个人信息保护

安全应对指南

前 言

随着网络信息技术的持续演进，互联网对整个经济社会发展的渗透、驱动作用越来越明显，带来的风险挑战也在不断扩大。

个人信息一旦进入互联网，就有可能在全球范围内得以传播，而且可以被人无休止地转载、复制。在网上宣扬、公开他人隐私；黑客篡改、监看他人电子邮件，以及网络银行账户、密码；垃圾邮件泛滥；专门非法获取、利用他人隐私的网络窥探业务；商家通过消费者网上购物，在消费者不知情的情况下获取关于其购物习惯、消费喜好、经济状况等信息，再经过专门的数据库分析，从而得到有价值的商业资料等等，网络安全威胁和风险日益增多，地下黑产、电信网络诈骗等各类违法犯罪活动时有发生，数据安全和侵犯个人隐私问题日益凸显。因此学会个人信息安全保护，是每一个人所需具备的基本素质。

时刻做好个人信息保护，针对当前个人网络信息安全意识教育的难点与痛点，杭州安恒信息技术有限公司利用多年从业经验，结合真实案例编撰本书，旨在提升个人上网意识，科普网络安全知识，逐步建立起全社会对网络安全问题的认识和应对技能。

主要包括以下内容：

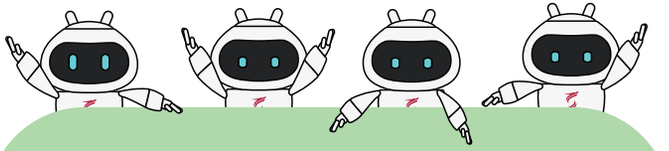
- 终端安全
- 沟通工具安全
- 内部资源保护
- 纸质文件保护
- 不明设备安全
- 敏感资料保护
- 熟知安全
- 邮件安全
- 个人信息安全
- 密码安全
- 二维码安全扫描
- 病毒处理
- 物联网设备安全
- 地理位置信息保护
- 移动安全
- 电信诈骗预防
- 预防诈骗总结
- 法律知识

目 录

01
工作篇

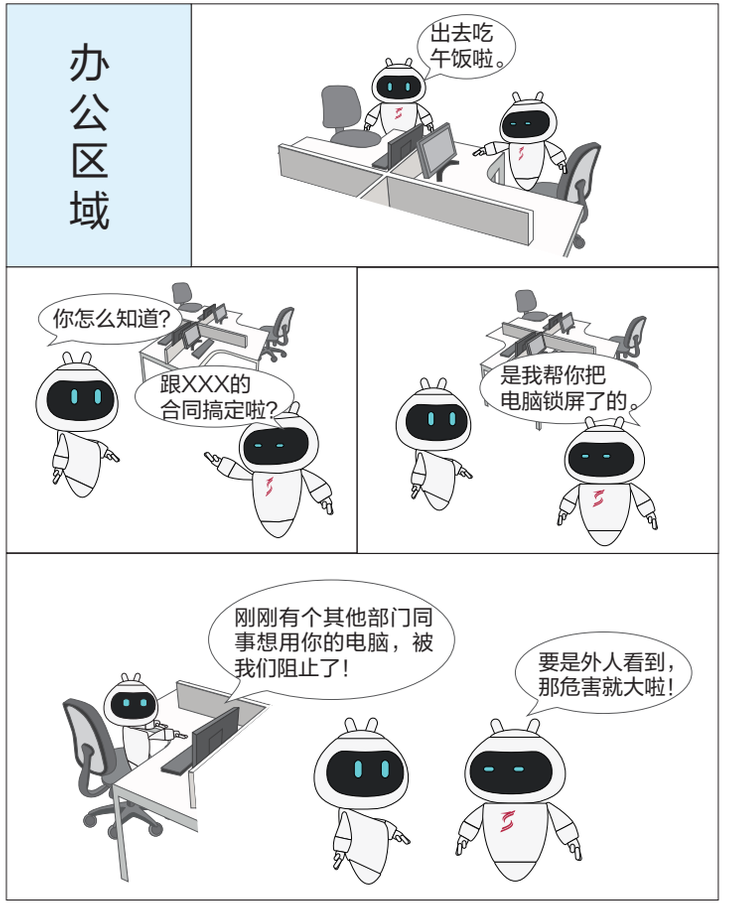
02
生活篇

03
法律篇



工作篇

一 | 电脑锁屏



- 案例解析　同事间的工作性质不同，工作内容不同，有权看到的信息级别也不同，甚至在开放的办公环境下，仍有可能来自外部门或外公司的人员，长时间离开电脑前，经过的人不光能看到屏幕内容，别有用心的人还会打开电脑中的各种文件，乃至拷贝。
- 安全建议　1.电脑设置屏幕保护，避免离开时忘记锁屏
  2.短时间离开电脑前要锁屏
  3.长时间离开电脑前建议关机
  4.提高使用电脑安全意识，一定要设置开机密码

使用正版软件 | 二

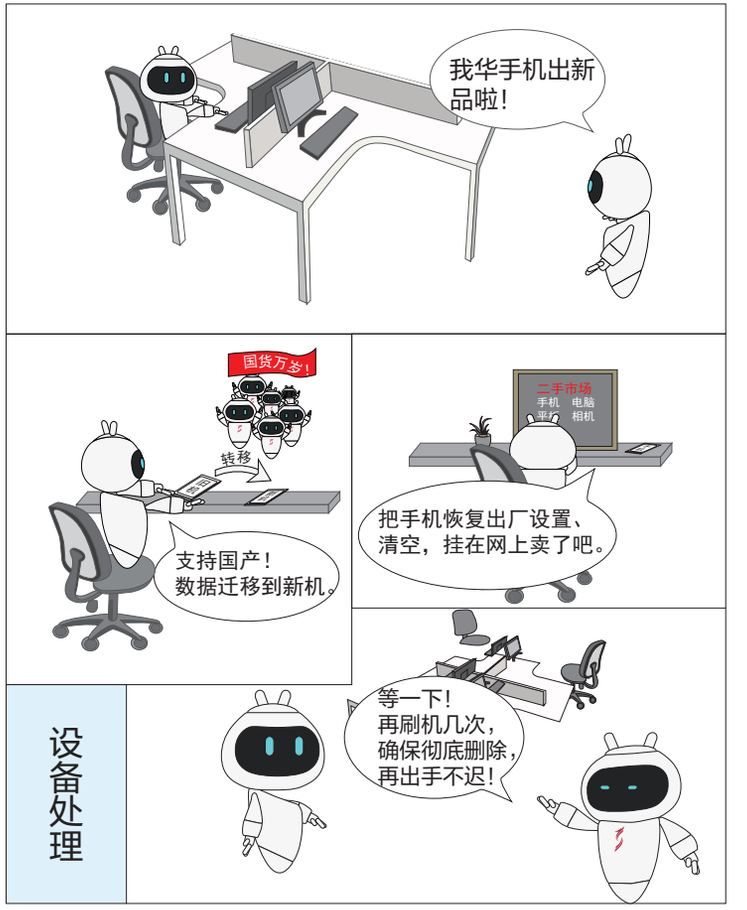
- 案例解析　不法分子会利用一些安全性不高的小软件下载站点，将病毒捆绑后进行分发，这些软件安装使用后在后台隐形的运行着病毒、木马，利用用户免费使用心理，提示用户关闭防火墙或信任、授权等错误行为，另有些病毒、木马有免杀毒版本，强行运行。
- 安全建议　1.下载应用软件到官方网站下载
  2.常用软件购买正版软件
  3.对于无法识别软件，请联系IT部门进行申请使用

