



ISC 互联网安全大会



360 互联网安全中心

智能终端大数据、NLP与个人黑产防范

张亚枫 魅族·通讯安全负责人

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
(原中国互联网安全大会)



IT大咖说
知识共享平台



ISC 互联网安全大会



360 互联网安全中心

目录

智能终端大数据、NLP与个人黑产 防范

通讯安全现状

黑产在哪里？

魅族通讯安全



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION



ISC 互联网安全大会



360 互联网安全中心

通讯安全识别现状

通话安全

短信安全



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

通讯安全现状



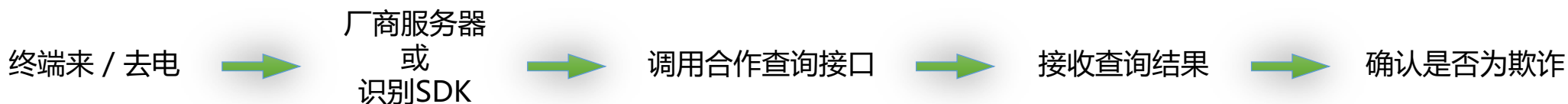
ISC 互联网安全大会



360 互联网安全中心

通话安全

目前普遍使用的「单一号码查询结果」



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

通讯安全现状



ISC 互联网安全大会



360 互联网安全中心

短信安全

目前普遍使用的「号码与关键词识别」

终端接收短信 → 查询识别SDK → 提取号码、关键词 → 查询云端结果 → 判断是否为欺诈



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION



ISC 互联网安全大会



360 互联网安全中心

黑产在哪里？



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

黑产在哪里？



ISC 互联网安全大会



360 互联网安全中心

新闻里的黑产

一个鲜活的生命



* 2016年山东考生，因9900元学费被全部骗走，报案回家路上心脏骤停，后抢救无效，当晚去世



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
TECHNOLOGY
IDENTITY SECURITY

