



漫话安全

网络安全知识科普

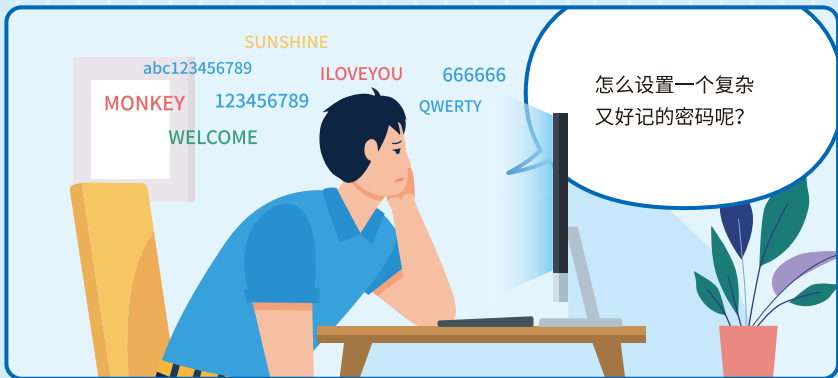
Contents

漫话安全·目录

- 01** 漫话安全之密码安全篇
 - 小密码大安全 01
- 02** 漫话安全之邮件安全篇
 - 看穿钓鱼邮件, 破解有招 04
- 03** 漫话安全之Wi-Fi安全篇
 - Wi-Fi的“信任危机” 07
- 04** 漫话安全之勒索病毒篇
 - 勒索病毒防患攻略 11
- 05** 漫话安全之数据泄露篇
 - 四招防范数据泄露 15
- 06** 漫话安全之网络安全合规篇
 - 合规不难, 应对有方 18



小密码大安全



小密码大安全



漫话安全之密码安全篇

小密码大安全



那么如何才能让自己的密码更安全呢?



1. 设置长度多于8位的高强度密码,且使用“字母大小写+数字+特殊字符”的无规律组合。



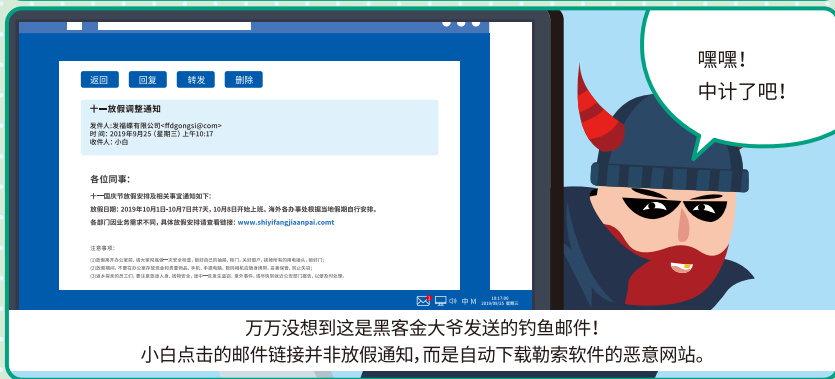
3. 对于重要系统需要定期更换密码,每隔两个月进行一次更换密码,并妥善保管不对外暴露。

漫话安全之邮件安全篇

看穿钓鱼邮件,破解有招



十一放假通知?
哈哈!可以提前计划
去哪浪了~



万万没想到这是黑客金大爷发送的钓鱼邮件!
小白点击的邮件链接并非放假通知,而是自动下载勒索软件的恶意网站。



最终不仅小白的电脑被加密勒索,更让黑客以此为跳板,入侵了连接公司内网的所有电脑,给公司带来严重的损失。

看穿钓鱼邮件，破解有招



第一、一定要核对网站域名，真实的钓鱼网站往往会隐藏在所显示域名后。



第二、钓鱼网站都比较粗糙，很多功能在点击后都无法使用。

看穿钓鱼邮件，破解有招



第三、钓鱼邮件目的是诱导用户点击链接或下载附件，所以对可疑的链接及附件一定要提高警惕!



