互联网信息安全意识培训

1 信息安全概述

2 个人安全意识

3 办公安全意识

信息安全概述

什么是信息安全?

信息安全就像刹车，

防止车祸的发生

信息安全三要素

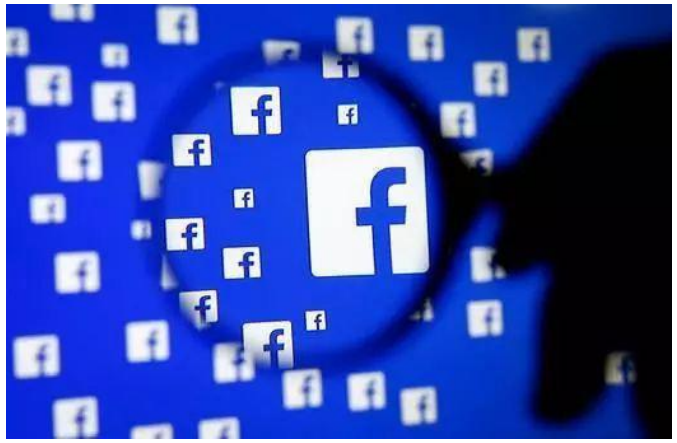
确保信息不会泄露给非授权个人或机构

确保信息或资源可以正常使用，不会被异常拒绝

确保信息不会被篡改

信息安全—机密性

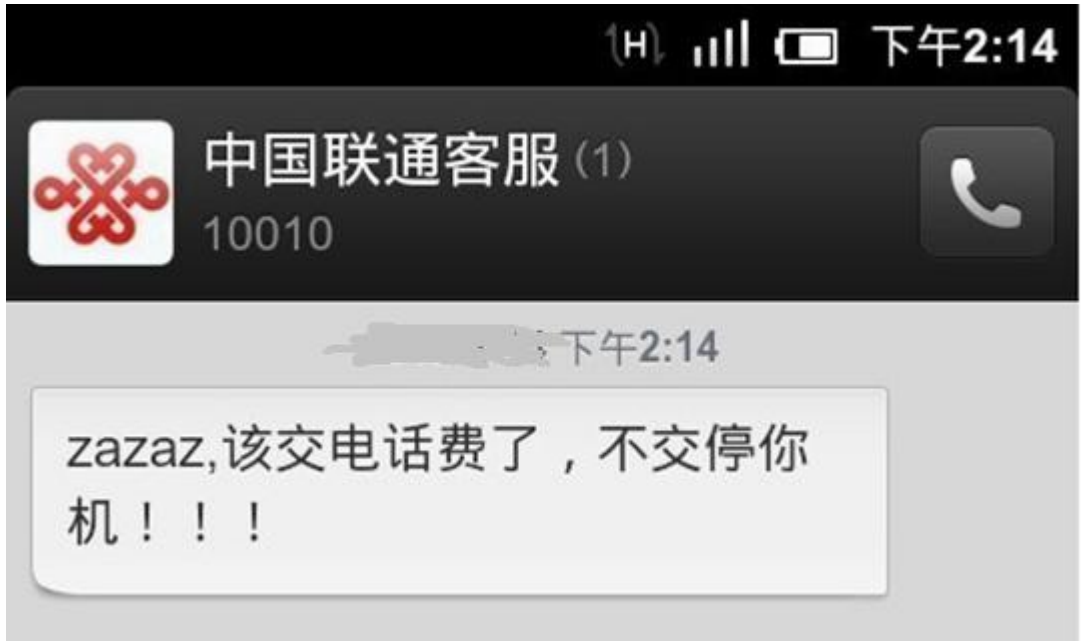
2018年3月
FACEBOOK
5000万用户数据
泄露

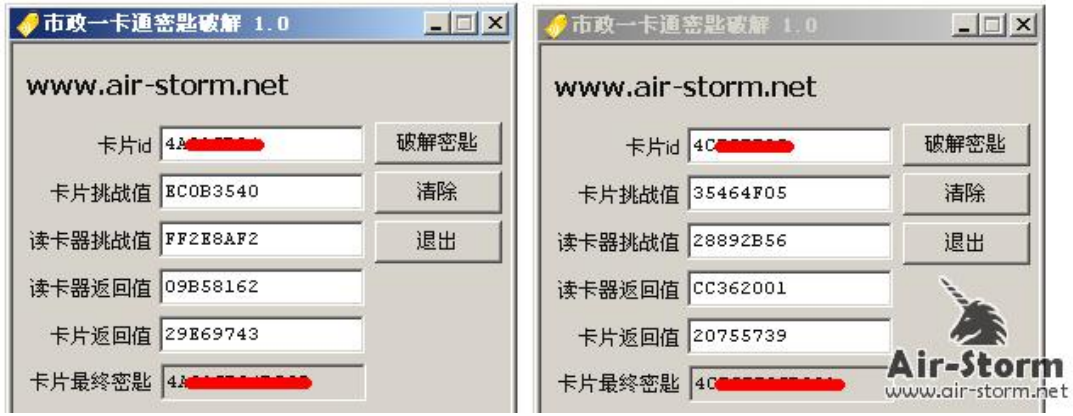


2018年8月
华住集团 5亿用
户信息泄漏

信息安全—完整性

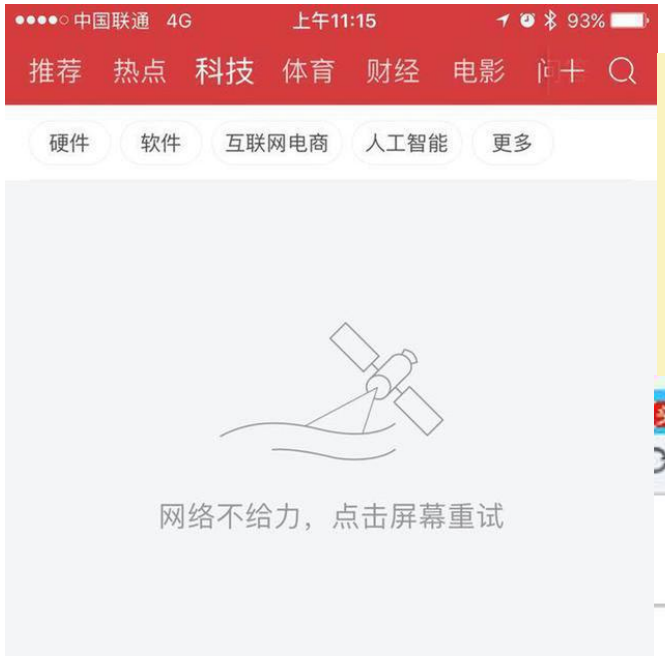

Carrier
密码不正确
请再试一次
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
紧急电话
0
取消


