网络安全意识培训

信息管理中心

2019-05-20

目录

CONTENTS

第一篇　上网安全

网络安全风险无处不在

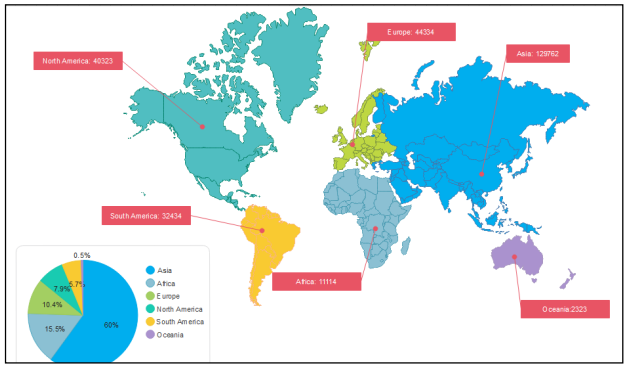
“四个假设”正在逐渐变为确定现实——

- 假设系统一定有未被发现的漏洞
- 假设一定有已发现但仍未修补的漏洞
- 假设系统已经被渗透
- 假设内部人员不可靠

最流行的网络攻击——勒索病毒：WannaCry 索要比特币

事件概况

2017年5月12日，黑客组织利用泄露的NSA黑客数字武器库中“永恒之蓝”工具发起蠕虫病毒攻击进行勒索，中毒计算机文件将被锁定，需支付赎金比特币才能解锁。



影响范围

- 勒索软件已攻击99个国家的数千家企业及公共组织，美国至少1600家、俄罗斯至少11200家受到攻击
- 我国感染范围覆盖了几乎所有地区，遍布高校、加油站、医院、政府办事终端等各大领域，超30万台机器中招，至少有28388个机构被感染

事件分析

- 虽然下黑手者目前还找不到，但其所用的工具，却明确无误地指向了一个机构——NSA，永恒之蓝就是NSA针对微软MS17-010漏洞所开发的网络武器，2013年6月，“永恒之蓝”等十几个武器被黑客组织“影子经纪人”（Shadow Brokers）窃取并公布；
- 2017年3月，微软已经放出针对这一漏洞的补丁，但是一方面由于一些用户没有及时打补丁的习惯，二是全球仍然有许多用户在使用已经停止更新服务的Windows XP等较低版本，无法获取补丁，因此在全球造成大范围传播。

启示：打补丁这件事不要心存侥幸！

最流行的网络攻击——勒索病毒：新一轮勒索“Petya”

事件概况

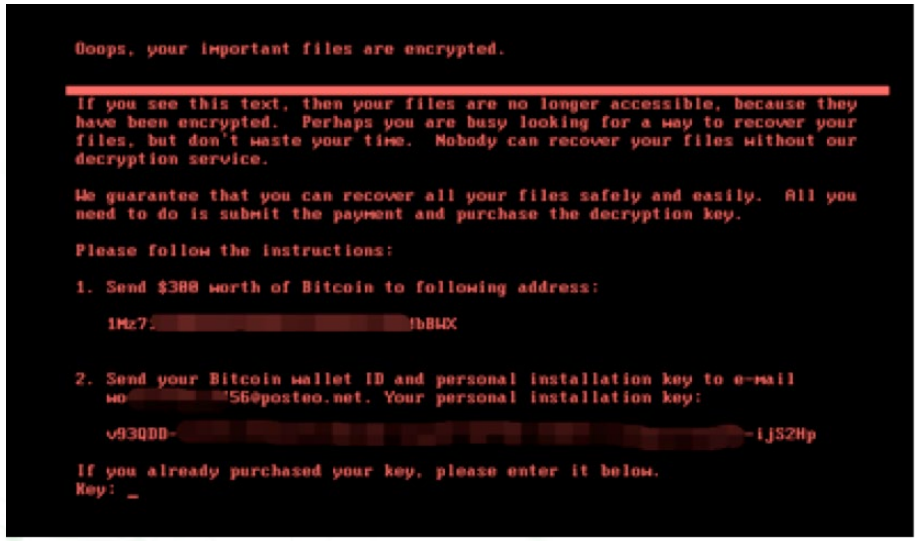
“WannaCry”还没有结束，2017年6月27日，新一轮勒索病毒“Petya”袭击了欧洲多个国家，包括乌克兰、俄罗斯、印度、西班牙、法国、英国、丹麦等国在内都遭受了攻击;

事件影响

此病毒相比“WannaCry”更具破坏性,开机界面上留下来的信息即使提供给黑客也是没有办法进行解密的，因此，不得不怀疑此次“Petya”病毒的真正目的。“Petya”更像是在做有目的性的攻击，对目标进行无法修复的破坏性攻击，而并非以敲诈勒索为目的。

事件分析

Petya同样利用了MS17-010(永恒之蓝)的SMB漏洞，感染局域网中开放445端口的所有终端及服务器。



启示：

（1）同样的漏洞有可能被重复利用；

（2）新一轮勒索软件的重要新用途之一不仅是敲诈勒索，而是无法修复的破坏!

安全软件务必装，自家大门要看好

安全软件

现代安全软件是电脑，手机的必备软件，一般包含以下几大功能：

- **防病毒，防木马**
- **反钓鱼，反诈骗**
- **打补丁，修系统**
- **垃圾清理，系统加速**
- **软件管理，权限管理**

一般来说，只要经常用安全软件给电脑、手机做体检，多数安全问题都能“一键”解决。

特别提示：

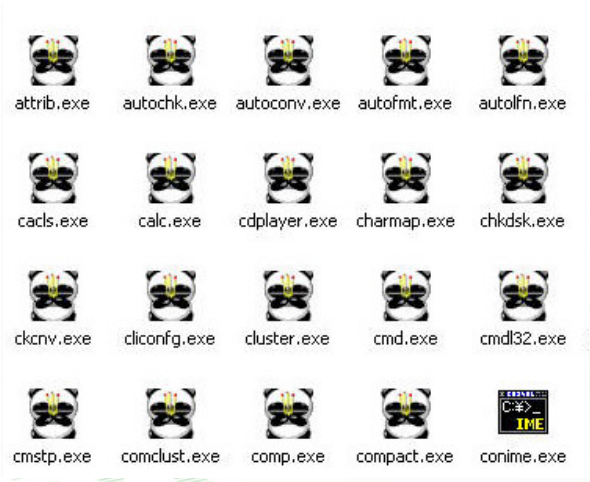
有些会“卖萌”的病毒或者是网络骗子会谎称安全软件有“误报”，建议你暂时关闭安全软件。千万不能信啊！

定期体检打补丁，提前免疫不得病

打补丁：

打补丁是为了修漏洞。系统不打补丁，就像家里不关门窗，很容易被入侵。存在漏洞的系统，安全软件也很难有效防护。

2003年8月，冲击波病毒利用微软已经修复的漏洞发起攻击，一周之内感染了全球约80%的电脑。



2007年1月，熊猫烧香病毒利用Windows漏洞肆虐全国，这是最为臭名昭著的一款“国产”病毒。

2017年5月，WannaCry勒索蠕虫利用漏洞永恒之蓝发起攻击，30个小时内就使100多个国家的大量机构陷入瘫痪。

打补丁工具

使用U盘先杀毒，危险文件入沙箱

U盘防护

U盘又称病毒“摆渡”，常用来攻击隔离网中的电脑。

著名的“震网病毒”就是通过U盘入侵伊朗核电站并实施破坏。

U盘、移动硬盘一定要先查毒，后使用

沙箱

一种虚拟的软件运行环境，木马病毒运行在其中，只会破坏沙箱内的虚拟系统，不会危及真实的电脑系统。

破解软件、外挂程序、种子文件、色情文件等，都有可能是木马程序。如果实在想要看看究竟，可以把它们丢进沙箱。

陌生来电不轻信，不明链接不要点

诈骗电话与骚扰电话

伪基站的仿冒短信

短信中的带毒短链接

社交软件欺诈链接

安全软件一般无法检测社交软件中网址链接的安全性

用社交软件转发网页，网址也会被隐藏

防骗，只能擦亮眼睛

特别提示：

外来的、陌生的、你不熟悉的东西都可能有危险，电话，短信、网络社交皆如此。

二维码中藏奥秘，随手扫描易中招

二维码

二维码实际上是一个图形化的数据信息，信息中可以存储文本、网址等各类信息。

二维码生成器

网上可以搜索到很多二位码生成器，任何人都可以很容易的生成一个二维码

随意扫码的风险

- 扫码打开的网页可能含有欺诈信息、木马病毒
- 扫码后被要求填表，可能泄露个人信息
- 扫码后可能会进行“无意识支付”，被骗钱财

特别提示

- 扫码后提示下载陌生文件的，谨慎
- 扫码后要求填写个人信息的，谨慎

删除资料能恢复，二手交易猫腻多

文件删除

无论是在电脑上还是手机中，被删除的文件通常可以使用某些专用工具恢复出来，想要彻底删除，需要进行文件“粉碎”。

文件恢复与文件粉碎功能

出厂设置

在手机上“恢复出厂设置”也不能彻底删除文件，仍然可恢复。

隐私擦除

彻底擦除手机隐私方法

- 删除信息后，用视频等大文件复制并占满手机存储空间，即可彻底擦除原有数据
- 使用360安全换机中的“隐私粉碎机”

