网络安全为人民 网络安全靠人民

树立网络安全观，共筑全民安全线

目标

- 建立对网络安全的敏感意识和正确认识
- 了解网络安全趋势和相关法律法规
- 了解工作和生活中可能面临的安全威胁和风险
- 在工作和生活中养成良好的安全习惯

目录
CONTENTS

01

网络安全发展形势

一、全球网络攻击事件更加频发

英特尔公司爆出“幽灵”“熔断”两个处理器漏洞，导致恶意程序可获取敏感信息；

英国政府通信总部发现家用新型智能电表存在安全漏洞，威胁数百万物联网设备安全，甚至可能影响国家电网的正常运转

黑客利用思科高危漏洞发起攻击，20余万台思科设备受到影响

软硬件设备安全漏洞频出

荷兰三大银行网络系统在一周内不断遭受分布式拒绝服务攻击；

美国赛门铁克公司发现黑客组织针对美国和东南亚国家卫星通讯、电信、地理太空拍摄成像服务和军事系统进行网络攻击。

美国国土安全部称黑客多次试图破坏美选举系统

关键信息基础设施遭受攻击

美媒报道特朗普大选期间聘用的“剑桥分析”从2014年起违法收集脸谱网上5000多万名美国用户的数据，用于预测和影响选民的大选投票取向。

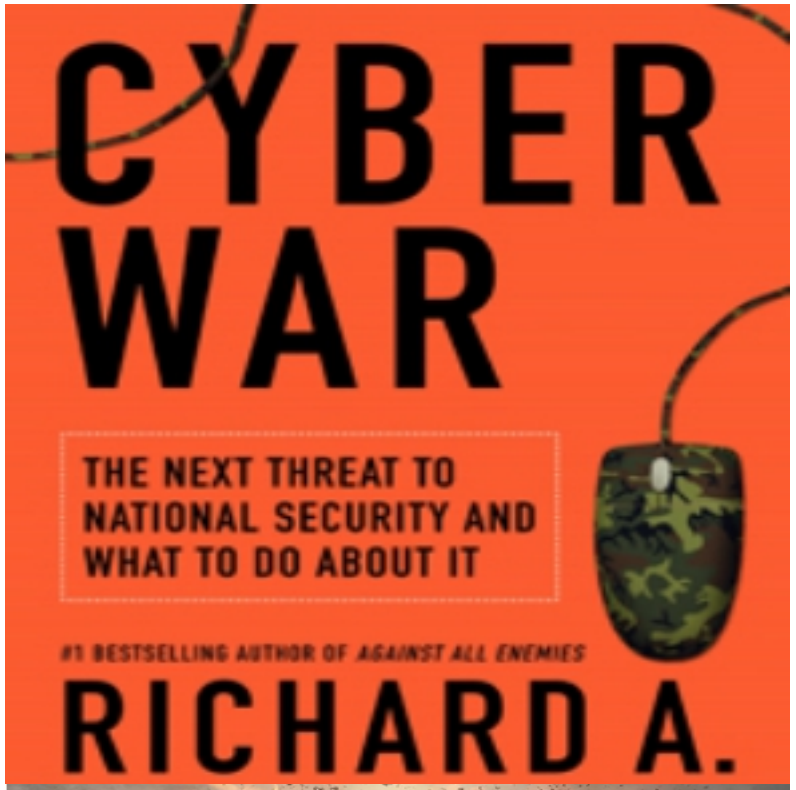
脸谱网遭受黑客攻击，5000多万用户的个人隐私信息面临风险

个人信息与商业数据遭大规模泄露

二、全球网络对抗态势进一步升级

网络攻击的频发为网络安全行业敲响了警钟,网络空间日益成为继陆、海、空、天之后的第五大主权领域空间,成为各国争夺的重要战略空间

- 2018年，美国发布两项重要国防战略，均显示出明显网络对抗战略意图。
- 7月，发布《2019年国防授权法案》，明确将中国、俄罗斯等国列为美国国家安全“威胁”，并建议增加网络冲突前线的军事部署。
- 9月，发布《国防部网络安全战略》，指出中国和俄罗斯对美国及其盟国的战略性威胁正在增大，为防范网络攻击要进行先发制人。



党中央对网络强国和网络信息安全工作高度重视

2014年2月27日，中央网络安全和信息化领导小组成立，习近平总书记亲自担任组长，李克强、刘云山任副组长。

没有网络安全就没有国家安全

中央网络安全和信息化领导小组第一次会议

指出，“**没有网络安全就没有国家安全**，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术。”

总书记4.19网信座谈会讲话

总书记要求“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”

全国网络安全和信息化工作会议

总书记指出“**没有网络安全就没有国家安全，就没有经济社会稳定运行**，广大人民群众利益也难以得到保障。要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。”

2014 2015 2016 2017 2018 2018

总书记在第二届世界互联网大会开幕式上的讲话

安全是发展的保障，发展是安全的目的。网络安全是全球性的挑战，没有哪个国家能够置身事外、独善其身，维护网络安全是国际社会的共同责任。

总书记在十九届中央政治局第二次集体学习时的讲话

要切实保障**国家数据安全**，要加强关键信息基础设施安全防护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。

总书记在第五届世界互联网大会的贺信中强调

世界各国虽然国情不同、互联网发展阶段不同、面临的现实挑战不同，但推动数字经济发展的愿望相同、应对网络安全挑战的利益相同、加强网络空间治理的需求相同。

没有网络安全就没有国家安全

总书记对2019年网络安全宣传周作出重要指示

举办网络安全宣传周、提升全民网络安全意识和技能，是国家网络安全工作的重要内容。国家网络安全工作要坚持网络安全为人民、**网络安全靠人民，保障个人信息安全**，维护公民在网络空间的合法权益。要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态。”

2019

全国习近平在中央政治局第十八次集体学习时强调

要加强对区块链技术的引导和规范，加强对区块链安全风险的研究和分析，密切跟踪发展动态，积极探索发展规律。要探索建立适应**区块链技术机制**的**安全保障体系**，引导和推动区块链开发者、平台运营者加强行业自律、落实安全责任。要把依法治网落实到区块链管理中，推动区块链安全有序发展。

2019

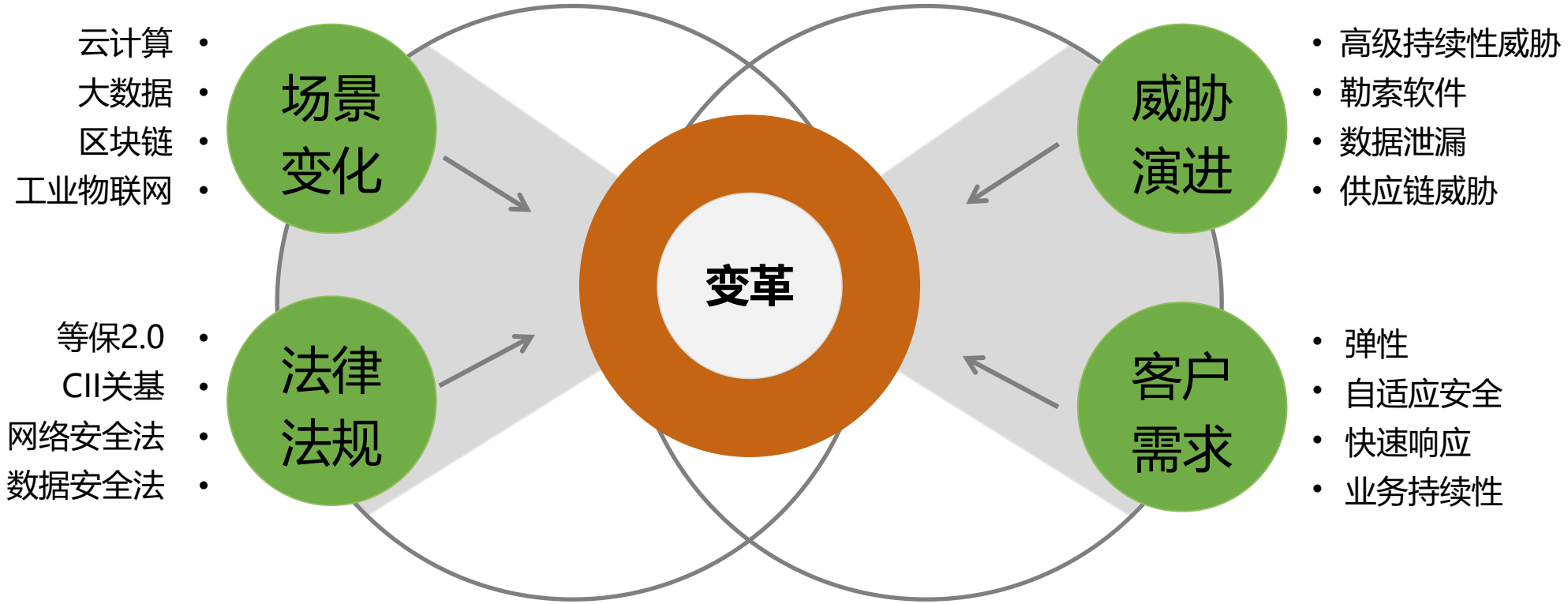
总书记在第六届世界互联网大会的贺信中强调

当前，新一轮科技革命和产业变革加速演进，人工智能、大数据、物联网等新技术新应用新业态方兴未艾，互联网迎来了更加强劲的发展动能和更加广阔的发展空间。发展好、运用好、治理好互联网，让互联网更好造福人类，是国际社会的共同责任。各国应顺应时代潮流，勇担发展责任，共迎风险挑战，**共同推进网络空间全球治理，努力推动构建网络空间命运共同体。**

2019

三、各国将更加重视数据安全治理

一方面，全球数字经济发展进入加速活跃期



各国将更加重视数据安全治理

另一方面，世界各主要国家数据安全战略布局加快

2018年起，世界主要国家和地区抓紧建立数据管理体系，并通过强化主体权责、实施长臂管辖等措施，加大数据安全管理范围和管理力度。

欧盟

- 2018年5月，《通用数据保护条例》（简称GDPR）正式实施，规定的罚款额度上限为2000万欧元或全球营业额的4%；截至2019年9月，欧盟22个国家数据保护机构已对87个案件做出3.73亿欧元的行政处罚。
- **“最高罚单”**：英国航空公司因泄露50万用户信息被英国信息专员办公室处以约15.8亿人民币罚款。
- **2019年11月12日，欧洲数据保护委员会（EDPB）对外发布了针对GDPR的域外适用效力的最终指南，明确了有关数据控制者或处理者对个人数据的处理活动需适用GDPR的地域范围。**

