
湖北美術学院

HUBEI INSTITUTE OF FINE ARTS

# 湖北美术学院信息安全意识培训

Contents

# 什么是信息安全意识?


**信息安全意识（Information Security Awareness），就是能够认知可能存在的信息安全问题，预估信息安全事故对组织的危害，恪守正确的行为方式，并且执行在信息安全事故发生时所应采取的措施。**

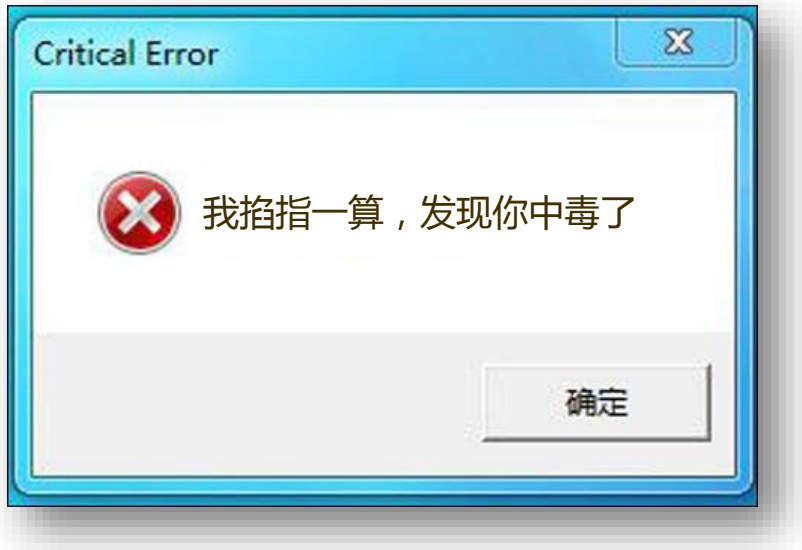
# 犯过以下的错误吗?

- 将口令写在便签上，贴在电脑监视器旁
- 开着电脑离开，就像离开家却忘记关灯那样
- 轻易相信来自陌生人的邮件，好奇打开邮件附件
- 使用容易猜测的口令，或者根本不设口令
- 不安装防病毒软件，或者病毒库更新不及时
- 不能保守秘密，口无遮拦，上当受骗，泄漏敏感信息
- 使用无线或者随意将无关设备连入工作网络
- 在系统更新和安装补丁上总是行动迟缓
- 只关注外来的威胁，忽视内部人员的问题

# 1、计算机安全防护知识

## 计算机安全状态的识别

- 计算机运行速度明显变慢
- 操作系统经常提示错误信息
- 一些应用程序打开出现异常
- 在上网过程中不断有广告窗口弹出



# 2、用户密码管理

用户名+口令是最简单也最常用的身份认证方式

口令是抵御攻击的第一道防线，防止冒名顶替

口令也是抵御网络攻击的最后一道防线

针对口令的攻击简便易行，口令破解快速有效


由于使用不当，往往使口令成为最薄弱的安全环节

口令与个人隐私息息相关，必须慎重保护

# 一些数字……

- 如果你以请一顿工作餐来作为交换，有70%的人乐意告诉你他（她）的机器口令
- 有34%的人，甚至不需要贿赂，就可奉献自己的口令
- 另据调查，有79%的人，在被提问时，会无意间泄漏足以被用来窃取其身份的信息
- 平均每人要记住四个口令，95%都习惯使用相同的口令（在很多需要口令的地方）
- 33%的人选择将口令写下来，然后放到抽屉或夹到文件里

# 脆弱的口令

- 少于8个字符
- 单一的字符类型，例如只用小写字母，或只用数字
- 用户名与口令相同
- 最常被人使用的弱口令：
  - 自己、家人、朋友、亲戚、宠物的名字
  - 生日、结婚纪念日、电话号码等个人信息
  - 工作中用到的专业术语，职业特征
  - 字典中包含的单词，或者只在单词后加简单的后缀
- 所有系统都使用相同的口令
- 口令一直不变