最后，重要邮件发送有什么需要注意的?
第一、不随意转发重要邮件，应将重要邮件设置为不可复制及转发。



第二、群发邮件要设置群发单显或分别发送，避免重要收件人名单泄露。

Wi-Fi的“信任危机”



Wi-Fi的“信任危机”



无线网络在办公场景中起着不可替代的作用，人们可以通过连接Wi-Fi上网工作、传输邮件、视频会议等等，但我们连接的Wi-Fi真的安全吗？



满格信号Wi-Fi，不用输密码直接连接？嘿嘿，试一下。



哈哈，又有人中招了，一旦连上我的钓鱼Wi-Fi，手机电脑里的工作文件、照片、支付账户、密码，就都是我的囊中之物了！



狡猾的金大爷设置的Wi-Fi名称相同，让人降低心理防备，同时不需要密码即可登录，方便了更多人连接。



既然随意连接的Wi-Fi不靠谱，那就自己搭建一个，网速一定飞起！



小白万万没想到自己连接的竟然是黑客金大爷布置的钓鱼Wi-Fi。

Wi-Fi的“信任危机”



小伙子,你还是太年轻了。
竟敢利用公司内网私搭Wi-Fi?
正好方便我入侵公司内网。嘿嘿



借助员工私自搭建的Wi-Fi,金大爷成功获取内网权限并窃取到了公司的机密。

第一式

应对高招!



第一式,不要利用公司内网私自搭建Wi-Fi,这种Wi-Fi就像定时炸弹,自身防御薄弱,随时都有可能被黑客攻击,轻松引爆。

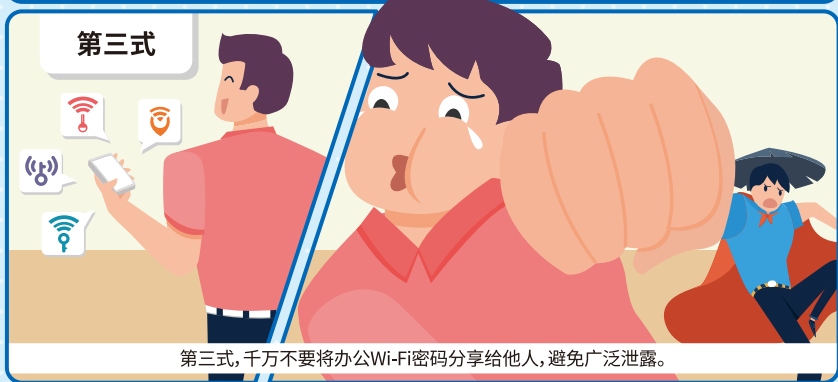
Wi-Fi的“信任危机”

第二式



第二式,对没有密码的Wi-Fi说不!记住!这很有可能是黑客设置的钓鱼陷阱。

第三式



第三式,千万不要将办公Wi-Fi密码分享给他人,避免广泛泄露。

第四式



第四式,拒绝使用简单的弱口令Wi-Fi密码,这样的密码在方便自己登录的同时也方便了黑客暴力破解。

勒索病毒防患攻略



勒索病毒防患攻略

软件到期
续费完又要吃土了!

您的软件即将在7天后过期
请您及时续费
立即续费



赶快在24小时内
缴纳赎金!
不然我就销毁你
电脑里所有数据!

23:58:40



对了!下载个
免费破解版不就行了吗,
机智如我!



原来小白下载的免费破解版软件是黑客金大爷事先传上去的含有勒索病毒的软件,会对小白电脑里的文件进行加密或窃取,一旦这些数据被禁用或者外泄,将给公司造成巨大损失。



天啊,
怎么回事?

正版软件下载

99\$

立即下载

想不到吧!
你的电脑和数据
被我加密了。
哈哈哈!

小白刚下载完破解版软件,但电脑上的其他文件都无法打开。



我的血汗钱呐~

可怜的小白只能乖乖缴纳赎金。



勒索病毒防患攻略



事实上,就算受害者缴纳赎金,黑客也不一定会真的兑现诺言.....