下午2:14
中国联通客服 (1)
10010
下午2:14
zazaz,该交电话费了，不交停你机！！！


市政一卡通密匙破解 1.0
www.air-storm.net
卡片id
卡片挑战值 EC0B3540
读卡器挑战值 FF2E8AF2
读卡器返回值 09B58162
卡片返回值 29E69743
卡片最终密匙
破解密匙
清除
退出
市政一卡通密匙破解 1.0
www.air-storm.net
卡片id
卡片挑战值 35464F05
读卡器挑战值 28892B56
读卡器返回值 CC362001
卡片返回值 20755739
卡片最终密匙
破解密匙
清除
退出
Air-Storm
www.air-storm.net

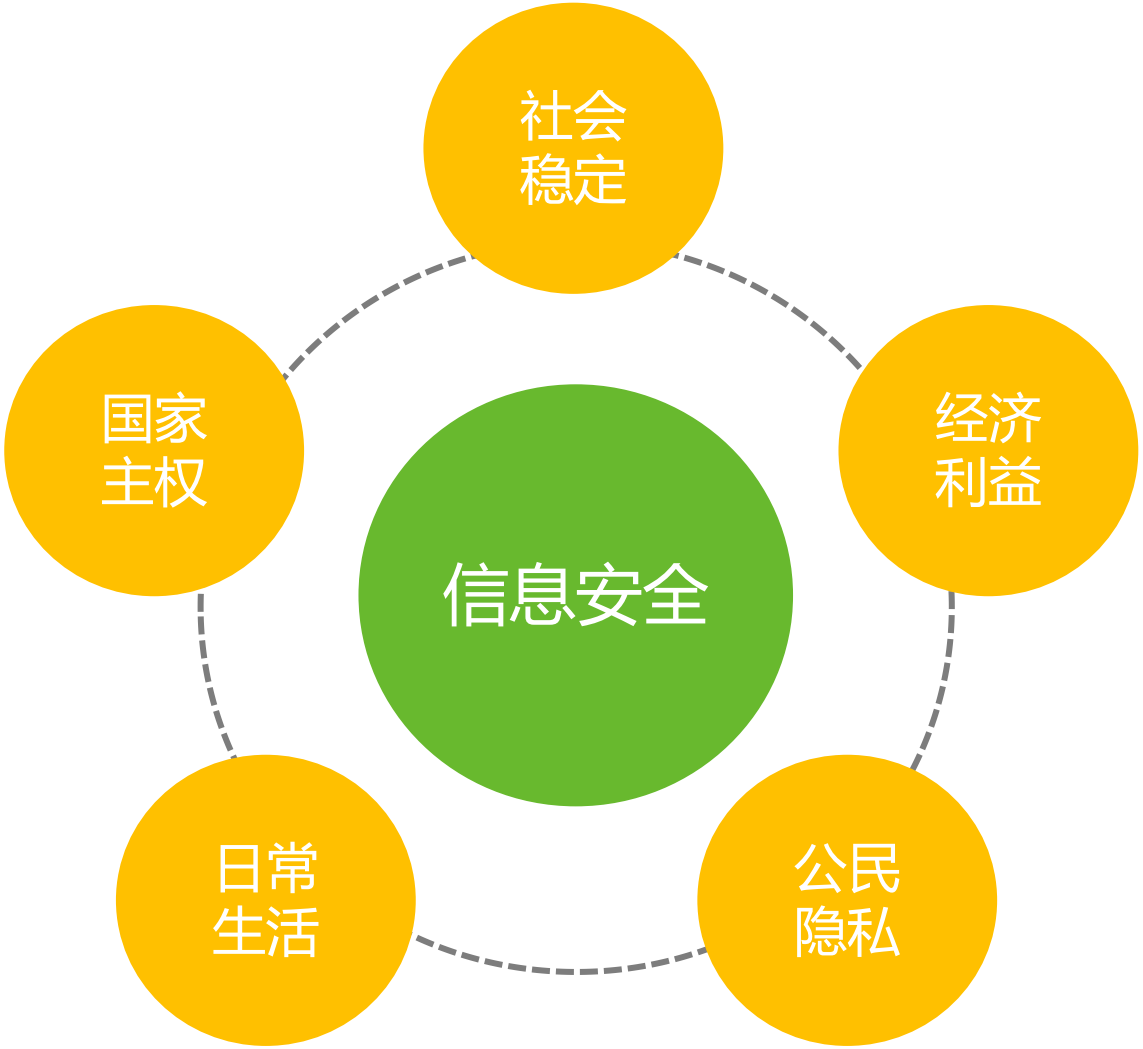
信息安全—可用性

2015年5月27日，支付宝断网事件



2017年1月 今日头条服务器宕机，影响长达30分钟

信息安全影响范围



国内信息安全现状

网络信息安全已纳入国家战略

大量网络安全事件发生

新兴技术应用带来的安全风险

常见安全隐患-钓鱼网站


文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
http://www.zysm2008.com/netpay/alipay.asp
这不是https加密链接
您好，欢迎使用
即时到账交易（非支付宝信用中介服务，快速）


我的支付宝 – 支付宝 - 世界之窗 3.2
https://lab.alipay.com/user/i.htm?nekot=a2dkaXdzcw%3D%3D1281079123124
我的支付宝 – 支付宝


