



信息安全意识培训

制造和数字化中心
二零二一年十月

1. 信息安全背景和政策介绍
2. 华谊集团网络安全现状
3. 个人信息安全建议

- 1. 信息安全背景和政策介绍**
- 2. 华谊集团网络安全现状**
- 3. 个人信息安全建议**

什么是信息安全

广义上讲

- 领域 —— 涉及到网络信息的保密性，完整性，可用性的相关技术和理论

本质上

- 保护 —— 网络系统的硬件、软件、数据
- 防止 —— 系统和数据遭受破坏，更改，泄露
- 保证 —— 系统连续可靠正常地运行，服务不中断

两个层面

- 技术层面 —— 防止非授权用户的非法入侵
- 管理层面 —— 内部员工的教育和管理

信息安全的目标

保密性

完整性

可用性

C

confidentiality

I

integrity

A

availability



网络安全和信息安全的区别

网络安全(Cybersecurity)是网络空间安全的简称

2016年12月，由国家网络安全和信息化工作办公室发表的《国家网络空间安全战略》提出

The screenshot shows the homepage of the Office of the Central Cyberspace Affairs Commission. The header features the Chinese Communist Party emblem and the text '中共中央网络安全和信息化委员会办公室' (Office of the Central Cyberspace Affairs Commission) in English below it. The URL 'WWW.CAC.GOV.CN' is visible. The main content area is titled '《国家网络空间安全战略》全文' (Full Text of the National Network Space Security Strategy). Below the title, the date '2016年12月27日 11:23:00' and source '中国网信网' are listed. There are also links for printing and sharing. The text of the strategy begins with a paragraph about the importance of network security.

战略指出：

网络空间已经成为与陆地、海洋、天空、太空同等重要的
人类活动新领域，国家主权拓展延伸到网络空间，网络空
间主权成为国家主权的重要组成部分。



网络安全和信息安全的关系

网络空间成为大国博弈的虚拟空间，呈现军事化趋势



国家网络空间安全保障体系

《国家安全法》

《数据安全法》

《网络安全法》

《个人信息保护法》

法律法规政策体系

战略	密码	数据安全	网络安全审查	个人信息/数据出境	互联网信息安全						应急	培训/教育	关于加强网络安全学科建设和人才培养的意见				
国家网络空间国际合作战略	网络安全国际战略合作	密码法	数据安全管理办法（征求意见稿）	网络安全审查办法	个人信息和重要数据出境安全评估办法（征求意见稿）	互联网信息服务管理规定	互联网新闻信息服务许可管理实施细则	互联网跟帖评论服务管理规定	互联网论坛社区服务管理规定	互联网群组信息服务管理规定	互联网新闻信息服务新技术新应用安全评估管理办法	具有舆论属性或社会动员能力的互联网信息服务安全评估规定	移动互联网应用程序信息服务管理规定	互联网信息搜索服务管理规定	金融信息服务管理规定 区块链信息服务管理规定 互联网直播服务管理规定 微博客信息服务管理规定	国家网络安全事件应急预案	一流网络安全学院建设示范项目管理办法

《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见（公网安[2020]1960号）》

《中华人民共和国关键信息基础设施安全保护条例（国务院令 第745）》

网络安全等级保护制度体系

《国家信息化领导小组关于加强信息安全保障工作的意见(中办发[2003]27号)》

《中华人民共和国计算机信息系统安全保护条例（国务院令 第147号）》

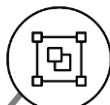
安全技术标准体系

国家推行《网络安全法》，实行信息安全“一把手”负责制

信息安全的管理水平关系到国家稳定、**关系到国企和央企领导者的管理能力评价**，新的网安法对关键信息基础设施和个人信息保护有明确要求，违反法律的企业其企业领导者的前途将受到直接影响

1. 网络运行安全

- 一般网络运营者安全保护义务
- 关键信息基础设施网络运营者安全保护义务
- 网络安全事件应急预案



2. 个人信息保护

- 个人权利
- 个人信息保护要求
- 投诉、举报处理机制



3. 监管机构互动

- 安全评估监测
- 安全事件上报
- 参与应急演练

网络安全法



国务院国有资产监督管理委员会办公厅文件

国资厅发综合〔2017〕33号

关于进一步加强中央企业网络安全工作的通知



“通知”的几项重点内容回顾

“通知”共提到8项工作，包括：充分认识网络安全工作的重要性、开展网安法宣传教育、强化关键信息基础设施保护、加强网络安全自查和风险防范、提高安全态势感知和预警处置能力、做好重大会议活动期间网络安全保障、增强企业间合作共享、加强领导和组织落实。**其中明确要求了央企是网络安全责任主体，要建立“一把手”负责制，层层落实推进网络安全工作。**

公安机关对网络违法犯罪案件实行“一案双查”

公安机关已实行“一案双查”制度，即在对网络违法犯罪案件开展侦查调查工作时，同步启动对涉案网络运营者法定网络安全义务履行情况的监督检查。对拒不履行法定网络安全义务、为网络违法犯罪活动提供帮助的网络服务提供者，公安机关将依法对其进行严厉查处。



层出不穷的客户信息泄露，伤害企业信誉同时带来社会安全隐患

近几年发生的大信息泄露事件：

- 网易、CSDN、天涯等国内知名网站的用户个人信息泄露，规模达上亿用户；
- 携程的用户和信用卡支付信息泄露；
- 中国人寿广东10万份保单或遭泄露；
- 数千万社保用户敏感信息或遭泄露；
- 20万儿童信息被打包出售，信息精确到家庭门牌号；
- 凯悦连锁酒店超过50%遭到恶意软件入侵，或泄露大量客户信息；
- MySpace 4.27亿数据泄漏，成互联网史上最大规模的泄露事件；
- 准大学生徐玉玉个人信息泄露，遭遇电信诈骗被骗光学费死亡，该事件是促成网安法对于个人信息保护要求的重要催化剂；
- 京东12G的数据包开始在黑市流通



发生数据泄露的行业



工控问题层出不穷

- 2010年, Stuxnet 病毒针对性的入侵ICS 系统, 严重威胁到伊朗布什尔核电站核反应堆的安全运营
- 2012年, 两座美国电厂遭USB病毒攻击, 感染了每个工厂的工控系统, 可被窃取数据
- 2015年, 攻击者使用附带有恶意代码的Excel邮件附件渗透了乌克兰电网工作站人员系统, 向电网网络植入了BlackEnergy恶意软件, 获得对发电系统的远程接入和控制能力。
- 2011年, 大庆石油厂装置控制系统感染Conficker蠕虫病毒等造成控制系统服务器与控制器通讯不同程度地中断
- 2014年6月, “蜻蜓组织” 利用恶意程序Havex(与震网类似), 对欧、美地区的一千多家能源企业进行了攻击
- 2016年10月17日, 工业和信息化部印发《工业控制系统信息安全防护指南》



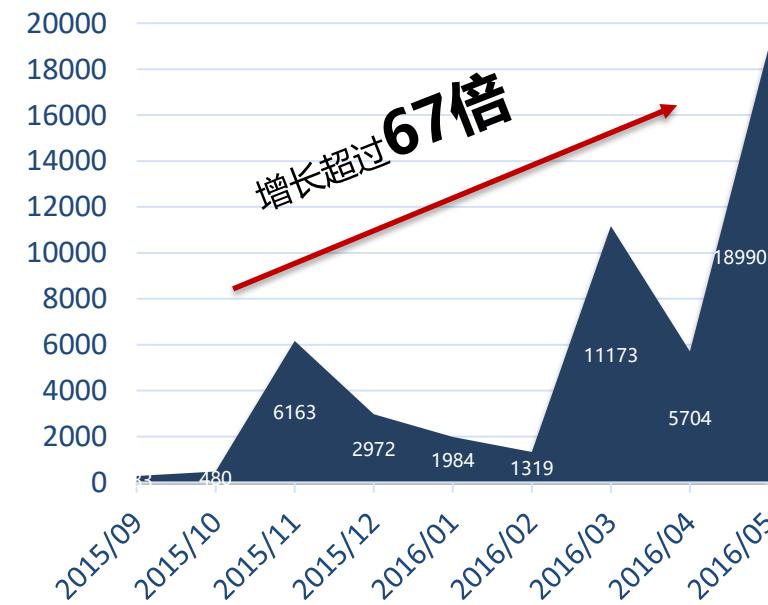
勒索软件

勒索软件 (ransomware) 是一种流行的木马，通过骚扰、恐吓甚至采用绑架用户文件等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。勒索软件已经从过去的可以忽略不计，增长到如今的数以万记，通过网页链接(URL)检测的勒索软件数量从283个增长到18990个，增长超过67倍。
勒索软件已成为一种新型商业犯罪模式。

Wannacry勒索软件中毒后画面



勒索软件病毒增长趋势



黑客产业化

地下黑市可以买到的各种信息和服务：



一些当前在暗网中正在出售的企业敏感数据...

