



2016乌云白帽大会·不插电

That's a Secret

黑色产业全纪实



乌云 WooYun



乌云白帽大会 · 2016
不插电

路人甲 (Rank: ¥999999999999999999999999999999)

最神奇的一群人，智慧低调又内敛，俗称马甲，打酱油的，不明真相的群众等

他于 1970-01-01 注册，已来到乌云 16973 天

个人主页：<http://www.youcangoanywhere.com>



黑产到底是什么



黑产到底有什么

超过40万人

规模上千亿

月入8万刀



乌云 WooYun



乌云白帽大会·2016
不插电



黑产到底做什么

盗刷银行卡

诈骗

倒卖数据



三要素

银行卡

手机验证码



乌云 WooYun



乌云白帽大会·2016
不插电

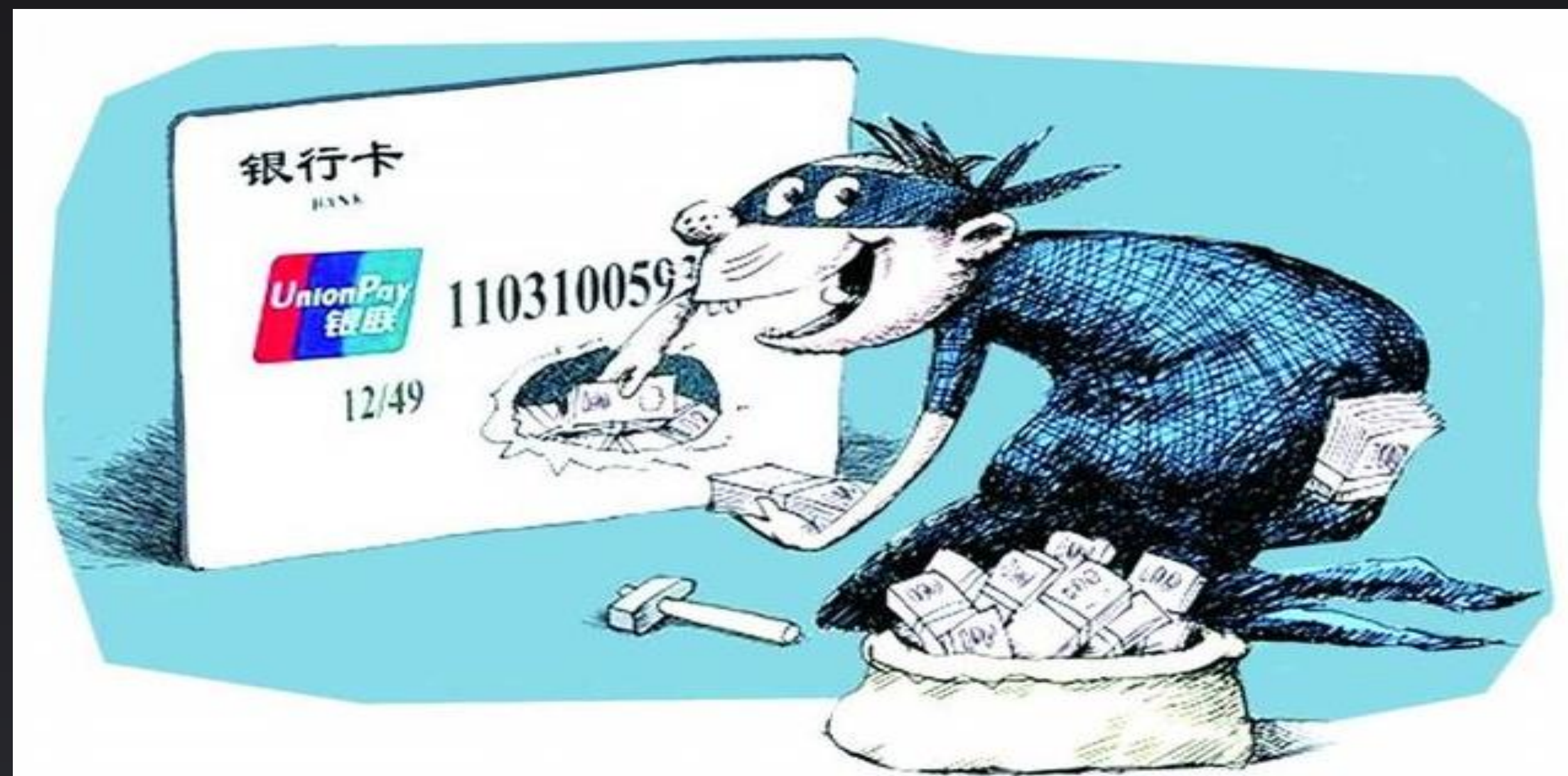
```
[√] Insert successfully!
*****
*****
短信类型：下行
手机号码：95588
中心号码：8613010112500
接收时间：2016/07/06 15:53:24
-----
短信验证码：914192，您正在查看定制的工银信使服务，请将验证码输入网页中。（短信编号：451881），请勿泄露短信验证码。【工商银行】
-----
95588
8613010112500
False
短信验证码：914192，您正在查看定制的工银信使服务，请将验证码输入网页中。（短信编号：451881），请勿泄露短信验证码。【工商银行】
2016/07/06 15:53:24
```

