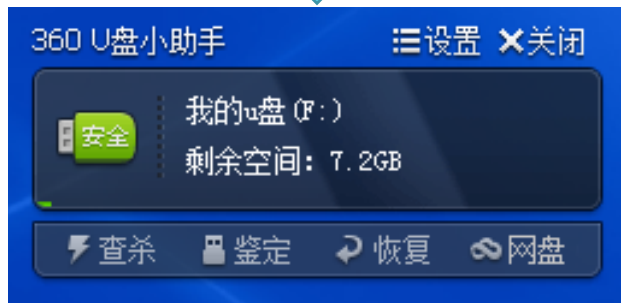
- 帐号一旦被盗，应立即修改所有其他相关帐号的密码
- 短信验证码是一种动态的密码，千万不要告诉任何人

# 使用U盘先杀毒，危险文件入沙箱

## U盘防护

U盘又称病毒“摆渡”，常用来攻击隔离网中的电脑。

著名的“震网病毒”就是通过U盘入侵伊朗核电站并实施破坏。



U盘、移动硬盘一定要先杀毒，后使用

## 沙箱

一种虚拟的软件运行环境，木马病毒运行在其中，只会破坏沙箱内的虚拟系统，不会危及真实的电脑系统。

破解软件、外挂程序、种子文件、色情文件等，都有可能是木马程序。如果实在想要看看究竟，可以把它们丢进沙箱。



# 陌生来电不轻信，不明链接不要点

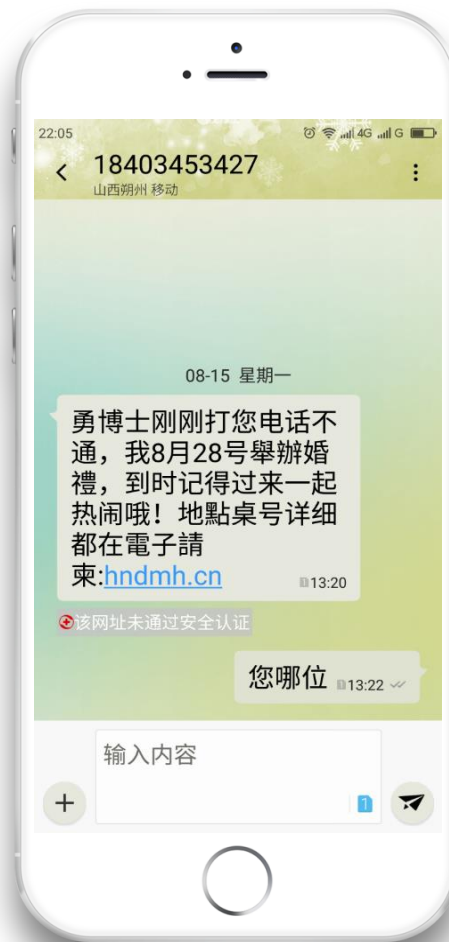
## 诈骗电话与骚扰电话



## 伪基站仿冒短信



## 短信中的带毒短链接



## 社交软件欺诈链接



安全软件一般无法检测社交软件中网址链接的安全性  
用社交软件转发网页，网址也会被隐藏  
防骗，只能擦亮眼睛

### 特别提示：

外来的、陌生的、你不熟悉的东西都可能有危险，电话，短信、网络社交皆如此。

# 删除资料能恢复，二手交易猫腻多



## 文件删除

无论是在电脑上还是手机中，被删除的文件通常可以使用某些专用工具恢复出来，想要彻底删除，需要进行文件“粉碎”。



## 出厂设置

在手机上“恢复出厂设置”也不能彻底删除文件，仍然可恢复。

## 隐私擦除

彻底擦除手机隐私方法

- 删除信息后，用视频等大文件复制并占满手机存储空间，即可彻底擦除原有数据
- 使用360安全换机中的“隐私粉碎机”

### 特别提示：

若未能妥善处理手机中原有资料，一旦手机被黑心二手商贩收购，他们很有可能会恶意恢复手机信息，并贩卖到网络黑市。

# 02

## 安全办公提高班

WiFi易成突破口，私建网络是祸根  
办公邮箱不乱用，到处注册风险多  
邮件附件常带毒，陌生来源勿打开  
收信看清发件人，冒名顶替要当心  
OA 钓鱼最危险，美国大选也中招  
骗你上当有理由，仿冒登录盗帐号  
安全习惯早养成，提高警惕少出错

