通用技术
GENERTEC
好 技 术 · 好 生 活

网络安全意识培训

员工篇

目录

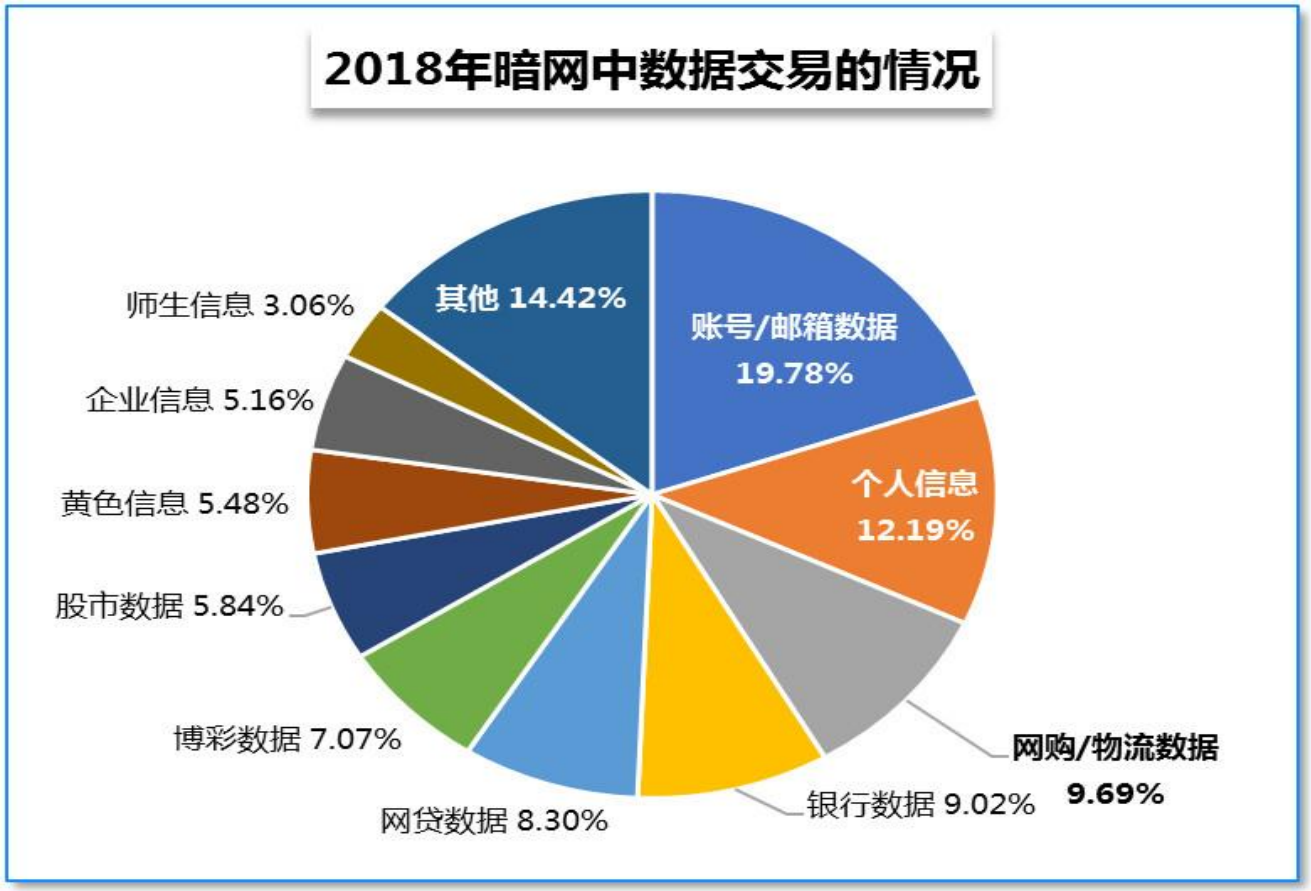
PART 01

网络安全形势

互联网分类

整个互联网可以划分为三个类别，分别是明网、深网以及暗网。

暗网交易情况

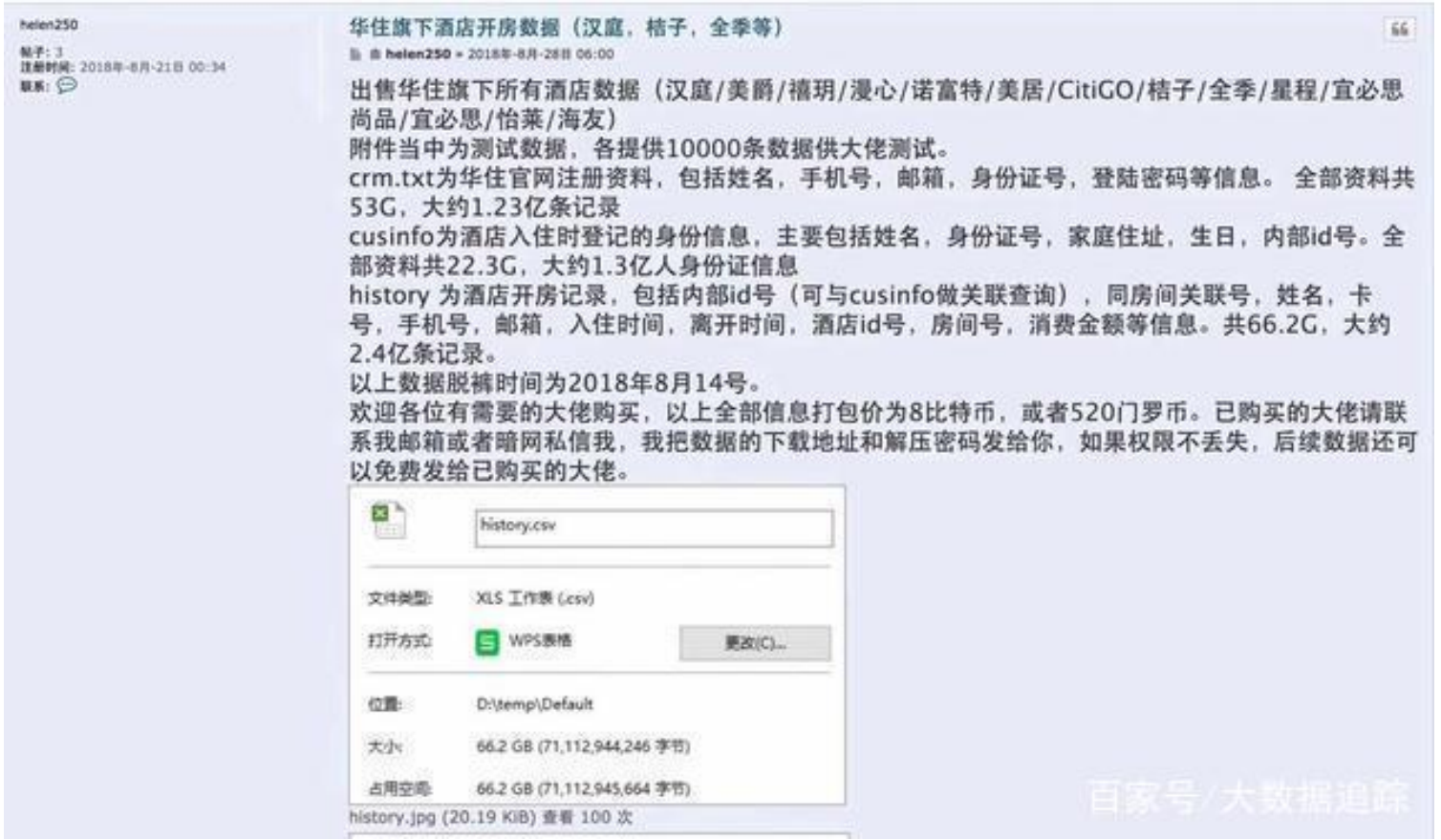


2018年暗网中数据交易分类

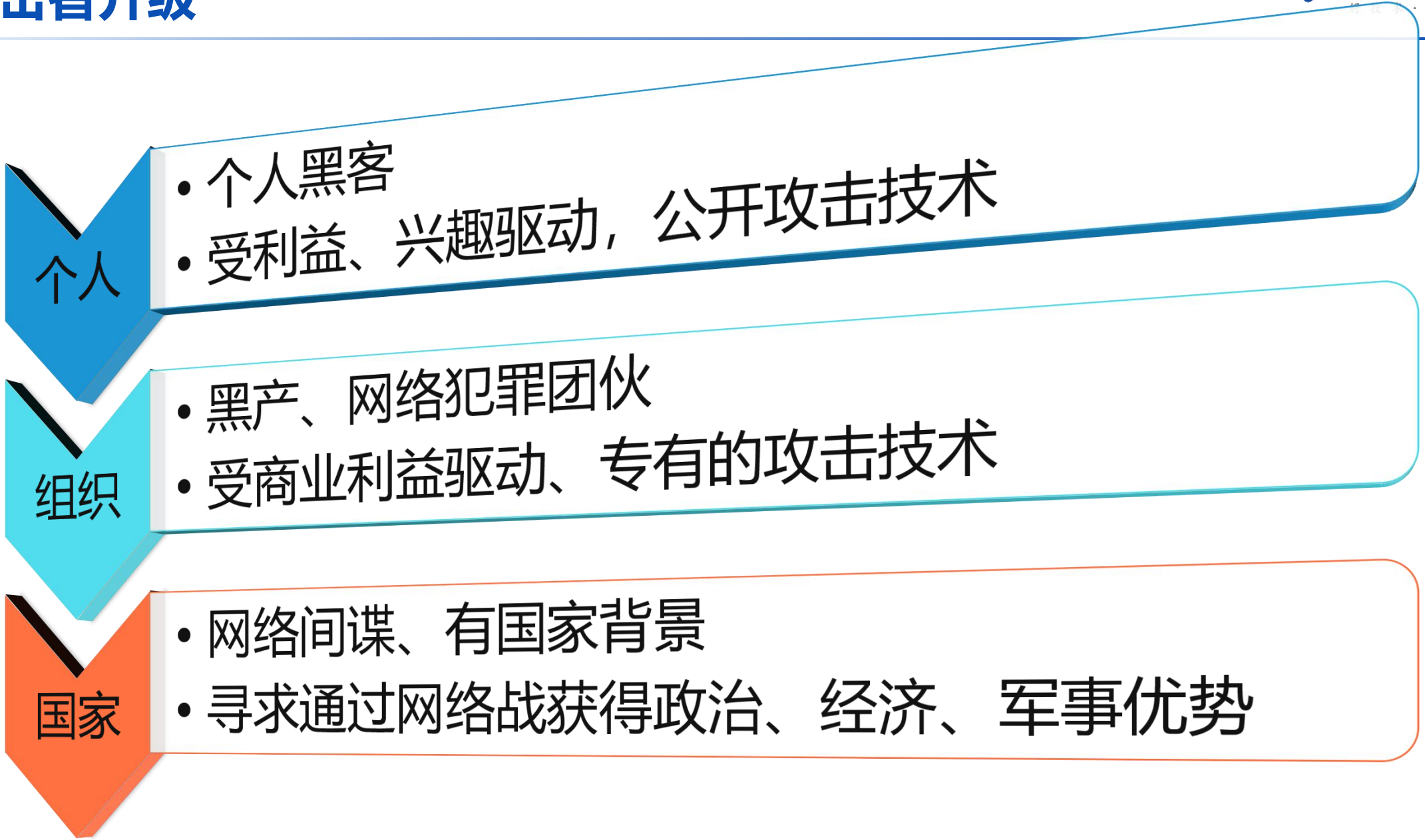
个人信息贩卖

华住旗下酒店开房记录在暗网出售，内容涉及大量个人入住酒店信息，主要为姓名、身份证信息、手机号、卡号等，约5亿条公民信息。

华住信息泄露

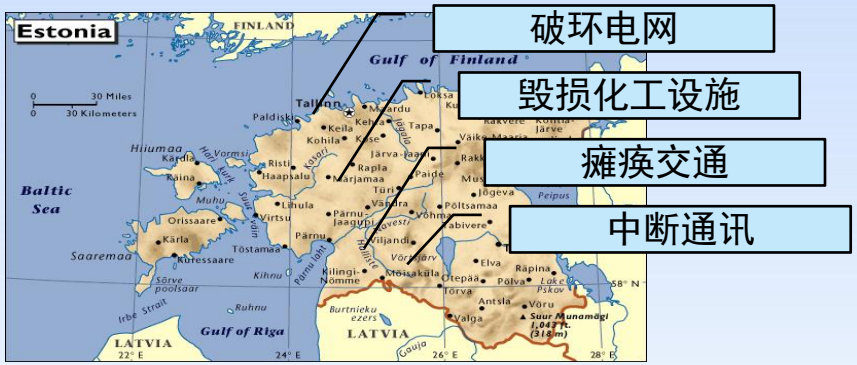


攻击者升级


个人
• 个人黑客
• 受利益、兴趣驱动，公开攻击技术
组织
• 黑产、网络犯罪团伙
