

2015年教职工信息技术培训

- 上海师大智慧校园介绍
- 智能终端的信息安全



上海师大智慧校园

微信企业号服务介绍



上海师范大学信息化办公室
Informatization Office of Shanghai Normal University

主要内容



智慧校园微信企业号简介



如何关注



更优服务



上海师范大学信息化办公室

Informatization Office of Shanghai Normal University

智慧校园微信企业号简介

精准

安全

便捷



建设历程

2014年10月

- 申请微信企业号

2014年12月

- 微信企业号架构和服务应用初建

2015年3-4月

- 师生需求调研、公共服务应用丰富

2015年5-6月

- 试点单位推广

2015年7-8月

- 应用服务建设

2015年9月

- 学生用户推广试用
- 数理学院试点推广

2015年10月

- 迎校庆微信企业号正式推广



上海师大智慧校园 CAZMPUS SERVICE MANAG.
COMVIANT QUICK CLEAR SMART



定位

对接学校各类
校内业务

为师生提供一
站式移动服务



综合业务
管理应用

教学科研
支撑应用

校园公共
服务应用

统计分析
决策应用

...

校公共数据库

历史数据仓库



上海师范大学信息化办公室

Informatization Office of Shanghai Normal University

功能简介

四大服务板块

公共
服务

教师
服务

学生
服务

管理
服务



上海师范大学信息化办公室

Informatization Office of Shanghai Normal University

功能简介

公共服务



校园卡信息查询与业务办理



徐汇、奉贤校区校内办公电话一览表



我的二维码证件



课程表



上海师范大学信息化办公室

Informatization Office of Shanghai Normal University

功能简介

教师服务



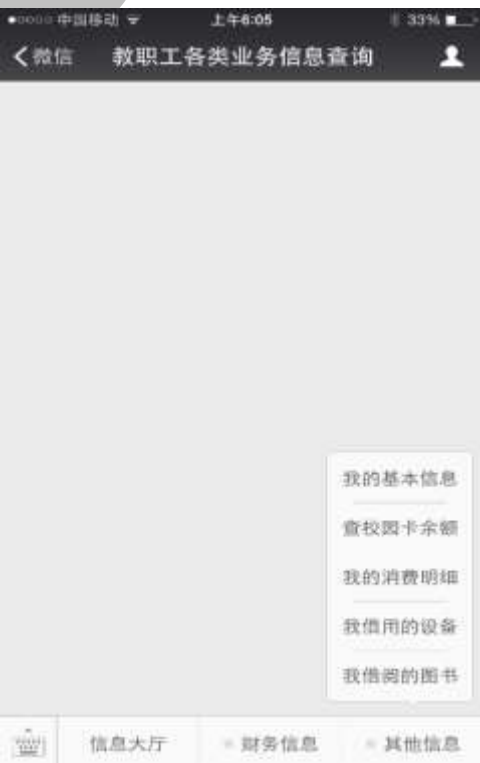
教职工各类业务信息查询



教职工奉贤校区住宿预约登记



我所在部门的成员通讯录



功能简介

学生服务



学生各类业务信息查询



学费缴纳情况查询



功能简介



人文与传播学院信息服务窗



商学院信息服务窗



生命与环境科学学院信息服务窗



教育学院



人文学子



生环学子



马院学子



对外汉语学子



法政学子



团委



财务处



信息化办公室服务区

管理服务

- 学院、部门自己建设管理的个性化应用
- 提高服务效能的应用



上海师范大学信息化办公室

Informatization Office of Shanghai Normal University

如何关注



二维码扫描



搜索企业号



上海师范大学信息化办公室
Informatization Office of Shanghai Normal University

二维码扫描关注

- 将二维码通过任何方式发送给同事扫码关注，例如通过邮件方式发送二维码或者集会扫码。



搜索企业号关注



输入“上海师大智慧校园”



关注成功

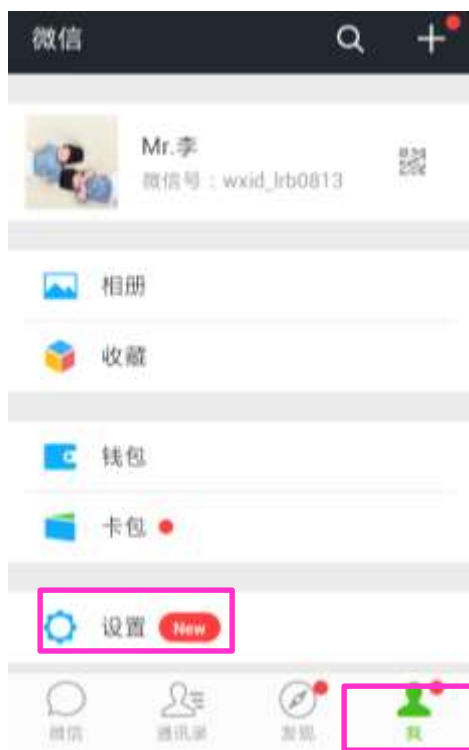
- 成功关注的用户在上海师大智慧校园企业号中即时显示有权限的应用列表



未成功关注
需要身份验证

如何查看微信是否已经绑定手机或邮件

- 登录微信后，点击“我”，再点击“设置”
- 点击“帐号与安全”
- 查看“手机号”或“邮件地址”是否绑定



通过智慧校园小助手完成身份验证

关注身份验证

关注身份验证

10月10日



请点击图文进行身份验证以成功关注“上海师大智慧校园”

