企业安全短板和社工威胁演示

徐鹤军
中国信息安全技能竞赛 组委会秘书长

2015年电信诈骗损失222亿RMB

- 2016年一季度

  收到诈骗短信人数 6.4亿

  诈骗电话播出次数10.1亿次

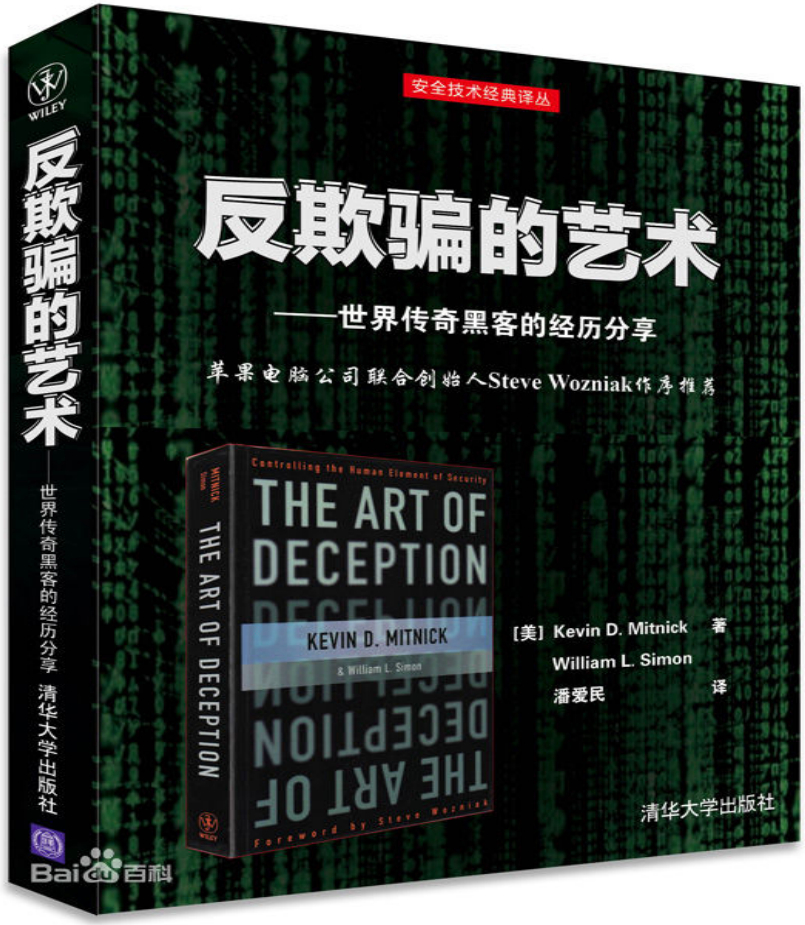
  损失金额 35.7亿人民币

  信息来自：2016年4月1日 腾讯

  《反电信网络诈骗大数据季度报告》

凯文·米特尼克

第一个被美国联邦调查局通缉的黑客



Social Engineering

- 社会工程 攻击排名十大黑客攻击方式之首

- 定义：　　社会/社交工程学是一种利用人的弱点如人的本能反应、好奇心、信任、贪便宜等弱点进行诸如欺骗、伤害等危害手段，获取自身利益的手法。

下面两个小测试

- 请在3秒钟内
- 凭你的直觉
- 选择答案A或者答案B

小测试（请按第一直觉答题）

A）参加“教你如何挣到10万RMB的讲座”

B）参加“教你如何节省10万RMB的讲座”

请选答案B的举手

小测试（请按第一直觉答题）

A）参加“消防培训”

B）参加“理财培训”

请选答案B的举手

如何解读测试的反馈？

- 人更愿意看到想看的

针对企业领导的邮件钓鱼步骤

1）基于目标社交画像

2）能够引起收件方

兴趣的内容

（ 把握时鲜 ）

3）选择合适时机

惊动百度Robin的电邮的过程

1）得知对方关注低功耗服务器
2）直接电邮附件公司产品资料
3）惊动百度Robin
4）Robin 询问 CTO
5）CTO询问 系统部朱总监
6）朱总监安排系统部魏老师确认
7）半夜接到魏老师的咨询电话

如果那封电邮有0day ……

应对之策

- 加强企业员工安全意识培训
- 增加安全意识培训的体验性
- 对违反安全制度员工的处罚

黑客行微博