安恒信息 DAS-security 安全中国

人人都是安全官 CYBERSECURITY MASTER

网络信息安全意识培训

演讲人

2020.07.08

www.dbappsecurity.com.cn

目录

Contents

Part01

信息安全意识是什么?

信息安全意识

信息安全意识就是能够认知可能存在的信息安全问题，预估信息安全事故对组织的危害，恪守正确的行为方式，并且在信息安全事故发生时采取的正确的应对措施。

Part02

为什么培训信息安全意识

信息安全意识

- 清楚可能面临的威胁和风险
- 建立信息安全的敏感意识和正确认识
- 遇到信息安全事件时采取正确的方式与方法
- 在日常工作中养成良好的安全习惯
- 遵守各项安全策略和制度

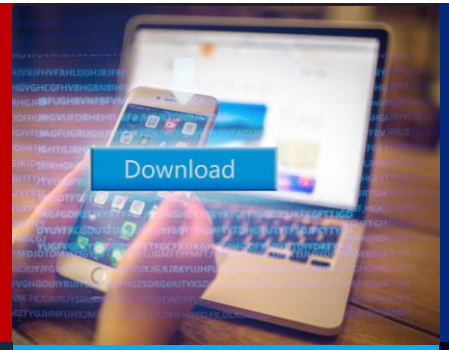
Part03

信息安全有什么

信息安全包含

电脑锁屏

纸质文件

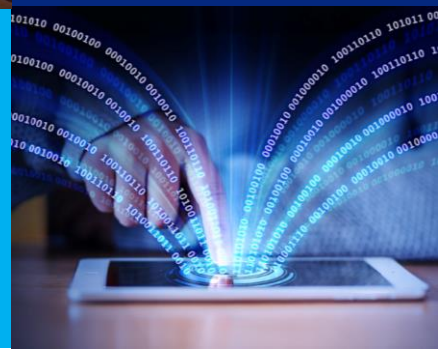


正版软件

计算机故障

出差旅途

手机通讯



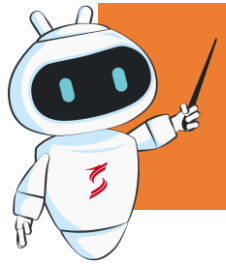
两方面进行网络信息安全意识培训

工作篇

生活篇

工作第一步：走进公司

大门，作为进入办公区域的第一道防线，可以有效的防范商业间谍或黑客进入后产生的物理风险。
然而，当有急事或注意力被转移的时候，会忘记关门或忘记确认身后是否有人尾随，随手关门习惯的养成能有效的将风险扼制在门外。

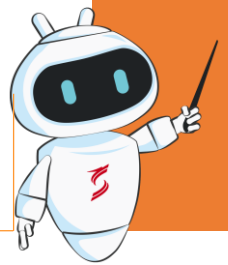


Tips

- ✓ **非自动闭合的大门应注意随手关门**
- ✓ **外部人员进入工作区需登记并全称陪同**

坐到工位

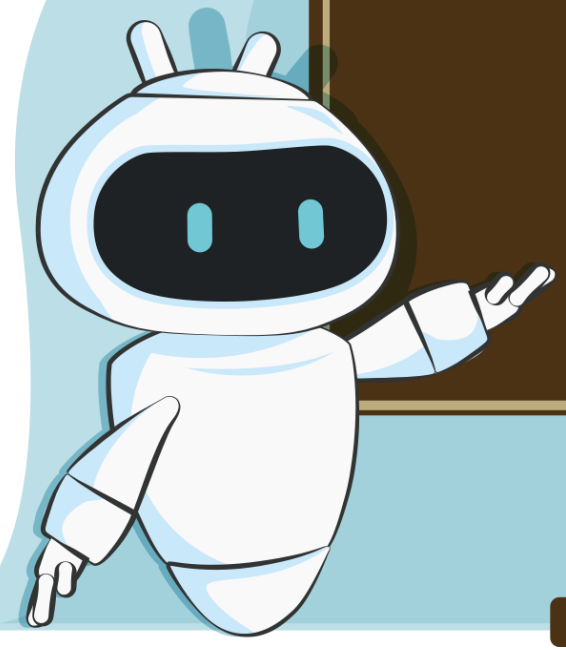
U盘，因其方便快捷的使用，被方便存储数据的同时，也成为了各种信息安全事件的高发地。
纸质文件不同于电子设备，但也会涉及到信息安全的泄露。