三 | 云储存安全使用

三 | 云储存安全使用

- 案例解析　云储存是互联网存储工具，通过互联网为企业和个人提供信息的存储、读取、下载等服务，存储量大，应用简便成为了大众喜爱的存储方式，但也容易成为黑客攻击的目标。“技术贼”利用专业技能破译密码，WI-FI钓鱼，同时云盘本身可能存在的漏洞被利用。
- 安全建议　1.在云储存应用过程中设定时间维度，并及时清理文件
  2.不与他人共享使用 ，不存储机密、敏感文件
  3.移动端使用关闭自动备份功能

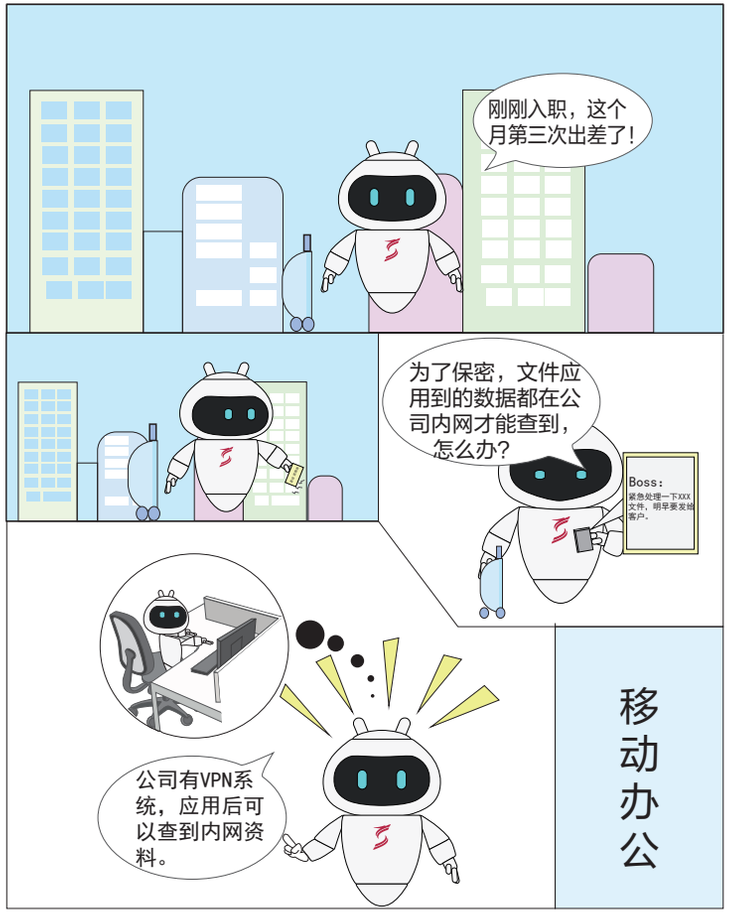
设备维修/报废 | 四



设备维修/报废 | 四

- 案例解析　使用旧版的移动设备相对更易遭到攻击，在应用中一定要确保系统已经更新，在更换手机后，将旧手机恢复出厂设置是必要的，但也只是把系统文件简单还原、用户数据简单删除，在手机芯片上并未彻底删除。
- 安全建议　1.对于移动设备的安全应用，首先设置访问密码、指纹、面部识别以防万一
  2.手机出售前，还需要用大的视频文件反复拷贝删除几次
  3.手机不慎丢失后，第一时间到运营商补卡，让旧卡失效，及时修改移动支付登陆密码，支付密码

五 | 外出办公安全



五 | 外出办公安全

- **案例解析** VPN被定义为通过一个公用互联网络建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定隧道，使用这条隧道可以对数据进行几倍加密达到安全使用互联网的目的，广泛使用企业办公当中。
- **安全建议** 1.公司内部资料应建立内部服务器资源，便于员工应用，且降低遗失、盗用的风险
  2.建立VPN系统，无论员工出差或在家中都能时刻访问内网资源

办公通讯安全 | 六

办公通讯安全 | 六

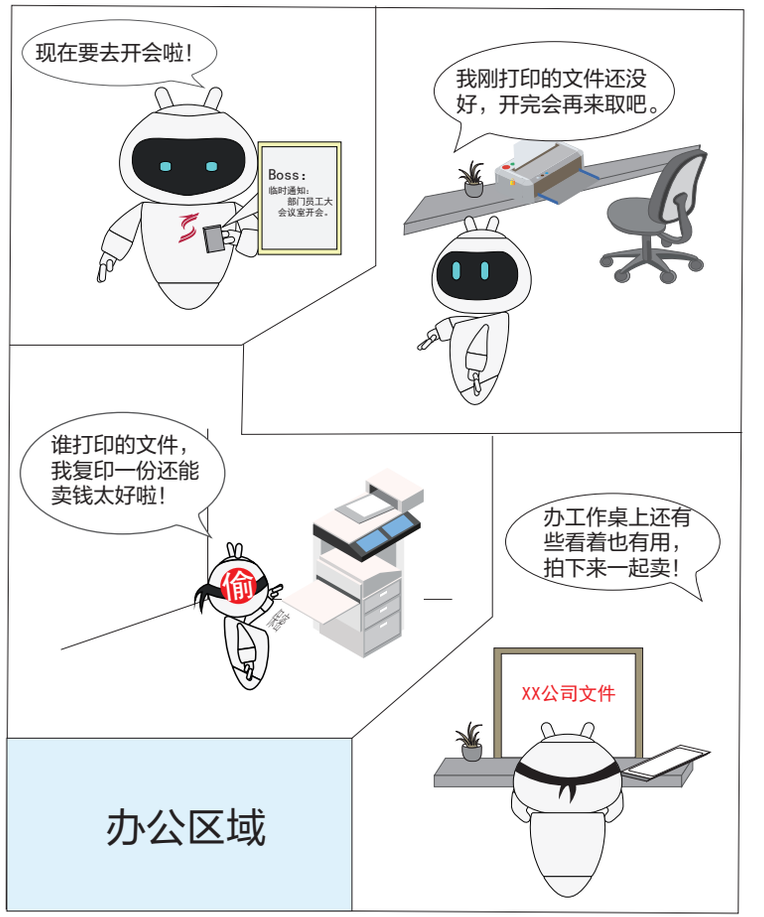
- **案例解析** 互联网的应用让沟通更便捷，同时也带来了很多网络安全隐患，在沟通工具的选择上要注意，曾经国家计算机病毒应急处理中心通过对互联网监测发现，一种恶意木马程序变种Trojan_FakeQQ.CTU。该变种通过伪装成即时聊天工具，诱使计算机用户点击运行。
- **安全建议** 1.在沟通交流前，首先做好重要文件的备份
  2.对重要、敏感文件进行加密，避免被直接利用
  3.在工作沟通工具上，与日常社交工具区分开

七 | 通讯录安全

七 | 通讯录安全

- **案例解析** 很多人仍然没有意识到，类似公司通讯录等信息属于商业机密，黑客攻击方式不单纯在代码中，社会工程攻击，同样是实施网络攻击流程中的一环，通过与他人的合法地交流，来使其心理受到影响，做出某些动作或者是透露一些机密信息的方式。
- **安全建议** 1.在接到电话、短信、邮件等方式所要公司内部资源，如文档、客户信息等，首先要验证对方身份
  2.验证身份的同时，要通过正规流程知晓对方获取资料的权限范围
  3.对于已离职员工，及时清理出工作交流群组