美国

- 2018年3月，美国国会正式通过《澄清数据在海外的合法使用法》（CLOUD法案）明确授权美国执法机构访问在美国境内运营的企业储存在海外的用户数据。
- 2018年6月，美国加州州批准《2018年加州消费者隐私法案》（CCPA），加强消费者隐私权和数据安全保护。（属人原则）

各国将更加重视数据安全治理

——习近平总书记有关数据安全重要批示指示精神

党的十八大以来，以习近平同志为核心的党中央高度重视数字经济发展和数据安全工作，多次做出重要批示，明确指出要构建以数据为关键要素的数字经济，推动互联网、大数据、人工智能和实体经济深度融合，突出强调要切实保障国家数据安全，加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。

- **党的十九大报告：** “加强关键信息基础设施网络安全防护，不断增强网络安全防御能力和威慑能力，加强网络安全预警监测，切实保障国家数据安全”。
- **2017年中央政治局第二次集体学习：** “推动实施国家大数据战略，加快完善数字基础设施，推进数据资源整合和开放共享，保障数据安全。”
- **2019年贵阳数博会贺信：** “处理好大数据发展在法律、安全、政府治理等方面挑战。”

——党中央、国务院有关数据安全的重大决策部署

- 中央经济工作会议和《政府工作报告》就**打击侵犯公民个人信息**等工作提出明确要求。
- 国务院陆续制定出台的《促进大数据发展行动纲要》《国家网络空间安全战略》等战略规划，都提出**健全大数据安全保障体系的要求。**
- 今年中央网信工作要点明确部署网信、工信等部门要**加强大数据综合治理。**

四、我国网络安全能力建设工作将不断强化

2021年，我国将继续加强对网络安全核心技术研发的支持，强化网络安全复合型人才的培养力度，鼓励企业通过多种方式开展合作，进一 步提高我国的网络安全能力

02

国内外典型安全事件

网络安全事件

由数以百万监控摄像头组成的僵尸网络对美国Dyn的DNS服务器发起DDoS攻击，导致域名无法解析，多个知名网站无法访问

WannaCry勒索病毒全球大爆发，至少150个国家、30万名用户中招，造成损失达80亿美元，已经影响到金融，能源，医疗等众多行业，造成严重的危机管理问题

思科公司发现路由器蠕虫VPNFilter，感染50万台设备

反序列化漏洞被黑客频繁使用，远程代码执行漏洞是黑客的最爱。网站漏洞利用周期大幅缩短到小时级，网站管理员需要提高升级效率

2016年10月

2016年8月19日

山东临沂徐玉玉，因被诈骗电话骗走上大学的费用9900元，伤心欲绝，郁结于心，最终导致心脏骤停，经医院抢救不幸离世。2018年2月1日，案件入选“2017年推动法治进程十大案件”。

2017年8月

2018年3月

挖矿类恶意程序在春节过后持续升温。在各类挖矿病毒中，针对门罗币的WannaMine 尤为活跃，在挖矿活动中占比 超过70%，造成大量服务器和终端资源浪费。

2018年5月

2019年

2018年8月

华住集团旗下连锁酒店用户数据在暗网售卖。泄露的信息包括登记的身份信息及酒店开房记录，住客姓名、手机号、邮箱、身份证号、登录账号密码等。卖家对这个约5亿条数据打包出售价格为8比特币或520门罗币。

被黑客改变的美国总统大选

1. 利用Twitter来散播虚假信息，恣意挑衅、毫无来由地攻击任何人）
2. **攻击选民登记数据库，篡改选民信息**
3. 大选前发布竞选人黑料
4. 希拉里“邮件门”

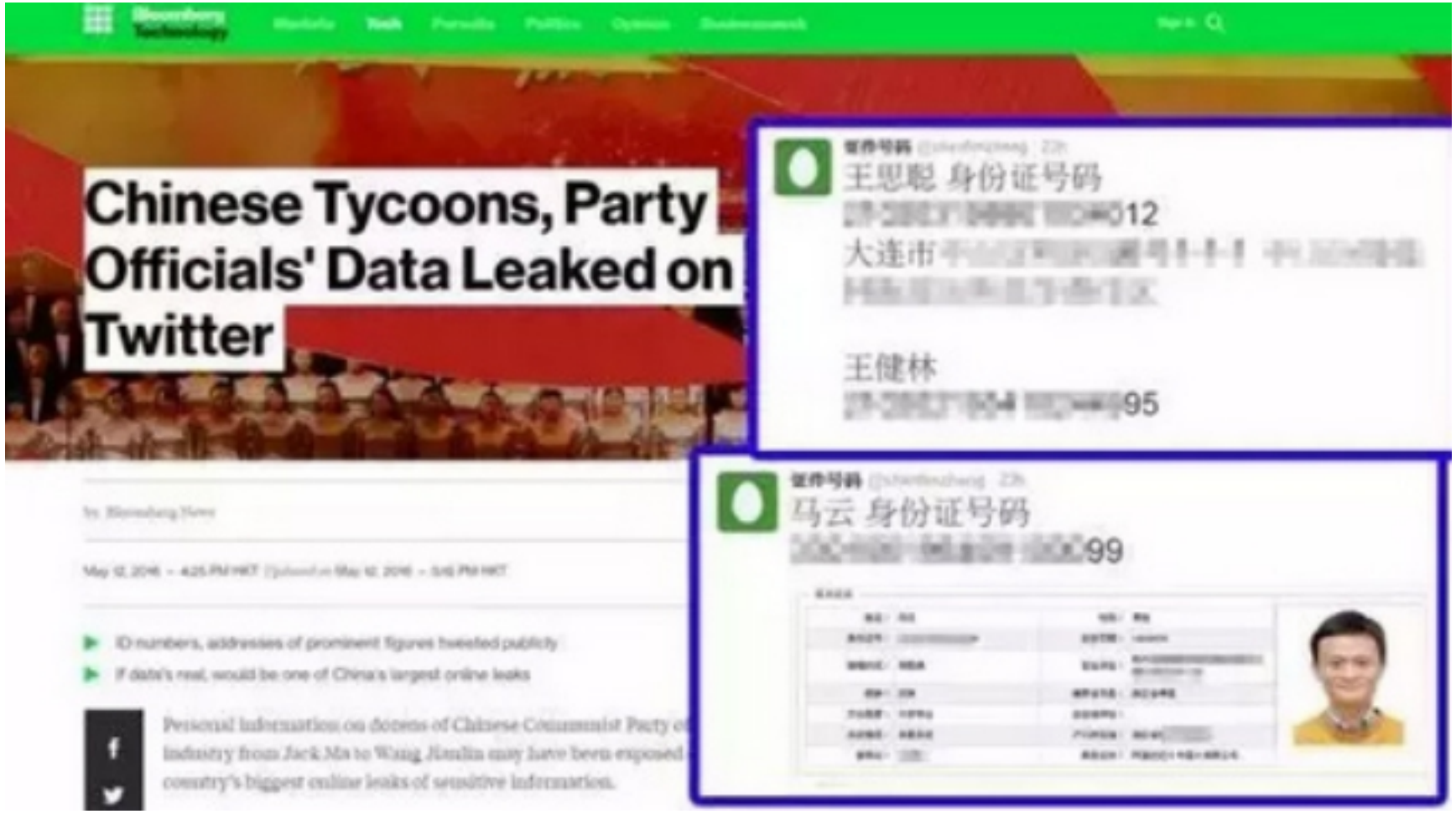
银行卡信息泄漏，卡内余额被盗刷

2015年1月，国内某支付机构泄露了上千万张银行卡信息，涉及全国16家银行，之后半年多的时间里因伪卡形成的损失高达3900多万元

2017年，两则新闻”银行卡在身边被接连盗刷10多万法院判银行全额赔偿”，”银行卡遭盗刷57余万元 银行被判全额赔偿损失”

信息泄漏层出不穷，名人明星多烦扰

- 根据《彭博社》报道，包括马云、马化腾、李彦宏、刘强东、王思聪在内的名人的身份证信息、家庭住址、门牌号、籍贯都被一位Twitter ID为“shenfenzheng”的用户泄漏了。



拼多多现优惠券漏洞，遭黑产团伙盗取数千万元

关键词：黑灰产，薅羊毛

事件回顾：

2019年1月20日凌晨，拼多多被曝出现重大BUG，用户可领100元无门槛券。网友称“有大批用户开始‘薅羊毛’，一晚上200多亿都是话费充值”。当天上午9点，拼多多已经把100元无门槛优惠券的领取方式全部下架，之前领到未使用的优惠券也全部下架。

在“薅羊毛”事件发生几个小时后，1月20日中午12点，认证为拼多多微博客服的@拼多多客户服务终于对此事发布了官方回应《关于“黑灰产通过平台优惠券漏洞不正当牟利”的声明》，声明全文如下：

1月20日晨，有黑灰产团伙通过一个过期的优惠券漏洞盗取数千万元平台优惠券，进行不正当牟利。针对此行为，平台已第一时间修复漏洞，并正对涉事订单进行溯源追踪。同时我们已向公安机关报案，并将积极配合相关部门对涉事黑灰产团伙予以打击。