Tips

- ✓ 使用过的U盘应妥善存放，避免资料的泄露和病毒木马的植入
- ✓ 禁止随意放置或丢弃含有敏感信息的纸质文件
- ✓ 复印或打印的文件及时取走，避免信息泄露
- ✓ 离开工位时，含有机密信息的资料锁入柜中，并对计算机进行锁屏

安全小贴士



工作环境与物理安全

- 工位，是一天中在公司停留时间最长的位置，也是最容易发生信息事故的位置。未锁屏的电脑、没放好的U盘、摊开放的笔记本、准备报销的发票、刚打印的业务文件...

- 信息泄露威胁无处不在，信息安全防护也不单指电子设备，物理环境也同样需要引起重视，提高安全防范意识。

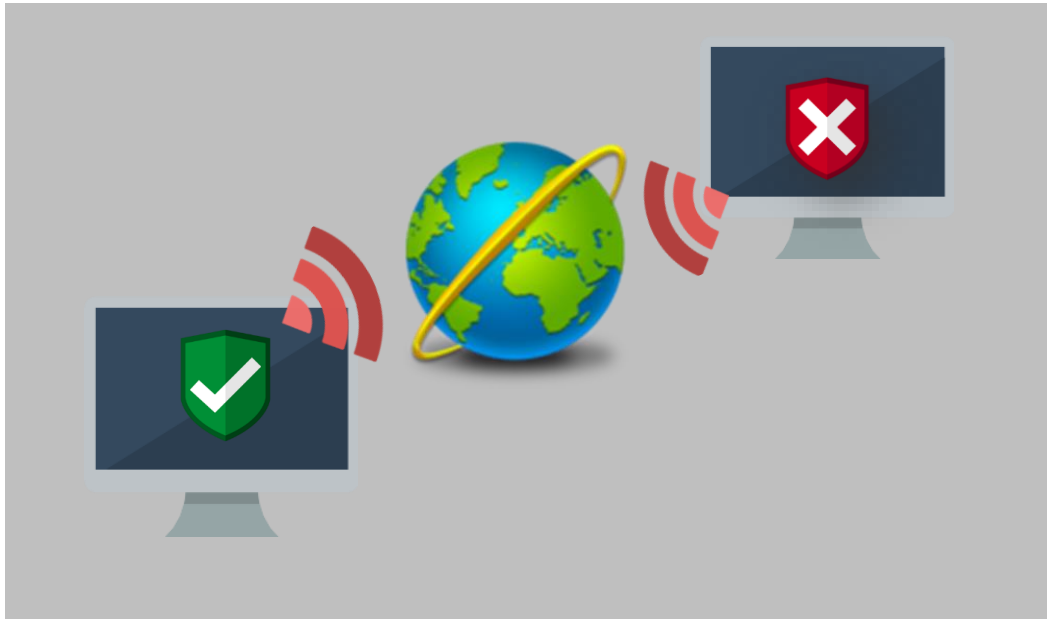
工作篇

计算机：系统和软件

互联网作为第五大媒体已经越来越多的融入人民的生产生活中，2020年以来，工作、教育对于网络的依赖性更强，网络带来的信息安全风险也不容小觑。

Tips

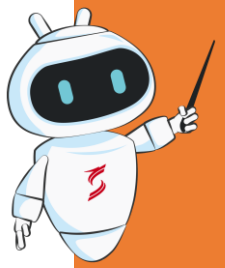
- ✓ 应安装杀毒软件，随时打开防火墙
- ✓ 尽量使用官方渠道下载的正版软件或系统
- ✓ 及时检查系统更新
- ✓ 不私自安装不明程序，不随意打开莫名软件、文件或链接



工作篇

Wi-Fi连接

Wi-Fi信号具有一定覆盖范围，机场、餐厅等公共场所通常都部署了免费Wi-Fi，免费热点在帮助人们节省流量费用、提高网络速度的同时，也存在着信息泄露、流量挟持、密码破解等风险。

