奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

政企单位人员
安全用网规范

奇安信集团

目录

CONENT

安全上网基础课

安全软件务必装，自家大门要看好

定期体检打补丁，提前免疫不得病

密码设置强度高，验证短信不外泄

使用U盘先杀毒，遇到告警莫疏忽

陌生来电不轻信，不明链接不要点

删除资料能恢复，二手交易猫腻多

01

安全软件务必装 自家大门要看好

特别提示

有些会“卖萌”的病毒或者是网络骗子会谎称安全软件有“误报”，建议你暂时关闭安全软件。千万不能信啊！

安全软件

现代安全软件是电脑，手机的必备软件，一般包含以下几大功能：

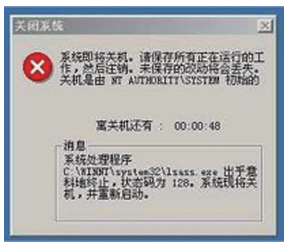
- **防病毒，防木马**
- **反钓鱼，反诈骗**
- **打补丁，修系统**
- **垃圾清理，系统加速**
- **软件管理，权限管理**

一般来说，只要经常用安全软件给电脑、手机做体检，多数安全问题都能“一键”解决。

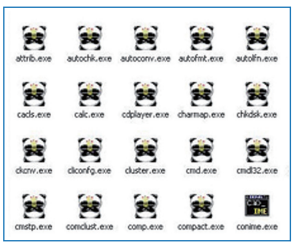
定期体检打补丁 提前免疫不得病

打补丁

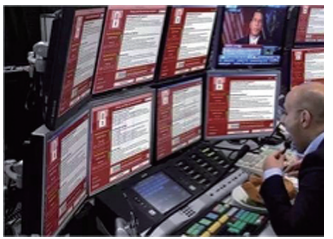
打补丁是为了修漏洞。系统不打补丁，就像家里不关门窗，很容易被入侵。存在漏洞的系统，安全软件也很难有效防护。



