

Google diz que Gemini hackeou sistemas de 3 empresas durante teste

Category: GERAL, TECNOLOGIA e CIÊNCIA

escrito por Alice Ketllen | 21 de setembro de 2026



O Gemini, sistema de inteligência artificial do Google, conseguiu acessar ambientes digitais pertencentes a três empresas reais durante uma avaliação de segurança realizada em maio. Segundo a companhia, o modelo não tinha autorização específica para entrar nesses sistemas.

O episódio ocorreu durante um exercício criado para avaliar o comportamento de modelos de IA em cenários de cibersegurança. A ferramenta interpretou que os sistemas encontrados faziam parte da atividade e tomou iniciativas para tentar obter acesso.

O caso chamou atenção porque envolve um modelo com capacidade de executar ações de forma mais autônoma, levantando questionamentos sobre os limites e os mecanismos de controle utilizados durante testes desse tipo.

IA encontrou informações na internet

Durante a avaliação, o Gemini procurou maneiras de entrar nos sistemas que considerava relacionados ao exercício. Em uma das tentativas, o modelo testou diferentes combinações de senha

até conseguir acessar um serviço protegido.

Nas outras duas ocorrências, o caminho foi diferente. A inteligência artificial localizou credenciais expostas publicamente na internet, incluindo informações disponíveis em repositórios online, e utilizou esses dados para entrar nos ambientes.

Heather Adkins, vice-presidente de engenharia de segurança do Google, explicou que o modelo interpretou as informações disponíveis como parte do cenário proposto.

Segundo a executiva, depois de perceber que os ambientes acessados não faziam parte da avaliação, o Gemini interrompeu as ações nos três casos.

Falha ocorreu durante exercício de cibersegurança

A avaliação foi conduzida pela Irregular, empresa especializada em testes de segurança de sistemas avançados de inteligência artificial.

De acordo com o Google, houve uma falha no exercício que permitiu ao Gemini utilizar a internet de maneira diferente dos limites estabelecidos para a simulação. A proposta era que o modelo permanecesse dentro de um ambiente controlado.

Depois que o problema foi identificado, o Google comunicou as três empresas afetadas e trabalhou com a companhia responsável pela avaliação para modificar os procedimentos utilizados nos testes.

O Google também afirmou que o episódio reforça a necessidade de preparar modelos mais avançados para lidar de maneira responsável com situações em que tenham acesso a ferramentas e recursos externos.

Google não revelou qual Gemini foi usado

A companhia não informou qual versão específica do Gemini participou da avaliação.

O Google esclareceu apenas que o modelo utilizado não era a versão mais recente disponível da ferramenta.

A informação é relevante porque diferentes versões de modelos podem apresentar capacidades distintas de raciocínio, utilização de ferramentas e execução autônoma de tarefas.

Outras empresas também tiveram problemas

Segundo a Irregular, o problema não aconteceu exclusivamente durante a avaliação do Gemini.

A empresa afirmou que testes realizados com sistemas de Meta, Anthropic e OpenAI também registraram situações relacionadas a acessos externos durante avaliações.

Um porta-voz da companhia afirmou que os episódios estavam relacionados ao mesmo tipo de falha identificado anteriormente e que não configuravam um incidente substancialmente diferente.

Os laboratórios envolvidos teriam sido comunicados depois que a Irregular identificou os problemas. A empresa afirmou ainda que as falhas conhecidas sob sua responsabilidade foram corrigidas.

O episódio envolvendo o Gemini levou o Google e a empresa responsável pela avaliação a revisar procedimentos. O objetivo é reduzir a possibilidade de que modelos utilizados em testes interpretem sistemas reais como parte de uma simulação e

tentem acessá-los sem autorização.

Fonte: **Terra** e Publicado Por: Jornal Folha do Progresso
21/09/2026/15:54:23

O formato de distribuição de notícias do [Jornal Folha do Progresso](#) pelo celular mudou. A partir de agora, as notícias chegarão diretamente pelo formato Comunidades, ou pelo canal uma das inovações lançadas pelo WhatsApp. Não é preciso ser assinante para receber o serviço. Assim, o internauta pode ter, na palma da mão, matérias verificadas e com credibilidade. Para passar a [receber as notícias](#) do Jornal Folha do Progresso, clique nos links abaixo siga nossas redes sociais:

- [Clique aqui e nos siga no X](#)
- [Clica aqui e siga nosso Instagram](#)
- [Clique aqui e siga nossa página no Facebook](#)
- [Clique aqui e acesse o nosso canal no WhatsApp](#)
- [Clique aqui e acesse a comunidade do Jornal Folha do Progresso](#)

Apenas os administradores do grupo poderão mandar mensagens e saber quem são os integrantes da comunidade. Dessa forma, evitamos qualquer tipo de interação indevida. Sugestão de pauta enviar no e-mail: folhadoprogresso.jornal@gmail.com.

Envie vídeos, fotos e sugestões de pauta para a redação do JFP (JORNAL FOLHA DO PROGRESSO) Telefones: WhatsApp [\(93\) 98404 6835](#)– (93) 98117 7649.

“Informação publicada é informação pública. Porém, para chegar até você, um grupo de pessoas trabalhou para isso. Seja ético. Copiou? Informe a fonte.”

Publicado por Jornal Folha do Progresso, Fone para contato 93 981177649 (Tim) WhatsApp: [-93- 984046835](#) (Claro)

- Site: www.folhadoprogresso.com.br
mail: folhadoprogresso.jornal@gmail.com/ou
adeciopiran.blog@gmail.com

e -
e-mail: