JPMORGAN CHASE & CO.

网络安全

网络安全十大防范措施*

网络犯罪对全球各地的个人、家庭和企业无不持续构成严重威胁。为了避免遭受各种网络威胁攻击，甚至成为网络诈骗目标，培养良好的上网习惯成为我们日常生活中不可或缺的一部分。

立即行动，刻不容缓。请尽快采取下列网络安全防范措施：

网络安全 10 大防范措施

1. 为工作、个人用途、提醒通知、AI 工具等分别建立电子邮件账户
2. 点击发送给您的电子邮件或短讯中包含的链接或附件时，必须三思而后行
3. 透过电子邮件或短讯传送敏感资料时，必须加密并使用安全的讯息工具
4. 创建复杂的长密码，并且定期更改
5. 切勿多个账户使用相同的密码
6. 切勿使用不安全的公共网络
7. 只要有提供，都要使用多因素验证
8. 在家里设置一个主网，并为访客、子女和智能设备单独设网
9. 在所有设备安装防毒软件，并且保持更新至最新版本
10. 通过社交媒体及 AI 工具分享有关自己、家庭、工作或业务方面的资料时应加倍审慎

电子邮件

- ✓ 使用单独电子邮件账户：分别为工作、个人用途、用户 ID、提醒通知和 AI 工具创建单独的电子邮件账户
- ✓ 选择可提供垃圾邮件过滤和多因素身份验证的知名电子邮件服务供应商
- ✓ 在与经过验证的财务或个人资料请求进行通讯时，加密并使用安全的讯息工具
- ✗ 切勿点击发件人不明的链接或附件；警惕垃圾邮件及钓鱼邮件

密码

- ✓ 创建复杂此长密码；应使用由数字、大小写字母和特殊字符混合组成的密码
- ✓ 每年多次更换密码
- ✓ 考虑使用密码管理工具
- ✗ 切勿多个账户使用相同的密码
- ✗ 切勿点击您访问的网站上的「记住我的密码」或「记住我」功能

互联网使用

- ✓ 只从可信来源下载软件
- ✓ 完全退出网站，而非只是关闭会话窗口
- ✓ 寻找 https:// 网址进行安全会话验证
- ✓ 尽可能启用私密浏览功能
- ✓ 定期删除 Cookies
- ✗ 切勿点击来源不明或不可信来源上的链接
- ✗ 切勿允许电子商务网站储存您的信用卡资料
- ✗ 切勿点击弹出窗口将其关闭；必须使用屏幕右上角的「X」按钮

移动设备及应用程序

- ✓ 经常保持锁屏；选择高强度密码，尽可能使用生物识别工具
- ✓ 定期检查您的隐私、位置和密码设置
- ✓ 定期更新应用程序（例如安全补丁）
- ✓ 留意应用程序可访问资料的权限，定期检查授权情况
- ✓ 不需使用时，必须关闭蓝牙功能
- ✓ 确保应用程序设置为保存数据“仅在使用中允许”或“仅联系人”
- ✓ 妥善备份个人资料
- ✓ 在设置中开启远程自动删除功能，以确保一旦丢失有关设备时可以自动删除您的个人资料
- ✗ 警惕点击社交媒体、互联网等的广告

病毒和恶意软件防护

- ✓ 安装并随时更新所有设备上的杀毒和广告拦截软件
- ✓ 不时更新软件、浏览器和操作系统
- ✓ 定期备份您的数据
- ✗ 切勿安装或使用盗版软件

家用网络

- ✓ 设置一个只供自己使用的网络，并且为访客、子女和智能设备另建一个网络
- ✓ 修改您的无线网络的默认密码
- ✓ 开启路由器的加密和防火墙功能
- ✓ 透过路由器软件为您的主网络名称 (SSID) 考虑开启「不允许广播」选项
- ✗ 切勿使用预设的路由器名称 / 密码

公共 Wi-Fi / 热点

- ✓ 无法避免使用公共 Wi-Fi 时，应使用虚拟私人网络 (VPN)，这有助保护您的会话安全性并将其加密
- ✓ 关闭自动加入非首选网络功能
- ✓ 关闭文件分享功能，仅在必要时方才使用
- ✓ 停用允许计算机之间及移动设备之间进行直接传输的临时组网
- ✗ 切勿使用公共 Wi-Fi 在网站上输入个人登录信息；黑客可以捕获您的击键