• 受商业利益驱动、专有的攻击技术
国家
• 网络间谍、有国家背景
• 寻求通过网络战获得政治、经济、军事优势

国际网络战

2007年，北约成员国**爱沙尼亚**遭到大规模网络攻击，国内网络陷入瘫痪。北约当时**束手无策**，只派出观察员前往爱沙尼亚。



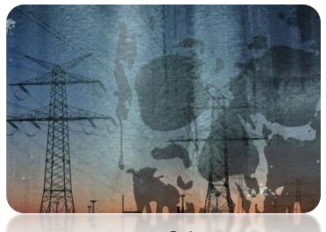
网络战

2011年12月13日至15日，北约举行了一场以**中国**为假想敌的**网络防御演习**，以检验应对大规模网络攻击的能力。此次演习表明，网络战正变得与常规战争一样重要，网络将会成为**破敌制胜的重要平台**。

网络安全影响

基础设施

2019年3月7日，委内瑞拉大部分地区停电超过24小时，造成大规模交通拥堵，学校、医院、工厂、机场等都受到严重影响，手机和网络无法正常使用。委内瑞拉总统马杜罗指出，停电 “是美国方面的攻击行为造成的”。



委内瑞拉电力

经济命脉

2017年1月，在移动支付逐渐成为主角的时候，移动支付巨头支付宝被披露存在账号绕过漏洞，攻击者无需密码可任意登录支付宝并修改密码，该漏洞随即被支付宝母公司阿里巴巴确认，并对支付宝进行了紧急升级。

账号绕过漏洞

社会稳定

2016年8月21日，因被诈骗电话骗走上大学的费用9900元，伤心欲绝，导致心脏骤停，不幸离世。

事件的起因，是黑客攻击“山东省2016高考网上报名信息系统”，获得考生个人信息，并以0.5元每条进行低价贩卖。

山东徐玉玉案

政治选举

2016年，美国总统大选中，支持率遥遥领先的希拉里，因为机密邮件泄漏，导致特朗普逆袭。据美国国家安全局公布，有证据表明，此次希拉里的邮件泄漏，和俄罗斯黑客的网络安全攻击有直接关系。

希特大战

国际安全发展

在新的网络时代，第五空间主权意识的觉醒

- 网络空间安全战略：国家战略、国际战略、行动战略三大战略
- 网络安全立法：横三竖二；《网络安全保护法案》
- 全球网络空间秩序处于极不平衡的状态，美国拥有绝对的优势