抖音千万级账号遭撞库攻击，牟利百万黑客被捕

关键词：网络攻击，撞库

事件回顾：

2019年2月，北京字节跳动公司向海淀警方报案，其公司旗下抖音APP，遭人拿千万级外部账号密码恶意撞库攻击，其中上百万账号密码与外部已泄露密码吻合。

字节跳动系统实时监测到攻击后，为防止黑客利用撞出账户实施不法行为，字节跳动公司通过安全系统，实时对所有疑似被盗账号设置了短信二次登陆验证。

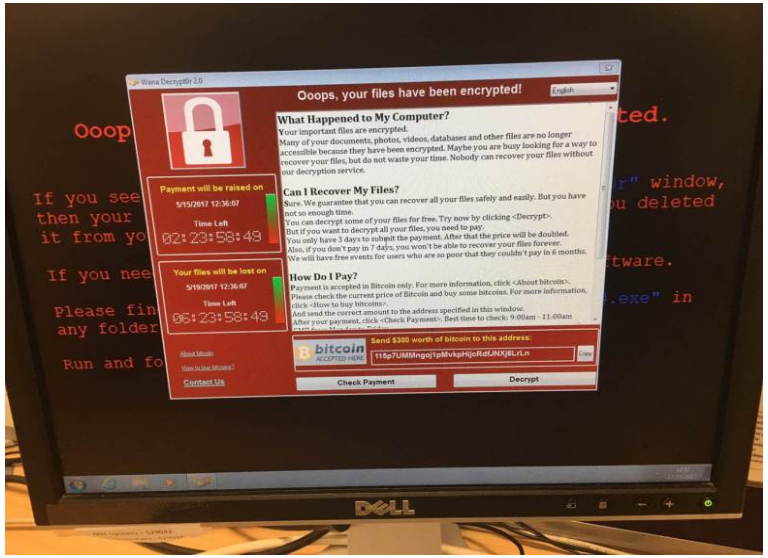
经警方侦查，发现湖北籍男子汪某有重大作案嫌疑，5月底，海淀警方将汪某在家中抓获。据了解，汪某毕业后一直无业，便利用其掌握的计算机能力，控制了多个热门网络平台的大量账号，随后通过在网上承接点赞刷量、发布广告等业务牟利。同时汪某还编写了大量撞库代码，对目前网络上比较热门的网络平台进行撞库，然后控制撞库获取的账户，累计获利上百万元。

境外黑客利用勒索病毒攻击部分政府和医院机构

关键词：网络攻击，勒索病毒

事件回顾：

2019年3月13日，有消息显示，我国部分政府部门和医院等公立机构遭遇到国外黑客攻击。此次攻击中，黑客组织利用勒索病毒对上述机构展开邮件攻击。

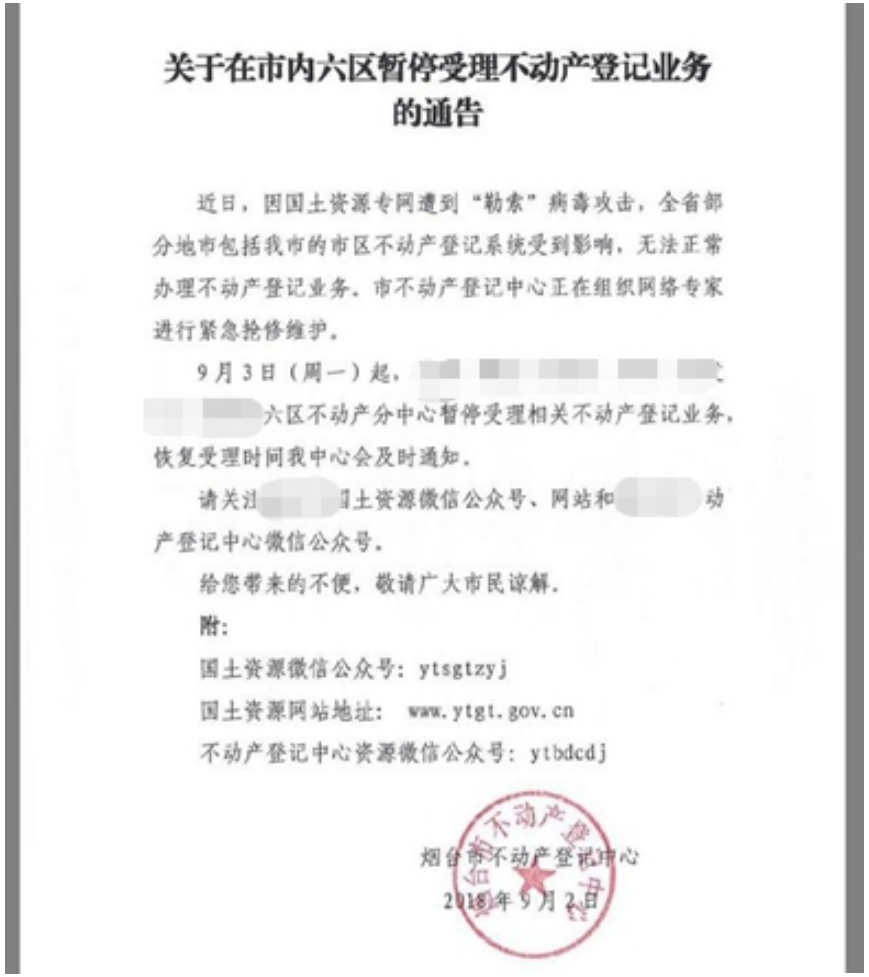


从2019年3月11日起，境外不明黑客组织对我国部分政府部门开展勒索病毒邮件攻击。这些邮件的标题是“你必须在3月11日下午3点向警察局报到!”，这些邮件的发件者名为“Min,GapRyong”(部分部门反映还有其他的假冒发件人约70多个)，另外这些邮件中无一例外都附有名为“03-11-19.rar”的压缩文件，而不明真相者一旦打开这些附件将会中招。

另外，据了解，多个政府单位和企业收到了紧急通知，湖北省宜昌市夷陵区政府、中国烟草旗下福建武夷烟叶有限公司、中国科学院金属研究所等在其官网发布了上述消息。腾讯、360等互联网安全公司发布了预警信息。

山东多地不动产登记系统遭到勒索病毒攻击!

1. 没有重视网络安全，没有进行常规安全检查和杀毒扫描，从而加强防护工作；
2. 没有按照等级保护合规进行建设；亦或形式上的“过等保”，自以为可以高枕无忧；
3. 勒索病毒多次爆发，重点系统的相关负责人仍没有意识做安全检查、整改等工作。



关于在市内六区暂停受理不动产登记业务的通告

近日，因国土资源专网遭到“勒索”病毒攻击，全省部分地市包括我市的市区不动产登记系统受到影响，无法正常办理不动产登记业务。市不动产登记中心正在组织网络专家进行紧急抢修维护。

9月3日（周一）起，[redacted]六区不动产分中心暂停受理相关不动产登记业务，恢复受理时间我中心会及时通知。

请关注[redacted]国土资源微信公众号、网站和[redacted]动产登记中心微信公众号。

给您带来的不便，敬请广大市民谅解。

附：

国土资源微信公众号：ytsgtzyj

国土资源网站地址：www.ytgt.gov.cn

不动产登记中心资源微信公众号：ytbdcdj

烟台市不动产登记中心

2018年9月2日

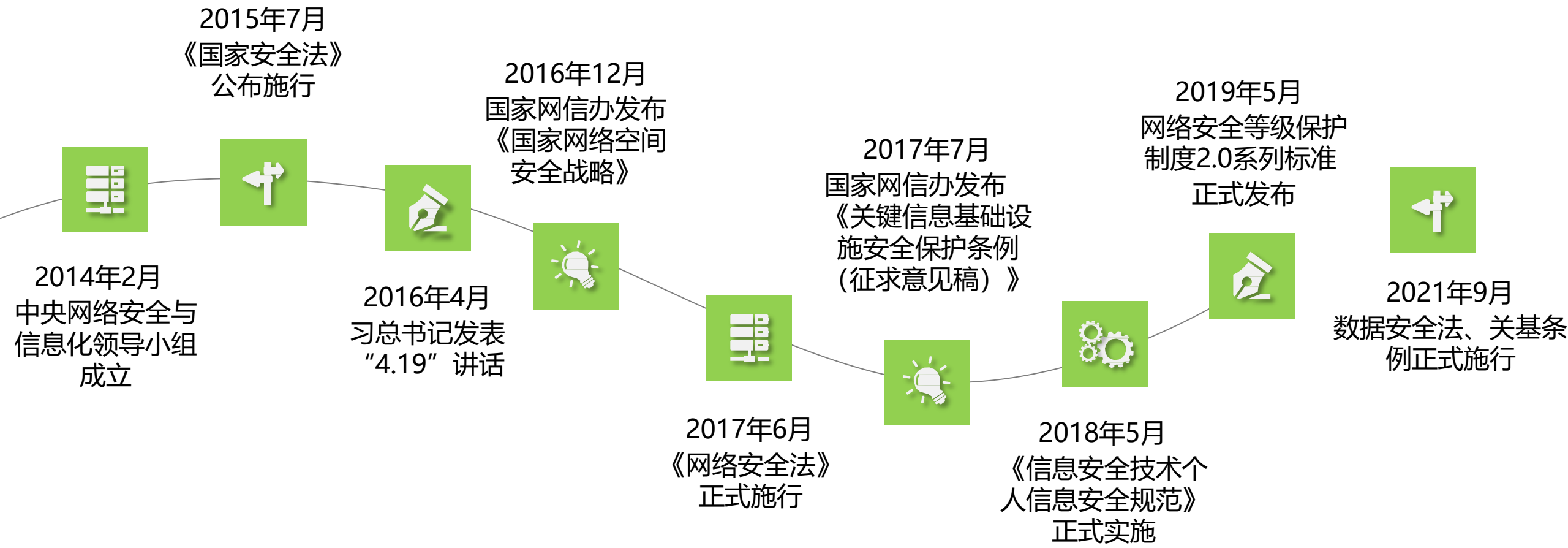
总结

从数字货币到勒索软件，从网络欺诈到舆论控制，从商业竞争到国家安全，随着数字化世界的到来，网络攻击对政治、经济、军事、国家、社会安全，甚至是人身安全的影响越来越大。

03

网络安全法律法规

国家高度重视网络安全，相关政策法律密集出台



《中华人民共和国网络安全法》

1. **明确了网络空间主权的原则**
   《网络安全法》第1条明确规定要维护我国网络空间主权。网络空间主权是一国国家主权在网络空间中的自然延伸和表现。
2. **明确了网络产品和服务提供者的安全义务**
   《网络安全法》明确网络产品和服务提供者需要尽到相应的责任和义务
3. **明确了网络运营者的安全义务**
   网络安全法明确规定网络运营者应接受社会监督、受理公众举报
4. **进一步完善了个人信息保护规则**
   网络安全法聚焦个人信息安全保护
5. **建立了关键信息基础设施安全保护制度**
6. **监测预警与应急处置措施制度化、法制化**

