



# 个人简介



电子数据取证与鉴定

全国电子物证分技术委员会专家工作组成员

中国电子学会计算机取证专家委员会委员

公安部/司法部 能力验证专家

国家认可委 实验室 / 能力验证认可评审员

上海市司法鉴定协会电子证据司法鉴定专业委员会委员

上海辰星电子数据司法鉴定中心 技术主管

中国政法大学电子证据研究中心特聘研究员

“宋慈” / “鼎永杯” 优秀司法鉴定文书获奖者

多个公共安全行业标准和司法鉴定技术规范起草者



# 诈骗屡屡发生的背景：电子商务迅速发展

## 2015年中国电子商务交易总额达18万亿元

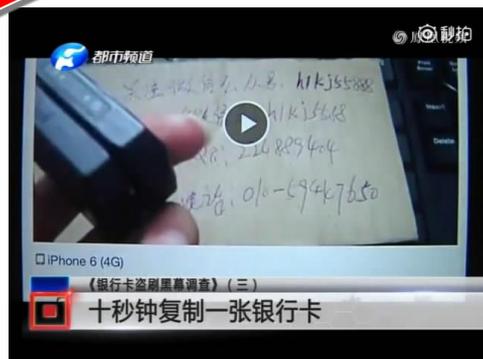


# 银行卡犯罪的现状:盗刷现象愈演愈烈



# 银行卡

# 盗刷愈演愈烈!



# 盗取银行卡信息的方法

## 钓鱼/病毒短信



通过伪基站发送带有网址链接的短信，大多是冒充运营商、各大银行等号码，以“积分兑换”“银行卡激活”等理由让你点击短信中的链接，一旦点击就会进入一个和正规网站外观几乎完全一样的钓鱼网站，并诱导你在上面填写银行卡账号、密码、持卡人姓名、手机号、识别码等信息。

## 病毒二维码



在公共场所张贴内置病毒的二维码，并使用“扫一扫就可打折促销、会议签到、下载软件”等词语诱导用户扫描，一旦扫描即自动下载木马病毒，手机上银行卡及相应软件账户密码等信息就会被窃取。

## 钓鱼WIFI



在公共场所架设免费WIFI，待有人连接此WIFI上网后，所有互联网的数据都可以被黑客监听或窃取。这个在2016年的3.15晚会上已经现场做过实验。

## 改装POS机



利用改装的POS机或银行卡测录器提取用户银行卡信息。即通过对POS机进行改装，加装破译芯片、电子按键软膜、手机通信发射器、内存卡等，实现用户刷卡时银行卡各类信息自动发送到洗料人处。