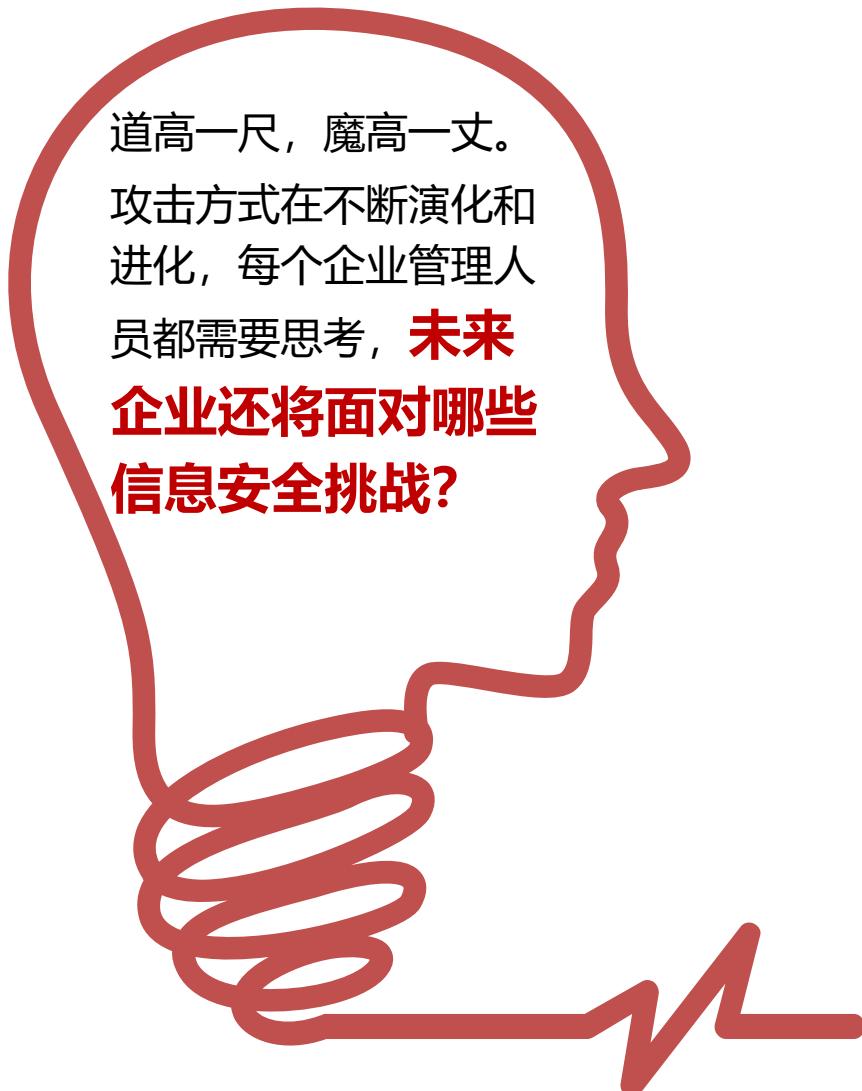
The screenshot shows a forum post titled "1500条平安车险回访电话录音数据" (1500平安车险回访电话录音数据) by MarianaTrench. The post includes a screenshot of a file explorer window showing a list of files, one of which is a musical note icon labeled "15261140132". Below the file list is a small image of a pingan.png file.

Another post titled "北京银行会员26万余条低价处理" (Beijing Bank members 260,000 at low price) by YUHONG shows a list of names and addresses, such as Wang Hui, Wang Ming, Wang Jinming, etc., from Beijing SunTrust Bank.

A third post titled "Hacked SunTrust Bank Logins 10 000 \$" shows a list of hacked accounts with details like "Price: \$ 180 / 0.046169 BTC / 3.196634 LTC / 3.596073 XMR / 1.342112 ETH".

The bottom part of the screenshot shows a user profile for "smart666tiger" with a level of 8 and a rating of 27.60%.