通过管理后台
预设的手机或
学校的邮箱收
取验证码，完
成验证

绑定卡号



绑定校园卡卡
号，通过学校
统一身份认证
完成验证



上海师范大学信息化办公室

Informatization Office of Shanghai Normal University

通过手机或邮件进行验证



注意:

- 认证手机号码须为微信管理后台绑定的号码;
- 认证邮箱须为学校邮箱。

绑定卡号验证

- 智慧校园小助手菜单【绑定卡号】
- 填写校园卡卡号、输入校统一身份认证密码。
- 微信号、手机号与邮箱必须至少填写一项，才能提交验证信息。

64321010



中国移动 3G 72% 20:46

上海师范大学智慧校园企业...

校园卡卡号 (必填)

1000347

统一身份认证密码 (必填)

.....

本微信号

填写微信号

本微信绑定的手机号

188

本微信绑定的邮箱

填写邮箱

说明：本微信号、本微信绑定的手机号、本微信绑定的邮箱必填其一，使用校园卡号及统一身份认证密码进行身份认证，认证完成后将绑定本微信和您的校内身份。
注意：每个校内身份只能绑定一个微信号，请仔细核对，如有疑问请联系信息办。

提交

更优服务



WHAT I CAN DO



上海师范大学信息化办公室
Informatization Office of Shanghai Normal University

- J
-  校内各部门成员通讯录
-  校园卡信息查询与业务办理
-  教职工奉贤校区住宿预约登记
-  教职工各类业务信息查询
- K
-  课程表
- W
-  我的二维码证件
-  无线上网临时帐号申请
- X
-  信息化办公室服务区
-  徐汇、奉贤校区校内办公电话一览表

F
G
J
K
W
X
Z

你所看到的每个应用，都将为您带来便捷、精准、安全、贴心的服务.....

Surprise!



教职工各类业务信息查询

- 收到工资短信时，您是否希望能更快了解所发放工资各项目的具体金额？绩效明细？
- 您知道您负责管理的所有设备信息么？
- 您的人事信息是否及时更新了？





教职工各类业务信息查询

- 教职工各类业务信息查询系统已经整合了学校各相关业务系统的权威数据，包括：财务系统、图书借阅管理系统、人事管理系统、设备管理系统、校园卡系统等。





教职工各类业务信息查询

- 财务信息——选择查询年月，查看具体明细
 - 个人工资查询、绩效明细查询、住房公积金、养老保险

个人工资查询结果

你的校园卡号 1000307556

发放年月: 2015年10月

项目名称 (类别)	发放金额(元)
岗位工资(C)	■■■■.00
岗位工资补(C)	0.00
薪级工资(C)	■■■■.00
薪级工资补(C)	0.00
交通补贴(C)	■■■■.00
交通补贴补(C)	0.00
独生子女费(C)	0.00
独生子女补(C)	0.00
粮油补贴(C)	■■■■.00

住房公积金查询结果

你的校园卡号 1000307556

公积金账号: 119580871

缴存月份	发公积金 (单位缴存部分)	扣公积金 (月缴存额)
2015年10月	■■■■.00	■■■■.00

说明: 每月15日后学校进行公积金汇缴工作, 实际到帐时间以公积金中心数据为准。

绩效明细查询

查询年月

最近一月

年月

查询

< > 完成

最近一月

指定年月

最近一年

最近两年

最近三年

全部 (查询时间较长)





教职工各类业务信息查询

○ 其他业务信息——

- 个人信息、图书借阅信息、仪器设备信息、一卡通余额、一卡通消费



一卡通消费查询		
您的校园卡号: 1000307856		
本次查询共有10条消费记录。		
地点	方式/金额	消费时间
新玉兰	消费 2.00	10月27日 07时26分
海内蓝包	消费 7.00	10月26日 12时26分
普陀餐厅	消费 4.00	10月26日 12时12分
新玉兰	消费 3.10	10月26日 07时47分
新玉兰	消费 2.00	10月26日 07时39分
海内蓝包	消费 7.00	10月23日 12时26分
普陀餐厅	消费 4.00	10月23日 12时12分
新玉兰	消费 2.40	10月23日 07时20分
东北水饺	消费 20.00	10月22日 18时10分
普陀餐厅	消费 4.00	10月22日 12时00分
新玉兰	消费 2.00	10月22日 07时20分
普陀餐厅	消费 7.00	10月21日 11时39分



校园卡信息查询与业务办理

- 校园卡日常使用中会遇到很多问题.....



卡内余额不够了!

校园卡的密码忘记了!

食堂阿姨多打了三五毛!

不知不觉的大额消费!

校园卡找不到了!!!



刚挂失的校园卡又找到了!!!



