2022年“首都网络安全日”

# 上网安全手册

▶▶▶ 办公安全防护 个人信息保护

2022 | 第3届
首都网络安全日
BEIJING CYBER SECURITY DAY

# CONTENTS

## 目录



2022 | 第3届
首都网络安全日
BEIJING CYBER SECURITY DAY

# 前言

如今网络科技正以新理念、新业态、新模式全面赋能人类经济、政治、文化、社会、生态文明建设各领域，成为人们生产生活不可或缺的组成部分。随着网络普及率的不断提升，中国的网民规模不断壮大，网络技术在带动国家快速发展、便利服务百姓的同时，也让网络世界中的安全隐患更加突出，清朗的网络空间正遭受各类威胁。

值此第九届“首都网络安全日”活动到来之际，北京市公安局、北京市互联网信息办公室共同指导的《2022 年“首都网络安全日”上网安全手册》，从办公安全防护、个人信息保护两方面，揭露网络犯罪手段，提示日常网络安全风险点，并结合具体案例进行分析，提出防范技巧，进一步普及网络安全知识，提高安全防范意识，确保群众远离不法网络侵害，共享安全网络生活。

# 办公安全防护

## 一、邮件安全

网络信息化时代，电子邮件已然成为企业对内和对外工作交流的一种重要工具。然而，随着邮件的广泛使用，网络钓鱼、电信诈骗、勒索病毒等事件频发，政企单位的邮件安全正在面临着巨大的威胁和挑战。

## 案例一：国内某大型国有企业遭遇钓鱼邮件攻击

1

此前，某大型国企众多员工收到管理员账号发送的 OA 钓鱼邮件。根据员工反馈的截图显示，邮件发送方以集团信息管理部名义向全员发送的“集团通知”邮件，要求全员点击邮件中地址进行备案。该“邮箱升级审核系统”要求员工输入用户名、登录地址、邮箱密码等信息。据统计，本次钓鱼邮件攻击给该企业造成了重大危害，包括集团领导在内的 200 名员工邮箱、联系方式、公司组织架构，以及十余名员工邮箱内的全部邮件内容均遭到泄露。

## 案例二：谨慎“仿冒近期回信”的新型钓鱼邮件攻击手段

2

上海交通大学网络信息中心此前发现一种新类型的钓鱼邮件攻击手段，黑客盗取用户近期邮件联系过的接收方账号后，以回复过往真实邮件的主题为诱饵，在邮件正文中虚构邮件无法显示等问题，诱导用户点击外部链接“获取全文”，以试图骗取用户账号信息。该外部链接可能部分或全部仿冒了学校的校徽及正规登录入口。据调查，邮件的链接样式各不相同，但都导向各种恶意网站，也都会索要用户账号信息。

# 电子邮件的常见威胁及防范措施

## 1 威胁一：钓鱼邮件

攻击者利用伪装的电邮，以熟人的名义将钓鱼信息发送给指定收件人，进而盗取信息。

- 收到各类邮件时首先核对发件人邮箱地址是否正确
- 如果发现邮件存在不合常理的地方，立即通过其他沟通方式与发件人本人确认

## 2 威胁二：恶意链接


攻击者通过诱骗目标点击嵌入邮件的恶意链接以植入木马或恶意程序，进而窃取敏感数据。

- 收到包含链接的邮件时，应确认链接是否与邮件正文所描述的系统一致
- 如需访问业务系统，建议通过浏览器预先保存的书签点击进入，尽可能不点击外部发来的链接
- 手机丢失时，谨防邮箱内收到的“查找手机位置”的邮件

## 3 威胁三：病毒附件

附件病毒最常见的当属勒索病毒。攻击者通常将恶意内容伪装成重要信息进行传播，诱骗受害者下载附件。

- 在收到可疑邮件后，应避免打开其附件文件
- 在 Office 中避免启用宏和 ActiveX 功能，尤其注意避免外来文件启用上述功能
- 在处理外部邮件附件前，首先使用防病毒软件查杀病毒

## 4 威胁四：垃圾邮件

垃圾邮件不但侵占邮箱空间，还可能携带恶意程序或链接，造成信息泄露或财产损失。

- 不轻易留下电子邮件地址
- 不回应任何垃圾邮件
- 将垃圾邮件地址加入黑名单

## 5 威胁五：邮件截获

安全性较差的网络或传输协议很容易被攻击者入侵，导致邮件信息被篡改或截获。

- 不使用邮箱客户端时，采用更为安全的 SSL（TLS）端口
- 使用 WEB 邮箱时应确认网页协议为 HTTPS
- 使用安全的网络进行邮件通信

# 办公安全防护

## 二、无线网络安全

无线网络作为工作、生活中的基础设施，在各种各样的场景都起着不可替代的作用，人们可以通过 Wi-Fi 进行信息检索、文件传输、视频会议等诸多操作。然而，我们连接的 Wi-Fi 真的安全吗？

## 1

## 案例一：使用“蹭网”软件致信息被盗

2020 年 2 月，王女士在手机上安装了某“蹭网”软件，无需输入密码，便自动连接上公共 Wi-Fi。从那以后，王女士经常收到陌生人打来的推销电话。经调查发现，在安装和使用过程中，该软件还会索取手机通话记录、位置信息、微信信息、相机、已安装应用软件列表等权限。这些权限明显与软件提供的服务业务没有直接关联，根本目的是索取王女士的隐私信息并进行非法利用。

## 2

## 案例二：连接公共 Wi-Fi 被勒索 5000 元

市民宋女士在机场连接 Wi-Fi 后，手机突然黑屏重启，随后手机进入锁屏状态，同时弹出一行字，“如需解锁请联系 QQ：2729354××”。无奈之下，宋女士只好用他人手机添加屏幕上显示的 QQ 号码，联系后，对方要求支付宝转账 5000 元，否则不仅手机要变成“砖头”，手机内保存的私密信息也要被公之于众，无奈之下宋女士答应了对方的转账要求。

# 无线网络三大陷阱

## 1 陷阱一：盗取数据

在公共场所经常有免费的 Wi-Fi， 不法分子会架设与公共 Wi-Fi 同名的网络， 吸引公众连接， 然后在 Wi-Fi 路由器上劫持 DNS， 将用户引入钓鱼网站获取账号密码， 或者在路由器上监听手机流量， 获取明文密码。

## 2 陷阱二：监听手机


如果不慎连接了钓鱼 Wi-Fi， 那么你的手机很有可能被“劫持”。 黑客可以远程盗取相册、 通讯录、 通话记录等隐私内容， 甚至还可以远程监听手机通话， 开启摄像头进行监控等。