特别提示：

若未能妥善处理手机中原有资料，一旦手机被黑心二手商贩收购，他们很有可能会恶意恢复手机信息，并贩卖到网络黑市。

“把电脑拿去修，是我活这么大最后悔的一件事。”

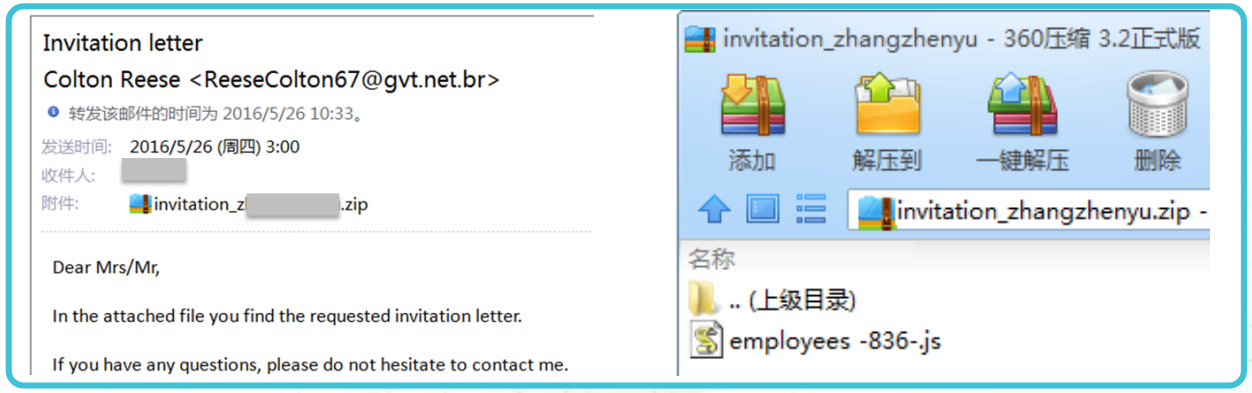
—— 陈冠希

第二篇 办公安全

邮件附件常带毒，陌生来源勿打开

勒索邮件

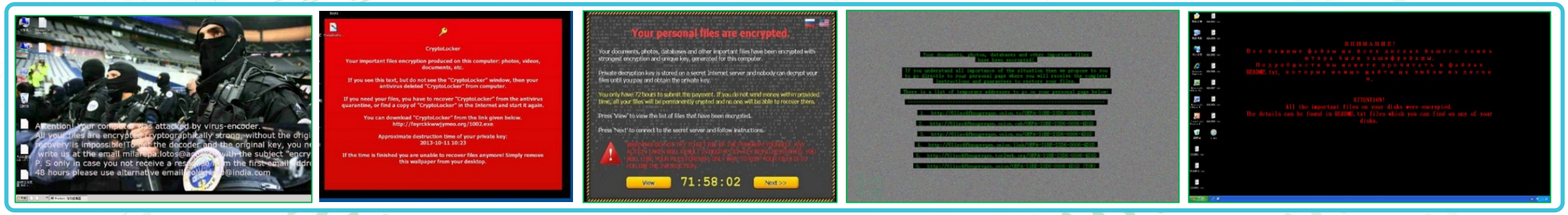
下面这封不起眼的邮件携带了一个ZIP格式的附件，解压后生成一个JS文件，它实际上是一个勒索软件，一旦点击打开，电脑中所有的办公文档、照片、视频都会被加密，只有向勒索者支付赎金后才能解密。



