

信息安全意识培训讲座





本次干货由作者授权达人圈发布，更多干货请关注我们公众号



联系内推小能手，加入高薪求职大家庭

□ 什么是信息安全意识?



信息安全的内涵除了那道千万别忘记关的门，以及那颗永远别忘记关门的心——**信息安全意识**

□ 培训目标

- **生活**：如何保护个人生命财产安全、减少隐私泄漏；
- **工作**：如何避免发生安全事故，保障公司、组织和个人利益。
- 了解当前关于网络安全法律法规



提高信息安全意识!

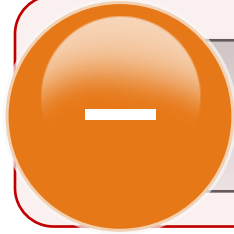
目录

CONTENTS

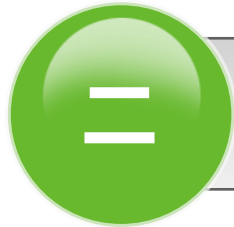
- 一 生活中的信息安全
- 二 工作中的信息安全
- 三 信息安全形势与政策法规

目录

CONTENTS



生活中的信息安全



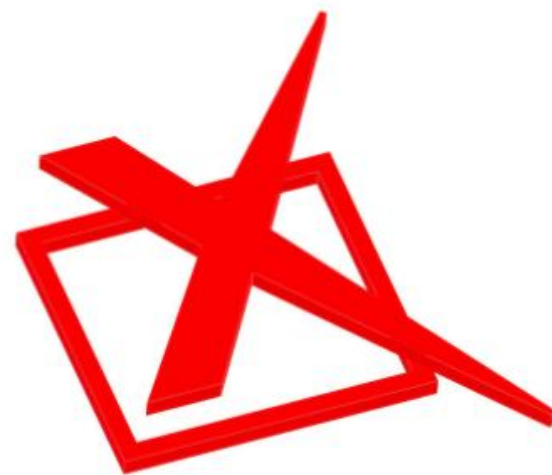
工作中的信息安全



信息安全形势与政策法规

❑ 你在生活中是否犯过这些错误？

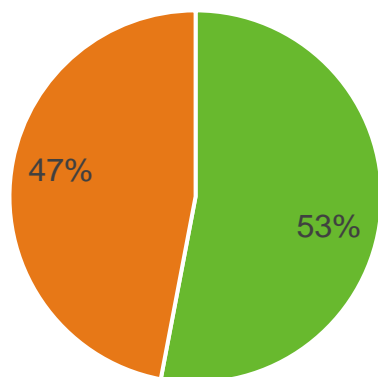
- ❑ 网银、电商网站、聊天软件、视频网站等统统使用相同的密码，且有规律可循
- ❑ 随意登录公共WIFI
- ❑ 随意关联银行卡输入密码
- ❑ 轻信钓鱼网站发的短信
- ❑ 随意注册各种网站
- ❑ 办会员、填调查问卷时，留自己的手机号、住址等信息
- ❑ Root、越狱手机安装不安全的APP
- ❑ 允许APP获取个人敏感信息
- ❑ 随意扫描二维码



□ 中国人愿意用隐私换取便利---李彦宏

- 2017年5月31日,《南方都市报》与中国政法大学传播法研究中心联合发布《互联网企业隐私政策透明报告》。对1000家常用网站、APP的用户信息保护政策透明度进行排名,结果显示,测评的生活服务、休闲娱乐、医疗健康等各个领域1000家平台中,超过50%的网站与APP评分为“低”级别,令人担忧。

你愿意提供个人信息以获得更便利的服务吗?



■ 愿意 ■ 不愿意



2018年数据泄露调查报告

数据泄露原因



行业分布



黑客攻击

62%的数据泄露与黑客攻击有关。

弱口令

81%的数据泄露涉及到撞库或弱口令。也就是说，直到2018年，人们使用密码的习惯依然不太好，绝大部分人并没有养成定期修改密码的习惯。

金融行业

金融行业依然首当其冲，24%的数据泄露事件和金融机构有关；

其他行业

其次是医疗保健行业15%；再往后是销售行业15%以及公共部门12%。其中医疗行业是勒索的重灾区，真可谓“不给钱就撕票”

□ 公司某系统用户弱口令调查

行标签	计数/password
123456	83
123	39
654321	23
huizhou	4
159357	3
2822	2
shicai	1
123321	1
100905	1
12345ssdlh	1
123461cy	1
A123457	1

弱口令!!!

公司某业务系统存在弱口令

The screenshot shows a web browser window displaying the TMS (Transport Management System) interface. The browser's address bar shows the URL `yhtms.yuhong.com.cn/Default.aspx`. The page content includes a navigation menu, a welcome message for user 123456, and a dashboard with various statistics and data tables.

The browser's developer tools are open, showing the request and response details for the login attempt. The request is a POST to `/diyh/dologin.do` with the following parameters:

```
POST /diyh/dologin.do HTTP/1.1
Host: hse.yuhong.com.cn
Proxy-Connection: keep-alive
Content-Length: 118
Cache-Control: max-age=0
Origin: http://hse.yuhong.com.cn
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
Referer: http://hse.yuhong.com.cn/diyh/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cookieLeftMenuSG00000001=0,0; UM_distinctHm_lvt_32d4a7cf09119b58f47c04ff6baf64fd=15285604pgv_si=s4287456256; _ga=GA1.3.1343142788.152856
Connection: close

value%28username%29=123456&passText=%E5%AF
```

The response shows a successful login, with the page content displaying the user's name and a welcome message. The dashboard includes a navigation menu, a search bar, and several data tables. The '今日发运计划' table shows a total of 98 items, and the '今日车辆统计' table shows 0 vehicles. The '今日发运详情' table lists various items and their weights.