简介

《网络安全法》是我国第一部网络安全领域的法律，**是保障网络安全的基本法**。网络安全法是我国网络安全管理的基础法律，与其它相关法律在相关条款和规定上互相衔接，互为呼应，共同构成了我国网络安全管理的综合法律体系。

等级保护2.0

网络运营者要对信息系统（含网络）进行**分等级保护、分等级监管**。将全国的信息系统（包括网络）按照**重要性和遭受损坏后的危害性**分成 5 个安全保护等级（从第一级到第五级，逐级增高）。

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	**第二级**
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

数据安全法&个人信息保护法

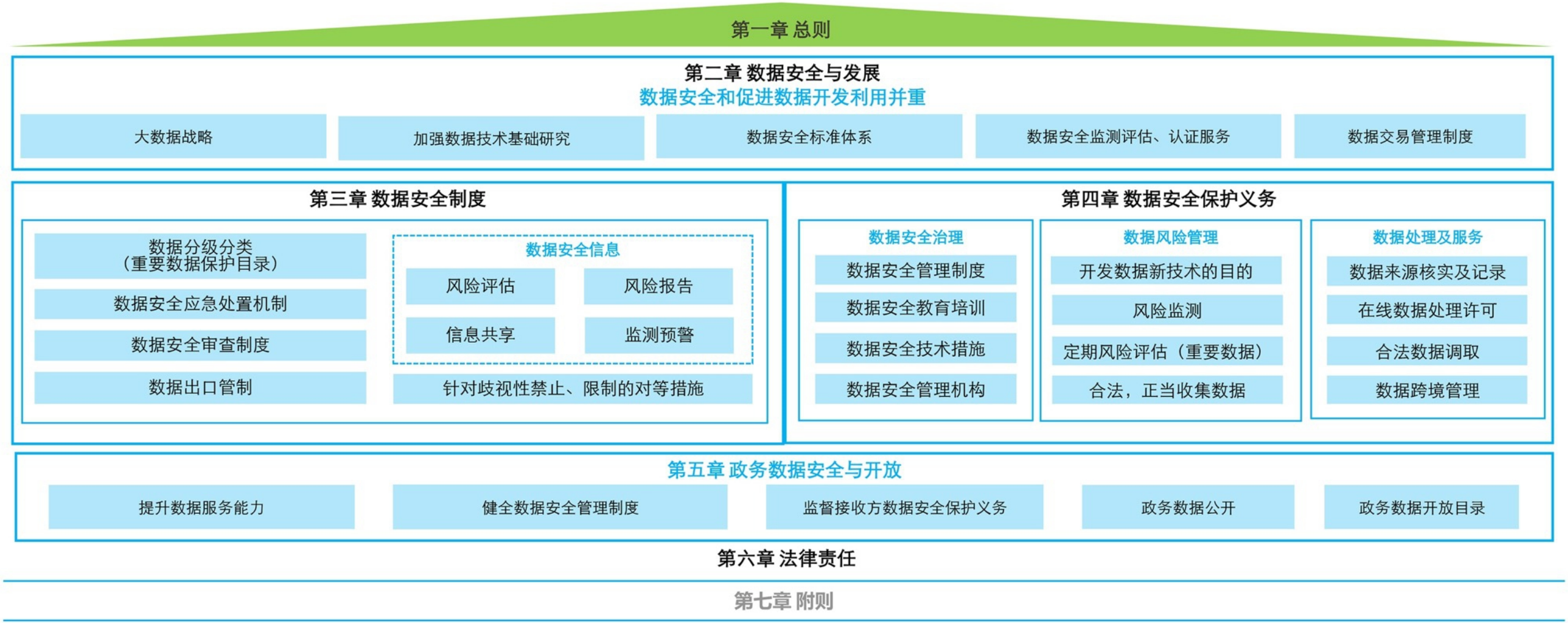
数据安全保护

- 2019年5月28日《**数据安全管理办法**》（征求意见稿）
- 2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过《**中华人民共和国数据安全法**》，自2021年9月1日起施行

个人信息保护

- 2018年5月1日起施行《**信息安全技术个人信息安全规范**》
- 2019年10月1日起施行《**儿童个人信息网络保护规定**》
- 2021年8月20日，《**中华人民共和国个人信息保护法**》表决通过，自2021年11月1日起施行

数据安全法



数据安全法于2021年6月10日颁布，9月1日正式实施。
第一章第四条 维护数据安全，应当坚持总体国家安全观，**建立健全数据安全治理体系，提高数据安全保障能力。**

数据安全保障措施

建立健全全流程
数据安全管理制度

采取响应的技术措施

在网络安全等级保护基础上
履行数据安全保护义务

数据安全保护责任

数据安全教育培训

- 第二十九条：加强**风险监测**，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施
- 第三十二条：任何组织、个人收集数据，应当**采取合法、正当的方式**，不得窃取或者以其他非法方式获取数据。

网络安全监管机构职责

01

中央网络安全与信息化委员会

着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。

02

公安部

负责公共信息网络的安全监察工作、信息安全及等级保护的监督管理工作和信息安全产品的销售许可工作等。

03

工信部

拟定实施行业规划、产业政策和标准；指导推进信息化建设；协调维护国家信息安全等；指导软件发展；拟定并组织实施软件、系统集成及服务的技术规范和标准；推动软件公共服务体系建设；指导、协调信息安全技术开发等。

04

国家保密局

管理和指导保密技术工作，负责办公自动化和计算机信息系统的保密管理，指导保密技术产品的研制和开发应用，对从事涉密信息系统集成的企业资质进行认定。

05

国家密码管理局

主管全国商用密码管理工作，包括认定商用密码产品的科研、生产、销售单位，批准生产的商用密码产品品种和型号等。

06

国家版权局

主管全国新闻出版事业与著作权管理工作，负责软件著作权的登记和管理工作

04

个人终端安全防护

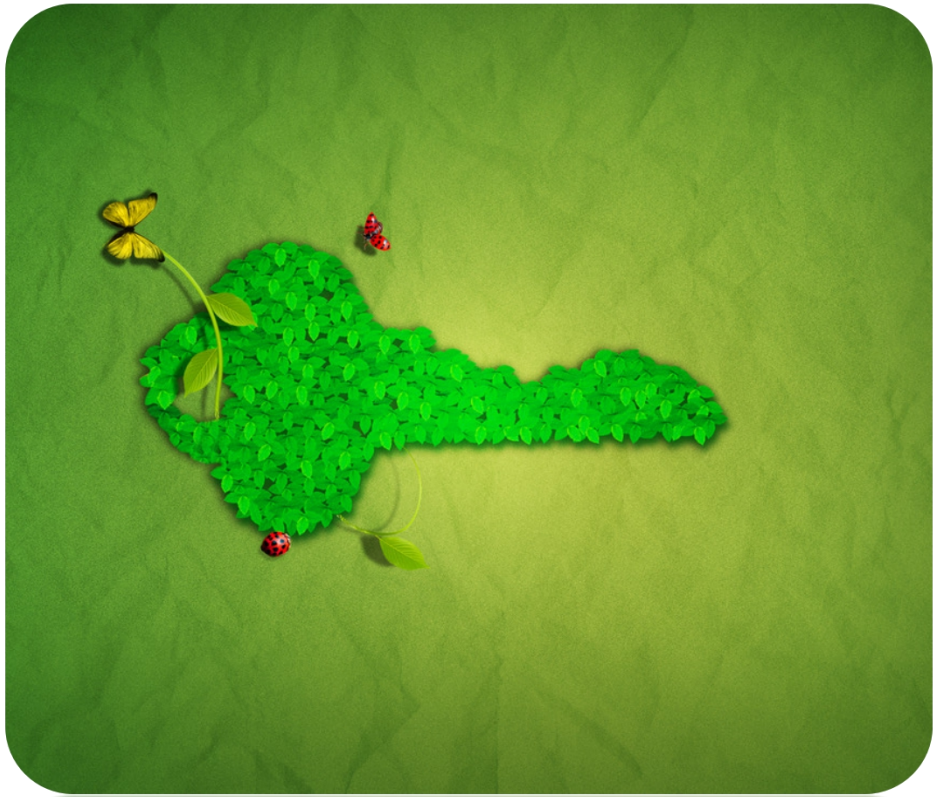
一、网络环境之险

一张图片能泄露什么？


Bai du 地图
拾取坐标系统
120.71150833333334,31.284997222222223
州市[更换城市]
当前层级：17级
金鸡湖国际
高尔夫俱乐部
金鸡湖酒店集团
凯宾斯基大酒店
凯宾美食廊
独墅湖大道
中国联通 4G
13:35
52%
朋友圈
BETTER YOUR BEST
2019 加油 小伙伴们
苏州 · 苏州金鸡湖凯宾斯基大酒店
2小时前
杭州互联网法院首例涉微信小程序案今日宣判
2小时前

