

信息安全意识培训

上海极道云计算科技有限公司



极道科技

一、信息安全概念及当前趋势

二、常见的漏洞攻击手段与安全隐患

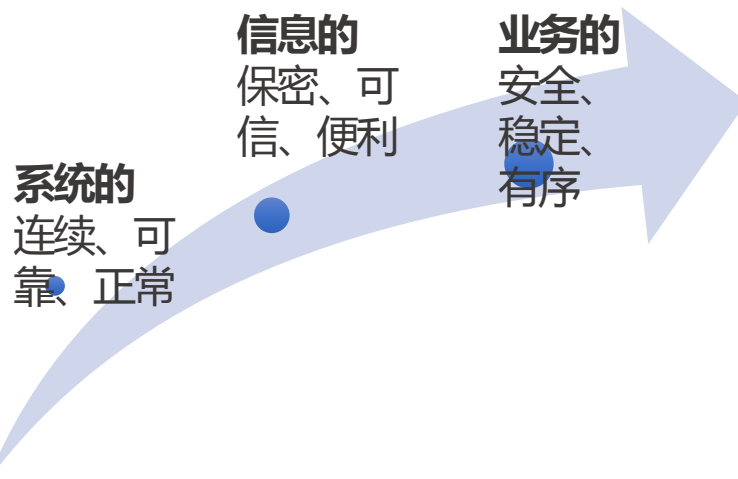
三、日常工作中的规范建议与防范意识



极道科技

一、信息安全基本概念：什么是信息安全

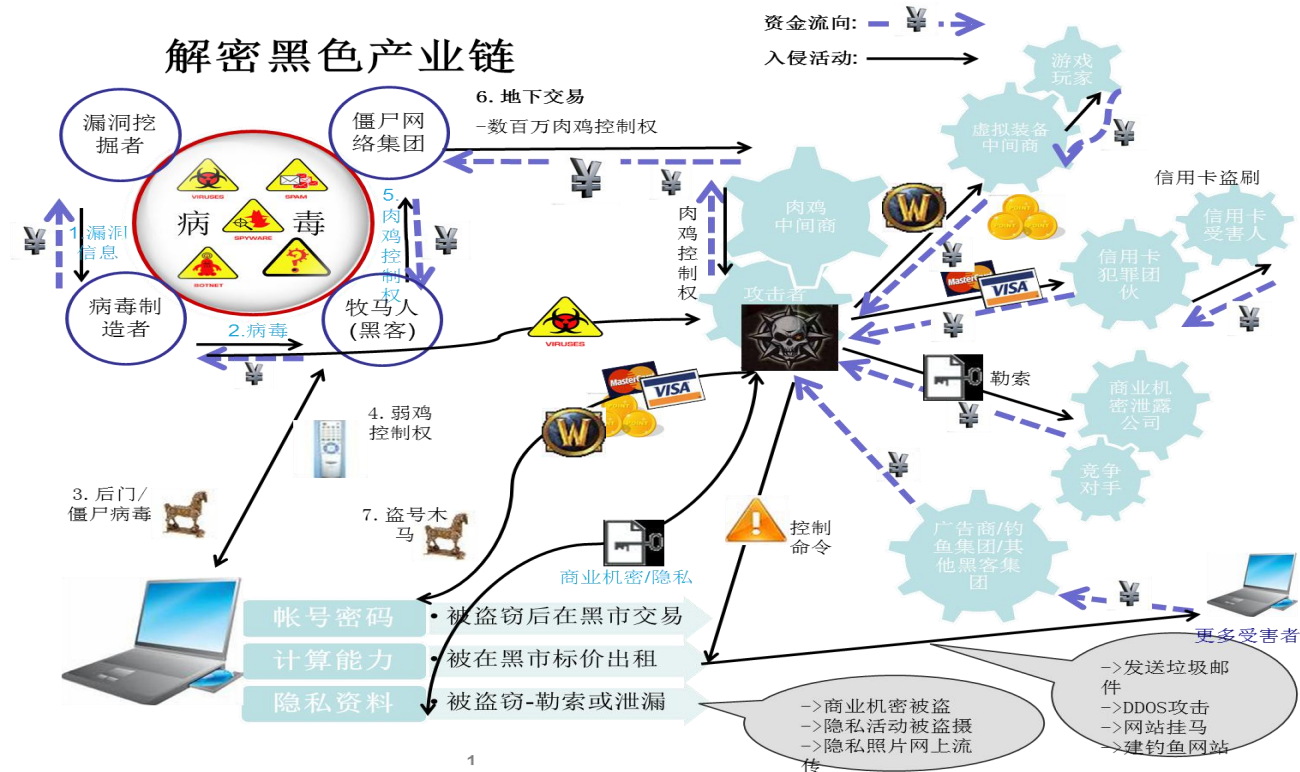
信息安全，就是采取措施**保护信息资产**，使之不因偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够**连续、可靠、正常**地运行，使安全事件对业务造成的**影响减到最小**，确保组织业务运行的**连续性**。