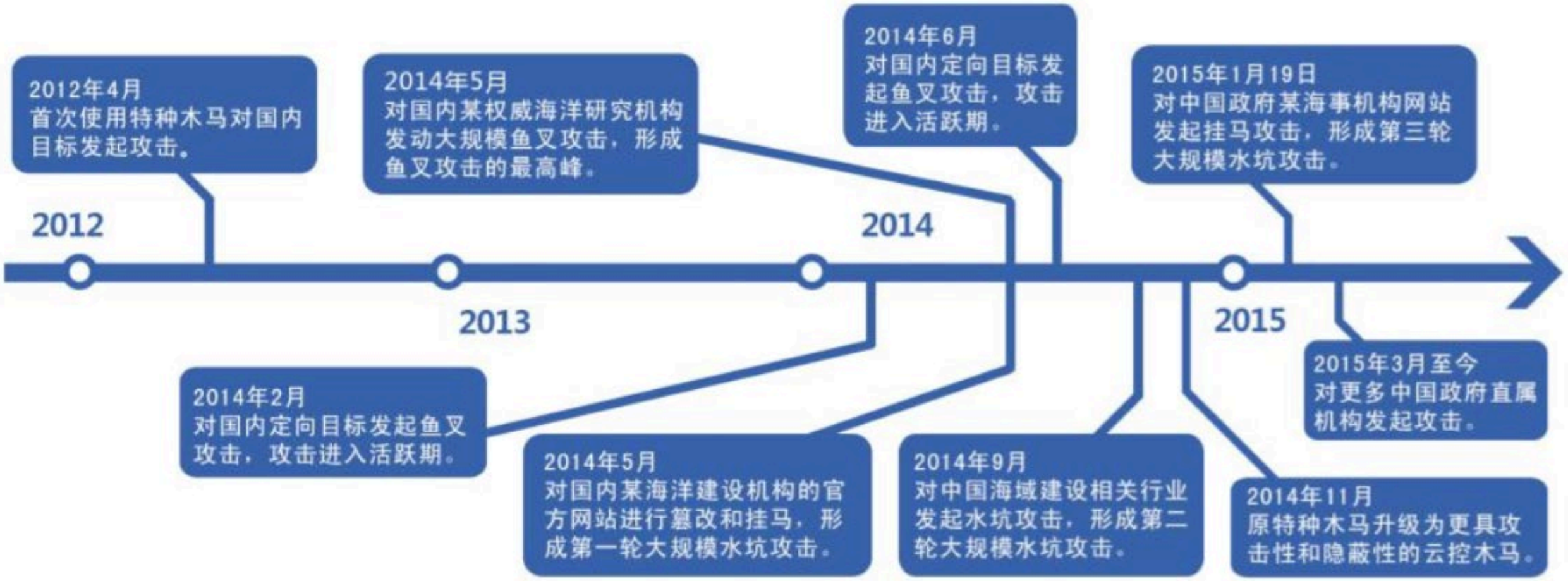
窃密邮件

2016年6月，一封带毒邮件盗走日大型旅社800万用户资料。

勒索软件中招后屏幕的现象



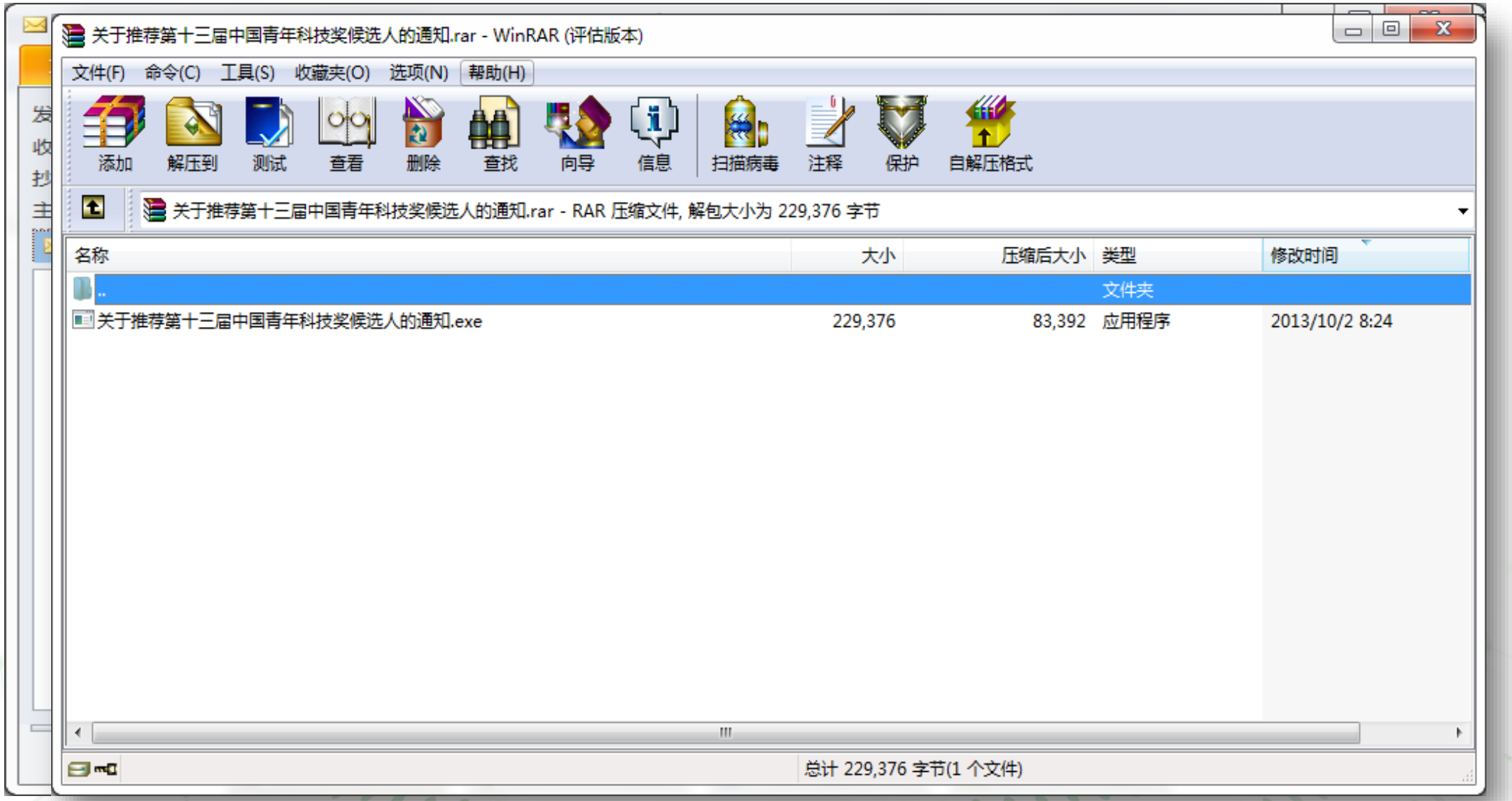
“海莲花”APT攻击


2012年4月
首次使用特种木马对国内目标发起攻击。
2014年5月
对国内某权威海洋研究机构发动大规模鱼叉攻击，形成鱼叉攻击的最高峰。
2014年6月
对国内定向目标发起鱼叉攻击，攻击进入活跃期。
2015年1月19日
对中国政府某海事机构网站发起挂马攻击，形成第三轮大规模水坑攻击。
2012
2013
2014
2015
2014年2月
对国内定向目标发起鱼叉攻击，攻击进入活跃期。
2014年5月
对国内某海洋建设机构的官方网站进行篡改和挂马，形成第一轮大规模水坑攻击。
2014年9月
对中国海域建设相关行业发起水坑攻击，形成第二轮大规模水坑攻击。
2014年11月
原特种木马升级为更具攻击性和隐蔽性的云控木马。
2015年3月至今
对更多中国政府直属机构发起攻击。

走过最深的路就是黑客的“套路”

走过最深的路就是黑客的“套路”

- 可疑邮件

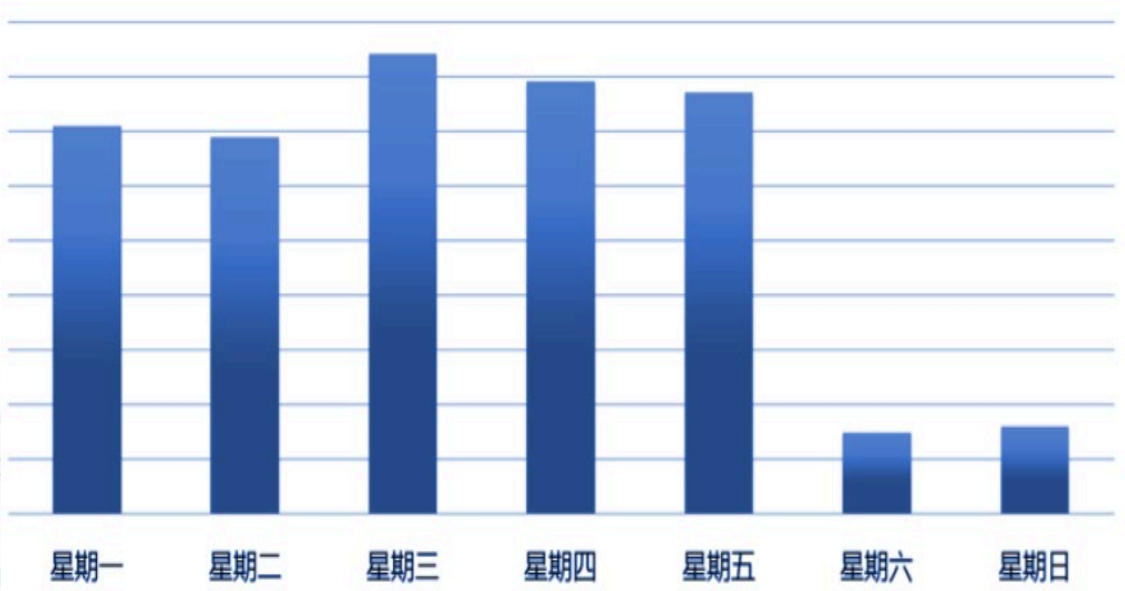


走过最深的路就是黑客的“套路”

鱼叉攻击

相关文件名
关于国家***研究中心工程建设的函.exe
国家**局的紧急通报.exe
最新新疆暴动照片与信息.jpg.exe
本周工作小结及下周工作计划.exe
厅关于印发《2014 年应急管理工作要点》的通知.exe
2015 年 1 月 12 日下发的紧急通知.exe
商量好的合同.exe
部关于开展 2015 年调查工作的通知.exe

鱼叉邮件附件



鱼叉攻击周期

收信看清发件人，冒名顶替要当心

电子邮箱收件人的信息由邮件显示名和邮件地址两部分组成，而邮件地址又是由邮箱帐号和邮箱域名组成。

特别提示：

- **显示名很容易被仿冒**

  邮件的显示名通常可以由发件人任意编写.骗子们经常把邮件显示名伪装成：管理员、XX机构、XX领导等。

- **邮箱帐号也可能被仿冒**

  如，真实邮箱是zhangsan@263.com,仿冒邮箱却是zhangsan@qq.com，不仔细看很难分辨。

  所以，收到邮件不能光看显示名，还要认真查看发件人的邮件地址以及邮箱域名，稍不留心就可能上当受骗。

办公邮箱不乱用，到处注册风险多

电子邮箱

电子邮件是政企机构办公的重要工具。
中国境内企业级电子邮箱活跃用户规模约为1.2亿。
企业级用户平均每天收发到电子邮件约16.1亿封。

特别提示：

切勿使用办公邮箱注册游戏、购物、社交、论坛等第三方应用账户，否则会有如下风险：

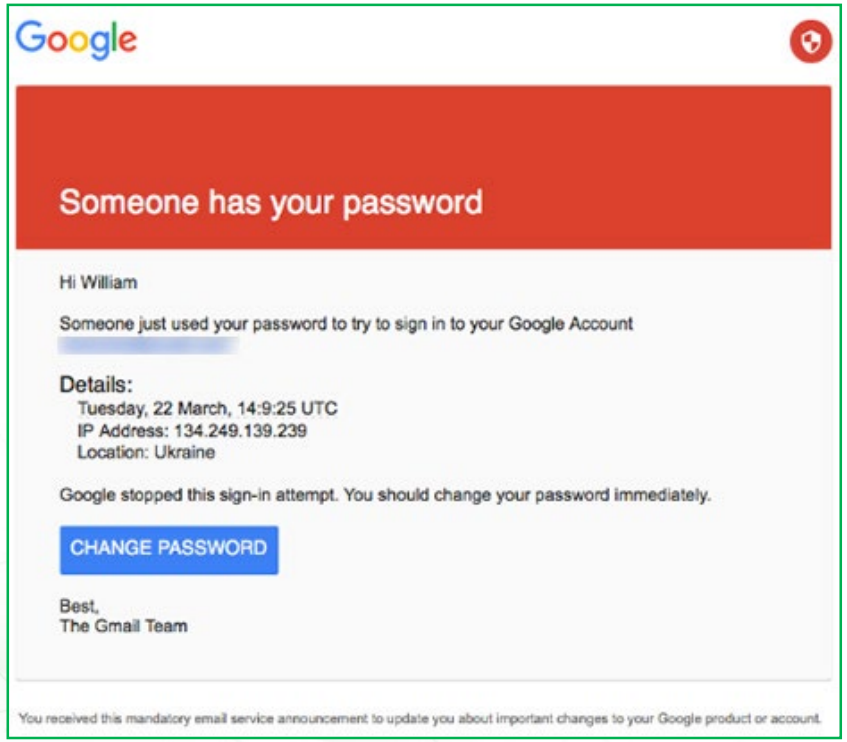
- 您的办公邮箱中会收到很多垃圾邮件。
- 一旦第三方应用平台被黑，您办公邮箱的帐号和密码也可能会
- 同时泄露，造成邮件中的机密外泄。
- 办公邮箱密码泄露，可能引发连锁反应，进而泄露机构内网帐
- 号，导致内网被黑客入侵。