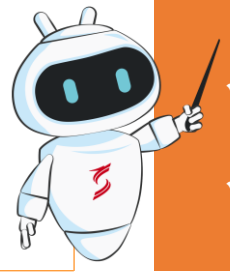


Tips

- ✓ 公共场合连接Wi-Fi，要注意周边提示，接入官方网络
- ✓ 处理敏感信息或进行移动支付时，尽量不连接公共网络，而使用4G/5G
- ✓ 在办公区域，不自行搭建Wi-Fi热点，不使用密码共享类APP

数据删除与恢复

在进行文件删除和磁盘清空时，如果仅清空回收站，或者仅使用“快速格式化”功能，由于磁盘上的数据并没有彻底清除和覆盖，黑客还可以使用专业工具将其进行恢复。

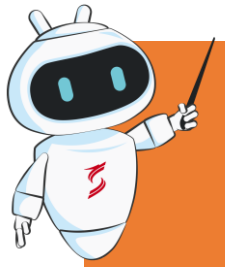


Tips

- ✓ 养成定期备份数据的习惯删除单个敏感文件时，使用杀毒软件自带的“文件粉碎”功能
- ✓ 保密性要求较高的数据在备份时设定完善的访问控制机制并存放在安全的地方
- ✓ 谨慎使用各大云平台自动备份功能，不要上传敏感数据

云储存安全使用

云储存作为互联网最常使用的存储工具，有存储、读取、下载等服务，存储量大，应用简便，是大众喜爱的存储方式，也成为了黑客攻击的首选目标。密码破译、Wi-Fi钓鱼以及云盘本身的漏洞，都是“技术贼”攻击的入口。



Tips

- ✓ 云储存应用过程中设定时间维度，并及时清理文件
- ✓ 不与他人共享使用，不存储机密、敏感文件
- ✓ 移动端使用时关闭自动备份功能

邮件安全

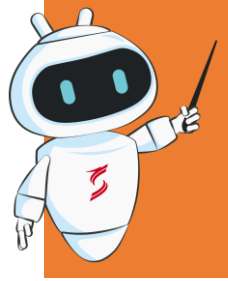
电子邮件作为一种通信手段，其重要性和防护日益增加的同时安全问题也逐渐增多。假冒攻击、账号泄露、流量监测、勒索病毒、钓鱼邮件，针对邮件的攻击手段让人防不胜防。

Tips

- ✓ 收发邮件过程中，应确保传输通道加密
- ✓ 收到邮件时，核对发件人信息是否正确，并通过其他渠道再和发件人本人确认
- ✓ 收到可疑邮件时，绝对不要打开任何未知文件类型的邮件附件
- ✓ 手机丢失时，谨防邮箱内收到的“查找手机位置”的邮件

日常不可少：会议安全

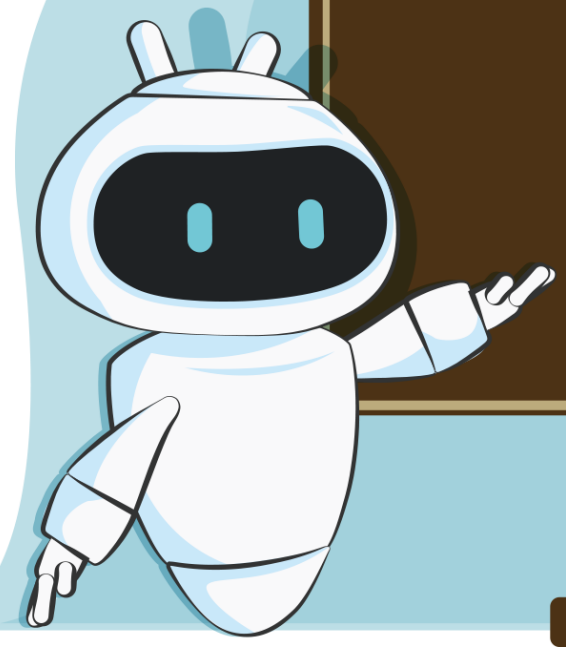
会议召开时，组织者应确认在场参会人员，特别是在进行人数较多的大型会议时。会议中会使用到梳理、重点、思路、核心数据等，要确保场地的安全性、参会人员的可靠性、知情等级，以确保会议信息不被泄露。