盗刷三要素

手机号

姓名&运气

手机验证码



盗刷就这么简单

```
手机号码：95588
中心号码：8613010112500
接收时间：2016/07/05 17:45:26
-----
您尾号6189卡7月5日17:45网上银行收入(支付宝转账)100元，余额100元。【工商银行】
-----
95588
8613010112500
False
您尾号6189卡7月5日17:45网上银行收入(支付宝转账)100元，余额100元。【工商银行】
2016/07/05 17:45:26
```

盗刷就这么简单

手机号

一点点运气

一台电脑和几部手机





盗刷就这么简单

一次真正的盗刷



盗刷就这么简单

身份认证被弱化

溯源难度大

手机验证码不可靠



“大数据”下的诈骗



乌云 WooYun



乌云白帽大会 · 2016
不插电

受信任的大型电商

陌生来电

正确的信息

订单退款



“大数据”下的诈骗



“大数据”下的诈骗

一次真正的诈骗

网易旗下考拉海购

陌生来电

知道姓名，化妆品被扣

订单退款

“大数据”下的诈骗

另一次真正的诈骗



乌云 WooYun



乌云白帽大会·2016
不插电

交出数据不可避免

无力分辨客服

我们能做什么

信息来源？

“大数据”下的诈骗



乌云 WooYun



乌云白帽大会·2016
不插电



“大数据”的源头



购物订单

快递信息

企业信息

身份信息



“大数据”的源头

灰太狼 16:31:08

录入有啥要求么~

腾彤锡馨 16:31:45

腾彤锡馨 16:38:51

是 打定速度怎么样

腾彤锡馨 18:05:21

灰太狼 16:39:2

还行吧，比一

要 数字键

腾彤锡馨 16:54

打五笔的吗

灰太狼 16:55:3

数字键？直接

不是往

腾彤锡馨 16:57

那个

灰太狼 18:0

一天时

给个结

灰太狼 18:0

无比多一点

灰太狼 17:04:0

汉字70+，数

腾彤锡馨 17:04

五笔，不过

给你个

腾彤锡馨 17:04

打用这

那你

灰太狼 18:1

录入都是唯

腾彤锡馨 18

是的

🙄

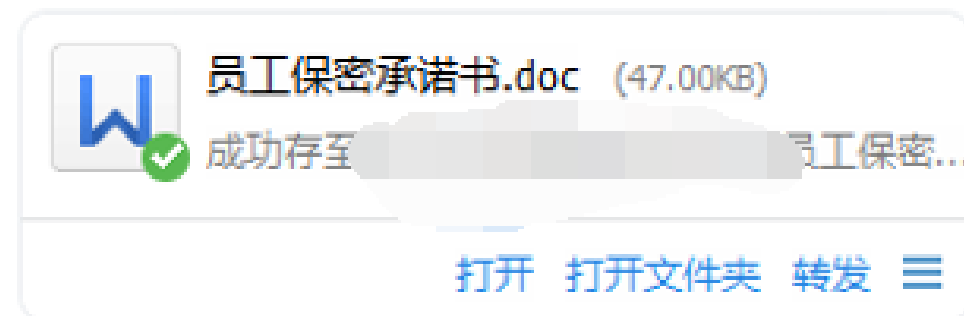
灰太狼 18:19:58

腾彤锡馨 18

邮寄到哪里~

腾彤锡馨 18:20:13

最迟



确定没有问题的话，把这个签好，寄给我

是的

打印签好字，再复印一张身份证复印件

“大数据”的源头

还是一个真正的例子



员工保密承诺书 2012 V1.0

员工保密承诺书

本人因在_____（以下简称“公司”）工作，已经或将要知悉、掌握公司的商业秘密。本人承诺对本承诺书所述商业秘密承担保密义务。

一、保密范围：

本承诺书所指商业秘密包括但不限于以下内容：

- 1、技术信息，其范围包括技术方案、信息系统设计方案、操作流程、制造方法、技术指标、技术文档、计算机软件、数据库、图纸、样品、样机、模具、操作手册、涉及商业秘密的业务函电等等；
- 2、经营信息，其范围主要包括客户资料、营销计划、市场拓展筹备计划、合同内容、投标中的标底与标书内容、采购资料、定价策略、进货渠道、产品策略、财务报表及财会档案、工资福利分配方案、人力资源信息等等；
- 3、属于公司外第三人的商业秘密但依照法律规定或者有关合同的约定，公司承诺对外承担保密义务的事项；
- 4、公司未予公开的其他商业信息。

二、保密承诺：

“大数据”的源头

所谓保密协议



乌云 WooYun



乌云白帽大会·2016
不插电

“大数据”的源头

这不是个例

【宗师】招输单员(3339056972) 22:01:33

招顺丰录单熟手一名，要求：1，熟手！质量好，熟悉各种碎片的录入规则以及各种增值服务的录入，速度过得去，2，晚上能跟单结束(结束时间1点左右)，。单量有保障，票值高，有意私聊，不符合条件的勿扰

【掌门】招收输单员，不接受酱油(2168243379) 22:14:32

合用工号兼职打附加，自由的很

别涉及到手机月结这些东西

没有身份验证

内部数据外放

完全没有约束

企业管理与责任

“大数据”的源头

THANKS



乌云 WooYun



乌云白帽大会 · 2016
不插电