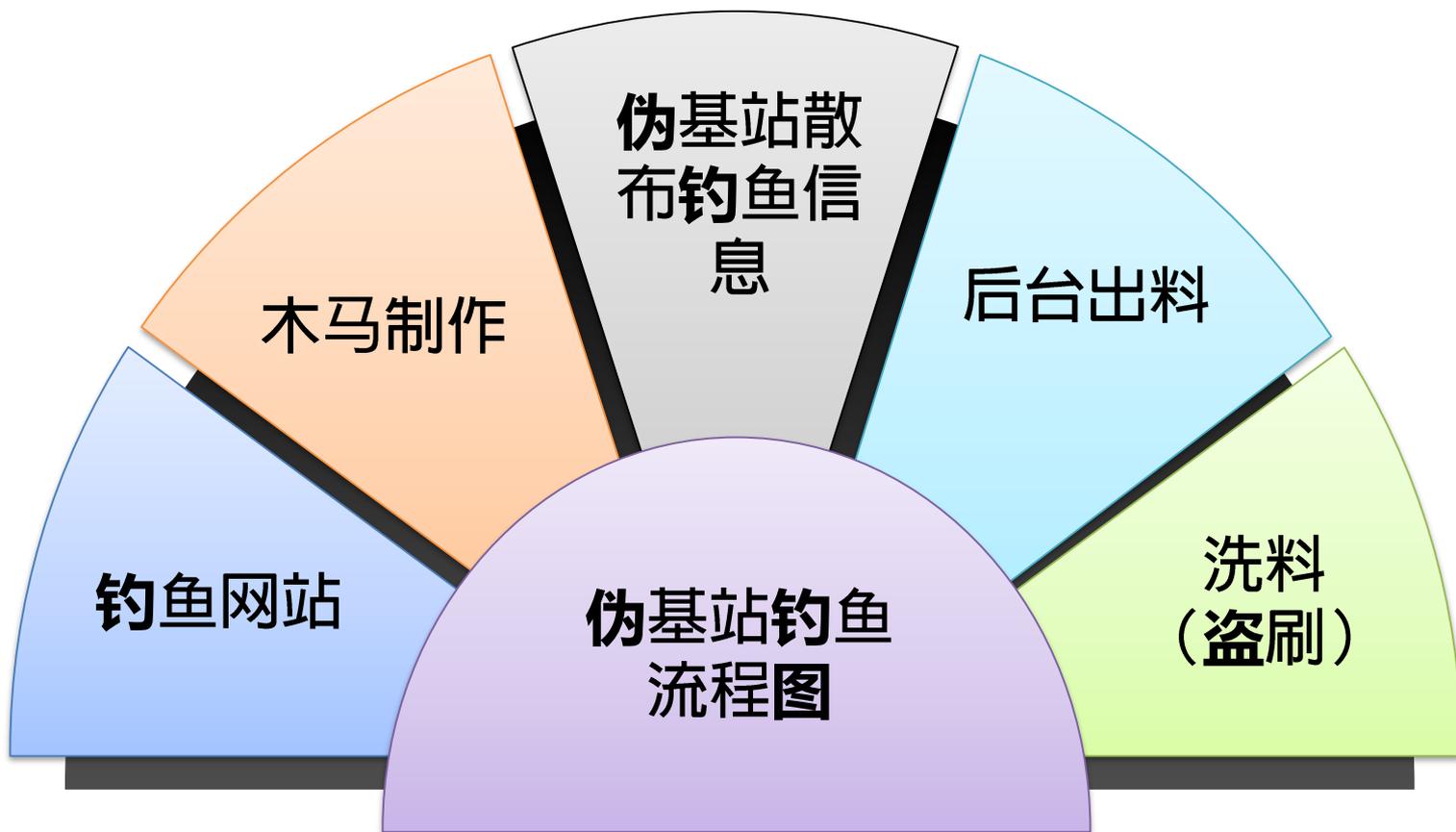
# 诈骗犯罪的产业链



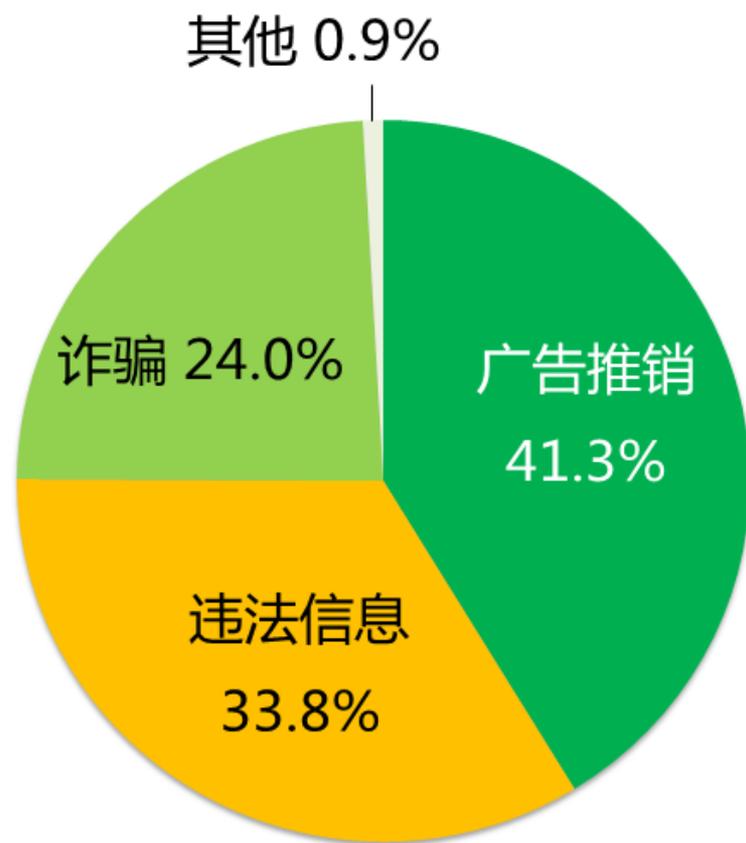