# WiFi易成突破口，私建网络是祸根



## 私建WIFI热点的风险

私自搭建WiFi热点，并将内网中的设备与热点相连，将会在内网边界上打开突破口，使网络隔离完全失效。



一旦内网出现突破口，木马、病毒、黑客，都会乘虚而入。



WannaCry勒索蠕虫会攻击隔离网设备的重要原因之一就是员工在内网之中自搭乱建WiFi热点。

# 办公邮箱不乱用，到处注册风险多



## 电子邮箱

电子邮件是政企机构办公的重要工具。  
中国境内企业级电子邮箱活跃用户规模约为1.2亿。  
企业级用户平均每天收发到电子邮件约16.1亿封。

### 特别提示：

切勿使用办公邮箱注册游戏、购物、社交、论坛等第三方应用账户，否则会有如下风险：

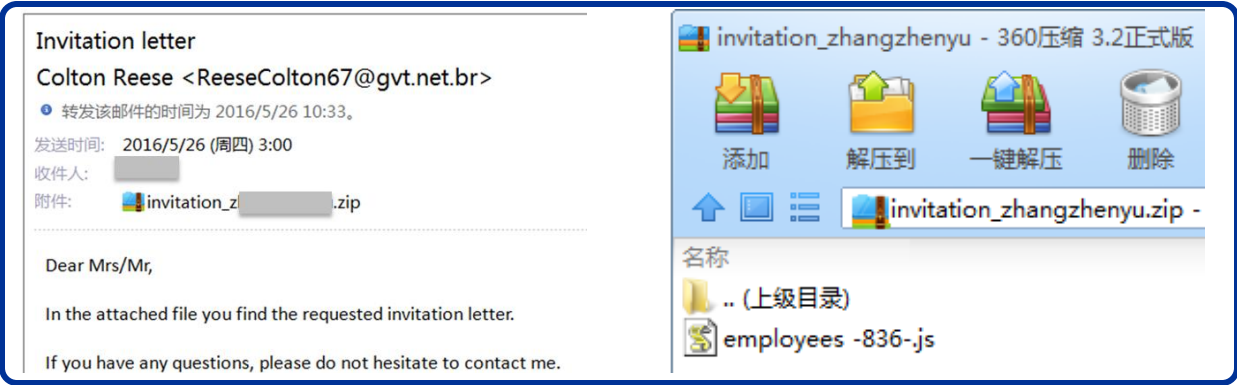
- 您的办公邮箱中会收到很多垃圾邮件。
- 一旦第三方应用平台被黑，您办公邮箱的帐号和密码也可能会
- 同时泄露，造成邮件中的机密外泄。
- 办公邮箱密码泄露，可能引发连锁反应，进而泄露机构内网帐号，导致内网被黑客入侵。



# 邮件附件常带毒，陌生来源勿打开

## 勒索邮件

下面这封不起眼的邮件携带了一个ZIP格式的附件，解压后生成一个JS文件，它实际上是一个勒索软件，一旦点击打开，电脑中所有的办公文档、照片、视频都会被加密，只有向勒索者支付赎金后才能解密。