IDENTITY
AUTHENTICATION

ISC 互联网安全大会 中国·北京

Internet Security Conference 2018 Beijing · China

黑产在哪里？



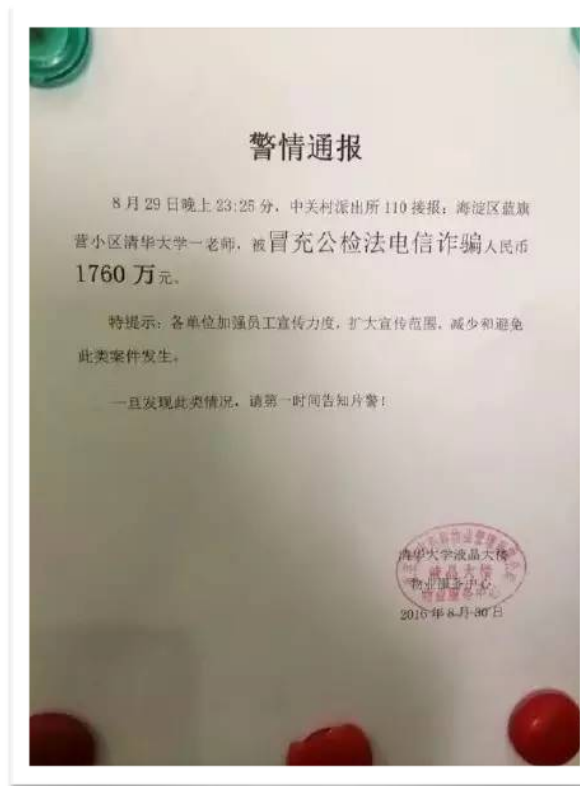
ISC 互联网安全大会



360 互联网安全中心

新闻里的黑产

一所价值连城的房子



* 2016年清华教授被冒充公检法人员骗走1760万房款



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

黑产在哪里？



ISC 互联网安全大会



360 互联网安全中心

新闻里的黑产

极具规模的黑产集团

“

该团伙在实施犯罪时，先由一线“话务员”以**赠送**迷信挂件为诱饵，将获取的客户信息转交给二线“话务员”；

二线“话务员”主动进行**电话联系**，假冒“风水大师”，以卖开光摆件和挂件的方式进行诈骗活动；

接下来再由同组“话务员”**假冒**“风水大师”的师傅或修行更深的高僧，以“消灾解难”为由让客户向寺庙**指定账号**捐款，继续实施诈骗活动。



* 2018-05-29，黑龙江破获5.6特大系列电信诈骗案 涉案金额7000余万



360 技术

IT大咖说

知识共享平台

CURITY

ISC 互联网安全大会 中国·北京

Internet Security Conference 2018 Beijing · China



ISC 互联网安全大会



360 互联网安全中心

知道自己手机有标记功能的举个手



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION



ISC 互联网安全大会



360 互联网安全中心

接到过标记电话的举个手



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION



ISC 互联网安全大会



360 互联网安全中心

标记过电话的举个手



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION



ISC 互联网安全大会



360 互联网安全中心

魅族通讯安全

风险场景识别 1.0

风险场景识别 2.0



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

风险场景识别 1.0



ISC 互联网安全大会



360 互联网安全中心

通话安全

通话结果增加场景判断

终端来/去电 → 厂商服务器 → 调用合作查询接口 → 接收查询结果 → 数据模型判断



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

风险场景识别 1.0



ISC 互联网安全大会



360 互联网安全中心

通话安全

数据模型判断

呼叫状态是呼入还是呼出

过往是否有通话记录

来电归属地与所在地是否一致

疑似诈骗

185****506

4

广东珠海移动



静音



消息

接听时长是多少

号码是否有标记，结果、类型是什么

是否为联系人

响铃时间多长



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

风险场景识别 1.0



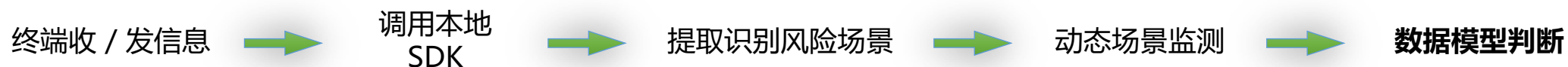
ISC 互联网安全大会



360 互联网安全中心

短信安全

对发送回复内容增加场景判断



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

风险场景识别 数据模型判断

特征识别

局部识别、匹配识别

- 关键词匹配
- 简单规则匹配

产出：

命名实体

如：手机号，银行，地址，确认信息
等...

