
网络与信息安全意识培训

目　录

Contents

01 引言篇

安全事件、安全视频

袋鼠逃跑了……

袋鼠跑出笼子，饲养员不断加高围墙，加到100米的时候，长颈鹿问袋鼠“你明天还出吗？”“应该会出去，如果他们依然忘记关门的话。”袋鼠回答。

这个故事就很好的诠释了意识的重要性，如果意识不到门没关，一味的加高围墙，只能是本末倒置。

你是否遇到过类似问题？

一．经常被营销电话骚扰

二．快单直接丢弃

三．街头调研经常会留下真实的姓名和电话

四．经常收到中奖的消息

1、微盟删库事件

微盟研发中心运维部核心运维人员贺某，贺某于2020年 2 月 23 日晚 18 点 56 分通过个人 VPN 登入公司内网跳板机，对微盟线上生产环境进行了恶意的破坏（删除生产数据库），目前已被拘留。当天微盟市值蒸发9亿元，筹集1.5亿元赔付商家。

2、中国电信超2亿条用户信息被卖

2020年1月3日上午消息，日前，中国裁判文书网公布了《陈德武、陈亚华、姜福乾等侵犯公民个人信息罪二审刑事裁定书》。

经法院二审审理查明：2013年至2016年9月27日，被告人陈亚华从号百信息服务有限公司（为中国电信股份有限公司的全资子公司）数据库获取区分不同行业、地区的手机号码信息提供给陈德武，被告人陈德武以人民币0.01元/条至0.2元/条不等的价格在网络上出售，获利金额累计达人民币2000余万元，涉及公民个人信息2亿余条。

中国电信
CHINA TELECOM

3、全国200多家三甲医院中招勒索病毒

全国200多家三甲医院中招勒索病毒：2018年9月，在一份报告中爆出，在全国三甲医院中，有247家医院检出了勒索病毒，以广东、湖北、江苏等地区检出勒索病毒最多。互联网时代，随着移动医疗、AI医疗影像、电子病历等等数字化程序的普及，医疗数据被泄露屡见不鲜。