Request	Payload	Status
80	!QAZ2wsx	302
0		200
1	QWEasd123	200
3	123ASDasd	200
4	123ZXCzxc	200
5	QWEqwe123	200
6	ASDasd123	200
7	ZXCzxc123	200
9	!@#123QWEasd	200
12	12QWaszx	200
11	1qazXSW@	200
13	@WSX1qaz	200
15	zaq!@#123	200
16	ZAQ!@#123	200

Request	Response
Raw	Params Headers Hex
POST /diyh/dologin.do HTTP/1.1	
Host: hse.yuhong.com.cn	
Proxy-Connection: keep-alive	
Content-Length: 118	
Cache-Control: max-age=0	
Origin: http://hse.yuhong.com.cn	
Upgrade-Insecure-Requests: 1	
Content-Type: application/x-www-form-urlencoded	
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_	
Accept: text/html,application/xhtml+xml,application/xml;q=0.9	
Referer: http://hse.yuhong.com.cn/diyh/	
Accept-Encoding: gzip, deflate	
Accept-Language: zh-CN,zh;q=0.9	
Cookie: cookieLeftMenuSG00000001=0,0; UM_distinctHm_lvt_32d4a7cf09119b58f47c04ff6baf64fd=15285604pgv_si=s4287456256; _ga=GA1.3.1343142788.152856	
Connection: close	
value%28username%29=123456&passText=%E5%AF	

今日发运计划	今日车辆统计
1、今日发运计划一共 98 条	1、应到车辆数量0辆
2、未处理数量 98 条	2、车辆签到数量0辆,剩余未到数量0辆
	3、已出厂车辆数量0辆

今日发运详情
【】 241.00m3(M3) 总重: 73.03吨
【保温】 720.00袋(DA) 总重: 18.36吨
【防水涂料】 240.00瓶(BOT) 总重: 0.14吨
【防水涂料】 10105.00桶(TO1) 总重: 202.43吨
【其他】 43.00桶(TO1) 总重: 0.90吨
【砂浆】 1085.00箱(XI) 总重: 22.79吨
总计: 803.92吨

今日发运详情
【】 6.00支(ZH) 总重: 0.00吨
【防水卷材】 7304.00卷(JU) 总重: 442.50吨
【防水涂料】 6.00袋(DA) 总重: 0.00吨
【防水涂料】 1964.00箱(XI) 总重: 42.55吨
【砂浆】 54.00桶(TO1) 总重: 1.03吨
【砂浆】 324.00支(ZH) 总重: 0.18吨