支付宝 知托付!
不安全 https://www.alipay.com
个人 企业 合作伙伴
支付宝 ALIPAY
首页 财富

常见安全隐患-钓鱼短信

常见安全隐患-朋友圈隐私泄露

- 晒娃
- 购物
- 旅游
- 美食
- 炫富

常见安全隐患-随意连接公共WIFI

黑客伪装成常用公共wifi，例如：cmcc-Starbucks

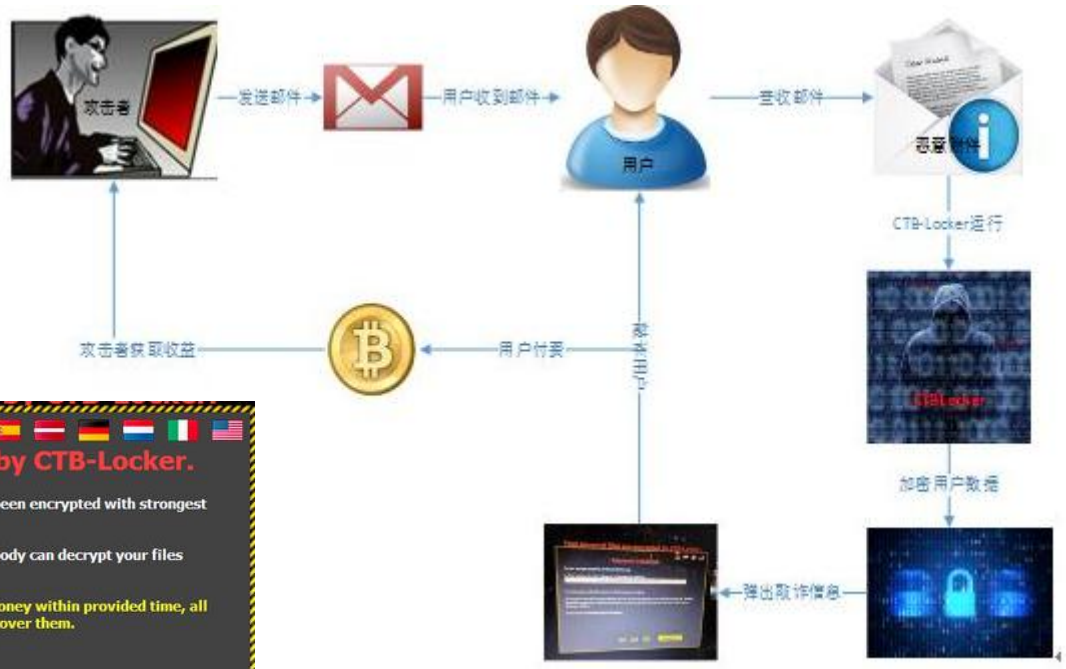
手机自动连接上后，黑客能得到你的手机型号、登录历史、设备使用者名称、语言设置和设备操作系统版本。

如果你在此时登录了你的邮箱或支付宝等，那么这些信息很容易就会被黑客获取。

更加恐怖的是，黑客还可以转移你访问的地址，他可以让你登录伪造的银行网址等，这样的网站完全受黑客控制，但你却一无所知。

常见安全隐患-勒索病毒邮件

攻击流程：

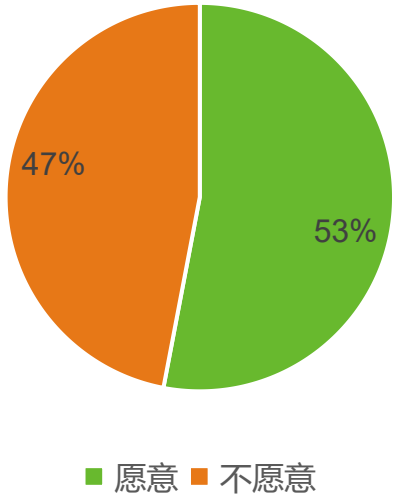


个人安全意识

中国人愿意用隐私换取便利---李彦宏

- 2017年5月31日，《南方都市报》与中国政法大学传播法研究中心联合发布《互联网企业隐私政策透明报告》。对1000家常用网站、APP的用户信息保护政策透明度进行排名，结果显示，测评的生活服务、休闲娱乐、医疗健康等各个领域1000家平台中，超过50%的网站与APP评分为“低”级别，令人担忧。**中国人对隐私问题更加开放，或者说没有那么敏感，如果要用隐私来交换便捷性或者效率的话，很多情况下中国用户是愿意这么做的。**

你愿意提供个人信息以获得更便利的服务吗?



神奇的“读心”大师


优酷
Your entire life is online.
网上有你的整个人生。
Heel je leven staat online.
Toute votre vie est en ligne.

二维码安全隐患

张先生是做家具定制生意的，近几年生意越做越大，他也开了一家网上旗舰店，双十一期间生意特别好。

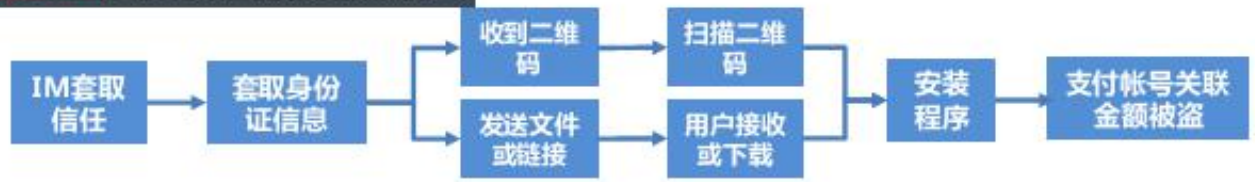
“前几天，有个人说他家里要装修，想定制些家具。那个人就和其他前来咨询的客人一样，没什么特别。”张先生每次回想这个事情，都特别懊悔。

“只是聊着聊着，那个买家突然说，他在外面，手机流量有限发不了那么多图，让我**扫描一个二维码**，下载后可以看到他想要的家具的图片和尺寸。”张先生说，“现在都流行扫一下二维码，我之前扫描过，很方便，就拿手机扫了一下。但是扫描后，我啥也没看到。”

