福建卫生职业技术学院

2020年网络信息安全专题培训

2020年6月29日

请您
签到

2020年网络信息安全专题培训

扫描二维码进行签到

行政楼114会议室

2020-06-29 14:30 - 15:50

请您
签到

SANGFOR
深信服科技

网络信息安全专题培训

福建卫生职业技术学院 深信服科技

深信服 金欣 18695673207

主讲人简介：2014年毕业于西安交通大学，任职深信服安全解决方案专家，福建省网络与信息安全发展促进会副会长，具有CISP、CIIP-A、C-CCSK、ISO27001-Foundation等认证，曾出席第二届数字峰会分论坛担任演讲嘉宾，曾多次参与政府、医疗、教育、大企业等安全建设方案规划交流

SANGFOR
深信服科技

目录

SANGFOR
深信服科技

信息安全发展背景解析

安全意识

SANGFOR 深信服科技

概念

- 所谓的**安全意识**是指人们发现可能存在的威胁、判断其危害性并及时预防或化解威胁的一种能力。
- 加强自身对威胁相关知识的掌握以及正确的使用习惯可以提升这种能力。这也就是我们常说的提高安全意识。

必要

- 网络的基础元素是用户，网络应用的多样化、用户个体习惯的多样化。
- 对于学校来说网络安全主要是管理和制度的问题，对于个人来说网络安全主要是意识和使用习惯的问题。技术仅仅是辅助手段。

目的

- 从根本上认识到安全是自身的需求，而不仅仅是工作上面的要求；
- 增强自主安全意识，让养成良好的网络及系统使用习惯。

SANGFOR 深信服科技

背景一：法律监管

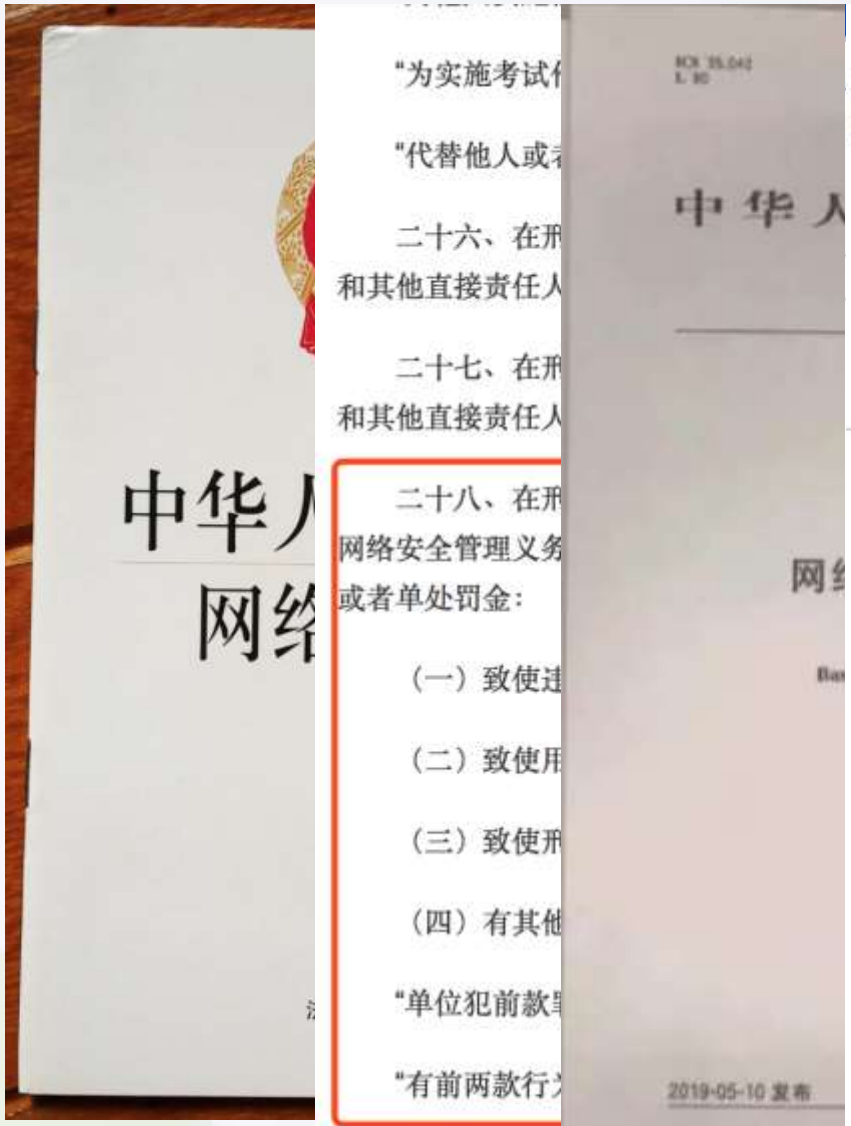
《网络安全法》、《刑法》（第九修正案）

《网络安全等级保护条例（征求意见稿）》

《网络安全等级保护基本要求》、《设计要求》等

《关键信息基础设施安全保护条例（征求意见稿）》

信息安全发展背景之一——法律监管



国家互联网信息办公室关于《关键信息基础设施安全保护条

见的通知

2017年07月11日 09:00:02　　来源：中国网信网

国家互联网信息办公室关于《关键信息基础设施安全保护条例（征求意见稿

为保障关键信息基础设施安全，根据《中华人民共和国网络安全法》，我办会同相关部门起草了稿）》，现向社会公开征求意见。有关单位和各界人士可以在2017年8月10日前，通过以下方式提出