Copyright © 2016 上海齐炫信息技术有限公司 版权所有

防范措施

□

□

□

□

□

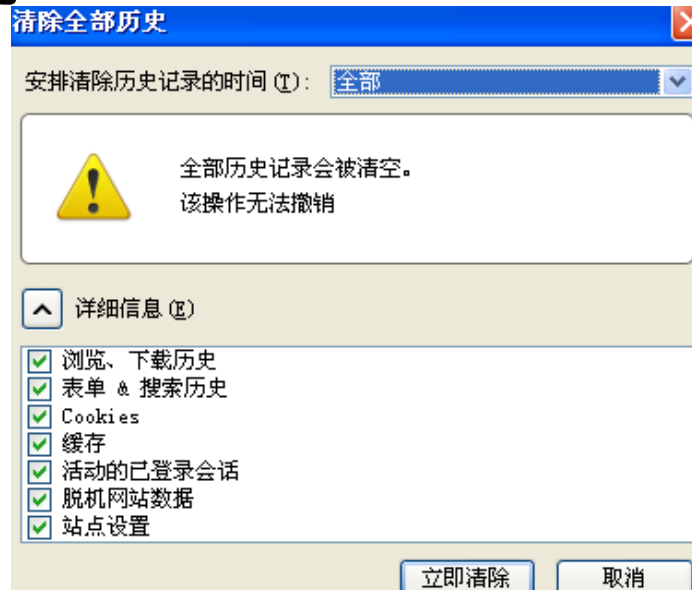


使用多个帐号密码体系：

- 一般网站群：视频网站、游戏网站、各类论坛 等等...
- 重要帐号：微信、支付宝、网银

□ 防范措施-弱口令

- 尽量不使用自动登录
- 尽量不使用记住密码功能
- 关闭浏览器时可以先清空本地缓存



□ 移动应用

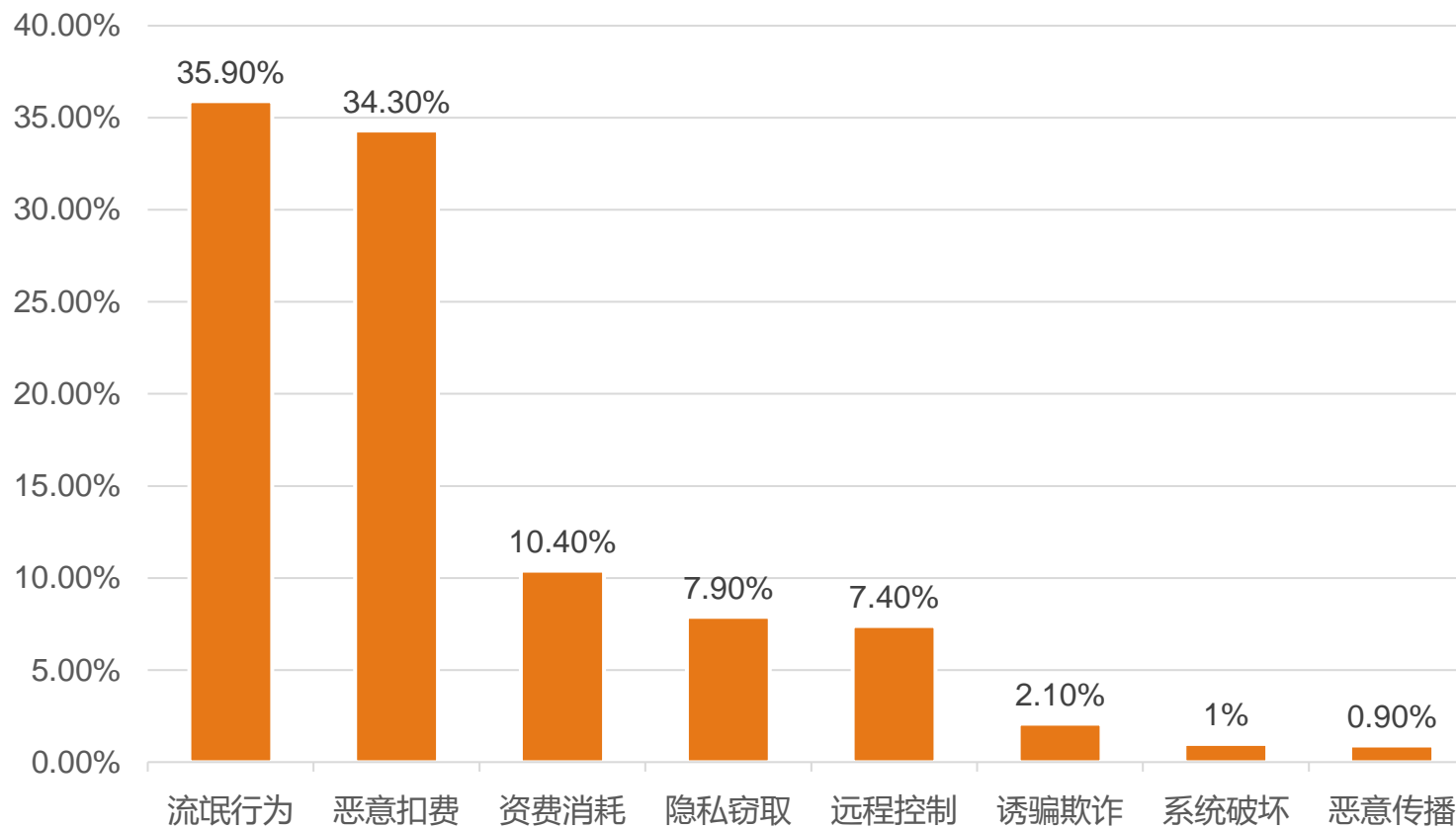


安全吗? ? ?



移动应用行为统计

2018年互联网恶意程序数量按行为属性统计



手机APP侵犯消费者信息情况调查

APP信息泄露检测

2017年8月，江苏省消协工作人员通过现场检测，在手机下载的100多个手机APP中，79个APP可获得定位权限，23个APP可直接向联系人发送短信。点开“电话与联系人”一项，有14个APP可以监听电话和挂断电话，结果非常惊人。



在所获取的个人信息中，“位置信息”和“读取通讯录和短信”是最容易被读取。



❑ 恶意软件-监视用户

❑ 2016年8月，研究人员透露了Pegasus（飞马）的存在

- Pegasus利用iOS中的三个零日漏洞，可以劫持任何iPad或iPhone，能以静默方式对设备越狱，并收集被攻击用户的相关数据，并对这些用户进行监视

IOS



恶意软件

Android

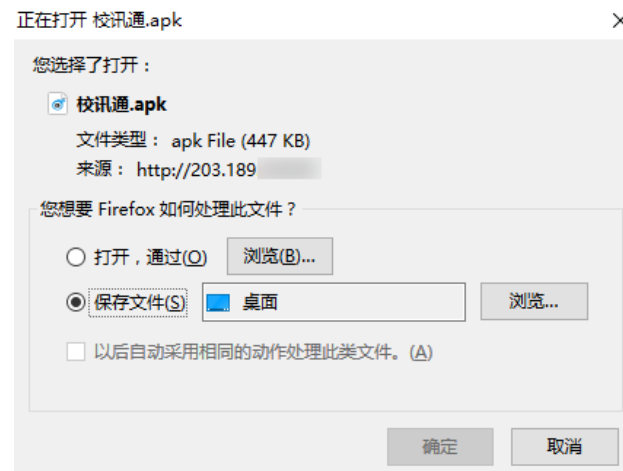
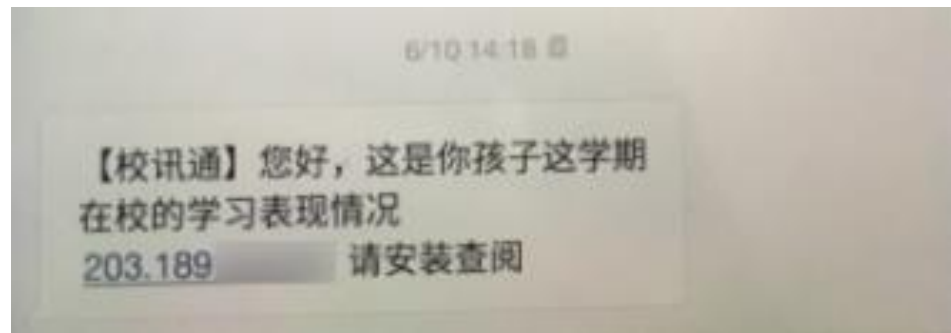
- 2017年4月，恶意软件作者再次袭击，这一次的飞马间谍软件版本的android 伪装成一个正常的应用程序下载，从而秘密获取设备root权限，来监视用户。