2003年8月，冲击波病毒利用微软已经修复的漏洞发起攻击，一周之内感染了全球约80%的电脑。



2007年1月，熊猫烧香病毒利用Windows漏洞肆虐全国，这是最为臭名昭著的一款“国产”病毒。



2017年5月，WannaCry勒索蠕虫利用漏洞永恒之蓝发起攻击，30个小时内就使100多个国家的大量机构陷入瘫痪。

打补丁工具

密码设置强度高 验证短信不外泄

密码的四项基本原则

密码是所有账号安全的基本保障，设置密码一般需遵守以下原则：

- **15位以上**
- **数字+字母+特殊符号**
- **定期修改（建议180天）**
- **支付、社交、邮箱等核心账号单独设密码**

动脑时间

你能在2分钟内记住下面三个密码吗？哪一个密码最安全？你知道怎样构造一个又长又好记的密码吗？

chuangqianmingyueguangyishidishangshuang

xiaobaitu2baiyoubai3liangzhierduoshuqilai4

@xiyangyang#yuhuitailang$123

特别提示

账号一旦被盗，应立即修改所有其他相关账号的密码

短信验证码是一种动态的密码，千万不要告诉任何人

使用U盘先杀毒 遇到告警莫疏忽

U盘防护

U盘又称病毒“摆渡”，常用来攻击隔离网中的电脑。

著名的“震网病毒”就是通过U盘入侵伊朗核电站并实施破坏。

U 盘、移动硬盘一定要先查毒，后使用

安全软件告警

收到新文件或下载新文件后，如果安全防护软件弹出告警提示，千万不要疏忽，在不能完全确定安全的情况下，应该阻止其运行，并进行删除。

陌生文件遇到告警一定要先阻止运行

陌生来电不轻信 不明链接不要点

诈骗电话与骚扰电话

伪基站的仿冒短信

短信中的带毒短链接

社交软件欺诈链接

安全软件一般无法检测社交软件中网址链接的安全性

用社交软件转发网页，网址也会被隐藏

防骗，只能擦亮眼睛

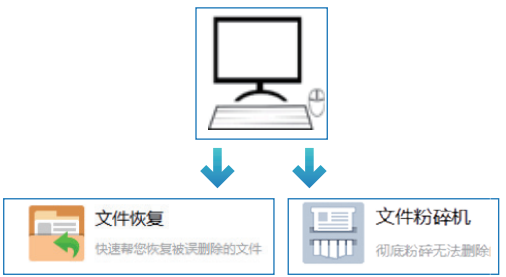
特别提示

外来的、陌生的、你不熟悉的东西都可能有危险，电话，短信、网络社交皆如此。

删除资料能恢复 二手交易猫腻多

文件删除

无论是在电脑上还是手机中，被删除的文件通常可以使用某些专用工具恢复出来，想要彻底删除，需要进行文件“粉碎”。



出厂设置

在手机上“恢复出厂设置”也不能彻底删除文件，仍然可恢复。

隐私擦除

彻底擦除手机隐私方法

删除信息后，用视频等大文件复制并占满手机存储空间，即可彻底擦除原有数据。

特别提示

若未能妥善处理手机中原有资料，一旦手机被黑心二手商贩收购，他们很有可能会恶意恢复手机信息，并贩卖到网络黑市。

安全办公提高班

WiFi易成突破口，私建网络是祸根

办公邮箱不乱用，到处注册风险多

邮件附件常带毒，陌生来源勿打开

收信看清发件人，冒名顶替要当心

OA钓鱼最危险，美国大选也中招

骗你上当有理由，仿冒登录盗账号

安全习惯早养成，提高警惕少出错

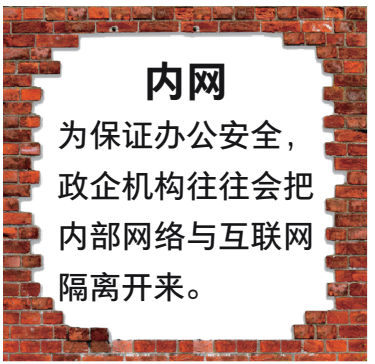