社交工程及隐私

- ✓ 透过其他渠道，核实要求您提供信息、或访问您的数据或设备的请求者身份
- ✓ 限制您在网上发布的个人资料信息，如位置、旅行计划、交易等
- ✓ 检查社交媒体平台上的隐私设置；少分享
- ✓ 警惕放到 AI 工具的数据，因这可能对造成您不利
- ✗ 切勿开启您并非预期收到、由熟人发送的附件；应先致电核实后才点击
- ✗ 切勿仅因为请求者知道您或您公司的信息便假设有关请求真实无讹
- ✗ 在保护您的网上账户时，切勿使用在社交媒体上可广泛获取的个人信息（例如宠物的名称、子女的生日等）

挑选服务、软件和设备时，应考虑下列因素：

	需要具备的功能	
密码管理器 网络漏洞源自个人如何选择和管理密码的方式，这可能使得黑客轻而易举地便可以获取您的密码，入侵个人账户。 密码管理工具可以帮助用户储存和整理密码，甚至可以提供例如表单填写和密码生成等额外功能。	**加密** 应采用至少 256 位 AES 加密方式来储存密码 **密码生成器** 可以自动生成复杂的高强度密码	**同步处理** 密码管理器允许从任何地方进行安全访问，并进行跨设备的同步 **多因素身份验证** 提供多因素身份验证
	寻找一款可支持您所使用浏览器、操作系统和移动设备的密码管理工具	
虚拟私人网络 (VPN) VPN 是一种可以为您的网上活动提供防护的数字方式，情况犹如您在 ATM 提款机上用手遮挡输入的 PIN 码一样。VPN 加密为设备与网络之间的敏感数据传输提供保护。 当您通过公共网络、出行时或不安全的 Wifi 网络使用个人设备时，这种防护方式尤其适合。	**资料保存** 选择不保留数据记录或网络浏览记录的供应商 **代码混淆器** 供应商应在多个不同国家 / 地区设有服务器，以便由此分配的 IP 地址难以追踪您的位置所在	**兼容性** 可以安装在桌上计算机、平板计算机和移动设备 **信誉可靠** 选择过往记录和表现稳定可靠，并且专注于网络安全和使用便利性的知名供应商
	应清楚明白到 VPN 不能保护您免受病毒攻击。此外，一些国家政府可能禁止使用 VPN。出行前应先行了解清楚。	
病毒和恶意软件防护 当您使用计算机或移动设备进行银行业务、购物、收发电子邮件和即时讯息，但却没有采取足够的防范措施，那么您成为网络攻击受害者的风险就会较高。 运行实时防毒产品，并且保持更新至最新版本，对于降低恶意软件攻击风险至关重要。 移动设备应安装病毒及恶意软件防护软件。	**侦测** 应该可侦测恶意软件的现有和新变种版本。 **清除** 有效隔离或删除被感染设备上的恶意软件。 **保护** 通过主动预防恶意软件感染而保持系统的良好运作。	**性能** 不会降低您的系统运行速度。 **家长监控** 可选功能，当子女使用移动设备时帮助您对内容设限。 **备份** 可选备份保护，以防系统发生故障。
	应考虑每个供应商允许您购买的每个杀毒产品可安装软件的设备上限。	
无线路由器 无线路由器可以将设备连接至互联网，并与其他联网设备通讯。 路由器就像计算机一样，具备自己的操作系统、软件和漏洞。如果黑客入侵了您的路由器，他们就可以访问您的文件、记录击键、登入您的账户、感染您的联网设备。	**自动更新** 选择可自动更新软件（即固件）的路由器。 **防火墙** 可以保护您的网络免遭入侵。	**访客网络** 可以为访客、子女和智能设备设置单独安全的网络和登录讯息。
	路由器的覆盖范围必须配合您的家居面积，并且支持您希望联网的设备数量。	

* 本文仅供教育和参考之用，无意对本文所讨论之主题每个方面均面面俱到，不应对其加以如此的依赖。本文所提供的信息旨在帮助客户防范网络诈骗，并不提供形形色色的网络诈骗活动的完整清单，且并未提出所有类型的最佳网络安全实践。您、您的公司或组织负责决定如何以最佳方式防范网络诈骗活动以及选择最适合您需求的最佳网络安全实践。严禁任何人士或任何实体复制、转发、分发或未经授权而使用本文件或其中所含信息。

© 2024 年。摩根大通。保留所有权利。