攻击面扩大化，各式攻击层出不穷



- 1. 信息安全背景和政策介绍**
- 2. 华谊集团网络安全现状**
- 3. 个人信息安全建议**

华谊集团网络安全意识调查结果展示



7月26日至7月30日，项目团队对2家一级公司和23家二级公司领导和员工进行了人员安全意识调查，共1251人参与调研，部分结果展示：

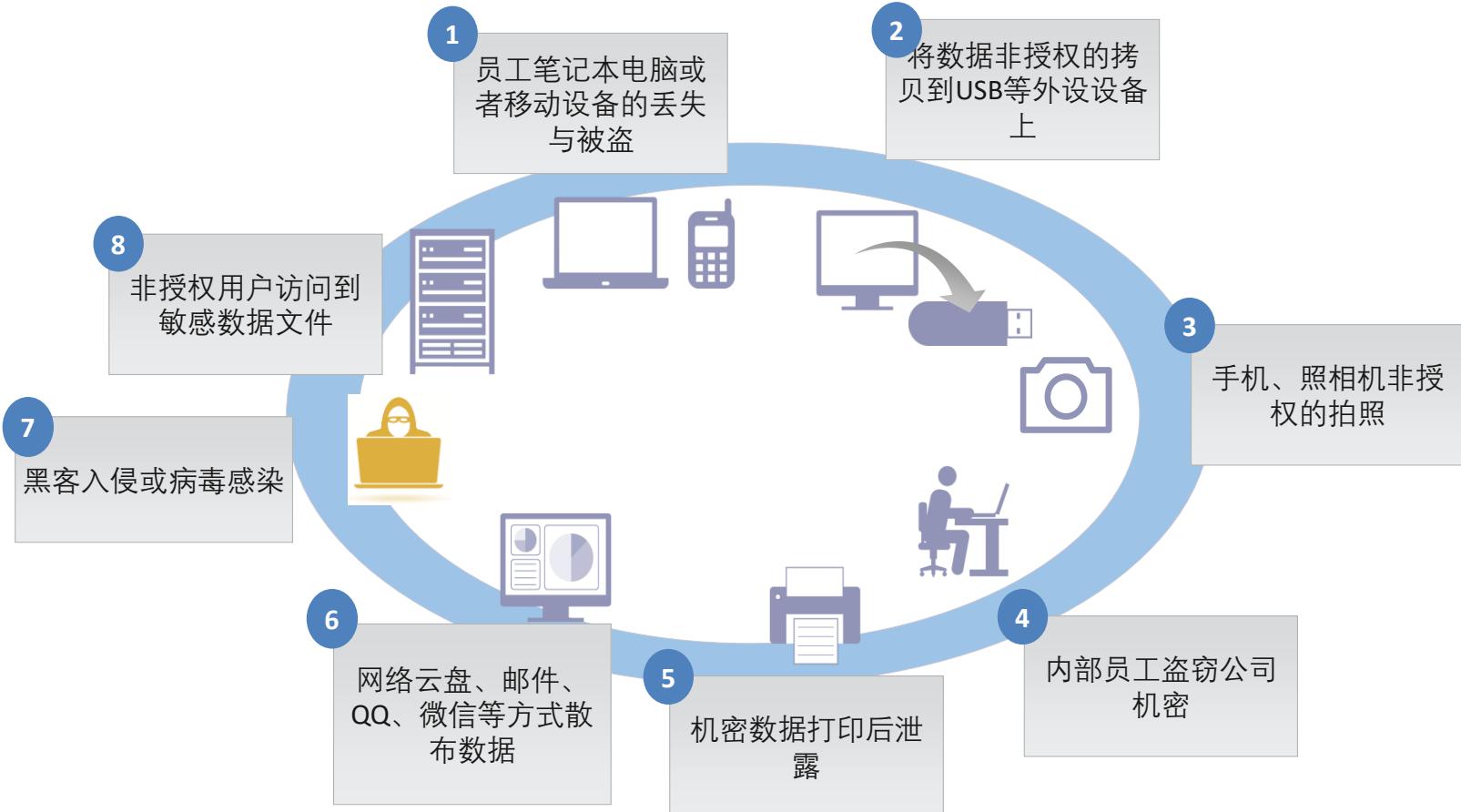
(一) 最突出的3个问题：

- 仅**55.47%**的参与调研人员表示了解集团/公司的网络安全及信息安全的管理规定；
- 76.58%**的参与人员表示曾使用个人电子邮件、个人社交媒体发送或接收公司信息；
- 9.75%**的参与人员表示曾在网络上发布公司的敏感信息

(二) 员工针对网络安全提出最多的4项建议：

- 建议加强网络安全知识宣传，安排相关培训，并发布标准化可操作的指导书；
- 建议加强对终端设备和信息传输管控，如禁止使用U盘、个人微信传输公司信息；
- 建议统一安装正版办公软件、正版杀毒软件；
- 建议制定企业邮箱反垃圾策略，增强垃圾邮件的过滤能力

华谊集团数据泄露的8大场景及应对措施



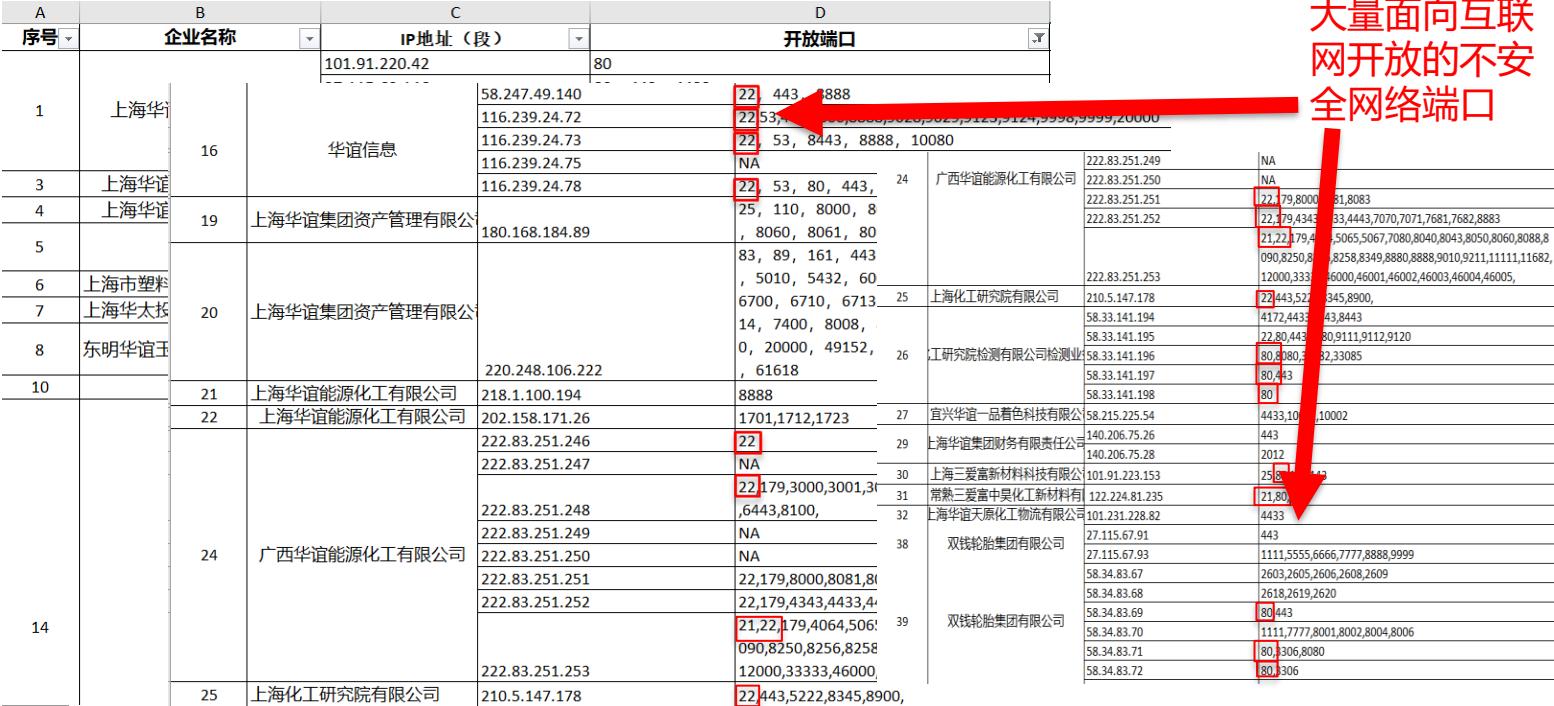
应对措施

- | 序号 | 应对措施 |
|----|---|
| 1 | <ul style="list-style-type: none">设置开机密码，密码有复杂度要求BitLocker，防止电脑被破解磁盘加密 |
| 2 | <ul style="list-style-type: none">重要数据的终端禁用USB接口部署终端安全系统 |
| 3 | <ul style="list-style-type: none">重要区域禁止携带拍照设备数字水印技术重要区域部署行为分析摄像机 |
| 4 | <ul style="list-style-type: none">保密协议，竞业协议安全合规意识宣贯闭路电视用户和实体行为分析 |
| 5 | <ul style="list-style-type: none">数字水印碎纸机 |
| 6 | <ul style="list-style-type: none">部署终端安全系统部署数据防泄漏系统 |
| 7 | <ul style="list-style-type: none">边界防护：如防火墙，入侵防御，WAF安装杀毒软件及时更新补丁和病毒库数据备份 |
| 8 | <ul style="list-style-type: none">网络安全准入最小权限分配安全审计定期账号梳理统一身份管理 |