OA 钓鱼最危险，美国大选也中招

OA钓鱼

冒充系统管理员发送的欺诈邮件被称为OA钓鱼。
OA钓鱼多用于盗号。

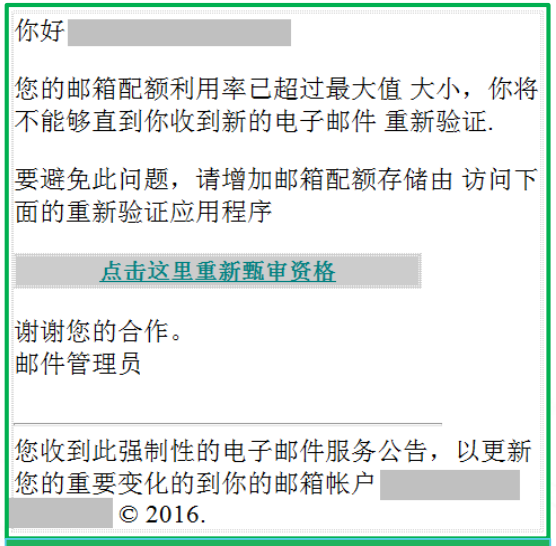
2016年美国大选，黑客组织冒充Google邮件系统安全管理员给希拉里竞选团队负责人发信，骗取了负责人的邮箱密码，盗取并公布了希拉里竞选团队的机密邮件，最终使得希拉里败选，特朗普上台。



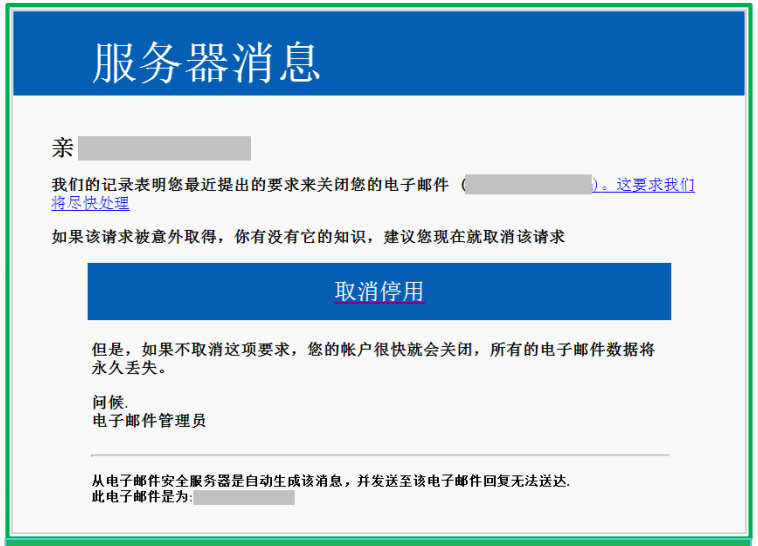
希拉里竞选团队成员William Rinehart收到的伪装成Google安全团队的鱼叉邮件

骗你上当有理由，仿冒登录盗帐号

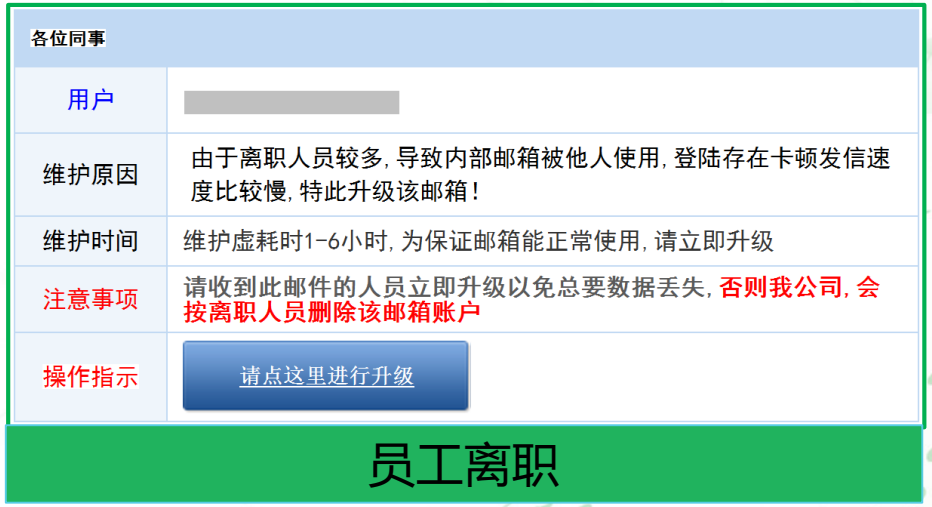
安全性升级



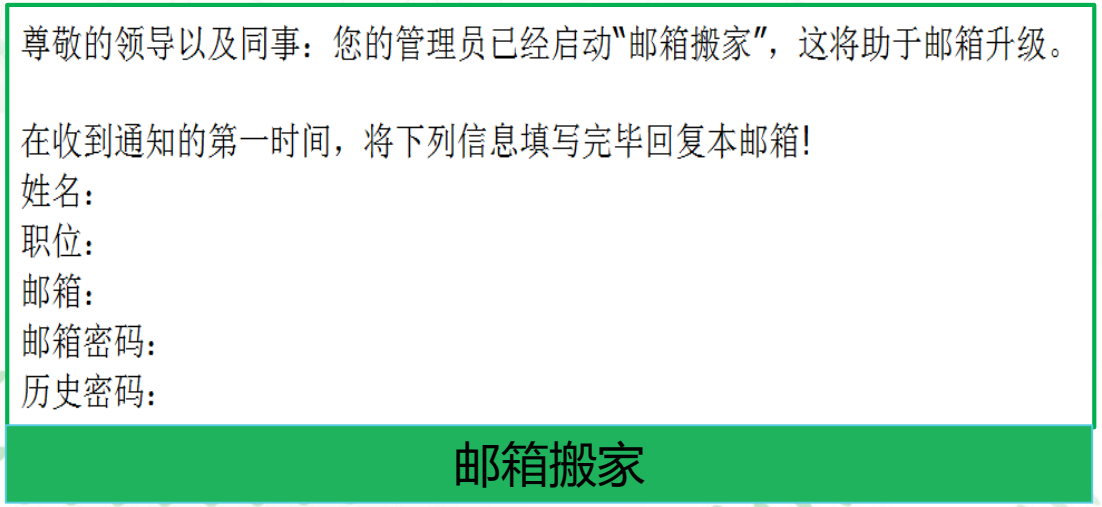
邮箱扩容



邮箱停用



员工离职



邮箱搬家

OA钓鱼手法

- OA钓鱼的目的是诱骗受害者在虚假的登录页面上输入帐号和密码，进而实现盗号。
- OA钓鱼的“理由”有很多，左边几个都是，您能认得出吗?