校园卡信息查询与业务办理

- 校园卡信息查询与业务办理，让师生们能够更方便、更安全地使用校园卡。
 - 立即充值：微信支付分分钟搞定余额不足
 - 信息查询：实时了解校园卡消费充值结果
 - 卡务办理：自助办理个人卡务事宜，免去了去现场人工办理的麻烦。

及时！ 高效！ 安全！



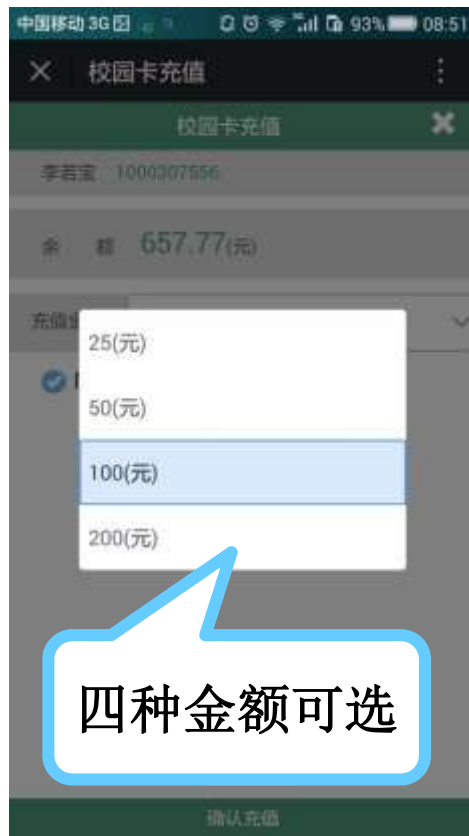
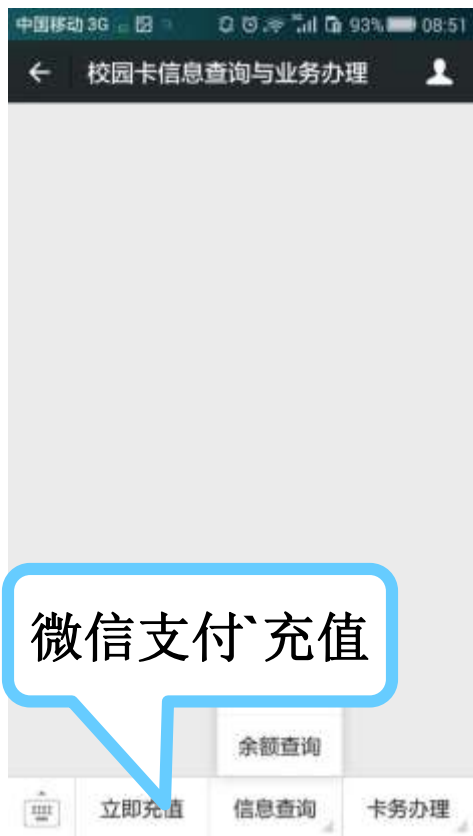
上海师范大学信息化办公室

Informatization Office of Shanghai Normal University



校园卡信息查询与业务办理

- 立即充值——**微信支付**方便快捷
点击“立即充值”，想充就充！





校园卡信息查询与业务办理

○ 信息查询——消费充值、余额查询



你的校园卡号 1000307556

本次查询共有93条消费记录。

地点	方式/金额(元)	消费时间
新玉兰	消费 2.40	10月23日 07时32分
东北水饺	消费 20.00	10月22日 18时16分
教师餐厅	消费 6.00	10月22日 12时06分
新玉兰	消费 2.00	10月22日 07时33分
教师餐厅	消费 7.50	10月21日 11时39分
教师餐厅	消费 1.60	10月21日 07时54分
教师餐厅	消费 1.40	10月21日 07时53分
教师餐厅	消费 6.00	10月20日 12时09分
新玉兰	消费 3.10	10月20日 07时38分
教师餐厅	消费 6.00	10月19日 11时55分
新玉兰	消费 2.40	10月19日 07时33分
教师餐厅	消费 6.00	10月16日 12时10分



余额 **657.77**(元)

状态 使用

由于数据传输到本系统存在延时现象，所查余额仅作参考。

可查询2个月之内的记录!





校园卡信息查询与业务办理

- 卡务办理——密码重置、挂失及解挂、大额消费提醒





教职工奉贤校区住宿预约登记

- 今年9月，配合《上海师范大学奉贤校区教职工夜间住宿管理办法》的实施，上海师大智慧校园推出了教职工奉贤校区住宿预约的应用。



上海师范大学奉贤校区教职工夜间住宿管理办法

为更好地做好保障服务工作，为因工作需要夜间留在奉贤校区住宿的教职工提供良好的休息场所，学校结合奉贤校区的实际情况，整合现有教职工的临时住宿房源，制定本办法：

一、入住对象

因工作需要夜间需在奉贤校区住宿的在编在岗教职工。

二、住宿房源

1. 32号宿舍 (免费)
2. 迎宾楼 (免费)

三、住宿规定

1. 教职工根据本人工作需要，自行提前登录上海师范大学“教职工奉贤校区住宿预约登记”系统选择住宿地点。（详见教职工奉贤校区住宿预约登记操作说明）

当天下午14点以后（最晚23：30之前），教职工可前往住宿点前台或管理处，出示本人校园卡，经前台管理员核实后办理当天入住手续，不能代办入住手续，次日12点之前办理退房手续。