美国

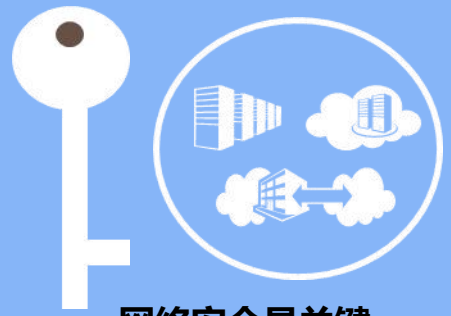
欧盟

三位一体：立法、战略与实践

日本

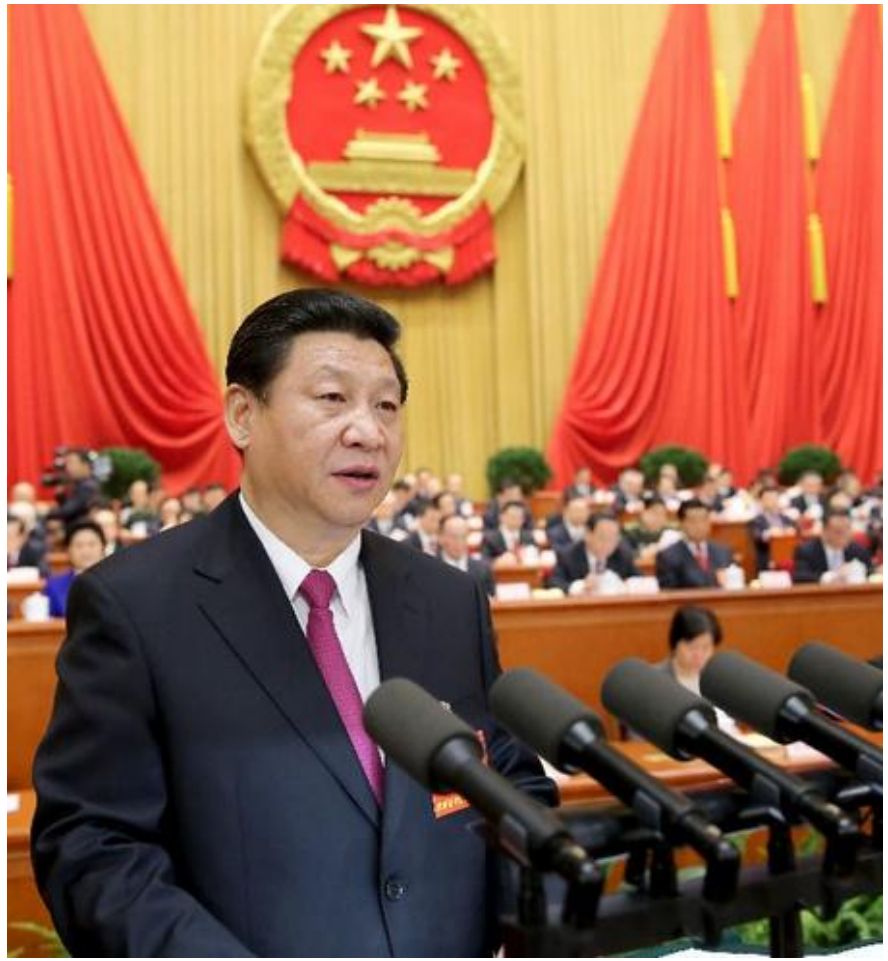
通过了《网络安全基本法》，创建了网络安全战略本部，强化政府与民间在网络安全领域的“协同作战”

陆→海→天→空→网



网络安全是关键（key）因素

国家顶层战略



习近平总书记指出：

没有网络安全，就没有国家安全

以互联网为核心的网络空间已成为继陆、海、空、天之后的**第五大战略空间**，各国均高度重视网络空间的安全问题。

网络安全法形成

网络运营者

关键信息基础设施运营者

网络产品或服务提供者

信息发送或软件发布服务提供者

网信部门和有关部门

罚款

治安管理处罚
民事责任

刑事责任

PART 02

网络攻击场景


计算机
信息安全
人
手机

计算机安全

- 系统软件
- 电子邮件
- 密码安全

勒索病毒

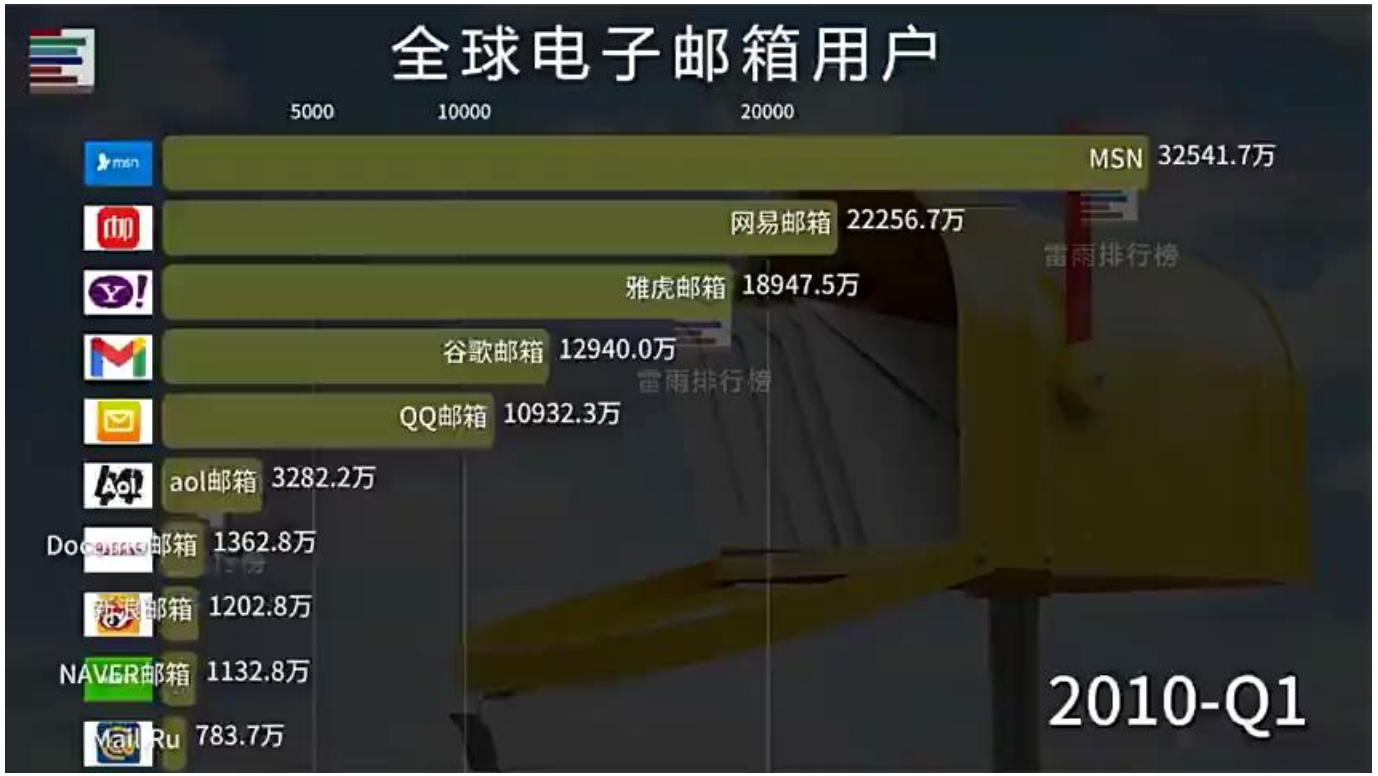
- 2017年5月12日，一种名为“想哭”的勒索病毒（永恒之蓝）袭击全球150多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信和汽车制造业。
- ……

计算机安全——系统和软件

木马病毒

计算机安全——电子邮件

电子邮件：正式的工作分配和工作汇报方式



在这里分享一些关于Email的关键数字：

- 据统计，有超过87%的病毒是借助Email进入企业的。

计算机安全——电子邮件

钓鱼邮件

2019/3/13 (周三) 14:52

M Miaao [redacted]@163.com>

Re:流量安全警告：监测恶意流量

收件人 Help Center

thank you.

