网络安全知识培训

上海极道云计算科技有限公司

目 录

信息安全基本概念：什么是信息

信息的定义

信息是信息论中的术语，常常把**能够传递的有意义的内容**称为信息。

信息的种类

- 数据　文本
- 图像　声音

—— 我们平常接触到的信息

前情提要：

小王对小李说稍后去你办公室，若张处长不在你就敲两下桌面，若他在呢你就什么都不做；

案例场景：

五分钟后，小李正在写材料，看到小王进来后继续埋头写仿佛没看见，于是小王获得张处长在岗的信息。

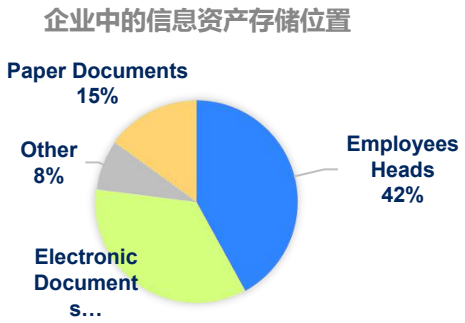
—— 什么都不做也能传达信息

信息安全基本概念：什么是信息

信息都在哪里

对企业有价值的信息统称为**信息资产**，以包括软硬件、人员、文档等各种形式存在

据Delphi机构统计，机构价值的26%体现在固定资产和一些文档上，而**高达42%**的价值是存储在员工的脑子里，而这些信息的保护没有任何一款产品可以做得到



内部信息

组织不想让其竞争对手知道的信息

客户信息

顾客/客户不想让组织泄漏的信息

共享信息