教职工奉贤校区住宿预约登记

- 凡具备可预约权限的教职工用户（资产处确定权限范围）
- 通过“教职工奉贤校区住宿预约”可以进行次日开始一周内的奉贤住宿床位预约，预约成功即可在预约日免费入住。



选择入住日期和住宿楼宇，提交

预约错了，或者预约日不能入住，**须及时取消预约！**

实时了解当日预约入住情况





我的二维码证件

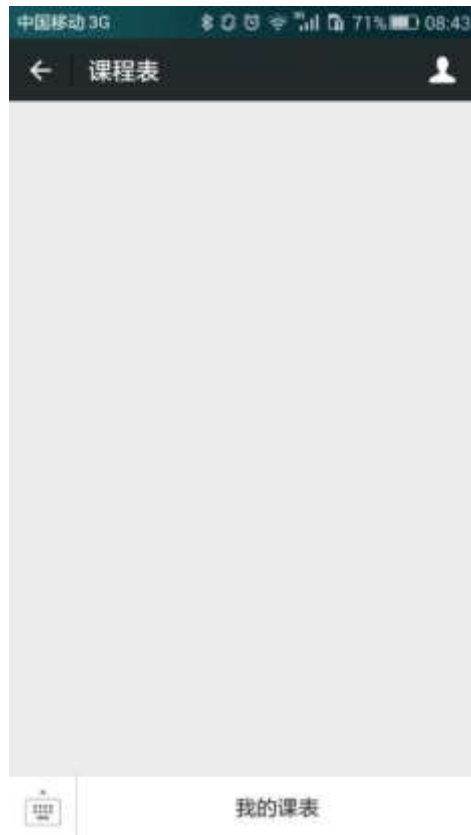
- 我的二维证件码，为今后的二维码签到的实现奠定了基础
- 今后的蓝图：开会时忘记带校园卡了，通过扫描条形码或二维码成功签到。





课程表

- 教师的课表可以及时查看每周的课程安排。





我所在部门的成员通讯录

- 我所在部门的成员通讯录（对于申请开放访问权限的单位提供该服务）
- 本部门用户只能查到本部门人员的联系方式，方便老师们的联系沟通



- 随时查看本部门人员的手机、邮件
- 支持搜索查询
- 免去单位印刷通讯录的操作





无线上网临时帐号申请

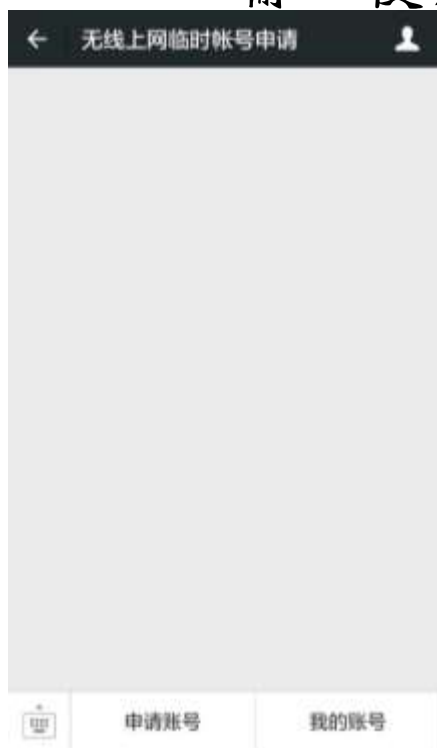
- 已经开放针对临时用户的shnu-guest信号
- 连接后需打开浏览器，在认证页面完成接入认证操作





无线上网临时帐号申请

- 每位教职工可申请2个当日临时无线帐号
- 临时无线帐号申请：
 - 选择申请帐号
 - 输入使用者姓名、手机、申请事由，提交





徐汇、奉贤校区校内办公电话一览表

- 学校的办公电话黄页
- 可以按部门、按字母排序查看办公电话信息

× 徐汇校区校内电话信息
上海师范大学徐汇校区 电话一览表
学校办公室 主任室: 66054 党办: 62631 行政、接待: 62881、64360512(F) 用印: 62430 信息机要: 68655 秘书科: 62668、64322150(F) 机要: 64321578 信访接待: 62431 基金会: 68645 校友办公室: 62622、62871
纪委办公室、监察处 处长室: 60960 副处长室: 64186 办公室: 62204
组织部
宣传部

× 奉贤校区校内电话信息
上海师范大学奉贤校区 电话一览表
管委会 李刚: 52389 王军: 53508
学校办公室 主任室: 52254 行政、接待: 52472 内勤: 53902 传真: 52441
纪委办、监察处 办公室: 52285
组织部
宣传部
统战部
学生工作部(处)
保卫处
工会、妇委会



部门的专享应用

- 每个部门可以根据本部门的管理需求申请建设上海师大智慧校园微信企业号中的部门专享应用。
- 对于一些职能部门，可以开放全体教职工访问权限，自己建立所需要的小组。实现更多信息分享。