记住这几点,让勒索病毒防患于未然!
1、一定要在可靠的软件平台下载正规应用程序!

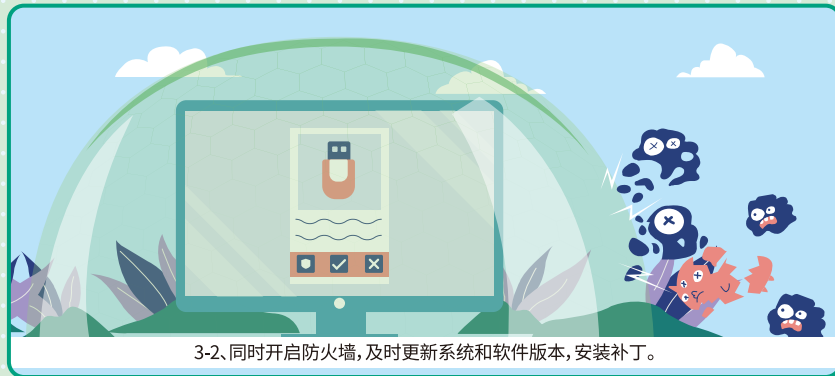


2、不可信的邮件,尤其是附件、链接,谨慎点击!

勒索病毒防患攻略



3-1、使用安全可靠的移动存储设备(U盘、移动硬盘等),并安装安全防护软件。



3-2、同时开启防火墙,及时更新系统和软件版本,安装补丁。



4、养成定期备份重要数据的习惯,即使遭受勒索病毒封锁数据,在使用杀毒软件查杀病毒后,可通过恢复备份数据来降低损失。

四招防范数据泄露



还有那么多待处理工作？看来今天又要加班了。



发个朋友圈让老板知道我在努力加班，说不定年底就升职加薪了！



嘿嘿，这张图上有他们公司业务系统的地址和员工账户名称，登录进去就可以拿到公司业务数据，登录一下试试。



四招防范数据泄露

有密码？不急，暴力破解来帮忙。



哈哈，拿到数据简直太容易啦！



黑客金大爷成功暴力破解了小白的弱口令密码，登录业务系统后获取了公司的大量敏感信息。

江湖险恶，做人好难！到底要怎样防止数据泄露呢？



这次数据泄露事件不仅让该公司遭受巨大经济损失，还引发了勒索、诈骗等多次生安全问题。

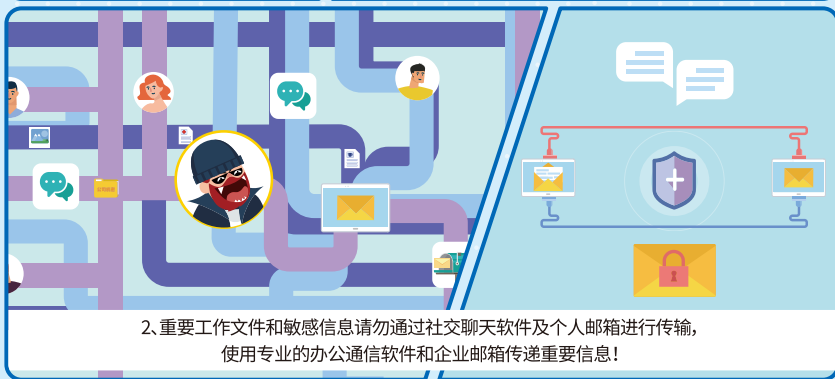


调查研究显示，造成数据泄露的原因主要有三方面，内部人员操作不当、网络攻击以及内鬼窃取。

漫话安全之数据泄露篇
四招防范数据泄露



1、不在论坛、贴吧等公众社交平台上发布或讨论公司的敏感信息，黑客隔墙有耳！



2、重要工作文件和敏感信息请勿通过社交聊天软件及个人邮箱进行传输，使用专业的办公通信软件和企业邮箱传递重要信息！

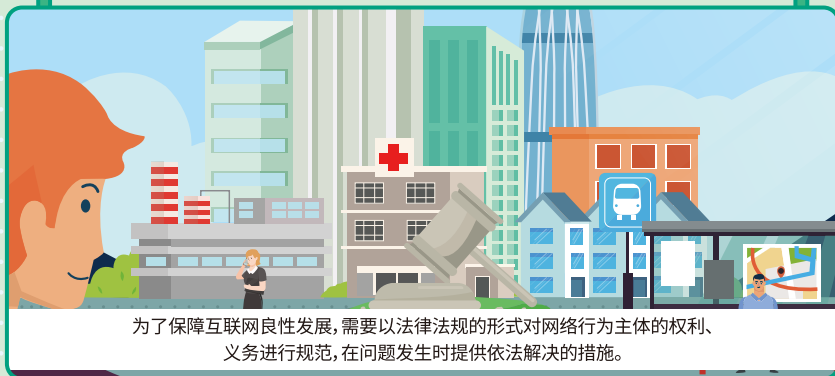