❑ 恶意软件-银行卡盗刷

❑ 受害者发现银行卡莫名被盗刷8万1千元：

交易日期	摘要	收入/支出	币种	余额	对方信息	操作
2016-06-12	卡取	-172.90	人民币	0.00		详情
2016-06-11	跨行费	-2.00	人民币	172.90		详情
2016-06-11	ATM取款	-500.00	人民币	174.90		详情
2016-06-11	平安	-1,000.00	人民币	674.90	平安付科技服务有限公司客户备付金	详情
2016-06-11	平安	-20,000.00	人民币	1,674.90	平安付科技服务有限公司客户备付金	详情
2016-06-11	平安	-50,000.00	人民币	21,674.90	广州银联网络支付有限公司客户备付金	详情
2016-06-10	网转	-50,000.00	人民币	71,674.90		详情
2016-06-10	网转	-20,000.00	人民币	121,674.90		详情
2016-06-10	平安	-10,000.00	人民币	141,674.90	平安付科技服务有限公司客户备付金	详情
2016-06-09	网转	-5,000.00	人民币	151,674.90		详情

❑ 通过检查问题手机，发现如下短信：

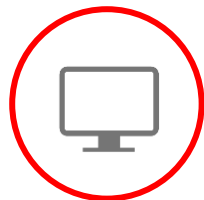


二维码用途



信息获取

(名片、地图、WiFi密码、资料)



网站跳转

(跳转到微博、银行网站、手机网站)



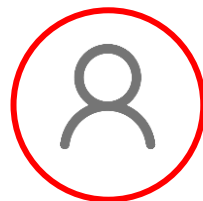
广告推送

(用户扫码, 直接浏览商家推送的视频、音频广告)



防伪溯源

(用户扫码、即可查看生产地;
同时后台可以获取最终消费地)



会员管理

(用户手机上获取电子会员信息、VIP服务)



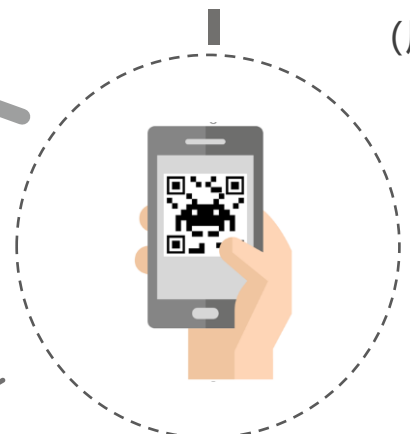
优惠促销

(用户扫码, 下载电子优惠券, 抽奖)

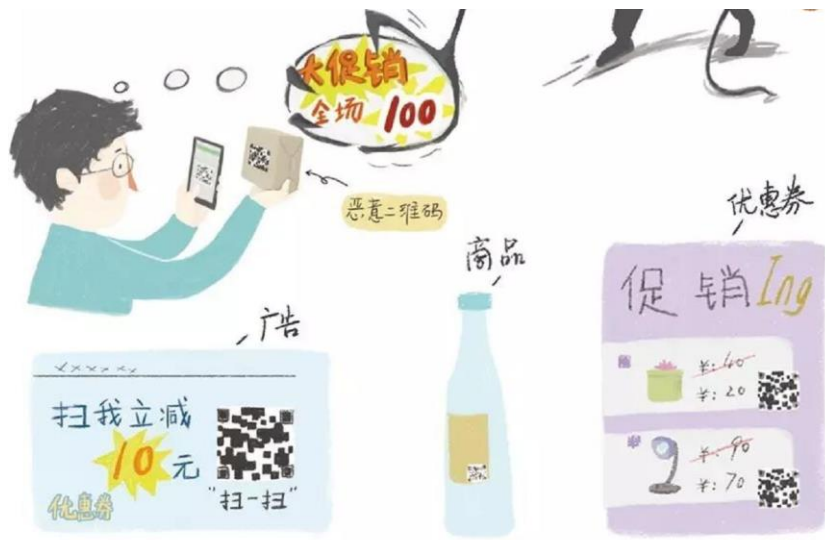


手机支付

(扫描商品二维码, 通过银行或第三方支付提供的手机端通道完成支付)



❑ 伪造二维码



伪造付款二维码

虚假“优惠促销”



假

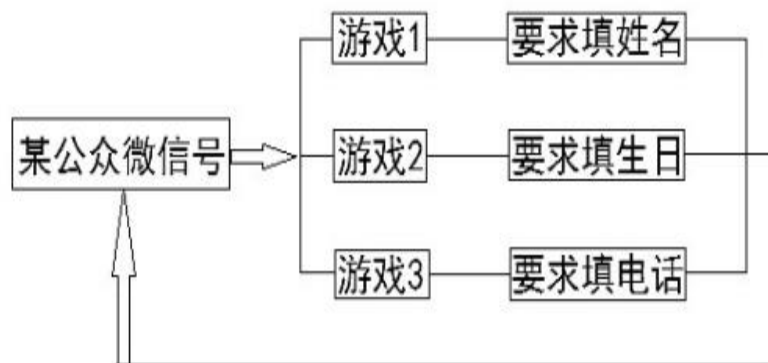


假



假

□ 公众号测试



□ 防范措施-移动安全



01 手机不要root、越狱!