## 3 陷阱三：盗用无线


如果你的 Wi-Fi 突然变慢了， 除了网络本身的问题， 也可能是“有心人”在偷偷蹭网。 Wi-Fi 密码过于简单， 不仅方便别人“蹭网”， 还有可能被有心人利用， 控制路由器， 偷窥你的隐私。

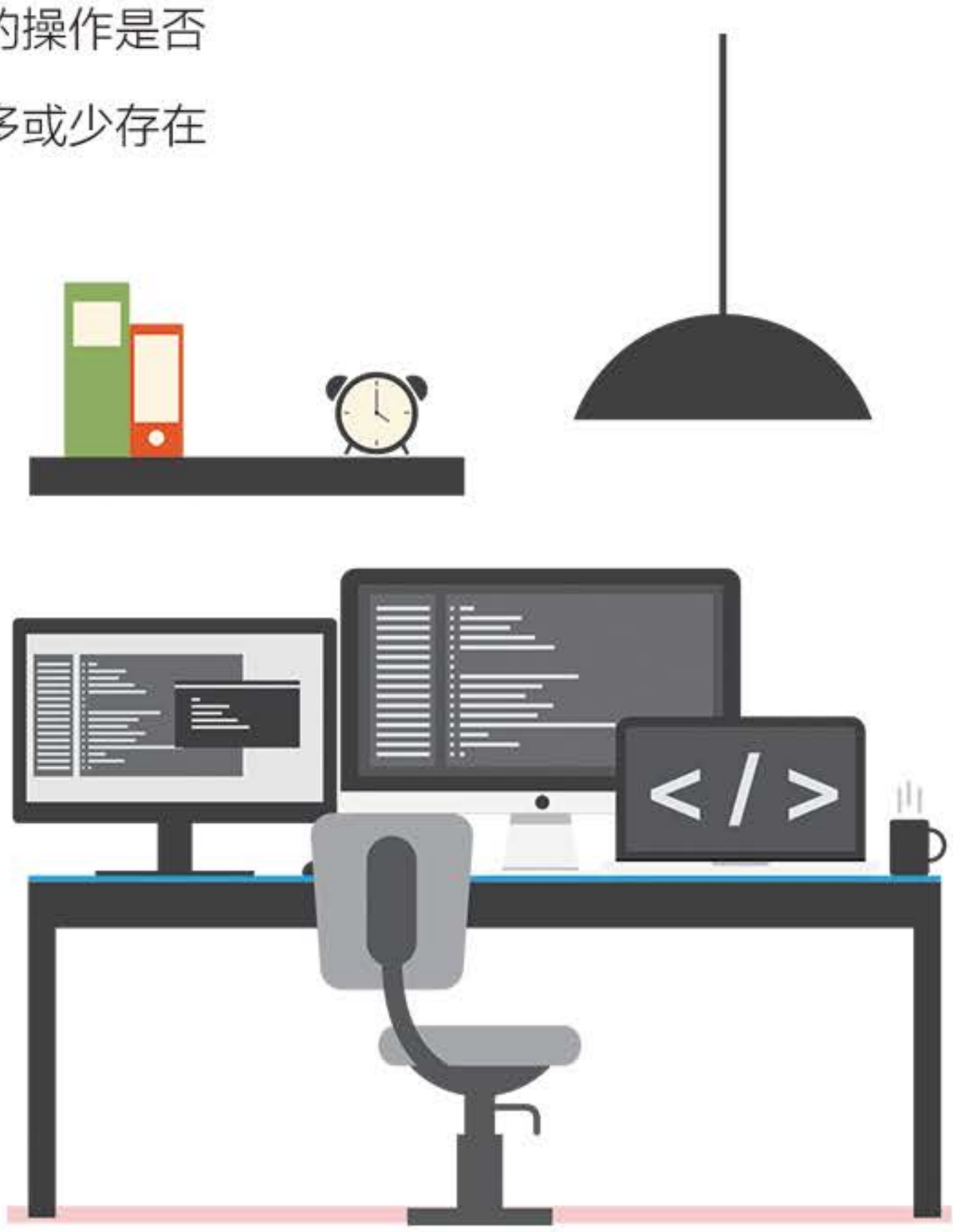
## 防范措施

- 设置禁止自动连接 Wi-Fi
- 拒绝连接来源不明的 Wi-Fi
- 使用安全防护软件检测 Wi-Fi
- 不使用陌生 Wi-Fi 进行网购等敏感操作
- 警惕同一地区多个相同或相似名字的 Wi-Fi

# 办公安全防护

## 三、办公设备安全

现代化办公时代，电脑、手机、平板、打印机、扫描仪等办公设备影响着我们工作的方方面面。然而，办公设备安全却成为了政企单位最担心的问题之一。理由很简单：员工在使用网络时缺乏一定的判断能力，不会考虑网络环境是否安全或进行的操作是否存在风险，操作办公设备时也或多或少存在可能造成办公威胁的不安全行为。



## 案例：黑客利用电脑漏洞植入病毒非法获利

不久前，某市公安局抓获一名利用电脑系统漏洞植入病毒进行非法获利的犯罪嫌疑人。据了解，该男子利用漏洞入侵了当地一些企业的计算机，这些被远程操控的计算机称为“肉鸡”，利用漏洞控制服务器后将服务器转变为一台挖矿的“肉鸡”，从而获得比特币等虚拟货币。据悉，该男子利用系统漏洞向 100 多台电脑植入了勒索病毒，而被侵入后，电脑实际使用者完全感知不到。