一、通过信函方式将意见寄至：北京市西城区车公庄大街11号国家互联网信息办公室网络安全协见”。

二、通过电子邮件方式发送至：security@cac.gov.cn。

附件：关键信息基础设施安全保护条例（征求意见稿）

信息安全发展背景之二——个人信息与数据安全

SANGFOR 深信服科技

背景二
个人数据和隐私安全事件会更加突出

信息安全发展背景之二——个人信息与数据安全

SANGFOR 深信服科技

为了数据背后的利益
黑客会想尽办法入侵！窃取！

徐玉玉事件

时间：2016年8月21日

泄露规模：五万余条山东省2016年高考考生信息

行业：教育

事件简介：

- 2016年，以568分的成绩被南京邮电大学英语专业录取。
- 2016年8月21日，刚接到大学录取通知书的山东临沂市高三毕业生徐玉玉接到诈骗电话，对方声称有一笔2600元助学金要发放给她。在这通陌生电话之前，徐玉玉曾接到过教育部门发放助学金的通知。由于前一天接到的教育部门电话是真的，所以当时他们并没有怀疑这个电话的真伪。
- 随后被告人陈文辉等人以发放助学金的名义，骗走了徐玉玉全部学费9900元，徐玉玉在报警回家的路上猝死。

攻击过程简述：

- 犯罪嫌疑人陈文辉租住房屋，购买手机、手机卡、无线网卡等工具，从犯罪嫌疑人杜天禹手中购买五万余条山东省2016年高考考生信息，雇佣郑贤聪、黄进春冒充教育局工作人员以发放助学金名义对高考录取生实施电话诈骗。其间，郑金锋又与陈文辉商议，由郑金锋负责提取诈骗所得赃款。在得到“得逞后抽成10%好处费”的约定后，郑金锋联系陈福地，由陈福地向郑金锋提供多张用于实施诈骗的银行卡。后郑贤聪拨打徐玉玉电话，骗取其银行存款9900元。得手后，陈文辉随即让郑金锋在福建省泉州市取款，郑金锋随后又指挥熊超将9900元提取。

信息安全发展背景之三——内部人员风险行为带来安全威胁

背景三
教职工风险行为成为攻击发起点

信息安全发展背景之三——内部人员风险行为带来安全威胁

入侵政府网站篡改考试成绩案件：

9名被告人从多家医院的财务工作者和5家会计从业资格考试培训机构的学生中招揽没有通过考试的考生，以3000元至1.1万元不等的价格承诺为其修改成绩。后来，这9名被告人又多次通过QQ联系“黑客”入侵内蒙古财政厅的网站篡改成绩，将多名考生的成绩由“不合格”改为“合格”，致使多名本不该取得会计从业资格证的考生取得了从业资格证。

安全事件分析：教育局相关人员不规范的电脑操作行为，对陌生邮件没有足够的重视，随意点击不明链接，导致主机被黑客控制，从而利用主机权限植入恶意脚本，窃取录入权限的账户信息

安全事件

SANGFOR 深信服科技

20-30%

- 由黑客入侵或其他外部原因造成

70-80%

- 由于内部教职工的疏忽或有意泄露造成的

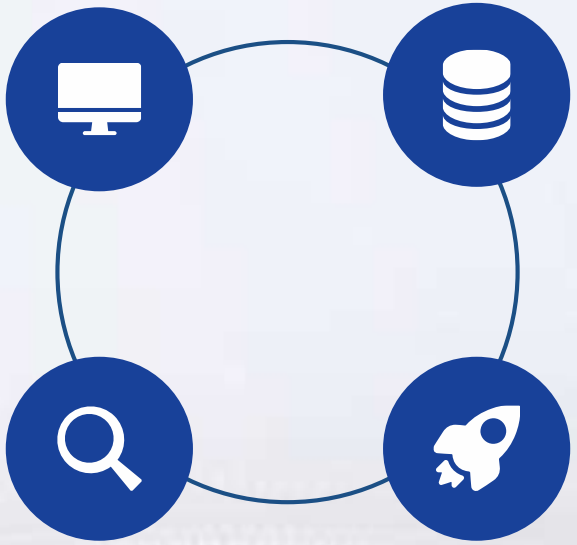
78%

- 来自内部教职工的不规范操作

威胁无处不在

人员威胁

黑客渗透、木马后门、病毒蠕虫、流氓软件、拒绝服务、社会工程等



自然威胁

洪水、台风、地震、雷电等

系统威胁

系统漏洞、敏感端口开放、弱密码、网络或服务故障等

环境威胁

电源故障、污染、液体泄漏、火灾等

面对信息安全，我们需要保持清醒的认识

SANGFOR 深信服科技

SANGFOR
深信服科技

常见网络安全风险与应对方法

一、木马、病毒等

什么是木马和病毒？通俗来讲

木马：控制你电脑的一段恶意代码

病毒：破坏你电脑功能或存储的文档数据的恶意代码

本质：恶意代码被执行

哪些行为可能会使你的电脑中毒

- 浏览网站——主动或被动浏览非法网站
- 电子邮件——打开不明邮件链接或下载附件
- 移动存储介质——U盘、移动硬盘、手机
- 即时聊天——引诱点击或下载不明文件或打开不明链接（仿造链接，例如www.tmalI.com等）
- 网络下载——论坛、各类资料库等等免费资源
- 网络共享——FTP、企业网盘等

