网络安全重要提示*

网络犯罪仍然对全球的个人、家庭和企业构成威胁，因此，将良好的网络实践纳入我们的日常活动中，以避免各种网络威胁和潜在的欺诈行为至关重要。

如果您还没有，请尽快实施这些保障措施：

10 个关键网络安全提示

1. 为工作、个人使用、警报通知和其他兴趣创建单独的电子邮件帐户
2. 谨慎点击电子邮件或短信中发送给您的链接或附件
3. 通过电子邮件或短信传输敏感信息时使用安全消息工具
4. 创建强密码并定期更改
5. 不要对多个帐户使用相同的密码
6. 尽量减少使用不安全的公共网络
7. 在工作中，将网络使用限制在核心业务相关网站
8. 在家里，建立一个主网络以及一个单独的供客人、儿童和智能设备使用的网络
9. 在您的所有设备上安装防病毒软件并保持其最新状态
10. 谨慎对待您通过社交媒体分享的有关您自己、家人、工作或业务的内容

电子邮件

- ✓ 使用单独的电子邮件帐户用于工作、个人使用、用户 ID、警报通知、其他兴趣
- ✓ 选择信誉良好，提供垃圾邮件过滤和多因素身份验证的电子邮件供应商
- ✓ 回复已验证的财务或个人信息请求时使用安全消息工具
- ✓ 在通过电子邮件发送重要文件之前对其进行加密
- × 请勿打开来自未知发件人的电子邮件

密码

- ✓ 创建至少 10 个字符的复杂密码；使用数字、大写和小写字母以及特殊字符的组合
- ✓ 每年至少更改四次密码
- ✓ 考虑使用密码管理工具
- × 请勿对多个帐户使用相同的密码
- × 请勿勾选您访问的网站上的“记住我的密码”或“记住我”

互联网的使用

- ✓ 仅从可信来源下载软件
- ✓ 退出站点，而不是简单地关闭会话窗口
- ✓ 寻找带有 https://使用安全会话验证的网址
- ✓ 尽可能启用无痕浏览
- ✓ 定期删除 Cookie
- × 请勿点击未知或不可信来源的链接

- ✗ 不允许电子商务网站存储您的信用卡信息
- ✗ 请勿点击弹出窗口将其关闭；而是使用屏幕右上角的“X”

移动设备

- ✓ 保持屏幕锁定；选择强密码并使用可用的生物识别工具
- ✓ 选择具有防盗功能的设备
- ✓ 不需要时关闭蓝牙
- ✓ 定期更新应用程序（例如安全补丁）
- ✓ 安全地备份您的数据
- ✓ 查看您的隐私、位置和密码设置
- ✓ 注意应用程序可以访问的信息并定期查看权限
- ✓ 在设置中启用远程自动擦除功能，以确保如果您将设备报告为丢失，您的个人信息会自动擦除
- ✗ 上网时不要点击广告

病毒和恶意软件保护

- ✓ 安装防病毒和广告拦截软件并使其保持最新
- ✓ 使软件、浏览器和操作系统保持最新
- ✓ 定期备份您的数据
- ✗ 请勿安装或使用盗版软件
- ✗ 请勿安装文件共享程序
- ✗ 请勿将电子邮件设置为自动打开附件

家庭网络

- ✓ 为您自己创建一个网络，为宾客、儿童和智能设备创建另一个网络
- ✓ 更改无线网络的默认密码
- ✓ 打开路由器的 WPA2 加密和防火墙
- ✓ 通过路由器软件在您的主网络名称 （SSID） 上启用“请勿广播”
- ✗ 请勿使用默认路由器名称/密码

公共 Wi-Fi/热点

- ✓ 尽量减少使用不安全的公共网络
- ✓ 关闭与非首选网络的自动连接
- ✓ 关闭文件共享
- ✓ 如果无法避免公共 Wi-Fi，请使用虚拟专用网络 （VPN） 来帮助保护您的会话
- ✓ 禁用临时网络，它允许直接从计算机到计算机的传输
- ✗ 切勿使用公共 Wi-Fi 在网站上输入个人凭据；黑客可以捕获您的击键

社会工程

- ✓ 如有人请求信息或访问您的数据或设备，请通过其他经过验证的方法来确认此人的身份
- ✓ 限制您在网上发布的个人信息的数量

- ✓ 查看社交媒体帐户的隐私设置
- × 请勿打开您认识的人的邮件的附件，如果您并不预料会从此人处收到邮件；请在点击之前致电确认
- × 不要仅仅因为请求者知道有关您或您的公司的信息而假设请求是真实的
- × 请勿使用社交媒体上广泛提供的个人信息（宠物姓名、孩子的出生日期）来保护在线帐户

当您选择服务、软件和设备时，请考虑以下事项：

	需要寻找的功能	
密码管理器 弱点来源于个人如何选择和管理密码，这可以使黑客很容易地访问它们并破解个人帐户。 密码管理工具可帮助用户存储和组织密码，甚至可以提供附加功能，例如表格填写和密码生成。	**加密** 存储的密码应至少使用 256 位 AES 加密。 **密码生成器** 可以自动生成强而复杂的密码。	**同步** 密码管理器应允许从任何地方进行安全访问，并跨设备同步。 **多因素身份验证** 提供多因素身份验证。
	寻找支持您使用的浏览器、操作系统和移动设备类型的密码管理工具。	
虚拟专用网络（VPN） VPN 是一种数字方式来保护您的活动，就像用您的手在 ATM 上覆盖您的 PIN 输入一样。VPN 可防止通过查看或跟踪您的通信内容的窥探行为。 在使用公共、旅行或不安全的 Wifi 网络时，在个人设备上使用这一点尤为重要。	**数据保留** 寻找不保留您的数据日志或 Web 流量的供应商。 **模糊化** 供应商应在多个国家/地区拥有服务器，以使您的 IP 分配不容易被追溯到。	**兼容性** 能够在台式机、平板电脑和移动设备上安装。 **声誉** 信誉良好的供应商需要拥有可靠的业绩记录，并专注于安全性和易用性。
	请了解 VPN 不会保护您免受病毒侵害。此外，某些政府可能禁止使用 VPN。请在旅行前自行了解。	
病毒和恶意软件保护 如果您使用计算机或移动设备上网、购物、银行、电子邮件和即时通讯，并且没有足够的保护，则您成为受害者的风险更高。 运行实时防病毒产品并保持其最新是降低恶意软件风险的重要步骤。	**检测** 应检测恶意软件的现有和新变体。 **清除** 从受感染的设备中有效隔离或删除恶意软件。 **保护** 通过主动预防恶意感染，帮助维持健康的系统。	**性能** 不会减慢你的系统。 **家长控制** 当儿童使用设备时，有帮助限制内容的可选功能。 **备份** 系统故障时的可选备份保护。
	考虑每个供应商允许每次购买许可订购时安装软件的设备数量。	

无线路由器 无线路由器允许您将设备连接到互联网，并与网络上的其他设备通信。 路由器就像计算机，有自己的操作系统、软件和漏洞。如果黑客获得了您的路由器访问权限，他们就可以访问您的文件，记录击键，访问您的帐户，并可以感染您网络上的设备。	**自动更新** 选择自动更新其软件的路由器，也称为固件。 **防火墙** 保护您的网络免受入侵者的影响。 **寻找一个适合您家庭大小的路由器，并支持您想要连接到它的设备数量。**	**访客网络** 允许为访客、儿童和智能设备提供独立且安全的网络和凭据