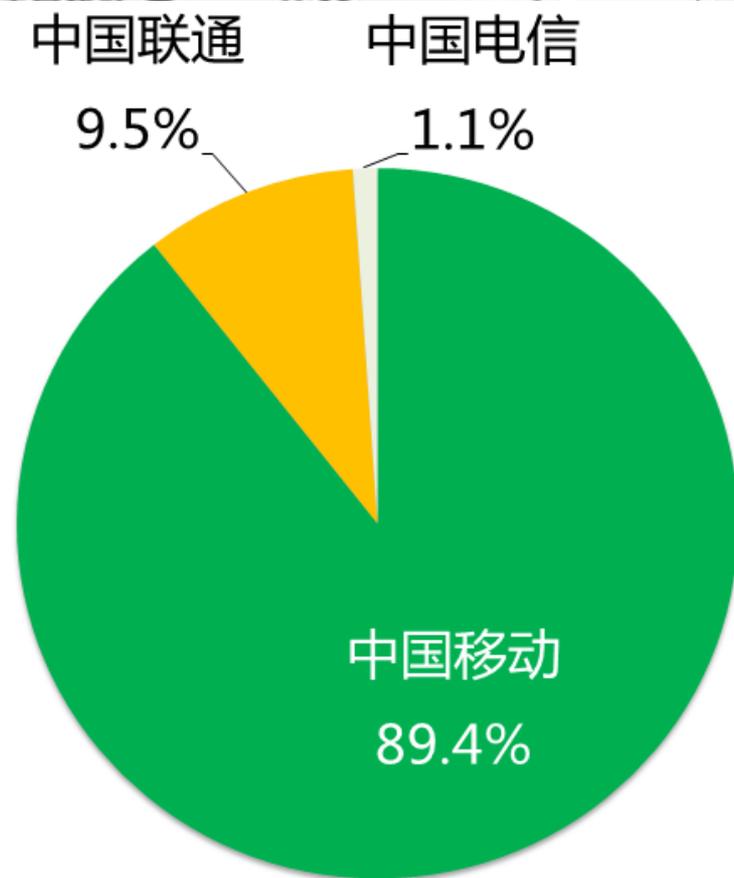
从业者：**160万+**