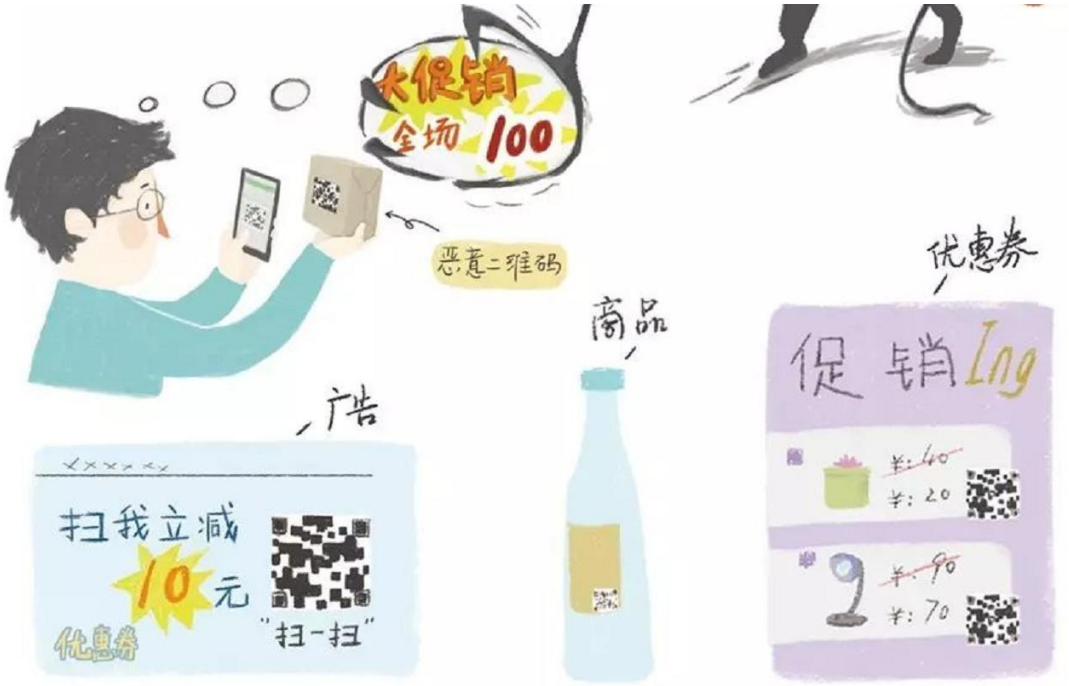
“后来我又和买家沟通了一会，他说先付些订金，问我要了姓名、身份证、银行卡、手机号等信息，说晚上回到家再汇款就下线了。”

晚上，张先生登录网银，看看买家的订金到账没有，却震惊地发现**银行卡内少了好几万**。张先生马上意识到自己被盗了，赶紧冻结了银行卡并向警方报案。

共同案情回放：



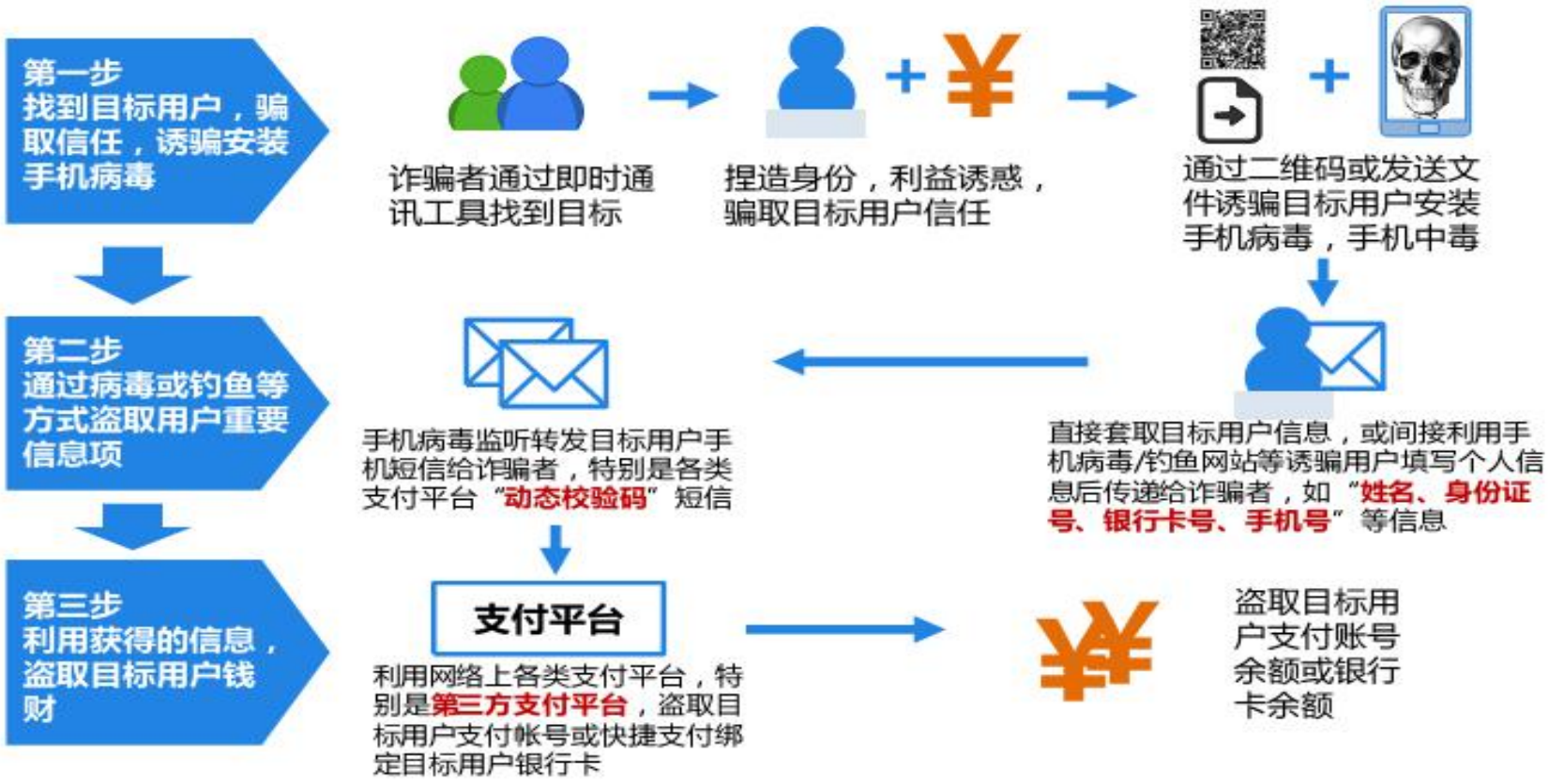
二维码安全隐患



虚假“优惠促销”