Tips

- ✓ 会议组织者现场确认参会人员身份
- ✓ 召开重要会议时，选择隔音封闭的会议室，并检查是否存在窃听、摄像头等设备
- ✓ 会后及时整理会场，确保不遗留资料

安全小贴士

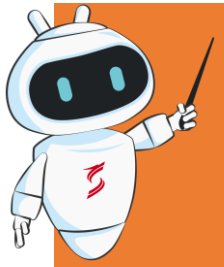


安全会议≠会议安全

- 会议安全是一件很复杂的事，不止包含秩序、财产、出行、饮食，也有数据安全。外部人员的加入、重要资料的遗留、会后公开的讨论都会带来安全风险。
- 安全会议是保证会议顺利进行的前提，会议安全是保障公司数据的重点。

外出办公

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。

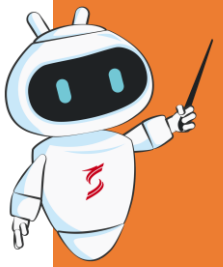


Tips

- ✓ 公司内部资料建立内部服务器资源
- ✓ 建立VPN系统，无论员工出差或是在家都能时刻访问内网资源

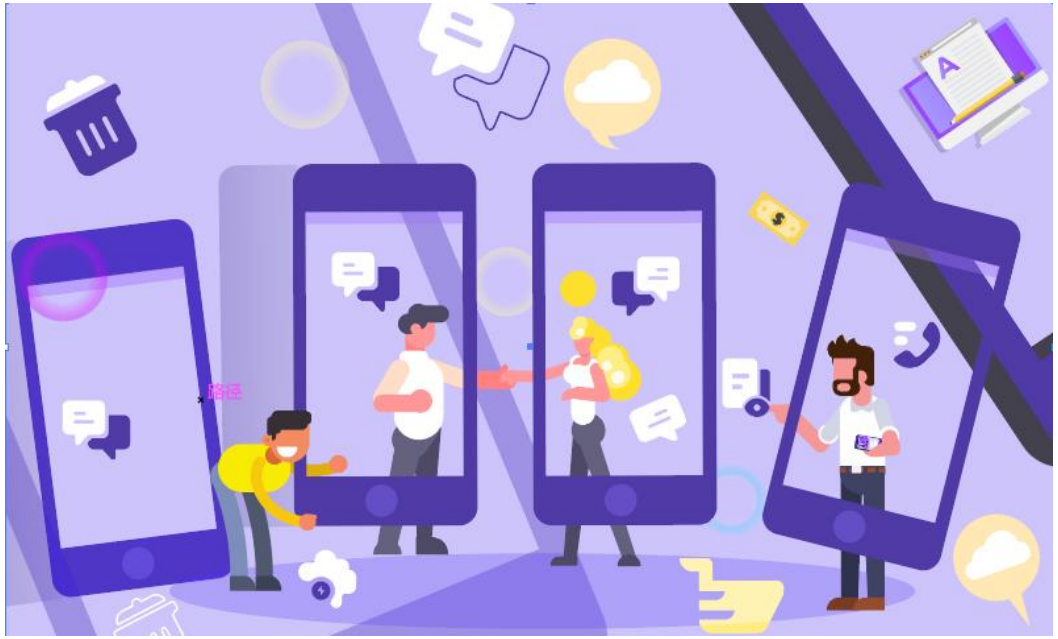
移动通讯安全

移动通讯工具相较台式机、笔记本等有便携常用的特点，智能手机、APP的普及也给工作沟通带来方便的同时，也加大了信息安全、隐私数据泄露的风险。越来越多的黑客专门针对移动通讯工具研究漏洞并窃取数据。



Tips

- ✓ 工作沟通的工具和日常社交的工具区分开
- ✓ 手机中安装移动安全软件，进行骚扰拦截，防范短信电话的诈骗风险
- ✓ 针对重要的平台，开启双因素认证，可绑定常用的手机邮箱
- ✓ APP的权限根据需要进行开通