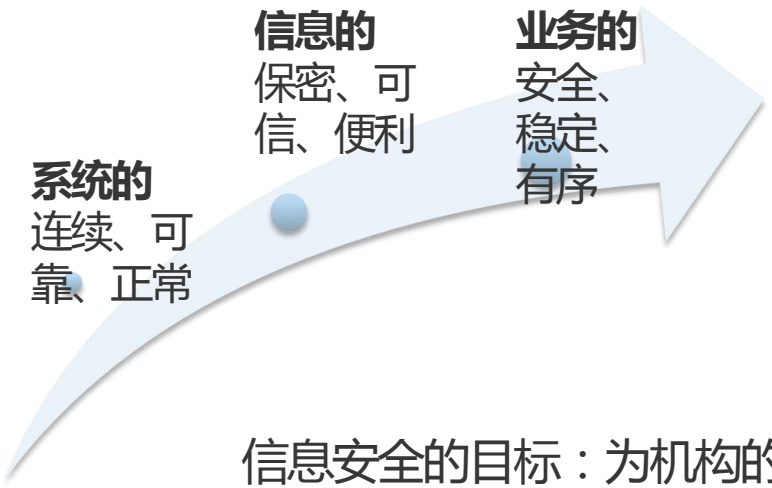
需要与其他业务伙伴分享的信息

信息需要流通，也需要保护；如何保护机构的信息资产，**不仅仅是** IT 和安全部门的职责

你脑子里的信息，只能通过自己安全意识的提高和工作流程的规范来保护

信息安全基本概念：什么是信息安全

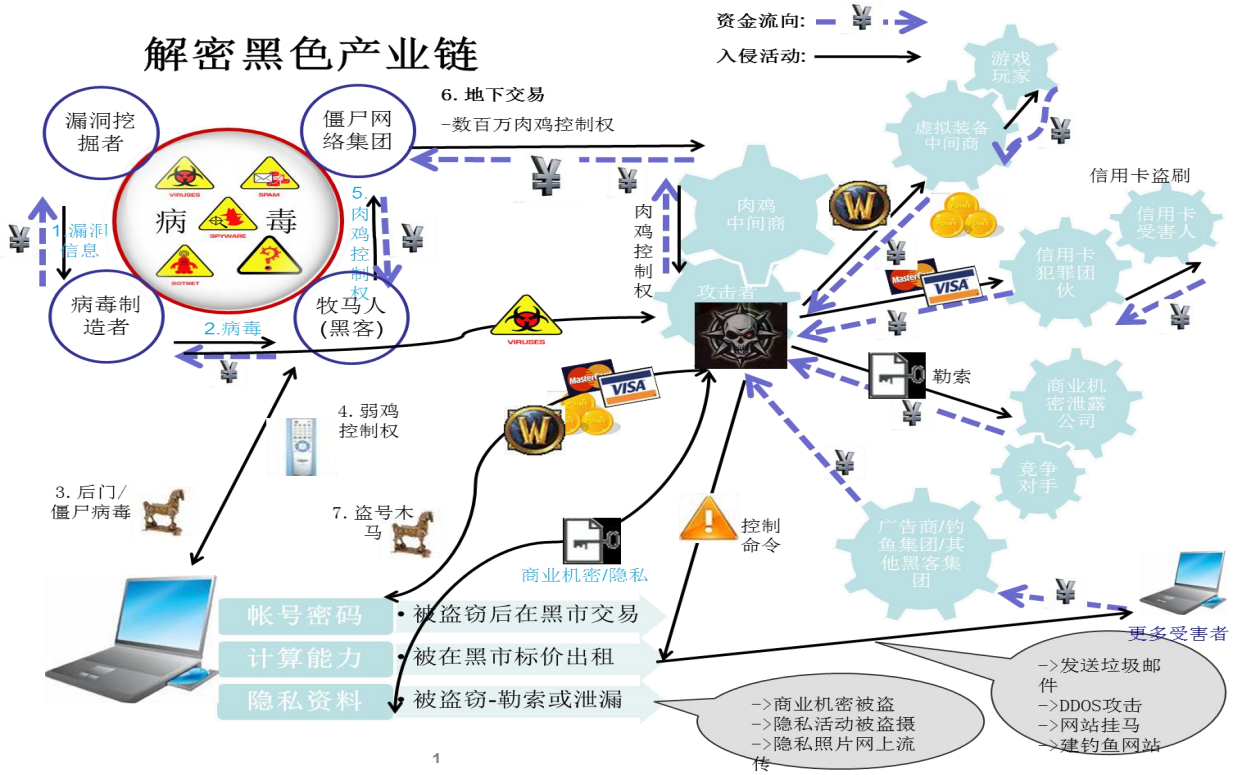
信息安全，就是采取措施**保护信息资产**，使之不因偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够**连续、可靠、正常**地运行，使安全事件对业务造成的**影响减到最小**，确保组织业务运行的**连续性**。



信息安全的目标：为机构的业务活动护航

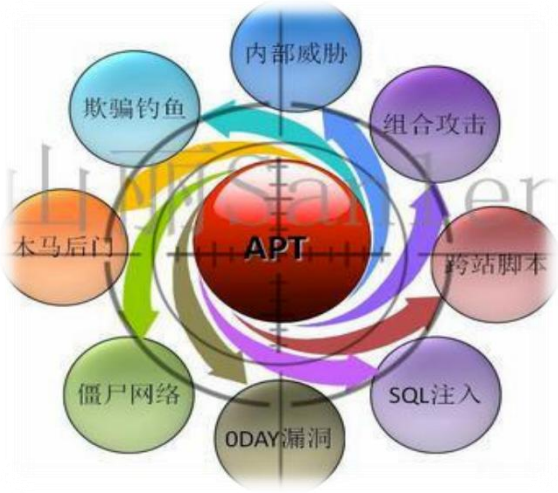
攻击从个人英雄向组织犯罪转变

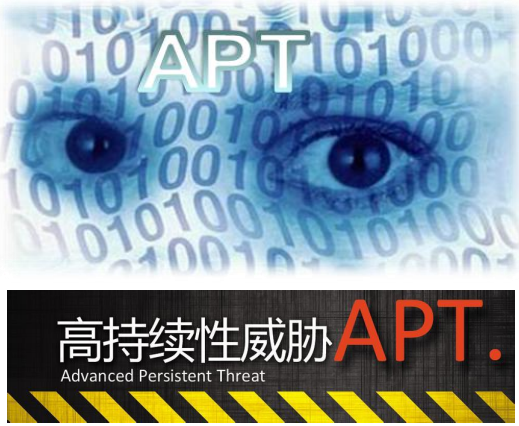
- 攻击变得越来越有组织性，攻击从个人英雄向组织犯罪转变;
- 有组织的攻击犯罪攻击资源更多，更加有效，造成的安全威胁更大