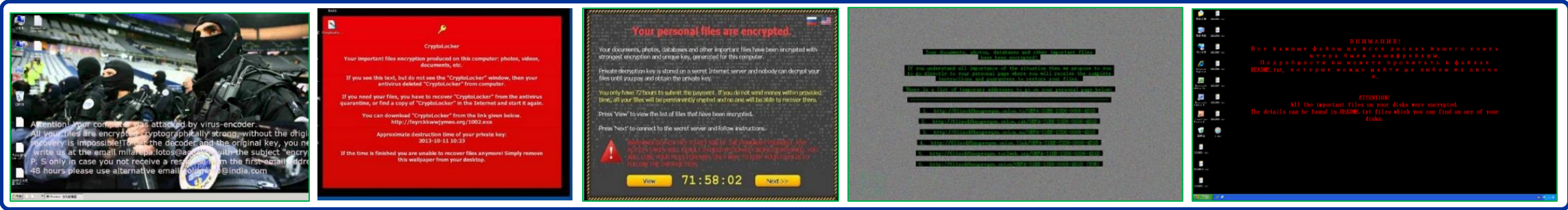


## 窃密邮件

2016年6月，一封带毒邮件盗走日大型旅社800万用户资料。



## 勒索软件中招后屏幕的现象



# 收信看清发件人，冒名顶替要当心



电子邮箱收件人的信息由邮件显示名和邮件地址两部分组成，而邮件地址又是由邮箱帐号和邮箱域名组成。

## 特别提示：

- 显示名很容易被仿冒

邮件的显示名通常可以由发件人任意编写。骗子们经常把邮件显示名伪装成：管理员、XX机构、XX领导等。

- 邮箱帐号也可能被仿冒

如，真实邮箱是zhangsan@263.com,仿冒邮箱却是zhangsan@qq.com，不仔细看很难分辨。

所以，收到邮件不能光看显示名，还要认真查看发件人的邮件地址以及邮箱域名，稍不留心就可能上当受骗。

# OA 钓鱼最危险，美国大选也中招

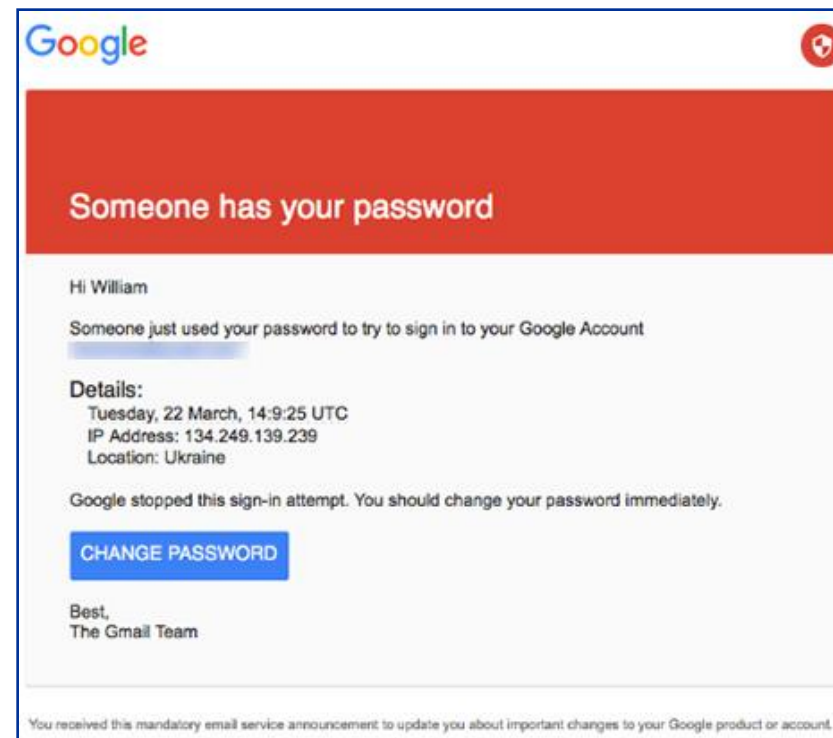


## OA钓鱼

冒充系统管理员发送的欺诈邮件被称为OA钓鱼。  
OA钓鱼多用于盗号。



2016年美国大选，黑客组织冒充Google邮件系统安全管理员给希拉里竞选团队负责人发信，骗取了负责人的邮箱密码，盗取并公布了希拉里竞选团队的机密邮件，最终使得希拉里败选，特朗普上台。



希拉里竞选团队成员William Rinehart收到的伪装成Google安全团队的鱼叉邮件

# 骗你上当有理由，仿冒登录盗帐号



安全邮箱升级Mail

尊敬的用户 [ ]

由于你目前使用的安全连接协议版本存在漏洞，可能导致帐户的相关数据可被窃听，我们暂时阻止你登录邮箱使用功能，给您带来不便敬请谅解。本次需要您在72验证升级完成激活邮箱才能解除困扰，超时系统将对您的账号冻结！