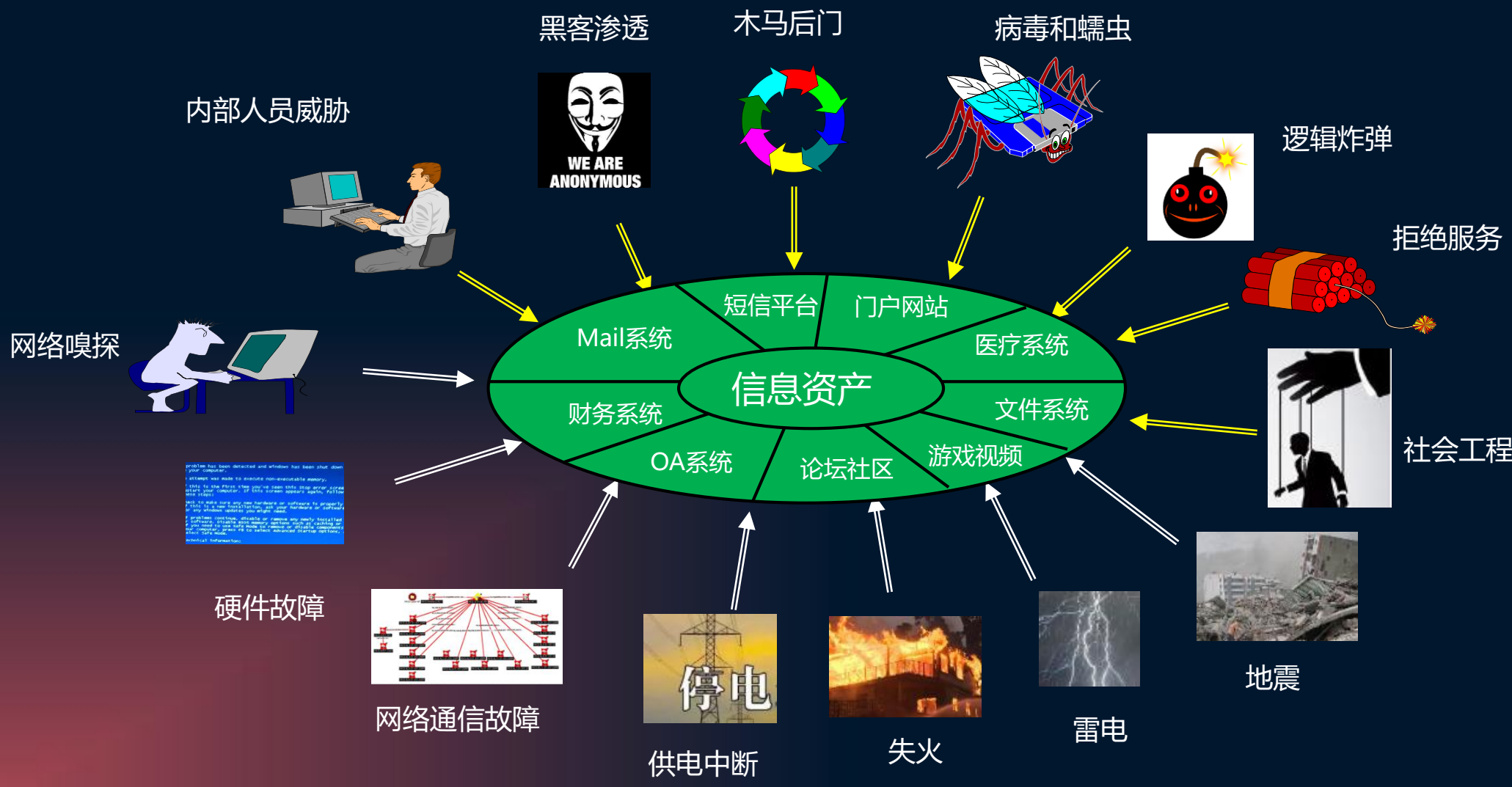
4、电信诈骗

山东徐玉玉因被电信诈骗骗走9900元学费，心脏骤停不幸离世。

实质是不法分子冒充教育局和有关部门，通过电话实施诈骗行为，不法份子通过黑客攻击手段获取了山东省高考网上报名系统中的考生信息，获取考生个人资料实施诈骗。

威胁来自什么地方？

安全事件起因分析


黑客渗透
木马后门
病毒和蠕虫
内部人员威胁
WE ARE ANONYMOUS
逻辑炸弹
拒绝服务
网络嗅探
短信平台
门户网站
Mail系统
医疗系统
信息资产
财务系统
文件系统
OA系统
论坛社区
游戏视频
社会工程
硬件故障
网络通信故障
停电
供电中断
失火
雷电
地震

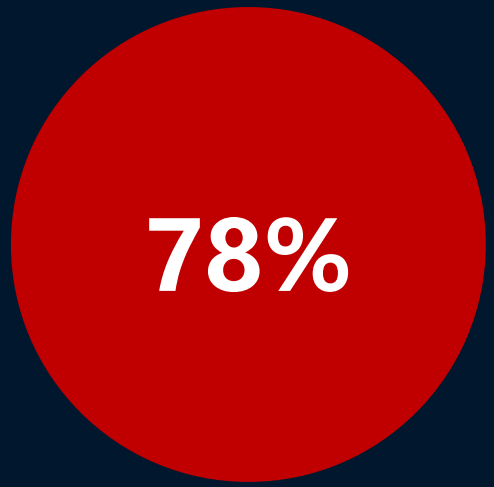
安全事件起因分析

⌦技术弱点	系统、程序、设备中存在的漏洞或缺陷
⌦操作弱点	配置、操作和使用中的缺陷，包括人员的不良习惯、审计或备份过程的不当等
⌦管理弱点	策略、程序、规章制度、人员意识、组织结构等方面的不足

企业安全事件起因分析

由黑客入侵或其他外部原因造成

由于内部员工的疏忽或有意泄露造成的



来自内部员工的不规范操作

➢ 什么是信息安全?

