English → Chinese (Simplified)

微软错误导致机密邮件泄露给人工智能工具 Copilot

两天前

分享 节省

莉芙·麦克马洪
科技记者

盖蒂图片社

微软承认其人工智能工作助手出现错误，导致其误访问并汇总了一些用户的机密电子邮件。

这家科技巨头一直大力推广 Microsoft 365 Copilot Chat，将其作为企业及其员工使用其生成式 AI 聊天机器人的安全方式。

但该公司表示，最近出现的一个问题导致该工具向一些企业用户显示了存储在其草稿和已发送邮件文件夹中的消息信息，包括标记为机密的消息。

微软表示，已推出更新来修复该问题，并且“没有向任何人提供他们未经授权查看的信息”。

然而，一些专家警告说，各公司竞相添加新的人工智能功能的速度意味着这类错误是不可避免的。

Copilot Chat 可在 Microsoft 程序（如 Outlook 和 Teams）中使用，用于电子邮件和聊天功能，以获取问题的答案或总结消息。

微软发言人告诉 BBC 新闻：“我们发现并解决了一个问题，即 Microsoft 365 Copilot Chat 可能会返回用户在 Outlook 桌面的草稿和已发送邮件中标记为机密的电子邮件的内容。”

他们补充说：“虽然我们的访问控制和数据保护策略仍然有效，但这种行为并不符合我们预期的 Copilot 体验，该体验旨在将受保护的内容排除在 Copilot 访问之外。”

“我们已在全球范围内为企业客户部署了配置更新。”

科技新闻媒体**Bleeping Computer**最先报道了这一失误，并表示他们看到了一条服务警报，证实了这一问题。

它引用了微软的一份通知，称“带有机密标签的用户电子邮件正在被 Microsoft 365 Copilot 聊天错误处理”。

该通知还补充说，Copilot Chat 中的工作选项卡会汇总存储在用户草稿和已发送文件夹中的电子邮件，即使这些邮件已设置敏感标签并配置了数据丢失防护策略以防止未经授权的数据共享。

有报道称，微软最早于1月份发现了这个错误。

该漏洞的通知也发布在英格兰 NHS 工作人员的支持仪表板上——其根本原因归咎于“代码问题”。

英国国家医疗服务体系 **(NHS) IT** 支持网站上的通知部分内容暗示其已受到影响。

但该公司告诉 BBC 新闻，Copilot Chat 处理的任何草稿或已发送电子邮件的内容都将保留在其创建者手中，患者信息并未泄露。

数据泄露将会发生

面向拥有 Microsoft 365 订阅的组织的 Microsoft 365 Copilot Chat 等企业级 AI 工具，通常具有更严格的控制和安全保护措施，以防止敏感企业信息的共享。

但对一些专家来说，这个问题仍然凸显了在某些工作环境中采用生成式人工智能工具的风险。

Gartner 的数据保护和人工智能治理分析师 Nader Henein 表示，“鉴于人工智能新功能的频繁发布，这种失误是不可避免的”。

他告诉 BBC 新闻，使用这些人工智能产品的机构往往缺乏保护自身和管理每个新功能所需的工具。

“在正常情况下，各组织会直接关闭该功能，然后等待相关管理措施跟上，”Henein说道。

“不幸的是，铺天盖地的未经证实的AI炒作所造成的压力，使得这几乎不可能实现，”他补充道。

萨里大学网络安全专家艾伦·伍德沃德教授表示，这表明将此类工具默认设置为私密且仅限选择加入的重要性。

“这些工具不可避免地会出现漏洞，尤其是在它们以惊人的速度发展的情况下，所以即使数据泄露可能并非有意为之，但它仍然会发生，”他告诉 BBC 新闻。

亚马逊股价下跌，此前该公司加入大型科技公司人工智能领域的投资热潮。
Xbox制作人告诉员工，要利用人工智能来减轻失业带来的痛苦。
微软推出人工智能截图工具，被指“隐私噩梦”

Tech Decoded
The world’s biggest tech news in your inbox