更优服务

上海师大智慧校园的应用服务
还在不断完善与丰富……



上海师范大学信息化办公室
Informatization Office of Shanghai Normal University

智能终端的信息安全



主要内容

一、智能终端的便利与隐患

二、智能终端的安全举措

I. 密码设定

II. 恶意软件的防范

III. 良好的上网习惯

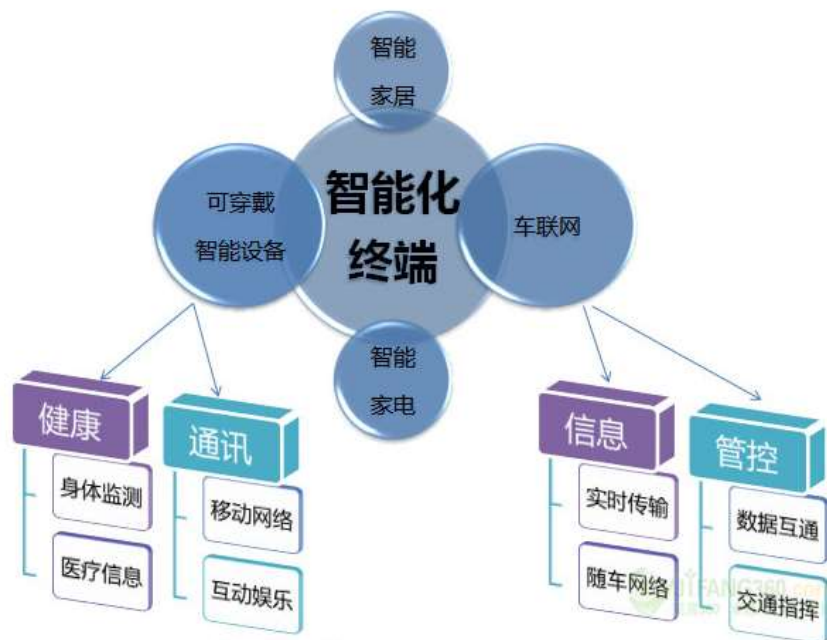
IV. 应用程序的权限

V. 手机上数据的保护

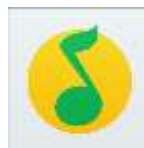
三、交流与讨论



智能终端的便利与隐患



智能终端带来的美好生活



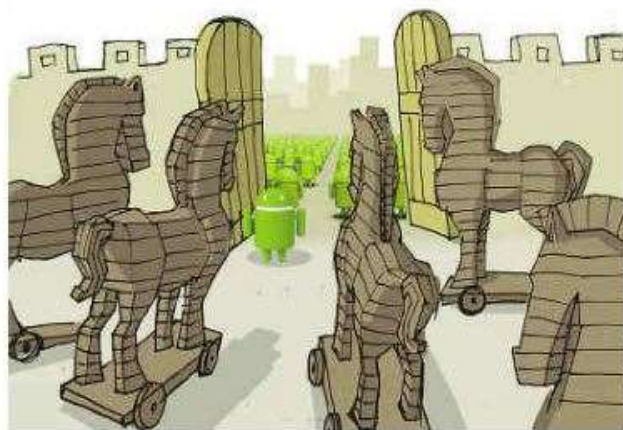
上海师范大学信息化办公室

Informatization Office of Shanghai Normal University

智能终端安全吗？

智能手机迅速发展

目前，智能手机已经成为人们生活中不可或缺的重要工具，随着3G,4G时代的到来，手机智能化越来越高，使手机集通讯、电子商务、信息处理、个人娱乐等多种功能为一体，给人们带来众多便利的同时，也带来了越来越多的信息安全隐患。



智能终端安全吗？

- 智能终端基于软件操作系统运行各类应用
- 主流操作系统
 - Android
 - iOS
 - Windows Phone
- 存在漏洞、存在安全隐患



智能终端安全吗？

你知道你手机中的APP在做什么吗？

**IT'S 2AM.
WHAT ARE YOUR APPS DOING?**

现在是凌晨2点，你知道你手机中的APP正在做什么吗？



智能终端安全吗？

它或许正在进行短信欺诈！

12月2日一大早，王先生的手机收到正在出差的“老婆发来的短信”：“忘记带钱包，同事很着急，老公麻烦帮我同事手机187****充值500。”

手机显示发件人是他“老婆”。
于是赶紧上网帮他“老婆”充了500元话费!!!