纸质文件保护 | 八



八 | 纸质文件保护

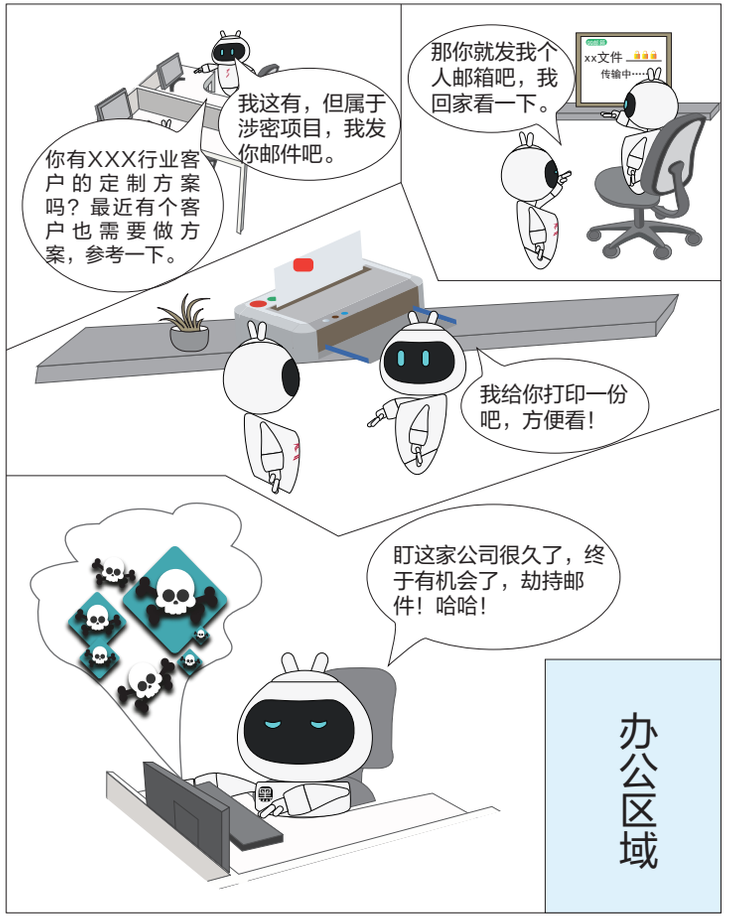
- **案例解析** 办公场所往往是安全事件迸发的根源，陌生人进入、同事信息等级知晓权限等，都会对事件产生根源性变化，纸质文件的应用与废弃一定要妥善，否则易造成资料丢失、信息泄漏等安全隐患。
- **安全建议** 1.离开座位时将纸质文件放在抽屉或文件夹等不易暴漏的位置
  2.内部纸质资料，使用完毕后要用碎纸机销毁
  3.在打印的过程中，不要离开，等待打印完成，及时带走文件

九 | 不明设备安全

九 | 不明设备安全

- 案例解析　不明来源的移动设备，容易携带病毒、木马，自从发现U盘autorun.inf漏洞之后，U盘病毒的数量与日俱增。U盘病毒并不是只存在于U盘上，中毒的电脑每个分区下面同样有U盘病毒，电脑和U盘交叉传播。
- 安全建议　1.点击U盘前，首先进行查杀
  2.关掉系统的自动播放功能
  3.一般建议插入U盘时，不要双击U盘，用右键点击U盘，选择“资源管理器”来打开U盘

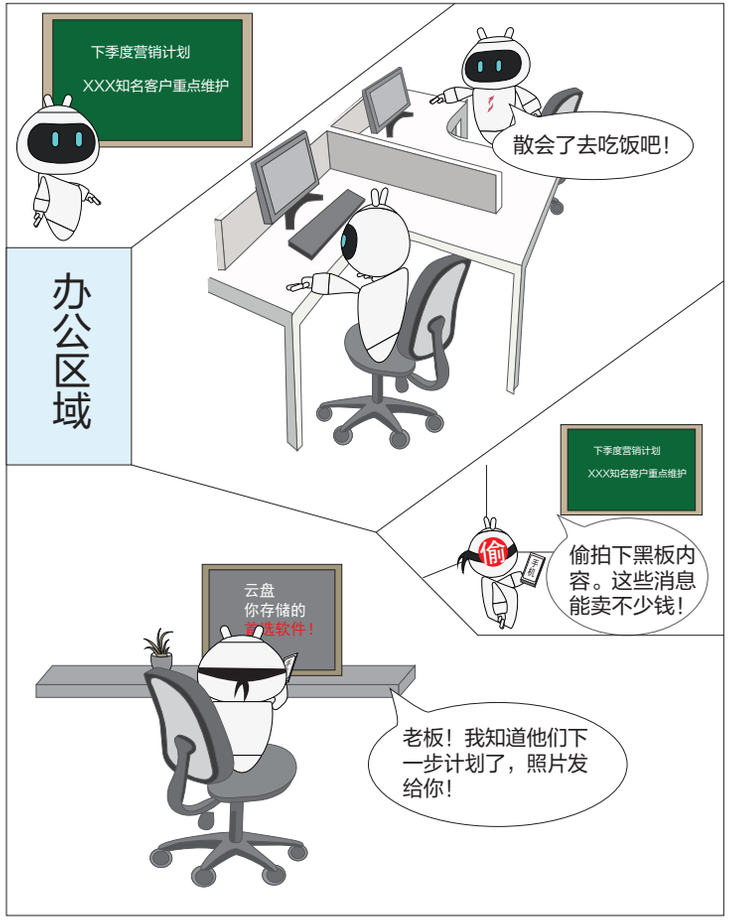
资料分级 | 十



十 | 资料安全

- 案例解析　文件对于企业、单位来说分为不同等级，不同人应该有不同的使用权限，与客户签订的项目或多或少包含有涉密部分，必须从技术、管理等多方面确保文件的安全性，纸质文档更要妥善处理，电子档避免直接暴露在公网上，给双方造成损失。
- 安全建议　1.禁止把涉密文档分享给未授权人员
  2.禁止把涉密文件裸露在办公桌上
  3.禁止通过非涉密网传输文档
  4.涉密文档禁止外部扫描

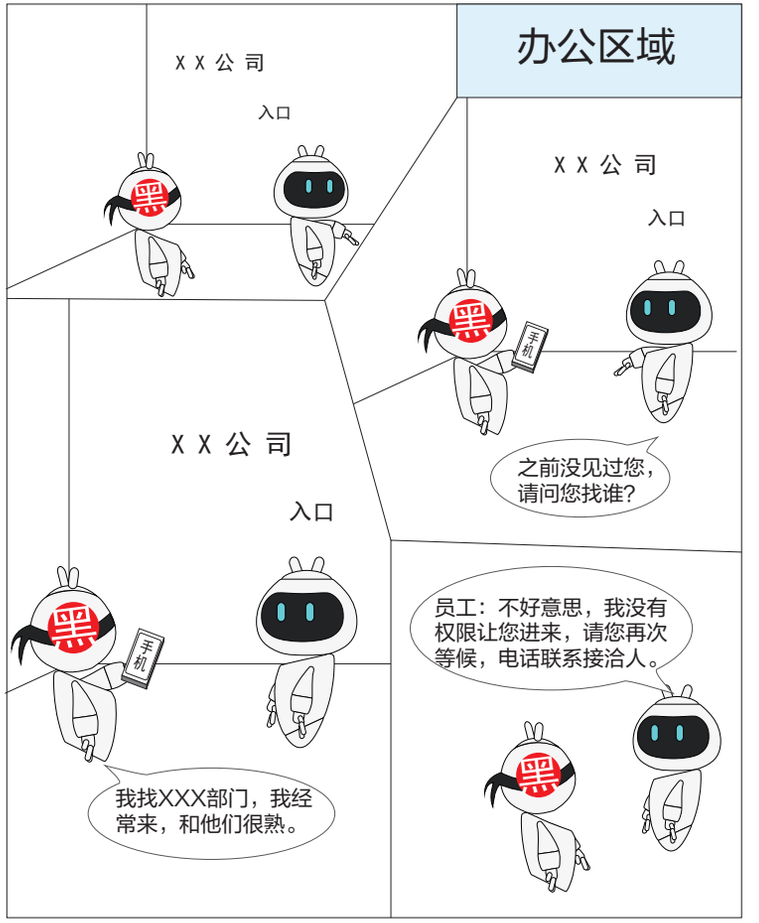
十一 | 会议安全



十一 | 会议安全

- 案例解析　会议进程中会经常用到黑板，记录、梳理主要论点、思路，还有一些核心数据等，在开会进程中，要保证会议场地的信息安全性，参会人员可靠性，知情权等级，稍有不慎则有可能被非授权人无意识听到、看到，并且有意识或无意识的传播。
- 安全建议　1.重要会议，选择隔音效果好的会议室
  2.会议期间拉紧窗帘或关闭门窗
  3.重要会议禁止拍照、录音等行为
  4.会后及时清理黑板，桌面文件，多媒体设备存档