密码设置强度高，验证短信不外泄

密码的四项基本原则

密码是所有帐号安全的基本保障，设置密码一般需遵守以下原则：

- **15位以上**
- **数字+字母+特殊符号**
- **定期修改（建议180天）**
- **支付、社交、邮箱等核心帐号单独设密码**

动脑时间

你能在2分钟内记住下面三个密码吗？哪一个密码最安全？你知道怎样构造一个又长又好记的密码吗？

chuangqianmingyueguangyishidishangshuang

xiaobaitu2baiyoubai3liangzhierduoshuqilai4

@xiyangyang#yuhuitailang$123

特别提示：

- 帐号一旦被盗，应立即修改所有其他相关帐号的密码
- 短信验证码是一种动态的密码，千万不要告诉任何人

安全习惯早养成，提高警惕少出错

尽量不要在微信上谈工作

微信是比较开放的社交环境，不适合谈论工作。办公社交建议使用企业级社交软件。

不在电脑桌前电脑要锁屏

电脑锁屏，既可以防止他人偷窥到自己电脑中的文件，又可以防止他人胡乱操作损坏文件。

保存文件尽量不要用密字

保存文件时文件名尽量不要包含密、秘密、保密、绝密等字样，这些字很容易被黑客盯上。

下班以后一定要关闭电脑

很多人为图方便，下班以后不关电脑，这就给黑客留出了更多电脑前无人值守的攻击时间。

连接WiFi要谨慎，蹭网心态吃大亏

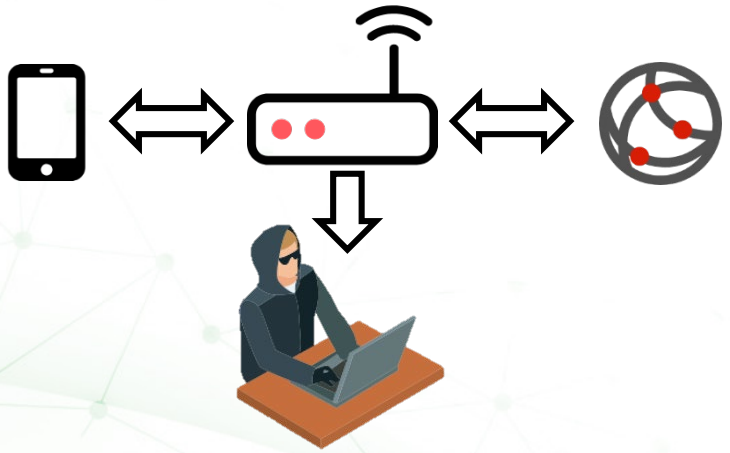
WiFi的安全风险

WIFI是一种短距离局域网无线传输技术，数据在传输过程中通常不加密。如果有黑客恶意监听无线路由器上传输的数据，数据将被黑客窃取。

2015年央视315晚会，安全专家现场演示如何通过免费WiFi盗取现场观众的上网信息，演示包括对照片、文字、帐号和密码等信息的窃取。

蹭网软件的风险

- 蹭网软件可以帮你免费使用他人WiFi
- 但也可能泄露自己家中的WiFi密码
- 连接不安全的WiFi可能被盗号、诈骗



特别提示：

公共场合链接WiFi，一定要选择官方的，有密码的。无密码的WiFi最危险。

WiFi易成突破口，私建网络是祸根

私建WIFI热点的风险

私自搭建WiFi热点，并将内网中的设备与热点相连，将会在内网边界上打开突破口，使网络隔离完全失效。

一旦内网出现突破口，木马、病毒、黑客，都会乘虚而入。

WannaCry勒索蠕虫会攻击隔离网设备的重要原因之一就是有员工在内网之中自搭乱建WiFi热点。

2015年3月，天河一号内部员工私自搭建WiFi热点，导致超级计算机天河一号被入侵，大量敏感信息疑遭泄漏。

第三篇　谨防诈骗

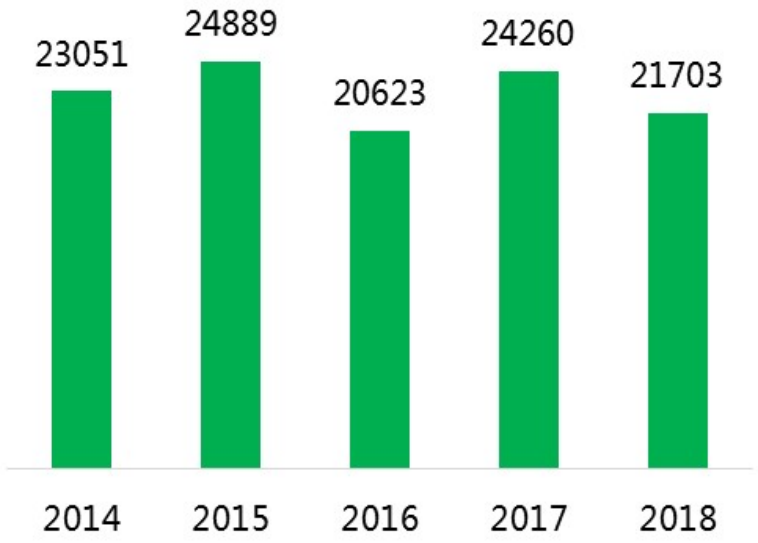
网络诈骗/电信诈骗

坏人猖獗，形势严峻

网络诈骗依然很猖獗

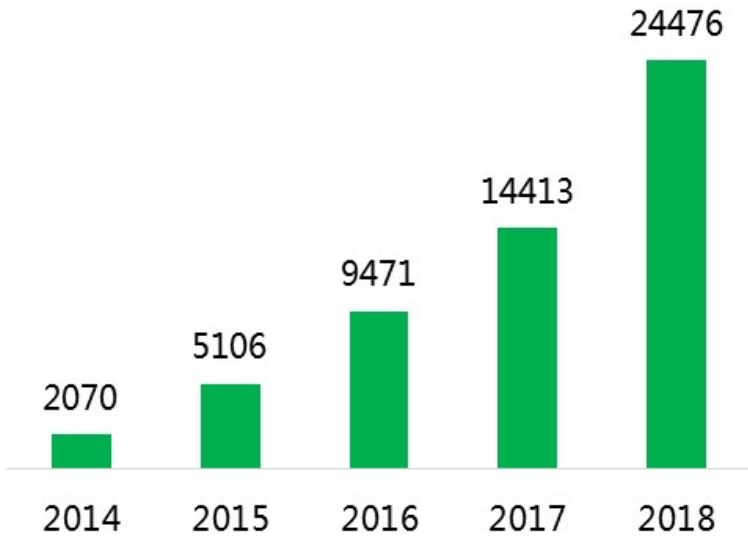
2014-2018年网络诈骗举报数量及人均损失

2014-2018年网络诈骗举报数量



猎网平台

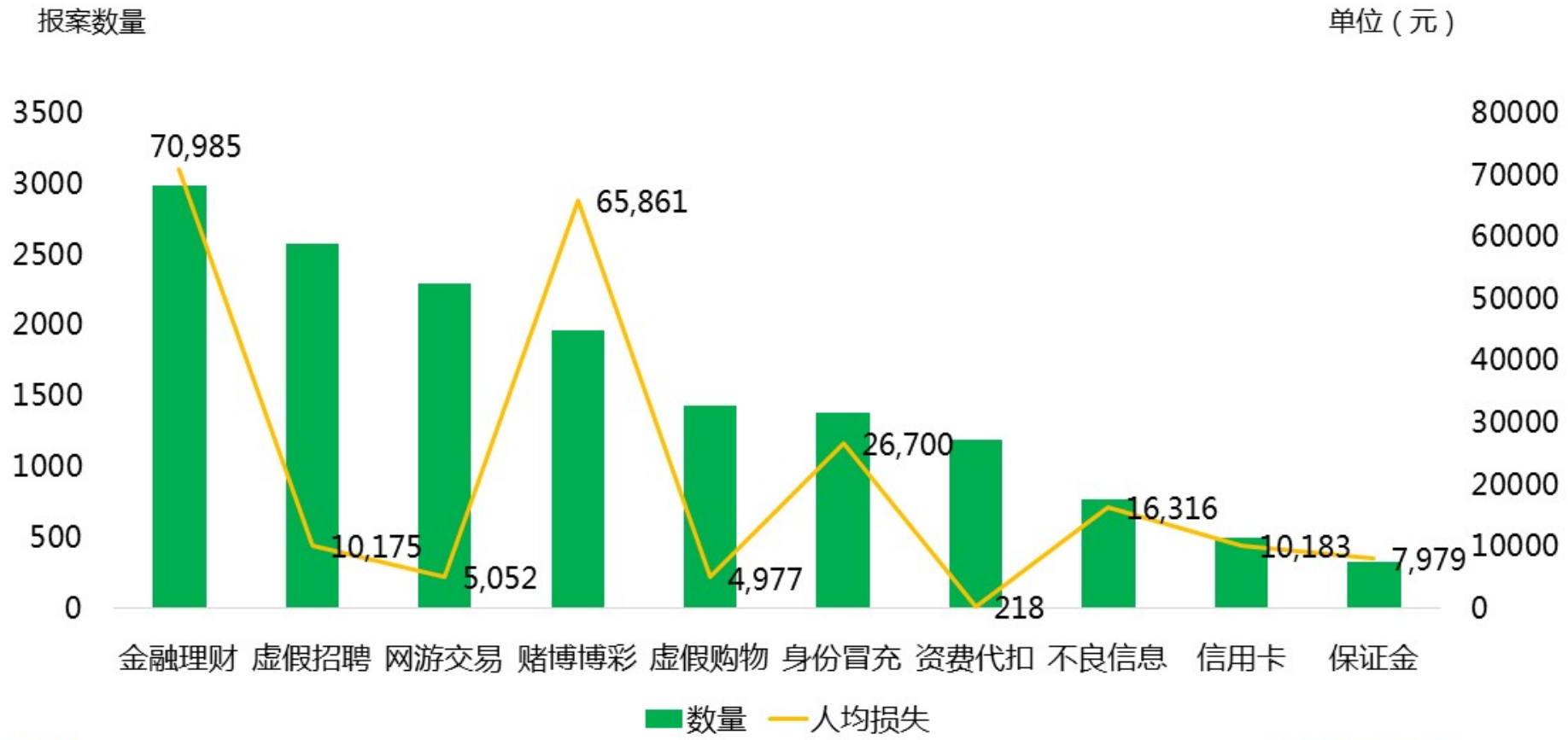
2014-2018年网络诈骗人均损失（元）



360 互联网安全中心

网络诈骗依然很猖獗

2018年网络诈骗主要类型举报量及人均损失



猎网平台

360 互联网安全中心

七大类典型电信诈骗

43.2%金融理财诈骗

3.3% 虚假中奖诈骗

25.2%身份冒充诈骗

2.8% 充值优惠诈骗

10.2% 推销违法业务诈骗

8.4% 推销假冒伪劣商品

2.4% 推销假医假药保健品

骗子们的十大冒充十大“装”