一、木马、病毒等防范方法

SANGFOR 深信服科技

意识先行！！！ 不明后缀的文件一定要谨慎点击运行

- **安装防病毒软件和主机防火墙**

  尽可能安装正版防病毒软件，并及时更新病毒库；内网环境也要关注，配合信息安全机制落地

- **及时备份关键数据、资料**

  对于个人数据及时通过移动介质、云盘等方式备份；学校或组织关键信息由组织统一协调备份

- **及时更新操作系统补丁**

  不要随意关闭系统自动更新，或通过终端软件及时更新补丁

- **U盘等外设管理**

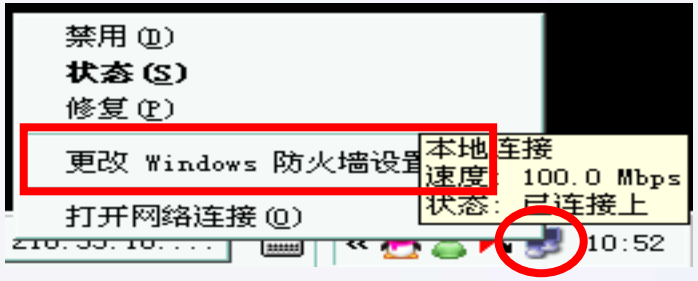
  避免U盘随意插拔，如有业务上的必要尽量做到专机专用

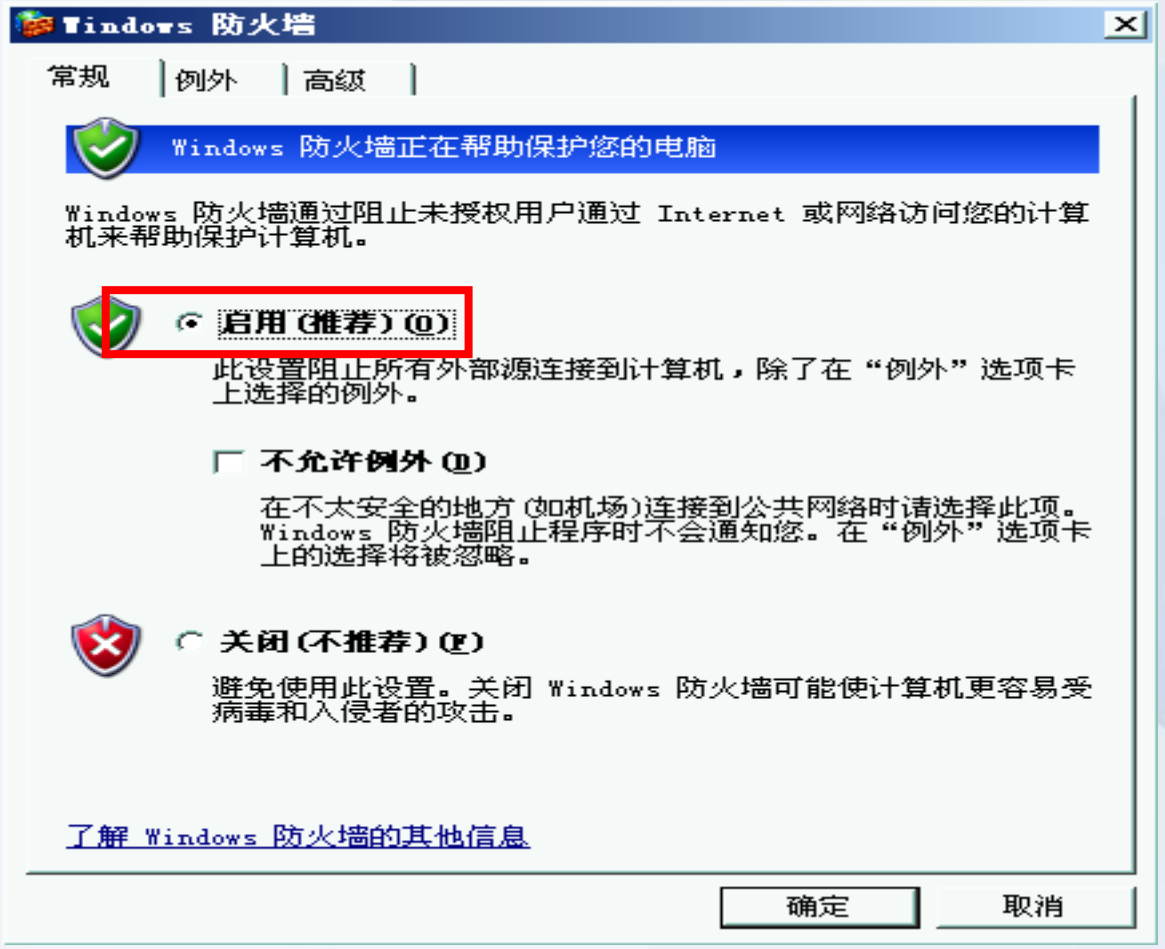
  强调：在禁止插拔U盘的场景下，不要随意将手机连接电脑，即使是仅为了充电