At 2019-03-13 14:45:55, "Help Center" <help-center@ioa-cstnet.org> wrote:

尊敬的[redacted]

您收到的是来自 Coremail 专业邮件系统的信件.

本邮件由系统自动发送，请不要回复此邮件。

您收到本邮件，仅说明我们检测到您计算机网络的异常流量。

邮箱需要经过系统的验证后才能接收到来自本 Coremail 专业邮件系统的邮件，

请点击下面的链接完成验证：：

立即验证

https://mail.ioa-cstnet.org/cstnet?em=bGZoQG1haWwuaW9hLmFjLmNu==

如果上面的链接不能点击， 请将上面的地址复制到浏览器的地址栏后回车 。

多谢您的支持，请在稍后时间重新尝试投递，或者联系联系管理员、技术中心协助。

如果您有其他问题，欢迎向客服中心联系 。

中国科学院 |中国科学院 计算机网路络信息中心

©1994-2019 版权所有：中国科学院计算机网络信息中心 科技云运行与技术发展部 Email: 58812000@cstnet.cn

伪装成中国科学院计算机网路络信息中心管理员对该所人员发起鱼叉式攻击活动，试图窃取科研人员邮箱账密。

安全警告 宏已被禁用。 启用内容

H13

中华人民共和国国家卫生健康委员会

National Health Commission of the People's Republic of China

这是一个受保护的文档，点击“启用内容”以编写详细信息

武汉旅行信息收集申请表

请填写不适用并发送（如果需要）：

人信息		你遇到的人的细节	
姓名	当前位置	姓名	当前位置

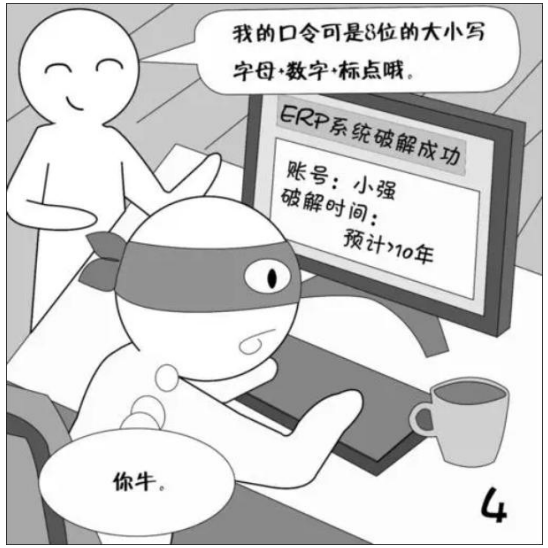
申请表格.xlsm
武汉旅行信息收集申请表.xlsm
收集健康准备信息的申请表.xlsm
新型冠状病毒感染引起的肺炎的诊断和预防措施.xlsm
卫生部指令.docx

计算机安全——电子邮件


发件人： Alibaba
发件人显示为Alibaba，非常具有迷惑性
发送时间： 2012-12-12 08:52:58
收件人：
抄送：
主题： Confirm your membership to avoid service suspension.
胡乱编造的主题，阿里巴巴不会以这种理由就关闭会员的账号
阿里巴巴 Alibaba.com.cn
称谓十分模糊，真正的阿里巴巴邮件都以准确的公司名字、会员姓名作为称谓
亲爱的卖家，
目前，我们正在从事的帐户维护
作为用户，您需要确认您的维续
未能确认您维续是其成员将导致
http:/www.webalex.com.br/central/modules/Alibaba-cn.htm
单击以跟踪链接
点击这里更新您的阿里巴巴帐户。
把鼠标放在超链接上可以看到是非常明显的钓鱼链接：链接的一级域名并非www.alibaba.com，而是一些胡乱的域名
问候
?012阿里巴巴公司保留所有权利
邮件落款没有明确的部门，且整篇邮件语言不通顺，内容简单

计算机安全——密码安全

密码爆破



计算机安全——密码安全

脆弱的口令……

- 少于8个字符
- 单一的字符类型，例如只用小写字母，或只用数字
- 用户名与口令相同
- 最常被人使用的弱口令
- 所有系统都使用相同的口令
- 口令一直不变
- 数据字典多少条