模式识别

整体识别、匹配识别

结合NLP和大数据归集算法，
产出短信内容的识别模式可选
集合，经过人工鉴定和编辑整
理，并编译成本机识别代码

产出：

模式识别脚本

脚本识别算法包

预测识别

整体识别、预测识别

长时间、大容量的模式识别数
据积累，结合机器学习算法对
模式识别数据进行深度学习

产出：

预测识别数据

预测识别数据模型

风险场景识别 1.0



通话安全

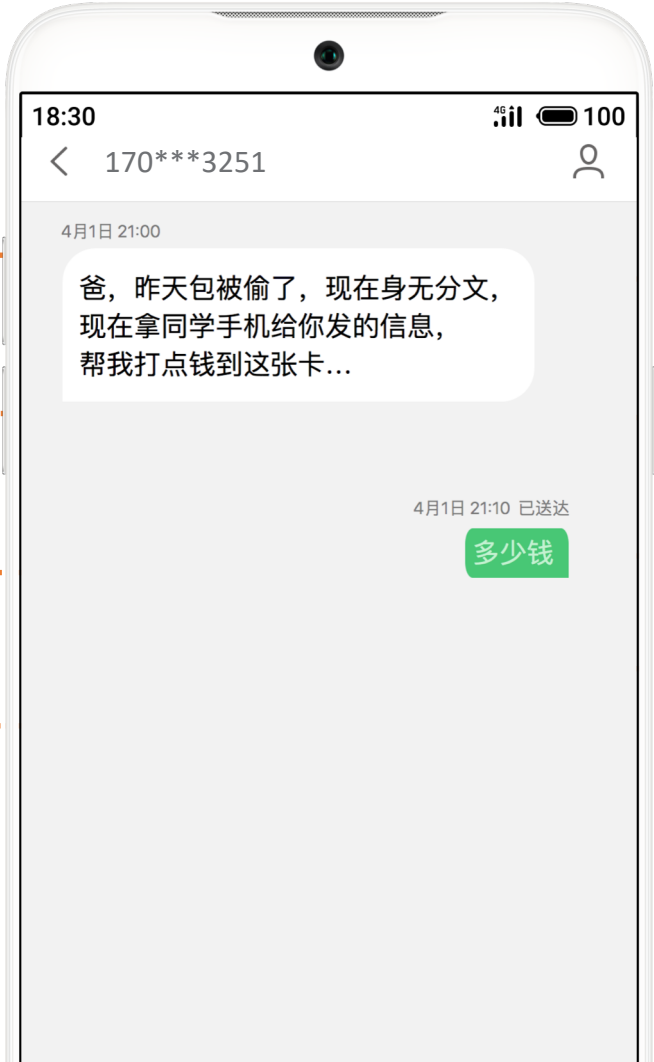
数据模型判断

发信号码是否具有风险

过往是否有联络记录

内容是否包含号码、网址

来信归属地与所在地是否一致



是否有涉及到金融类模型

接收到阅读，用时多久

是否回复

回复内容是什么，是否涉及风险模型



实验结果



ISC 互联网安全大会



360 互联网安全中心

魅族家庭守护数据

欺诈场景识别数据



29万 用户、**6万** 个家庭



15万 次通话场景识别



47万 次短信场景识别



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TECHNOLOGY
TERMINAL AGE
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION