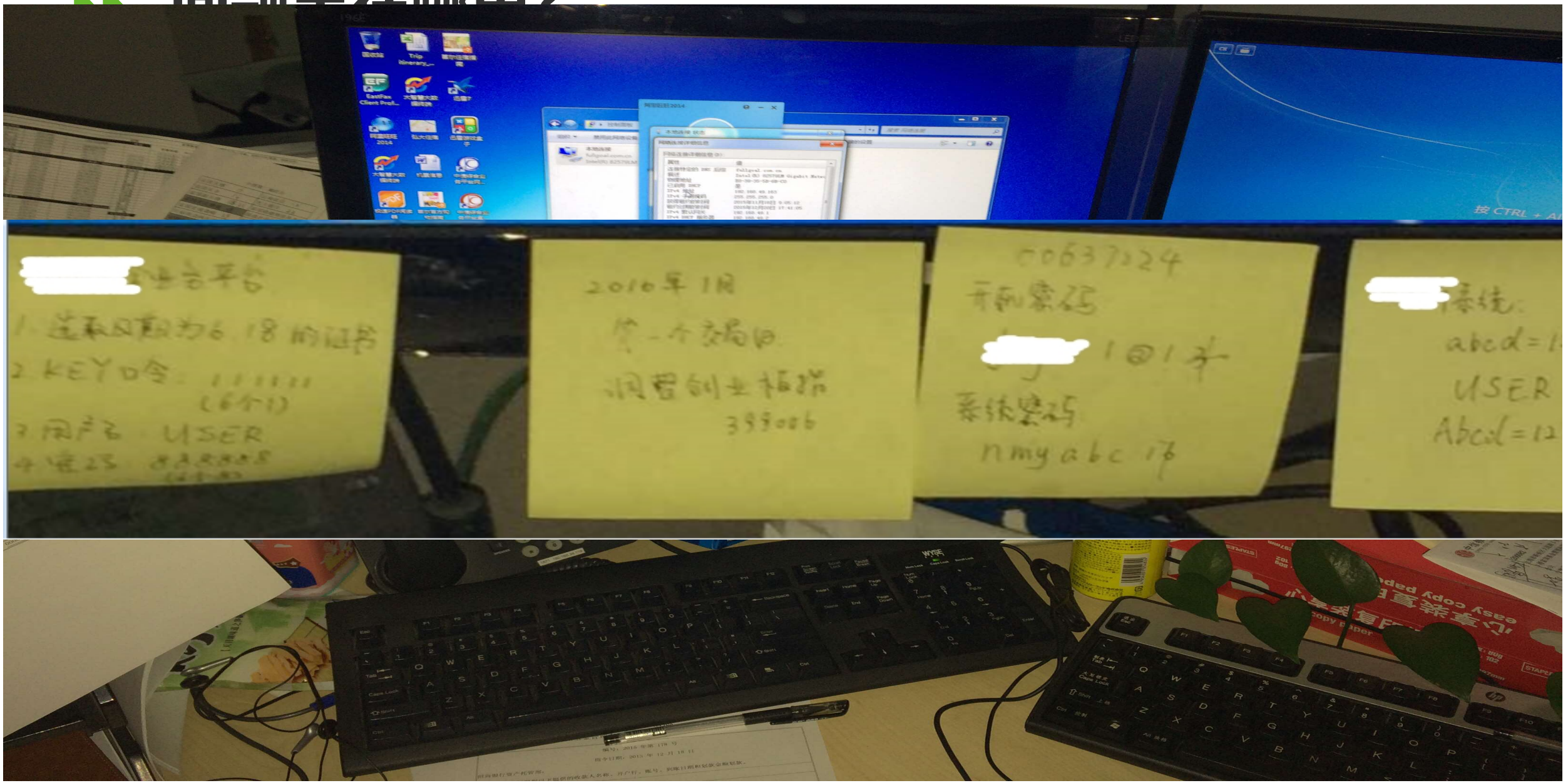
二、解决之道

提高信息安全意识

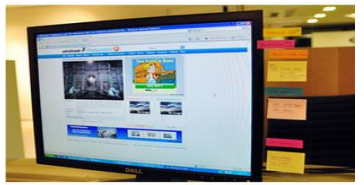


信息安全意识（Information Security Awareness），就是能够认知可能存在的信息安全问题，预估信息安全事故对组织的危害，恪守正确的行为方式，并且执行在信息安全事故发生时所应采取的措施。

问题出在哪里？



将口令写在便签上，贴在电脑监视器旁



开着电脑离开工位

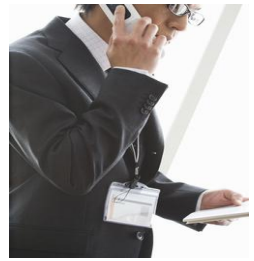
轻易相信来自陌生人的邮件，好奇打开邮件附件

使用容易猜测的口令，或者根本不设口令

随便拨号上网，或者随意将无关设备连入公司网络

没有安装防病毒软件、在系统更新和安装补丁上总是行动迟缓

打印机密文件未及时取走

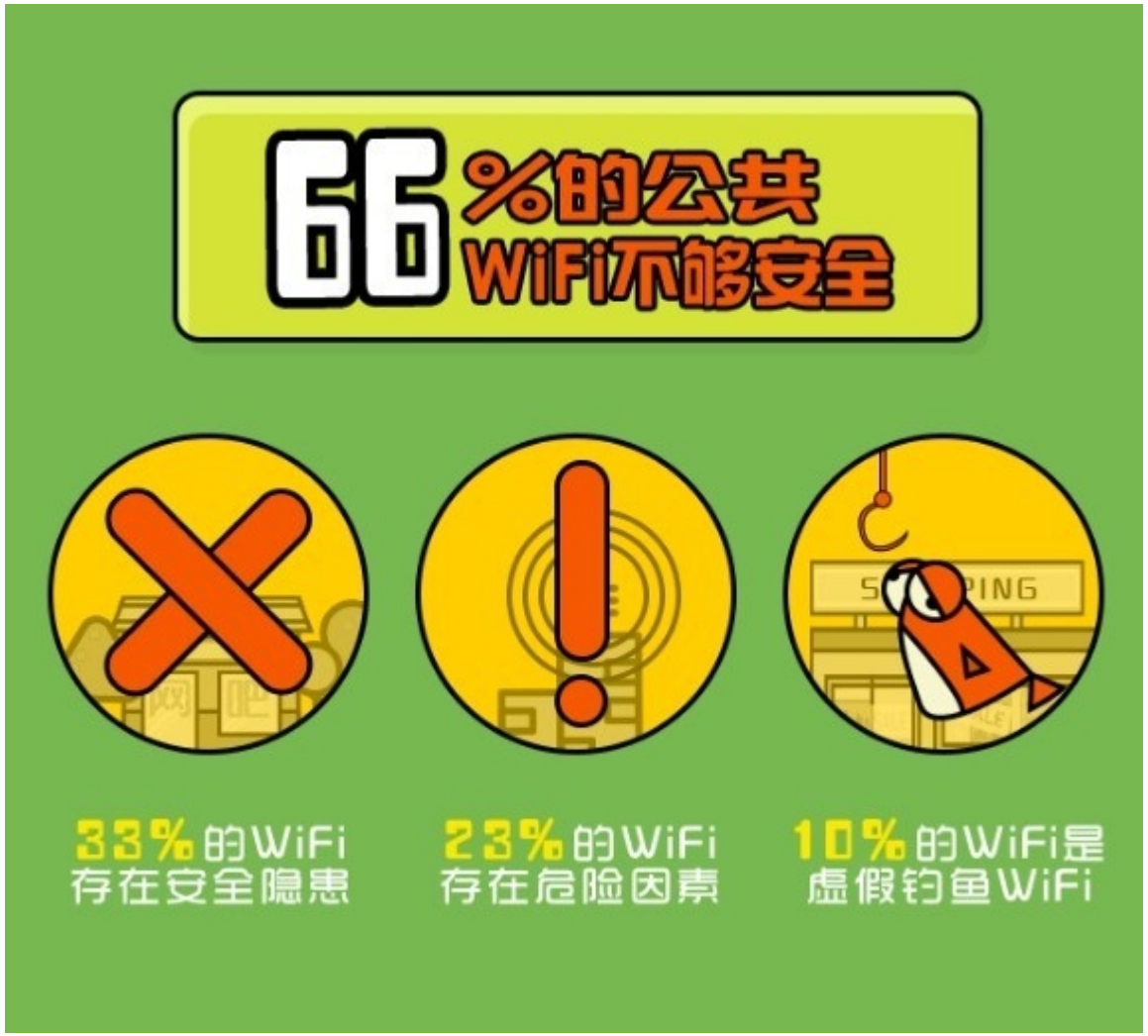


随意发布，泄漏公司机密文件

不能保守秘密，上当受骗，泄漏敏感信息

事不关己，高高挂起，不报告安全事件

上网习惯 – “免费”WiFi不免费



无论在家中，或者外出，民众对无线上网的需求越来越高。而手机上网已成为网民上网的首选，截止目前，手机网民已超过6.3亿。值得注意的是，其中92%的手机网民使用WiFi接入互联网，平均每天每人连接WiFi时长1.1小时。由此可见，WiFi已经成为民众日常生活中不可或缺的一部分。