- 不要安装来路不明的应用，只安装手机品牌商店中的应用。



02

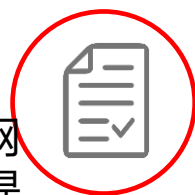
安装软件少点“允许”

- 手机安装软件时，常被要求“使用你的位置”、“获取短信权限”、“获取照片权限”、“获取通话记录”等。



03 不要随意扫描二维码

- 不要见“码”就扫，对于街头及网上发布的不明来历的二维码需要提高警惕。
- 扫描二维码后，应仔细检查页面上的所有文字，如需安装新的应用程序时，则不要轻易安装。



04

网上测试小心有诈

“测测你的心理年龄”、“测测你前世是谁”……测试时输入的姓名、生日、手机号码等，会存入后台，对其梳理，有可能拼凑出完整个人信息。

WiFi安全

我国WiFi使用现状

2017年公共WiFi总数超过3.36亿，手机网民已超过7.88亿。值得注意的是，其中92%的手机网民使用WiFi接入互联网，平均每天每人连接WiFi时长1.1小时。由此可见，WiFi已经成为民众日常生活中不可或缺的一部分。



《公众网络安全意识调查报告》显示，有高达80.21%的网友会寻找公共免费WiFi，在连接之后浏览网页和使用即时通信工具的用户高达45.29%，还有38.96%的用户会进行网上支付等金融操作



□ 利用**WiFi**可以做什么？

□ 钓鱼WiFi:

在繁华的街道设立名字叫做“CMCC”、“KFC”的WiFi热点

□ Karma:

伪装成受害设备以前连接过的公开WiFi热点。

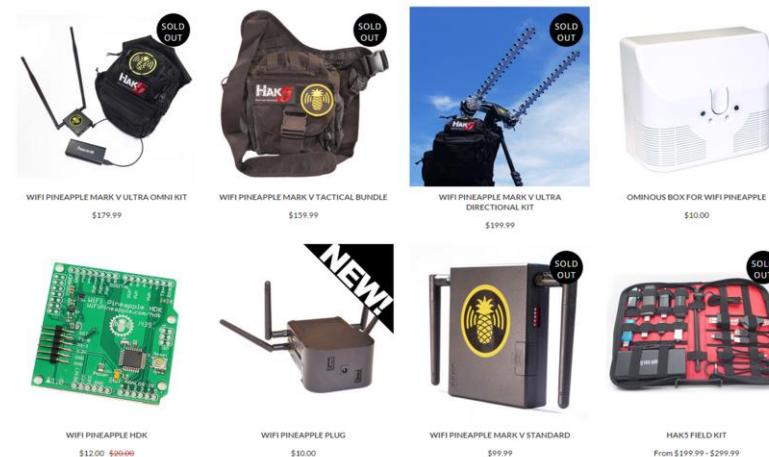


❑ 域名劫持:

劫持、篡改DNS查询结果，即使输入正确的网站网址也会访问攻击者预设的、相似度极高的山寨钓鱼网站

❑ 流量劫持:

可以监听受害终端发出的数据
可以篡改服务器返回的数据



□ 防范措施-WIFI安全



□ 识别钓鱼网站和短信：

a) 查看通讯协议：

查看域名前的协议是 <http://> 还是 <https://>

涉及金钱交易的网站均使用[https](https://)，并且浏览器会在[https](https://)前显示绿色安全标志

b) 正确识别主域名：

<http://zhidao.baidu.com>

<http://baidu.zhidao.com>

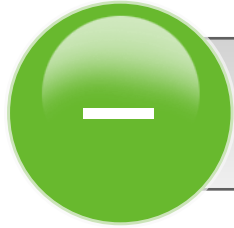
<http://abc.baidu.zhidao.com>

c) 不泄漏账户、密码、验证码：

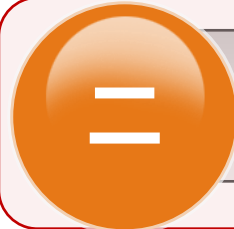
不以任何方式泄漏各类验证码、身份认证信息

目录

CONTENTS



生活中的信息安全



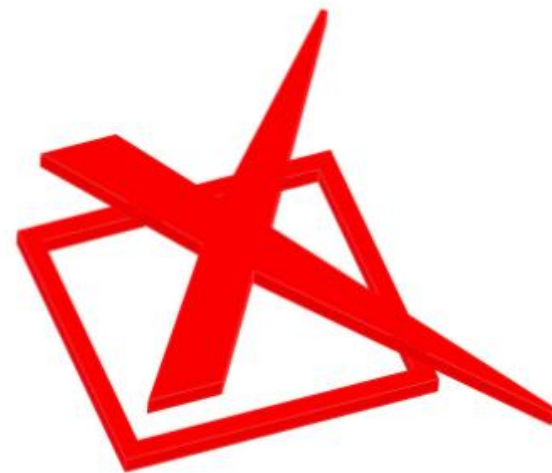
工作中的信息安全



信息安全形势与政策法规

□ 工作中常犯的一些错误

- 开着电脑离开，就像离开家却忘记关灯那样
- 轻易相信来自陌生人的邮件，好奇打开邮件附件
- 使用容易猜测的口令，或者根本不设口令
- 随便拨号上网，或者随意将无关设备连入公司网络
- 事不关己，高高挂起，不报告安全事件
- 在系统更新和安装补丁上总是行动迟缓
- 只关注外来的威胁，忽视企业内部人员的问题
- 在公共场合谈论公司信息
- 会后不擦黑板，会议资料随意放置在会场