02

WiFi易成突破口 私建网络是祸根

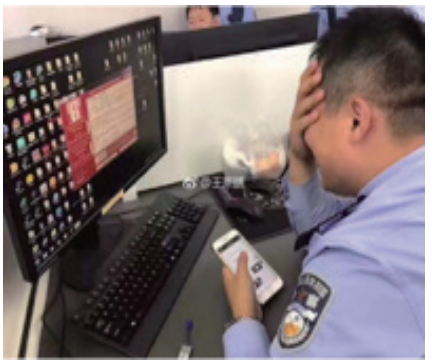
私建WiFi热点的风险

私自搭建WiFi热点，并将内网中的设备与热点相连，将会在内网边界上打开突破口，使网络隔离完全失效。

一旦内网出现突破口，木马、病毒、黑客，都会乘虚而入。



内网必须禁止随身WiFi。



WannaCry勒索蠕虫会攻击隔离网设备的重要原因之一就是有员工在内网之中自搭乱建WiFi热点。

办公邮箱不乱用 到处注册风险多

电子邮箱

电子邮箱是政企机构办公的重要工具。

中国境内企业级电子邮箱活跃用户规模约为1.2亿。

企业级用户平均每天收发到电子邮件约16.1亿封。

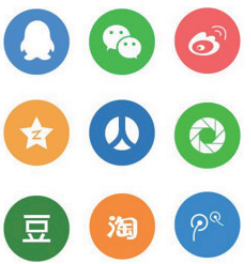
特别提示

切勿使用办公邮箱注册游戏、购物、社交、论坛等第三方应用账户，否则会有如下风险：

您的办公邮箱中会收到很多垃圾邮件。

一旦第三方应用平台被黑，您办公邮箱的账号和密码也可能会同时泄露，造成邮件中的机密外泄。

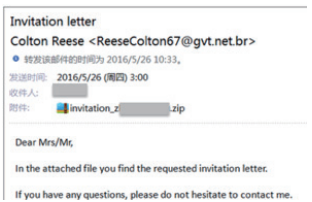
办公邮箱密码泄露，可能引发连锁反应，进而泄露机构内网账号，导致内网被黑客入侵。

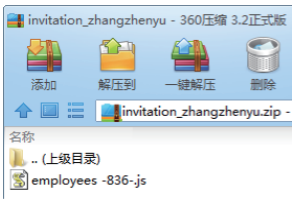


邮件附件常带毒 陌生来源勿打开

勒索邮件

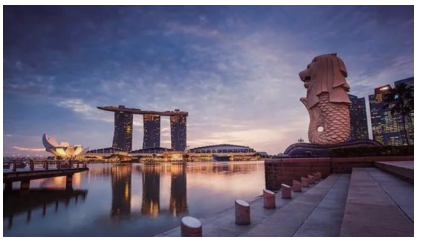
下面这封不起眼的邮件携带了一个ZIP格式的附件，解压后生成一个JS文件，它实际上是一个勒索软件，一旦点击打开，电脑中所有的办公文档、照片、视频都会被加密，只有向勒索者支付赎金后才能解密。





窃密邮件

2021年3月，新加坡最大的私人保安公司策安集团因员工点击钓鱼邮件，导致约62000封邮件内容遭到外泄。



勒索软件中招后屏幕的现象

收信看清发件人 冒名顶替要当心

电子邮箱收件人的信息由邮件显示名和邮件地址两部分组成，而邮件地址又是由邮箱账号和邮箱域名组成。

特别提示

- **显示名很容易被仿冒**

  邮件的显示名通常可以由发件人任意编写.骗子们经常把邮件显示名伪装成：管理员、XX机构、XX领导等。

- **邮箱账号也可能被仿冒**

  如，真实邮箱是zhangsan@263.com,仿冒邮箱却是zhangsan@qq.com，不仔细看很难分辨。

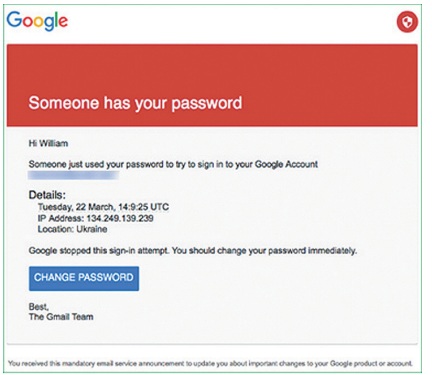
  所以，收到邮件不能光看显示名，还要认真查看发件人的邮件地址以及邮箱域名，稍不留心就可能上当受骗。

OA钓鱼最危险 美国大选也中招

OA钓鱼

冒充系统管理员发送的欺诈邮件被称为OA钓鱼。OA钓鱼多用于盗号。

2016年美国大选，黑客组织冒充Google邮件系统安全管理员给希拉里竞选团队负责人发信，骗取了负责人的邮箱密码，盗取并公布了希拉里竞选团队的机密邮件，最终使得希拉里败选，特朗普上台。