攻击手段体系化

- 采用体系化攻击手段的APT攻击呈爆发趋势，带来越来越大的安全威胁。
- APT攻击以窃取核心资料为目的，会运用各种攻击工具、受感染的各种介质、供应链和社会工程学等体系化的攻击手段实施先进的、持久的且有效的威胁和攻击。





信息安全上升到国家安全高度

- 美国 --- 《网络空间安全国家战略》，
  - 美国21世纪的经济繁荣依赖于网络空间安全
  - 将网络空间安全威胁定位为举国面临的最严重的国家经济和国家安全挑战之一
- 英国 --- 《英国网络安全战略》
  - 使英国面对网络攻击的恢复力更强，并保护其在网络空间中的利益；
  - 帮助塑造一个可供英国大众安全使用的、开放的、稳定的、充满活力的网络空间，并进一步支撑社会开放；

- 中国 --- 国家网络安全战略形成
  - 十六届四中全会首次明确将信息安全作为国家安全的主要内容
  - 2014年2月27日，中央网络安全和信息化领导小组宣告成立，中共中央总书记、国家主席、中央军委主席习近平亲自担任组长。网络安全上升到国家安全战略。
  - 习近平指出，没有网络安全就没有国家安全。

目 录

网络安全法-适用范围

2017年6月1日，《中华人民共和国网络安全法》开始施行

在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理。

网络安全法-权利

个人信息保护

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。

2020年10月13日，十三届全国人大常委会委员长会议提出了关于提请审议个人信息保护法草案的议案。

草案规定侵害个人信息权益的违法行为，情节严重的，没收违法所得，并处5000万元以下或者上一年度营业额5%以下罚款

网络安全法-义务

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

网络安全法-处罚

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。
违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。
《治安处罚法》、《刑法》
第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

网络安全法-处罚

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

网络安全法-处罚

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。
涉及法律法规：《治安处罚法》、《刑法》

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

目 录

伊朗核电站震网攻击事件

- 攻击者收集电站工作人员和家庭成员的信息，首先通过诱骗工作人员及其家人下载免费软件控制了这些家庭用的主机。
- 然后通过跳板攻击渗透进入物理隔离的伊朗核电站内部网络，成功控制了离心机的控制系统，修改了离心机数据，使其发电正常但生产不出制造武器的物质，但在人工检测显示端显示一切正常。成功的将伊朗制造核武器的进程拖后了几年。

北京移动盗窃案

- 资深软件研发工程师程稚瀚被指控侵入北京移动公司充值中心数据库，盗窃价值370多万元的充值卡密码

- 31岁的程稚瀚被捕前是UT斯达康（中国）有限公司深圳分公司资深软件研发工程师，其主要工作是帮助公司解决网络安全问题。此前，程稚瀚曾任华为技术有限公司工程师，负责西藏移动等公司的设备安装。

- 程稚瀚听同事说移动公司花上亿元安装了一个网络安全系统，于是决心“测试”一下，由于西藏移动公司的业务系统是他在华为公司时安装的，他知道进入系统的密码，所以就选择从西藏移动公司业务系统进入北京移动公司计费中心数据库，程稚瀚发现：“对管理员来说，网络安全系统没什么用”。

CSDN信息泄露事件

- CSDN创立于1999年，是中国最大的中文IT知识服务集团。目前，网站拥有2000万注册用户、50万注册企业及合作伙伴，日访问量约2000万次
- 2011年12月21日，国内大型IT专业社区CSDN被曝用户帐户遭泄漏，涉及账户600万。
- 由于互联网用户普遍在多个网站平台（甚至网银系统）上使用相同的用户名和密码，因此本次账号密码泄露造成了非常深远的影响。