- **积极配合信息安全部门相关政策**

开启防火墙

鼠标右键点击计算机屏幕右下角网络连接标志

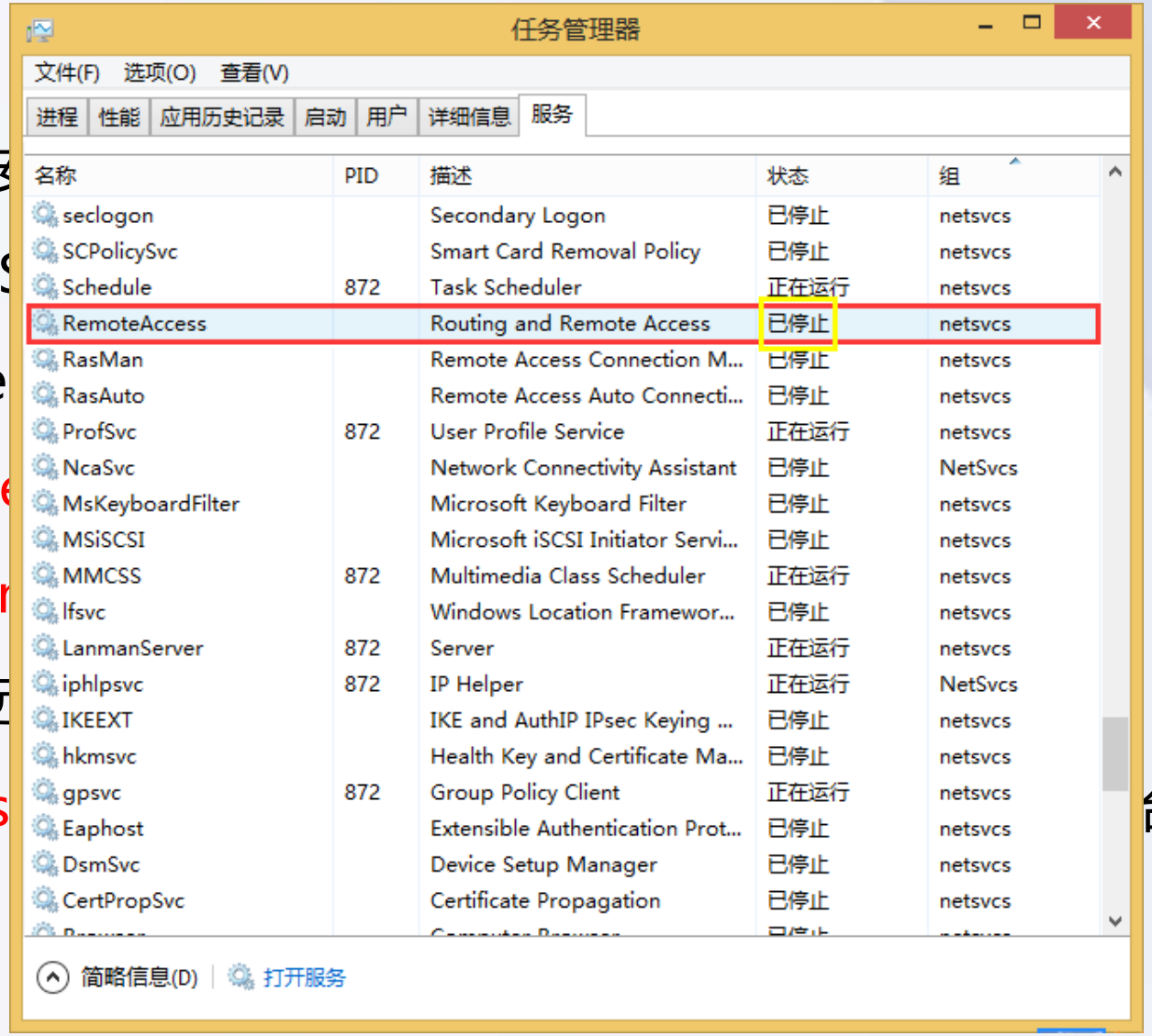




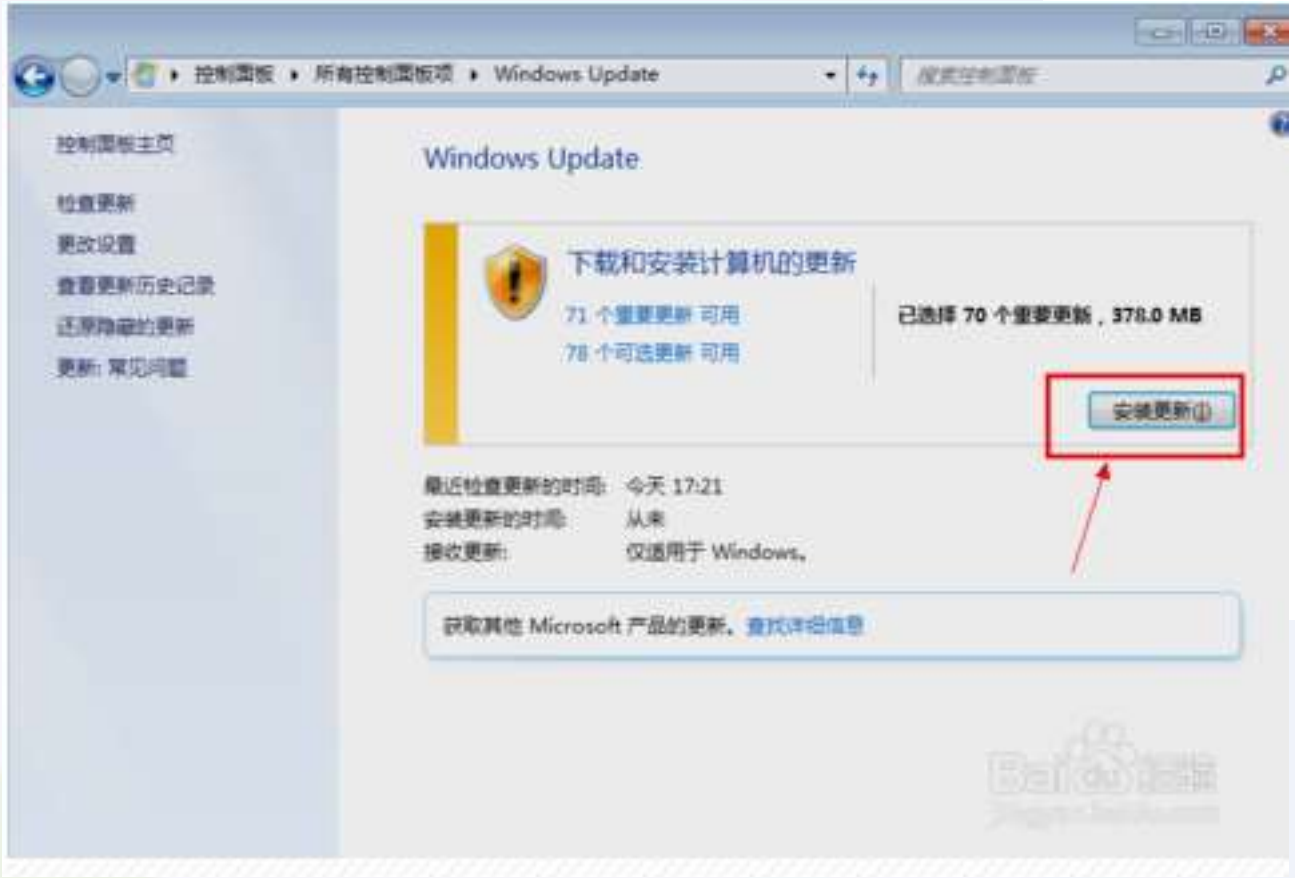
服务配置

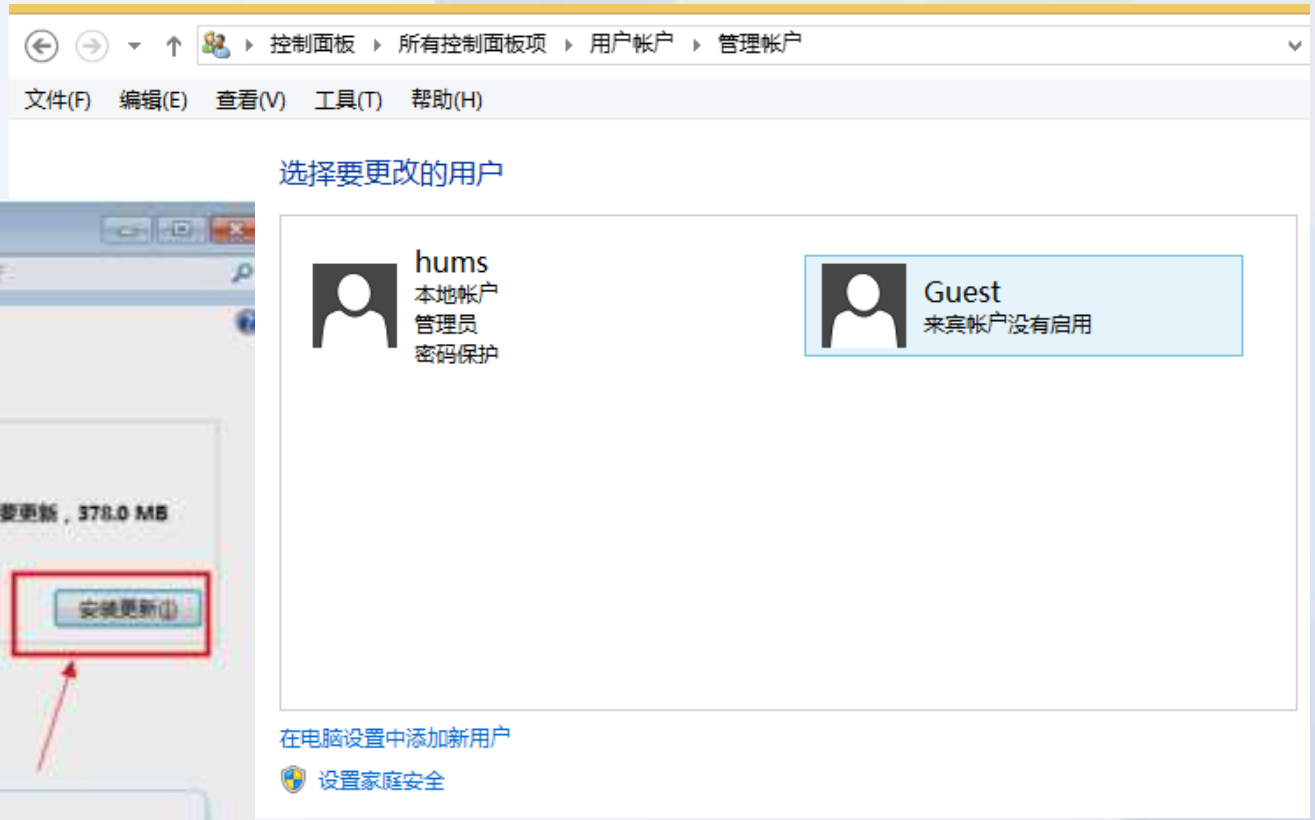
- 建议禁用的不安
  - Fast User S
  - Messenge
  - Remote Re
  - Routing an
  - Telnet （远
  - Terminal s

台机器）



其他简单措施





腾讯安全管家等进行补丁的更新；

二、信息泄露

大数据时代

- 个人信息数据变成高价值资产，个人信息类型也变得更加多样复杂，存在有意或无意泄露的情况

黑灰产

- 各类互联网公司为了更加准确分析，通过交易的方式获取私人信息，由此滋生黑灰产

危害学校

- 个人信息泄露不仅关乎个人隐私，对学校和教育局形象危害也很大，例如密码字典

二、信息泄露防范——数据安全

公开	内部公开	秘密	机密、绝密
Public	Internal Use（缺省）	Confidencial	Secret

数据保密管理（举例）

- 根据需要，在合同或个人协议中明确安全方面的承诺和要求；
- 明确数据管理人员责任，控制数据使用及分发；
- 明确部门在使用授权数据时的保护责任；
- 基于业务需要，决定是否对重要数据进行加密保护；
- 软件开发剩余信息保护

数据保密使用（举例）

- 学校数据文件职工有责任和义务保护，防止数据泄漏
- 个人电脑不存储敏感数据，严禁私自拷贝业务数据带离工作场所
- 纸质文件指派专人保管，定期销毁
- 纸质文件打印件应设置标识，及时取回，并妥善保存或处理
- 禁止将客户数据或客户标识用于非项目相关的场合如培训材料；