# 办公设备安全常见威胁

## 1 威胁一：使用已过时的系统

过时的系统或应用程序不仅会在功能和稳定性上大打折扣，还存在着很多安全漏洞，这些漏洞一旦被攻击者发现，很可能会被攻击者有目的地利用。

**措施：** 及时升级操作系统和各类软件安全补丁

## 2 威胁二：设置太简单的密码

政企单位的数据泄露事件中，很多都是由密码强度过弱或是密码被盗引起的。

**措施：** 采用复杂的密码设置

## 3 威胁三：连接不安全的网络

私自搭建无线热点或使用不安全的网络可能会导致信息泄露、流量劫持等风险。

**措施：** 使用单位提供的安全的网络接入方式

## 4 威胁四：下载不安全的程序

很多人喜欢在不安全的网站上下载“绿色版”、“破解版”的应用程序，这些程序可能被植入恶意后门，使网络安全遭受严重威胁。

**措施：** 选择官方渠道下载应用程序

## 5 威胁五：设备被盗或丢失

当办公设备被盗或丢失时，泄露个人及工作信息的风险非常高，即便设有密码，破解对于一名黑客而言也是轻而易举的。

**措施：** 妥善保管重要的办公设备

## 6 威胁六：打印机和扫描仪安全漏洞

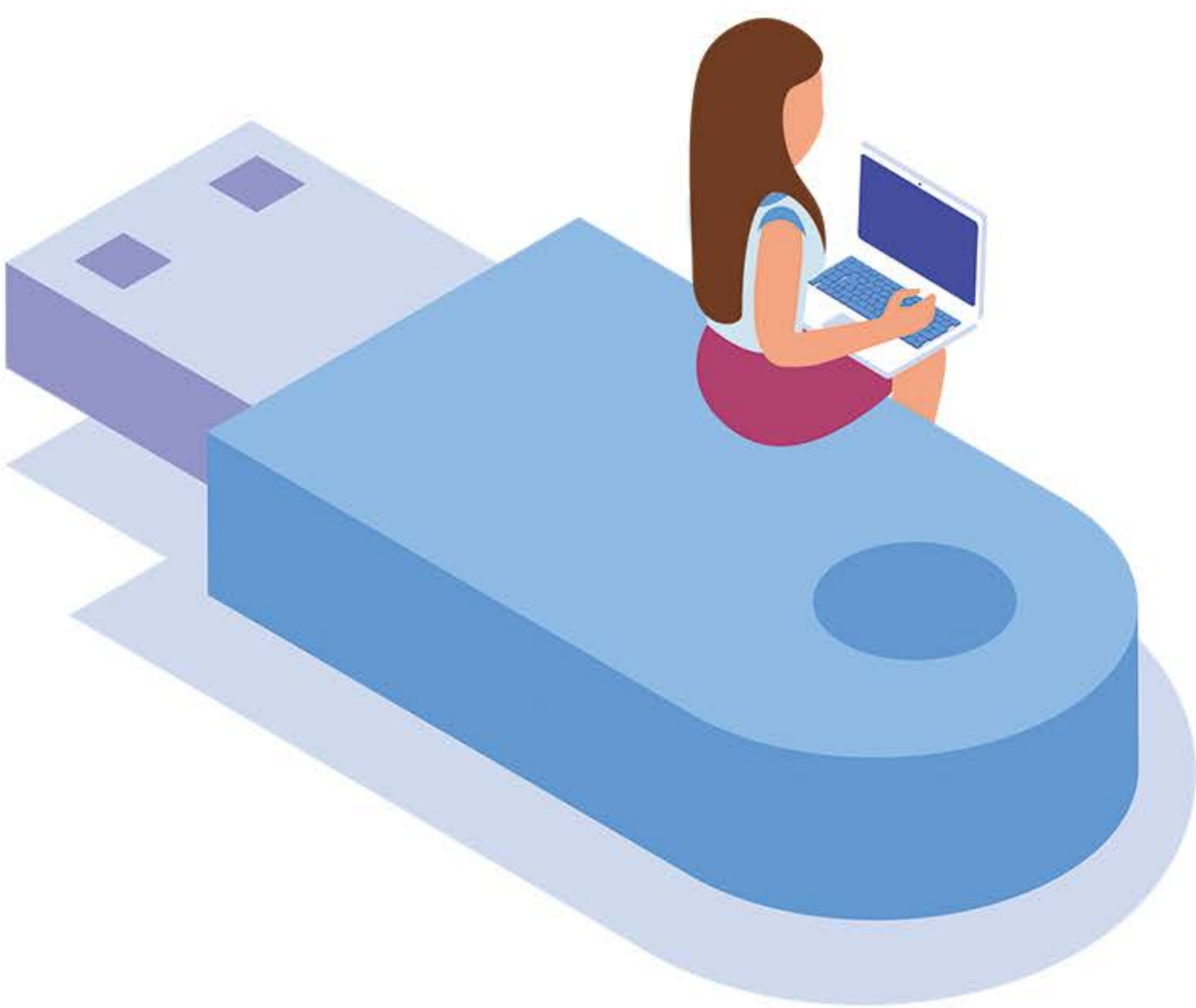
插在打印机、扫描仪上的 U 盘以及无人看管的纸质文件都是容易造成资料丢失、信息泄漏的安全隐患。