案例1

控制域	风险描述	对应弱点	风险级别
A.17	华谊下级公司暂未落实和实施工业控制系统的网络安全应急预案	缺乏工控安全应急预案	高
示意图		造成影响	
<p>《华谊集团工业控制系统网络安全管理办法(更新V1.1)》内容涉及工控安全应急预案、工业事故管理和处置条例。根据访谈得知目前钦州生产基地、上海新材料公司尚未执行工控安全应急演练及员工的工控安全培训</p>		未落实和实施工业控制系统安全事件应急演练，和事件响应者应对工业控制系统特定情况的培训，将导致意外发生时无法及时有效处理安全事件，削弱系统防御力，增加总体成本。	
<p>访谈纪要</p> <p>时间: 2021年7月20日 14: 00 - 15: 00 上海新材料访谈对象: 祚董、张总、王经理、黄经理、徐经理 参会人员: 智造中心: 张一民; 德勤: 李啸、唐瑞擎、吴明瑾</p> <p>1. 安全事件及应急演练 1) 是否有网络运行状态及员工上网行为管理设备, 定期检查是否存在异常用户行为? • 公司定期巡检员工的上网行为 2) 本公司是否会定期开展针对信息安全相关的应急演练, 如网络攻击、计算机病毒等? • 没有信息安全和工控安全相关的应急演练 • 重大化工危险源的实时监控将传至集团应急管理处和上海应急管理处</p> <p>2. 员工安全意识培训 3) 请介绍本公司是否会对于员工进行定期信息安全意识培训? 如: 员工入职培训是否包含信息安全培训? 是否有信息安全相关的激励机制和惩处措施? • 每年将参加国资委组织的网络信息安全培训, 培训文档在内部传阅 • 现阶段没有对专业信息化人员进行信息安全培训, 缺少培训管理制度, 集团计划于下半年制定信息安全考试题目, 发布至各单位组织进行信息安全知识考核 • 工控系统的操作培训: 工控系统的终端主机具有物理封锁; 工程师定期到厂商做专业仪器培训; 但是公司内部目前没有完善的培训系统, 未来将使用专业的培训指标、和考核记录, 逐年形成经验总结并保存。</p>		<p>管理办法</p> <p>时间: 2021年7月21日 15: 00 - 17: 00 广西能化访谈对象: 孟总、顾经理、叶经理、林经理、李经理、白仪院: 刘慧芳 参会人员: 智造中心: 张一民; 德勤: 李啸、唐瑞擎、吴明瑾</p> <p>1. 安全事件及应急演练 1) 本公司是否会定期开展针对信息安全相关的应急演练, 如网络攻击、计算机病毒等? • 没有信息 (工控) 安全相关的应急演练, 未配置安全负责人</p> <p>2. 员工安全意识培训 2) 请介绍本公司是否会对于员工进行定期信息安全意识培训? 如: 员工入职培训是否会包含信息安全培训? 是否有信息安全相关的激励机制和惩处措施? • 现阶段没有对专业的信息化人员进行信息安全培训, 本公司具有培训管理制度但是待完善</p> <p>第十二条 远程访问安全 1. 禁止工业控制系统面向其他网络开通 HTTP、FTP、Telent 等高风险通用网络服务。 2. 禁止通过远程访问方式操作工业控制系统。 3. 保留并定期备份工业控制系统的相关访问日志, 对操作过程进行安全审计, 通过审计账户登录、访问时间、操作内容等日志信息, 追踪并定位非授权的访问行为。</p> <p>第十三条 安全监测和应急预案演练 1. 应在工业控制网络设置网络安全监测设备, 及时发现、报告并处理网络攻击或异常行为, 监测行为应不影响工业控制系统原有正常应用功能。 2. 企业应制定工控安全事件应急预案, 当遭受安全威胁导致工业控制系统出现异常或故障时, 应立即采取紧急防护措施, 防止事态扩大, 并第一时间上报集团制造和数字化中心。 3. 企业应定期组织工业控制系统操作、维护、管理等相关单位人员开展工控安全事件应急预案演练。</p> <p>第十七条 日常检查、事故事件管理与处置 集团制造和数字化中心组织对各单位工业控制系统网络安全防护工作进行日常检查考核, 各公司一旦发生工控安全事件, 应在事件发生三十分钟内上报集团制造和数字化中心, 并按照应急预案开展先期处置。信息公司工控安全专业团队应积极协助企业开展工控安全事件处置。</p>	
<p>初步建议</p> <p>建议各生产基地落实对工业控制系统的应急演练, 定期对应急响应预案进行修订</p>			

案例2

控制域	风险描述	对应弱点	风险级别
A.12	针对华谊的公网IP地址进行了端口扫描，发现大量面向互联网开放的不安全的网络端口	缺乏技术脆弱性管理	高
现状示意图		造成影响	
 <p>大量的不安全端口，如20,21,22,23,80等开放或不正确配置和加固，容易暴露一部分高中危甚至是严重的漏洞，导致系统遭受黑客攻击、病毒入侵等威胁。</p>		初步建议	
<p>建议设立面向互联网端口的安全标准，逐步梳理和关闭不安全网络端口。</p>			

案例3

控制域	风险描述	对应弱点	风险级别
A.18	根据调研，当前网络日志存储未满足180天的要求	安全审计	高
示意图		造成影响	
 <p>全国人民代表大会常务委员会公报版 中华人民共和国网络安全法 中国民主法制出版社</p>		 <p>第二十一条：采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月</p> <p>最佳实践：部署集约化管理的中央日志服务器，统一存储网络日志，避免日志受未预期的删除，未来还可以联动大数据平台进行数据分析</p>	

案例4

控制域	风险描述	对应弱点	风险级别
A.12	据调研, 当前针对恶意代码缺乏从设备终端、重要网络区域到恶意软件监控的安全纵深防御	缺乏恶意软件的管控	高
示意图		造成影响	
<ul style="list-style-type: none">部分单位终端未安装杀毒软件较多单位安装的是免费版杀毒软件 <ul style="list-style-type: none">未在重要网络环境部署防病毒设备 <ul style="list-style-type: none">无恶意软件的统一管理系统, 无法及时追踪和监控终端设备与网络环境的杀毒状态和效果		<p>若未能及时安装防恶意代码软件和安装最新的安全补丁, 容易造成恶意软件入侵, 感染传播病毒。</p>	
		初步建议	
		建议建立防病毒和防恶意软件入侵管理机制, 对办公系统、工业控制系统及临时接入的设备采取病毒查杀等安全预防措施。	

案例5

控制域	风险描述	对应弱点	风险级别
A.9	办公网络有线、无线网络缺少企业级安全准入	缺乏访问控制管理	高
示意图		造成影响	
		<ul style="list-style-type: none">1. 攻击者将可以轻松进入华谊内部网络实施网络攻击2. 一旦发生网络事件，将无法追溯定位到操作用户3. 无法根据用户角色分配网络权限和资源。	
		<p>初步建议</p> <p>梳理办公网络访问控制策略，从集团到二级公司和生产基地，逐步开展企业级安全准入控制。</p>	

信息安全管理抓手和关键点



- | | |
|--|---|
| <p>01 网络安全组织落实
确定安全负责人或接口人</p> <p>03 安全管理制度
根据集团要求和业务特征制定
安全管理制度</p> <p>05 前置安全需求
在项目建设前期明确安全需求，
规划方案报审集团</p> <p>07 厘清保护重点
盘点组织的敏感和重要数据</p> <p>09 差距与整改
配合集团安全评估工作和积极整改</p> | <p>02 安全意识和培训
定期参加和组织培训</p> <p>04 安全事件和应急预案
制定安全事件相应流程和应急预案</p> <p>06 暴露面管理
非必要网络端口禁止开放在互联
网上</p> <p>08 统一部署
贯彻集团“一张网，一朵云，
一个平台”要求</p> <p>10 沟通和协作
和集团以及兄弟单位定期组织
安全主题的沟通交流会议</p> |
|--|---|