棱镜门

棱镜计划（PRISM）是一项由美国国家安全局（NSA）自2007年小布什时期起开始实施的绝密电子监听计划，该计划的正式名号为“US-984XN”。英国《卫报》和美国《华盛顿邮报》2013年6月6日报道，美国国家安全局（NSA）和联邦调查局（FBI）于2007年启动了一个代号为“棱镜”的秘密监控项目 ，直接进入美国网际网络公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、苹果等在内的9家国际网络巨头皆参与其中。

希拉里邮件门

希拉里邮件门指美国前国务卿、民主党潜在总统候选人希拉里·克林顿被曝担任国务卿期间使用私人电子邮箱、而非官方电子邮箱与他人通信，涉嫌违反美国《联邦档案法》。

2015年3月，希拉里承认在任职国务卿期间使用私人邮箱处理约6万封邮件，其中3万封因涉及私人生活已被其团队删除，剩余约3万封公务邮件已于2014年底全部上交国务院。

王珞丹住址信息泄露事件

- **在Baidu上搜索到了王珞丹的博客和微博，并对其上的信息进行筛选，获得了以下两张比较有价值的图片，是她发表在微博上的从她家里往外拍的照片**

分析推测

一张是从窗内俯瞰小区绿化植物的照片，一张是从窗内拍摄的窗外全景图。照片透露几个主要信息：

- 第一，楼体外观和窗框难擦干净的痕迹，说明这是已经建成一段时间的西式小区。
- 第二，王珞丹家在顶层。
- 第三，小区内有三个在一条直线上大小一样的正方形花坛。

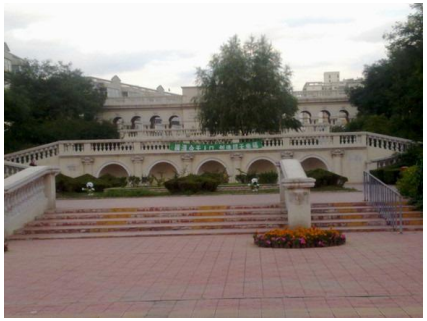
打开Google Earth。下面这张图是截取的一张北京城区的俯视图，为了方便解说分析过程，将其划分为九个区域。划分方式我是按照四环为标准的，也就是E区域的边界便是四环

区域搜索

请注意图片中间左部的三个正方形区域，注意这三个正方形在俯视图上的不同体现，再加上正方形区域边上的那个长方形区域，我们基本上可以确定，这就是我们所要找的目标小区。

实地检验

为了验证这个确实是所寻找的目标小区，博主还特意前往此地，下图是在现场拍摄的照片。和之前她从阳台上往外照的照片进行比较，便可获证这确实是所寻找的目标小区。



可以看到三个正方形花坛中的一个，以及背后的长方形拱形门

安全不仅仅是系统的安全

欺骗的艺术—社会工程学

利用社会交往（通常是在伪装之下）从目标对象那里获取信息，例如：

- 电话呼叫服务中心
- 在走廊里的聊天
- 冒充服务技术人员

著名黑客Kevin Mitnick更多是通过社会工程来渗透网络的，而不是高超的黑客技术

如果你给一个黑客100万，要求他窃取竞争对手的资料，你猜他首先会想到怎么做？

安全不仅仅是系统的安全

社会工程学

社会工程学是一种通过对目标心理弱点、本能反应、好奇心、信任、贪婪等心理布下的心理陷阱，诸如欺骗、伤害等危害手段取得自身利益的手法。

社会工程学陷阱就是通常以交谈、欺骗、假冒或口语等方式，从合法用户中套取用户系统的秘密，社会工程学需要搜集大量的信息针对对方的实际情况，进行心理战术的一种手法。

社会工程学是一种黑客攻击方法，利用欺骗等手段骗取对方信任，获取机密情报。总体上来讲，社会工程学就是使人们顺从你的意愿、满足你的欲望的一门艺术与学问。

攻击者/黑客瞄准的是人性的弱点

- 如果你接到一个口音浓重的电话：“小王啊，明天到我办公室来一趟”，大概**你会直接挂掉**

- 刚下完某宝、某东订单，接到自称客服电话说系统异常，您的订单未能成功下单，需要进行xxx操作；
- 你的订单号、姓名、地址对方报的都完全正确，但多心的你登录自己的账号却发现并没有问题，**那问题出在哪里？**
- 上面一步有细心同学可能已经不会中招，但如果有熟悉的合作伙伴向你索要一份文件并说明你的主管已经同意了，你会再确认一次吗？