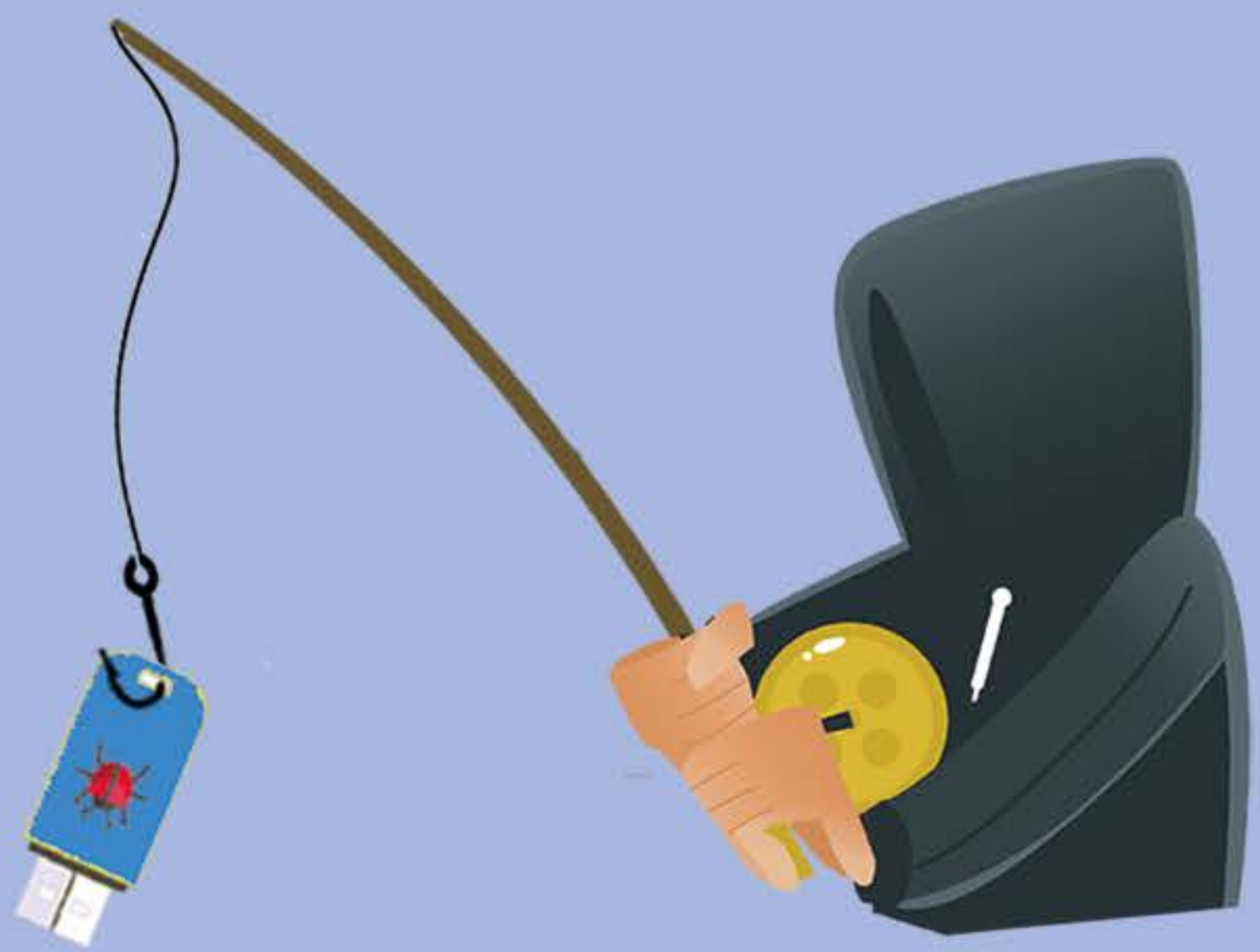

**措施：** 打印敏感文件应全程看护并及时取走

# 办公安全防护

## 四、存储介质使用安全

U 盘、移动硬盘、内存卡等存储介质作为移动办公数据存储的首选，得到了人们的广泛应用，大量的敏感信息、秘密数据和档案资料被存储在这些移动存储设备中。它们在为我们工作带来便利的同时，也带来了不容忽视的安全隐患。





## 案例：警惕移动存储介质成为泄密工具

董某是某高校的知名教授，从事涉密科研工作，平日里兢兢业业，经常在家熬夜加班。董某白天在单位用涉密电脑工作，晚上回家用互联网电脑接着工作，并且经常用U盘将未完成的工作，在两个电脑之间交叉拷贝。然而，董教授电脑中的涉密文件资料，却鬼使神差地“溜”进了互联网，造成了重大泄密，后经调查，是U盘感染病毒所致。

# 移动存储介质存在的安全隐患

作为档案资料保管的存储介质如果保管不善，很容易造成存储介质不能读取，信息不能复用，失去电子档案的保存价值。

## 隐患二
## 保管不当导致信息失效


很多人喜欢将U盘等移动存储介质随身携带并在不同环境下使用，造成单位资料和个人资料混杂在一起，当移动存储介质被借用时，存储在其中的一些重要信息存在泄露的隐患。

## 隐患四
## 公私混用

1 2 3 4 5

## 隐患一
## 体积小、易丢失

移动存储介质由于体积小、重量轻，很容易丢失。而移动介质本身往往没有任何防护措施，一旦丢失或被盗，就会造成大量信息外泄。

## 隐患三
## 病毒感染

在使用过程，如果不及时对移动存储介质查杀病毒，轻易将染毒文件通过单位内的办公设备打开，很容易将病毒传播到内网中，影响整个内部系统的运转。

## 隐患五
## 管理困难

很多单位缺少有效的管理监督机制，对移动存储介质的信息安全检查不到位，造成了很多安全隐患。

## 防范措施

- 保管好移动存储介质，防止被盗、丢失或损坏
- 移动存储介质应先杀毒、再使用
- 关闭移动存储介质的自动播放功能
- 不要使用私人存储介质拷贝、处理工作文件
- 文件若不再使用应及时清理
- 采取必要手段对敏感文件进行加密
- 合理管控移动存储介质的使用

# 办公安全防护

## 五、远程办公安全

新冠疫情的反反复复，改变了我们的生活节奏，也改变了我们的工作方式。远程办公已成为企业的常态，它不仅可以避免办公室人群聚集、交叉感染，还能让很多企业保持正常的运营状态。然而，伴随疫情出现的，可不只是远程办公带来的方便快捷，其中还隐藏着很多网络安全隐患。

## 案例：某职员违规处理文件遭严重处分

由于疫情原因，某单位职员小吴一直在家远程办公。一天，同事小李让小吴将某重要文件邮件发送给他，由于当时小吴忙于其他事务，为了图方便，他索性直接在微信上发送，没想到误发到了其他群组，发现时已无法撤回。此事件给该单位造成了很大的负面影响，不久后，小吴就因为泄露单位机密而遭到了严重处分。