3、不要将公司文件和数据上传至私人网盘，安全性难保证！

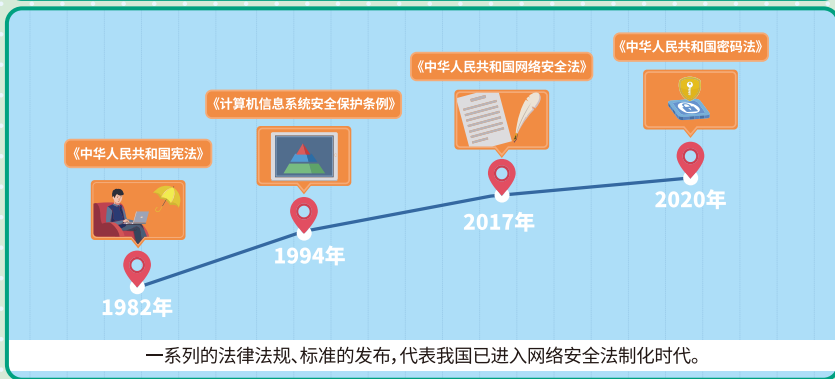
4、重要文件要加密保存，设置高强度密码，即使文件外泄，黑客也无法获取明文信息！

漫话安全之网络安全合规篇

合规不难，应对有方



为了保障互联网良性发展，需要以法律法规的形式对网络行为主体的权利、义务进行规范，在问题发生时提供依法解决的措施。



一系列的法律法规、标准的发布，代表我国已进入网络安全法制化时代。



网络运营者需要根据相关要求进一步规范自身相关义务和责任，网络安全建设也需要更加合法合规。

合规不难，应对有方

哎，公司漏洞怎么这么多，最近又接到了进行网络安全合规建设的任务，好烦啊！先缓缓吧。



嘿嘿，这个网站存在漏洞，入侵一下~哇，存在好多用户信息，又能卖钱了~

顺便再把网页篡改下，发布些虚假诈骗广告信息。



小白没想到，这些被大规模泄露出去的用户敏感信息以及被篡改的公司网站，对公共互联网网络安全造成了严重威胁。

合规不难，应对有方

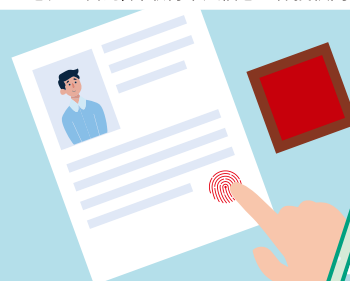


那么，网络安全合规需要做到哪些点？



- 1、网络运营者落实网络安全等级保护制度义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。
- 2、网络运营者应制定网络安全事件应急预案，并定期组织演练以及保留相应记录。

- 3、在个人信息安全方面，网络运营者应仅采集业务所需的个人信息，并在收集前向个人告知信息处理目的，并取得个人信息主体授权同意。



- 4、在数据安全方面，网络运营者应在数据采集、存储、传输、应用、销毁的每个阶段，都应按照相关规定做好安全防护措施。