访客安全 | 十二

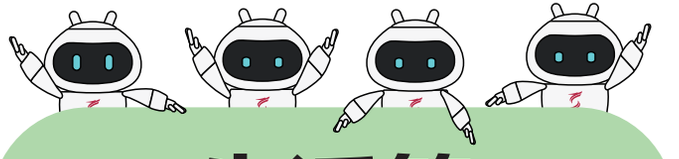


十二 | 访客安全

- 案例解析　乔装改扮是窃贼、商业间谍或黑客进行作案的重要方式之一，当您进入需要刷卡、指纹或受限工作区域时，要确保身后没人，或无权限的尾随者。当有陌生者尾随，可以礼貌应对。
- 安全建议　1.进出带有刷卡、指纹等门禁区域注意是否有尾随人员
  2.带外人进入后，需在前台登记，并全程陪同
  3.对于不能自动闭合的大门，进入后应确保大门闭合
  4.常见快递收发等事项，在门外进行

十三 | 邮件安全

- 案例解析　“邮件病毒”其实和普通的电脑病毒一样，只不过由于它们的传播途径主要是通过电子邮件，所以才被称为“邮件病毒”。“邮件病毒”主要是为了让用户的计算机感染病毒，或者是成为黑客手中的肉鸡。
- 安全建议　1.在收到信的时候，不管是不是认识的还是不认识的，附件一定先不要打开 2.看见带有附件的邮件，可以把附件下下来，然后用杀毒软件杀毒，如果还是怕中毒，你可以这样做。（1）打开我的电脑，在工具栏中找到工具选择文件夹选项，在弹出的对话框中选择查看这个选项，把“隐藏已知文件类型的扩展”前面的勾去掉。（2）在邮件的附件上右击 选择另存为，在要你重命名的时候在文件名的后面打上“*.txt”然后再杀毒。

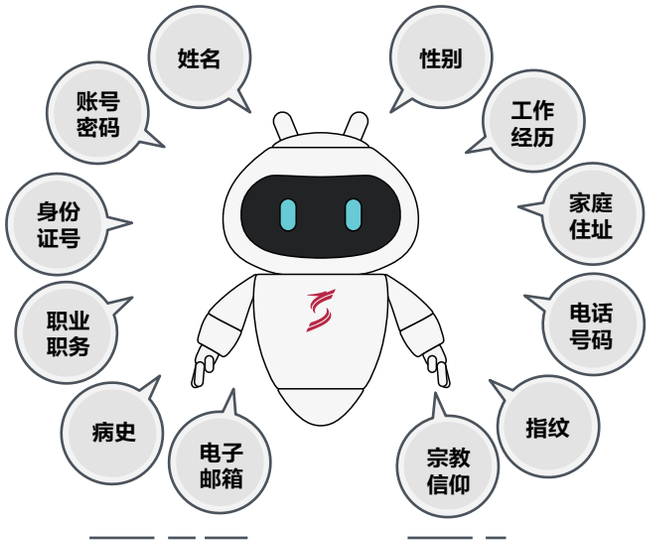


生活篇

一 | 个人信息安全

个人信息：

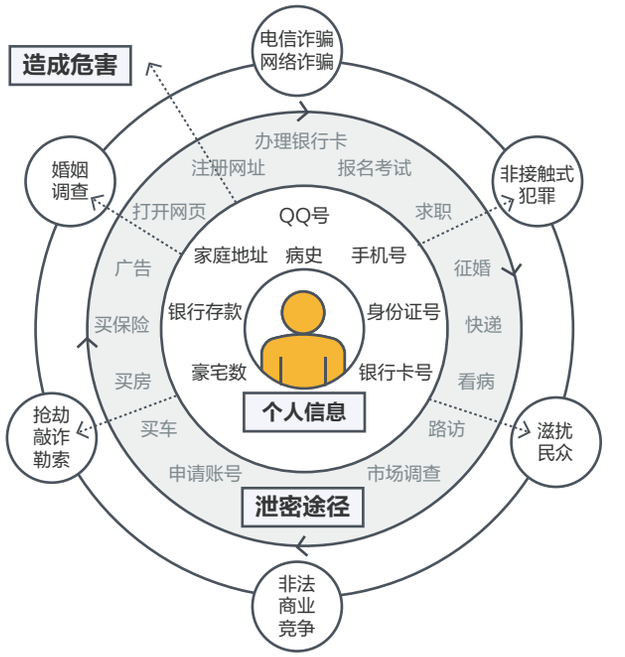
个人信息一般包括姓名、职业、职务、年龄、血型、婚姻状况、宗教信仰、学历、专业资格、工作经历、家庭住址、电话号码（手机用户的手机号码）、身份证号码、信用卡号码、指纹、病史、电子邮件、网上登录账号和密码等等。覆盖了人的心理、生理、智力，以及个体、社会、经济、文化、家庭等各个方面。



个人信息可以分为个人一般信息和个人敏感信息。

个人一般信息是指正常公开的普通信息，例如姓名、性别、年龄、爱好等。

个人敏感信息是指一旦遭泄露或修改，会对个人造成不良影响的个人信息。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。



泄密原因

个人：疏忽管理，过量提供，随意丢弃

企业：贩卖牟利，随意保存，内部员工非法泄密，超授权使用，未及时销毁

犯罪份子：黑客攻击，恶意电话和短信，网站钓鱼，病毒和木马，社会工程攻击

如何防范个人信息泄露?

1、培养安全意识，做到不主动透露个人信息，不被利益诱惑泄露个人信息；

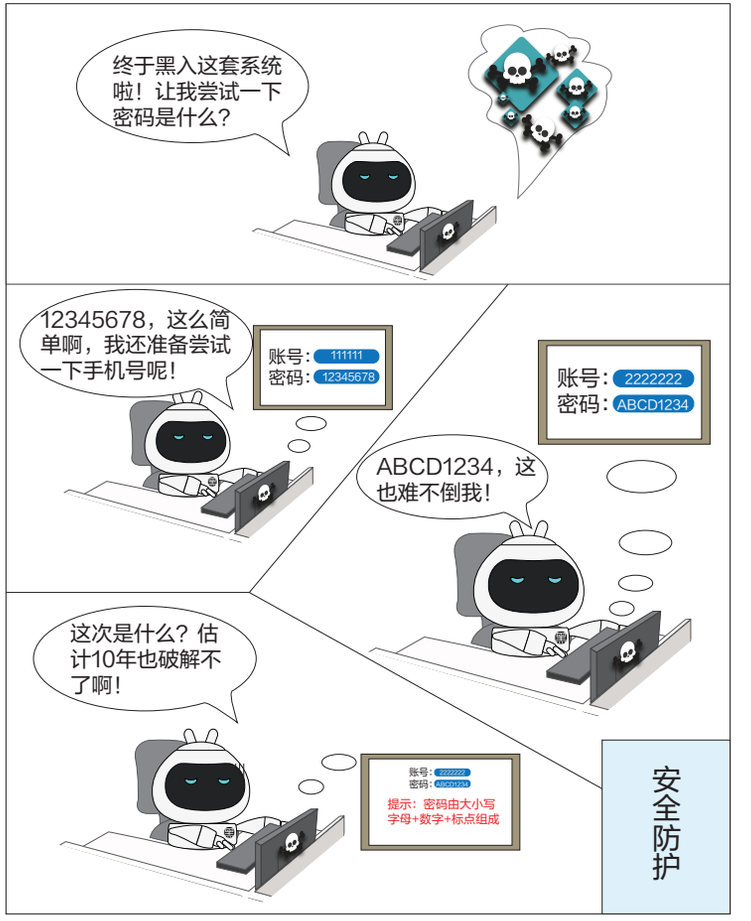
2、养成安全习惯，如密码设置、软件及时更新、软件授权、数据备份、不随意连接WiFi、勿见二维码就刷等；