# 远程办公四大网络安全隐患

1

## 隐患一：办公私人设备带来的安全防护隐患

- 带恶意程序的盗版软件
- 放任子女使用、下载不明程序

2

## 隐患二：家庭无线网络带来的网络攻击隐患

- Wi-Fi 密码过于简单
- 安全漏洞常年未修复

3

## 隐患三：即时通讯软件带来的文件传输隐患

- 文件本身没有加密，多次转发可能泄露
- 即时通讯软件可能存在安全漏洞

4

## 隐患四：网络社交媒体带来的数据泄露隐患


- 发布包含企业机密的动态信息
- 与人闲聊可能泄露企业机密

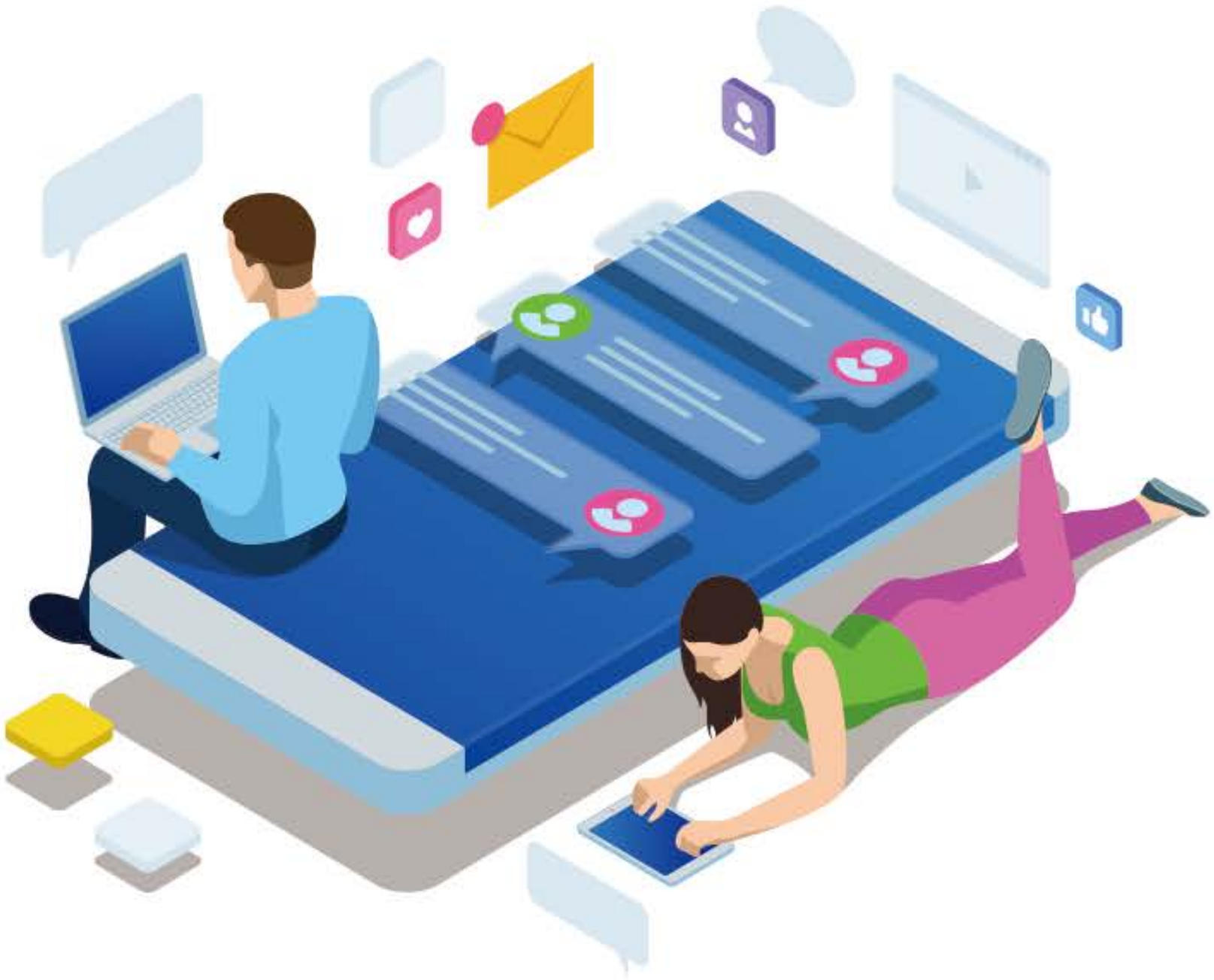
## 防范措施

- 使用已授权的终端设备开展工作
- 在正规网站下载正版软件
- 办公设备应限制他人使用
- 及时更新办公设备的系统和软件补丁
- 给家庭网络设置高强度密码
- 确保路由器软硬件的及时更新
- 使用企业级通讯软件传输重要文件
- 传输前应对文件进行加密保护
- 不要在社交媒体讨论、发布敏感信息

# 个人信息保护

## 一、社交网络安全

近几年，社交网络迅猛发展，互联网用户之间的信息交流方式发生了巨大改变，社交网络在人们的日常生活中发挥越来越重要的作用。与此同时，社交网络也面临着日益严重的安全威胁，成为互联网上的重点攻击目标。



1

## 案例一：女子社交网络寻真爱被骗万元

常女士经历过一次婚姻的失败，想通过网络寻找幸福，手机上无意中收到了一个“有缘婚恋网”就注册了，她给网名为“一起幸福”的网友留了自己的电话，但不久，对方称忙于开业，需要常女士以送花篮名义汇款。常女士分两次转账 7800 元和 8000 元后，对方竟消失不见，常女士这才意识到被骗。

## 案例二：游戏装备免费领？扫码解冻是陷阱！

2

钟先生是一名游戏玩家，周末在家打游戏时偶然加入了一个可以“免费领取游戏道具”的 QQ 群。在该 QQ 群内，一名“热心”的管理员给钟先生发来一个二维码，说扫码便可领福利，钟先生想都没想便使用微信扫码并填写了相关信息。当点击确认领取后，网页忽然显示微信被冻结，钟先生便联系管理员，对方告诉他因为其操作不当，导致微信被冻结，现需要缴纳一定费用进行解冻。钟先生便按照对方教的方法，先后向其指定账户转账 18000 元，随即对方就没有了消息，钟先生这才发现被骗。

# 社交网络存在的安全隐患

## 1 隐患一： 与陌生人聊天被骗钱财

很多不法分子通过微信、 QQ 等方式交友， 经过一段时间的交流取得受害人信任后， 以各种合理的理由骗取钱财。

## 2 隐患二： 社交媒体乱晒敏感信息

很多人喜欢在网上晒出行、 晒身份。 但是， 这些行为可能会间接泄露你的个人信息， 对自己和家人的财产乃至人身安全造成危害。

## 3 隐患三： 浏览不明网站

如果不法分子通过盗号或伪装成你的好友向你分享一个不明链接， 其背后或许隐藏恶意程序和木马，随意点击可能导致信息泄露或资金被盗。

## 防范措施

- 不要在社交网络上晒车票、 手机号等敏感信息
- 不要轻易添加陌生人聊天
- 不要对陌生人开放社交网络访问权限
- 非必要不开启位置定位服务

# 个人信息保护

## 二、购物网络安全

近年来，电子商务迅猛发展，网上购物已成为大众接受的消费方式。然而，人们在享受网上购物带来便利的同时，各种网络购物陷阱也随之而来。


## 案例： 收到网购退款通知 填资料导致盗刷

徐女士在淘宝购物后，收到一条看似淘宝系统发出的短信。短信内容称：徐女士的订单未生效，可以进行快捷退款。徐女士点开短信中的链接后看到一个退款界面，要求填写姓名、身份证号、储蓄卡卡号及银行预留手机等信息。徐女士在填写相关信息不久后，收到银行发来的扣款短信，短信显示自己的银行卡被扣款 3000 元。

# 网络购物五大陷阱


## 陷阱二
## 虚假广告

很多“黑店”通过制作虚假广告引诱买家下单，把钱骗到手后即关店，然后再开一个新店铺继续故技重施、坑蒙拐骗。


## 陷阱四
## 扫码支付

不法分子冒充卖家，向买家提供一个二维码骗其扫码支付。

1 2 3 4 5

## 陷阱一
## 低价诱惑

不法分子会通过朋友圈等方式，散布明显低于市场价的虚假购物链接，以引诱买家上当受骗。


## 陷阱三
## 钓鱼网站

不法分子以支付系统出问题为由，诱导买家登录到钓鱼网站，然后偷偷窃取买家的个人信息。

## 陷阱五
## 私下交易

不法分子诱骗买家私下交易“优惠多”，收到货款后立即将买家拉黑。

## 防范措施

- 不要轻信网上的低价推销广告
- 选择知名、权威的网购平台购物
- 网购时要注意商家的信誉、评价和联系方式
- 不要轻易提供个人的银行账号、密码和证件号码等敏感信息
- 填写支付信息时，应核实支付网站的真实性
- 不要随意访问未经核实的链接和二维码
- 不要私下直接与“卖家”一对一转账支付