采取技术与管理措施保护信息资产，使之不因偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行，使安全事件对业务造成的影响减到最小，确保组织业务运行的连续性。

➢ 信息安全意识（Security awareness）

能够认知可能存在的安全问题，明白安全事故对组织的危害，恪守正确的行为方式，并且清楚在安全事故发生时所应采取的措施。

02 法规篇

常见类型安全防范规范

1、网络安全法

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

2、个人信息保护法（草案）

第一百〇一条. 政务部门法律责任政务部门违反本法规定，未落实个人信息安全保护义务的，由上一级政务部门责令改正；情节严重的，对负有责任的领导人员和直接责任人员依法给予处分。政务部门违反本法规定，侵害信息主体个人信息依法得到保护的权利的，由上一级政务部门责令改正；情节严重的，对负有责任的领导人员和直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任。

最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释

（一）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；违法所得五千元以上的情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金

（二）非法获取、出售或者提供公民个人信息“五百条以上”“五千条以上”“五万条以上”，或者违法所得五万元以上的，“造成重大经济损失或者恶劣社会影响；造成被害人死亡、重伤、精神失常或者被绑架等严重后果”，处三年以上七年以下有期徒刑，并处罚金。

03 规范篇

常见类型安全防范规范

十大安全类型防护

- 01-密码安全
- 02-工作环境安全
- 03-上网安全
- 04-电子邮件安全
- 05-移动存储安全
- 06-电脑安全
- 07-手机安全
- 08-社交安全
- 09-隐私安全
- 10-电信诈骗

01-密码安全

由于使用不当，往往使口令成为最薄弱的安全环节

口令也是抵御网络攻击的最后一道防线

口令与个人隐私息息相关，必须慎重保护

用户名+口令是最简单也最常用的身份认证方式

口令是抵御攻击的第一道防线，防止冒名顶替

针对口令的攻击简便易行，口令破解快速有效

01-密码安全

- 少于8个字符
- 单一的字符类型，例如只用小写字母，或只用数字
- 用户名与口令相同
- 最常被人使用的弱口令：
  - 自己、家人、朋友、亲戚、宠物的名字
  - 生日、结婚纪念日、电话号码等个人信息
  - 工作中用到的专业术语，职业特征
  - 字典中包含的单词，或者只在单词后加简单的后缀
- 所有系统都使用相同的口令
- 口令一直不变

01-密码安全

简单数字组合	顺序字符组合	临近字符组合	特殊含义组合
000000	abcdef	123qwe	admin
111111	abcabc	qwerty	password
11111111	abc123	qweasd	p@ssword
112233	a1b2c3		passwd
123123	aaa111		iloveyou
123321			5201314
123456			asdfghjkl
12345678			
654321			
666666			
888888			

中国用户常用的25个“弱密码”

01-密码安全

口令至少应该由8个字符组成

口令应包含大小写字母

口令应包含数字、特殊字符

不要使用字典中的单词

不要基于人的姓名、生日

01-密码安全

选择易记强口令的几个窍门：

- 口令短语
- 字符替换
- 单词误拼
- 键盘模式

密码： Quit@smoking4ever

解释：永远戒烟

密码： 1dcypsz1/2jss1/2j#f00

解释：一道残阳铺水中，半江瑟瑟半江红

02-工作环境安全

- 禁止随意放置或丢弃含有敏感信息的纸质文件，废弃文件需用碎纸机粉碎
- 废弃或待修磁介质转交他人时应经管理部门消磁处理
- 离开座位时，应将贵重物品、含有机密信息的资料锁入柜中，并对使用的电脑桌面进行锁屏
- 应将复印或打印的资料及时取走
- UKEY不使用时应及时拔出并妥善保管
- 禁止将手机和无线（例如：360wifi等）连接办公电脑