极道科技

一、攻击从个人英雄向组织犯罪转变

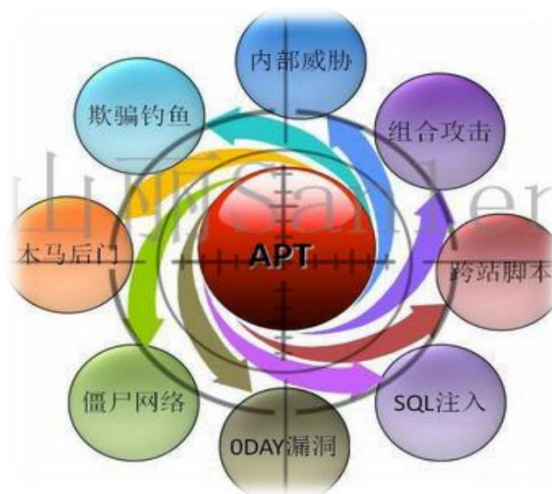
攻击变得越来越有组织性，攻击从个人英雄向组织犯罪转变；
有组织的攻击犯罪攻击资源更多，更加有效，造成的安全威胁更大



极道科技

一、攻击手段体系化

- 采用体系化攻击手段的APT攻击呈爆发趋势，带来越来越大的安全威胁。
- APT攻击以窃取核心资料为目的，会运用各种攻击工具、受感染的各种介质、供应链和社会工程学等体系化的攻击手段实施先进的、持久的且有效的威胁和攻击。



极道科技

一、信息安全重要性及当前趋势

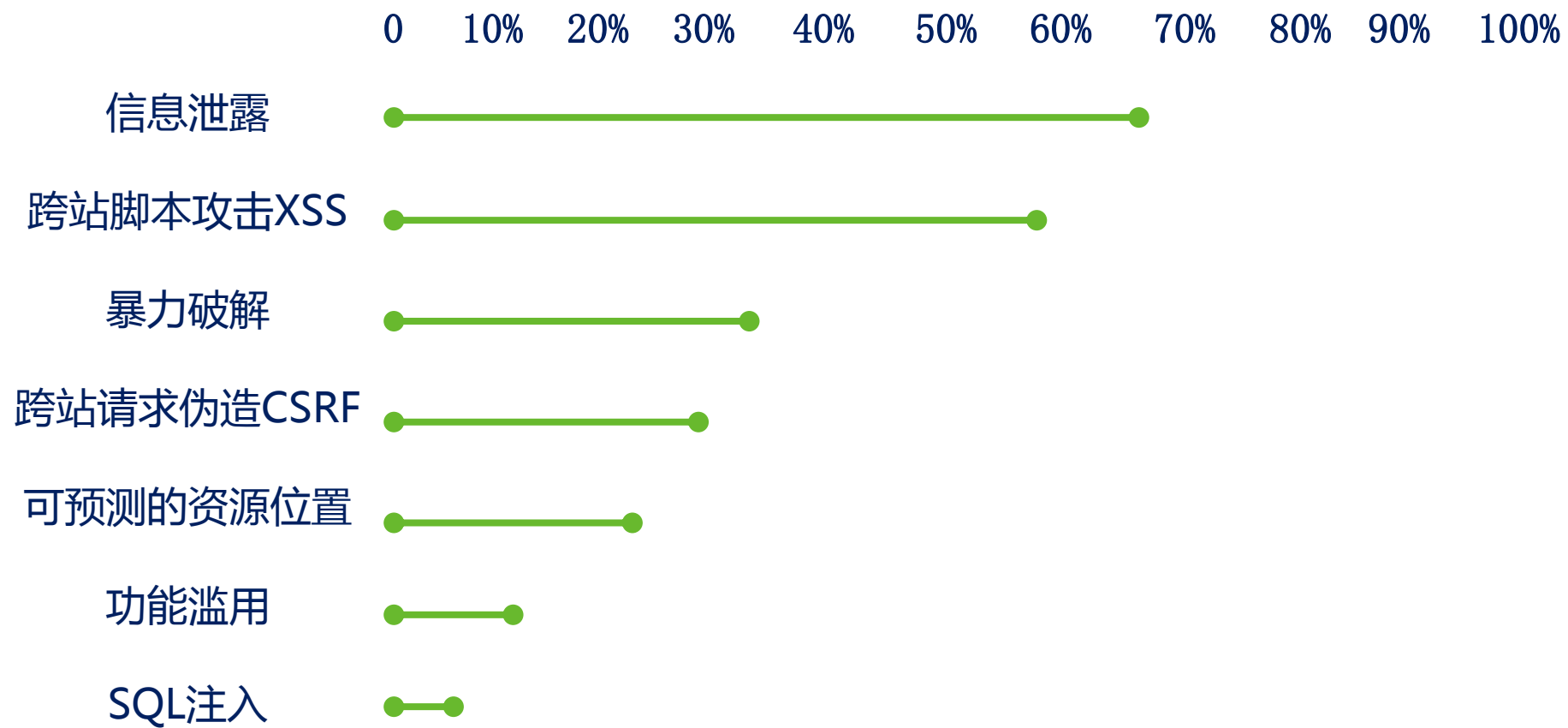
随着《网络安全法》、《网络安全等级保护》、《数据安全法》等安全法律法规的相继实施，对数据资产进行全生命周期的安全管控已成为未来可持续发展的必然要求。数据资产安全合规是可持续发展的首要条件，在数据资产的产生、存储、传输、交换、使用等全生命周期的各重要环节如何做到数据资产防泄漏、防篡改、防滥用是数据资产所有者当前及今后面临的数据资产安全管控的永恒命题。