二、信息泄露防范——个人数据

不泄露

- 查看社交网络或应用的隐私设置，保护自身敏感信息
- 在社交网络谨慎发布、公开个人信息

不留底

- 不要在电脑上自动保存重要系统或应用的口令
- 打印、借用他人电脑时，确保关键资料不被复制或留存在回收站

不相信

- 不要忽略各类APP的权限获取内容，避免被恶意搜集
- 不要参与不规范的网络、街头市场调研，防止个人信息被利用

法律支持

- 国家目前正积极推进《个人信息保护法》的颁发，对于有侵权行为，要及时运用法律武器

三、密码管理——弱密码

- 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
- 黑客攻击最常用的手段是利用密码字典进行爆破

现实是

- 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

我们从现状看看弱密码情况！

三、密码管理——密码设置建议

密码长度应尽量长

- 密码长度增加是最好的防破解方式
- 密码长度不低于8位
- 一定要记得住，不要写在纸上

密码需要具备复杂度

- 多字符混合
- 至少包含大小写字母和数字

用户名与密码一致

- 黑客破解字典中一定有用户名

尽量不用自身常见信息为密码

常见信息包含：

- 生日、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

不要所有系统使用同一密码

- 通过普通会员卡等密码匹配关键密码的方式是最常见的破解方法

密码定期更换

- 保持一定的评率对密码进行更新
- 未破解密码更新可固定几个密码轮换

三、密码管理——一些小技巧

口使用一些喜欢的诗句、名言俚语、容易记得顺口溜等等，通过一定规则变换

- 例子1：

密码： 1/2Jss1/2J#f00

解释：半江瑟瑟半江红

- 例子2：

密码：Quit@smoking4ever

解释：永远戒烟

口对于不同系统间的用户名可以在口令上加入前后缀

- 例子1：

密码根： 1/2Jss1/2J#f00

网易邮箱：1/2Jss1/2J#f00%Wmail

OA系统： 1/2Jss1/2J#f00%OAsys

四、安全浏览网页

- 使用安全浏览器（从官网下载）
- 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，特别是重要系统账号

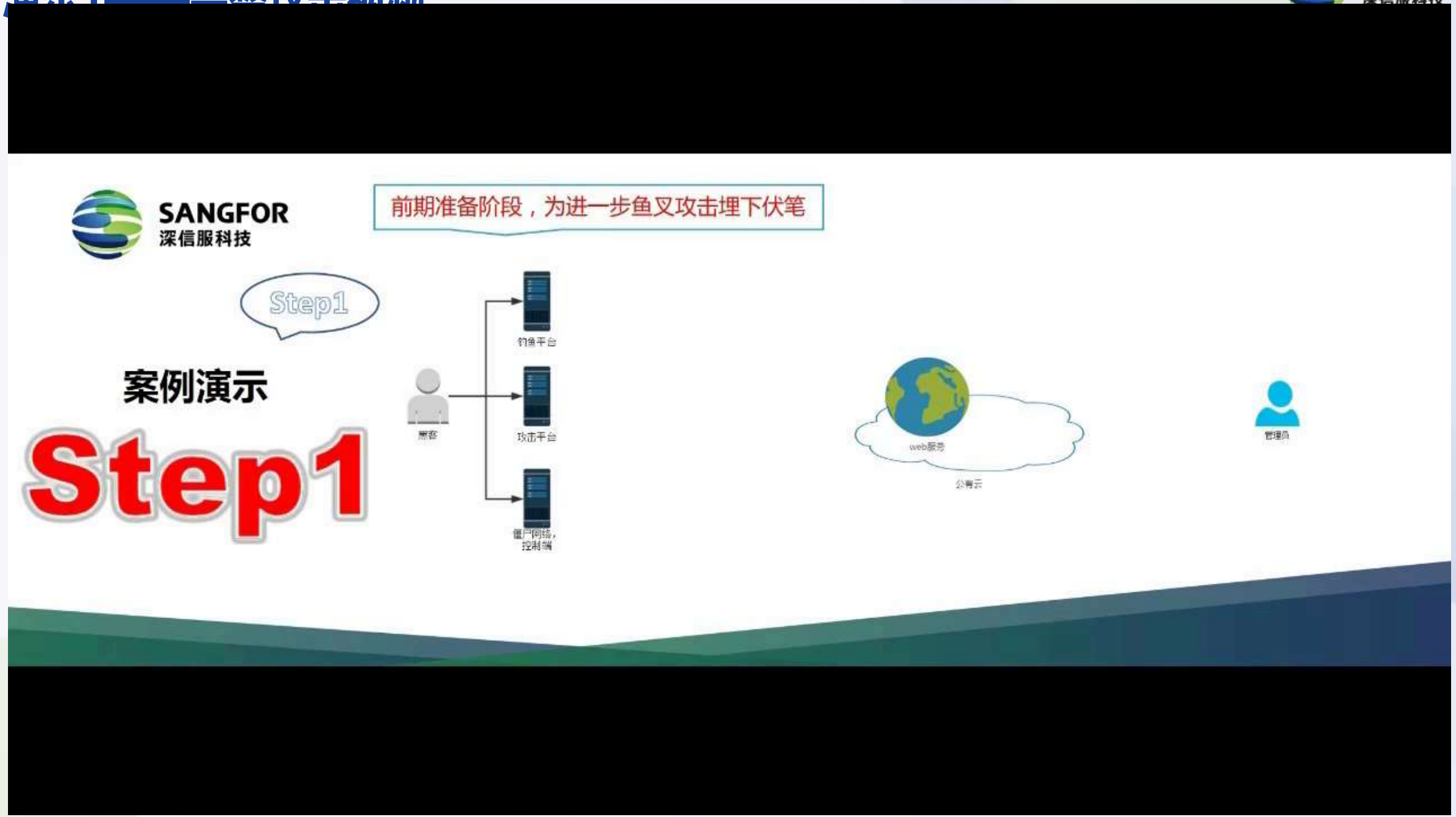
五、电子邮件使用安全

- 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。

五、电子邮件使用安全

- 业务与工作往来尽量使用企业级邮箱，禁止使用个人有限
- 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

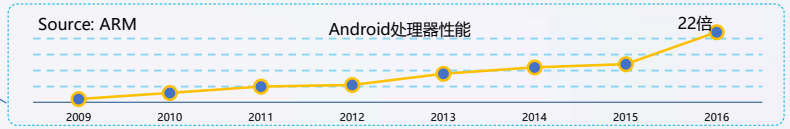
演示1——完整攻击视频


SANGFOR
深信服科技
前期准备阶段，为进一步鱼叉攻击埋下伏笔
Step1
案例演示
Step1
钓鱼平台
攻击平台
僵尸网络，
控制端
web服务
公有云
管理员