26.0%运营商

21.2%领导

快递14.3%

12.5%医保社保机构

5.7%有关部门

5.7%商家客服

5.3%银行

3.9%公检法

2.9%学校

1.5%亲友

网络诈骗的产业规模

从业人口：160万+

产业规模：1152亿+

计算方法：

诈骗电话：1601万次/天（360，2015Q2）

电话诈骗经理：至少16万人（100个/人天）

产业链人数：>=1+9=10

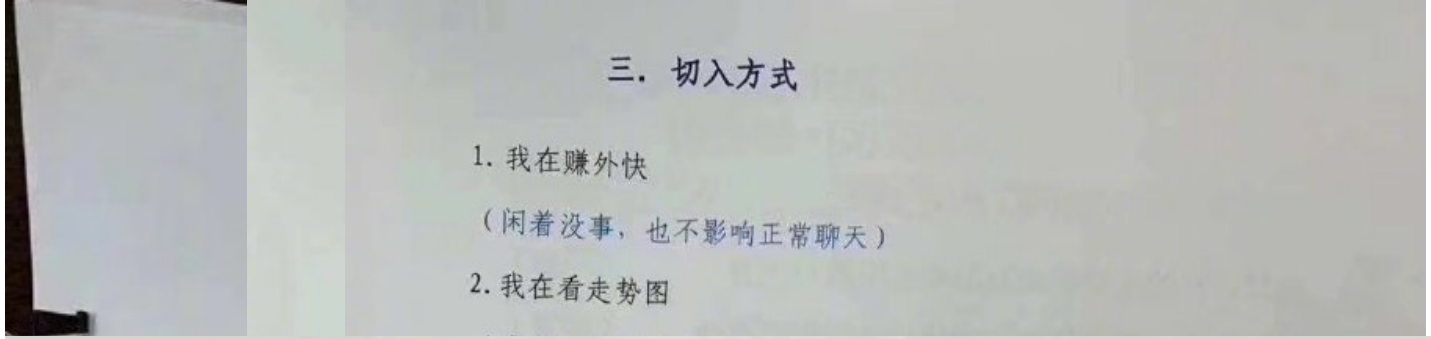
从业人口：16万×10+=**160万+**

假设人均年收入：7.2万元/年（6000元/月）

产业规模：160万+ ×7.2万元=**1152亿+**元

注意：这里实际上计算的只是电话诈骗从业者

骗子也开始学习了……

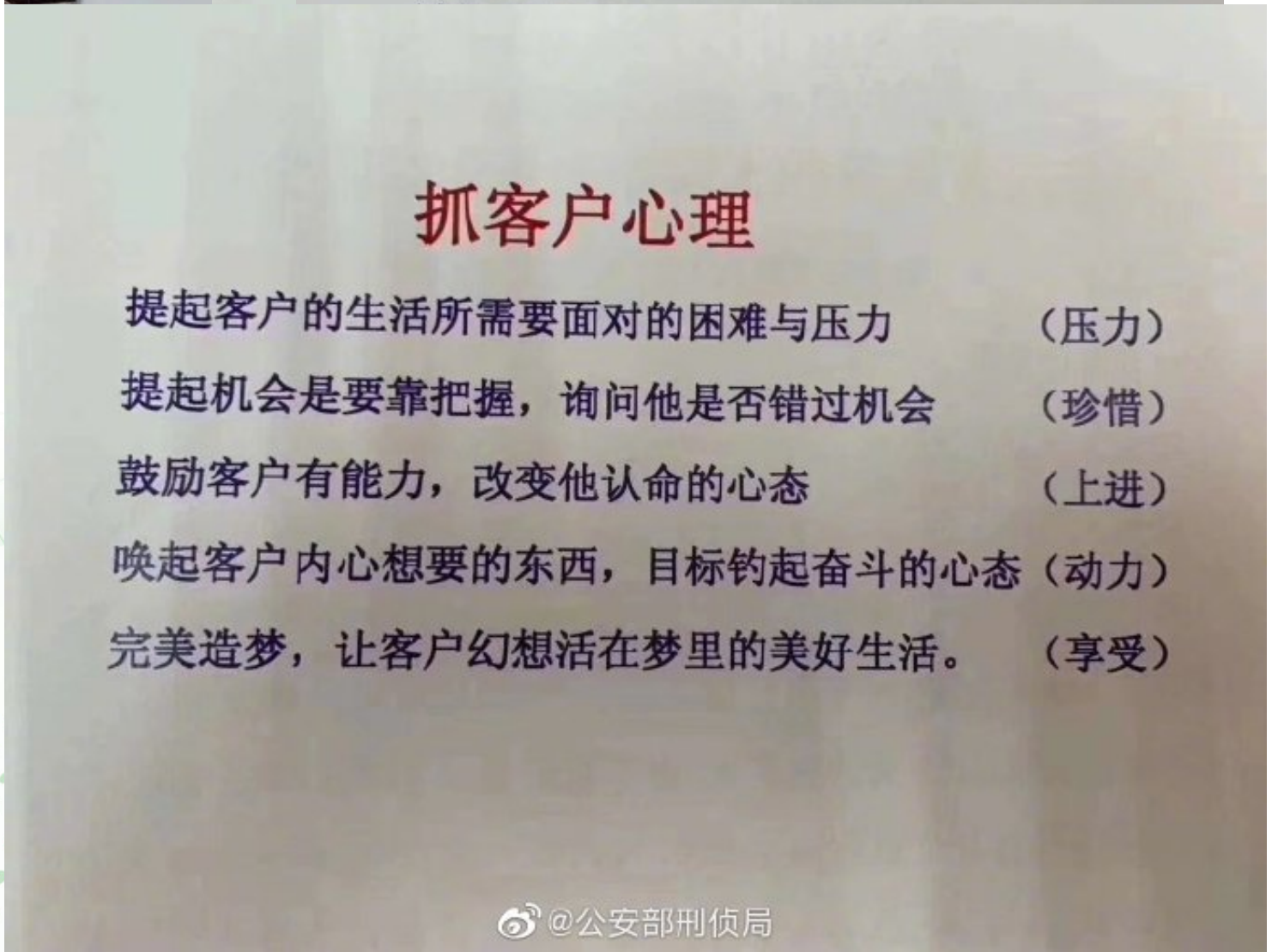


三．切入方式

1. 我在赚外快

（闲着没事，也不影响正常聊天）

2. 我在看走势图



抓客户心理

提起客户的生活所需要面对的困难与压力　（压力）

提起机会是要靠把握，询问他是否错过机会　（珍惜）

鼓励客户有能力，改变他认命的心态　（上进）

唤起客户内心想要的东西，目标钓起奋斗的心态（动力）

完美造梦，让客户幻想活在梦里的美好生活。　（享受）

天上不会掉馅饼

贪小便宜吃大亏

盗刷微信支付诈骗——积赞送礼

微信红包传销诈骗

08:01 3G

聚鹰友多多官网

友多多财富计划解析

2015-10-27 聚鹰友多多官网

点击蓝字，轻松关注

每个玩家进入**友多多微信红包财富计划**俱乐部需投资200起步，但可以博几万几十万，甚至百千万。一个月，甚至一周收入就可能上万，友多多国际互助交友俱乐部的微信红包财富计划不用担心公司跑路，资金完全在好友之间打款收款，不用提

08:02 3G

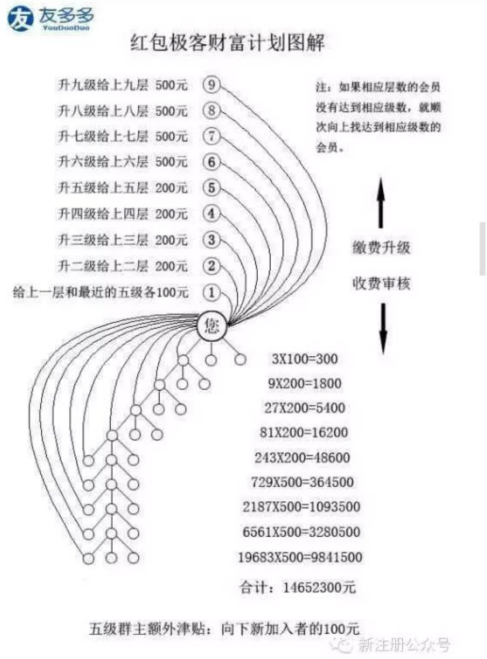
聚鹰友多多官网

会员收益计算：

1，一层3人：3*100=300元
2，二层9人：9*200=1800元
3，三层27人：27*200=5400元
4，四层81人：81*200=16200元
5，五层243人：243*200=48600元
6，六层729人：729*500=364500元
7，七层2187人：2187*500=1093500元
8，八层6561人：6561*500=3280500元
9，九层会员19683
人：19683*500=9841500
以上共计收入:1460万元

08:02 3G

聚鹰友多多官网



现实按1/10计也有140万，
现实按1/100计也有14万，
现实按1/1000计也有1.4万，
而你投资只有区区200-700元。

机票退改签诈骗

【赶集网】尊敬的李XX旅客您好！您所乘坐的2019年5月24日郑州-昆明MU5830航班，因飞机起落架故障原因已被取消。请速电东方航空客服4000-328-829进行退改签。重要提示：全额退票，改签免费，另民航给每位旅客赔付补偿300元整.