!@#$%^&*(✗

password ✗

marry820312 ✗

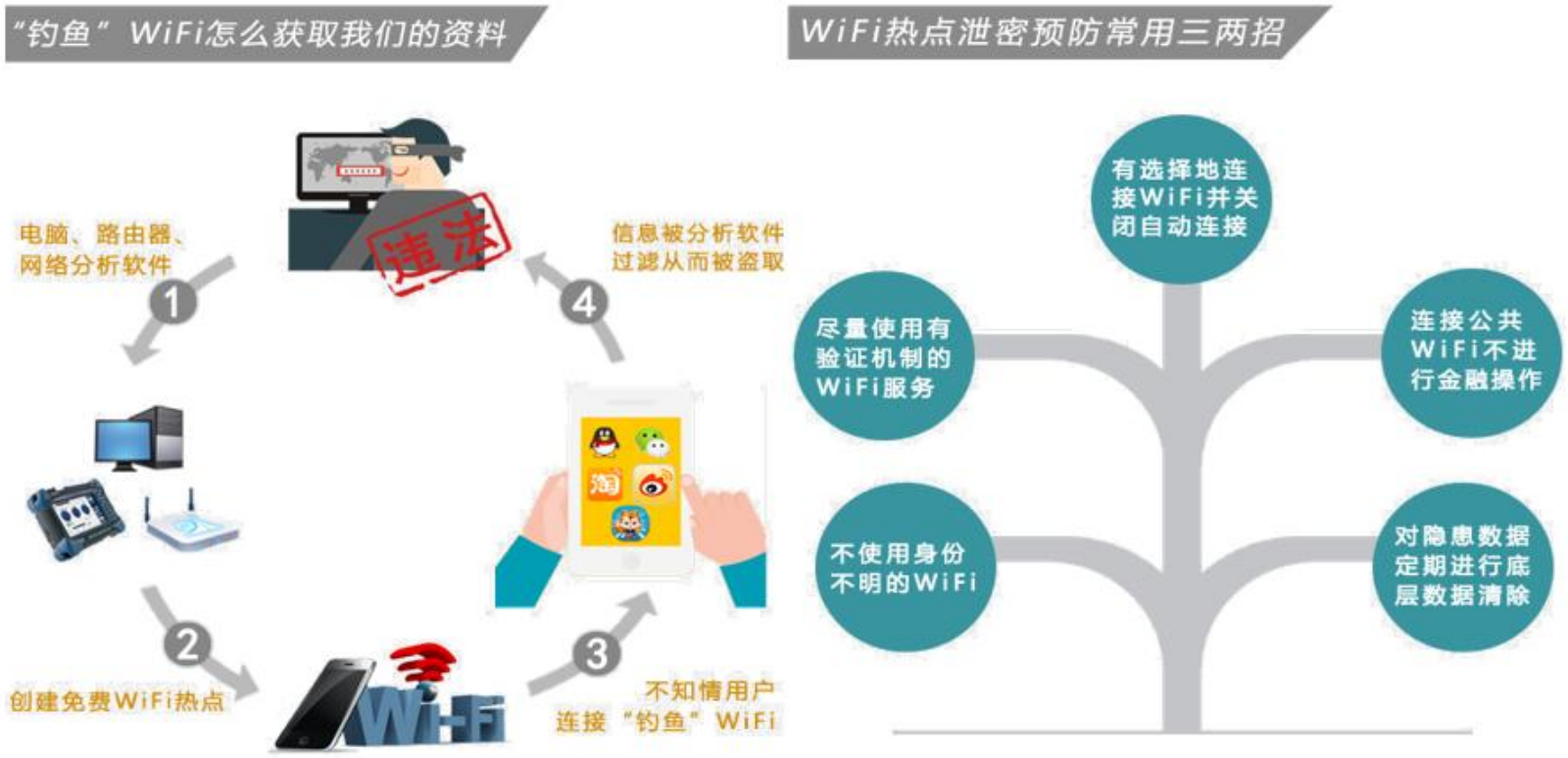
xEc@ser92% ✓

手机安全

- 公共wifi
- 不明软件下载
- 二维码

手机安全——公共WIFI

公共WiFi慎连



手机安全——短信

短信钓鱼

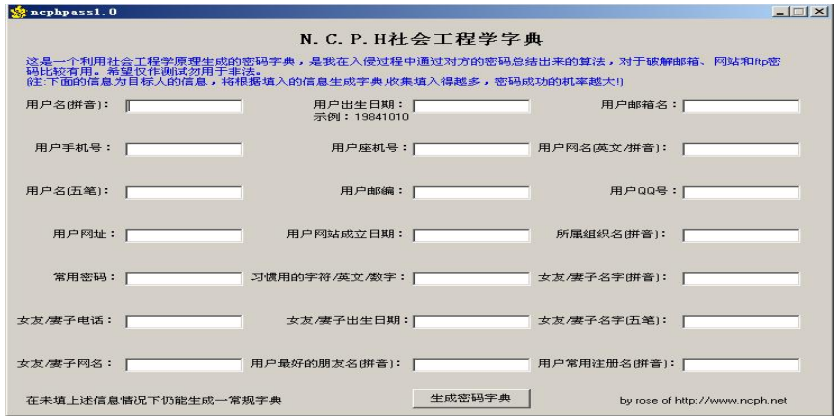

+61449038737
●●●●● 中国移动 17:21 41%
信息
106575007592
联系人
短信/彩信
今天 17:09
【交科视讯】你的手机号码已选为《奔跑吧兄弟》获奖用户，获得16万奖金以及笔记本一台，登陆 bsske.com
验证码：7763 领取
伪基站假冒交通银行客服号码95559发送的欺诈短信
官方网站地址应为：
www.bankcomm.com
输入信息