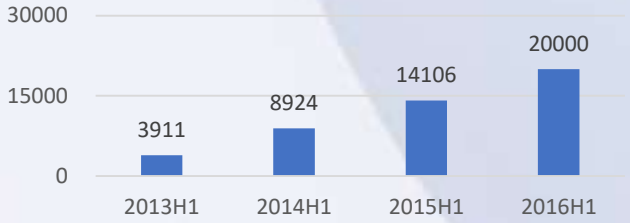
六、移动终端风险——趋势

- 用户App下载量剧增，手机流量的使用持续快速增长

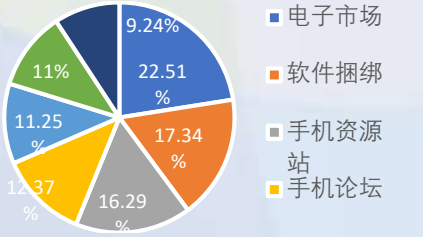
- 智能手机性能提升，移动应用体验增强

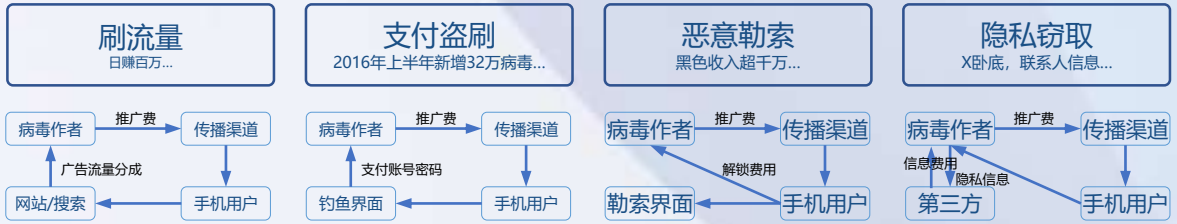


2013-2016年，手机木马病毒感染用户年增长72.3%



多种恶意软件传播渠道





- 移动终端及APP的使用成为了主要的生活和办公方式
- 各种各样的APP都在采集你的信息，泄密通道多、互联网传播快
- 自带设备（BYOD）在个人场景和业务场景之间切换的情况成为主流
- 电话诈骗之外，移动端的黑色产业链发展飞速，并形成许多自动化工具，降低攻击成本

六、移动终端风险——注意事项

保持系统更新

目前，Android中被发现逾800个安全缺陷。而iOS的封闭特性，使得研究人员很难发现它内部的“奥秘”，但并不代表绝对安全。”

