

网络安全管理知识培训

课程目标

通过本课程的学习，学员可以加强对信息安全的认识程度，了解常见的安全技术和控制措施，最重要的，能够极大的提升学员的信息安全意识。本课程的目的是使学员理解信息安全是和每个人都息息相关，信息安全的和管理和技术控制措施有效性，极大的依赖员工的信息安全意识水平。

课程内容：

一、网络安全形势态势分析

- 国内外近期网络安全大事件
- 微软 XP、Win7 事件拷问中国网络安全
- 斯诺登引发全球网络空间安全思考
- “华为中兴事件”到“斯诺登”的顿悟
- 互联网星系图上的三个世界
- 中央网信小组应对全球复杂时局
- 信息安全要素
- 信息安全法律法规

二、网络安全法律体系建设

- 计算机犯罪
- 我国立法体系
- 网络安全相关法规解读
- 关键信息基础设施安全保护条例解读
- 数据安全法解读
- 个人信息保护条例解读
- 国家网络安全政策
- 我国信息安全标准介绍

三、国家攻防演习介绍

- 案例讲解-攻防对抗的思路（参考公安部护网行动思路）
- 安全防护思路及主要工作
- 防护清理
- 防护加固

四、密码安全

- 密码的重要性
- 密码的常见问题
- 使用密码的安全习惯
- 【演示】Windows 密码的快速破解
- 如何设置安全的密码
- 企业密码安全策略的意义

五、上网安全防护

- 如何安全地下载程序
- 公共区域上网的安全隐患
- 网络行为的安全

- 避免使用与公司有关的信息（如邮箱，账户/密码）提交注册信息
- 【演示】渗透攻击中的情报收集

六、正确地安装安全防护软件

- 安装防病毒软件
- 安装个人主机网络防火墙
- 安装终端安全软件
- 如何保持安全软件的有效
- 使用安全软件保障电脑的安全
- 正确的补丁下载与选择安装
- 【演示】消除令人讨厌的弹窗广告

七、邮件安全

- 邮件可能产生的安全问题
- 如何正确地收发邮件
- 安全处理邮件正文的内容
- 正确处理邮件的附件 – 防范勒索病毒
- 正确处理钓鱼邮件 – 钓鱼邮件的识别和防范
- 邮件地址的安全防护
- 正确处理个人邮件与工作邮件
- 【案例】入侵希拉里——美国大选中的黑客战争

八、正确处理计算机病毒

- 病毒的危害
- 感染病毒的一些不良习惯
- 及时有效地处理计算机中毒状况
- 如何有序地清除病毒
- 【案例】最新勒索病毒的肆虐

九、如何应对木马和后门

- 木马后门与病毒的区别
- 木马后门的危害
- 区别对待木马与病毒
- 检查网络流量
- 如何有序地处理感染木马的计算机
- 【演示】使用木马控制电脑

十、安全使用移动存储介质

- 移动存储使用中可能存在的安全隐患
- 如何正确地使用移动存储设备
- 移动存储设备免疫常见病毒的方法
- 正确的使用移动存储设备的习惯

十一、数据安全保护与备份

- 个人电脑的数据备份
- 使用加密软件 PGP 进行文件加密
- 使用 WinRar 等压缩软件进行文件加密
- 如何安全删除数据
- 【案例】PGP 加密软件如何更好地保护数据-----加密和备份自己的重要数据
- 【演示】常见的办公文件加密与破解

十二、社会工程学攻击与防范

- 什么是社会工程学攻击
- 社会工程攻击的形式
- 社会工程攻击的案例
- 【案例演示】社会工程攻击的防范

十三、未来网络安全技术发展趋势

- 云安全
- 数据安全
- 5G 安全
- 零信任安全
- 信创安全