# May error sa Microsoft na nagpapakita ng mga kumpidensyal na email na nalantad sa AI tool na Copilot

2 araw na ang nakalipas



**Liv McMahon**

Tagapagbalita ng teknolohiya


Mga Larawan ng Getty

Kinilala ng Microsoft ang isang error na naging dahilan kung bakit hindi sinasadyang na-access at naibubuod ng AI work assistant nito ang mga kumpidensyal na email ng ilang user.

Itinulak ng higanteng teknolohiya ang Microsoft 365 Copilot Chat bilang isang ligtas na paraan para sa mga lugar ng trabaho at kanilang mga kawani na gamitin ang generative AI chatbot nito.

Ngunit sinabi nito na isang kamakailang isyu ang naging dahilan upang maglabas ang tool ng impormasyon sa ilang mga enterprise user mula sa mga mensaheng nakaimbak sa kanilang mga draft at mga ipinadalang email folder - kabilang ang mga minarkahan bilang kumpidensyal.

Sinabi ng Microsoft na naglabas na ito ng update upang ayusin ang isyu, at "hindi ito nagbigay sa sinuman ng access sa impormasyong hindi pa nila awtorisadong makita".

Gayunpaman, nagbabala ang ilang eksperto na ang bilis ng pakikipagkumpitensya ng mga kumpanya upang magdagdag ng mga bagong tampok ng AI ay nangangahulugan na ang ganitong uri ng mga pagkakamali ay hindi maiiwasan.

Maaaring gamitin ang Copilot Chat sa mga programa ng Microsoft tulad ng Outlook at Teams, na ginagamit para sa mga email at mga function ng chat, upang makakuha ng mga sagot sa mga tanong o ibuod ang mga mensahe.

"Natukoy at natugunan namin ang isang isyu kung saan maaaring magbalik ang Microsoft 365 Copilot Chat ng nilalaman mula sa mga email na may label na kumpidensyal na isinulat ng isang user at nakaimbak sa loob ng kanilang Draft at Sent Items sa Outlook desktop," sinabi ng isang tagapagsalita ng Microsoft sa BBC News.

"Bagama't nanatiling buo ang aming mga kontrol sa pag-access at mga patakaran sa proteksyon ng data, ang pag-uugaling ito ay hindi nakamit ang aming nilalayon na karanasan sa Copilot, na idinisenyo upang ibukod ang protektadong nilalaman mula sa pag-access ng Copilot," dagdag nila.

"Isang update sa configuration ang naipatupad sa buong mundo para sa mga enterprise customer."

Ang pagkakamali ay unang iniulat ng tech news outlet **na Bleeping Computer** , na nagsabing nakakita ito ng isang service alert na nagkukumpirma sa isyu.

Binanggit nito ang isang abiso ng Microsoft na nagsasabing "ang mga mensaheng email ng mga user na may nakalagay na kumpidensyal na label ay hindi wastong pinoproseso ng Microsoft 365 Copilot chat".

Idinagdag sa abiso na ang isang work tab sa loob ng Copilot Chat ay nagbubuod ng mga mensaheng email na nakaimbak sa mga draft at ipinadalang folder ng isang user, kahit na mayroon itong sensitivity label at patakaran sa pag-iwas sa pagkawala ng data na naka-configure upang maiwasan ang hindi awtorisadong pagbabahagi ng data.

Ayon sa mga ulat, unang nalaman ng Microsoft ang error noong Enero.

Ang abiso nito tungkol sa bug ay ibinahagi rin sa isang support dashboard para sa mga manggagawa ng NHS sa England - kung saan ang ugat ng sanhi ay iniuugnay sa isang "isyu sa code".

Ang isang seksyon ng **abiso sa site ng suporta sa NHS IT** ay nagpapahiwatig na naapektuhan ito.

Ngunit sinabi nito sa BBC News na ang nilalaman ng anumang draft o ipinadalang mga email na pinoproseso ng Copilot Chat ay mananatili sa kanilang mga tagalikha, at ang impormasyon ng pasyente ay hindi pa ibinubunyag.

## 'May mangyayaring pagtagas ng datos'

Ang mga tool para sa enterprise AI tulad ng Microsoft 365 Copilot Chat – na available sa mga organisasyong may subscription sa Microsoft 365 – ay kadalasang may mas mahigpit na mga kontrol at proteksyon sa seguridad upang maiwasan ang pagbabahagi ng sensitibong impormasyon ng korporasyon.

Ngunit para sa ilang eksperto, itinatampok pa rin ng isyu ang mga panganib ng pag-aampon ng mga generative AI tool sa ilang partikular na kapaligiran sa trabaho.

Sinabi ni Nader Henein, analyst ng data protection at AI governance sa Gartner, na "hindi maiiwasan ang ganitong uri ng pagkakamali", dahil sa dalas ng paglalabas ng "mga bago at nobelang kakayahan sa AI".

Sinabi niya sa BBC News na ang mga organisasyong gumagamit ng mga produktong AI na ito ay kadalasang kulang sa mga kagamitang kailangan upang protektahan ang kanilang sarili at pamahalaan ang bawat bagong tampok.

"Sa ilalim ng normal na mga pangyayari, papatayin lang ng mga organisasyon ang tampok na ito at maghihintay hanggang sa makahabol ang pamamahala," sabi ni Henein.

"Sa kasamaang palad, ang dami ng presyur na dulot ng pagdagsa ng walang-patunay na hype tungkol sa AI ay halos imposibleng mangyari," dagdag niya.

Sinabi ng eksperto sa cyber-security na si Propesor Alan Woodward ng University of Surrey na ipinakita nito ang kahalagahan ng paggawa ng mga naturang tool na pribado-by-default at opt-in lamang.

"Hindi maiiwasang magkakaroon ng mga bug sa mga tool na ito, lalo na habang sumusulong ang mga ito sa napakabilis na bilis, kaya kahit na maaaring hindi sinasadya ang pagtagas ng data, mangyayari pa rin ito," sinabi niya sa BBC News.

**Bumagsak ang mga share ng Amazon habang sumasali ito sa paggastos ng Big Tech AI**
**Sinabihan ng prodyuser ng Xbox ang mga kawani na gumamit ng AI upang maibsan ang sakit ng pagkawala ng trabaho**
**Inilunsad ng Microsoft ang AI screenshot tool na tinaguriang 'privacy nightmare'**