1. 信息安全背景和政策介绍
2. 华谊集团网络安全现状
3. 个人信息安全建议



怎样才能保护自己的隐私？

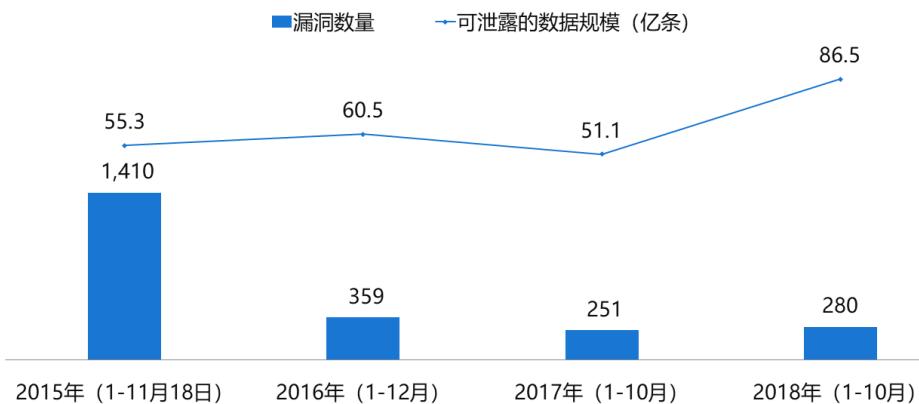
信息泄露-1

Facebook事件

2018年3月，剑桥分析公司获得Facebook个人数据超过8700万

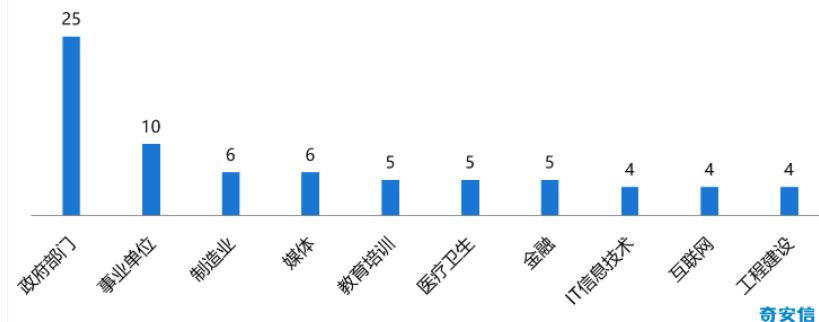


2015-2018年网站漏洞可导致数据泄露情况对比

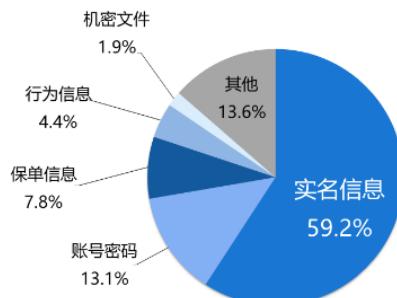


奇安信
新一代网络安全

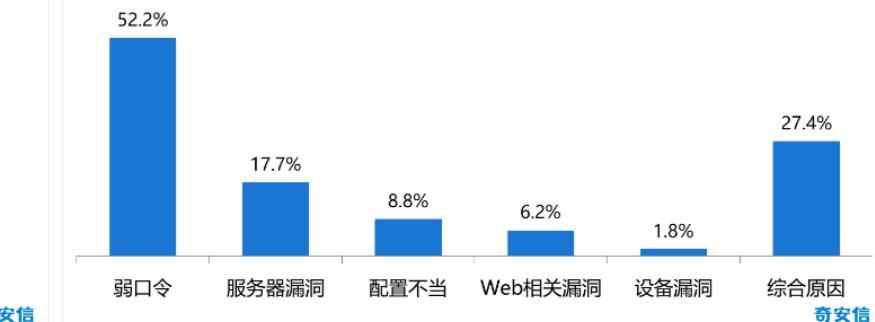
2018年奇安信安服团队处置数据泄露事件的行业分布



2018年全球重大数据泄露事件泄露数据的类型分布



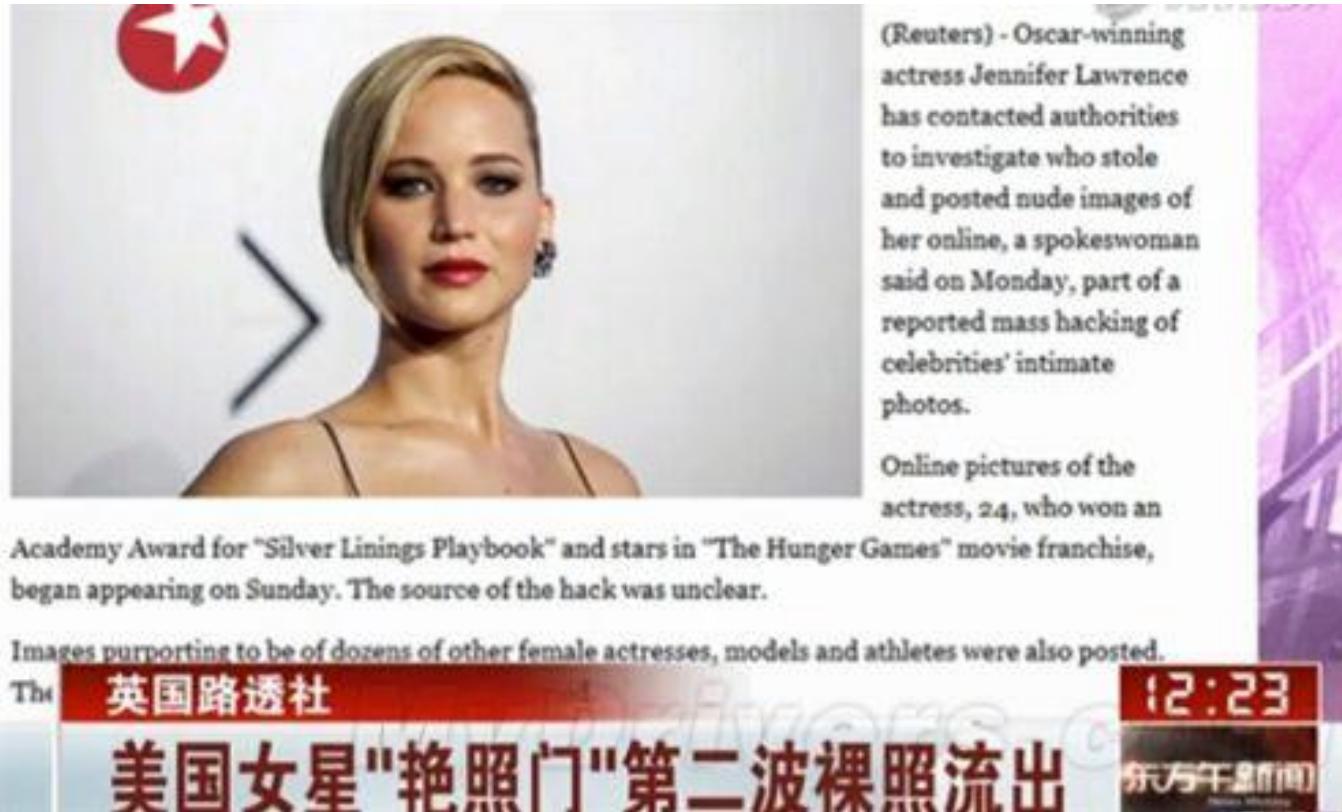
2018年政企机构遭受数据泄露的主要原因



奇安信
新一代网络安全

信息泄露-2

云空间的漏洞：苹果iCloud漏洞事件



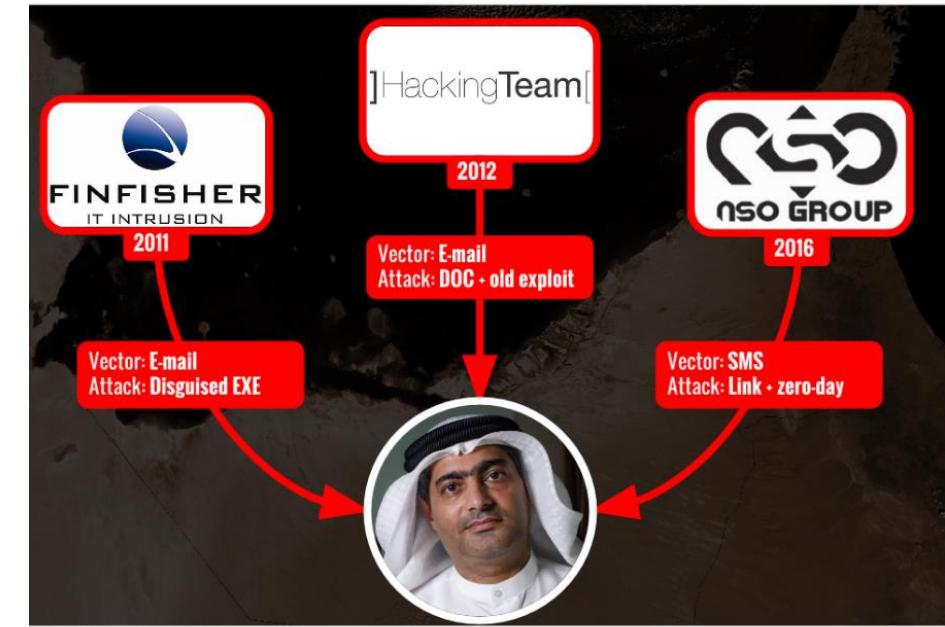
iOS三叉戟漏洞



NSO
以色列



THREE "LAWFUL INTERCEPT" PRODUCTS USED AGAINST MANSOOR



CITIZEN LAB 2016
安全智 (Dotzoo.com)