伪造付款二维码

二维码骗钱原理还原



不要轻信“二维码”！

个人信息安全概述

01 手机安全

02 社交安全

03 WIFI安全

04 个人安全防护

手机安全-系统及应用安全

- 操作系统不要越狱
- 采用指纹解锁
- 在安装手机软件时选择正规的软件市场下载安装
- 安装APP之前阅读隐私条例
- 及时安装系统和应用更新

手机安全-安全使用习惯

- 不要轻易的扫二维码
- 不要把手机连接到公共计算机上
- 不要使用公共充电器
- 借助第三方软件来保证手机的安全
- 不要把敏感信息存储在手机中
- 经常备份手机中的重要文件

社交安全-微信朋友圈

- 家人照片
- 地址
- 车牌号
- 贵重物品
- 行程信息
- 位置信息
- 个人身份信息

社交安全-微信安全使用习惯

- 给微信好友起个备注名
- 不要加陌生人为好友
- 与好友聊天过程中不要涉及敏感信息
- 借助第三方软件来保证手机的安全
- 不要把敏感信息存储在手机中

公共WIFI安全

01 接入公共场所WiFi网络时，应向店家确认WiFi名称和密码，避免接入未知来源的公共WiFi网络

02 尽量避免通过公共WiFi操作敏感业务，比如网银、购物或收发涉密邮件文件等。

03 不要将手机设置为自动连接WiFi网络。

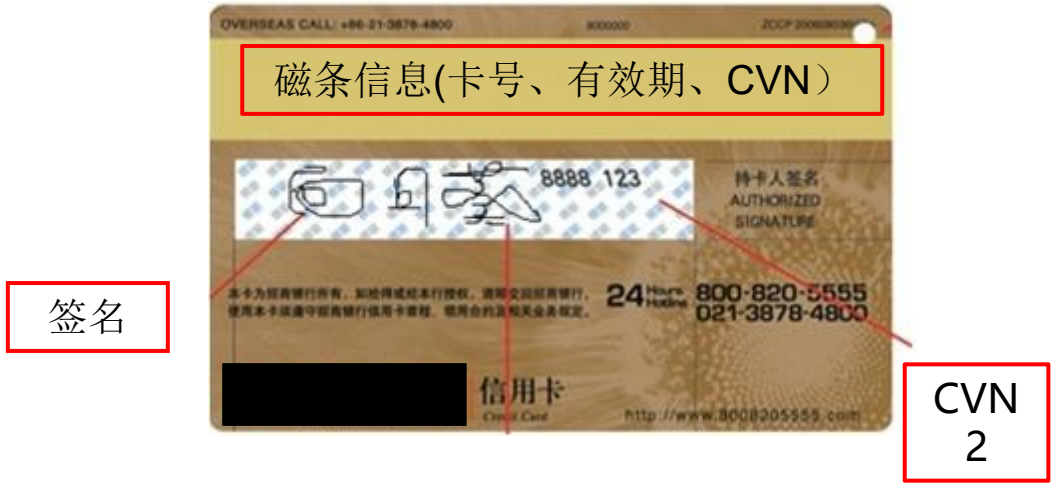
04 不要随意点击WiFi下推送的广告、下载链接等

个人安全防护-电脑安全

- 启用防火墙和防病毒功能
- 关闭USB设备自动播放
- 设置10分钟自动锁屏
- 不用的共享目录要及时关闭
- 使用非IE内核浏览器，谷歌、firefox等
- 设置强密码并定期修改
- 使用onedrive进行重要文件备份
- 使用BitLocker对磁盘进行加密

个人安全防护-支付安全

- **把磁条卡更换成芯片卡**
- **NFC信用卡使用卡套阻隔信号**
- **设置刷卡限额**
- **重点保护密码、磁道信息，卡片验证码（CVN和CVN2）、卡片有效期**



个人安全防护-四不提醒

- ✓ **不轻信**任何转账要求，务必电话确认。
- ✓ **不透露**短信验证码，发现手机收不到短信验证码马上送检。
- ✓ **不随意**点击链接，特别是聊天中发来的链接不要随意打开。
- ✓ **不在**非官方网站输入账号密码。

办公安全意识

安全小故事-1


1
会议室
为了便于工作沟通，我们今后建一个A产品QQ群进行沟通，离职员工会自踢的。
2
我已经离职一周了，也没人踢我。
A产品文档
一个月后……
3
你作为这个产品的经理，为什么竞争对手会拿到我们的产品研发文档？
4
得了，最近比较忙，忘了向HR要离职人员信息了，没有踢除QQ群里的离职员工。

安全小故事-2


ABC公司
哈哈，终于进了ABC公司内网了，看来破解一下ERP用户的密码。
1
这也太弱了吧
ERP系统破解成功
账号：小明
破解时间：1秒
破解结果：123456
2
这也难不倒我
ERP系统破解成功
账号：小红
破解时间：1分钟
破解结果：ABC123
3
我的密码可是8位的大小写字母+数字+标点哦！
ERP系统破解成功
账号：小强
破解时间：
预计10年
你牛，不搞你。
4

WANNACRY勒索蠕虫

- **时间：**2017年05月12日
- **目标：**未打MS17-010漏洞的windows系统
- **影响：**全球爆发了一系列勒索软件（Wannacry）的感染事件。国内大量企业遭到感染，多个高校的教育网受到感染，导致系统瘫痪。同时据英国广播电视台BBC报道，全球同一时间也爆发了多起勒索软件感染的事件，英国多家医院被感染，该勒索软件会加密被感染系统上的资料和数据，要求支付相应的赎金才会解密和恢复。包括俄罗斯，意大利，大部分欧洲国家，以及国内多所高校均被感染。

GLOBEIMPOSTER变种勒索病毒

- **时间：**2017年05月
- **方式：**通过垃圾邮件、社交工程、渗透扫描、RDP爆破、恶意程序捆绑等方式进行传播
- **影响：**近期我们发现GlobeImposter3.0变种勒索病毒在国内较大范围内传播。通过分析本次捕获的最新样本并未发现样本具备其他新的传播方式。该家族加密的后缀名也随着变种的不同在进行变化，已经出现的变种加密后的后缀名有：.CHAK、.crypted!、.doc、.dream、.TRUE、..726、.Alcohol、.FREEMAN、.ALC0、.ALC02等，本次截获的最新本加密文件后会修改文件后缀名为“.Tiger4444”，该变种依旧是利用RSA+AES加密的方式，用户中招后无法对文件进行解密。

勒索软件

什么是勒索软件?

