மைக்ரோசாப்ட் பிழை, ரகசிய மின்னஞ்சல்கள் AI கருவி கோபிலட்டுக்கு வெளிப்படுவதைக் காண்கிறது.

2 நாட்களுக்கு முன்பு

லிவ் மெக்மஹோன்
தொழில்நுட்ப நிருபர்

கெட்டி இமேஜஸ்

மைக்ரோசாப்ட் தனது AI பணி உதவியாளர் சில பயனர்களின் ரகசிய மின்னஞ்சல்களை அணுகி சுருக்கமாகக் கூறியதில் ஏற்பட்ட பிழையை ஒப்புக்கொண்டுள்ளது.

தொழில்நுட்ப நிறுவனமான மைக்ரோசாப்ட் 365 கோபிலட் அரட்டையை பணியிடங்களும் அவற்றின் ஊழியர்களும் அதன் ஜெனரேட்டிவ் AI சாட்பாட்டைப் பயன்படுத்துவதற்கான ஒரு பாதுகாப்பான வழியாக முன்மொழிந்துள்ளது.

ஆனால் சமீபத்திய சிக்கல் காரணமாக, சில நிறுவன பயனர்களுக்கு அவர்களின் வரைவுகள் மற்றும் அனுப்பப்பட்ட மின்னஞ்சல் கோப்புறைகளில் சேமிக்கப்பட்ட செய்திகளிலிருந்து - ரகசியமானது எனக் குறிக்கப்பட்டவை உட்பட - தகவல்களை இந்த கருவி வெளிப்படுத்தியதாக அது கூறியது.

இந்த சிக்கலை சரிசெய்ய ஒரு புதுப்பிப்பை வெளியிட்டுள்ளதாகவும், "ஏற்கனவே பார்க்க அங்கீகரிக்கப்படாத தகவல்களை யாருக்கும் அணுக அனுமதிக்கவில்லை" என்றும் மைக்ரோசாப்ட் கூறுகிறது.

இருப்பினும், புதிய AI அம்சங்களைச் சேர்க்க நிறுவனங்கள் போட்டியிடும் வேகம், இதுபோன்ற தவறுகள் தவிர்க்க முடியாதவை என்று சில நிபுணர்கள் எச்சரித்தனர்.

மின்னஞ்சல்கள் மற்றும் அரட்டை செயல்பாடுகளுக்குப் பயன்படுத்தப்படும், கேள்விகளுக்கான பதில்களைப் பெற அல்லது செய்திகளைச் சுருக்கமாகக் கூற, Outlook மற்றும் Teams போன்ற Microsoft நிரல்களுக்குள் Copilot Chat பயன்படுத்தப்படலாம்.

"மைக்ரோசாப்ட் 365 கோபிலட் அரட்டை, ஒரு பயனரால் எழுதப்பட்டு, அவர்களின் வரைவு மற்றும் அனுப்பப்பட்ட பொருட்களில் அவுட்லுக் டெஸ்க்டாப்பில் சேமிக்கப்பட்ட ரகசியம் என்று பெயரிடப்பட்ட மின்னஞ்சல்களிலிருந்து உள்ளடக்கத்தைத் திருப்பி அனுப்பக்கூடிய ஒரு சிக்கலை நாங்கள் கண்டறிந்து சரிசெய்தோம்" என்று மைக்ரோசாப்ட் செய்தித் தொடர்பாளர் பிபிசி செய்தியிடம் தெரிவித்தார்.

"எங்கள் அணுகல் கட்டுப்பாடுகள் மற்றும் தரவு பாதுகாப்பு கொள்கைகள் அப்படியே இருந்தபோதிலும், இந்த நடத்தை எங்கள் நோக்கம் கொண்ட கோபிலட் அனுபவத்தை பூர்த்தி செய்யவில்லை, இது கோபிலட் அணுகலில் இருந்து பாதுகாக்கப்பட்ட உள்ளடக்கத்தை விலக்க வடிவமைக்கப்பட்டுள்ளது," என்று அவர்கள் மேலும் கூறினர்.

"நிறுவன வாடிக்கையாளர்களுக்காக உலகளவில் ஒரு உள்ளமைவு புதுப்பிப்பு பயன்படுத்தப்பட்டுள்ளது."

இந்த தவறை முதலில் தொழில்நுட்ப செய்தி நிறுவனமான **Bleeping Computer** தெரிவித்தது , இந்த சிக்கலை உறுதிப்படுத்தும் சேவை எச்சரிக்கையைக் கண்டதாகக் கூறியது.

"ரகசிய லேபிள் பயன்படுத்தப்பட்ட பயனர்களின் மின்னஞ்சல் செய்திகள் மைக்ரோசாப்ட் 365 கோபிலட் அரட்டையால் தவறாக செயலாக்கப்படுகின்றன" என்று மைக்ரோசாப்ட் அறிவிப்பை அது மேற்கோள் காட்டியது.

அங்கீகரிக்கப்படாத தரவுப் பகிர்வைத் தடுக்க உள்ளமைக்கப்பட்ட உணர்திறன் லேபிள் மற்றும் தரவு இழப்பு தடுப்புக் கொள்கை இருந்தபோதிலும், Copilot Chat-க்குள் உள்ள ஒரு பணி தாவல், பயனரின் வரைவுகள் மற்றும் அனுப்பப்பட்ட கோப்புறைகளில் சேமிக்கப்பட்ட மின்னஞ்சல் செய்திகளைச் சுருக்கமாகக் கூறியுள்ளதாக அறிவிப்பில் மேலும் கூறப்பட்டுள்ளது.