03-上网安全

- 使用安全浏览器
- 收藏经常访问的网站
- 安装杀毒软件，开启实时防护功能，并保持更新；
- 对超低价、超低折扣、中奖等诱惑要提高警惕；
- 警惕色情、赌博、反动等非法网站，避免访问；
- 防止网页自动记住账号密码。

04-电子邮件使用安全

应警惕的邮件内容：

- 伪造发件人信息
- 模仿单位领导
- 索取个人信息

进行网上交易时要注意做到以下几点：

- 核对网址
- 选妥和保管好密码、做好交易记录。
- 避免公用计算机使用网上交易系统；
- 不通过搜索引擎上的网址或不明网站的链接进入。
- 在网络交易前，对交易网站和交易对方的资质全面了解。

04-电子邮件使用安全

01 工作邮件建议使用自建邮箱，严禁使用境外邮箱；

02 为电子邮箱设置高强度密码，并设置每次登陆时必须进行帐号密码验证；

03 开启防病毒软件实时监控，检测收发的电子邮件是否带有病毒

04 不打开或转发来历不明的电子邮件及附件

05-移动存储安全

- 内外网数据交换需使用专用的保密U盘或刻录光盘；
- 移动存储使用时，关闭Windows上的自动播放功能。使用移动介质时，增加两三次的鼠标点击操作，减少计算机感染及传播病毒的机会。
- 使用移动存储前需要使用杀毒软件进行病毒扫描，使用后内容及时清除。
- 对存储介质内的重要敏感信息进行加密处理，对工作用硬盘进行密码保护。
- 废弃或待修磁介质转交他人时应经IT管理部门消磁处理。
- 离职人员的电脑要及时交由IT部门格式化磁盘。
- 智能手机、平板电脑、U盘等移动设备随身携带。
- 办公废弃的纸张使用粉碎机粉碎，而不是直接丢到垃圾桶。

06-电脑安全

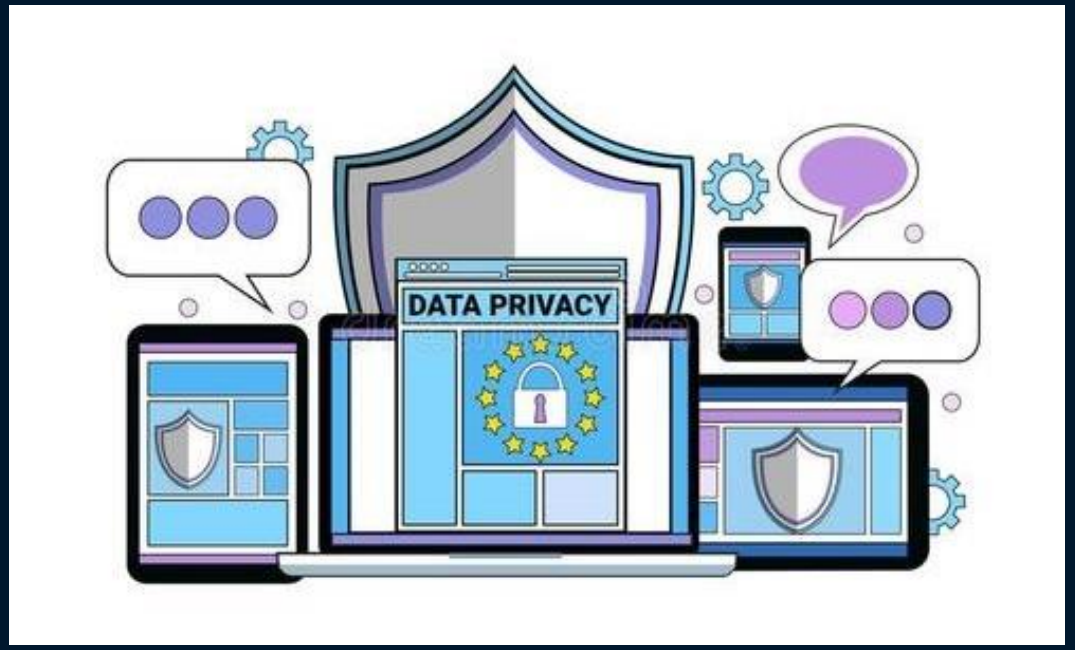
- 安装正版操作系统
- 安装正版应用软件
- 及时升级系统、软件补丁
- 开启系统防火墙
- 关闭非必要服务、端口
- 安装安全防护软件（如防病毒）
- 删除或禁止多余账户
- 设置强密码
- 采用多因子认证
- 打开文件或运行软件时先进行安全检查（如杀毒）
- 禁止U盘自动运行、并查杀病毒