信息泄露之内部盗窃



远超斯诺登事件 CIA大规模数据泄露



T-Mobile员工盗卖户数据



京东数据泄露内鬼被抓 涉案50亿条公民信息泄露



英国超市莫里森遭遇内部攻击



上海疾控中心员工
贩卖新生儿信息



零售巨头遭遇上亿数据泄露



中航信陷旅客信息泄露漩涡



eBay发生1.28亿用户数据泄露事件

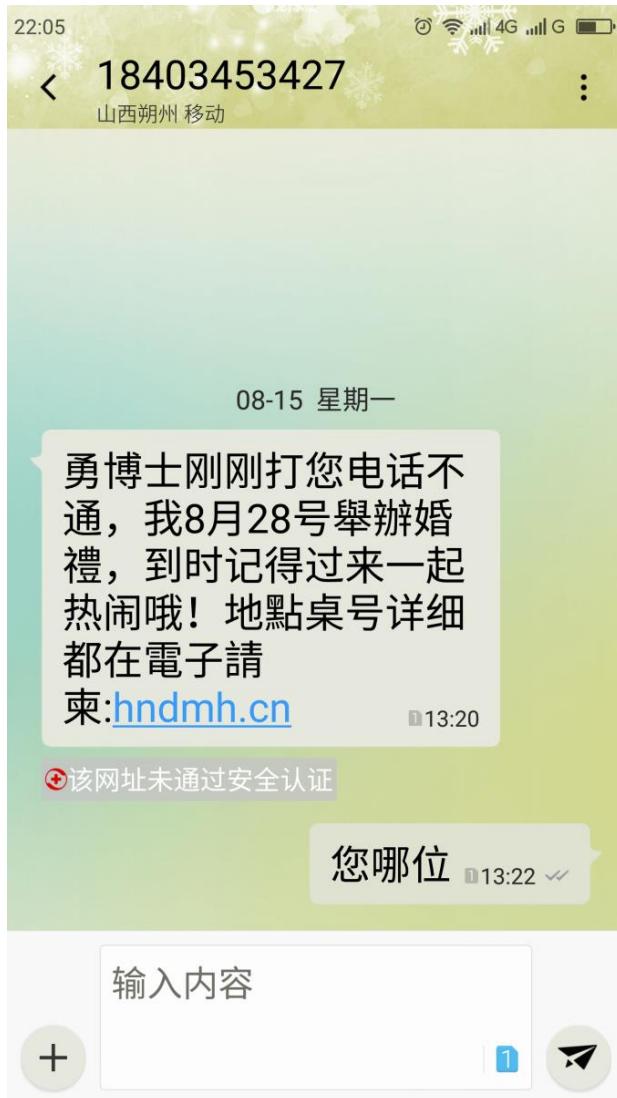


内部威胁代名词 斯诺登事件

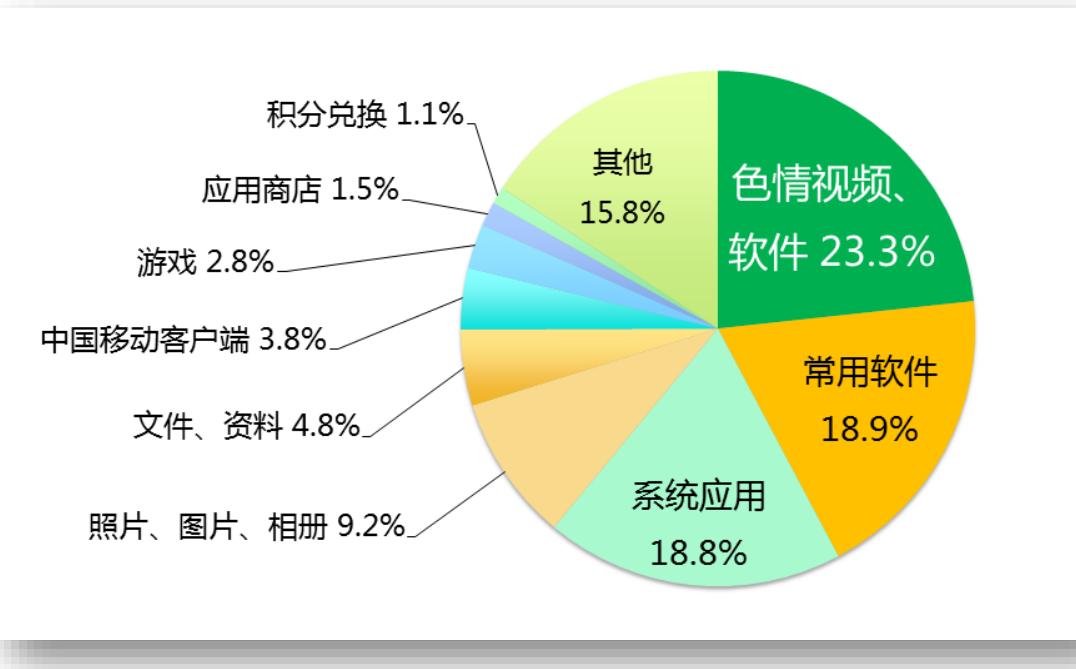


软件商泄露280家企业客户的雇员信息

信息泄露之窃密木马



信息种类	人均手机信息存储量	中毒后手机信息窃取率	年度恶意程序感染量评估	个人信息年度窃取量评估
联系人	385条	100%	31.1万×12	14.4亿条
短信	586条	90%	113.4万×12	71.8亿条
通话记录	986条	100%	43.5万×12	51.5亿条
照片	195张	100%	1077×12	252.0万张