常见安全隐患-钓鱼网站

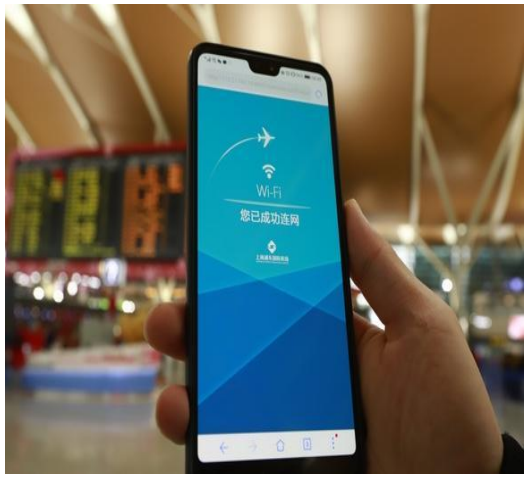

http://www.zysm2008.com/netpay/alipay.asp
这不是https加密链接
支付宝
您好，欢迎使用
即时到账交易（非支付宝信用中介服务，快速）


我的支付宝 – 支付宝 - 世界之窗 3.2
https://lab.alipay.com/user/i.htm?nekot=a2dkaXdzcw%3D%3D1281079123124
我的支付宝 – 支付宝
支付宝 知托付!
不安全
https://www.alipay.com
个人
企业
合作伙伴
支付宝
ALIPAY
首页
财富

常见安全隐患-WIFI连接

WI-FI信号具有一定的覆盖范围，机场、餐厅等公共场所通常都部署了免费WI-FI，免费热点在帮助人们节省流量费用、提高网络速度的同时，也存在着信息泄露、流量劫持、密码破解等风险。

- ✓ 公共场合连接WI-FI，要注意周边提示，接入官方网络
- ✓ 处理敏感信息或进行移动支付时，尽量不连接公共网络，而使用4G/5G
- ✓ 在办公区域，不自行搭建WI-FI热点，不使用密码共享类APP



常见安全隐患-电信诈骗

网络诈骗的手段多种多样，其中电信诈骗是应用最多的诈骗手段。

电信诈骗不仅有冒用他人身份这一种诈骗手段，利用恶意链接与挂马页面，也是一种手段，手机中毒后，黑客通过监听、截获短信等方式，结合其他途径活得的身份证、银行卡、支付账号进行盗刷盗用。

网络诈骗已经形成了一条完整的违法产业链，网络诈骗的不法分子结成团伙作案，各环节互不认识但分工协作，勾连紧密。

常见安全隐患-勒索病毒邮件

目 录

科研工作与信息安全

病毒传播

中国教育和科研计算机网ERNET网络中心统计，2017年5月12日-14日在近1600个高校用户中，确认感染病毒的高校66所，占比4%，涉及数百个IP地址，致使许多实验室数据和毕业设计被锁。

勒索软件攻击在2020年中断了1,681所学校、学院和大学的学习，今年到目前为止至少发生了544例。

科研工作与信息安全

数据泄露

1、由于恶意攻击者攻击导致的窃密

2、由于内部人员有意或无意导致泄密

3、由于数据维护及处置不当导致失密

在商业活动中，数据关乎巨大的经济利益
在科研活动中，数据可能涉及个人前途，甚至国家机密

科研工作中影响信息安全的因素

技术因素

主要原因是多数实验室属于局域网，不具有网络攻击防护技术措施。

- 1. 计算机系统存在漏洞，是病毒快速传播的基础；
- 2. 办公电脑未安装防病毒软件，或病毒库未及时更新；
- 3. 数据未进行异地备份，导致数据丢失后无法恢复；
- 4. 接入交换机安全配置不合规，无法防止病毒扩散；
- 5. 缺少数据防泄漏设备与机制，无法及时发现数据被泄露。