病毒危害1：伪造银行等公共短信钓鱼。



病毒危害2：伪造亲友短信诈骗钱财

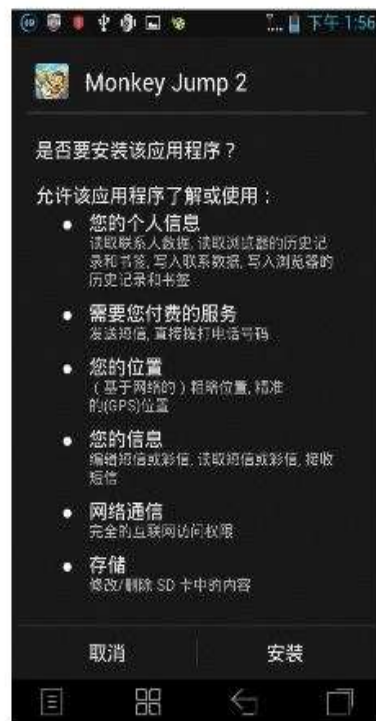


智能终端安全吗？

它或许正在窃取你的隐私！

“Monkey Jump2”，一款游戏应用居然：

- 读取你的通讯录？
- 读取你的上网记录？
- 获取你的位置？
- 发送短信，直接拨打电话？



智能终端安全吗？

使用手机带来的安全疑问

疑问一：手机可能泄露哪些信息？

【回应】通讯录、密码、短信、通话、照片都可能被窃取

疑问二：手机泄密渠道有哪些？

【回应】手机木马与恶意软件最危险；隐私窃取木马会监听并上传通话录音；一些看似普通的软件可能读取私人短信

疑问三：公共场所使用免费WiFi安全吗？

【回应】未经加密处理的用户名和密码信息可能被窃取，手机网银等加密资料不易被窃



智能终端的安全威胁

- Android（安卓）：幽灵推、
a.expense.GhostPush.a
- iOS（苹果）：Xcode Ghost
- 安全威胁的方式：
 - 消耗资源、破坏数据
 - 窃取用户隐私、账户信息、
 - 恶意吸费、网络诈骗
 -
- 根源：任何软件系统都存在漏洞



智能终端的安全状况

○ 恶意程序



数据来源: 《2015年第三季度中国手机安全状况报告》

智能终端的安全状况

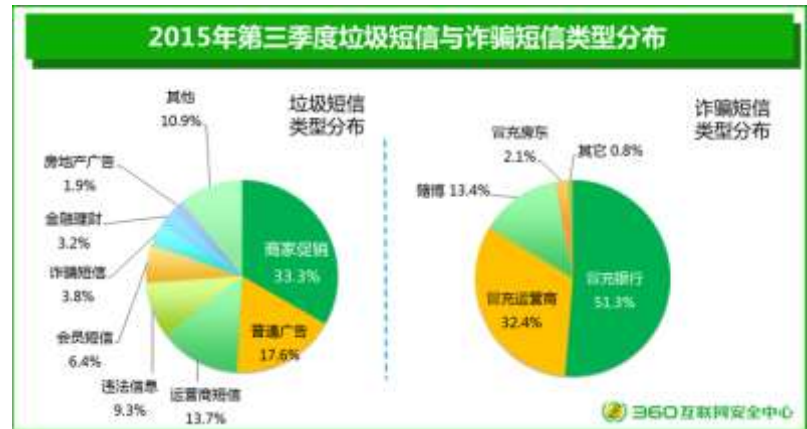
○ 钓鱼网站



数据来源：《2015年第三季度中国手机安全状况报告》

智能终端的安全状况

○ 电信骚扰



数据来源：《2015年第三季度中国手机安全状况报告》

智能终端的安全状况

○ 网络诈骗



数据来源: 《2015年第三季度中国手机安全状况报告》

智能终端的安全状况

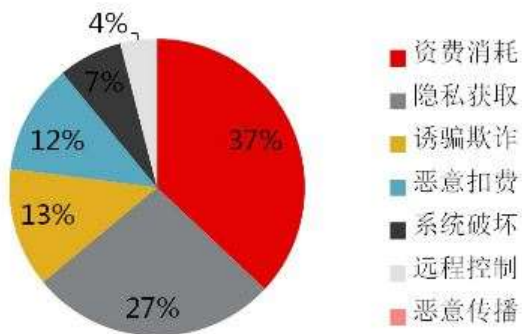
○ 受害者的性别差异及年龄分布



数据来源：《2015年第三季度中国手机安全状况报告》

智能终端的安全威胁

恶意应用主要来源和恶意行为分类



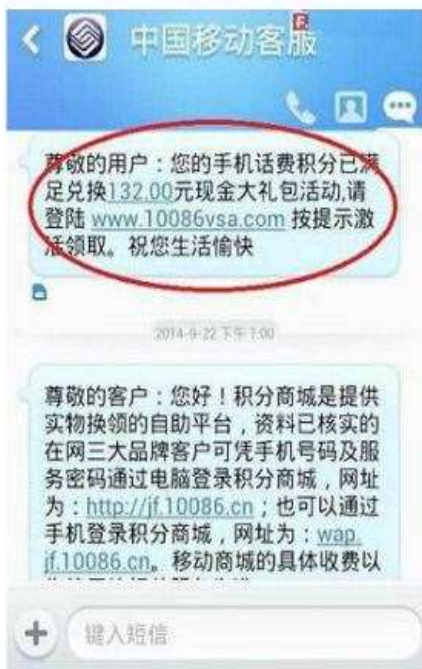
恶意行为分类



恶意应用主要来源

智能终端的安全威胁

10086发的短信也可能是骗子发的



前段时间不少市民都收到类似这样的“10086”发来的短信。其中一张女士介绍，今年6月的一天，她的手机收到了一条号码为10086发来的短信息，提醒她所使用手机号码的积分可以兑换几百元的短信费。张女士没多想把它点进去看有600块钱，就说可以兑换积分嘛，就把这个网址输进去，准备兑一个东西，还把身份证和（银行）卡号输进去了，第二天就发现银行卡上的存款不见了。

智能终端的安全威胁

10086发的短信也可能是骗子发的



日前，多名网友向本网反映，在接收到10086发送的积分兑换通知后，登陆提示的网站操作险些上当，后经咨询人工客服后发现短信内容并非移动官方所发，而是有人冒充中国移动号码的骗钱招数，移动方面称近期也接到多次类似情况的反映，但目前尚无应对办法，只能机主自己加强防范。