ISC 互联网安全大会



360 互联网安全中心

为什么要做场景识别？



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

场景识别 2.0



ISC 互联网安全大会



360 互联网安全中心

风险场景识别 2.0 对通话结果增加场景判断

陌生来电



收到短信



地理位置变化



金融 App
转账通知



综合分析后
输出风险等级提示



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION



ISC 互联网安全大会



360 互联网安全中心

实际案例



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

实际案例



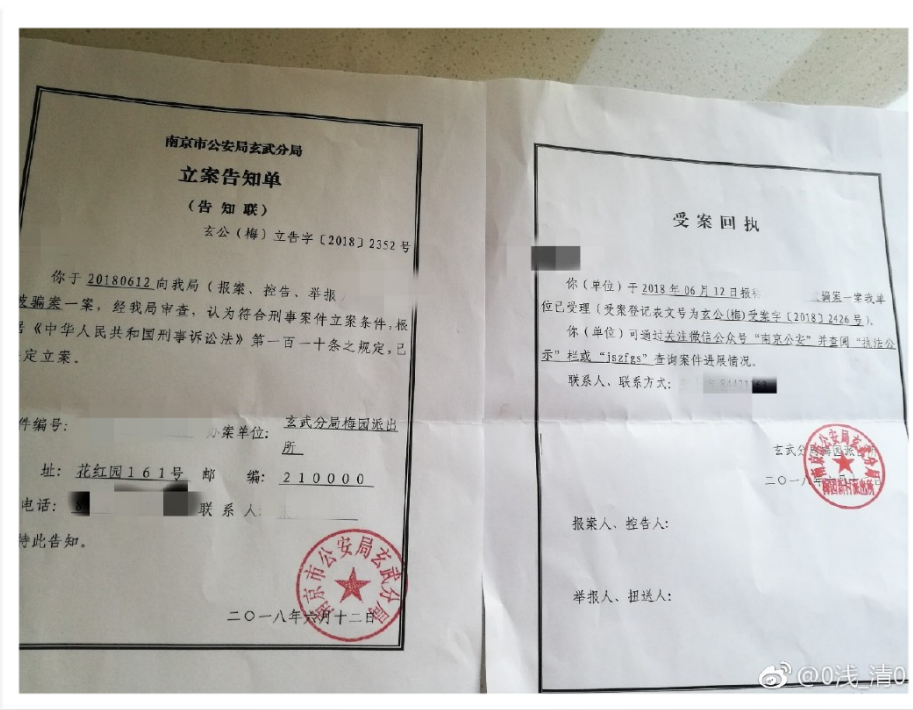
ISC 互联网安全大会



360 互联网安全中心

女大学生家人遭电信诈骗近4万：曾想学徐玉玉自杀

—— 红星新闻 2018年6月18日



* 女大学生小舒@0浅_清0 发微博求助称，父亲遭遇了短信诈骗，骗子冒充自己说要报哈佛教授的课程，急需38500元学费，结果家人把钱汇过去之后才发现被骗。



360 技术

IT大咖说

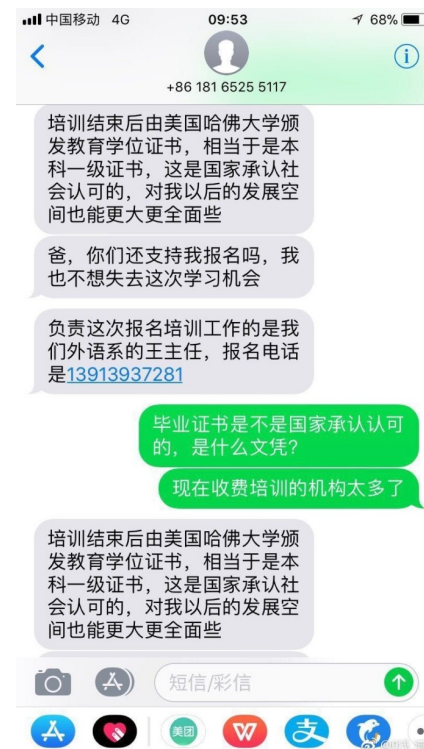
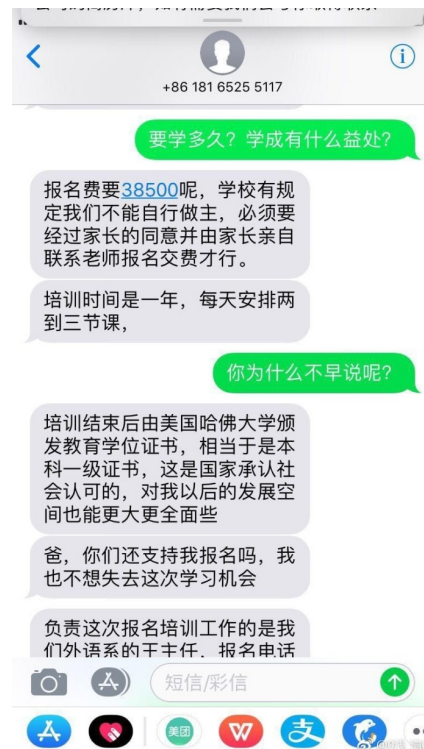
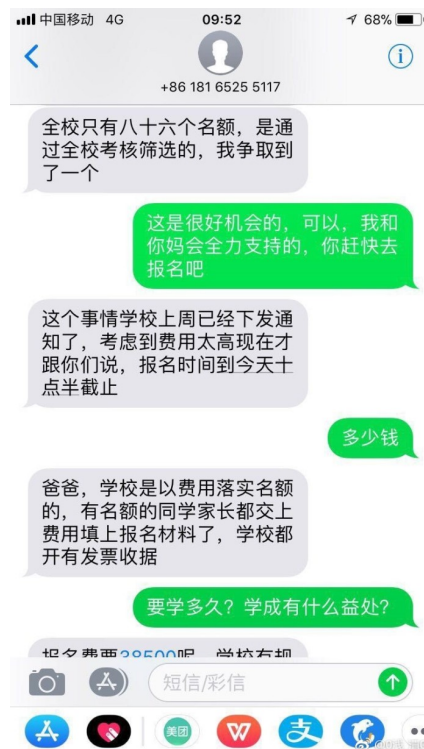
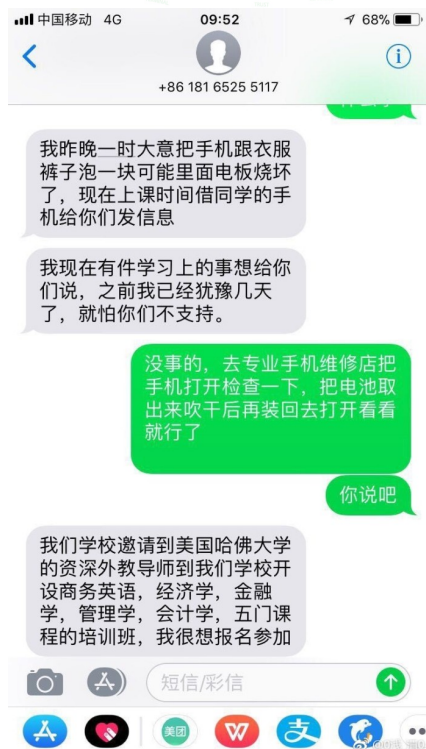
知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