当前网络攻击正在向高级威胁过渡，复杂化、组织化、专业化成为网络攻击愈加明显的特征，网络攻击分子会千方百计地寻找网络资产中的暴露面，寻找潜在的安全漏洞，这将带来持续增长的网络安全风险。并且，政府、行业、企业监管都对于网络资产安全治理提出了愈发严格的要求。



极道科技

二、常见的漏洞出现比例



极道科技

二、社会工程学

欺骗的艺术—社会工程学

利用社会交往（通常是在伪装之下）从目标对象那里获取信息，例如：

- 电话呼叫中心
- 在走廊里的聊天
- 冒充服务技术人员

黑客更多是通过社会工程来渗透网络的，而不是高超的黑客技术

如果你给一个黑客100万，要求他窃取竞争对手的资料，你猜他首先会想到怎么做？



极道科技

二、社会工程学

社会工程学

社会工程学是一种通过对目标**心理弱点、本能反应、好奇心、信任、贪婪**等心理布下的心理陷阱，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。

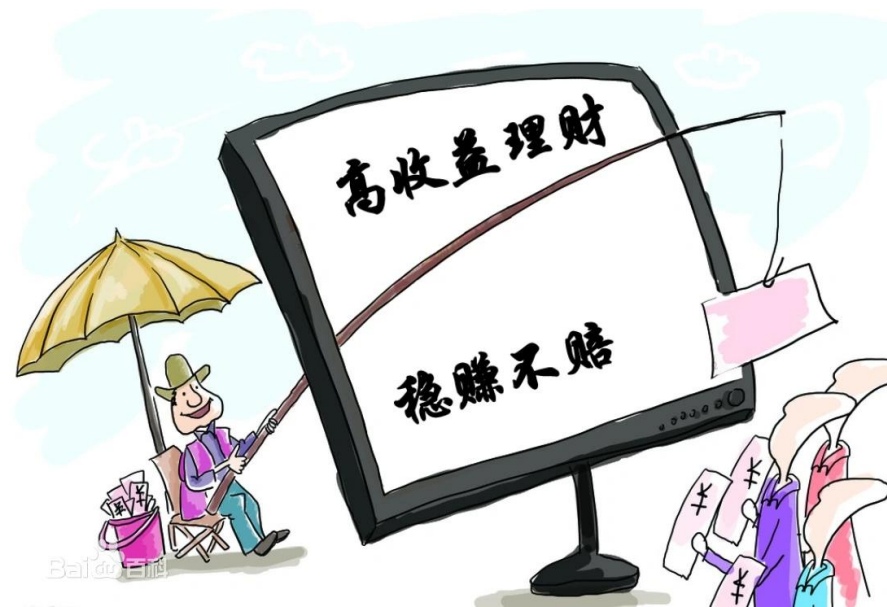
社会工程学是一种黑客攻击方法，利用欺骗等手段骗取**对方信任**，获取机密情报。总体上来讲，社会工程学就是使人们顺从你的意愿、满足你的欲望的一门艺术与学问。