智能终端的安全威胁

智能手机开始成为病毒滋生的温床



安全的第一步：密码



手机突然失踪了，我的支付宝安全吗

- 有密码保护
- 损失情况可控
- 无密码保护
- 个人信息泄露
- 个人隐私泄露
- 更多财产损失

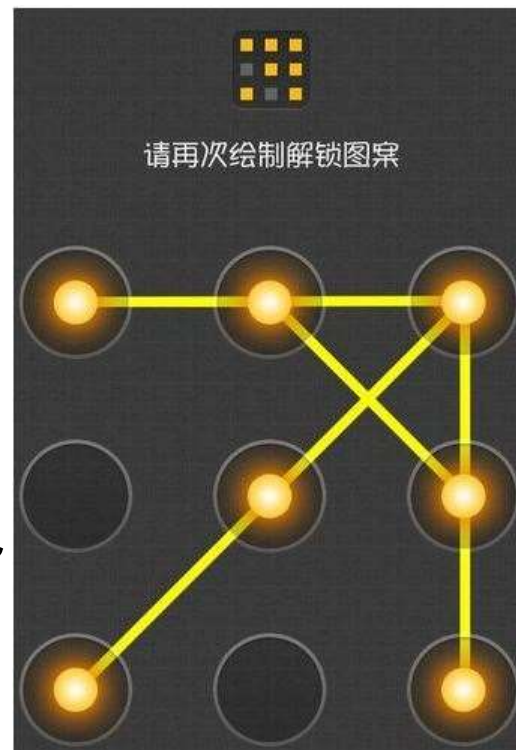


上海师范大学信息化办公室

Informatization Office of Shanghai Normal University

设置密码

- 手机使用中的密码
 - 开机密码
 - SIM卡启用PIN码
 - 屏幕解锁密码
 - 设置锁屏图案不可见
 - 存储卡加密
 - 部分安卓手机支持应用软件密码保护
- 设置强密码
- 启用密码与使用便利性的平衡





恶意软件的防范

选择可靠的应用商店、软件安装包的源

- 苹果的应用商店
 - AppStore
 - 第三方的应用商店（设备需要越狱，存在安全隐患）
- 安卓的应用商店
 - 厂商的应用商店
 - 第三方的应用商店（存在安全隐患）
 - 应用开发商的官方地址下载
 - 软件下载网站（存在安全隐患）
- Windows Phone的应用商店
 - 微软官方应用商店
 - 第三方应用商店（存在安全隐患）

选择可信任的应用开发商

- 开发者的选择
 - 公司与个人的区别
- 判断开发者的专业性、安全意识
 - 互联网的大公司
 - 软件升级中是否有安全性相关条目



谨慎选用免费类软件

- 免费软件的开发者的源动力是什么
 - 开放软件
 - 公司商业行为
 - 业余爱好
 - 黑客、犯罪组织的违法行为
- 免费软件不等于不需要付出，甚至是付出更多！
- 商业营销手段



识别非法渠道的应用安装行为

- 非法安全应用的行为
 - 安卓系统
 - 应用软件中的推广行为
 - 浏览网页时的入侵行为
 - 利用系统漏洞安装应用程序
 - iOS系统
 - 利用漏洞安装应用程序
 - Masque Attack (假面攻击)
 - 浏览网页时下载安装应用
 - Windows Phone



关注并及时更新

- 手机系统更新
- 应用商店中软件更新
- 应用软件自身的更新



安装杀毒软件

- 安卓系统
 - 安装杀毒软件
 - 及时升级病毒库
 - 定时查杀病毒
- 使用免费的还是付费的查毒软件





养成良好的上网习惯

免费（公共）WiFi中安全威胁

- 手机连接网络时在做什么事情？
 - 表象：只是使用浏览器上网
 - 内部：后台程序在数据交互
 - 各类账号信息
 - 个人隐私文件
 - 案例：央视 315晚会 免费WiFi网络 用户微信
照片 邮箱账号密码
- 不要免费蹭网
- 关闭后台运行的程序



上网的良好习惯

- 管理数据流量：防止超出套餐使用流量，防止吸费软件的攻击。
- 指定软件是否可以使用WiFi、数据。
- 不随意使用WiFi管理软件，特别是可以免费使用他人加密WiFi的软件。



不随意打开网页链接

- 链接的来源
 - 社交网络
 - 聊天工具
 - 短信
 - 电子邮件
 - 二维码
- 微信中查看网页服务器、链接地址



应用程序的权限



应用程序的权限

智能手机安全隐患：都是权限惹的祸！



42%的用户基本不知道“权限”是什么

97%的用户不懂应用权限的风险

用户要用，只能选择“安装”

Monkey Jump 2

是否要安装该应用程序？

允许该应用程序了解或使用：

- 您的个人信息
读取联系人名单、读取浏览器历史记录、读取日历、写入联系人数据、写入日历事件、写入日历提醒
- 需要您付费的服务
为应用程序提供付费服务
- 您的位置
(基于网络)、粗略位置、精确的位置设置
- 您的信息
编辑设备名称、读取设备名称、设备名称
- 网络通信
接收来自网络的广播
- 存储
写入或删除SD卡中的内容