科研工作中影响信息安全的因素

人为因素

主要原因是科研人员保密意识薄弱，防范意识不强。

- 1. 科研资料保管失控，个人电脑科研档案加密不严；
- 2. 电子信箱信件交往失误；
- 3. 学术会议交流、学术报告、讲课讲出属于保密的重要科研内容；
- 4. 论文投稿科研成果被窃取，被审稿者、编辑者窃取最多；
- 5. 科研项目基金申请，科研内容被暴露或窃取；
- 6. 科研信息网络搜索、数据库信息检索活动被跟踪分析、监控；
- 7. 被科研情报间谍跟踪；
- 8. 在办公室电脑上访问非正规网站，或使用破解版软件；
- 9. 对陌生邮件不加识别，打开可疑附件或链接
- 等等

科研活动中如何保证信息安全

如何做

- **绝大多数科研泄密是无意的，保密意识是数据防泄漏的关键因素。**

  与科研同行交流、论文投稿、信息检索等活动必须谨慎，应有保密意识和防范办法。

  特别是国内外原创性科研项目和科研成果必须绝对保密。

- 办公电脑
- 与科研同行交流、论文投稿、信息检索等活动必须谨慎，应有保密意识和防范办法。
- 特别是国内外原创性科研项目和科研成果必须绝对保密。

日常工作的规范建议

- 终端安全
- 账户和密码安全
- BYOD移动设备及存储介质安全
- 网络安全
- IT应用与工具安全
- 会议安全
- 个人信息保护

终端安全-设备使用

设备使用 → 合理使用机构配发的办公设备

如何做

- 谨防信息泄露，不随意刻录保密信息
- 计算机屏幕定期锁定，离开工位前一定要锁屏
- 不随意将工作电脑用于非工作用途，或随意借给他人使用
- 不私自拆卸和向外部送修设备

案例：技术服务部某员工违规将便携机借给合作方员工使用，合作方员工利用上班时间用QQ传递工作所需文件；并且未经审批在机房使用移动存储设备给用户拷贝用户文档或版本文件；

分析：便携机上保存的很多工作文档，自己可能司空见惯，觉得没什么大不了，可是其他人拿到就不一定了

终端安全-病毒防范

恶意代码防范 → 安装防病毒软件并按要求进行更新

如何做

- 安装机构统一的杀毒软件，升级杀毒软件的病毒特征库
- 不访问不良网站，不下载来历不明电子邮件
- 移动存储介质拷贝文件需谨慎，不双击打开移动存储介质
- 不安装机构明令禁止的软件（见管理规定附录二）

案例：长时间未使用的服务器开机，或长期出差员工的笔记本电脑接入机构网络，其病毒特征库升级前直接使用，都可能带来严重的安全隐患

终端安全-软件安装控制

软件安装控制 → 不根据个人喜好随意安装工作无关软件

如何做

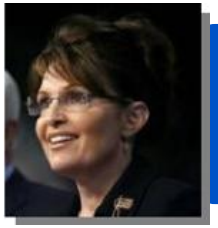
- 使用信息技术部门统一提供的办公软件处理工作
- 不在未批准的情况下，随意安装盗版和来路不明软件
- 不随意卸载和修改机构统一安装的控制管理软件和防病毒软件
- 不在未批准的情况下，自行安装多操作系统和虚拟机

账户和密码安全

密码安全 → 删除不必要的用户，按照要求设置强壮的密码

如何做

- 无论是工控系统还是个人电脑，删除不必要的账户（如供应商默认账户等）、禁用guest账户
- 不使用用户名（账号）、生日、单词等作为密码
- 不要将密码写在纸上，不将密码存储于电脑文件中
- 定期修改密码，不把密码告诉任何人
- 不同的账户尽可能不使用相同的用户名和密码
- 密码找回问题不要使用公开信息