3、善用法律维权，当发现个人信息泄露的确凿证据时，积极向监管单位进行举报。

二 | 密码等级安全

- 案例解析　我们日常接触到的计算机、手机开机密码、电子邮箱登陆密码、微信密码、QQ密码、银行卡支付密码，实际上是一种简单、初级的身份认证手段，是个人网络信息安全的一把钥匙，也是保护个人网络信息安全的第一步。
- 安全建议　1.不要把密码直接记录在纸质文件上
  2.对于不同重要程度的账号，设计相关联的联想密码
  3.在输入账号、密码时，留意身边不被他人看到

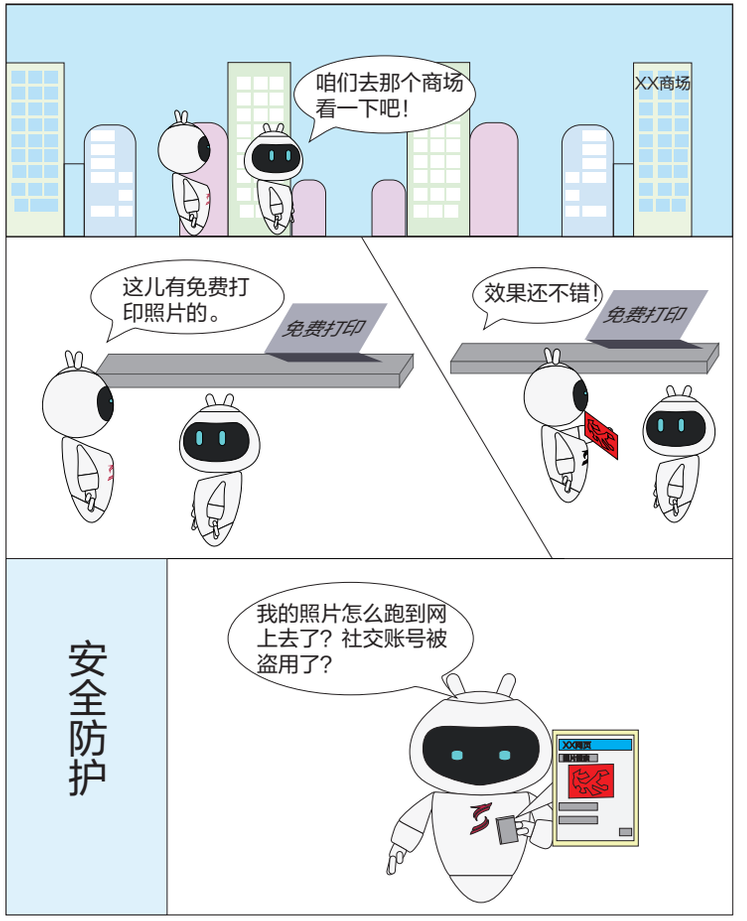
密码强度安全 | 三



三 | 密码强度安全

- 案例解析　黑客最常用的一个攻击方式，就是获取目标口令，有了对方的密码口令，将相当于有了你家的入户钥匙，常见的破译方式有：猜解简单口令、字典攻击、暴力穷举，对于高强度密码：遍历攻击、击键攻击、屏幕记录、网络嗅探器、网络钓鱼等方式。
- 安全建议　1.针对密码安全，首先在设置上包含大小写字母、数字和标点符号，位数在8位以上
  2.不能包含名字、生日、手机号、车牌号、门牌号等关联号码
  3.定期修改密码，不勾选网站或其他平台保存密码一键登录

四 | 二维码安全扫描



案例解析 照片是需要上传才能打印，那么问题来了，上传后的照片去哪里了呢？答案是，会一直存在电脑后台，只要管理员不“监守自盗”。所以事实是，的确存在着安全隐患。更大的隐患却是，在这种情境下，利用病毒二维码取代正规二维码引诱用户扫描的情况时有发生。

安全建议 1.避免扫描陌生二维码
2.在移动支付扫码前，看清二维码是否有伪造，重复贴码的痕迹，并与商家取得确认

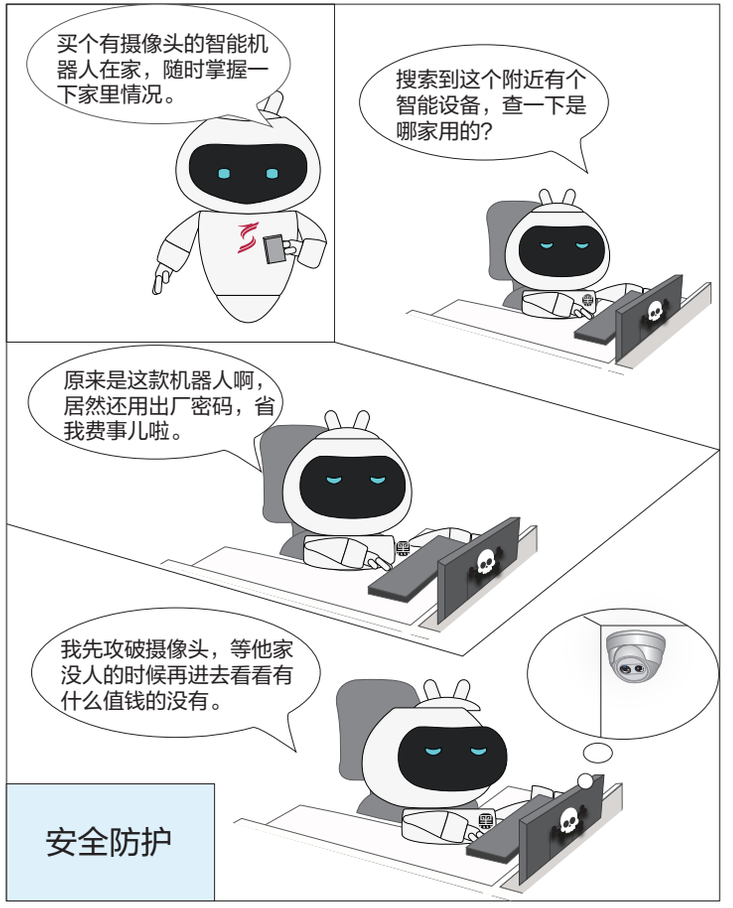
病毒处置方式 | 五

五 | 病毒处置方式

案例解析 在办公电脑应用的过程中，发现电脑运行缓慢、有窗口弹出，或者某些程序无法运行，后台无故运行大量程序，那么所应用的电脑很有可能已经中了病毒，要及时断网，联系公司技术人员处理，防止病毒扩散。