# 个人信息保护

## 三、APP 安全

近年来，移动 APP 的种类和数量呈爆发式增长，人们的工作和生活也因此越来越便利。然而，越来越多的 APP 出现违法或恶意行为，引发了诸多安全威胁和风险，逐渐成为国家和社会的关注焦点。


## 案例：APP 向老人推送有欺骗套路的广告

不久前，70 多岁的李女士通过智能手机看新闻、小说时，手机屏幕总会自动蹦出一些“安全提示”：“病毒”“垃圾”“内存严重不足”，按照提示李女士清理了手机，但她发现这些“安全提示”越清理越多，手机越用越慢。后经调查发现，李女士手机里有一款“手机管家 PRO”APP，这款 APP 表面上看起来是在清理手机垃圾，背地里实则在不断偷偷大量获取手机里的信息。

# 恶意 APP 有哪些特征

## 1 特征一：违规收集信息

一些恶意 APP 为了更好地对用户进行行为分析，违规收集用户信息，给用户带来了极大的安全风险和隐患。

## 2 特征二：恶意吸费

一些恶意 APP 中内置了恶意扣费代码或者病毒，或是在用户容易“误点击”的位置放置扣费广告链接，用户很有可能就会因为踩中这样的“陷阱”而被扣费。

## 3 特征三：捆绑软件


一些恶意 APP 会强行捆绑推广其他应用软件，在用户不知情的情况下，自动下载推广软件。


4

## 特征四：过度索取授权

很多恶意 APP 会利用弹窗等手段，反复申请与当前服务场景无关的权限，用户如果拒绝，则无法使用 APP。

### 防范措施

- 通过正规渠道下载 APP
- 安装 APP 前应仔细阅读用户协议
- 关闭 APP 的敏感权限
- 慎重填写个人信息
- 使用安全的防病毒软件监控 APP 行为

# 个人信息保护

## 四、密码使用安全

网络时代，密码无处不在，小小的密码不仅守护着我们的隐私，还守护着我们的权益，密码越简单，意味着安全隐患就越大。

## 案例一：荷兰网络专家再次猜中特朗普的推特密码

不久前，美国前总统特朗普的推特密码再次遭到荷兰漏洞披露协会主席 Gevers 破解。早在 2016 年，Gevers 就成功猜到了特朗普的推特账户密码：youarefired（你被解雇了！特朗普的口头禅）。然而这么多年过去了，特朗普并没有吃一堑长一智，新密码 “maga2020”（maga 是特朗普的竞选口号）再次被人尽皆知。

## 案例二：微信商城密码被陌生人轻松破解

2021 年 6 月，高女士开设了微信商城，售卖纯手工食品。为方便操作，高女士将商城管理员的账号密码设置成了 “888”。既好记，寓意也好，但是这却给了投机分子可乘之机。没过几天，朱某某采用随机猜测管理员账户用户名及密码的方法，登录了高女士的管理员账户，随后向自己的账户虚拟充值人民币 25,000 元，并申请提现人民币 21,125 元。

# 弱密码有哪些特征

## 1 特征一：不够长度

密码长度少于 6 位很容易被人破解


## 2 特征二：不够复杂

组成元素单一，仅由数字或字母组成


## 3 特征三：不够个性

常见单词或键盘连续字母同样很容易被别人猜到

## 4 特征四：不够多样

多个账号、平台使用同一密码且长期不更换是大忌

# 如何保护密码安全


· 避开常见简单密码

· 重要密码要单独设置

· 不同平台使用不同密码

· 定期更换登录密码

· 开启登录短信提醒功能

· 采用多重验证的登录方式

· 使用专业软件系统地管理密码

# 密码设置五步走

确定一个足够的长度

一般要大于等于 8 位

选一个看似随机但方便记忆的基础密码如“首都网络安全日”字母缩写：sdwlaqr

加上数字可以让基础密码更强化，如 sdwlaqr2022

加上特殊字符，进一步强化，如 sdwlaqr*2022

使用大写进一步强化，如 SdwlaqR*2022

# 关注网络安全

企业介绍

美团

美团的使命是“帮大家吃得更好，生活更好”，公司聚焦“零售 + 科技”战略，和广大商户与各类合作伙伴一起，努力为消费者提供品质生活，推动商品零售和服务零售在需求侧和供给侧的数字化转型。

2018 年 9 月 20 日，美团正式在港交所挂牌上市。美团将始终坚持以客户为中心，不断加大在科技研发方面的投入，更好承担社会责任，更多创造社会价值，与广大合作伙伴一起发展共赢。

地址：北京市朝阳区望京东路 4 号恒电大厦 BC 座 100102

电话：010-10107888

公司网址：www.meituan.com

奇安信

新 一 代 网 络 安 全 领 军 者

奇安信科技集团股份有限公司成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，在人员规模、收入规模和产品覆盖度上均位居行业第一。

2019 年 5 月，中国电子以 37.31 亿元战略入股奇安信，奇安信正式成为网络安全国家队。2019 年 12 月，奇安信成为北京 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。2020 年 7 月 22 日，奇安信在科创板挂牌上市。2021 年，奇安信在〝中国网安产业竞争力 50 强〞榜单中排名第一，并被评为北京市第一批〝隐形冠军〞企业。2022 年 3 月 13 日，奇安信圆满完成了北京冬奥会和冬残奥会网络安全保障工作，兑现了北京冬奥网络安全〝零事故〞的承诺，为我国关键信息基础设施和重大活动的网络安全保障提供示范样本和有益经验。

地址：北京市西城区西直门外南路 26 号院 1 号楼

电话：95015

电子邮件：Kefu@qianxin.com

公司网址：https://www.qianxin.com

360政企安全

数 字 安 全 的 领 导 者

360 政企安全集团，是数字安全的领导者。过去 17 年专注为国家、城市、行业、企事业提供网络安全技术、产品和服务，是国内较早涉足 To G To B 领域的安全企业之一，目前已与众多部委、央企、大型金融机构、运营商以及上百万中小企业开展了网络安全合作。

360 政企安全集团基于十余年在安全大数据、知识库、安全专家方面的积累，已成为唯一掌握全网态势感知、唯一具有 17 年攻防实战经验的网络安全公司，同时也成为云端安全大脑为核心的数字安全能力体系创立者，帮助国家、城市、行业、企事业应对数字时代安全挑战。目前，这套体系服务于重庆、天津、青岛、鹤壁、苏州、郑州、上海、周口等城市的安全基础设施建设和运营，提升了我国应对高级威胁的安全能力。