2008年美共和党副总统候选人莎拉·佩林的邮箱被黑客入侵，正是通过答出他的安全问题（我的生日，首次遇到丈夫的地方）直接获得了邮箱密码

账户和密码安全

密码设置 → 设置强壮和易于记忆的密码，设置安全的找回问题

如何做

- 什么样的密码是强壮的？

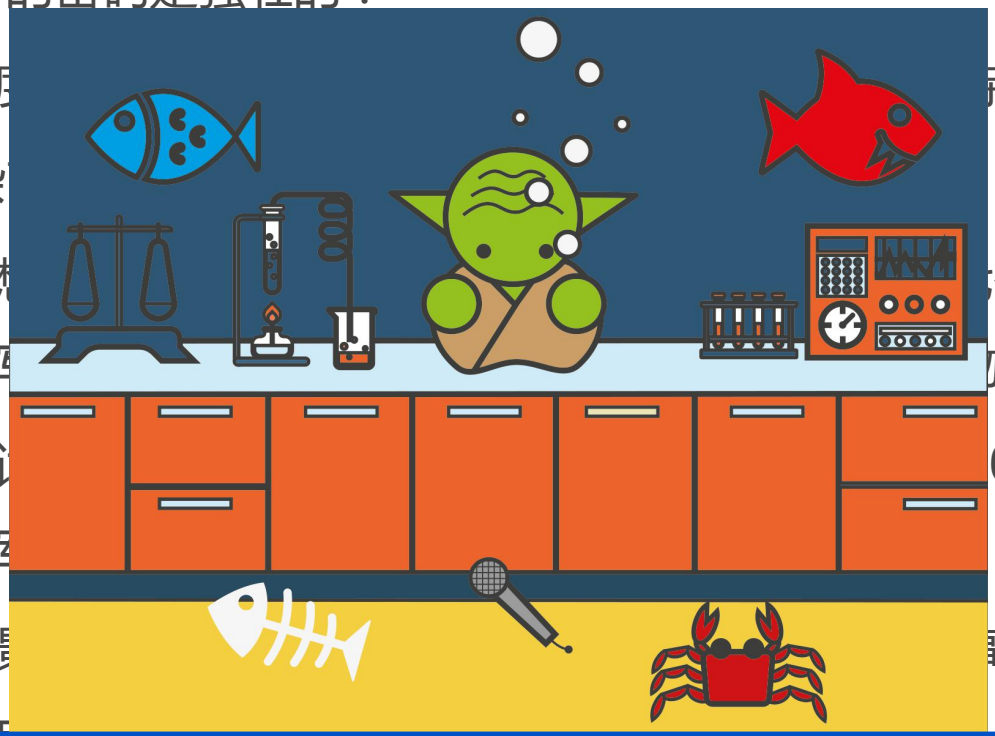
  长度 … 特殊字符

- 太复杂

  ✓ 联想 … 夕，每次

  ✓ 诗词 … 0ng = 将军

  ✓ 场景 … 再把它变



Master Yoda and two fish in a lab = MY&2f@lab

BYOD可移动设备及介质安全

可移动设备和存储介质安全

可移动设备及介质（U盘等）的不规范使用往往会引起设备或信息丢失、感染病毒等安全事件。

如何做

- 保障物理设备安全，不随意放置在不安全的地方，定期接入机构网络以获得安全更新（笔记本电脑等）
- 设置一定复杂度的密码或PIN码（如果可以设置的话）
- 只使用机构制定USB设别，不“破解” “越狱”机构配发设备
- 养成用完移动介质要彻底删除的习惯，个人USB移动介质坚决不能随便插入工控系统
- 移动介质使用前进行查杀病毒，一定要安装防病毒软件

网络安全-上网安全

上网安全

访问互联网资源同时也存在安全风险，不应访问与工作无关的网络资源

如何做

- 机构网络属于公共资源，上班时间应仅用于工作用途
- 禁止修改浏览器默认安全选项
- 在没有安装防病毒软件的情况下不应上网，互联网上下载的文件应先扫描病毒后使用
- 通过互联网传输敏感信息和文件时，应使用加密的方式
- 不通过外部邮箱和网盘传播机构的保密信息（秘密级以上）
- 不随意下载网站上提供的免费软件

网络安全-信息发布

信息发布

不浏览可能包含恶意内容的站点

不发布可能影响机构形象和业务的言论

如何做

- 不要随意浏览色情、暴力、赌博等网站或参与相关话题
- 不参与涉及政治、宗教、种族的敏感话题
- 不发布与散播有关机构的不良言论
- 不私自发布机构的非公开信息到互联网上