极道科技

二、常见的安全隐患-钓鱼网站

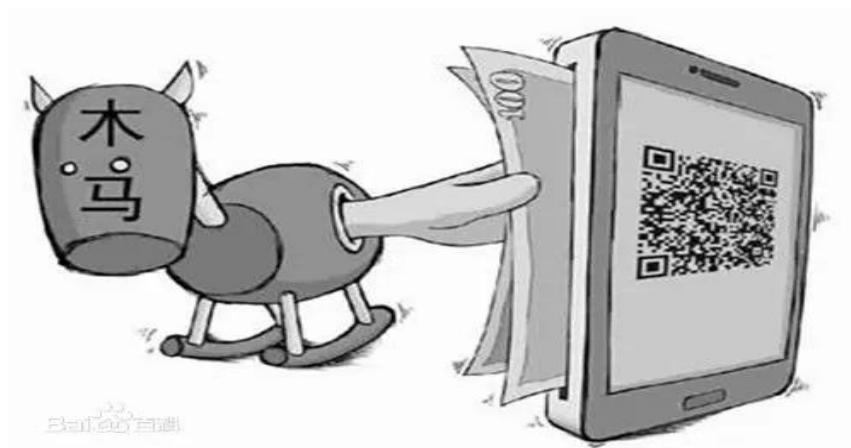
钓鱼网站是指欺骗用户的虚假网站。“钓鱼网站”的页面与真实网站界面基本一致，欺骗消费者或者窃取访问者提交的账号和密码信息。钓鱼网站一般只有一个或几个页面，和真实网站差别细微。钓鱼网站是互联网中最常碰到的一种诈骗方式，通常伪装成银行及电子商务、窃取用户提交的银行账号、密码等私密信息的网站。



极道科技

二、常见的安全隐患-木马病毒

木马病毒是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和攻击Dos等特殊功能的后门程序。



引诱用户下载安装的木马

利用系统漏洞传播木马

利用应用软件漏洞传播木马

可执行文件类型

exe 可执行文件标准后缀
pif dos格式的快捷方式后缀
scr 屏幕保护程序后缀

有的木马把文件名改为***. jpg. exe
有的木马把自己的图标弄成文件夹样子



极道科技

二、常见的安全隐患-WIFI连接

WI-FI信号具有一定的覆盖范围，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、流量劫持、密码破解等风险。

- ✓ 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

Wi-Fi信号满格



极道科技

二、常见的安全隐患-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，结合其他途径活得的身份证、银行卡、支付账号进行盗刷盗用。