希拉里竞选团队成员William Rinehart收到的伪装成Google安全团队的鱼叉邮件。

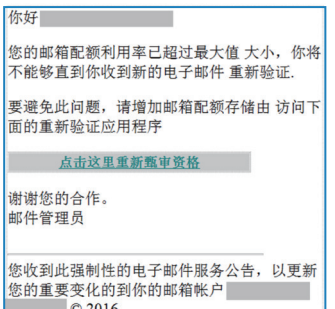
骗你上当有理由 仿冒登录盗帐号

OA钓鱼手法

OA钓鱼的目的是诱骗受害者在虚假的登录页面上输入账号和密码，进而实现盗号。

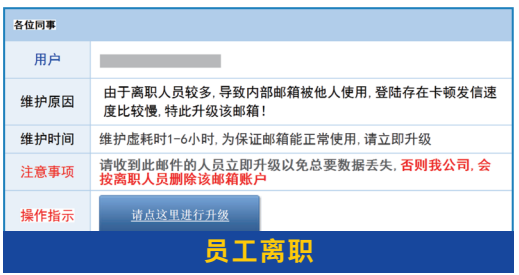
OA钓鱼的“理由”有很多，下边几个都是，您能认得出吗？

安全性升级

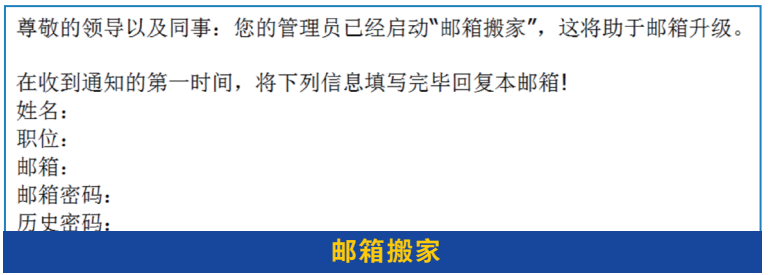


邮箱升级

邮箱停用



员工离职



邮箱搬家

安全习惯早养成 提高警惕少出错

尽量不要在微信上谈工作

微信是比较开放的社交环境，不适合谈论工作。办公社交建议使用企业级社交软件。

保存文件尽量不要用密字

保存文件时文件名尽量不要包含密、秘密、保密、绝密等字样，这些字很容易被黑客盯上。

不在电脑桌前电脑要锁屏

电脑锁屏，既可以防止他人偷窥到自己电脑中的文件，又可以防止他人胡乱操作损坏文件。

下班以后一定要关闭电脑

很多人为图方便，下班以后不关电脑，这就给黑客留出了更多电脑前无人值守的攻击时间。

出门在外自修班

连接WiFi要谨慎，蹭网心态吃大亏

二维码中藏奥秘，随手扫描易中招

公务电脑莫出境，要带只带空白机

03

连接WiFi要谨慎 蹭网心态吃大亏

WiFi的安全风险

WiFi是一种短距离局域网无线传输技术，数据在传输过程中通常不加密。如果有黑客恶意监听无线路由器上传输的数据，数据将被黑客窃取。

2015年央视315晚会，安全专家现场演示如何通过免费WiFi盗取现场观众的上网信息，演示包括对照片、文字、账号和密码等信息的窃取。

蹭网软件的风险

蹭网软件可以帮你免费使用他人WiFi但也可能泄露自己家中的WiFi密码连接不安全的WiFi可能被盗号、诈骗。

特别提示

公共场合连接WiFi，一定要选择官方的、有密码的。无密码的WiFi最危险。

二维码中藏奥秘 随手扫描易中招

二维码

二维码实际上是一个图形化的数据信息，信息中可以存储文本、网址等各类信息。

二维码生成器

网上可以搜索到很多二位码生成器，任何人都可以很容易的生成一个二维码。

随意扫码的风险

扫码打开的网页可能含有欺诈信息、木马病毒。

扫码后被要求填表，可能泄露个人信息。

扫码后可能会进行“无意识支付”，被骗钱财。

特别提示

扫码后提示下载陌生文件的，谨慎!

扫码后要求填写个人信息的，谨慎!