取消 安装

第三方应用都可以获得哪些权限？

 <p>隐私</p> <ul style="list-style-type: none">读取日历活动读取联系人数据读取浏览器历史和书签读取所有个人数据读取短信或彩信添加或修改日历活动写入联系人数据向邀请对象发送电子邮件读取日历日志文件	 <p>通信</p> <ul style="list-style-type: none">更改网络连接属性更改WiFi状态创建蓝牙连接蓝牙管理直接拨打电话号码完全的网络访问权限发送短信	 <p>系统</p> <ul style="list-style-type: none">更改用户界面设置删除所有应用程序缓存检查系统状态检查当前运行的程序继续刷新其文件系统的让应用程序始终运行设置时区关闭所有后台应用程序新启动的进程个数
 <p>硬件</p> <ul style="list-style-type: none">关闭更改音频设置格式化外部存储设备修改存储在SD卡中的内容录音防止手机休眠	 <p>位置</p> <ul style="list-style-type: none">基于网络粗略位置精确的GPS位置	 <p>账户</p> <ul style="list-style-type: none">使用用户的身份验证凭证作为用户身份验证程序管理账户列表改变账户同步设置



上海师范大学信息化办公室

Informatization Office of Shanghai Normal University

手机的硬件资源、个人隐私信息的授权

○ 目的

- 防止远程控制硬件资源
- 防止读取个人隐私信息



权限列表（以安卓平台为例）

○ 隐私数据

- 读取联系人
- 读取短信/彩信
- 读取通话记录
- 读取日程
- 读取联系信息
- 读取本机设备码
- 新建/修改联系人
- 新建/修改通话记录
- 删除联系人
- 删除通话记录

○ 安全防御

- 拨打电话
- 发送短信
- 发送彩信
- 调用摄像头
- 录音
- 移动数据
- WLAN数据
- 蓝牙



如何分配权限

- 最小授权原则（只给必要的权限）
- 单次授权原则（使用时授权，按需授权）



第三方授权、认证

- OAuth: 开放的授权标准 (Open Authorization)
- 允许用户授权第三方网站访问他们存储在另外的服务提供者上的信息
- 不需要将用户名和密码提供给第三方网站或分享他们数据的所有内容
- 授权&认证



使用第三方认证的注意事项

- 仅在经常使用的网站进行授权认证
- 注意授权认证中网站提示信息（涉及个人的信息）
- 避免对小公司、陌生应用进行授权认证



手机上数据保护



安卓平台的磁盘数据安全

- 超过90%的Android设备正面临磁盘数据泄漏的风险
- 不仅仅局限于隐私数据，同时还包括了大量和App认证相关的数据
- 安卓平台使用的存储介质：Flash Memory(闪存)

安卓平台删除数据是否安全

- 安全的方法（仅适用于Android4.0及以后的版本）
 - Google官方Recovery
 - Fastboot擦除数据(操作复杂)
- 不安全的方法
 - 删除文件（数据残留率：100%）
 - 卸载应用
 - 第三方软件的Recovery
- 对TF卡进行加密存储



如何处理手机

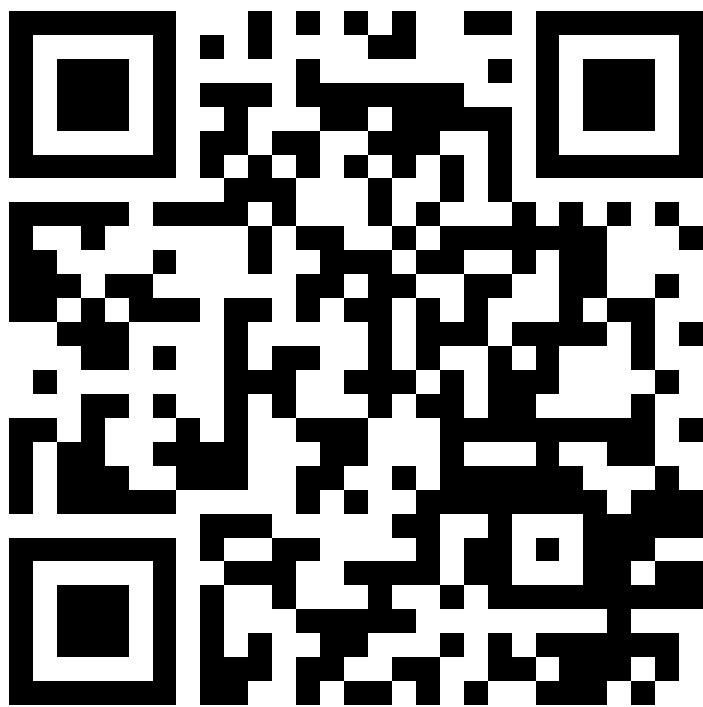
- 在丢弃/赠送/出售手机前，确保使用正确的Recovery进行恢复出厂设置。
- 有能力的用户请使用fastboot模式对磁盘进行清理。



交流与讨论



请您为本次培训提供宝贵意见



谢谢!



上海师范大学信息化办公室
Informatization Office of Shanghai Normal University