上网习惯 – “免费”WiFi不免费

- **钓鱼WiFi：**

  在繁华的街道设立名字叫做“CMCC”、“KFC”的WiFi热点。

- **Karma：**

  伪装成受害设备以前连接过的公开WiFi热点。

- **ARP欺骗：**

  攻击者与受害者接入同一个WiFi热点

  通过发送特定数据伪装成数据网关

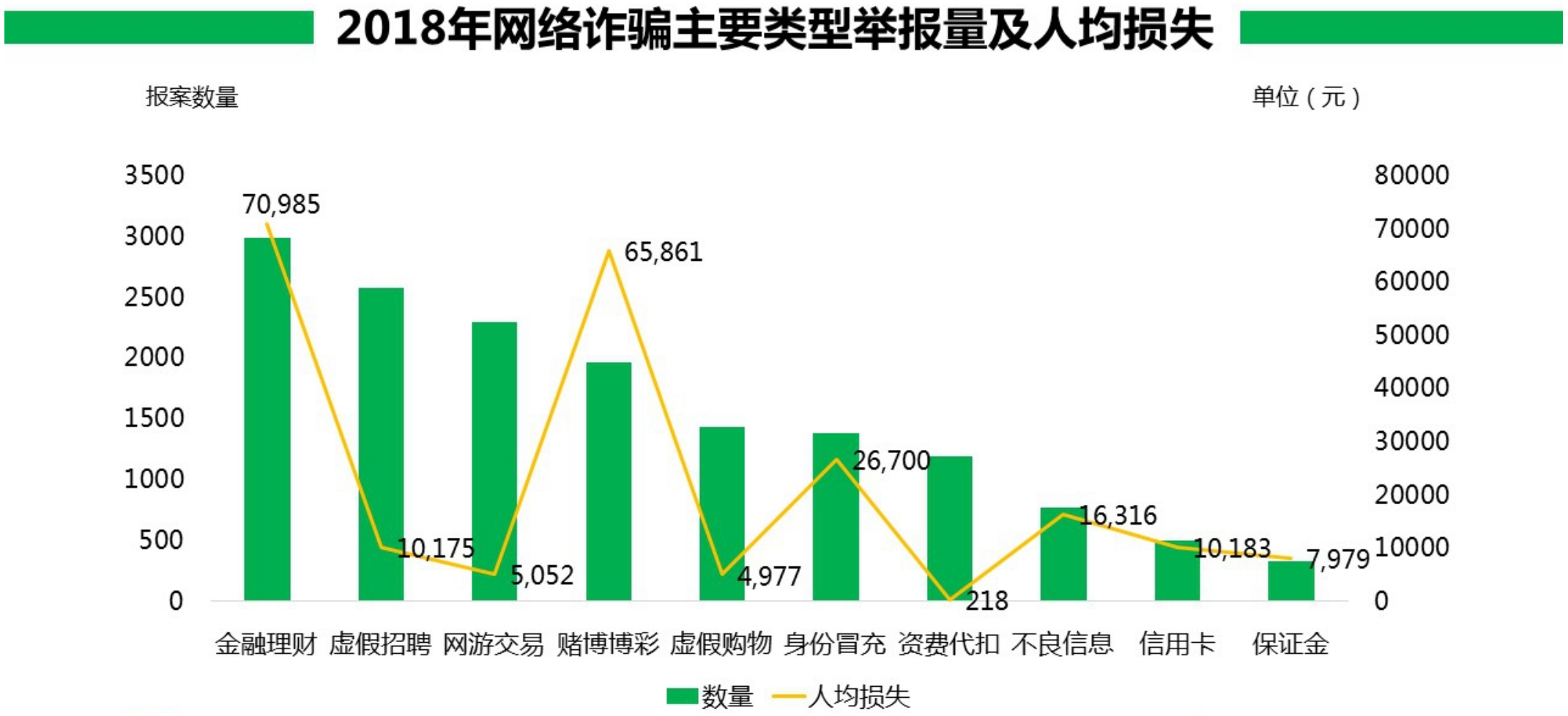
上网习惯 – “免费”WiFi需谨慎

有网友在微博表示公共场合的WIFI存在安全危机，黑客可以监视到所有连接至该网络的用户正在浏览的内容，甚至用户名、密码等信息也能手到擒来

安全建议：

- 用户应核对清楚WIFI名称
- 禁止手机自动连接WIFI
- 给手机和电脑安装杀毒软件
- 不要或尽量减少浏览不正规网站的次数

防范电信诈骗


2018年网络诈骗主要类型举报量及人均损失
报案数量
单位（元）
3500
3000
2500
2000
1500
1000
500
0
80000
70000
60000
50000
40000
30000
20000
10000
0
70,985
10,175
5,052
65,861
4,977
26,700
218
16,316
10,183
7,979
金融理财
虚假招聘
网游交易
赌博博彩
虚假购物
身份冒充
资费代扣
不良信息
信用卡
保证金
数量
人均损失

防范电信诈骗

骗子们的十大冒充十大“装”

26.0%运营商

21.2%领导

快递14.3%

12.5%医保社保机构

5.7%有关部门

5.7%商家客服

5.3%银行

3.9%公检法

2.9%学校

1.5%亲友

真实案例

交友平台伪装身份诈骗

投资理财诈骗

社会工程学攻击

凯文米特尼克所
著《欺骗的艺术》

通过对受害者

本能反应、好奇心、信任、贪婪

等心理弱点进行如欺骗和伤害等攻击手段

社会工程学的攻击，成功于人们

普遍的对信息安全实践上的无知！

巡游五角大楼，登录克里姆林宫

进出全球所有计算机系统

摧垮全球金融秩序和重建新的世界格局

谁也阻挡不了我们的进攻，

我们才是世界的主宰！

社会工程学与一般攻击的区别

	一般黑客攻击	社工攻击
攻击对象	 网络设备 主机服务器 应用程序 网络服务	 人 对人 只对人
攻击方法		 欺骗 诱导

教你了解黑客利器-社工学

- **什么是社会工程学攻击?**

搜集足够多的信息，以便于伪装成一个合法的雇员、合作伙伴、执法官员，或者任意角色。

我就是我所声称的那个人！

采集信息 → **选择目标** → **建立信任** → **实施攻击**

寻找组织、员工的明显弱点，寻求突破。

典型的一个攻击案例

美国一家印刷公司，其**工艺专利和供应商名单**是公司的核心资产，也是竞争对手梦寐以求的资料。为了保证安全，公司雇佣克里斯，一名资深的社会工程师，进行社会工程学攻击审查，试探该公司的服务器是否能够被入侵。

收集服务器相关信息：
服务器IP地址、物理地址、操作系统、应用程序及相关版本

1

收集个人相关信息
爱好：常去的餐厅，喜欢的比赛和球队
家庭状况：家庭成员及相关经历
线索：家人与癌症奋斗并存活下来

2

收集癌症相关的信息
癌症医疗机构及相关信息
知名的癌症慈善机构
规律性的募捐活动和规则

3

印刷公司CEO

进入我们公司的服务器是几乎不可能的，因为我在用性命看管这些材料！

5

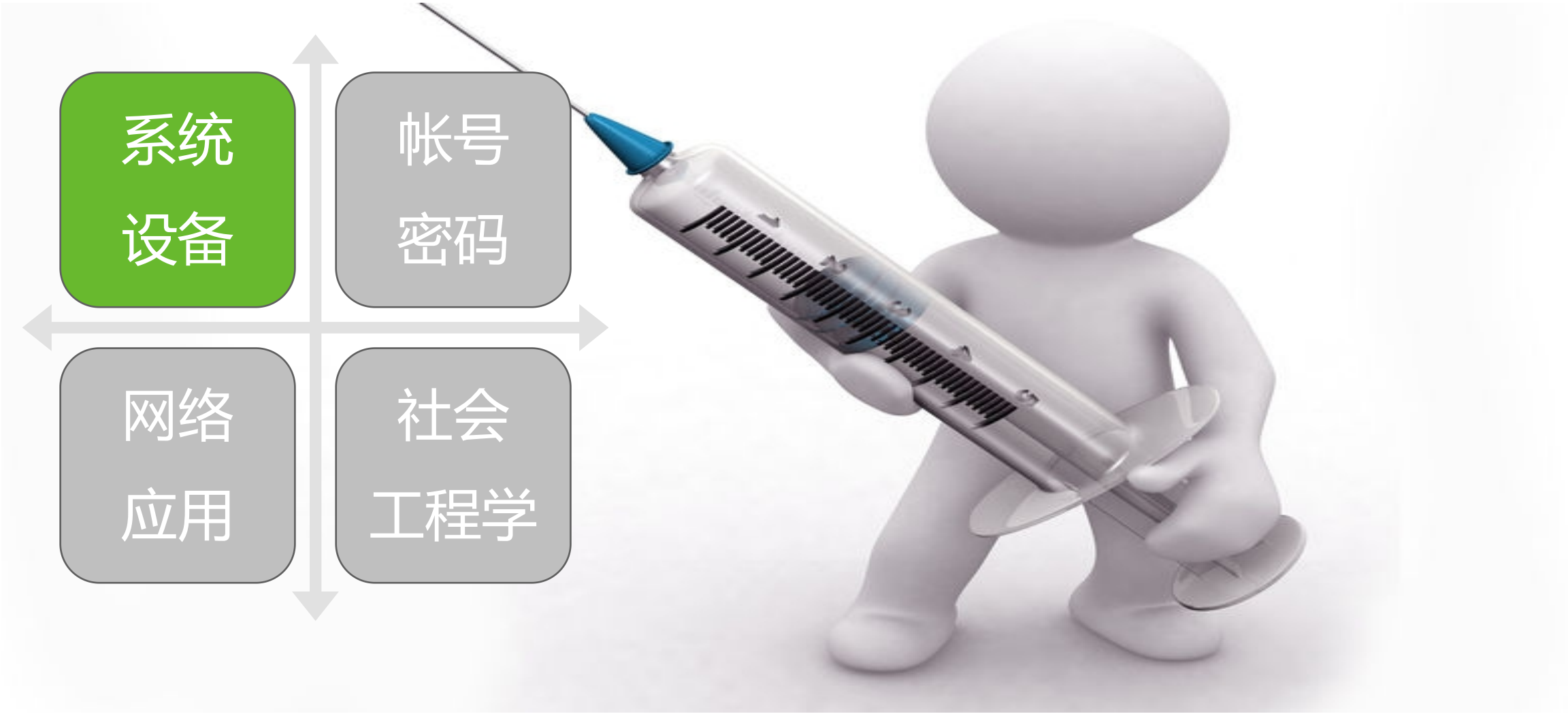
打动
奖品除了几家餐厅（包括他最喜欢的那家餐厅）的礼券外，还有他最喜欢的球队参加的比赛的门票

6

中招：
同意让克里斯给他发来一份关于募捐活动更多信息的PDF文档.当他打开PDF文档时电脑上已经被安装外壳程序

给所有职工的安全建议

- 系统设备
- 帐号密码
- 网络应用
- 社会工程学



操作系统

1. 安装防病毒软件，定期升级病毒库，定期查杀病毒
2. 配置操作系统补丁自动更新，及时修补漏洞
3. 设置用户帐号及密码，及时停用无用帐号，不留空口令
4. 关闭默认共享
5. 关闭自动播放

电脑

1. 设备出现故障，请联系信息管理中心，不要自行让外单位修理
2. 非单位资产的计算机等终端设备不能擅自接入单位内网
3. IP地址应按照单位要求进行设置，禁止私自更改固定IP
4. 离开终端前及时锁屏（Win+L键）

U盘

1. 未知U盘、移动硬盘等存储设备使用需谨慎
2. 存储设备使用前应先查杀病毒
3. 不要将重要的信息存储在U盘中；确需存储时采用加密U盘
4. 注意保管、防止丢失；若丢失应立即通知相关部门
5. 废弃设备应及对存储信息进行彻底可靠的销毁