网络诈骗已经形成了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，勾连紧密。

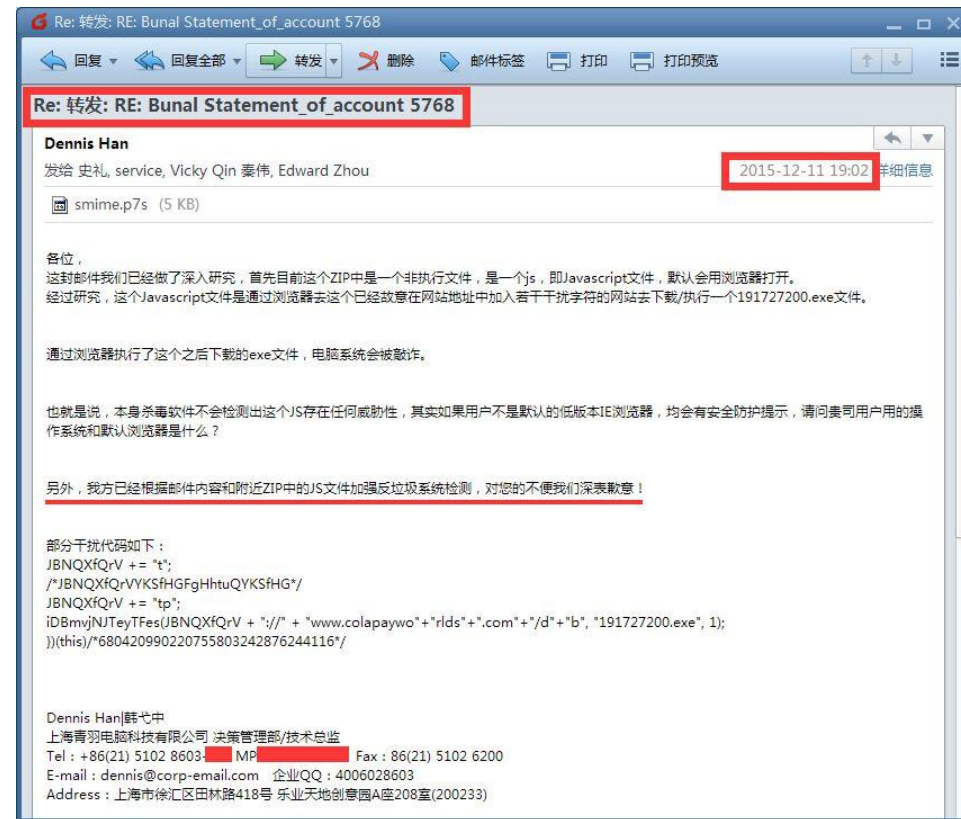


极道科技

二、常见的安全隐患-勒索病毒邮件

勒索病毒，是一种新型电脑病毒，主要以邮件、程序木马、网页挂马的形式进行传播。该病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解

邮件正文是关于订单和发票的内容，同时邮件包含带有zip的附件，附件名称中有payment字样，用户在收到这样邮件后，很容易点开附件查看，但打开附件后随即中刀，电脑中word，excel等文件被更改为.locky，告知用户付款后才能解锁。



极道科技

三、日常工作中的规范和防范意识

- 1. 计算机系统存在漏洞，是病毒快速传播的基础；
- 2. 办公电脑未安装防病毒软件，或病毒库未及时更新；
- 3. 数据未进行异地备份，导致数据丢失后无法恢复；
- 4. 接入交换机安全配置不合规，无法防止病毒扩散；
- 5. 缺少数据防泄漏设备与机制，无法及时发现数据被泄露。



极道科技

三、日常工作中的规范和防范意识

终端安全-设备使用

- 谨防信息泄露，不随意刻录保密信息
- 计算机屏幕定期锁定，离开工位前一定要锁屏
- 不随意将工作电脑用于非工作用途，或随意借给他人使用
- 不私自拆卸和向外部送修设备

案例：技术服务部某员工违规将便携机借给合作方员工使用，合作方员工利用上班时间用QQ传递工作所需文件；并且未经审批在机房使用移动存储设备给用户拷贝用户文档或版本文件；

分析：便携机上保存的很多工作文档，自己可能觉得没什么大不了的，可是其他人拿到就不一定了



极道科技

三、日常工作中的规范和防范意识

终端安全-病毒防范

- 安装杀毒软件，升级杀毒软件的病毒特征库
- 不访问不良网站，不下载来历不明电子邮件
- 移动存储介质拷贝文件需谨慎，不双击打开移动存储介质
- 不安装不正规的软件

案例：长时间未使用的服务器开机，或长期出差员工的笔记本电脑接入机构网络，其病毒特征库升级前直接使用，都可能带来严重的安全隐患



极道科技

三、日常工作中的规范和防范意识

终端安全-软件安装控制

- 使用正版或可信的办公软件处理工作
- 不在未批准的情况下，随意安装盗版和来路不明软件
- 不随意卸载和修改公司统一安装的控制管理软件和防病毒软件
- 不在未批准的情况下，自行安装多操作系统和虚拟机



极道科技

三、日常工作中的规范和防范意识

账户和密码安全

- 无论是公司电脑还是个人电脑，删除不必要的账户（如供应商默认账户等）、禁用guest账户
- 不使用用户名（账号）、生日、单词等作为密码
- 不要将密码写在纸上，不将密码存储于电脑文件中
- 定期修改密码，不把密码告诉任何人
- 不同的账户尽可能不使用相同的用户名和密码
- 密码找回问题不要使用公开信息



