

准备好应对

网络攻击

在过去十年中，网络攻击事件一直在上升。请了解如何保护自己免受金钱损失、个人信息被盗以及名誉和安全损害。



您知道吗...

2023 年，FBI 互联网犯罪投诉中心收到了超过 **880,000 起** 有关网络攻击的投诉，这些攻击造成 **125 亿美元的损失**。*



网络攻击是指试图访问或破坏设备的恶意行为。网络攻击者可能会窃取您的身份、实施欺诈、阻止您访问您的文档，并扰乱政府、企业和关键基础设施的运作。

保障自己免受网路攻击

- 用密码锁定所有电子设备。
- 设置软件和操作系统的自动更新。
- 使用防病毒解决方案、反恶意软件和防火墙来阻止威胁。
- 使用强密码（12 个以上字符，包含大小写字母、数字和特殊字符）。
- 不同的帐户，千万不要使用相同的密码。
- 使用双重身份验证。
- 提供个人信息前先确认合法性。
- 不要在不受信任的设备上保存登录凭据。
- 定期将重要文件备份到云端或外部硬盘。
- 定期检查您的金融账户对账单和信用报告。



- **公共无线网络不安全。**除非您使用 VPN，否则请勿在使用公共无线网络时登录银行或其他敏感网站。
- **更改家庭无线网络的默认名称和密码。**使用唯一的强密码，并定期更新。
- **在您的路由器上设置自动更新。**
- **为家用电器、汽车和玩具等设备创建访客无线网络，将它们与敏感数据分开。**

网络攻击发生时

- **注意异常活动：**
 - 信用卡扣款或拒绝交易
 - 信用报告上的异常账户
 - 您没有发布的社交媒体贴文
 - 有人收到了您从未发送过的电子邮件
- **断开互联网连接。**
- **更新您的安全软件，扫描并清理您的设备，或者关闭电源并将设备送至专业人员处。**
- **向学校和工作单位的 IT 部门报告异常活动。**
- **联系金融机构**（银行、信用卡公司、投资公司）。
- **告诉您的联系人**注意并删除您发送的可疑电子邮件或贴文。
- **重置您的密码。**

网络攻击发生后

- **如果有人非法使用您的社会保障号码：**
 - 请访问 identitytheft.gov 向联邦贸易委员会提交报告。
 - 如果您认为有人在使用您的社会保障号码，请拨打 1-800-908-4490 联系国税局 (IRS)。
- 请访问 [IC3.gov](https://ic3.gov) 向 **FBI 互联网犯罪投诉中心 (IC3)** 提交投诉。
- **了解更多提示和工具：**
 - StopThinkConnect.org
 - Ready.gov/cybersecurity