时间	地点	事件
2016-5-6 - 2:23:59	本地局域网	邮箱异常操作
2016-5-6 - 2:23:59	本地局域网	邮箱异常操作

(1) 请配合我们相关工作

(2) 点击这里解除 **立即恢复正常**

注：此邮件72小时内有效，请及时验证信息恢复正常使用，解除安全隐患！

Copyright ? 2005 - 2016 Tencent. All Rights Reserve

安全性升级

你好 [ ]

您的邮箱配额利用率已超过最大值 大小，你将不能够直到你收到新的电子邮件 重新验证。

要避免此问题，请增加邮箱配额存储由 访问下面的重新验证应用程序

[点击这里重新验证资格](#)

感谢您的合作。  
邮件管理员

您收到此强制性的电子邮件服务公告，以更新您的重要变化的到你的邮箱帐户 [ ]

© 2016.

邮箱扩容

服务器消息

亲 [ ]

我们的记录表明您最近提出的要求来关闭您的电子邮件 ( [ ] )，这要求我们 [将尽快处理](#)

如果该请求被意外取得，你有没有它的知识，建议您现在就取消该请求

[取消停用](#)

但是，如果不取消这项要求，您的帐户很快就会关闭，所有的电子邮件数据将永久丢失。

问候，  
电子邮件管理员

从电子邮件安全服务器是自动生成该消息，并发送至该电子邮件回复无法送达。  
此电子邮件是为： [ ]

邮箱停用

## OA钓鱼手法

- OA钓鱼的目的是诱骗受害者在虚假的登录页面上输入帐号和密码，进而实现盗号。
- OA钓鱼的“理由”有很多，左边几个都是，您能认得出吗？

各位同事

用户	[ ]
维护原因	由于离职人员较多，导致内部邮箱被他人使用，登陆存在卡顿发信速度比较慢，特此升级该邮箱！
维护时间	维护虚耗时1-6小时，为保证邮箱能正常使用，请立即升级
注意事项	请收到此邮件的人员立即升级以免总要数据丢失，否则我公司，会按离职人员删除该邮箱账户
操作指示	<a href="#">请点这里进行升级</a>

员工离职

尊敬的领导以及同事：您的管理员已经启动“邮箱搬家”，这将助于邮箱升级。

在收到通知的第一时间，将下列信息填写完毕回复本邮箱！

姓名：

职位：

邮箱：

邮箱密码：

历史密码：

邮箱搬家

# 安全习惯早养成，提高警惕少出错



## 尽量不要在微信上谈工作

微信是比较开放的社交环境，不适合谈论工作。办公社交建议使用企业级社交软件。

## 不在电脑桌前电脑要锁屏

电脑锁屏，既可以防止他人偷窥到自己电脑中的文件，又可以防止他人胡乱操作损坏文件。



## 保存文件尽量不要用密字

保存文件时文件名尽量不要包含密、秘密、保密、绝密等字样，这些字很容易被黑客盯上。

## 下班以后一定要关闭电脑

很多人为图方便，下班以后不关电脑，这就给黑客留出了更多电脑前无人值守的攻击时间。



# 03

## 业务安全必修班

网络安全法常记，法律要求是第一  
等级保护在手中，单位安全有保证

数据安全法牢记，  
个人信息保护法，

# 网络安全法常记，法律要求是第一

## 中华人民共和国网络安全法



由全国人民代表大会常务委员会于2016年11月7日发布

自2017年6月1日起正式实施

### 保障网络运行安全

- ★ 落实网络运营者第一责任人的责任，将信息安全等级保护制度上升为法律  
(相关条文：第二十一条)
- ★ 网络运营者依照法律、行政法规和标准，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，维护网络数据的完整性、保密性和可用性  
(相关条文：第三章第一节)

### 保障网络信息安全

- ★ 明确网络运营者、电子信息发送服务提供者和应用软件下载服务提供者处置违法信息的义务  
(相关条文：第四十七条、四十八条)
- ★ 规定了网络运营者对公安机关、国建安全机关为维护国家安全和侦察犯罪的活动提供技术支持和协助的义务  
(相关条文：第二十八条)
- ★ 赋予有关主管部门处置违法信息的权力  
(相关条文：第四十八条)