地址：北京市朝阳区酒仙桥路 6 号院 360 大厦 100016

电话：010-58781000 / 13811381012

电子邮件：wangdan-ms@360.cn

公司网址：https://360.net/

智联招聘

智联招聘是中国领先的人力资本生态价值链平台，为用户的整个职业生涯提供相关职业及发展机会，帮助用户实现个人价值和目标。

智联招聘以覆盖求职者整个职业生涯为出发点，打造“3 的三次方”产品模型，即为学生、白领、高端（专业人士或管理人士），匹配 3 类产品：职业测评（我是谁）、招聘（我能干什么）、教育培训（我如何进步），并通过线上、线下、无线三个渠道，为职场人的全面发展打造平台。从而实现从“简历仓库”到“人才加工厂”的战略转型，为中国人才市场打造一个闭环生态链。

地址：北京市朝阳区望京阜荣街 10 号首开广场 5 层 100102

电话：010-58692828

电子邮件：bjzhaopin@zhaopin.com.cn

公司网址：https://www.zhaopin.com/

百度安全以 AI 为核心，以大数据为基础，是百度在互联网安全 20 多年实践的总结。首创了强对抗安全、非对抗安全、数据安全与隐私保护三大维度，能够提供安全产品和全方位的安全解决方案。

百度安全参与制订了 170 多项国际标准、国家标准、行业标准、团体标准等，通过了 CMMI5 全球最高等级认证。在最近 5 年的安全顶会中，论文发表数量在国内科技公司中位列第一。

地址：北京市海淀区上地十街 10 号百度大厦 2 层 100085

电话：010-59928888

公司网址：http://home.baidu.com

长亭科技
CHAITIN

北京长亭科技有限公司（简称长亭科技），是国内顶尖的网络信息安全公司，专注于为企业级用户提供高质量的网络信息安全解决方案。

长亭科技坚持以技术为导向，历经数年研发，在全球范围内，首发基于语义分析的非规则运算引擎，颠覆了传统 Web 应用层的安全防护原理，为企业用户带来更快、更精准、更智能的产品及服务。

公司拥有顶尖的安全研究和技术研发团队，专注于解决互联网安全问题，致力提高国内安全水平，接轨国际最高标准。

地址：北京市海淀区学院路甲 5 号 B 座 3 号门 100083

电话：4000-327-707 / 13488694145

电子邮件：info@chaitin.cn

公司网址：https://www.chaitin.cn/zh/

ThreatBook

# 微步在线

微步在线成立于 2015 年，创始团队是来自公安部第三研究所、亚马逊、微软、BAT 等国内外顶尖机构的网络安全技术专家。

公司是国家级“专精特新”小巨人企业，利用云计算、人工智能等技术，分析全球公开的网络大数据，以威胁情报云的形式提供专业的威胁检测产品与服务，目前完成了 E+ 轮融资，已成为中国信息安全领域威胁检测与响应的领军企业。

作为唯一一家连续四次入选 Gartner《全球威胁情报市场指南》的中国公司，微步在线打破了该领域西方公司统治的局面。基于对微步在线技术实力的认可，公司先后参与了新中国成立 70 周年、2022 北京冬奥、夏季达沃斯论坛、中国国际进口博览会等重要网络安保支撑工作。

地址：北京市海淀区苏州街盈智大厦 3 层 100080

电话：4000301051 / 18801442461

电子邮件：guanpujing@threatbook.cn

公司网址：https://www.threatbook.cn/

美团

# EAT BETTER
# LIVE BETTER

## 我们的使命

帮大家吃得更好，生活更好。

We help people eat better, live better.

美团App / 微信扫码

美团的使命是“帮大家吃得更好，生活更好”，公司聚焦“零售 + 科技”战略，和广大商户与各类合作伙伴一起，努力为消费者提供品质生活，推动商品零售和服务零售在需求侧和供给侧的数字化转型。2018年9月20日，美团正式在港交所挂牌上市。美团将始终坚持以客户为中心，不断加大在科技研发方面的投入，更好承担社会责任，更多创造社会价值，与广大合作伙伴一起发展共赢。

网址：**www.meituan.com**

美团网客服电话：**010-10107888**

## 首都公安组局反诈剧本杀，邀您上美团参与线下体验

北京市反电信网络诈骗犯罪中心

海淀区反电信网络诈骗犯罪中心

天火同人 作品
TianhuoTongren

美团App / 微信扫码

扫码线下体验

全民反诈App

《王诈》是在北京市反诈中心的指导下，由海淀区反诈中心、海淀派出所联合中国人民大学、天火同人公司共同创作的国内首部反诈剧本杀，该作品除了能借助各种辅助道具帮玩家快速进入角色，还能通过还原作案手法，让玩家了解骗子的各种套路，提高防骗意识。作为反诈宣传的突破与尝试，《王诈》在助力公安机关开展全民反诈教育的同时，还能带动社会力量积极参与，对宣传防范工作及行业良性发展都能起到一定的推动作用。