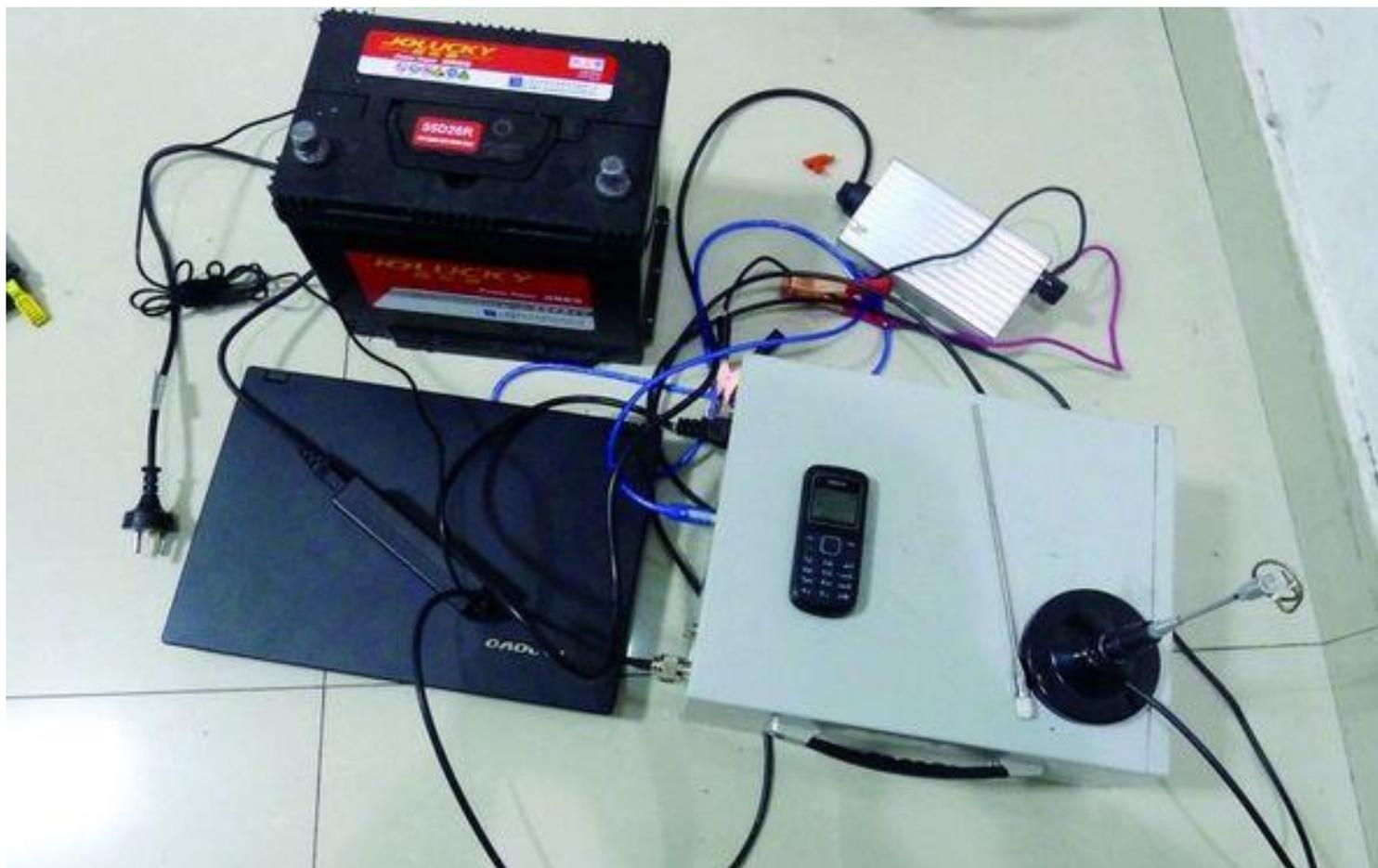
年产值：**1100亿+**



# 各种诈骗短信防不胜防

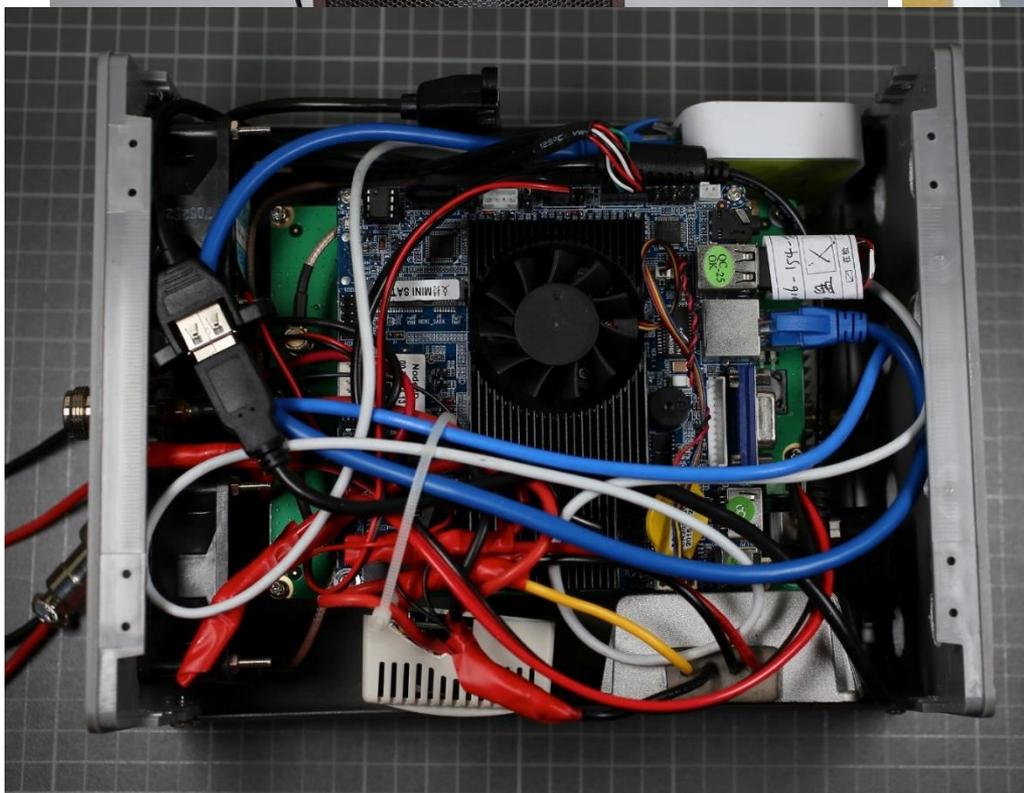


# “伪基站”的构成和工作原理



- ✓ “伪基站”是伪装成公共移动通信运营商基站
- ✓ 由主机或笔记本电脑 + 发射器(含天线) + 测频手机组成
- ✓ 通常采用OpenBTS + Gnuradio + USRP

# 技术不断更新的“伪基站”设备



# “伪基站”设备的检验鉴定

## 传统伪基站

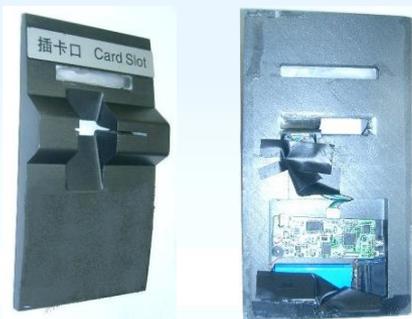
- ✓ 检材确认登记及拍照（通常是**笔记本硬盘**，系统为Ubuntu）
- ✓ 检材硬盘校验值计算
- ✓ 硬盘检验
  - 复制检材硬盘，装回检材启动检验
  - 使用仿真软件和只读接口直接进行系统仿真检验
- ✓ 系统时间检验
- ✓ 控制软件检验
- ✓ MySQL数据库检验
- ✓ IMSI记录检验
- ✓ 发送短信内容检验
- ✓ 计算所有导出文件的校验码
- ✓ 形成报告

## 新型伪基站

- ✓ 现场开机状态伪基站
  - 现场开机状态手机拍照固定
  - 开机状态拆机检验
  - 开机状态远程连接检验
- ✓ 关机状态伪基站
  - 检材确认登记及拍照（通常是**U盘**，系统为Ubuntu）
  - 检材U盘校验值计算
  - 检材U盘检验（同传统伪基站）
  - 控制软件检验
  - MySQL数据库检验
  - 计算所有导出文件的校验码
  - 形成报告