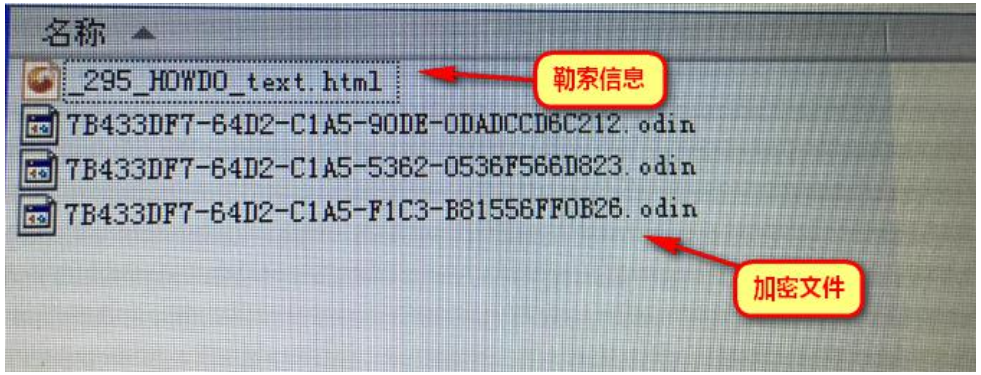
- 对受害者电脑进行文件加密并进行勒索;
- 支付赎金也未必能恢复文件;

勒索软件攻击流程

- 以钓鱼邮件的形式传播，邮件附件中往往包含经过伪装的恶意程序；受害者直接点击打开该恶意程序；（网页挂马、入侵、漏洞传播、文件感染）
- 恶意程序加密受害电脑上数据文件;
- 在受害者尝试使用文件时弹出勒索要求;

勒索软件 – 典型案例


管理功能
归档服务
FW: Orde
恢复
更多操作
主题: FW: Order Status #618540[报告垃圾邮件]
发件人: Graig Macias <MaciasGraig33@eclecticsofa.co.uk>
收件人:
附件: thank_you_order_618540.zip(8K) 全部打包下载
Dear henry,
We would like to thank you for your recent order.
Order Status updated on: 21/03/2016
Your Customer ID: 618540
Your Order ID: 4CE92A76AD-M-2016
Invoice Number: 3514560
Delivery Note:
We received your order and payment on 17/03/2016
Your order details are attached.
Best regards,
Graig Macias
Key Account Manager


名称
_295_HOWDO_text.html
勒索信息
7B433DF7-64D2-C1A5-90DE-0DADCCD6C212.odin
7B433DF7-64D2-C1A5-5362-0536F566D823.odin
7B433DF7-64D2-C1A5-F1C3-B81556FF0B26.odin
加密文件


!!!重要資訊 !!!!
的所有檔已被RSA-2048 和AES-128暗碼進行了加密。
獲取更多關於RSA的資訊，請參閱：
http://zh.wikipedia.org/wiki/RSA加密演算法
http://zh.wikipedia.org/wiki/高级加密标准
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
有我們的機密伺服器上的私人金鑰和解密程式才能解密您的檔。
要接收您的私人金鑰，請點擊以下其中一個連結：
1. http://6dtxgqam4crv6rr6.tor2web.org/85C5EC6C40
2. http://6dtxgqam4crv6rr6.onion.to/85C5EC6C40141
3. http://6dtxgqam4crv6rr6.onion.cab/85C5EC6C4014
4. http://6dtxgqam4crv6rr6.onion.link/85C5EC6C40141
果以上位址都無法打開，請按照以下步驟操作：
1. 下載並安裝洋蔥流覽器（Tor Browser）：https://www.torproject.org/download/download-easy.ht
2.安裝成功後，運行流覽器，等待初始化。
3. 在位址欄輸入: 6dtxgqam4crv6rr6.onion/85C5EC6C4
4.按照網站上的說明進行操作。
您的個人識別ID: 85C5EC6C40

勒索软件 – 如何防范

已经中招的用户暂时没有办法解密文件，可以将已加密的文件保管好等待互联网上安全人员研究并公开相关解密工具，不要寄希望于付费进行解密，在较大情况下都是骗局。

- 定期异地备份重要文件；
- 针对来历不明邮件中的附件，切勿随意打开；
- 在windows中设置显示文件扩展名，对于不熟悉的的文件扩展名，切勿双击打开；
- 针对office中的宏提示，不要进行点击运行。
- 设置高强度远程桌面登录密码并妥善保管；
- 安装防病毒软件并保持良好的病毒库升级习惯；
- 对内网安全域进行合理划分，各个安全域之间限制严格的ACL，限制横向移动；
- 关闭不必要的共享权限以及端口，如：3389、445、135、139。
- 完善安全防护体系，保持良好的上网习惯，安全意识是关键。

2018年度最不安全密码报告

最烂密码

2018年末，密码管理公司SplashData公布了2018年度最新最烂密码，他们从500万个密码样本总结了这个榜单：

	2018 最不安全密碼名單前 25 名	跟 2017 比較
第 1 名	123456	不變
第 2 名	password	不變
第 3 名	123456789	↑3
第 4 名	12345678	↓1
第 5 名	12345	不變
第 6 名	111111	新入圍
第 7 名	1234567	↑1
第 8 名	sunshine	新入圍
第 9 名	qwerty	↓5
第 10 名	iloveyou	不變

弱口令调查

2017年11月，科技行业咨询企业EPC Group对600名用户进行调查，发现：

- 37%的受访者承认只有当网站要求他们更换密码时才会更改；
- 11%的受访者表示，同一个密码（或者稍有变化）至少会用7年；

数据泄露 – 如何应对?