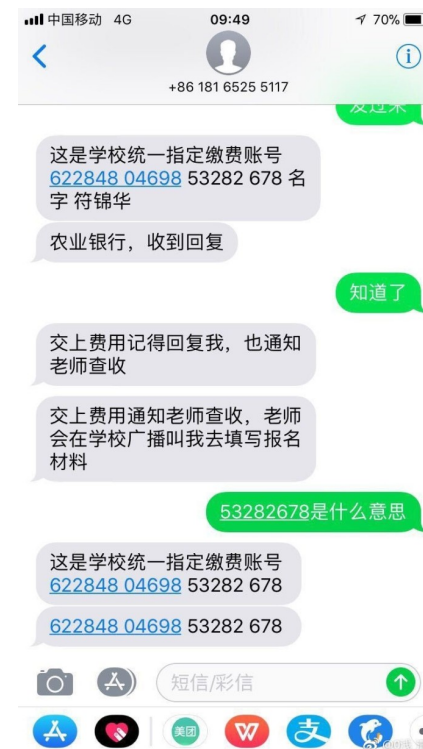
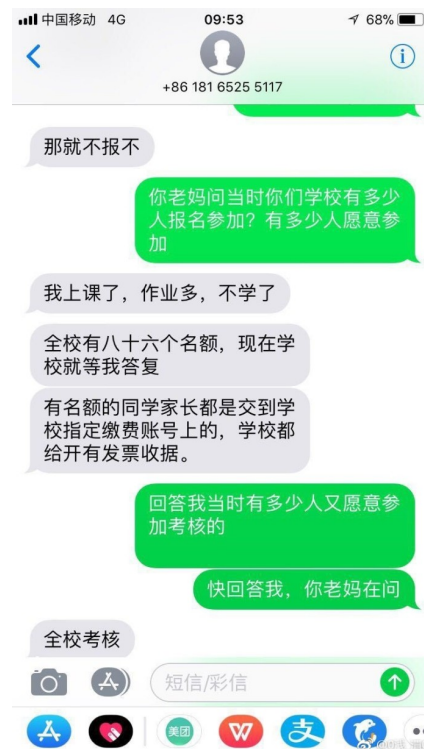
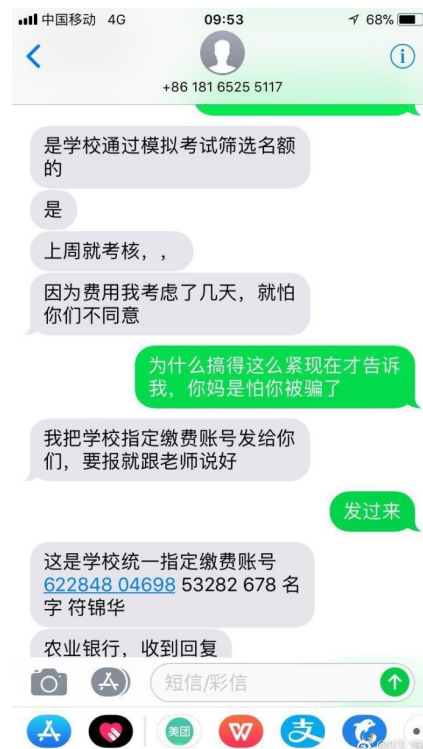
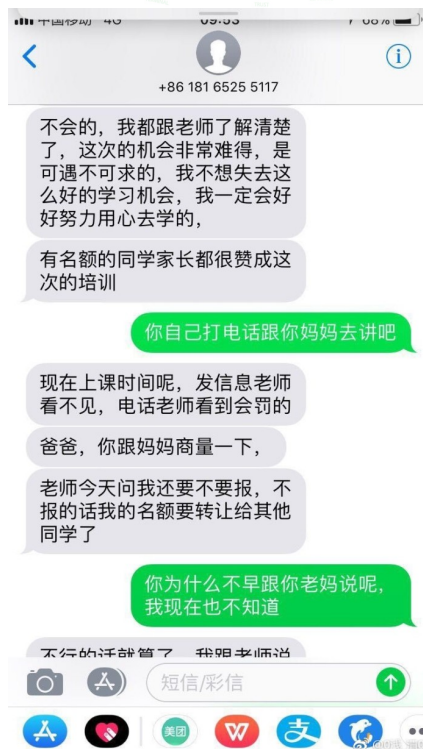
女大学生家人遭电信诈骗近4万：曾想学徐玉玉自杀