# 常见的盗卡方式及作案工具

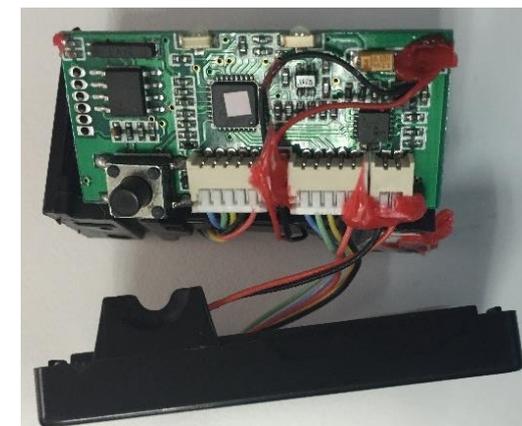
## ATM测录



## POS机测录



## POS机 操作员测录



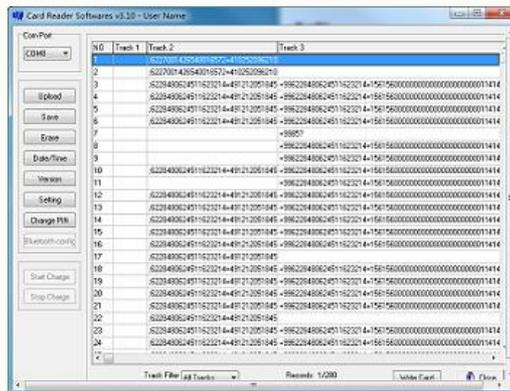
# 测录器设备的检验鉴定

## 直接读取

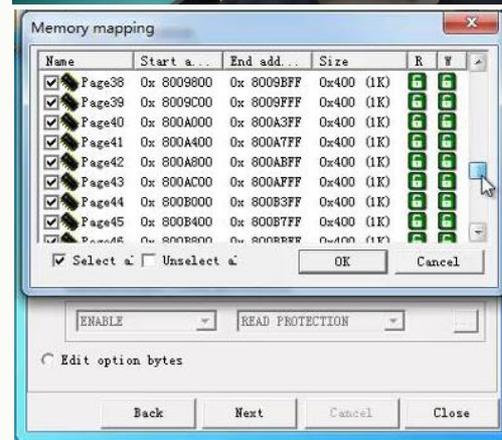


```
~H□ 9/02/23 22:15:26%996222
02100102182 =1561560000000000
000003095999216000491200000000
000000000000=00000000000=000000
00?;6222021001021822413=49121200
959991557?+Blank? □□□□□□□□□□
□□□□□□□□□□□□□□? K□ □ □ □
□ □ ~H□ 9/02/23 22:15:3
0%9962220210010218 =15615600
0000000000000309599921600049120
000000000000000000=00000000000
0=00000000?;Error?+Blank? 22413=
49121200959991557?+Blank? □□□□□
```