手机安全——不明软件下载

手机安全——扫二维码

社会工程学

- 敏感信息收集
- 伪装诱导欺骗
- 社工字典



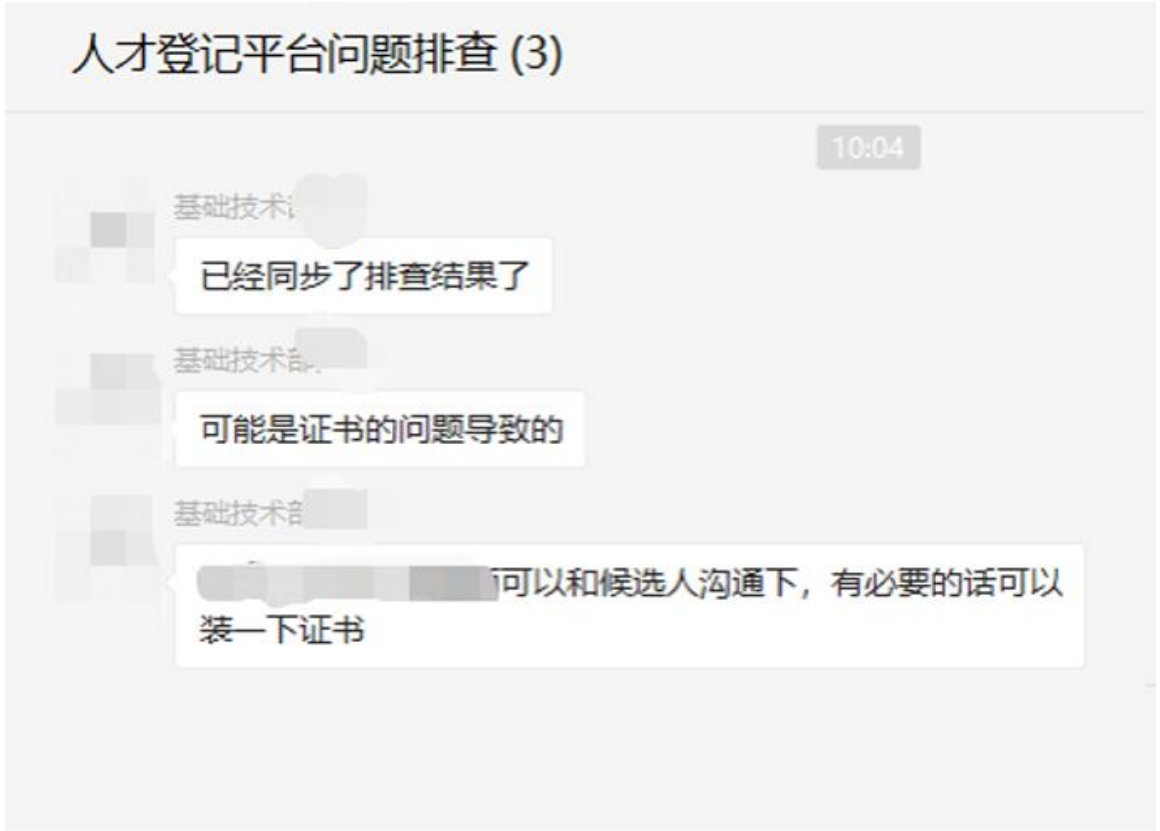
社会工程学——敏感信息收集

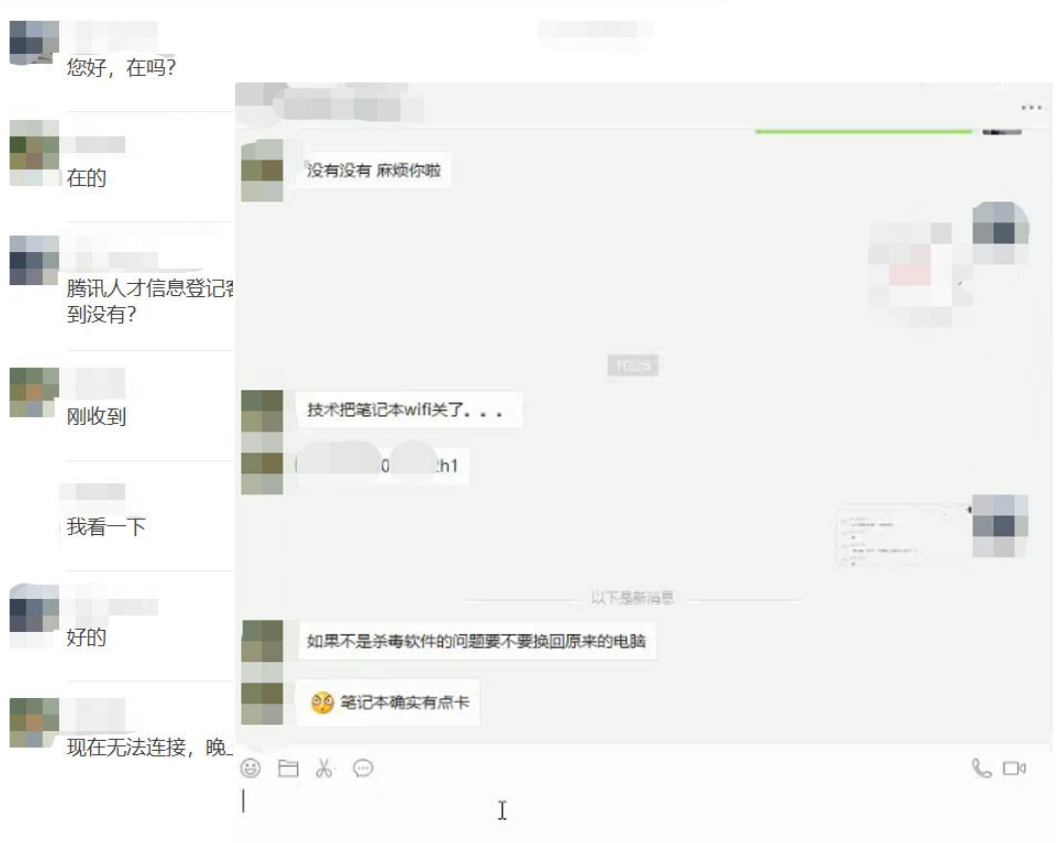
- 一些工作用到的书籍
- 一个打开的笔记本
- 一个U盘
- 一些发票
- 一些报表文件

这些物品会存在哪些潜在的安全隐患呢?