07-手机安全

- 为手机设置密码
- 利用手机中的各种安全功能
- 从正规网站下载手机应用程序和升级包
- 禁用Wi-Fi自动连接功能
- 为手机安装安全软件
- 为手机SIM卡设置密码
- 经常为手机做数据同步备份
- 减少手机中的本地分享
- 对手机中的Web站点提高警惕
- 对程序执行权限加以限制

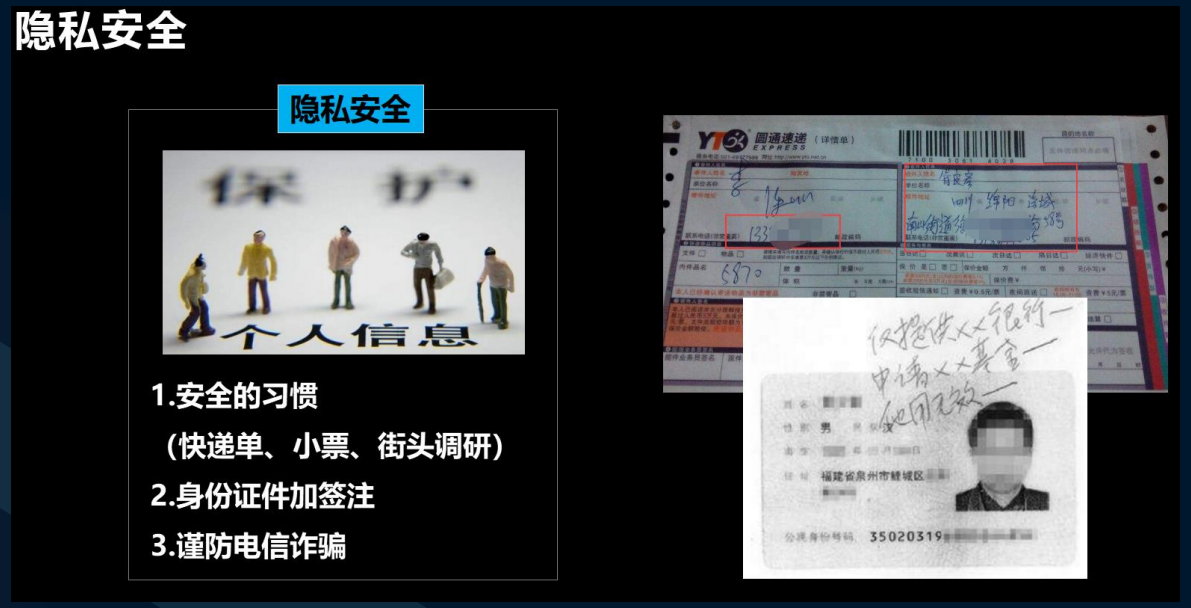
08-社交安全

- 不在朋友圈发送涉及个人隐私信息
- 不乱扫二维码
- 不应随意泄露个人信息
- 不随便接受来路不明的交友邀请
- 不要轻易相信对方的甜言蜜语，与陌生人见面
- 不轻易给QQ、微信等好友转账
- 火眼识破冒充好友（如聊天记录、语聊、提问）
- 不要随意连接陌生WIFI