信息泄露之钓鱼窃取



结论

普通人完全不具备保护自己个人信息的能力，包括技术能力和法律能力。

安全意识的提升在隐私保护方面的作用微乎其微。

首先“**假定**”自己的个人信息一定会泄露，且一定已经泄露，在此基础上再考虑怎样防骗，怎样保护自己。



黑客怎样猜中我们的口令？

口令和密码的区别

根据10月26日通过的《中华人民共和国密码法》规定：密码是指采用特定**变换**的方法对信息等进行**加密保护、安全认证**的技术、产品和服务。

虽然人脸、指纹本身不是密码，但网络系统为了防止信息泄露，在传输和存储这些“**口令**”信息时所使用的加密和认证技术就是密码了。

密码的技术分类

对称密码

非对称密码

杂凑函数

密码的法律分类

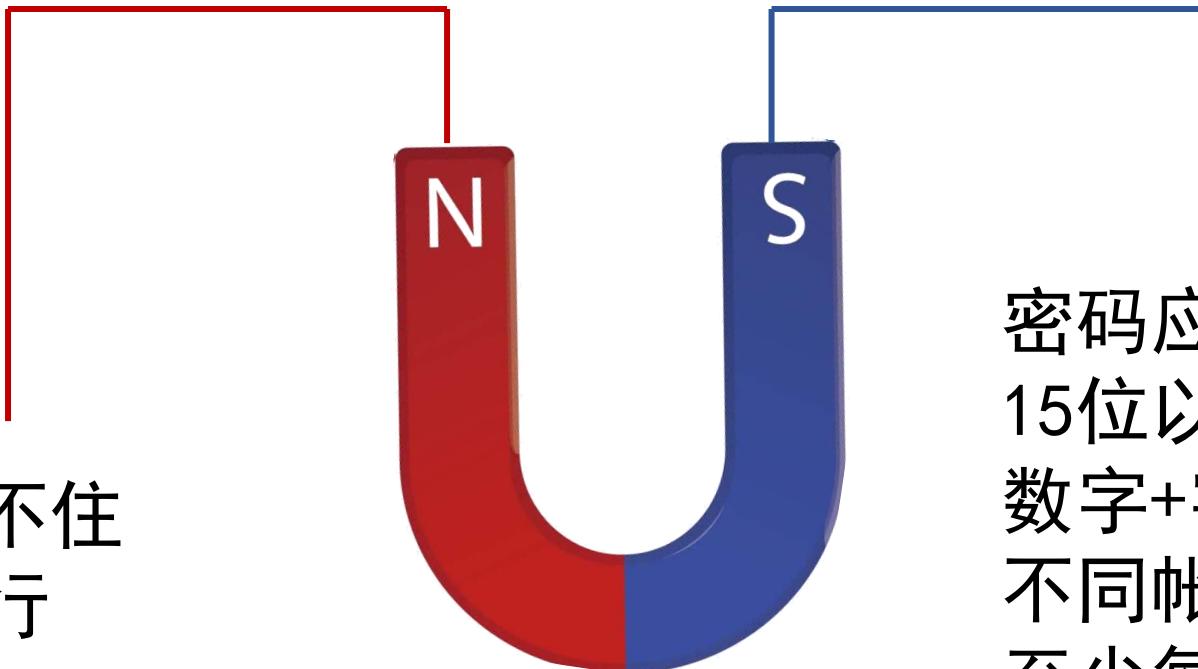
核心密码

普通密码

商用密码

关于口令设置的两个极端

太复杂了记不住
简单好记就行



密码应为随机数
15位以上
数字+字母+特殊符号
不同帐号用不同口令
至少每三个月换一次

四大法宝破解弱口令

暴力破解法

把密码所有可能的排列组合都试验一遍。用现代计算机手段，15位的纯数字密码，暴力破解只需0点几秒。

流行弱密码

世界上最流行的100个密码，可以登录全球70%的上网账户。

以下都是弱密码：123456、password、woaini1314-流行语）、!qaz@wsx-键盘组合



生日攻击法

姓名、单位、生日和电话，父母、子女、爱人的号码，排列~~排列~~，组合~~组合~~，又有20%的密码会被黑客们猜到了。

拖库与撞库

拿下一个网站，盗取所有人的帐号和密码，这叫拖库。用拖库得到的帐号密码，再去批量尝试登录其他的网站，十有八九也能成功，这就叫撞库。

口令安全原则是攻防对抗的产物

防暴力破解类

密码就要足够长，足够复杂，15位以上，数字 + 字母大小写 + 特殊符号

防流行弱密码

至少要让自己与众不同，安全水准超过平均水平

防生日攻击法

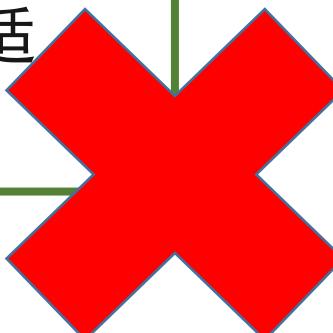
与个人信息、家人信息有关的密码一律不能用

防撞库

密码要独立设置，特别是社交、邮箱和支付账户一定要单独设置密码

防拖库

密码要经常改换，每隔3-6个月换一次比较合适



如何设置一个强度高，又好记的密码

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
- 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



安全办公与安全出行

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
之一就是有员工在内网之
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：

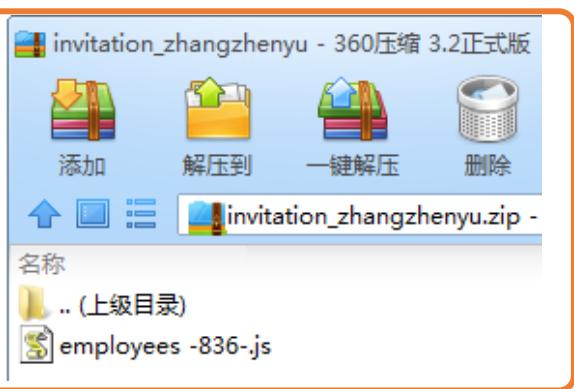
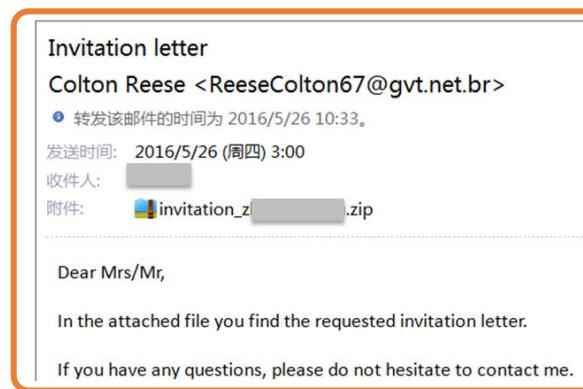
- 您的办公邮箱中会收到很多垃圾邮件。
- 一旦第三方应用平台被黑，您办公邮箱的帐号和密码也可能会同时泄露，造成邮件中的机密外泄。
- 办公邮箱密码泄露，可能引发连锁反应，进而泄露机构内网帐号，导致内网被黑客入侵。



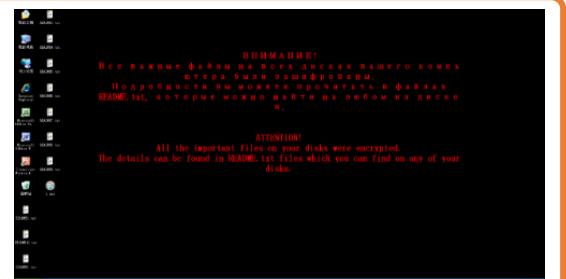
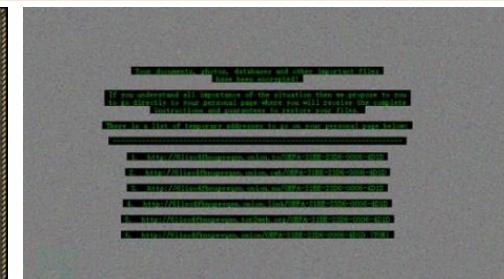
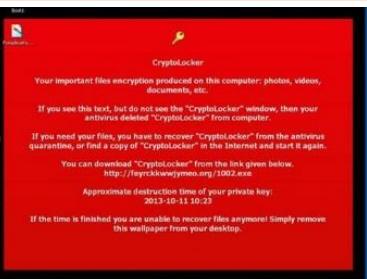
邮件附件常带毒，陌生来源勿打开