### 保障关键信息基础设施安全

- ★ 关键信息基础设施界定为是那些一旦遭到破坏、丧失功能或者数据泄露将对我国国际安全、国计民生、公共利益造成重大危害的重要网络设施和系统  
(相关条文：第三十一条)
- ★ 关键信息基础设施保护制度的主要内容包括：制定实施关键基础设施保护计划；加强组织机构和管理能力建设；定期进行安全风险评估；加强组织协调，共享安全信息，系统开展应急演练和应急响应，开展技术支持和协助等  
(相关条文：第三章第二节)
- ★ 建立关键信息基础设施运营者采购网络产品、服务的安全审查制度  
(相关条文：第三十五条)

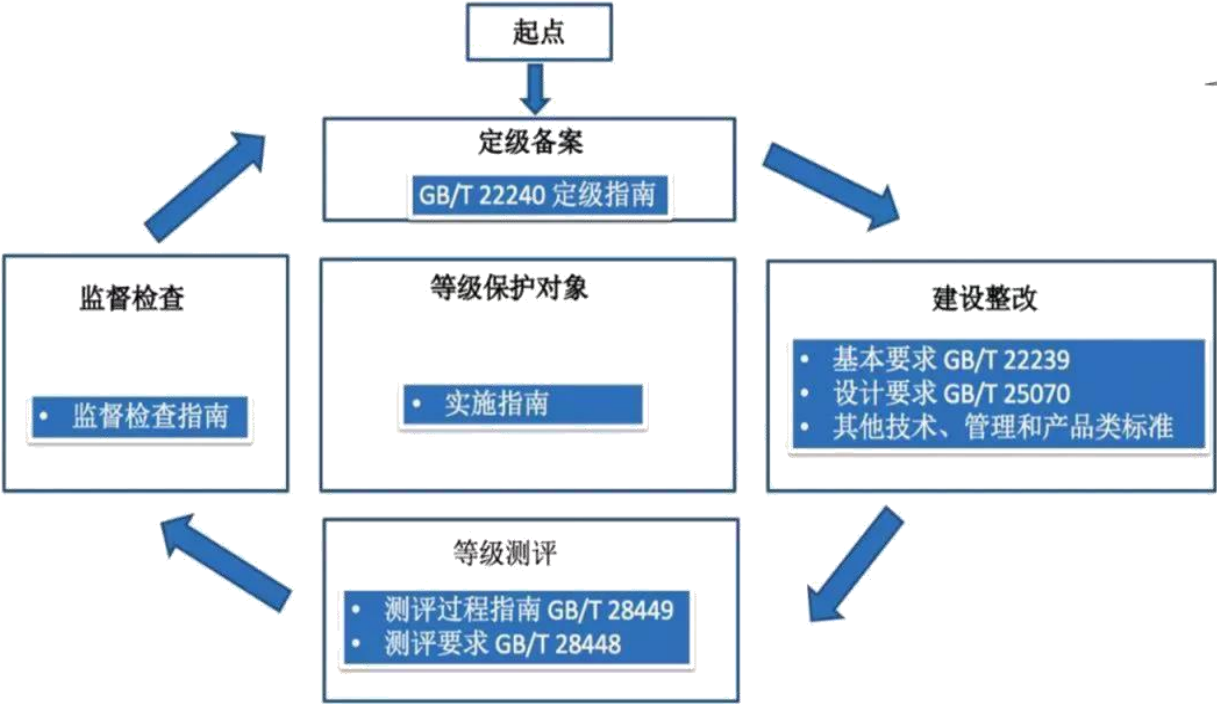
### 保障个人信息安全

- ★ 关键信息基础设施的运营者将在中国境内运营中收集和产生的个人信息及重要数据必须存储在中国境内，因业务需要经过安全评估可以向境外提供这些数据  
(相关条文：第三十七条)
- ★ 加强对公民个人信息的保护，防止公民个人信息数据被非法获取、泄露或者非法使用  
(相关条文：第四十一条至四十四条)
- ★ 网络运营者收集、使用个人信息，应当遵循合法、正当目的原则，遵守通知同意规则，保障信息主体的决定权、知情权、更正权、删除权等权利和数据质量与安全  
(相关条文：第四十一条、四十三条)