极道科技

三、日常工作中的规范和防范意识

账户和密码安全-密码设置

请问哪些是弱口令

123456

19890303

root@123

Admin!@#\$

Qwer1234!@#\$

2wsx1qaz

!QAZXSW@



极道科技

三、日常工作中的规范和防范意识

账户和密码安全-密码设置

使用自己不会忘记而别人不会知道的信息

奶奶的姓名 爸爸的生日

第一次牵手约会在哪里

小学时最好的朋友



极道科技

三、日常工作中的规范和防范意识

账户和密码安全-密码设置

- 什么样的密码是强壮的？

长度不小于八位，至少包括大小写字母、数字和特殊字符

- 太复杂了根本记不住怎么办？

✓ 联想记忆法：Ju\$t4U@7xi = Just for you @ 七夕，每次写密码还可以提醒自己，记得七夕给爱人买礼物

✓ 诗词记忆法：还能背诵《木兰辞》吧，Jlbz4-ZZ10ng = 将军百战死，壮士十年归

✓ 场景记忆法：想象一副图片，创建与之关联的故事再把它变成密码



极道科技

三、日常工作中的规范和防范意识

账户和密码安全-密码设置-高阶

密码: ppnn13%dkstFeb.1st,	密码: ppnn13%dkstFeb.1st, 解释: 娉娉袅袅十三余, 豆蔻梢头二月初
密码: for_\$n(@RenSheng)_\$n+=" die"	密码: for_\$n(@RenSheng)_\$n+=" die" 解释: 人生自古谁无死
密码: tcmlflw, syred>febhua]	密码: tcmlflw, syred>febhua] 解释: 停车坐爱枫林晚, 霜叶红于二月花
密码: dig?F*ckDang5	密码: dig?F*ckDang5 解释: 锄禾日当午



极道科技

三、日常工作中的规范和防范意识

上网安全

- 公司网络属于公共资源，上班时间应仅用于工作用途
- 禁止修改浏览器默认安全选项
- 在没有安装防病毒软件的情况下不应上网，互联网上下载的文件应先扫描病毒后使用
- 通过互联网传输敏感信息和文件时，应使用加密的方式
- 不通过外部邮箱和网盘传播公司的保密信息（秘密级以上）
- 不随意下载网站上提供的免费软件



极道科技

三、日常工作中的规范和防范意识

信息发布

不要随意浏览色情、暴力、赌博等网站或参与相关话题

不参与涉及政治、宗教、种族的敏感话题

不发布与散播有关公司的不良言论

不私自发布公司的非公开信息到互联网上

不浏览可能包含恶意内容的站点

不发布可能影响公司形象和业务的言论



极道科技

三、日常工作中的规范和防范意识

IT应用与工具安全-邮件安全

- 员工不应使用公共电子邮箱处理公务
- 发邮件时注意收件人是否合适，特别是前文历史和附件是否必须
- 收邮件时注意收件人是否正确，不打开可疑的链接和附件
- 谨慎使用回复所有人，须确保所有收件者能够知悉信息
- 向外部发送邮件时应，应告知对方对邮件内容的保密义务
- 含有保密信息的附件须进行加密，包括但不限于WinRAR等手段，密码通过电话、短信等其他渠道告知收件人



极道科技

三、日常工作中的规范和防范意识

IT应用与工具安全-即时通讯安全

- 尽可能使用企业微信进行办公和内部沟通
- 必须使用个人微信进行工作沟通时，应特别注意群组的使用，确认群组成员身份是否工作相关
- 其他法律规定的群主合规义务



私人事务



公司业务



极道科技

三、日常工作中的规范和防范意识

IT应用与工具安全-合同及重要文件存储与传输加密

工作中现在越来越多的人开始将资料存放在电脑里面，方便简单。但是放入到电脑里面的文件夹，如果涉及到比较隐私的资料，就会担心会不会被别人看到，或者在传递重要文件的时候都需要文件加密来确保存储、传递安全。



极道科技

三、日常工作中的规范和防范意识

事件上报

- 遵守信息安全管理规章制度
- 加强办公安全意识培训，破除“家丑不可外扬”的思维方式，形成“早发现、早报告”的习惯
- 了解专门的上报渠道
- 加强与信息安全部门的沟通



极道科技

• 总结一下

软件下载、运行要留心

熟人邮件、短信也要小心，链接不要随意点

口令设置要谨慎、复杂

系统勤打补丁和升级

电脑中不存储可能泄露身份信息的资料

不在云盘和网盘上存放敏感资料

自己的敏感信息要加密

互联网邮箱和工作邮箱要分开

关注安全新闻和安全知识



极道科技

谢谢



极道科技