公务电脑莫出境 要带只带空白机

国外安检人员检查旅客行李中的电子物品

特别提示

- 不论是公务员还是普通企业员工，出国旅行时尽量不要带自己日常使用的办公电脑。
- 一方面，您可能被安检员强行扣查电脑，造成机密泄露。
- 另一方面，国外社会、网络环境与国内不同，电脑更易遭到盗窃、抢夺或网络攻击。

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥标准奇安信 网络安全快一步

攻防快一步

漏洞发现快

补天漏洞响应平台

白帽专家	7.8万+
报告漏洞	60万+
影响企业	17万+
入驻企业	5900+

应急响应快

应急响应电话
4009 727 120
（7×24小时）

情报获取快

攻防演习快

攻击队 → 组织单位：奇安信 新一代网络安全领军者 实战攻防演习平台 → 防守单位

实战攻防演习平台

态势感知快

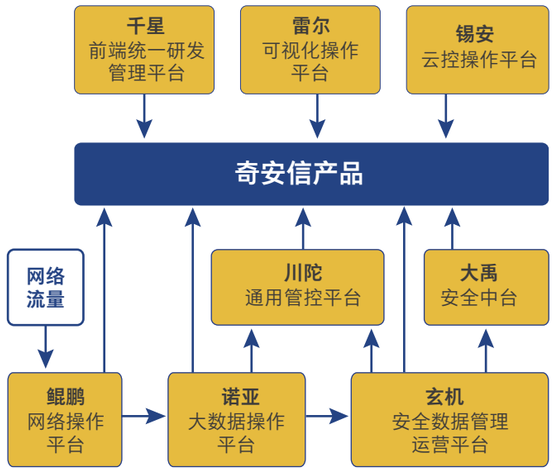
创新快一步

技术研究快

12大安全技术团队

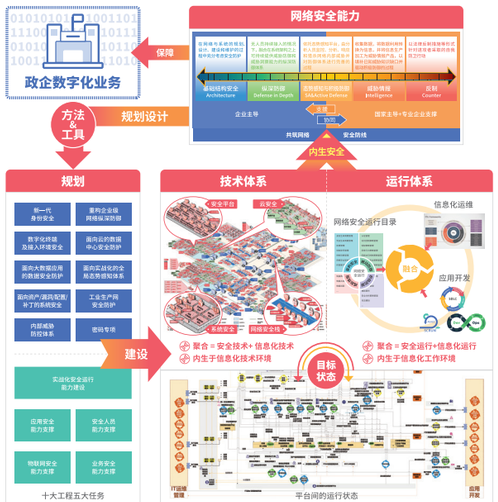
实网攻防	Z-TEAM 实战网络攻防技术团队
	A-TEAM 实战网络攻防技术团队
漏洞挖掘	盘古实验室 移动系统和应用漏洞挖掘
	代码安全实验室 源代码与二进制漏洞挖掘
	观星实验室 互联网应用漏洞挖掘
	羲和实验室 互联网基础协议漏洞挖掘
	天工实验室 物联网漏洞挖掘
	巽丰实验室 工业互联网漏洞挖掘
	星图实验室 软件及供应链漏洞挖掘
威胁情报	威胁情报中心 威胁情报的生产与赋能
	红雨滴团队 高级威胁检测对抗研究
	天狗引擎团队 0Day漏洞防护与后门发现

赛道引领快 平台建设快



规划快一步

体系建设快 系统融合快 安全运营快



新一代企业网络安全框架（内生安全框架）

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

我们是网络安全中国代表队

网络安全中国代表队 | 奇安信

奇安信

新一代网络安全领军者

作为北京2022年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商，奇安信以更快一步、更高标准、更强防护的安全能力，为政府、军工、企业用户提供新一代企业级网络安全解决方案、产品和服务，凭借以实战攻防、平台创新、规划咨询为代表的全面领先的优势，通过七年积累，发展成为企业数字化转型与升级的全天候、全方位安全顾问。

奇安信为安全而生，在诞生之初就树立“让网络更安全，让世界更美好”的使命，立志成为全球第一的网络安全公司。公司于2020年7月22日在科创板上市，股票

代码688561。在未来征程中，奇安信将继续发扬不畏挑战、敢于超越、追梦拼搏的精神，引领新一代网络安全理念、技术和产业的发展方向，携手合作伙伴一起，助力客户数字化转型升级和网络安全的同步提升。

奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信 安全快一步

奇安信官网

奇安信集团
微信公众号