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。



勒索软件中招后屏幕的现象



窃密邮件

2016年6月，一封带毒邮件盗走日本大型旅社800万用户资料。



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。

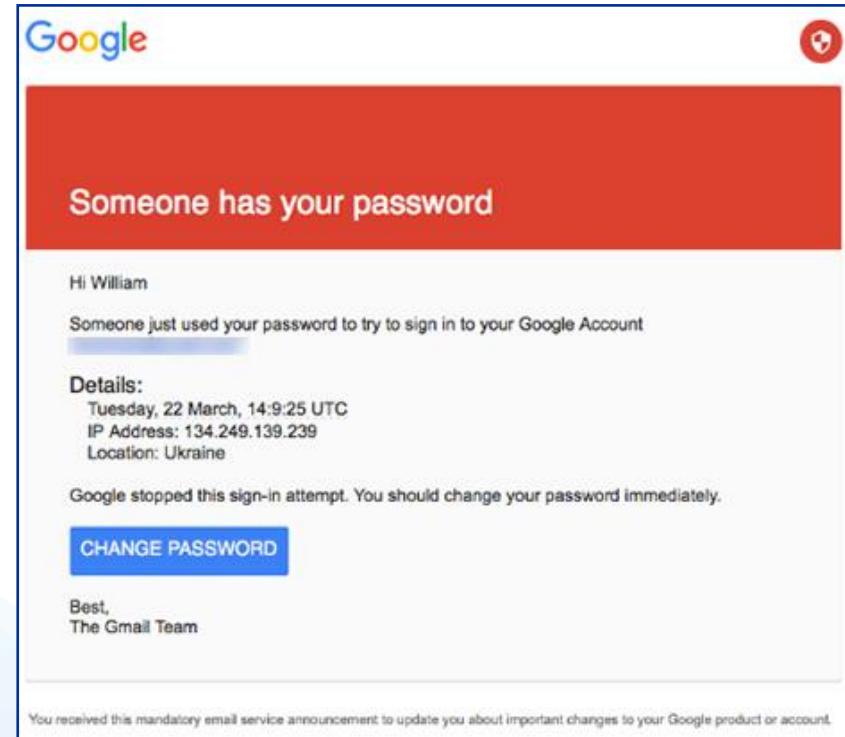
OA 钓鱼最危险，美国大选也中招

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。

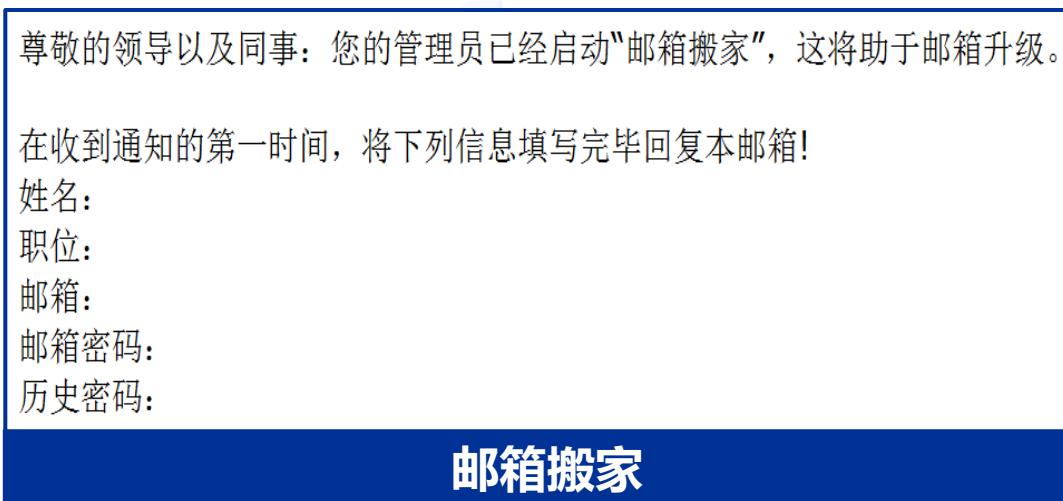
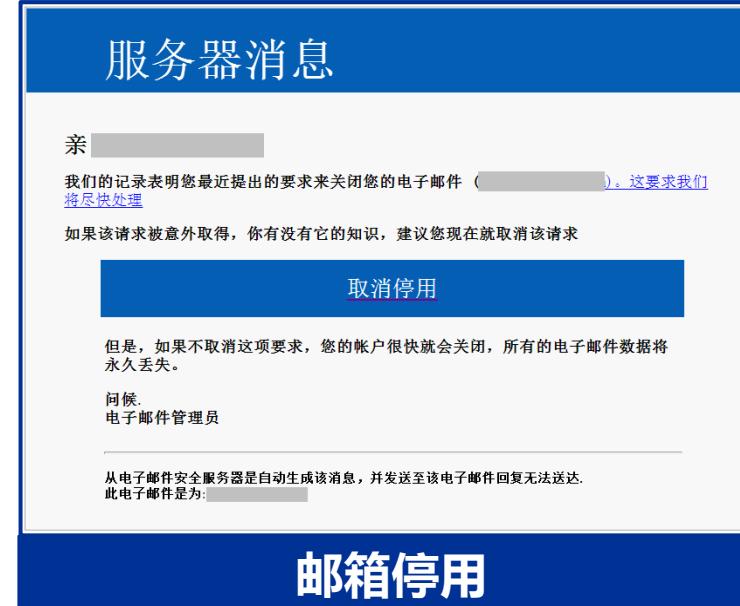


2016年美国大选，黑客组织冒充Google邮件系统安全管理员给希拉里竞选团队负责人发信，骗取了负责人的邮箱密码，盗取并公布了希拉里竞选团队的机密邮件，最终使得希拉里败选，特朗普上台。



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



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？

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。

连接WiFi要谨慎，蹭网心态吃大亏

WiFi的安全风险



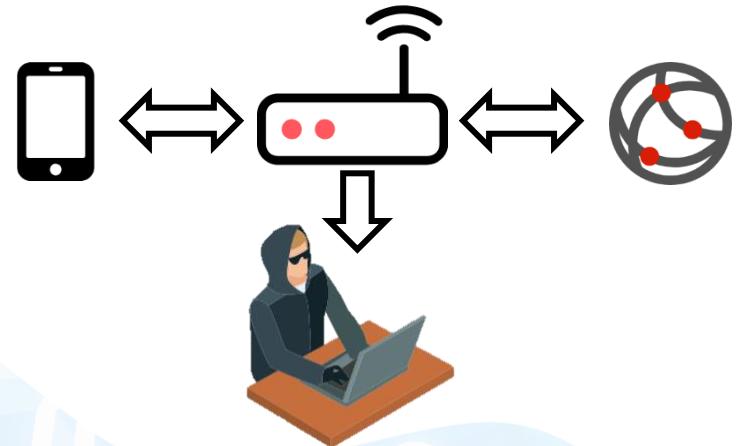
WIFI是一种短距离局域网无线传输技术，数据在传输过程中通常不加密。如果有黑客恶意监听无线路由器上传输的数据，数据将被黑客窃取。

2015年央视315晚会，安全专家现场演示如何通过免费WiFi盗取现场观众的上网信息，演示包括对照片、文字、帐号和密码等信息的窃取。



蹭网软件的风险

- 蹭网软件可以帮你免费使用他人WiFi
- 但也可能泄露自己家中的WiFi密码
- 连接不安全的WiFi可能被盗号、诈骗



特别提示：

公共场合链接WiFi，一定要选择官方的，有密码的。无密码的WiFi最危险。

二维码中藏奥秘，随手扫描易中招

二维码

二维码实际上是一个图形化的数据信息，信息中可以存储文本、网址等各类信息。



二维码生成器

网上可以搜索到很多二维码生成器，任何人都可以很容易的生成一个二维码

随意扫码的风险

- 扫码打开的网页可能含有欺诈信息、木马病毒
- 扫码后被要求填表，可能泄露个人信息
- 扫码后可能会进行“无意识支付”，被骗钱财

特别提示

- 扫码后提示下载陌生文件的，谨慎
- 扫码后要求填写个人信息的，谨慎

公务电脑莫出境，要带只带空白机



国外安检人员检查旅客行李中的电子物品

特别提示：

- 不论是公务员还是普通企业员工，出国旅行时尽量不要带自己日常使用的办公电脑。
- 一方面，您可能被安检员强行扣查电脑，造成机密泄露。
- 另一方面，国外社会、网络环境与国内不同，电脑更易遭到盗窃、抢夺或网络攻击。

谢谢 Thank you