手机

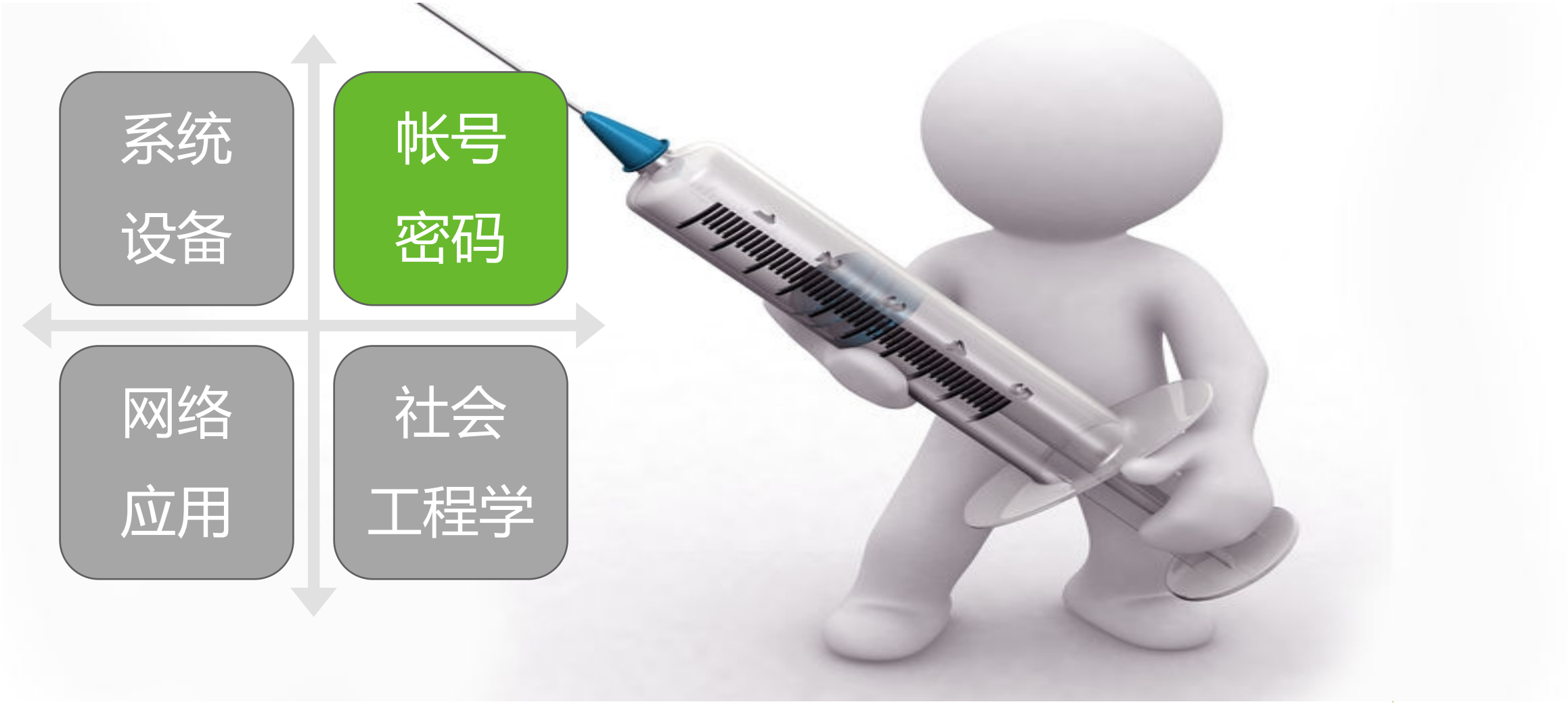
1. 设置锁屏
2. 切勿破解系统
3. 安装反恶意软件
4. 到官方应用平台下载APP应用
5. 不要将重要信息存储在手机内
6. 谨慎接入公共网络并传递机密数据信息

系统
设备

帐号
密码

网络
应用

社会
工程学



不少于8位

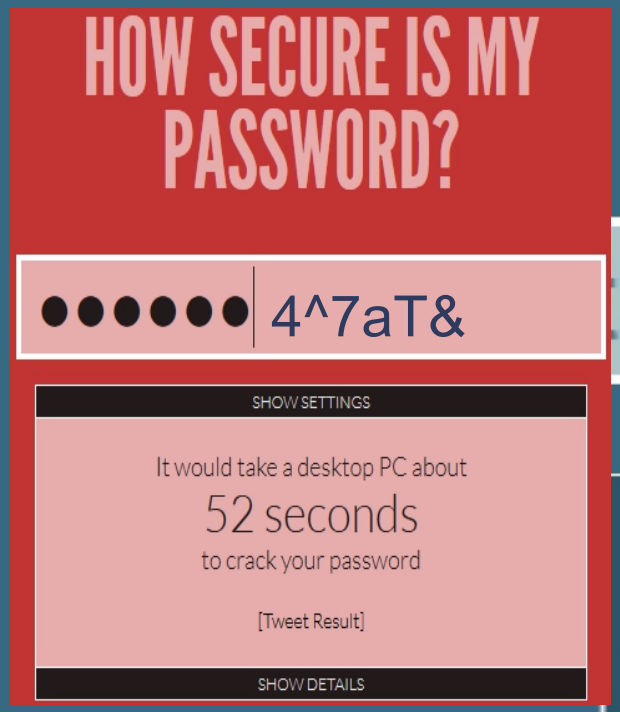
大小写组合

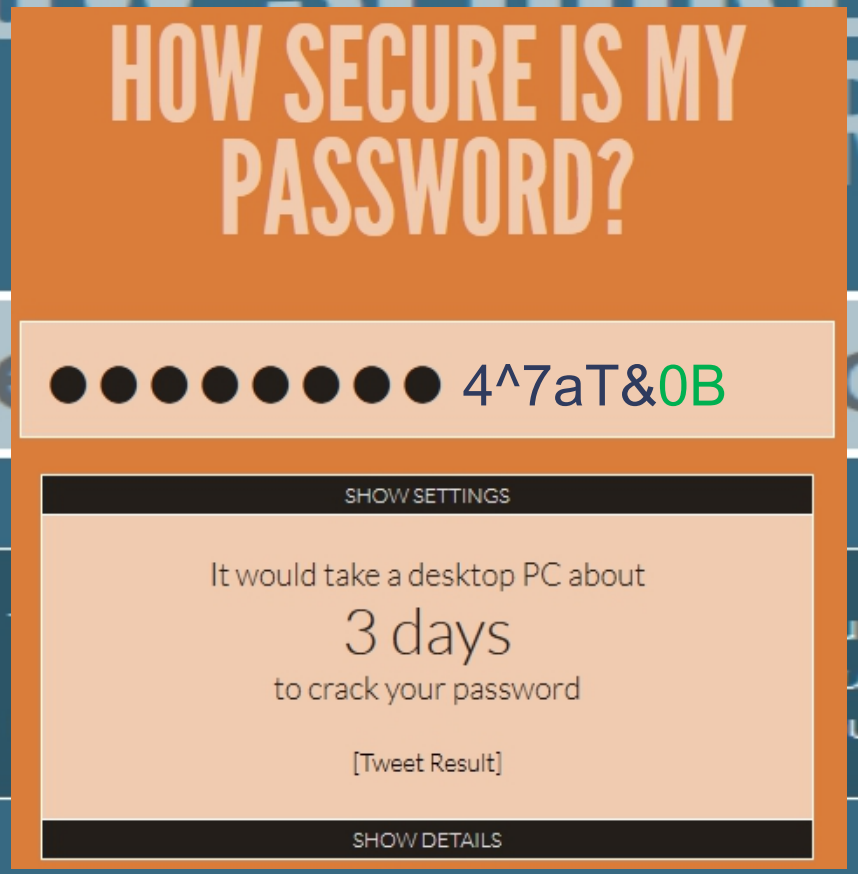
数字特殊符号

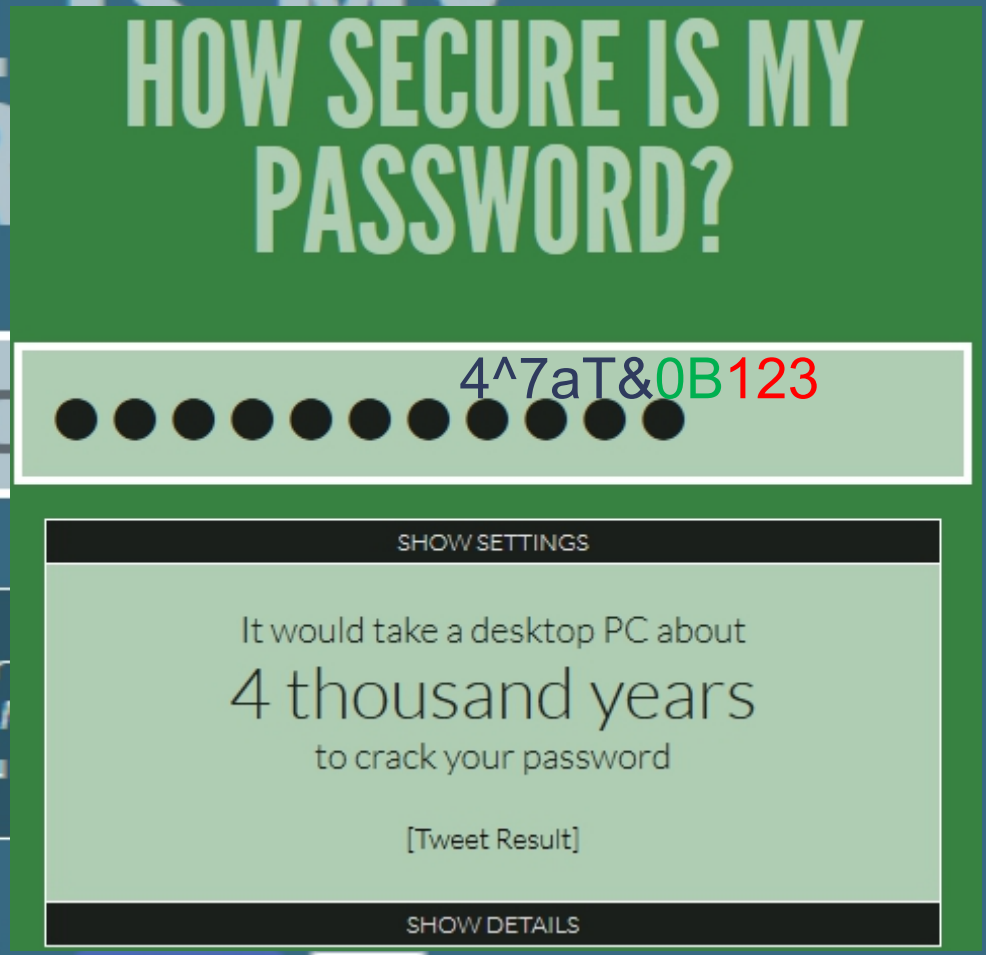
非常见字典单词

非常见用户名，宠物名等

https://howsecureismypassword.net/







Follow @hsimpnet

Like 8.1k

小测试

- 以下哪个是弱口令？你会选择哪个作为系统密码
- admin
- pssw0rd
- abc123!
- !3)dac21Yop@
- abcd@1234
- 1qaz!QAZ
- 19fzer+APP9_2019