两方面进行信息安全意识培训

工作篇

生活篇

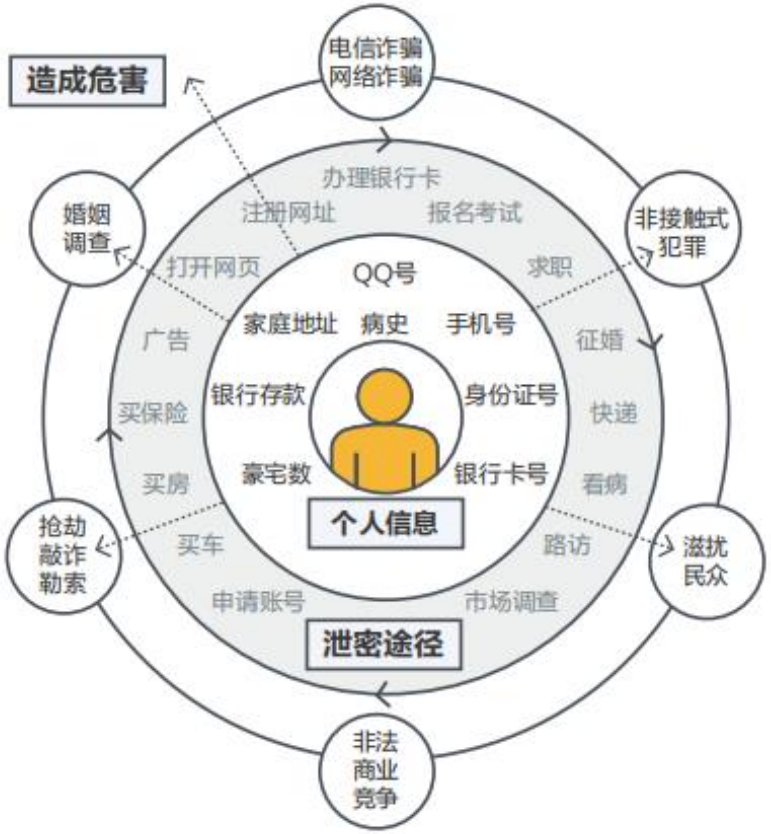
生活篇

个人隐私

各种软件APP的注册登录对个人信息的使用，使得个人隐私信息已经成为信息产业中重要的生产资料。广告投放，定向金融服务，保险，很多厂商都根据收集到的个人信息定向销售各类产品。但是个人信息的泄露，也让不法分子有了可乘之机。

- 扩充了不法分子的密码字典
- 冒充别人注册各类网上银行账号
- 利用网站找回密码机制，修改泄露信息人的账号密码
- 贩卖信息人的敏感信息以牟利

生活篇

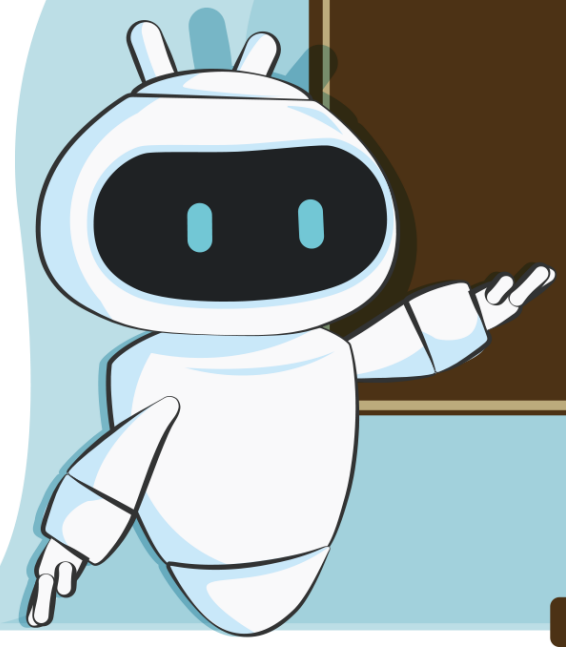


培养安全意识，做到不主动透露个人信息，不被利益诱惑泄露个人信息；

养成安全习惯，如密码设置、软件及时更新、数据备份、不随意连接wifi、不随意扫描二维码；

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。

安全小贴士



测一测

你的网络安全指数

个人信息安全十问

生活篇

密码安全

我们日常接触到的计算机、手机开机密码、邮箱登陆密码、微信密码、支付密码等，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。

- 单一的字符类型，并少于8位
- 最常被人使用的弱口令，如123456
- 包含名字、生日、手机号等关联密码
- 所有系统都使用相同的用户名和口令

生活篇

!@#$%^&*(	口令由大小写字母、数字、特殊字符的混合体，至少8个字符
password	不使用名字、生日等个人信息和字典单词
	不直接把密码记录在纸质文件上
marry820312	在输入账号、密码时，留意不被身边其他人看到
xEc@ser92%	定期修改密码，不勾选网站或其他平台的保存密码和一键登录