- 发生重要泄漏事件后

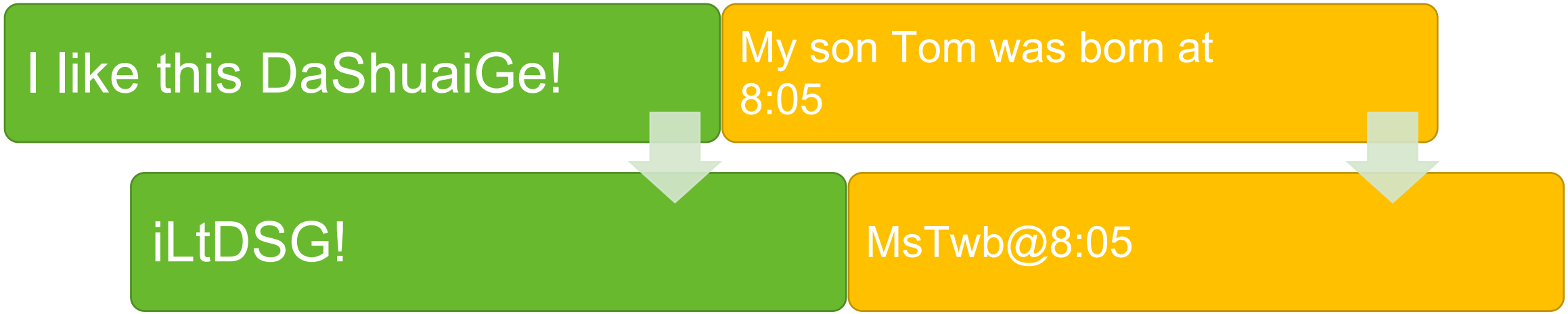
使用多个帐号密码体系：

- 一般网站群：视频网站、游戏网站、各类论坛 等等...
- 重要帐号：微信、支付宝、网银

数据泄露 – 如何应对?

口令设置

找到一个生僻但易记的短语或句子（可以摘自歌曲、书本或电影），然后创建它的缩写形式，其中包括大写字母和标点符号等。



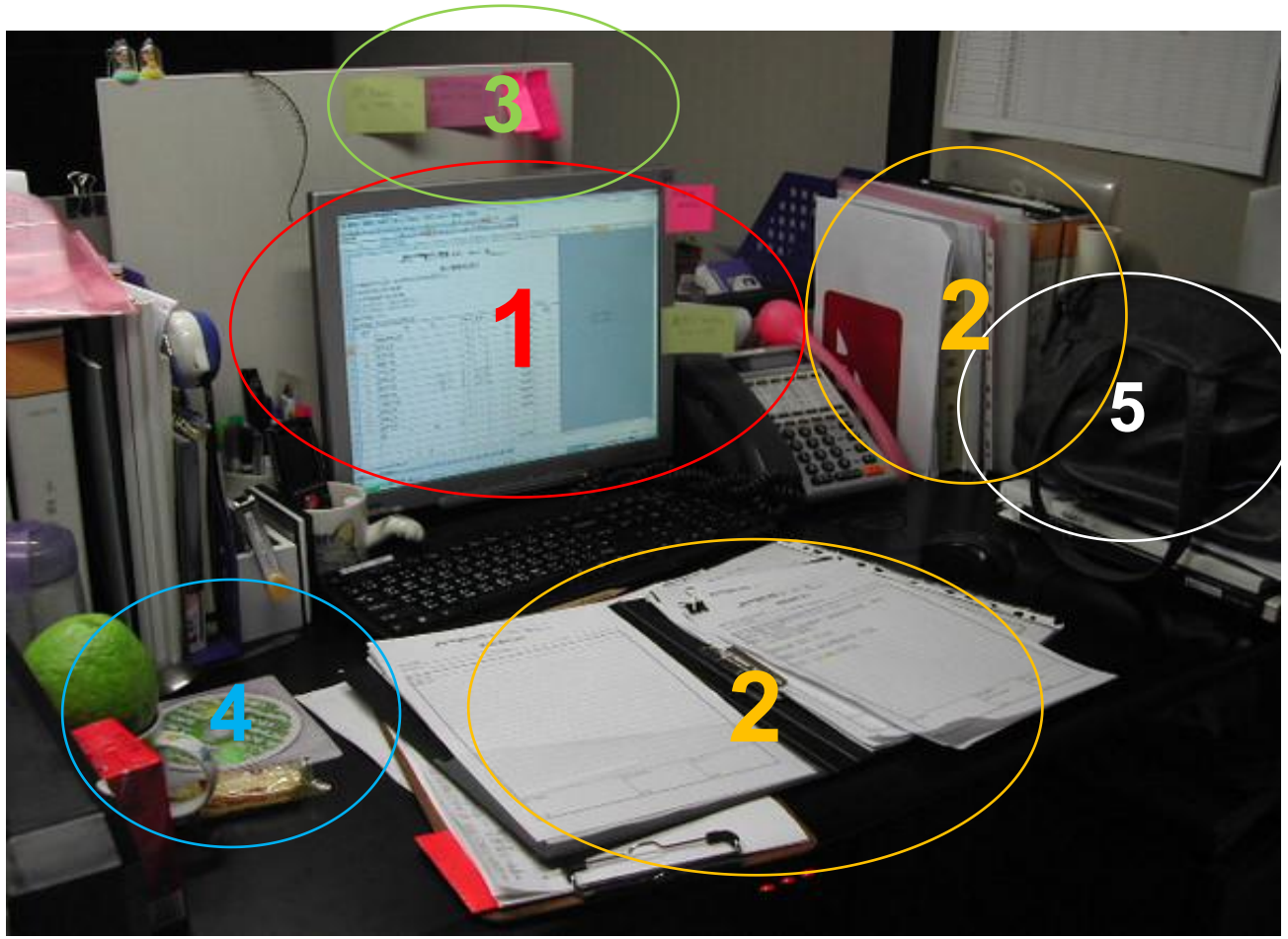
数据泄露 – 如何应对?

季军：FLZX3000cY4yhl9day
飞流直下三千尺，疑似银河下九天

亚军：han-shansi.location()!∈[gusucity]
姑苏城外寒山寺

冠军：hold?fish:palm
鱼和熊掌不可兼得

问题出在哪里?