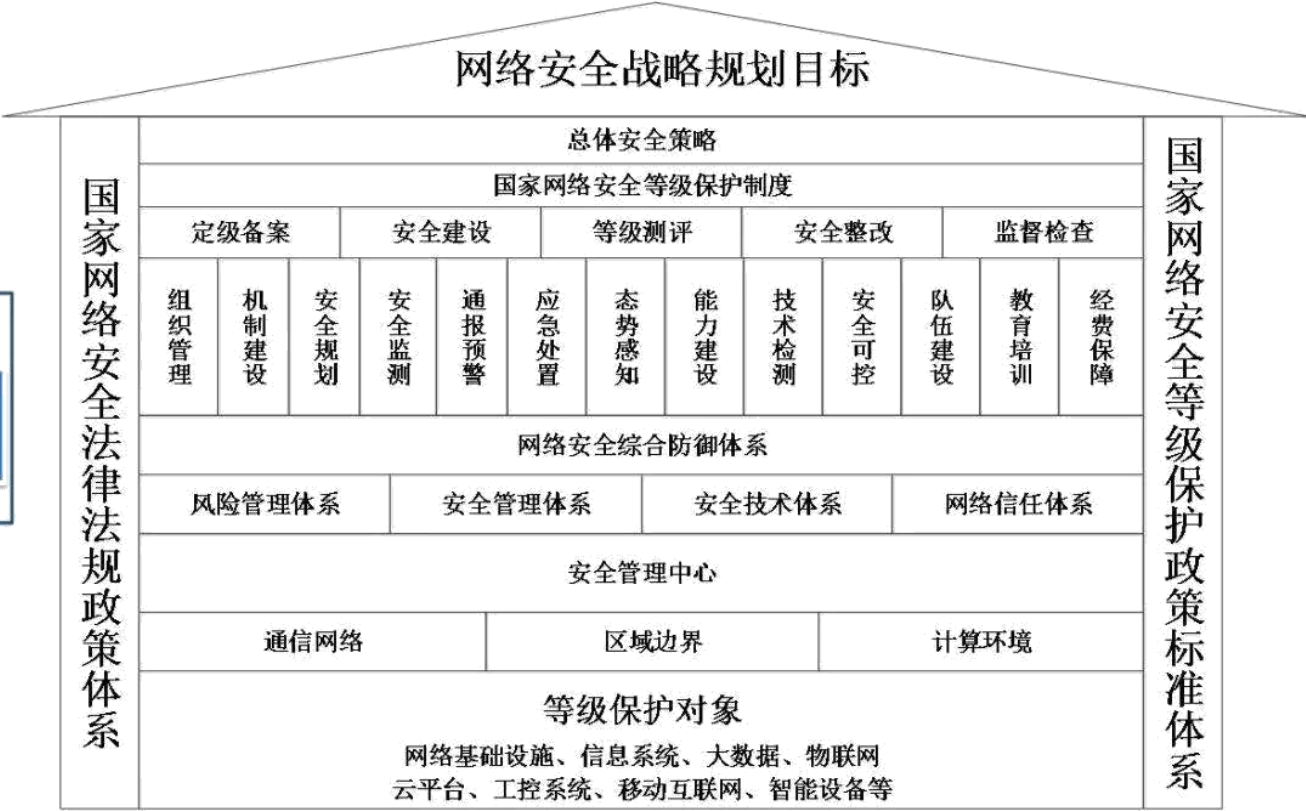
### 检测预警与应急处置

- ★ 明确建立国家统一的检测预警、信息通报和应急处置制度和体系  
(相关条文：第五十一条)
- ★ 发挥有关职能部门的作用、建立相关领域的网络安全检测预警、信息通报和应急处置制度  
(相关条文：第五十一条、五十三条)
- ★ 对政府部门进行网络安全信息的检测、分析和预警作了规定  
(相关条文：第五十四条、五十六条)
- ★ 对网络安全事件的应急处置作了规定  
(相关条文：第五十五条、五十七条)
- ★ 对网络通信临时显示措施作了规定  
(相关条文：第六十八条)