奇安信

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
# 网络安全零事故


## 奇安信圆满完成北京冬奥会及冬残奥会网络安全保障工作

### 冬奥会期间

**海量日志 严阵以待**

累计发现修复漏洞 **5782**个

日均监测日志超 **40亿**条

监测日志数量累计达 **1189亿**条

发现恶意样本数达 **54**条

排查风险主机 **150**条

累计监测到各类网络攻击超 **2.4亿次**（含社会面）

跟踪、研判、处置涉奥舆情和威胁事件 **105件**

**超凡投入 史无前例**

奥运史上首次系统性全局性网络安全规划

冬奥重保超 **800**天

网络安全专家 **3500**名

全国顶级白帽黑客 **数百**位

奇安信一线保障人员超 **600**名

**55款、813名网络安全设备全面覆盖**

**12**个 竞赛场馆

**26**个 非竞赛场馆

**188**个 服务场站

超**10000**台 终端

开通国内首个网络安全服务短号 **95015**

24小时提供覆盖全国的冬奥标准应急相应服务


奇安信 北京2022年冬奥会官方赞助商

95015 网络安全服务热线

新一代IT基础设施防护产品 | 大数据智能安全监测与管控产品 | 基础架构安全产品 | 新安全服务产品

公司地址 | 北京市西城区西直门外南路26号院1号楼

网站 | https://www.qianxin.com 邮箱 | Kefu@qianxin.com 邮政编码 | 100044

股票代码 688561

奇安信集团微信公众号

奇安信集团官网

INTRODUCE

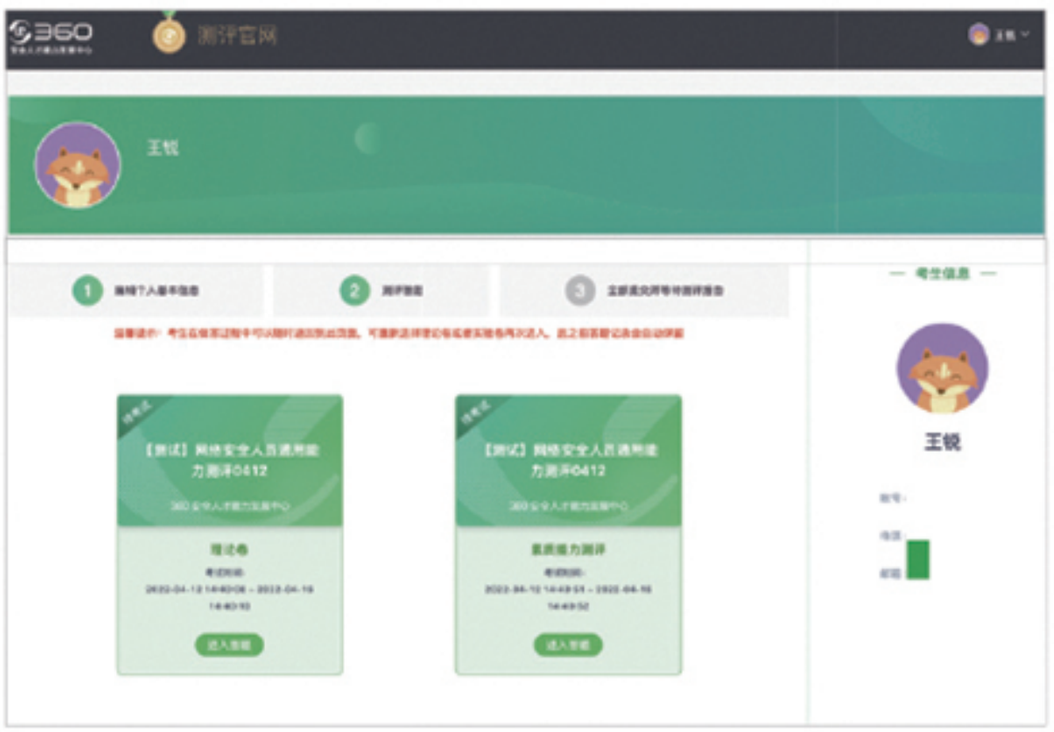
360 安全人才能力发展中心

**360 安全人才能力发展中心**（以下简称“中心”），是 360 政企安全集团旗下面向教育服务领域的官方机构，致力于为政府、企业、院校提供网络安全组织能力咨询、网络安全人才能力培养、人才能力评估和安全教育场景建设服务。

## 《网络安全人才能力发展白皮书》（2022版）即将发布

步入数字安全元年，中心将国内首个安全人才能力框架和职业指南——《网络安全人才能力发展白皮书》进行版本升级，重点优化网络安全专业领域及工作角色的归纳和分类，全面梳理了人才技能库、知识库和素养库，旨在更好的引领数字安全人才培养与发展。


## 网络安全人才能力评价平台即将上线





全面升级教育云平台，重磅打造“网络安全人才能力评价平台”，填补国内在网络安全行业人才评价方面的空白，结合学、测、评的持续迭代培养路径，将人才培养数据、测评数据、专业能力分析数据形成网络安全人才数据库，为人才职业路径发展和组织安全队伍建设提供强有力的数据支撑，有效实现从就业竞争力到职业竞争力的一站式贯通。

未来，360 安全人才能力发展中心将持续投入对数字安全领域人才发展与评估的深入研究，积极配合企业和组织完成数字安全人才能力标准建设，构建完整有效的数字安全人才培养方案。

扫码关注 了解详情

智联招聘

# 人力资本生态价值链平台

## 3的三次方

业内首创3的三次方概念：为职场人的全面发展打造平台，为中国人才市场打造人力资本生态。

- 3类用户：学生、白领、高端(专业人士或管理人士)
- 3类产品：测评(我是谁)、招聘(我能干什么)、教育培训(我如何进步)
- 3个渠道：线上、线下、无线


## 直播招聘 开启求职招聘新模式

直播招聘新产品上线，上智联靠谱人才视频见



国家网络空间安全基础能力的搭建者
Pioneer of National Cyberspace Security

EVERSEC 恒安嘉新

# 恒安嘉新(北京)科技股份公司

恒安嘉新是提供“云 - 网 - 边 - 端 - 用”综合解决方案的大数据智能运营运维产品，服务于产业互联网的科技工程企业。创立十余年来，始终专注于通信网和互联网数据智能分析领域，赋能智慧治理、智慧网络、智慧警务、智慧工业、智慧农业、智慧金融、智慧医疗、智慧教育等场景，为政企客户提供新一代网络信息安全、数据分析、智能业务应用解决方案和“管家式”运营运维服务。

**31** 省市
产品布局

**3000+** 个
核心网络结点

**500** Tnps
实时数据分析能力

**191** 项
计算机软件著作权

## 企业愿景

数据智能时代
基础能力的搭建者

## 价值观

成就客户、自我学习
结果导向、精诚团结
勇于创新、崇尚奋斗者

## 企业使命

让通信值得信赖
让数据和安全创造价值

## 公司主要客户

中华人民共和国工业和信息化部 | 中华人民共和国公安部 | 中华人民共和国国家安全部 | CNCERT/CC 国家互联网应急中心 | CNVD 国家信息安全漏洞共享平台 CHINA NATIONAL VULNERABILITY DATABASE

国家信息技术安全研究中心 National Research Center for Information Technology Security | CAICT 中国信通院 | 中国移动 China Mobile | 中国电信 CHINA TELECOM

China unicom 中国联通 | 中国交建 CHINA COMMUNICATIONS CONSTRUCTION | OTT 九度宽带 | 浩瀚深度 HAOHAN Data | SinoTelecom

北京市海淀区大钟寺东路9号京仪科技大厦D座5层，100086
010-62384566
www.eversec.com.cn

恒安嘉新官方公众号

扫一扫，开启阳光守护

2022 第9届
首都网络安全日
BEIJING CYBER SECURITY DAY

# NETWORK SECURITY

## 让网络更安全，让生活更美好

指导单位：北京市公安局 北京市互联网信息办公室

承办单位：中国电子国际展览广告有限责任公司

特别鸣谢：北京承制科技有限公司