保持关键应用更新

厂商们发布新固件往往都是修复大量Bug和漏洞，应用程序也是如此，即便新固件存在新问题，也能够让你的手机暂时更为安全。

六、移动终端风险——注意事项

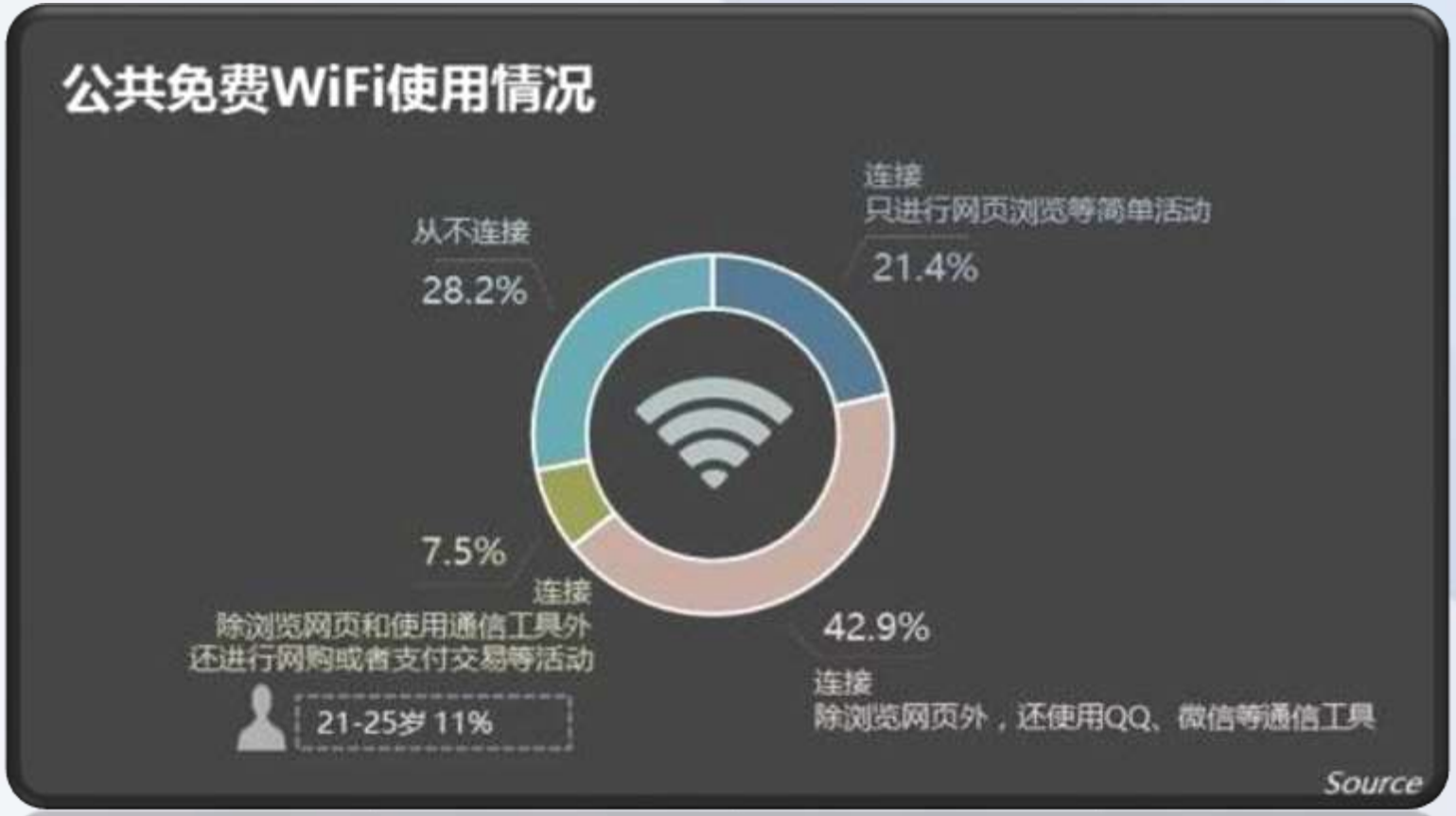
明确责任条款——用户协议关注度需得到提升

- 在下载软件或者注册网站之前，通常需要同意一些用户协议，对这些协议，仅有22%的用户会仔细阅读其内容，觉得合理才注册或下载。另有26%的用户表示从来都不关注这些用户协议。
- 用户协议往往关系到个人信息保护和责任条款，广大用户应该提升关注意识

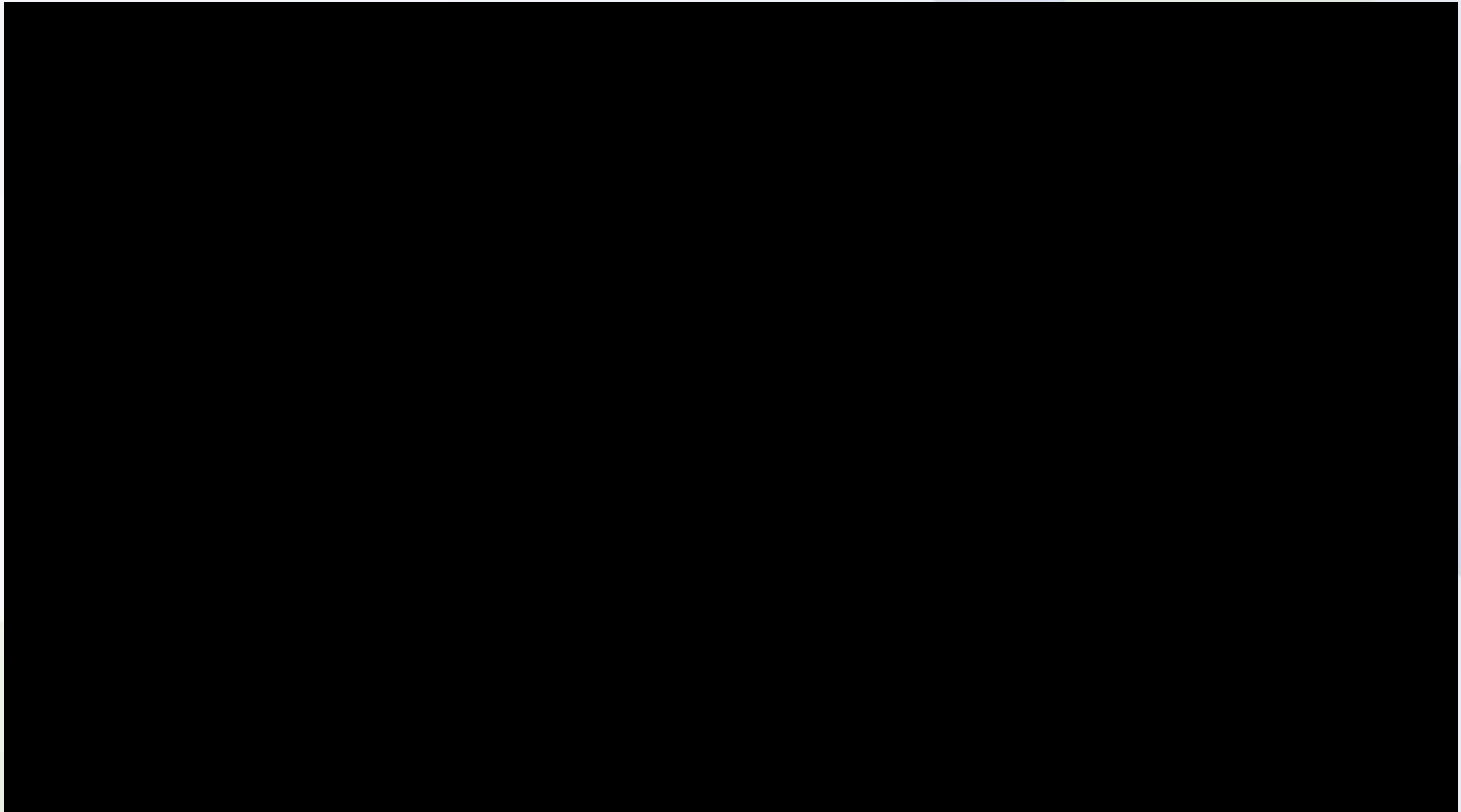
六、移动终端风险——注意事项

连接公共WIFI要谨慎——警惕钓鱼WIFI

- 72%的用户会在手机上使用公共免费WIFI，其中，64%的用户连接公共WIFI进行网页浏览，使用社交通讯工具，7.5%的用户还会进行网上支付。
- 不要随便连接公共场所的不明WiFi，尽量不要通过公共WiFi进行网上支付



演示2——钓鱼WIFI



六、移动终端风险——注意事项

谨慎打开网站、软件定期杀毒

- 在手机安全危害的防护措施上，用户最常用的是“只打开可信任的网站”、“下载手机杀毒软件”，针对前者，iOS系统用户使用的较多，而安卓系统手机用户则使用后者较多。
- 还有13.1%的用户并没有采取一定的手机安全危害防护措施，无疑这类用户的手机安全危害风险会更高。

SANGFOR
深信服科技

THANK YOU

安全意识培训