IT应用与工具安全-邮件安全

邮件安全

应使用机构电子邮件系统，遵循必要的操作规范，避免由此带来的安全问题

如何做

- 员工不应使用公共电子邮箱处理公务
- 发邮件时注意收件人是否合适，特别是前文历史和附件是否必须
- 收邮件时注意收件人是否正确，不打开可疑的链接和附件
- 谨慎使用回复所有人，须确保所有收件者能够知悉信息
- 向外部发送邮件时应，应告知对方对邮件内容的保密义务
- 含有保密信息的附件须进行加密，包括但不限于WinRAR等手段，密码通过电话、短信等其他渠道告知收件人

IT应用与工具安全-即时通讯安全

即时通讯

区分个人即时通讯软件和办公即时通讯软件

如何做

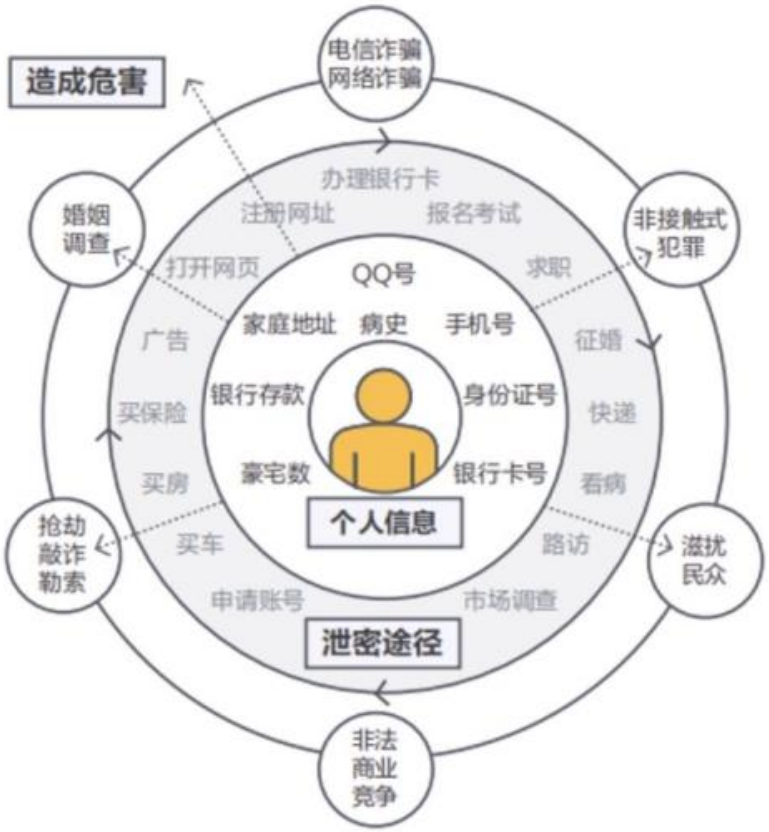
- 尽可能使用企业微信进行办公和内部沟通
- 必须使用个人微信进行工作沟通时，应特别注意群组的使用，确认群组成员身份是否工作相关
- 其他法律规定的群主合规义务

私人事务

机构业务

个人信息保护

如何做



个人隐私

密码安全

APP权限

刷脸数据

物联网设备

手机丢失

安全意识的培养

明白信息安全的重要性，并在面对新的挑战、业务工作时，主动思考安全问题。

-----安全冲突与备案

虽然我不是专业人员，但我知道出现安全事件后，寻求专业帮助的重要性和必要性。

-----安全事件的处置

安全意识的培养-事件上报

事件上报

信息安全事件的及时上报问题，可有效防止重大信息安全事件的发生

如何做

- 遵守信息安全管理的规章制度
- 加强办公安全意识培训，破除“家丑不可外扬”的思维方式，形成“早发现、早报告”的习惯
- 了解专门的上报渠道
- 加强与信息安全部门的沟通


Q&A

Thanks.

网络安全知识小课堂