□ 社会工程学攻击

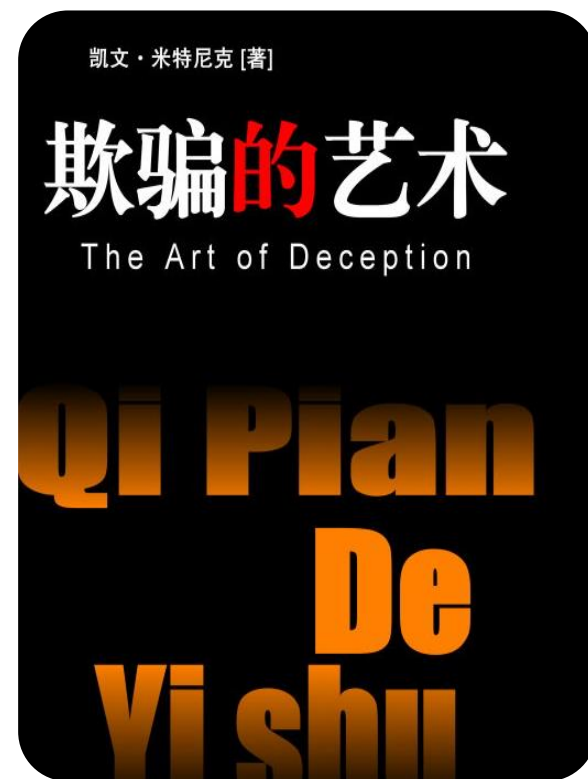
通过对受害者

本能反应、好奇心、信任、贪婪

等心理弱点进行如欺骗和伤害等攻击手段

社会工程学的攻击，成功于人们

普遍的对网络安全意识的薄弱！



□ 社会工程学



搜集足够多的信息，以便于伪装成一个合法的雇员、合作伙伴、执法官员，或者任意角色。



我就是我所声称的那个人！

采集信息

选择目标

建立信任

实施攻击



寻找组织、员工的明显弱点，寻求突破。



社会工程学 - 典型案例

美国一家印刷公司，其**工艺专利和供应商名单**是公司的核心资产，也是竞争对手的宝贵材料。为了保证安全，公司雇佣克里斯，一名资深的社会工程师，进行社会工程学攻击，探测该公司的服务器是否能够被入侵。

进入我们公司的服务器是几乎不可能的，因为我在用性命看管这些材料！

收集服务器相关信息：

服务器IP地址、物理地址、操作系统、应用程序及相关版本

1

收集个人相关信息

爱好：常去的餐厅，喜欢的比赛和球队
家庭状况：家庭成员及相关经历
线索：家人与癌症奋斗并存活下来

2

收集癌症相关的信息
癌症医疗机构及相关信息
知名的癌症慈善机构
规律性的募捐活动和规则

3

印刷公司CEO

接近

伪装成癌症慈善机构的工作人员，电话给CEO说明最近机构会有一次抽奖活动，来感谢好心人的捐赠

4

打动

奖品除了几家餐厅（包括他最喜欢的那家餐厅）的礼券外，还有他最喜欢的球队参加的比赛的门票

5

中招：

同意让克里斯给他发来一份关于募捐活动更多信息的PDF文档。当他打开PDF文档时，电脑上已经被安装外壳程序

6

□ 如何防范社会工程学攻击？

策略

安全策略是指导员工行为，保护企业信息系统与敏感数据所必须遵循的规则。

技术

必要的安全控制措施在一定程度上，能够缓解攻击所带来的损害。从企业信息资产调查开始，分离地看待每一个敏感的，关键的资产，寻找攻击者使用社会工程学策略可能危及这些资料安全的方法，实施相应的控制措施。

培训

安全培训能够让企业的所有员工了解公司的安全策略与控制程序。
改变组织的思维方式，持续地对员工进行培训，协助其识别安全威胁，及潜在的攻击方式；并提升个人成就感，每个人正在为公司的安全做出贡献。



□ 社交网络

一家负责维护世界杯安全工作的公司出现了一件令人啼笑皆非的低级失误：该公司一名工作人员在twitter上发布了一张安全监控中心的照片，而照片上直接出现了世界杯安全团队的WiFi密码……“神”一样的队友。



□ 数据泄露

- GitHub是全球最大的社交编程及代码托管网站。在GitHub, 用户可以十分轻易地管理、存储、和搜索程序代码, 其因此受到了广大程序员们的热爱, 而近两年有大量的攻击事件由GitHub泄露敏感信息引起。

```
{name: '谭', phone: ['13 jdbc.url=jdbc:oracle:thin:@[redacted]:e[redacted]sw
{name: '海', phone: [' jdbc.username=e[redacted]
{name: '向', phone: ['13 jdb 7
{name: '景', phone: ['1 # 8
{name: '日', phone: ['15 # 8
{name: '原', phone: ['18 dat 9
{name: '丹', phone: ['18
{name: '应', phone: [' #ft 10
{name: '源', phone: [' #eu 11
{name: '谭', phone: ['15 #ex 12
{name: '黄', phone: ['15 #ex 12
{name: '朱', phone: ['18 #eu 13
{name: '汤', phone: ['15 #ua 14
{name: '周', phone: [' #eu 14
{name: '陈', phone: [' #eu 15
{name: '罗', phone: ['13 #eu 16
{name: '谭', phone: ['13 #eu 16
{name: '张', phone: ['15211 17
{name: '谭', phone: ['13873 17
{name: '周', phone: ['13787 18
{name: '余', phone: ['18711 18
```