安全建议 1.在办公电脑应用过程中，一定要定期备份，避免文件丢失
2.在疑似电脑中毒时，立刻断网，防止病毒扩散
3.切勿隐瞒事件，掌握应急事件处置流程

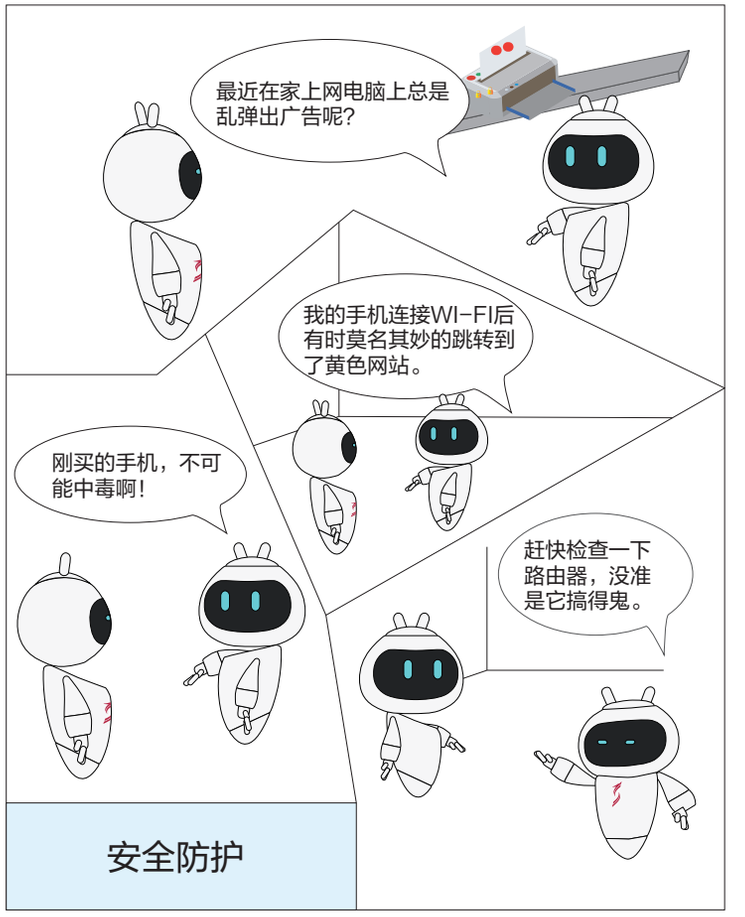
六 | 物联网设备安全使用



案例解析 物联网带来便利的同时，也给用户带来了受到网络攻击和身份盗用、隐私暴露等问题。网络犯罪分子可利社会工程学或系统漏洞和许多其他漏洞来远程访问设备并对设备或用户造成严重破坏。

安全建议
1.在心里上首先不抵触科技发展带来的便捷
2.在智能设备选择上，首先选择优质品牌
3.在应用中，关注补丁与升级公告，及时修改密码
4.定期测试在无操作情况下，设备是否异常运转

路由器安全 | 七

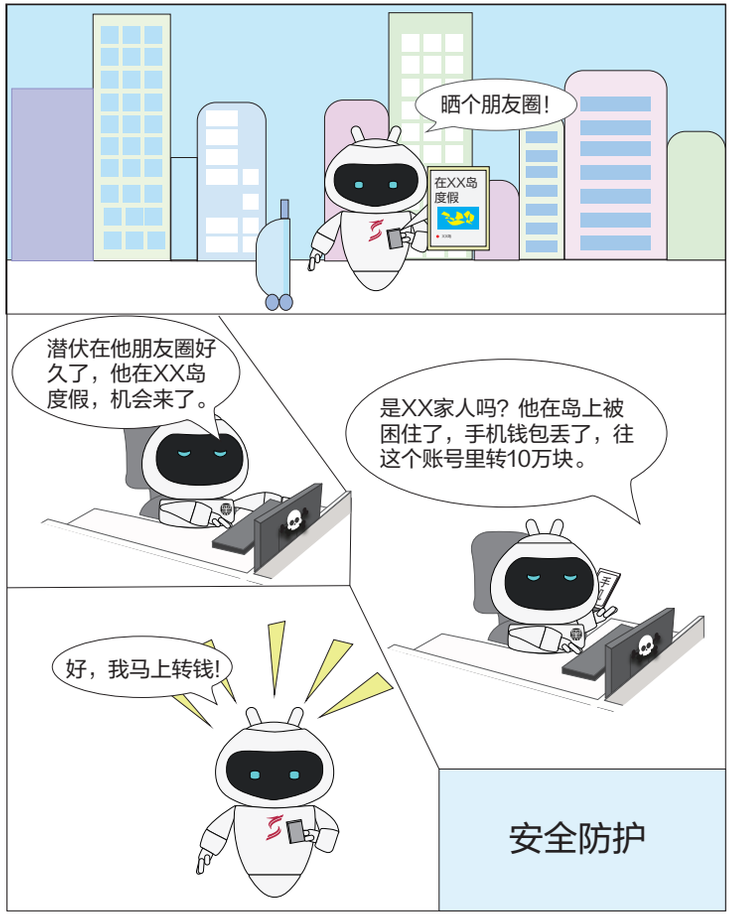


七 | 路由器安全

案例解析 2018年5月，美国联邦调查局发出警告称，俄罗斯计算机黑客已经入侵了数十万台家庭和办公室路由器，以收集用户信息或劫持网络流量。FBI敦促多个品牌路由器用户重启产品并更新固件。

安全建议
1.修改路由器登录名和密码
2.修改路由器默认的IP地址
3.安装杀毒软件

八 | 蓄意作案



案例解析 地理位置信息安全保护分为两个方面:第一，(LBS)基于位置的服务，可以在我们需要的时候提供帮助，比如导航等，但也可能成为坏人的入口；第二，地理位置也可能是我们自身疏忽暴露的，比如照片中有明显标识，蓄意作案的人，可以通过位置跟踪，或社会工程学来对您的家庭实施盗窃、诈骗等行为。

安全建议
1.社交软件中，对与好友认证提高防范意识，定期清理通讯录
2.在未完成行程时，不发布含有明显地理标识的照片或视频
3.手机应用过程中，注意关闭位置定位服务，应用时再打开

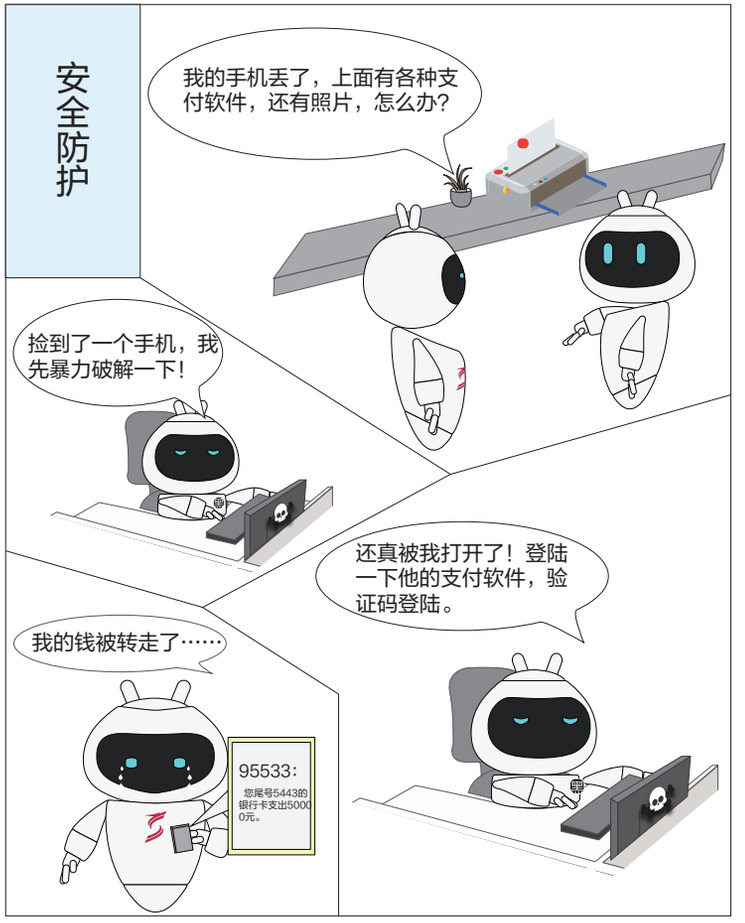
APP使用安全 | 九

九 | APP使用安全

案例解析 随着移动端用户群体的快速扩张，移动APP数量也呈现爆发式增长，移动APP的“脆弱性”也因此日益彰显，恶意扣费、个人隐私泄露、资金被盗等安全问题频频发生，令人堪忧。大量的APP安全事件中，主要是用户姓名、地址、账号、密码、手机号等信息泄露严重，尤其是游戏娱乐和生活服务类的APP是安全事件爆发的重灾区。