மைக்ரோசாப்ட் இந்த பிழையை முதன்முதலில் ஜனவரி மாதத்தில் அறிந்ததாக அறிக்கைகள் தெரிவிக்கின்றன.

இங்கிலாந்தில் உள்ள NHS ஊழியர்களுக்கான ஆதரவு டேஷ்போர்டிலும் இந்தப் பிழை குறித்த அதன் அறிவிப்பு பகிரப்பட்டது - அங்கு மூல காரணம் "குறியீட்டுச் சிக்கலுக்கு" காரணம் என்று கூறப்படுகிறது.

NHS IT ஆதரவு தளத்தில் உள்ள அறிவிப்பின் ஒரு பகுதி அது பாதிக்கப்பட்டுள்ளதாகக் குறிக்கிறது.

ஆனால், கோபிலட் சாட் மூலம் செயலாக்கப்படும் எந்தவொரு வரைவு அல்லது அனுப்பப்பட்ட மின்னஞ்சல்களின் உள்ளடக்கங்களும் அவற்றை உருவாக்கியவர்களிடமே இருக்கும் என்றும், நோயாளியின் தகவல்கள் வெளியிடப்படவில்லை என்றும் அது பிபிசி செய்திக்குத் தெரிவித்தது.

'தரவு கசிவு ஏற்படும்'

மைக்ரோசாஃப்ட் 365 சந்தா உள்ள நிறுவனங்களுக்குக் கிடைக்கும் மைக்ரோசாஃப்ட் 365 கோபிலட் அரட்டை போன்ற நிறுவன AI கருவிகள், முக்கியமான நிறுவனத் தகவல்களைப் பகிர்வதைத் தடுக்க பெரும்பாலும் கடுமையான கட்டுப்பாடுகள் மற்றும் பாதுகாப்புப் பாதுகாப்புகளைக் கொண்டுள்ளன.

ஆனால் சில நிபுணர்களுக்கு, இந்த பிரச்சினை இன்னும் சில பணி சூழல்களில் ஜெனரேட்டிவ் AI கருவிகளைப் பயன்படுத்துவதால் ஏற்படும் அபாயங்களை எடுத்துக்காட்டுகிறது.

"புதிய மற்றும் புதுமையான AI திறன்கள்" வெளியிடப்படும் அதிர்வெண்ணைக் கருத்தில் கொண்டு, "இந்த வகையான தடுமாற்றம் தவிர்க்க முடியாதது" என்று கார்ட்னரின் தரவு பாதுகாப்பு மற்றும் AI ஆளுமை ஆய்வாளர் நாடர் ஹெனைன் கூறினார்.

இந்த AI தயாரிப்புகளைப் பயன்படுத்தும் நிறுவனங்கள் பெரும்பாலும் தங்களைப் பாதுகாத்துக் கொள்ளவும் ஒவ்வொரு புதிய அம்சத்தையும் நிர்வகிக்கவும் தேவையான கருவிகளைக் கொண்டிருக்கவில்லை என்று அவர் பிபிசி செய்தி நிறுவனத்திடம் கூறினார்.

"சாதாரண சூழ்நிலைகளில், நிறுவனங்கள் இந்த அம்சத்தை அணைத்துவிட்டு, நிர்வாகம் சரியாகும் வரை காத்திருப்பார்கள்" என்று ஹெனைன் கூறினார்.

"துரதிர்ஷ்டவசமாக, ஆதாரமற்ற AI மிகைப்படுத்தலின் பெருவெள்ளத்தால் ஏற்படும் அழுத்தத்தின் அளவு அதை கிட்டத்தட்ட சாத்தியமற்றதாக்குகிறது," என்று அவர் மேலும் கூறினார்.

சர்ரே பல்கலைக்கழகத்தின் சைபர்-பாதுகாப்பு நிபுணர் பேராசிரியர் ஆலன் உட்வார்ட், இது போன்ற கருவிகளை இயல்புநிலையாக தனியார்மயமாக்கி, விருப்பத்தேர்வை மட்டுமே பயன்படுத்துவதன் முக்கியத்துவத்தைக் காட்டுகிறது என்றார்.

"இந்த கருவிகளில் தவிர்க்க முடியாமல் பிழைகள் இருக்கும், குறிப்பாக அவை அசுர வேகத்தில் முன்னேறும்போது, தரவு கசிவு வேண்டுமென்றே செய்யப்படாவிட்டாலும் அது நடக்கும்," என்று அவர் பிபிசி செய்தியிடம் கூறினார்.

பிக் டெக் **AI** செலவினக் களத்தில் அமேசான் இணைந்ததால் பங்குகள் சரிந்தன.
வேலை இழப்பு வலியைக் குறைக்க **AI** ஐப் பயன்படுத்துமாறு எக்ஸ்பாக்ஸ் தயாரிப்பாளர் ஊழியர்களிடம் கூறுகிறார்
மைக்ரோசாப்ட் 'தனியுரிமை கனவு' என்று அழைக்கப்படும் **AI** ஸ்கிரீன்ஷாட் கருவியை வெளியிடுகிறது