# 脆弱的口令

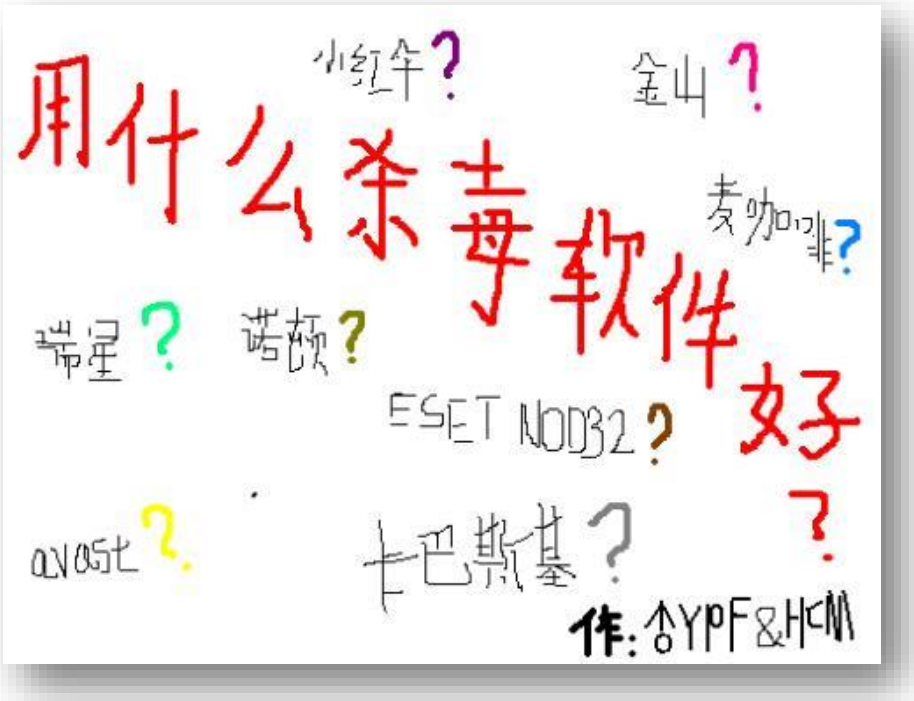

中国版25个“弱密码”
*本项统计基于国内流行的密码字典软件破解列表
*标红密码同时也是国外网民常用的“弱密码”
简单数字组合
000000
111111
11111111
112233
123123
123321
123456
12345678
654321
666666
888888
顺序字符组合
abcdef
abcabc
abc123
a1b2c3
aaa111
临近字符组合
qwerty
qweasd
特殊含义组合
admin
password
p@ssword
passwd
iloveyou
5201314

# 建议……

- 尽量使用“字母(大小写)+数字+特殊符号”形式的高强度密码；
- 网银、网上支付、常用邮箱、聊天账号单独设置密码，切忌“一套密码到处用”；
- 按照账号重要程度对密码进行分级管理，重要账号定期更换密码；
- 避免以生日、姓名拼音、手机号码等与身份隐私相关的信息作为密码，因为黑客针对特定目标破解密码时，往往首先试探此类信息。

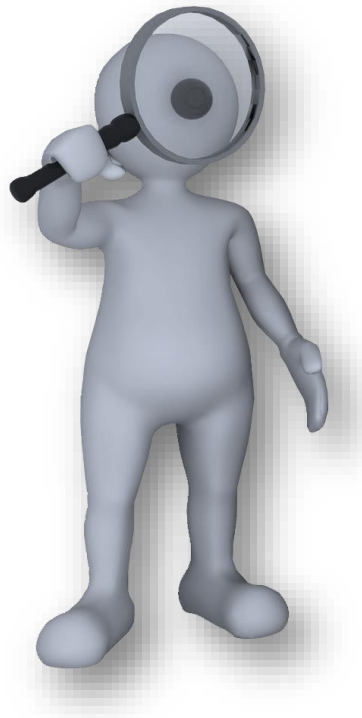
# 3、计算机病毒防范

- 安装病毒防护程序并及时更新病毒特征库；
- 在以下情况注意病毒防范：
  - ✓ 下载电子邮件附件时；
  - ✓ 在网络上下载文件时；
  - ✓ 使用移动存储介质时；
  - ✓ 安装不明来源的软件时；
  - ✓ 浏览网页时；计算机使用过程中发现异常时