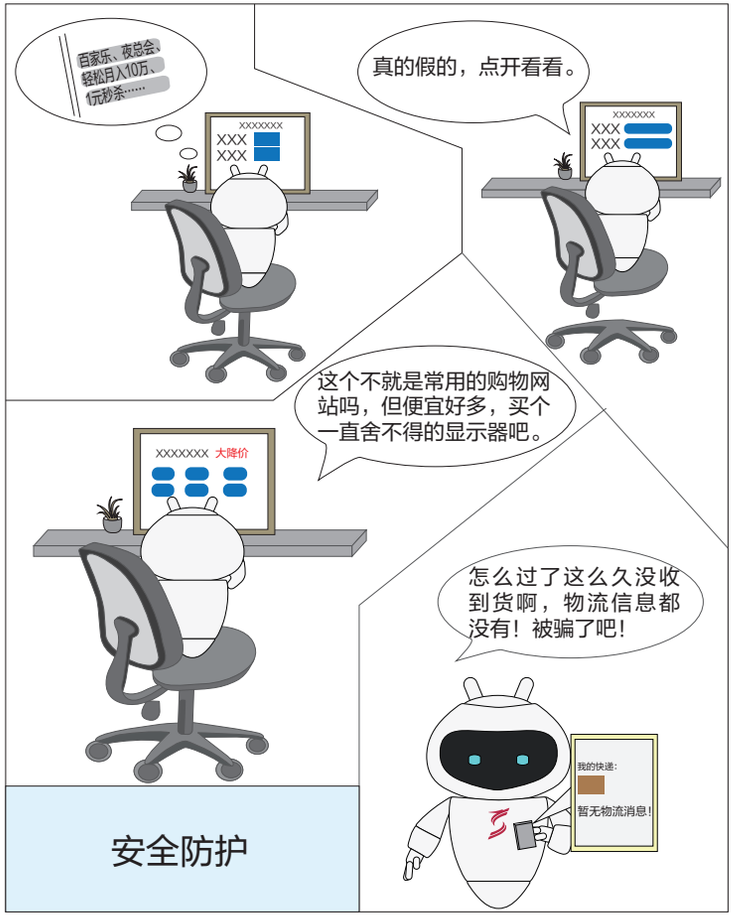
安全建议
1.在官网或指定应用商店下载APP
2.在选择同类型APP时选用星级较高的APP应用
3.关注APP升级与更新，谨慎“越狱”
4.忽略广告弹窗或不明二维码

十 | 手机丢失处理



- 案例解析　当丢失的手机落入不法分子手中，无法解锁手机时，会想尽办法得到或者修改你的密码，暴力破解不成，也会应用钓鱼链接等其他方式进行尝试。
- 安全建议　1.手机应用前提一定要设置开机密码、指纹识别、面部识别、远程锁定和擦除等功能
  2.丢失手机后，第一时间补办电话卡，让旧卡失效
  3.解绑原手机中社交账号、支付账号等核心应用
  4.告知家人朋友，避免上当
  5.收到邮件要谨慎，预防钓鱼事件

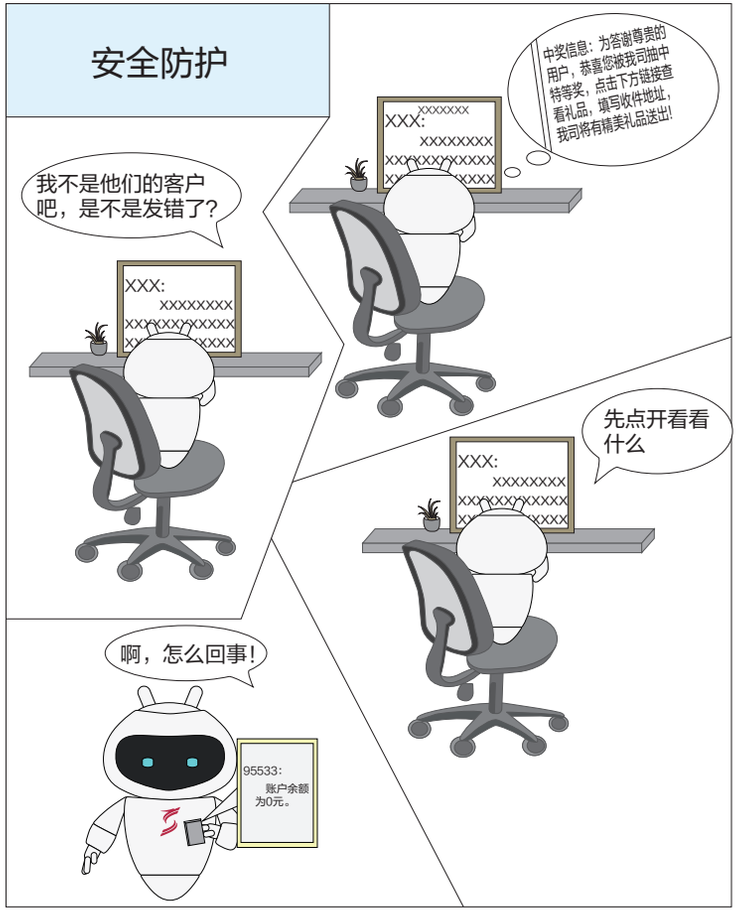
恶意链接 | 十一



十一 | 恶意链接

- 案例解析　恶意链接，单纯从外观上很难识别，比如说用0代替o，比如popa0.com 和 paopao.com，或者 popao.cm 之类的，或者如网址上的最后加个不易发现的字母，博彩、色情网站更是挂马、病毒的高发地。
- 安全建议　1.针对邮件或其他渠道所得的不明链接，不轻易点开
  2.针对不明付费网站认清识别，通过正规渠道购买
  3.在浏览器选择上采用非IE内核浏览器，漏洞相对较少

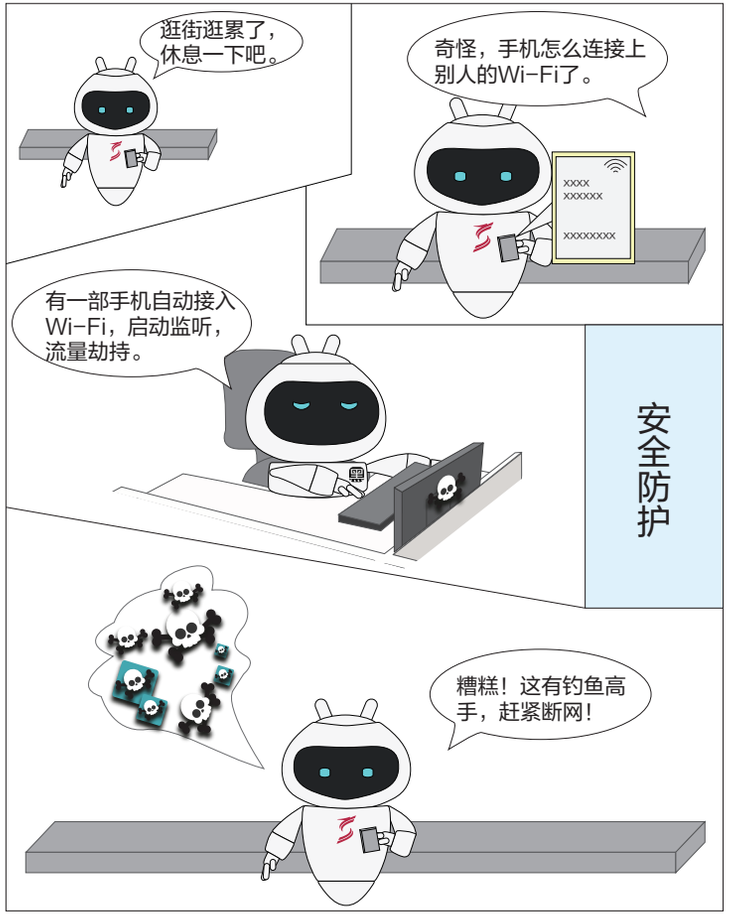
十二 | 电信诈骗



案例解析 电信诈骗不仅仅只有冒用他人身份一种诈骗手段，利用恶意链接与挂马页面，也是一种手段，手机中毒后，黑客通过监听、截获短信等方式，结合其他途径获取身份证、银行卡、支付账号进行盗刷、盗用。