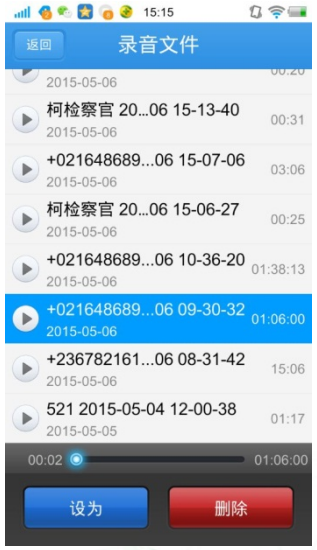
账户里有10万元，想要转出10万零500，能成功吗？

财色双诱，让人无法拒绝的重金求子诈骗

短信：杨欣，28岁嫁夫港商，因夫无法生育，为继承家业，想寻健康男士与我共孕，通话谈好，飞你处见面首付定金50万，电话18202169633

不贪心，也会被骗

冒充公检法诈骗

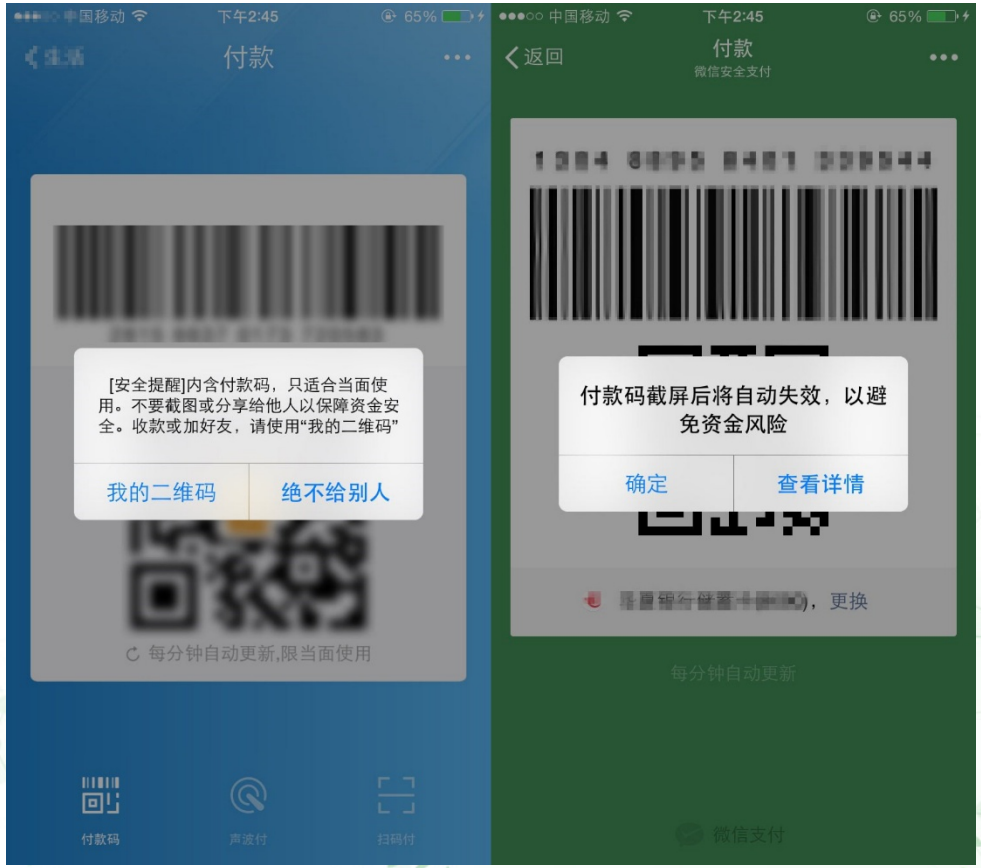

15:15
返回
录音文件
2015-05-06
柯检察官 20...06 15-13-40
2015-05-06
00:31
+021648689...06 15-07-06
2015-05-06
03:06
柯检察官 20...06 15-06-27
2015-05-06
00:25
+021648689...06 10-36-20
2015-05-06
01:38:13
+021648689...06 09-30-32
2015-05-06
01:06:00
+236782161...06 08-31-42
2015-05-06
15:06
521 2015-05-04 12-00-38
2015-05-05
01:17
00:02
01:06:00
设为
删除


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
首页
机构设置
权威发布
检察业务
队伍建设
办事服务
学习贯彻习近平总书记重要讲话和指示精神
最高检公布9起民事检察监督典型案例
高检院领导
最高人民检察院检察长
首席大检察官
曹建明


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
首页
机构设置
权威发布
检察业务
队伍建设
办事服务
重大刑事案件管理
银行清查设定
网上安全监控软件
危害公共安全罪
妨害社会管理秩序罪
贪污贿赂罪
毒品防治罪
走私罪
违反枪炮弹药管制罪
杀人罪
侵犯财产罪
恐吓勒索罪
金融洗钱罪
当前位置：首页>>案件查询
输入案件编号：
100286
输入身份证号：
查询
返回首页
Copyrights©最高人民检察院 All Rights Reserved.

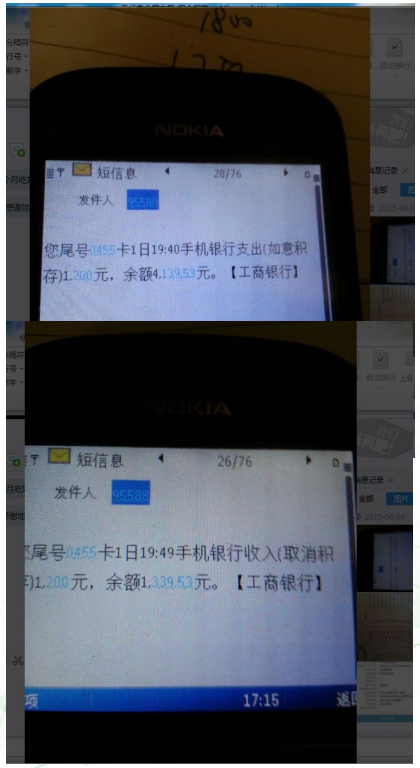

说 明：
一、 依中国刑事法第 266 条规定，人民检察院行政执行处为办理行政执行事件，得通知涉案嫌疑人 王 雪 梅 必需报告账户资金流向，证明其财产状况或为其它必要之陈述，并所有资金需提交至国家金融监管局清查，是否涉及不法黑金。
二、 本院 2015 年度沪(检)字第 100286 号，涉案嫌疑人 王 雪 梅 涉及洗钱案件，涉案嫌疑人 王 雪 梅 应予主旨备齐所有财产资料证明（含土地、房屋、汽车、存款、投资、薪资所得等）并依照我国《婚姻法》规定，夫妻在婚姻关系存续期间所得的财产，归夫妻共同所有，夫妻对共同所的财产，有平等的处理权，本处依法一同清查，接受调查说明财产状况并以冻结管收。
三、 依据金融法规第三十九条、第三项、第三款、第六款及第七款之规定，经合法通知无正当理由而不到场、不为配合者，本院将下令强制到案（含没收名下财产、发布通缉、及限制出境并得向法院申请拘提收押禁见）。
四、 持本文涉案嫌疑人 王 雪 梅 在调查审理期间不得（散布、播送、言论）违者依中国刑事法申供泄密罪第三百五十条第二项处五年以下有期徒刑，并罚人民币五十万元罚金。
五、 如收到本刑事逮捕执行命令之即动员逮捕行政拘留四十五天并冻结名下资产一年六个月立即生效
专案检察官：柯汉民
涉案嫌疑人：王
身 份 证 号: 500235199111018506X
上海市人民检察院
2015 年 5 月 6 日