生活篇

二维码扫描

扫码登记、扫码查询、扫码支付，2020年对二维码应用掀起了一波热潮，也让不发分子看到了可乘之机。二维码的安全隐患问题日趋突出。

- 病毒二维码取代正规二维码
- 二维码被伪造，重复贴码等
- 二维码扫描及信息填写没有必要

生活篇

- 不随意扫描陌生二维码
- 扫码前确认二维码的来源正规，渠道官方
- 在移动终端安装杀毒软件等相应的防护程序，及时提醒有害信息并删除。

生活篇

APP权限

为了保证安全性，在安装和首次打开APP的过程中，通常会弹出提示要求用户授予权限。但是，APP需要的是否是全部的权限，被开通的权限是否会有未经同意擅自泄露信息、擅自发送短信的风险，这些是生活中常见的问题，也是目前亟需解决的问题。

- 获取通讯录数据并发送短信等
- 擅自录音
- 访问好友信息进行广告推送

生活篇

- 应用程序安装或首次打开时，认真阅读APP要求的权限，仅授予必要的权限
- 慎用换脸软件、或其他上传个人隐私信息的APP软件
- 后续使用过程中，如果发现有未打开的权限，可通过设置中权限管理手动授权
- APP或小程序的详情页面，通常可以看到当前被授予的权限，其中敏感权限可进行手动关闭

生活篇

物联网设备

物联网带来便利的同时，也给用户带来了网络攻击和身份盗用、隐私暴露等问题。网络犯罪分子可利用社会工程学或系统漏洞来远程访问设备或对用户使用造成严重破坏。

掏出手机与家中的智能设备相连：

- 在夏天提前打开空调，在冬天提前打开加湿器
- 使用摄像头实时查看家里的情况
- 远程打开扫地机器人，清扫环境

生活篇

方便亦是威胁

在智能设备的选择上，优先选择优质高端品牌；

在应用中，关注补丁与升级公告，及时修改密码；

定期测试在无操作的情况下，设备是否运转；

建议使用安恒物联网安全心！

- 《什么鬼！正充电的手机，自动订了万元总统套房》
- 《网络监控有漏洞，家庭摄像机“全曝光”隐私》

安全小贴士

社会工程学

社会工程学是一种通过对目标人心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段取得自身利益的手法。

社会工程学陷阱就是通常以交谈、欺骗、假冒或口语等方式，从合法用户中套取用户系统的秘密,社会工程学需要搜集大量的信息针对对方的实际情况，进行心理战术的一种手法。

社会工程学是一种黑客攻击方法，利用欺骗等手段骗取对方信任，获取机密情报。国内的社会工程学通常和人肉搜索进行联系起来，但实际上人肉搜索并不等于社会工程学。总体上来说，社会工程学就是使人们顺从你的意愿、满足你的欲望的一门艺术与学问

生活篇

地理位置信息

地理位置信息安全的泄露主要包含两个方面

（LBS）基于位置的服务

可以在我们需要的时候提供帮助，但也可能成为坏人的入口；

自身疏忽

朋友圈视频中明显的位置标识，蓄意作案的人可能根据位置跟踪，或社会工程学对亲属实施盗窃欺诈的行为。

生活篇

- 手机应用过程中，注意关闭位置定位服务，需要时再打开
- 在未完成的行程时，不发布含有明显地理标识的照片或视频
- 社交软件中，对好友认证提高防范意识，定期整理通讯录