# 等级保护在手中，单位安全有保证



等级保护工作流程及标准



等级保护安全框架



## 第一章 总则

- 目标、范围
- 明确定义
- 国家战略
- 明确主体、职责
- 明确数据要素
- 依法利用、有序流动
- 宣传普及

## 第二章 数据安全与发展

数据安全和促进数据开发利用并重

- 大数据战略
- 数字经济
- 数据开发利用、数据安全技术研究
- 数据安全标准体系
- 数据安全监测评估、认证服务
- 数据交易管理制度
- 教育培训、人才培养

## 第三章 数据安全制度

数据分级分类  
(重要数据保护目录)

数据安全应急处置机制

数据安全审查制度

数据出口管制

数据安全风险信息  
获取、分析、研判、预警

风险评估

监测预警

信息共享

风险报告

针对歧视性禁止、限制的对等措施

## 第四章 数据安全保护义务

数据安全治理

数据安全管理制度

数据安全教育培训

数据安全技术措施

数据安全管理机构

数据风险管理  
发现、处置、告知、上报

开发数据新技术的目的

风险监测

定期风险评估  
(重要数据)

合法，正当收集数据

数据处理及服务

数据来源核实及记录

在线数据处理许可

合法数据调取

数据跨境管理

## 第五章 政务数据安全与开放

- 大力推进电子政务建设
- 健全数据安全管理制度
- 监督接收方数据安全保护义务
- 政务数据公开
- 政务数据开放目录
- 政务数据开放平台

## 第六章 法律责任

加大对违法行为的处罚力度

## 第七章 附则

# 个人信息保护法



## 第一章 总则

- 1-3 目标、宗旨、范围
- 4 关键定义
- 5 合法正当必要诚信原则
- 6 明确、合理原则
- 7 公开、透明原则
- 8 准确、完整原则
- 9 责任落实
- 10 强制要求
- 11-12 环境、合作

## 第二章 个人信息处理规则

第一节 一般规定			
13 处理前提	14 取得同意	15 撤回同意	16 不得拒绝服务
17 告知要求	18 例外情形	19 最短时间	20 共同处理
21 委托处理	22 信息转移	23 第三方共享	24 自动化决策
25 不得公开		26 公共采集	27 重新同意

第二节 敏感个人信息处理规则		
28 关键定义	29 单独同意	30 必要性告知
31 未成年保护		32 行政许可

第三节 国家机关处理个人信息的特别规定		
33 适用范围	34 范围限度	35 告知同意
36 境内存储		37 公共事务

## 第三章 个人信息跨境提供的规则

38 个人信息处理者向境外提供个人信息的前提条件 (具备下列条件之一: 安全评估、个人信息保护认证、订立合同、其他条件)
39 个人信息处理者向境外提供个人信息的前提条件 (需要按照本条列举的要求向个人如实披露相关信息, 并获其“单独同意”)
40 关键信息基础设施个人信息跨境要求 (需向境外提供的, 应当通过国家网信部门组织的安全评估; 法律、行政法规和国家网信部门规定可以不进行安全评估的, 从其规定)
41 外国司法或者执法机构关于提供存储于境内个人信息的请求 (非经中华人民共和国主管机关批准, 个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息)
42-43 限制清单、反制措施 (明确构建“个人信息提供黑名单制度”以及在个人信息保护领域的报复和反制措施)

## 第四章 个人在个人信息处理活动中的权利

44 个人对其个人信息的处理享有知情权、决定权	45 个人有权向个人信息处理者查阅、复制其个人信息
46 有权请求个人信息处理者更正、补充	47 个人信息处理者主动删除个人信息的情形规定
48 有权要求对其个人信息处理规则进行解释说明	49 自然人死亡后的近亲代行使权
50 便捷的个人行使权利的申请受理和处理机制	

## 第五章 个人信息处理者的义务

51 个人信息处理者基本义务	52 个人信息保护责任到人	
53 境外机构义务	54 合规审计	55 影响评估
56 评估内容 (处理目的、处理方式、处理影响等)		57 个人信息安全事件补救措施以及补救通知
58 大型互联网平台义务		59 受托人义务

## 第六章 履行个人信息保护的职责部门

60 职责部门
61 保护职责
62 工作说明
63 履职措施
64 约谈审计
65 投诉举报



谢谢