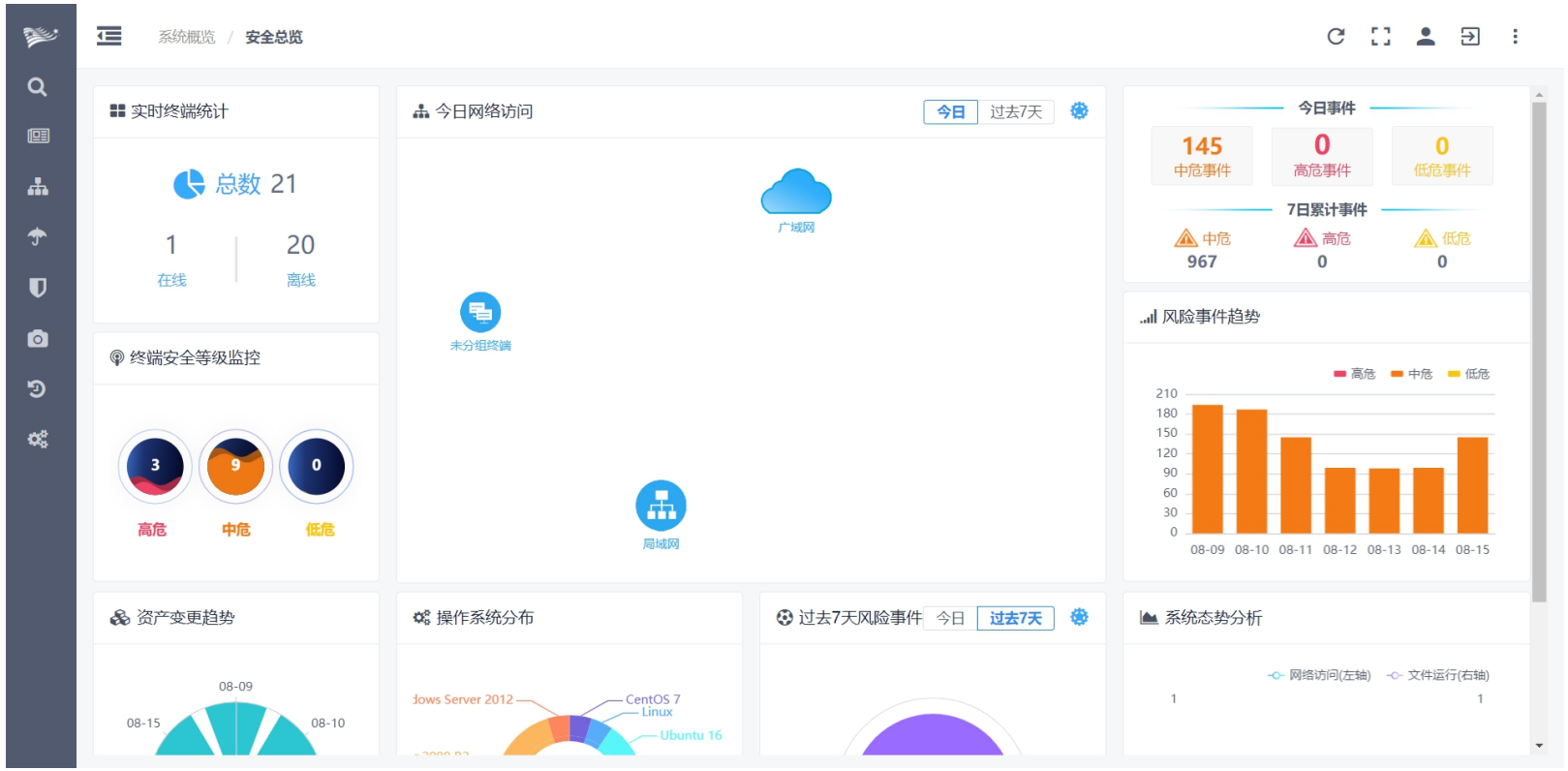
系统
设备

帐号
密码

网络
应用

社会
工程学

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。

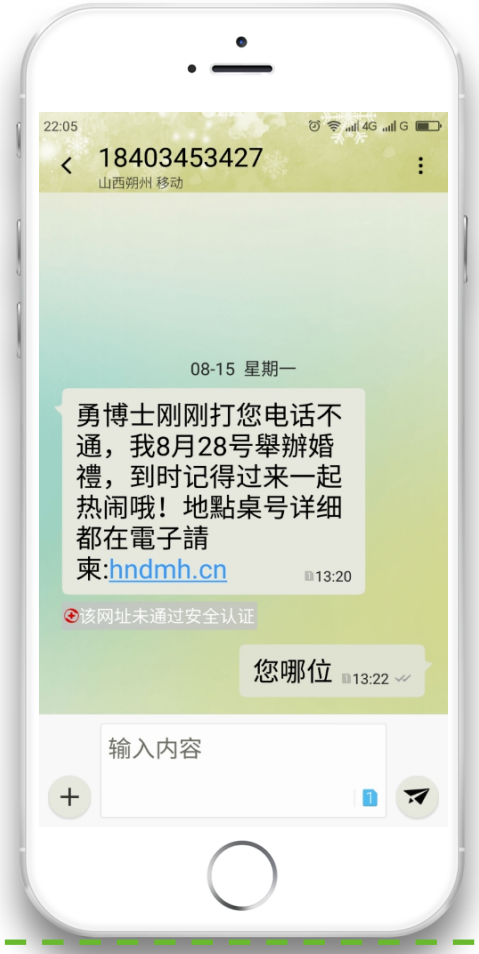
2017年5月，WannaCry勒索蠕虫利用漏洞永恒之蓝发起攻击，30个小时内就使100多个国家的大量机构陷入瘫痪。

陌生来电不轻信，不明链接不要点

诈骗电话与骚扰电话

伪基站的仿冒短信

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。

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位码生成器，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

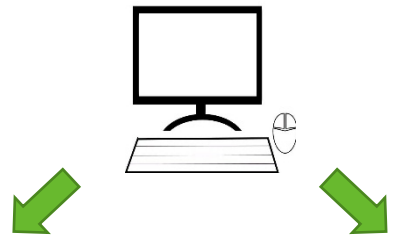
特别提示

- 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

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”。



文件恢复　　文件粉碎

文件恢复与文件粉碎功能

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

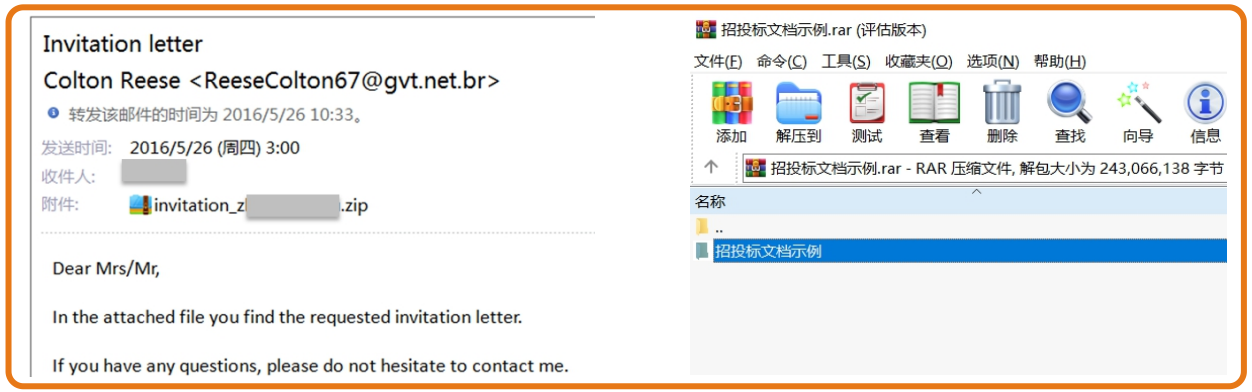
特别提示：

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。

邮件附件常带毒，陌生来源勿打开

勒索邮件

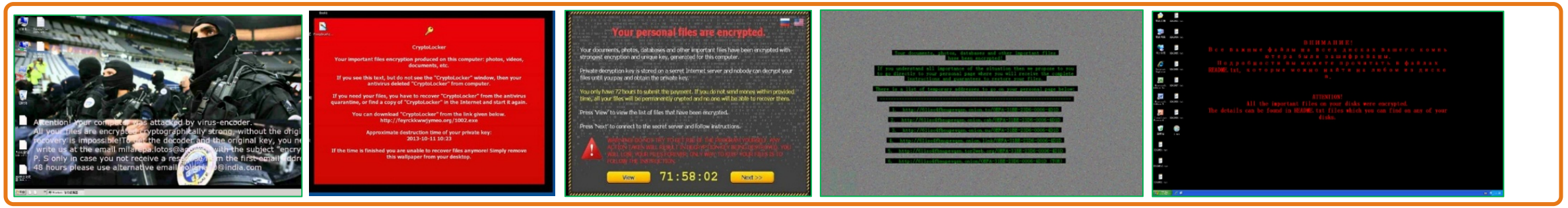
下面这封不起眼的邮件携带了一个ZIP格式的附件，解压后生成一个JS文件，它实际上是一个勒索软件，一旦点击打开，电脑中所有的办公文档、照片、视频都会被加密，只有向勒索者支付赎金后才能解密。



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



系统
设备

帐号
密码

网络
应用

社会
工程学

1. 提高安全意识
2. 辨别真假网站
3. 收藏夹打开网站
4. 安装安全软件屏蔽钓鱼网站
5. 连接地址和弹出图片谨慎点击

1. 不轻易相信陌生人发来的消息
2. 通过其他方式（如电话）确认对方身份
3. 对接收的文件进行病毒查杀
4. 机密信息和文件不要通过聊天工具发送
5. 不要谈论个人或学校机密信息

总结

安全上网建议

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

安全办公建议

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
连接WiFi要谨慎，蹭网心态吃大亏
二维码中藏奥秘，随手扫描易中招