安全建议 1.不要点击短信中的可疑链接
2.及时升级手机系统与应用软件
3.对疑似套取信息或金钱往来者进行身份核实

WI-FI安全 | 十三



十三 | WI-FI安全

案例解析 不法分子通常在机场、客运站、商场等公共场所搭建与场地名称相同的无密码WI-FI，吸引公众连接，然后再进行DNS劫持，进行钓鱼获取、监听等行为。

安全建议 1.不使用WI-FI时，关闭WI-FI避免自动连接
2.在公共场所使用移动支付时，使用4G网络，不要应用公共WI-FI
3.需要连接WI-FI时，与商家确认名称，发现异常及时断开

十四 | 电信诈骗预防

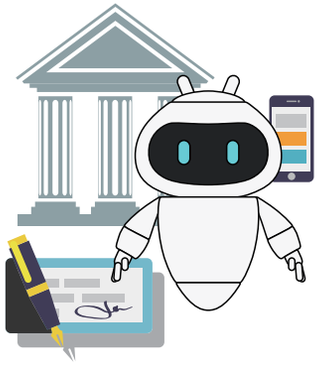
网络诈骗手段等多种多样，已经成为一条完整的违法产业链，网络诈骗的不法分子结成团伙作案，各环节互不认识但分工协作、勾联紧密的利益链条。

骗术大揭秘之一：

身份冒充

1、冒充公检法工作人员拨打电话，以身份信息被盗用、涉嫌洗钱、贩毒等理由，要求将钱转入到“安全账户”配合调查。

2、冒充公司领导，发出要求快速转帐汇款的指令等。



骗术大揭秘之二：

金钱诱惑

1、重金求子，引诱上当后，以检查费、诚意金等理由行骗。

2、高薪招聘，要求到指定地点面试，随后要求交培训费、服装费，甚至陷入传销团伙。

3、网络兼职，以打字员、刷单员为名义，要求缴纳信息费等。

骗术大揭秘之三：

有奖活动

1、发布集赞、转发有奖等虚假活动，要求提供姓名、电话、地址等信息，套取足够信息后要求缴纳保证金、个人所得税、快递费等。

2、以热播栏目节目组的名义发短信，称被选为幸运观众，有巨额奖品，后以个人所得税、快递费等借口要求转账汇款。

骗术大揭秘之四：消费退款

1、以系统卡单、故障、无货等理由，发来退款网址，此退款网址是钓鱼网站，若按要求填入信息，则支付宝、银行卡的钱会被快速转走。

2、群发假冒银行卡消费短信，后以境外大额消费涉嫌洗钱为由，套取个人信息及银行卡信息，通过第三方支付的快捷支付进行消费。

3、以机票改签等，诱骗进行汇款操作。

骗术大揭秘之五：恶意代码

1、利用伪基站群发网银系统升级、积分兑换等虚假链接，一旦点击后，手机便被植入盗取银行账号、密码、短信验证码的木马，从而实施犯罪。

2、以互联网公司的名义群发短信，包含钓鱼网站链接，进而获取账号密码等信息，转走账号中的资金。

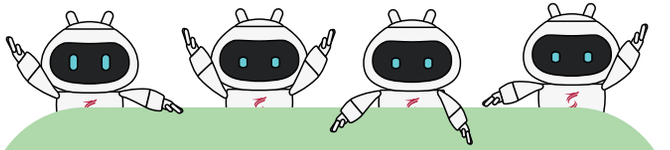
骗术大揭秘之六：其他骗术

1、在公共场所设置与正规WiFi类似的山寨免密WiFi，一旦连接上，通过截取数据传输，轻松获取手机上各类App的账号密码以及隐私。

2、骗子用受害者临时身份证办理补卡，同时用骚扰软件打电话发短信轰炸受害者手机，以掩盖补卡业务提醒短信。然后用补办的手机卡登录网银、第三方支付等平台，获取验证码盗取账户。

3、发布信用卡提额、低息贷款等广告，然后以验资、中介、手续费等名义要求转账。

4、发布虚假色情服务广告，待有人联系后，称需要先付款保证人身安全才能提供服务。



法律篇

法律知识

网络不是法外之地，有哪些需要了解的法律知识呢？

一、网上何种行为会被认定为寻衅滋事罪？

利用信息网络辱骂、恐吓他人，情节恶劣、破坏社会秩序的，依照刑法第二百九十三条第一款第（二）项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第(四)项的规定，以寻衅滋事罪定罪处罚。

二、网上何种行为会被认定为敲诈勒索罪？

以在信息网络上发布、删除等方式处理网络信息为由，威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

三、网上的哪些行为会被认定为捏造事实诽谤他人？

根据《刑法》第二百四十六条第一款规定，以下情况会被认定为捏造事实诽谤他人：

1.捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

2.将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

3.明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的，以“捏造事实诽谤他人”论。

情节严重的包括：

1. 同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的；

2.造成被害人或者其近亲属精神失常、自残、自杀等严重后果的；

3. 两年内曾因诽谤受过行政处罚，又诽谤他人的；

4. 其他情节严重的情形。

严重危害社会秩序和国家利益的包括：

1. 引发群体性事件的；

2. 引发公共秩序混乱的；

3. 引发民族、宗教冲突的；

4. 诽谤多人，造成恶劣社会影响的；

5. 损害国家形象，严重危害国家利益的；

6. 造成恶劣国际影响的；

7. 其他严重危害社会秩序和国家利益的情形。

四、网上何种行为会被认定为非法经营罪?

违反国家规定，以营利为目的，通过信息网络有偿提供删除信息服务，或者明知是虚假信息，通过信息网络有偿提供发布信息等服务，扰乱市场秩序，属于非法经营行为“情节严重”，依照刑法第二百二十五条第(四)项的规定，以非法经营罪定罪处罚。

五、明知他人利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪，为其提供资金、场所、技术支持等帮助的，会构成什么性质的犯罪?

以共同犯罪论处。

六、关于即时通信工具（如微信、腾讯 QQ 等）的公众信息服务有哪些管理规定?

国家互联网信息办公室2014年8月7日发布《即时通信工具公众信息服务发展管理暂行规定》，其中有以下几条：

第六条：即时通信工具服务提供者应当按照“后台实名、前台自愿”的原则，要求即时通信工具服务使用者通过真实身份信息认证后注册账号。即时通信工具服务使用者注册账号时，应当与即时通信工具服务提供者签订协议，承诺遵守法律法规、社会主义制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信息真实性等“七条底线”。

第八条：即时通信工具服务使用者从事公众信息服务活动，应当遵守相关法律法规。对违反协议约定的即时通信工具服务使用者，即时通信工具服务提供者应当视情节采取警示、限制发布、暂停更新直至关闭账号等措施，并保存有关记录，履行向有关主管部门报告义务。

当遇到安全事件时，可以向哪些专业机构求援?

类别	机构名称	网址
服务机构	国家互联网应急中心	www.cert.org.cn
	国家计算机病毒应急处理中心	http://www.cverc.org.cn
	中国信息安全测评中心	www.itsec.gov.cn
违法和不良信息举报	中国互联网举报中心	http://www.hsxcl.cn/12377/
	中国互联网协会反垃圾信息中心	www.12321.org.cn
	网络违法犯罪举报网站	www.cyberpolice.cn/wfjb
	网络不良与垃圾信息举报受理中心	www.12321.cn
	UTN统一信任网络	www.trustutn.org
	网络社会诚信网	www.zx110.org