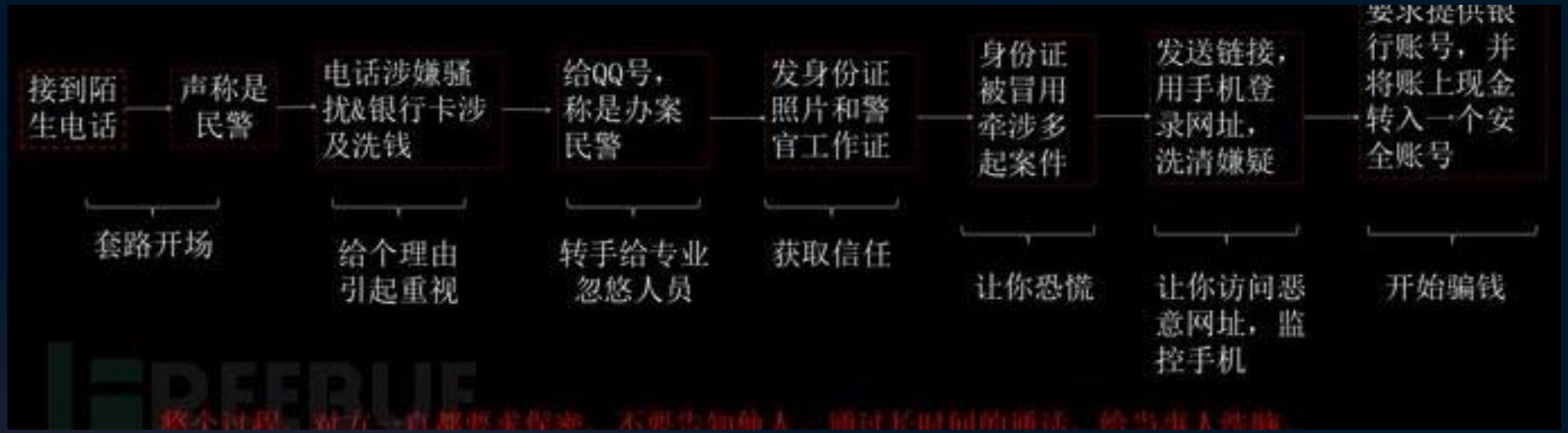


09-隐私安全

- 不要直接丢弃快递单，应去掉个人信息（快递单撕毁后或用马克笔涂掉个人信息）
- 街头或网络调研，尽量不要填写个人真实信息
- 复印件一定要加签注，不添加签注被盗用的风险极高，如去办理网络贷款等。



10-电信诈骗



对于电信诈骗的防护，接到陌生电话如果涉及洗钱、转账、公检法相关的直接挂掉就好，不要纠缠也不要想着反套路，术业有专攻。多关注媒体、公安部门通报的案情，增长防骗知识，如接到诈骗电话最好反馈给老师/同学，进行内部信息共享，规避其他同事/同学上当。

04 案例篇

二维码约鱼体验和手机入侵演示

01-二维码钓鱼体验

杀毒软件钓鱼
模拟体验

购物网站钓鱼
模拟体验

社交网站钓鱼
模拟体验

点击查看后台监控

02-实战演示

获取手机通话记录，应用列表，发送短信等。

外因是条件

内因才是根本

安全防范总览

不造谣、不信谣、不传谣

警惕网购骗局。

警惕网络黄赌毒。

了解相关法律法规，自觉约束个人行为

自觉抵制腐朽的网络文化，宣扬真善美，抵制假恶丑

警惕网络游戏的危害

拒绝诱惑

不做网络“黑客”

问 答

一、以下哪个密码非常容易被破解?

1、cyh19930425

2、qwer1234!@#$

3、Hisense$%^&

4、639DCB74ed46!

二、离开电脑时，锁定屏幕方法正确的是?

1、Ctrl键+L

2、 Windows键+L

3、Alt+键L

4、关闭显示屏

三、当您收到好友借款时，应当如何处理?

首先确认好友信息，确认好友信息是否可信后再作后续。

四、当发现终端可能中病毒或存在异常时候，您应当如何处理?

将设备异常信息主动上报安全部门，协助安全部门对重点进行排除处置。

提升信息安全意识，

增强安全防御能力！

外因是条件

内因才是根本

Thanks.