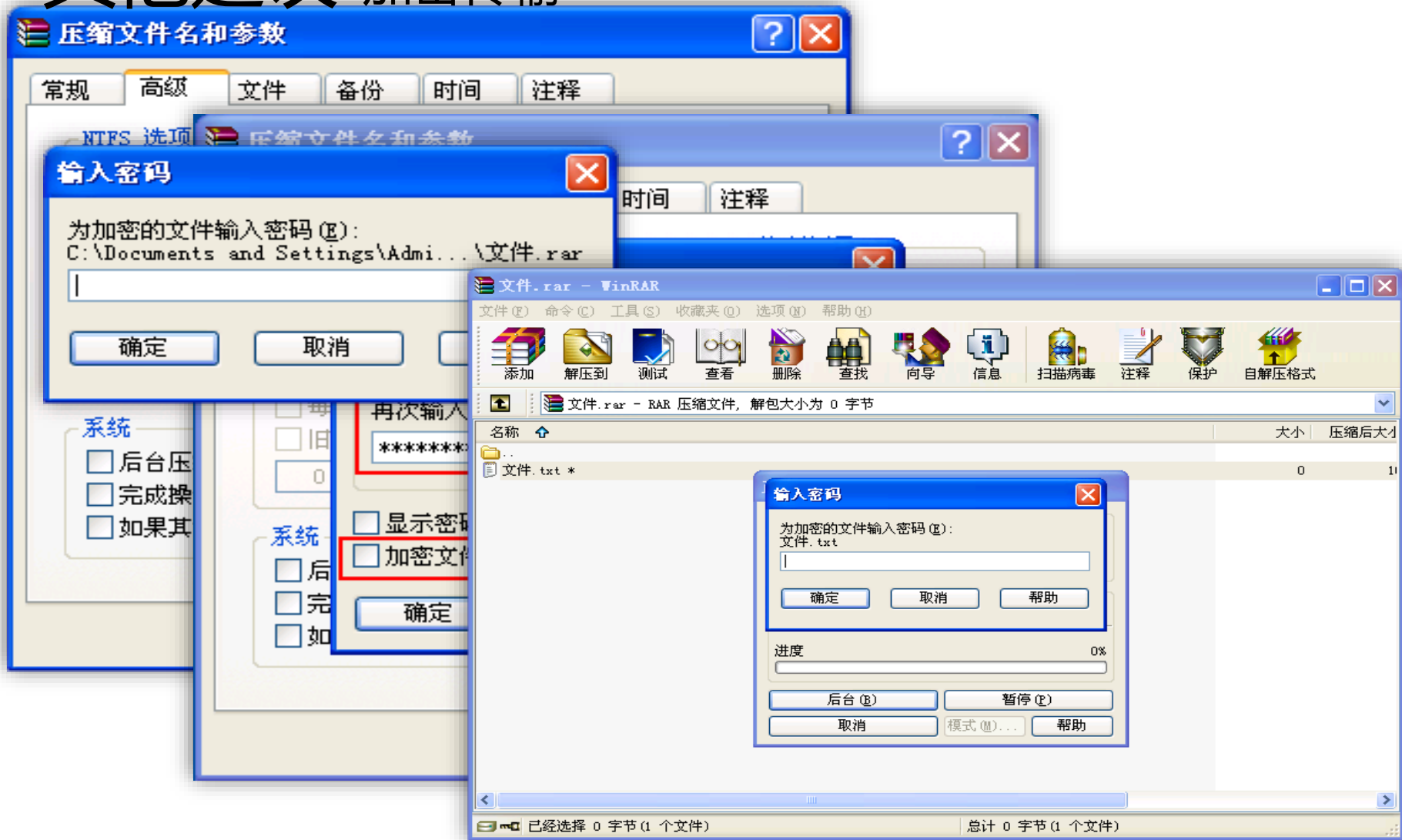
```
"sync_down_on_open": true,
"sync_same_age": true,

"host": "c[redacted].kr",
"user": "dcc120140248",
"password": "mkw0268",
// "port": "22",
"upload_on_save": true,
"remote_path": "/export/dcc_class/dcc/dcc120140248/hw1",
// "file_permissions": "664",
// "dir_permissions": "775",
```

□ 防范措施

- 避免将公司敏感资料上传至互联网第三方平台;
- 在公司内网搭建服务器进行资料保存;
- 对敏感资料进行加密保存;
- 对资料访问权限进行设置。

□ 其他建议-加密传输



□ 其他建议-安装杀软

□ 可根据个人使用习惯来选择且及时升级病毒库

The screenshot displays the Avira software interface. On the left, a red '安全警报' (Security Alert) window is open, reporting a detected threat: '在文件"C:\Documents and Settings\Freefinder\桌面\msf.doc"中发现了病毒或恶意程序"EXP/CVE-2012-0158"。' (A virus or malicious program 'EXP/CVE-2012-0158' was found in the file 'C:\Documents and Settings\Freefinder\Desktop\msf.doc'). Below this, a '安全漏洞' (Security Vulnerability) section is visible, with a search bar containing 'CVE-2012-0158'. On the right, the 'PC 防护' (PC Protection) settings window is open, showing 'Real-Time Protection' is turned on, and '开始更新' (Start Update) is available, with the last update time being '2013-1-18'.

AVIRA

安全警报

日期/时间：2013-1-18, 16:26:31
类型：检测

在文件"C:\Documents and Settings\Freefinder\桌面\msf.doc"中发现了病毒或恶意程序"EXP/CVE-2012-0158"。

我们已经阻止了对此文件的访问。

您可以删除该文件或了解有关该问题的更多信息。

安全漏洞

所有系统 | 所有类型 | CVE-2012-0158

分页 (1) 共 1 条记录

- 2012-04-11 Microsoft Windows Common Controls ActiveX控件远程代码执行漏洞(MS12-027)

分页 (1) 共 1 条记录

PC 防护

Real-Time Protection

扫描系统 上次扫描时间：未执行

备份文档 上次备份时间：-

开始更新 上次更新时间：2013-1-18

□ 其他建议-谨慎使用移动存储设备

- 请勿随意使用U盘等移动存储设备
- 使用完后进行擦除或粉碎操作
- 不要长期、大量存放涉密文件



□ 其他建议-打印复印

- 复印/打印时，禁止将敏感资料遗留在复印机/打印机旁边
- 对不再使用的资料，应使用碎纸机将其清理



□ 其他建议-培养安全办公习惯

- 进入大门、闸机时主动阻止陌生人尾随进入；
- 陌生人员未经陪同出现在办公区域，应主动上前询问；
- 废弃的纸质资料应该进行充分粉碎（碎纸机）；
- 废弃的移动存储设备应交由IT部门消磁处理；
- 离开工位时对办公电脑进行锁屏；
- 敏感资料应妥善保管，在离开工位时锁入柜中；
- 不应使用来历不明的移动存储设备；
- 不应接入来历不明的WiFi热点；
-