—— 红星新闻 2018年6月18日



女大学生家人遭电信诈骗近4万：曾想学徐玉玉自杀

—— 红星新闻 2018年6月18日



实际案例



ISC 互联网安全大会



360 互联网安全中心

女大学生家人遭电信诈骗近4万：曾想学徐玉玉自杀

—— 红星新闻 2018年6月18日

骗术逻辑拆解

骗子冒充受害者，发信息给受害者父母称，自己手机坏了



谎称，“学校邀请到哈佛大学资深教授到我校培训授课”



很急迫，“全校只有86个名额”
“在上课不方便接电话”



索要学费数万元，还发来“学校主任”电话和“缴费账号”



强调“**报名十点半截止**”、“学校开有**发票收据**”



360 技术

IT大咖说

知识共享平台

CURITY

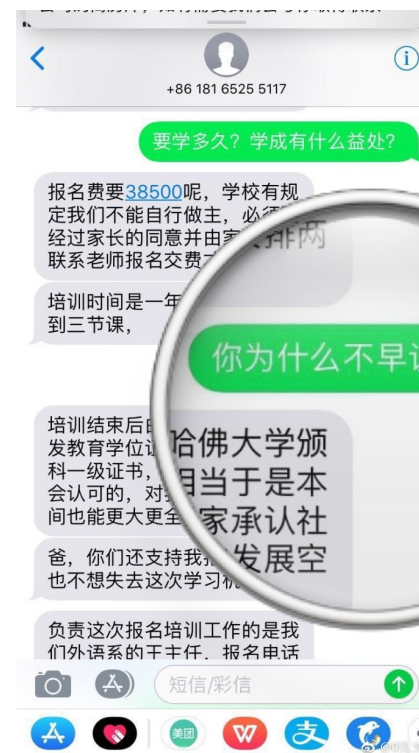
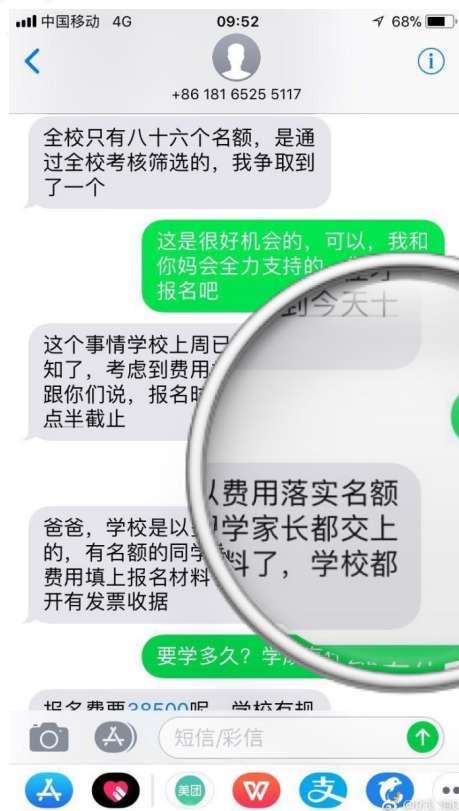
WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL AUTOMATION

实际案例

女大学生家人遭电信诈骗近4万：曾想学徐玉玉自杀

—— 红星新闻 2018年6月18日

受骗场景识别





ISC 互联网安全大会



360互联网安全中心

谢谢！

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
(原中国互联网安全大会)



IT大咖说
知识共享平台