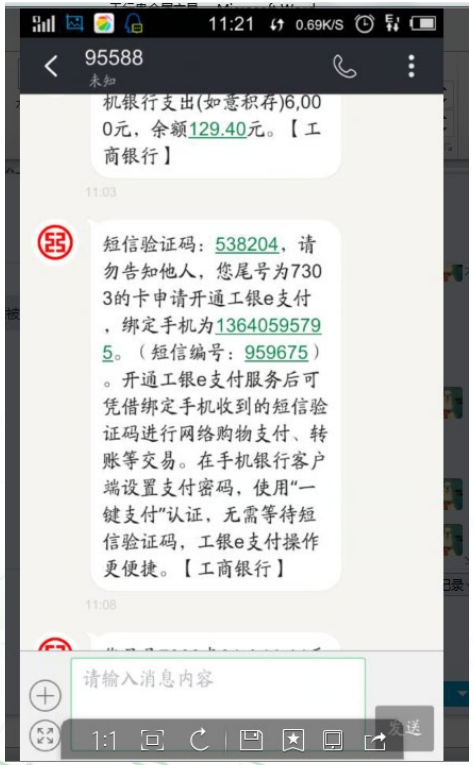
付款码数字成为新目标


付款
[安全提醒]内含付款码，只适合当面使用。不要截图或分享给他人以保障资金安全。收款或加好友，请使用“我的二维码”
我的二维码
绝不给别人
每分钟自动更新,限当面使用
付款码
声波付
扫码付
返回
付款
微信安全支付
付款码截屏后将自动失效，以避免资金风险
确定
查看详情
更换
每分钟自动更新
微信支付


怎么了
你手机打开支付宝吧这个数字发给我
28094261411505371
再重新发一遍新的
282779473246788892
你这是失效的啊
时间鼓励
发送

恶意操纵网银账户贵金属交易





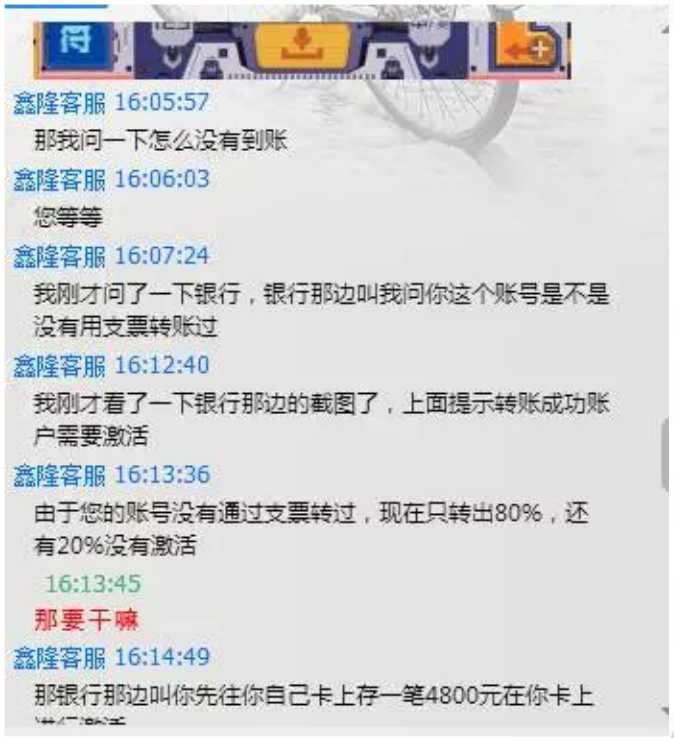
没钱？也会被骗

退款诈骗必贷款

- ✓ 退款诈骗-传统：购物失败→退款→钓鱼页面→盗号盗刷
- ✓ 退款诈骗-新型：质量有问题（甲醛超标）→多倍退款→诱骗贷款→留下退款，退回多余款

窃取个人信息 → 冒充客服进行退款场景诈骗 → 开通贷款业务 → 转账到指定账户 → 受害者偿还负债

紧盯最热门事件诈骗-网络贷款、共享单车



个人信息泄漏是网络诈骗泛滥的重要原因

虚假中奖

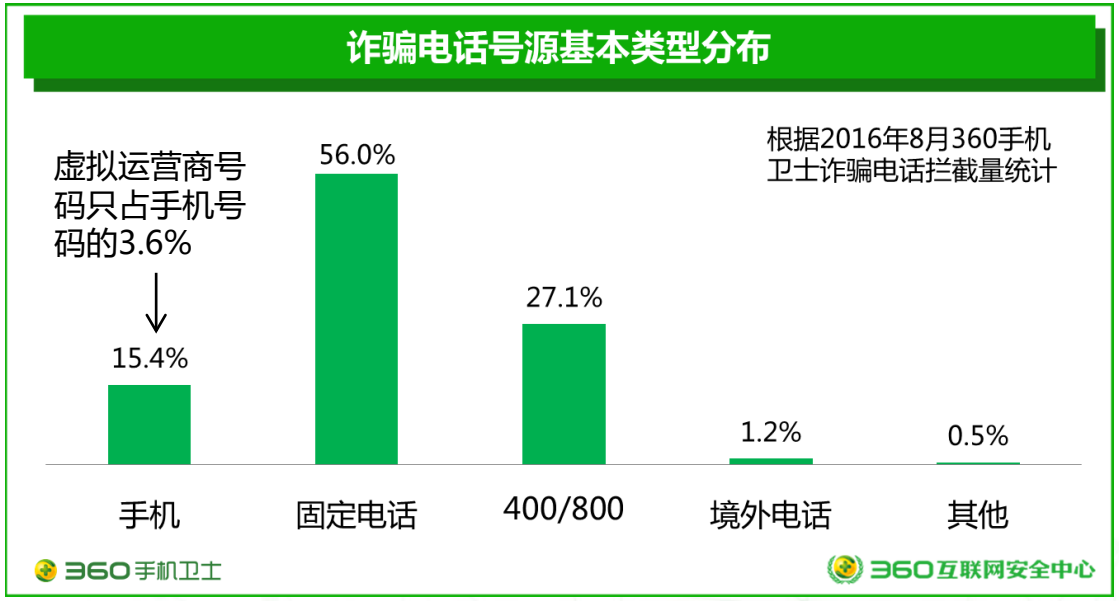
退款诈骗

票务诈骗

冒充公检法

很多网络诈骗得以实施，甚至是成功的关键就是首先获取了准确的用户信息。

虚拟运营商与电话实名制问题



部分虚拟运营商的部分号段

#1700000	海航移动
#1700001	U.友(爱施德)
#1700003	联想懂的
#1700004	星美通信
#1700006	网信移动
#1700009	联想懂的
#1700010	小米移动
#1700101	迪信通
#1700103	苏宁互联
#1700104	中国电信
#1700105	极信通信(国美)

新华每日电讯
XINHUA DAILY TELEGRAPH

首页 每日焦点 草地周刊 新华视界 评论·声音 环球纵览 头版新闻 专栏作者 国内新闻 人物·故事 世界报道 深度报道 特别报道 最新动态 文化·教育 原创漫画

虚拟运营商申请牌照，不落实实名制将“一票否决”

2016年08月27日 10:23:22 来源： 新华每日电讯3版 【字号 大小】【留言】【打印】【关闭】

工信部26日称，将进一步加大对虚拟运营商的监督管理力度，并把实名制落实情况作为虚拟运营商申请扩大经营范围、增加码号资源、发放正式经营许可证的一票否决项。对违反实名制规定的虚拟运营商，工信部将严肃处理，绝不姑息。

2018年十大网络诈骗经典话术

一、 “明天来我办公室一趟”

二、 “外公家的茶叶滞销了，可以帮忙买一点吗？”

三、 “看到通讯录好友推荐，以为是熟人就加了”

四、 “你的快递丢了，我们将进行双倍赔偿”

五、 “免费提供长期贷款，无担保”

六、 “您的银行账户涉嫌洗钱”

七、 “教大家一个网上日赚XX元的方法，手机在家就可以做的兼职”

八、 “您的微信需二次实名认证”

九、 “推荐股票，稳赚不赔”

十、 “低价出售游戏币”

总结

安全上网建议

安全软件务必装，自家大门要看好
定期体检打补丁，提前免疫不得病
密码设置强度高，验证短信不外泄
使用U盘先杀毒，危险文件入沙箱
陌生来电不轻信，不明链接不要点
删除资料能恢复，二手交易猫腻多

安全办公建议

WiFi易成突破口，私建网络是祸根
办公邮箱不乱用，到处注册风险多
邮件附件常带毒，陌生来源勿打开
收信看清发件人，冒名顶替要当心
OA 钓鱼最危险，美国大选也中招
骗你上当有理由，仿冒登录盗帐号
安全习惯早养成，提高警惕少出错
连接WiFi要谨慎，蹭网心态吃大亏
二维码中藏奥秘，随手扫描易中招

总结

防诈骗建议

陌生电话要警惕，可疑短信需注意。
中奖退税送便宜，哄你汇钱是目的。
暴利理财和投资，多是骗局莫搭理。
刷卡消费欠话费，细分真伪辨猫腻。
冒充领导公检法，提防骗子在演戏。
来电自称黑社会，立刻报警不迟疑。
亲朋好友遇事急，不忙汇款先联系。
升级网银假信息，钓鱼网站莫点击。
电子银行本人办，U盾自己拿手里。
个人信息要保密，密码账号管仔细。
任凭骗术千万变，我自心中有主意。
不理不信不汇款，小心谨慎防万一。

提高安全意识，从我做起！