## 专用程序读取



## Chip-off读取



# 个人信息保护的注意事项

## 妥善处置快递单等单据

对于已经废弃的包含个人资料，**一定要妥善处理好**。不经意扔掉，可能会落入不法分子手中，导致个人信息泄露

## 身份证复印件上要写明用途

在提供身份证复印件时，要在含有身份信息区域注明“**本复印件仅供XX用于XX用途，他用无效**”和日期。复印完成后要**清除复印机缓存**。

## 不要轻信任何中奖信息

不要轻易点击**中奖网站链接**；不要在通过点击电子邮件链接访问的网站上输入相关登录账号、密码等信息，也不要**在未知的网站上**提交个人重要信息。

## 不在网上透露个人信息

在微博、QQ空间、贴吧、论坛等社交网络要**尽可能避免透露**或标注真实身份信息。

## 慎重参加网上调查活动

参与此类活动前，要选择**信誉可靠的网站**认真核验对方的真实情况，不要贸然填写，导致个人信息泄露。

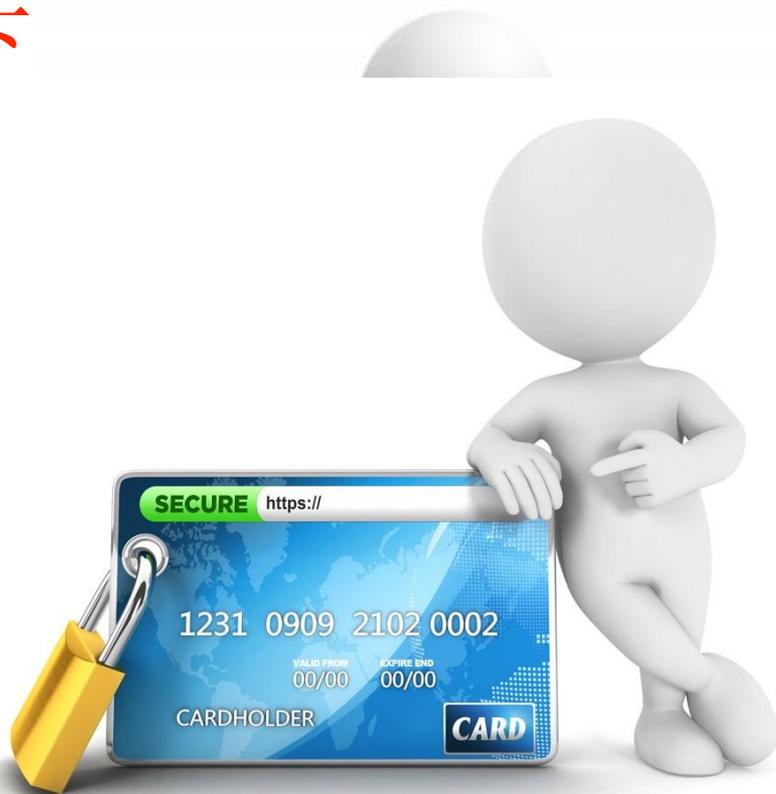
## 谨防钓鱼网站

当接收到包含网站链接的短信时，需仔细甄别网站的域名，钓鱼网站常常伪装成和真实网站相近的域名，如攻击者会使用如**1oo86.cn**等与**10086.cn**真实网站接近的域名。

# 银行卡使用的注意事项

## • 芯片卡 芯片卡 芯片卡

- **申请交易短信提醒** 在2000年就颁布了银行IC卡的国际标准，即EMV标准。
- **刷卡消费全程监督** 美国在2015年10月1日开始禁止使用磁条卡，转而使用更加安全的EMV芯片卡
- **注意保护密码** 英国在2006年就完全采用了EMV，伪卡欺诈行为大幅下跌，
- 中国也在积极广泛地组织实施“换芯计划”。按照国务院关于银行卡产业升级的五年规划和央行的要求，到2015年1月1日金融IC卡将全面取代磁条卡。



# 无线热点使用的注意事项

01

尽量不使用可疑或未加密的WiFi网络

使用虚拟专用网络 (VPN)

02

03

尽量使用HTTPS协议登录网站

关闭WiFi默认连接

04

# 万一被盗刷怎么办？



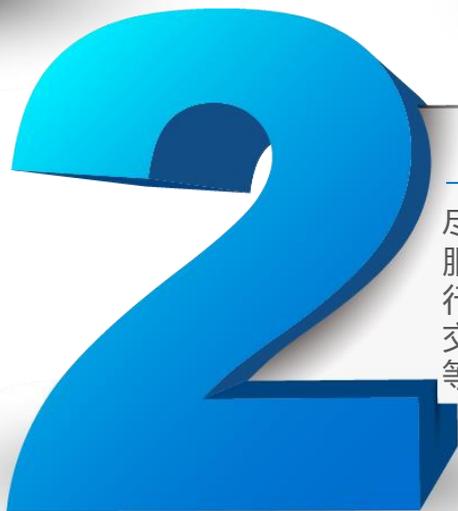
## 冻结卡片

立即致电发卡行客服电话,核实是否发生了账户异常变动的情形,确认发生后立即办理临时挂失。



## 立即报案

尽快到当地派出所报案,向办案人员出示银行卡原卡,取得报案回执或受案通知书等文件。



## 留取证据

尽快到最近的发卡行服务网点ATM机或银行营业场所办理用卡交易,如查询、取款等,证明人卡未分离。

谢谢观看



郭弘



guohong@stars.org.cn



18616359092



guohong197854