给普通员工的安全建议

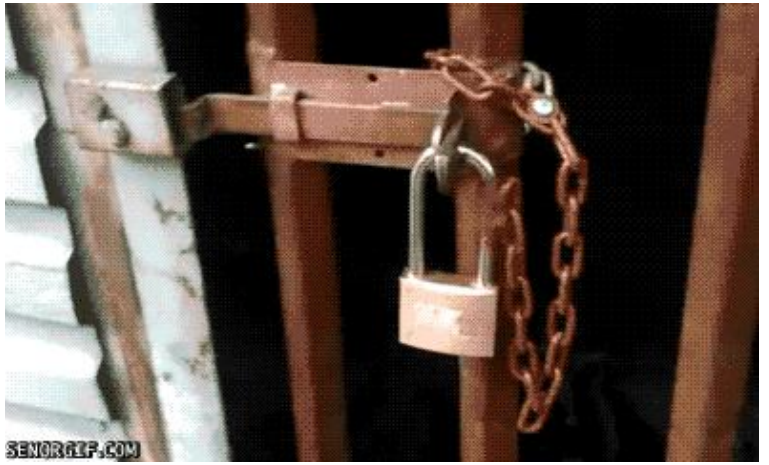
培养安全办公习惯

- 进入大门、闸机时主动阻止陌生人尾随进入；
- 陌生人员未经陪同出现在办公区域，应主动上前询问；
- 废弃的纸质资料应该进行充分粉碎（碎纸机）；
- 废弃的移动存储设备应交由IT部门消磁处理；
- 离开工位时对办公电脑进行锁屏；
- 敏感资料应妥善保管，在离开工位时锁入柜中；
- 不应使用来历不明的移动存储设备；
- 不应接入来历不明的WiFi热点；
- ……

环境安全

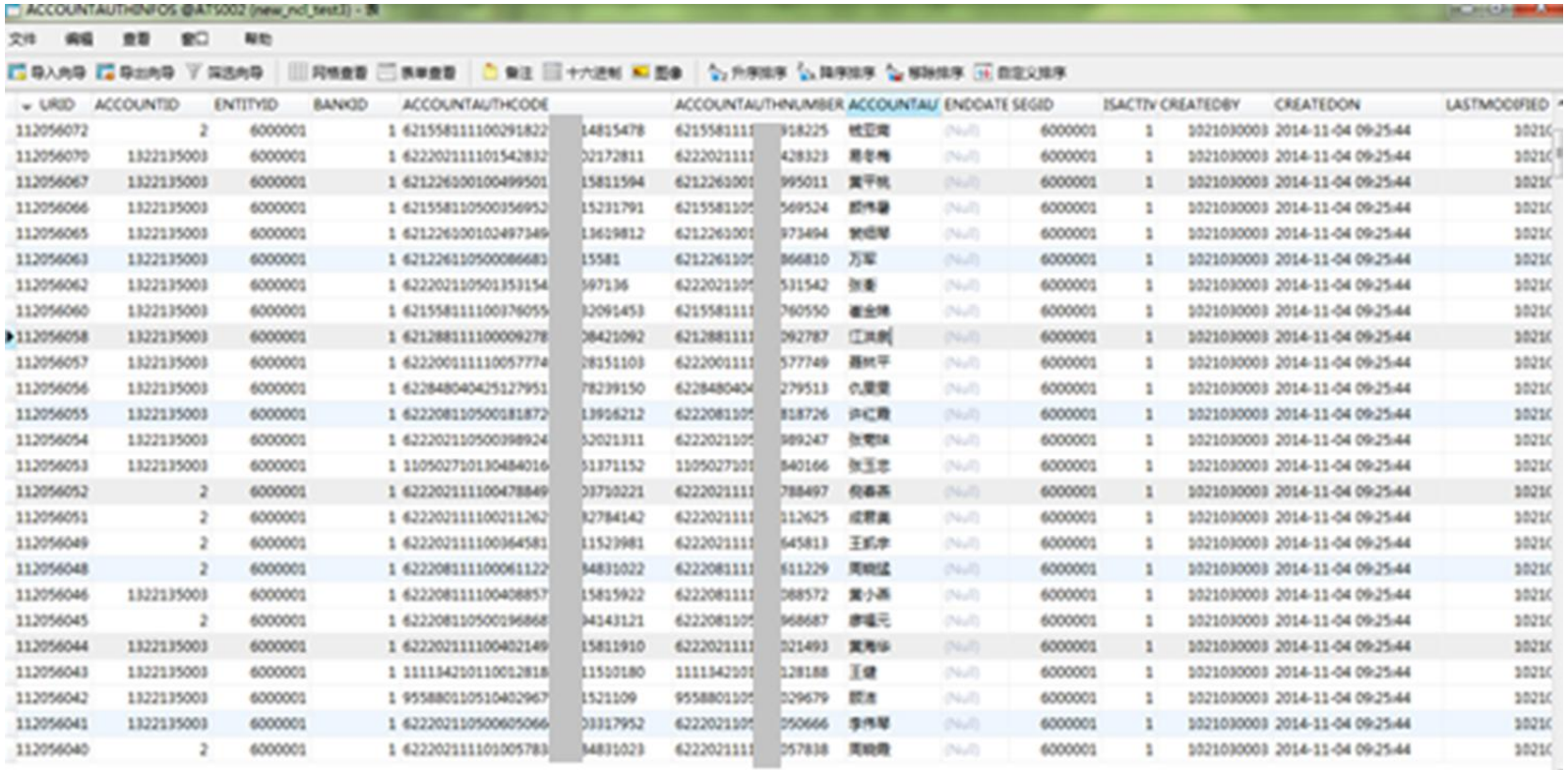
1. 不在网络或社交媒体上发布公司信息；
2. 不利用公司资源做非工作相关的信息交换；
3. 不在公共区域使用电话讨论公司机密信息；
4. 公司机密信息文件要妥善保存，不带离办公区域；
5. 不在微信群中讨论公司机密信息。

弱口令、弱口令、弱口令！



某大型保险公司全网测试

- 网络架构、防护措施到位，无可利用的系统和应用漏洞；
- 发现边界存在一台JBOSS主机，管理台存在**弱口令**；
- 逐层渗透，控制大约200台服务器，最终成功获取**核心交易数据。**



正确认识信息安全

“真正安全的计算机是拔下网线，断掉电源，放在地下掩体的保险柜中，并在掩体内充满毒气，在掩体外安排士兵守卫。”

------绝对的安全是不存在的！

正确认识信息安全

“安全不只一次性的静态过程，它密结合的系统工程，是过程。”

信息安全人人有责

遵守单位的操作规程

设置强壮的密码，并定期修改

在系统建设、维护和使用中，基于本职工作，多考虑安全问题

做好终端安全配置，减少暴露的风险点

提高安全防范意识，多留心可疑事件，及时向本部门安全员报告