# 4、浏览网页安全

- 使用安全浏览器（如：搜狗等安全浏览器）
- 收藏经常访问的网站
- 安装杀毒软件，开启实时防护功能，并保持更新；
- 对超低价、超低折扣、中奖等诱惑要提高警惕；
- 警惕色情、赌博、反动等非法网站，避免访问；
- 防止网页自动记住账号密码



# 5、邮件钓鱼如何防范

- 应警惕的邮件内容：
  - ✓ 伪造发件人信息
  - ✓ 模仿单位领导
  - ✓ 索取个人信息
- 进行网上交易时要注意做到以下几点：
  - ✓ 核对网址
  - ✓ 选妥和保管好密码、做好交易记录。
  - ✓ 避免公用计算机使用网上交易系统；
  - ✓ 不通过搜索引擎上的网址或不明网站的链接进入。
  - ✓ 在网络交易前，对交易网站和交易对方的资质全面了解。

# 6、电子邮件安全

- 机关工作人员工作邮件建议使用政府自建邮箱，严禁使用境外邮箱和商用邮箱
- 为电子邮箱设置高强度密码，并设置每次登陆时必须进行帐号密码验证；
- 开启防病毒软件实时监控，检测收发的电子邮件是否带有病毒
- 不打开或转发来历不明的电子邮件及附件

# 7、工作环境安全

- 禁止随意放置或丢弃含有敏感信息的纸质文件，废弃文件需用碎纸机粉碎
- 废弃或待修磁介质转交他人时应经管理部门消磁处理
- 离开座位时，应将贵重物品、含有机密信息的资料锁入柜中，并对使用的电脑桌面进行锁屏
- 应将复印或打印的资料及时取走
- UKEY不使用时应及时拔出并妥善保管
- 禁止将手机和无线（例如：360wifi等）连接办公电脑（内网）

# 8、手机安全建议

- 为手机设置密码
- 利用手机中的各种安全功能
- 从正规网站下载手机应用程序和升级包
- 禁用Wi-Fi自动连接功能
- 为手机安装安全软件
- 为手机SIM卡设置密码
- 经常为手机做数据同步备份
- 减少手机中的本地分享
- 对手机中的Web站点提高警惕
- 对程序执行权限加以限制

# 9、安全保密意识

- 敏感及内网计算机不允许连接互联网或其它公众网络
- 处理敏感信息的计算机、传真机、复印机等设备应当在单位内部进行维修，现场有专门人员监督，严禁维修人员读取或复制涉密信息；确需送外维修的，应当拆除涉密信息存储部件
- 敏感信息设备改作非涉密信息设备使用或淘汰时，应当将涉密信息存储部件拆除
- 敏感及内网计算机不得使用无线键盘、无线鼠标、无线网卡
- 敏感文件不允许在非涉密计算机上进行处理

# 11、新兴事物存在安全隐患

**手机扫描二维码存在安全隐患**

2016 年 3 月 15 日， 央视 315 晚会曝光称不法分子利用二维码生成器把病毒植入到普通的二维码中，当用户使用手机扫描这些二维码时，病毒便会植入到用户手机中。 这样，不法分子就就可以通过技术手段盗取用户信息，甚至拦截用户的通信信息，包括用户的身份证、验证码等，然后，不法分子便可以肆意更改用户的支付密码，从而盗取用户的钱财


二维码由于隐蔽性高，制作成本低，二维码背后未经安全认证的网站链接和应用程序逐步成为黑客的青睐对象。

# 12、勒索软件

2017年5月12日，新型“蠕虫式”勒索病毒 WannaCry 在全球爆发，全球上百个国家遭遇攻击，国内的重灾区是校园系统、医疗系统、能源行业，以及公安办事系统。一旦被感染，磁盘文件会被加密，只有支付高额赎金才能解密恢复，目前技术还无法解密该勒索软件加密的文件。此次WannaCry勒索病毒是黑客通过改造之前泄露的NSA黑客武器库中“永恒之蓝”攻击程序发起的网络攻击事件，利用了微软基于445 端口传播扩散的 SMB 漏洞MS17-010。

