做好应对

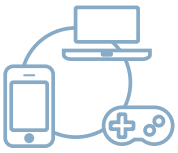
网络攻击准备

网络攻击可导致金钱损失、个人信息被盗，并损害您的声誉和安全。

FEMA

FEMA P-2257/2018 年 6 月

网络攻击是对损坏计算机系统的恶意尝试。



可使用电脑、手机、游戏系统和其他设备

可包括欺诈或身份盗窃

可阻止您访问或删除个人文件和图片

可能以儿童为目标

可能导致商业服务、交通和电力方面的问题

保护自己免受网络攻击

保持软件和操作系统为最新版本。

使用加密（安全）互联网通信。

使用强密码和双因素认证（两种验证方法）。

创建备份文件。

警惕可疑活动。如不确定，则勿点击。请勿提供个人信息。

保护您的家庭 Wi-Fi 网络。

网络攻击逼临时，
如何保持安全

保持您的防病毒软件更新。

使用强密码，具有12 个字符或更长。使用大小写字母、数字和特殊字符。每月更换密码。使用密码管理器。

使用更强的身份验证，例如只有您知道的 PIN 或密码。考虑使用可以接收代码或使用生物识别扫描的单独设备（例如指纹扫描仪）。

警惕以下可疑活动：要求您马上做某些事情、提供给您听起来好得难以置信的东西，或者需要您的个人信息。**点击前，请三思。**

定期查看您的账户报表和信用报告。

使用加密（安全）互联网通信。如果您将访问或提供任何个人信息，请使用带有 “HTTPS” 的网站。请勿使用证书无效的网站。使用创建安全连接的虚拟专用网络 (VPN)。

使用防病毒解决方案、防恶意软件和防火墙来拦截威胁。

定期备份您的文件。

限制您在网上所分享的个人信息。更改隐私设置，请勿使用定位功能。

定期变更网络管理和 Wi-Fi 密码来保护您的家庭网络。配置路由器时，选择 Wi-Fi Protected Access 2 (WPA2) 网络高级加密标准 (AES) 设置，这是最强的加密选项。

限制损害。警惕不明原因收费、您信用报告上的奇怪账户、信用卡意外被拒、帖子非您发表却出现在您的社交网络上，以及您没发电子邮件别人却收到。

立即更改您所有在线账户的密码。

对您的设备进行扫描和清理。

考虑关闭设备。将设备送至专业人员处 进行扫描和修复。

告知工作单位、学校或其他系统所有者。信息技术(IT) 部门可能需要警示他人，并升级系统.

联系银行、信用卡公司和其他金融账户。您可能需要对被攻击的账户进行冻结。关闭任何未经授权的信贷或收费账户。报告有人可能盗用您的身份。

如果您认为有人在使用您的社会安全号码，请向监察主任办公室 (OIG) 提交报告。**OIG 审查浪费、欺诈和滥用的案件。**要提交报告，请访问 www.idtheft.gov.

您也可以拨打社会保障局热线 1-800-269-0271。如需更多资源和更多信息，请访问 https://oig.ssa.gov/report 政府/报告。

向联邦调查局 (FBI) 互联网犯罪投诉中心 (IC3) 提出投诉，其网址为：www.IC3.gov。投诉将予以审查，并提交至适当的机构。

了解学习技巧、工具等，请访问，
www.stopthinkconnect.org.

FEMA

FEMA P-2257

主动掌控您的安全

请前往 **Ready.gov/zh-hans/cybersecurity。**请下载 **FEMA 应用程序**以获得更多有关准备应对**网络攻击**的信息。