生活篇

手机丢失

手机，作为日常使用频率最高的生活工具，也大大的增加了丢失以及丢失后被盗用信息的可能。

当丢失的手机落入不发分子手中，他们会想尽办法的得到甚至修改开机密码，暴力破解不成，也会应用其他钓鱼链接等其他方式进行尝试。

生活篇

- ✓ 设置开机密码
- ✓ 指纹识别
- ✓ 面部识别
- ✓ 远程锁定和擦除等功能

- ✓ 第一时间补办电话卡

- ✓ 解绑原手机中社交账号、支付账号等核心应用

- ✓ 告知家人朋友，避免上当受骗

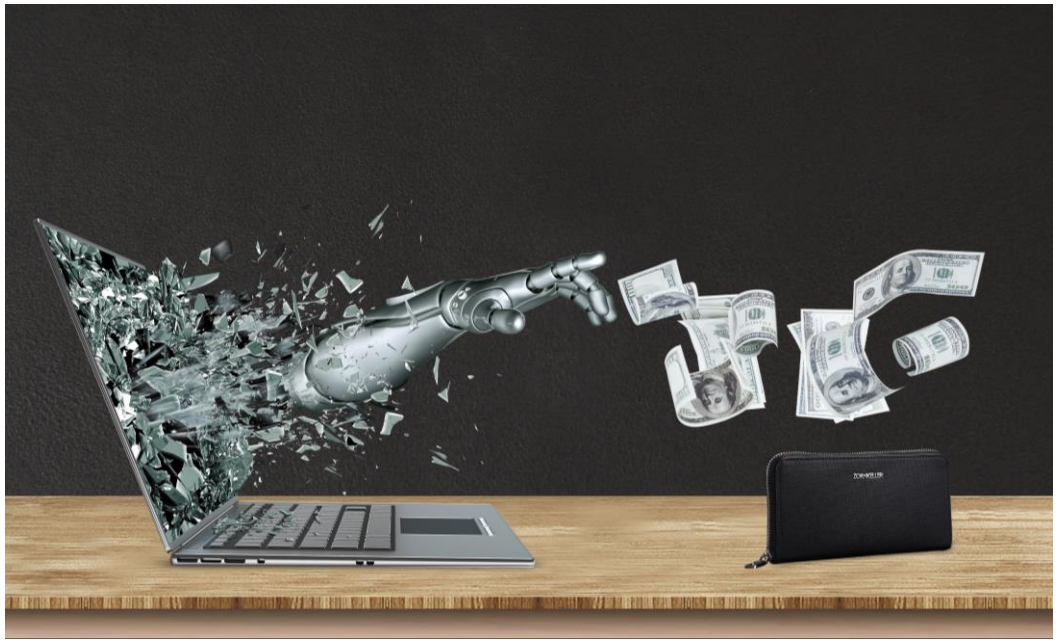
- ✓ 收到手机找回的邮件要谨慎，预防钓鱼邮件

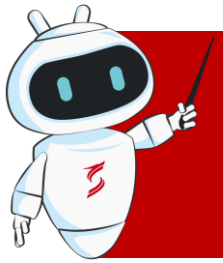
生活篇

电信诈骗

网络诈骗的手段多种多样，其中电信诈骗是应用最多的诈骗手段。

电信诈骗不仅有冒用他人身份这一种诈骗手段、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，结合其他途径获得的身份证、银行卡、支付账号进行盗刷盗用。





Tips

- ✓ 不要点击短信中的可疑链接
- ✓ 及时升级手机系统与应用软件
- ✓ 对疑似套取信息或金钱往来者进行身份核验

安全小贴士

网络诈骗的手段多种多样，已经形成了一条完整的违法产业链。网络诈骗的不发分子结成团伙作案，各环节互不认识但分工写作、勾连紧密

身份冒充

金钱诱惑

有奖活动

消费退款

安全小贴士

扫码走进官网，答案等你揭晓

Part04

做什么保护网络信息安全

- 使用容易猜测的口令，或者根本不设口令
- 将密码写在便签上，贴在计算机旁提醒
- 开着计算机离开，就像离开家却忘记关灯那样
- 轻易相信来自陌生人的邮件，并好奇的打开邮件附件
- 在系统更新和安装补丁上总是行动迟缓
- 重要资料未正确销毁，随意丢弃在垃圾桶里
- 只关注外来的威胁，忽视企业内部人员的问题
- 事不关己高高挂起，不报告安全事件
- 口无遮拦，上当受骗，泄漏敏感信息

信息安全培训须知

- ✓ 遵守法律法规和安全策略
- ✓ 公司资源只供公司所用
- ✓ 保守口令秘密
- ✓ 谨慎使用Internet、EMAIL、QQ
- ✓ 加强人员安全管理
- ✓ 识别并控制第三方风险
- ✓ 加强防病毒措施
- ✓ 留意物理安全
- ✓ 加强对敏感信息的保密
- ✓ 控制自己的好奇心
- ✓ 牢记天上不会掉馅饼
- ✓ 有问题及时报告

安全意识
无论是对个人还是组织都是一笔宝贵的财富

安恒信息 DAS-security 安全中国

人人都是安全官 CYBERSECURITY MASTER

谢谢观看

Thank you

www.dbappsecurity.com.cn