# 13、勒索软件安全思考及建议

WannaCry并非APT攻击，仅仅是病毒攻击行为，并不是不可防御的。并且，微软已在今年4月份发布了SMB 漏洞的补丁，用户有足够的时间做好预防工作，为什么还有大量用户受影响？并且其中还包括一些行业的与互联网隔离的专网。究其原因主要是以下几点：

1、大量用户缺乏全过程保护的安全体系

2、忽视了内部局域网、专网和数据中心的安全防护

3、忽视了内部局域网、专网和数据中心的安全防护

安全建议：

1、定期备份系统与重要文件，并离线存储独立设备；

2、使用专业的电子邮件与网络安全工具；

3、经常给操作系统、设备及第三方软件更新补丁；

4、使用专业的反病毒软件、防护系统，并及时更新；

5、设置网络安全隔离区，确保既是感染也不会轻易扩散；

6、加强员工（用户）安全意识培训，不要轻易下载文件、邮件附件或邮件中的不明链接。

# 14、WIFI安全隐患

**公共免费 WiFi 可瞬间盗取你的一切隐私**

2016 年 3 月 15 日，央视 315 晚会主持人进行了这样一个实验： 现场观众的手机都连上由主办方提供的免费无线网络，然后打开自己常用的一两个消费类软件，比如打车、订餐、购物的软件，浏览一下过去下的订单和消费记录。令人惊讶一幕出现了，现场的大屏幕上各种地址、姓名、身份证号、银行卡号都显示了出来。