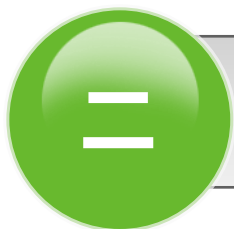


目录

CONTENTS



生活中的信息安全



工作中的信息安全



信息安全形势与政策法规

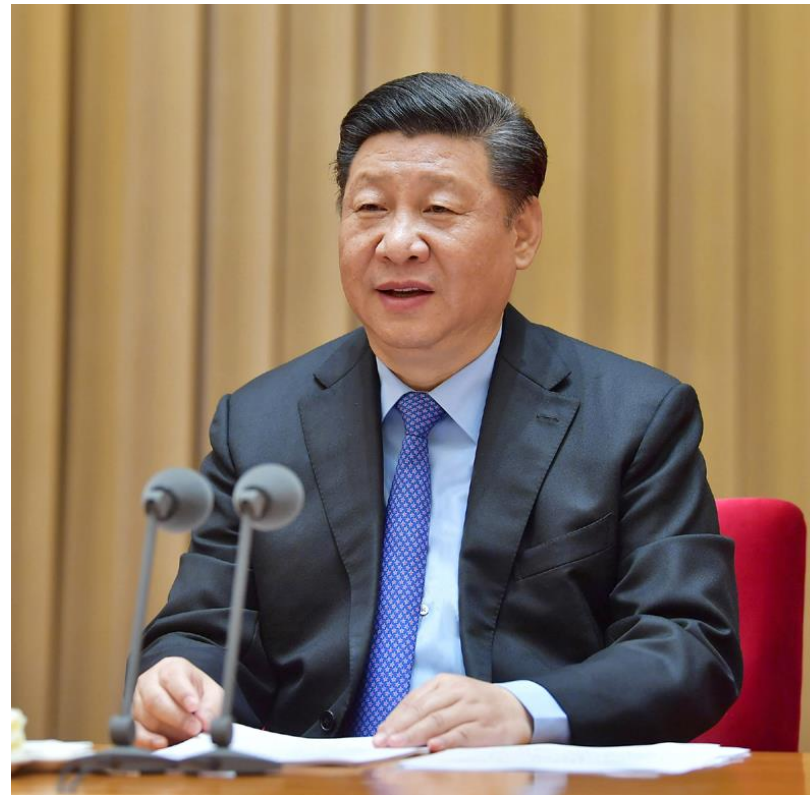
□ 中央网络安全和信息化领导小组

中央网络安全和信息化委员会

2014年2月27日，中央网络安全和信息化领导小组成立，习近平亲任组长。和以往国家层面信息安全领导机构相比，规格置顶。



没有网络安全，就没有国家安全；没有信息化，就没有现代化的指导精神。





中华人民共和国 网络安全法

2017年6月1日起施行

□ 网络安全法 - 国内背景



□ 网络安全法 — 制定历程

形成初稿

2014

- 2014年二月中央网络安全和信息化领导小组成立，习近平任组长。两会上，“维护网络安全”首次被写入政府工作报告。

2015

征求意见

- 6月：十二届全国人大常委会审议了《网络安全法（草案）》
- 7月：向社会公开征求意见，形成《网络安全法（草案二次审议稿）》

2016

审议通过

- 6月：十二届全国人大常委会对《网络安全法（草案）》进行了二次审议
- 7月：《网络安全法（草案）》二次审议稿正式在中国人大网公布，并向社会公开征求意见
- 11月：第十二届全国人民代表大会常务委员会第二十四次会议通过

2017

正式实施

- 2017年6月1日正式实施

□ 网络安全法主要内容

- 明确了网络空间主权的原则。
- 明确了网络产品和服务提供者的安全义务。
- 明确了网络运营者的安全义务。
- 进一步完善了个人信息保护规则。
- 建立了关键信息基础设施安全保护制度。
- 确立了关键信息基础设施重要数据跨境传输的规则。



□ 违法处罚案例

汕头某公司未及时履行网络安全义务，网警依据网安法责令改正

2017-08-08 10:47:01 微信公众号“西文”

腾讯微信、新浪微博、百度贴吧涉嫌违反《网络安全法》被立案调查

2017年08月17日 16:00:00

来源：中国网信网



【打印】 【纠错】

网信办约谈李文星事件涉事网站 责令BOSS直聘立即整改

重庆一网络公司未留存用户登录日志被网安查处

2017-08-04 22:42:22 来源：中青在线(北京)

四川查处违反网络安全法首案：一网站因高危漏洞遭入侵被罚

2017-08-11 17:26:00 来源：澎湃新闻(上海)

宿迁网警成功查处全省首例违反《网络安全法》接入违规网站案

株洲通报首起违反《网络安全法》案 一网络公司受行政处罚

2018-04-16 18:48 株洲新闻网 记者 李维熙 我要评论 0 扫描到手持设备 字号： T T

违规了！淘宝网等5家网站被责令限期整改

2017-08-17 19:04:34 来源：新华社

□ 个人法律合规要求

□ 规范上网行为：

- 诈骗、传授诈骗方法、制售违禁物品
- 不得危害网络安全（入侵、窃取等）、国家安全；
- 不得发布不良信息
- 不得侵犯他人权益

□ 不为上述违法行为提供便利






□ 正确认识网络安全

“真正安全的计算机是拔下网线，断掉电源，放在地下掩体的保险柜中，并在掩体内充满毒气，在掩体外安排士兵守卫。”

-----绝对的安全是不存在的!

“安全不只是产品的简单堆积，也不是一次性的静态过程，它是人员、技术、管理**三者紧密结合的系统工程，是不断演进、循环发展的动态过程。”**

史上最全的信息安全培训合集!

-  网络安全培训(安全意识).pptx
-  网络安全意识与案例分析.ppt
-  网络安全意识与必备技能培训.pptx
-  信息安全意识培训-JC.pdf
-  信息安全意识培训讲座.pptx



免费领取办法：扫上面二维码，备注：信息安全

谢谢!