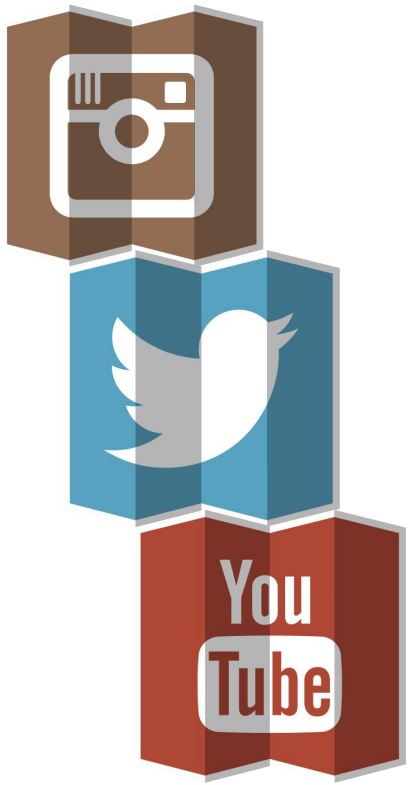
社会工程学——伪装诱导欺骗

社会工程学的一些利用





社会工程学——社工字典


You
Tube


ncphpass1.0
N.C.P.H社会工程学字典
这是一个利用社会工
码比较有用。希望仅
pass - 记事
文件(F) 编辑(E
pass - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

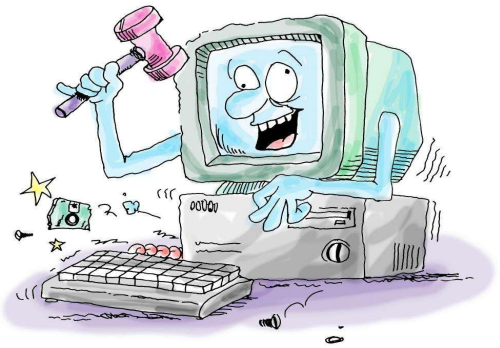

網易通行证 易证在手 网易任君游
网易首页 反馈意见 帮助
找回网易通行证密码：
1.输入通行证帐号
2.选择找回密码方式
3.找回密码
通过密码提示问题找回密码 [换一个找回方式]
请回答问题： 我就读的高中是哪里？
答案：
新密码：
密码长度为6-16位，可用英文字母、数字、特殊字符。
重复新密码：
验证码：
不区分大小写，换一张
完成

PART 02

网络安全知识

病毒防范

- 及时安装杀毒软件；
- 使用安全浏览器；
- 不随意点击链接，进去不安全的网站；
- 使用移动存储介质时,进行查杀病毒后打开；
- 浏览网页时,计算机使用过程中发现异常,断开网络全盘杀毒；
- 发现主机异常，及时报备；



邮件安全

- 尽量使用电子邮箱客户端进行发送或接收
- 不安全的文件类型：绝对不要打开任何以下文件类型的邮件附件：.bat, .com, .exe, .vbs
- 不要随意点击链接：如果邮件中附带链接，且邮件内容并没有明确提及点开的目的，我们尽量要与发件人进行沟通后再点击，如发件人为陌生人，切勿随意点击链接

密码安全

- 如果有初始密码,应尽快修改
- 密码长度不少于8个字符
- 不要使用单一的字符类型,例如只用小写字母,或只用数字
- 用户名与密码不要使用相同字符
- 常见的弱口令尽量避免设置为密码
- 自己.家人.朋友、亲戚、宠物的名字避免设置为密码

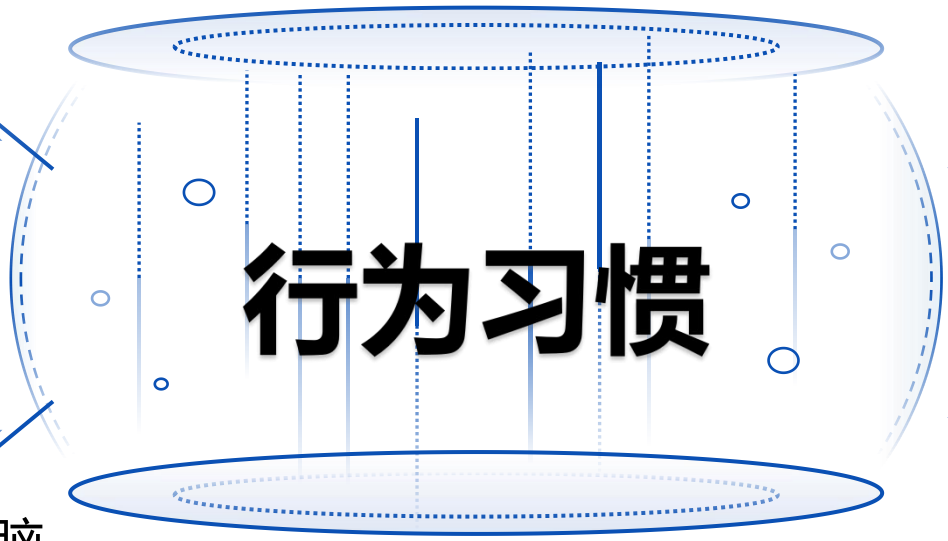
手机安全

- 手机设置自动锁屏功能,建议设置1-5分钟的,避免离开手机后被其他人恶意使用;
- 手机升级应通过自带的更新功能,避免通过网站下载更新;
- 尽可能通过手机自带的应用市场下载手机应用程序;
- 为手机安装杀毒软件;
- 经常为手机做数据同步备份;

社工安全

禁止随意放置或丢弃含有敏感信息的纸质文件

应将复印或打印的资料及时取走，重要文件加锁传输



离开座位时对使用的电脑进行锁屏，保密文件放入柜中

U盘不使用时应及时拔出并妥善保管，将各种介质都按需分配

结束

安全意识无论是对个人还是组织都是一笔宝贵的财富

通用技术

GENERTEC

好技术·好生活