Contents

# 网络安全法概览

**目标**

国家层面：维护网络空间主权和国家安全、社会公共利益

企业层面：规范相关行业

公民层面：保护公民、法人和其他组织合法权益

**范畴**

在中华共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

**总览**

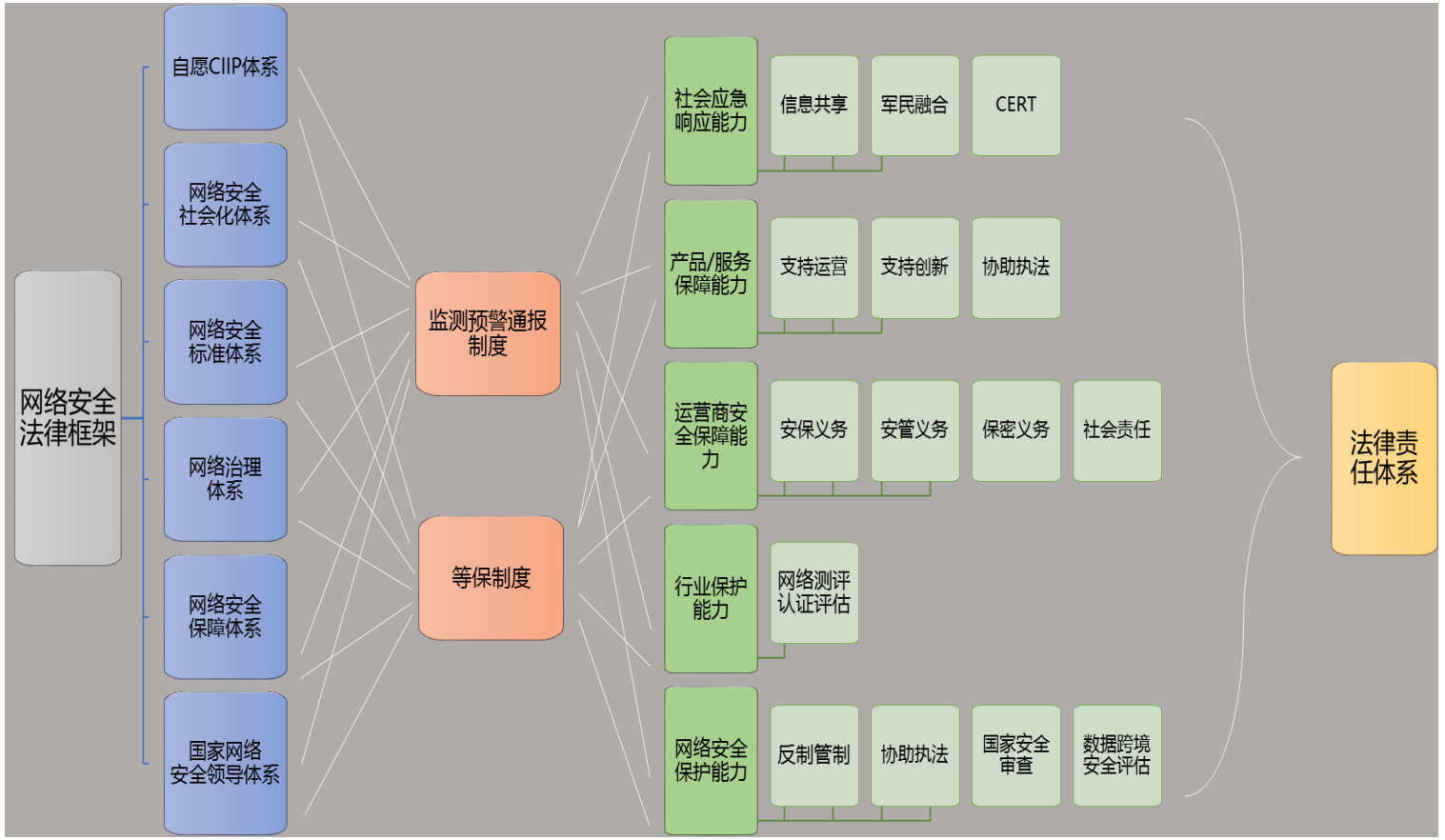
法律条文：共7章，79条，对企事业单位来说，有38条明确规范义务

量刑：对单位及责任人处以罚金，按严重程度可进行刑事处罚

2016年11月7日发布，2017年6月1日起施行

# 网络安全法的法律框架要点

- **理念：总体国家安全观**
- **方针：积极利用、科学发展**
  - 依法管理、自主可控
- **原则：安全与发展并重**
  - 诚实信用原则
  - 重点保护原则(关键基础信息建设）
  - 谁主管谁负责原则



《中华人民共和国网络安全法》,2017年6月1日起正式施行，网络安全法涉及的面很广，很多条款与我们息息相关。本次网络安全法对个人信息保护提出了严格的要求，对泄漏、丢失、出售或非法向他人提供个人信息进行了严厉处罚。

第四章网络信息安全

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

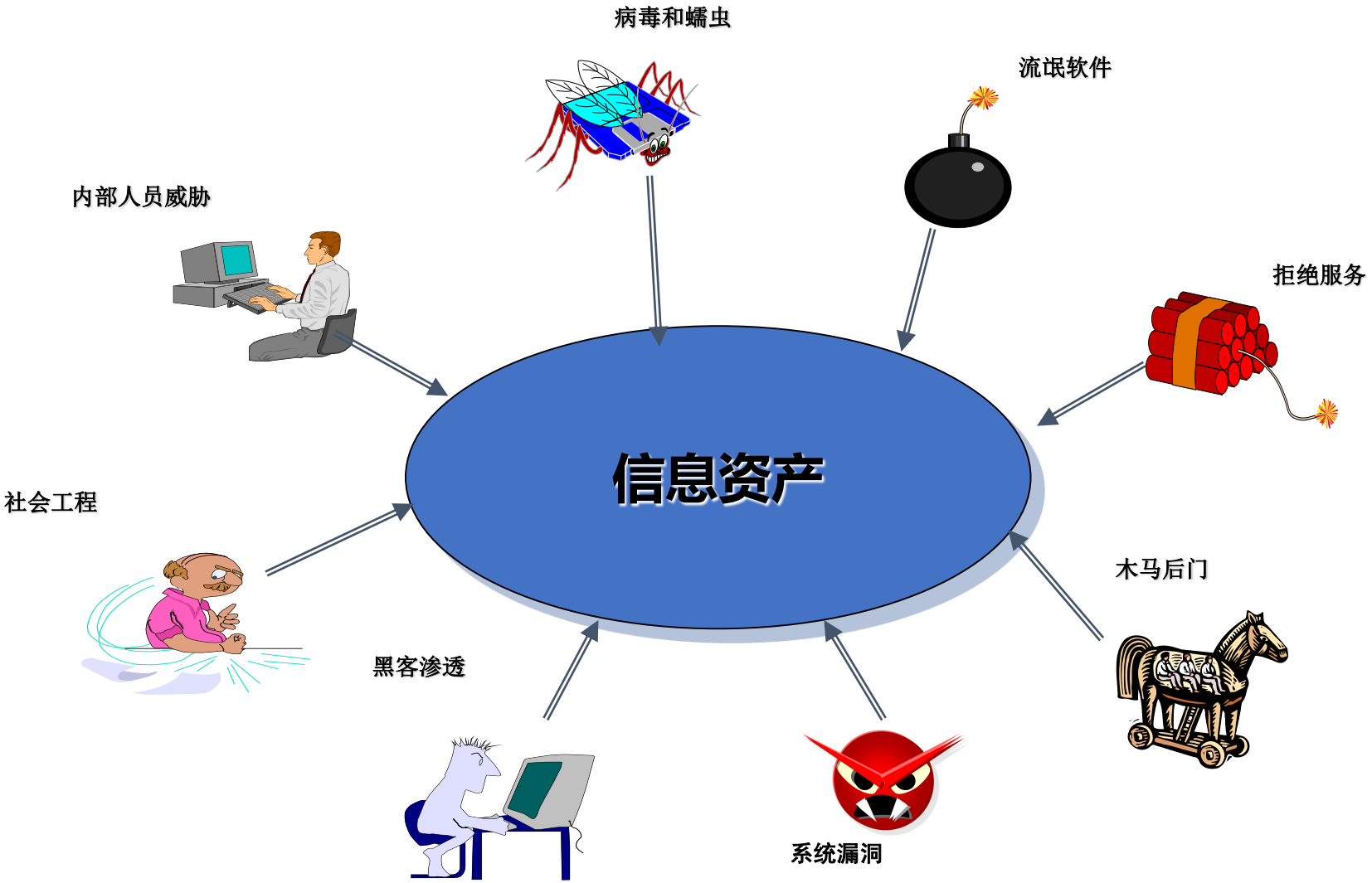
第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

除了网络运营者需要做好个人信息安全的防护外，我们个人也需要注意自己的信息安全。简单总结几条注意事项：

- 密码设置不能太简单，太简单的密码应用不能太重要，关系到钱的密码，字母数字大小写不能少，例如支付宝，微信等。不同应用的密码不能一样，不要一个密码玩通关，撞库就是这么来的。
- 一些短信、朋友圈分享有好处拿的，一些网址后缀很奇怪的，三思而后点，多看少动；
- 个人电脑，手机要有防火墙、杀毒软件之类的安全防护软件，这是最基本的，虽然有时会误操作，但是总比没有好；
- 小网站少看，少浏览一些动作片网站，你不去危险的地方，自然接触到危险的机会就少，就像社会一样，远离身边的垃圾人。

希望有一天在我们买完车、买完房、炒过股后没有无穷无尽的各种骚扰电话。经常都会接到要不要买房的电话。

# 威胁无处不在



# 内部威胁

使用者误操作

蓄意破坏

职责权限混淆

# 造成安全事件的主要根源

- **技术弱点**　系统、 程序、设备中存在的漏洞或缺陷
- **操作弱点**　配置、操作和使用中的缺陷，包括人员的不良习惯、审计或备份过程的不当等
- **管理弱点**　策略、程序、规章制度、人员意识、组织结构等方面的不足

一个巴掌拍不响！

外因是条件

内因才是根本！

# 信息安全趋势展望

1. **勒索软件依然会是低成本高收益网络犯罪主流**
2. **政治色彩严重的网络攻击已波及民生领域**
3. **大规模数据泄露事件频发，云安全问题应得到高度重视**
4. 第三世界金融系统成为黑客的提款机
5. 智能摄像头（家居，汽车）安全隐患进一步加剧。


# 湖北美術学院
HUBEI INSTITUTE OF FINE ARTS

湖北美术学院信息网络中心

info@hifa.edu.cn