Bảo vệ tài khoản Google Workspace trước những thách thức về bảo mật

Xác minh hai bước · https://gcs.vn/kho-tai-nguyen/google-workspace-admin-center/bao-ve-tai-khoan-google-workspace-truoc-nhung-thach-thuc-ve-bao-mat/

Thử thách bảo mật là các biện pháp bảo mật bổ sung để xác minh danh tính của người dùng. Có hai loại thách thức bảo mật:

- **Thử thách đăng nhập** —Nếu nghi ngờ rằng một người dùng trái phép đang cố đăng nhập vào tài khoản Google Workspace, chúng tôi sẽ đưa ra thử thách đăng nhập cho họ. Nếu người dùng không thể nhập thông tin được yêu cầu, chúng tôi sẽ không cho phép họ đăng nhập vào tài khoản.
- **Thử thách xác minh đó là bạn** —Nếu người dùng đang thực hiện các hành động được coi là nhạy cảm, chúng tôi sẽ đưa ra cho họ thử thách xác minh đó là bạn . Nếu người dùng không thể nhập thông tin được yêu cầu, chúng tôi sẽ không cho phép hành động nhạy cảm đó (họ có thể tiếp tục sử dụng tài khoản của mình như bình thường).

Trước khi bạn có thể sử dụng các thử thách bảo mật

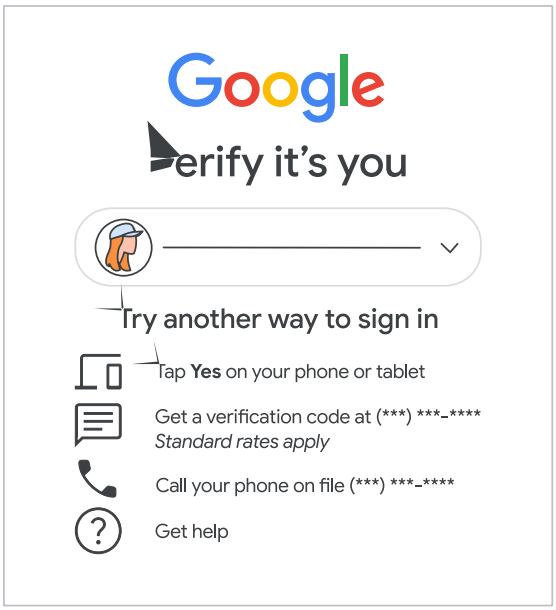
Đảm bảo tài khoản Google Workspace của bạn có thông tin chúng tôi cần:

- **Nhắc nhở nhân viên thêm số điện thoại và địa chỉ email khôi phục vào tài khoản của họ.** Chúng tôi sẽ định kỳ yêu cầu họ thêm những chi tiết này khi họ đăng nhập vào tài khoản của mình.
- **Thêm ID nhân viên vào tài khoản người dùng của bạn.** Xem Thêm ID nhân viên làm thử thách đăng nhập .

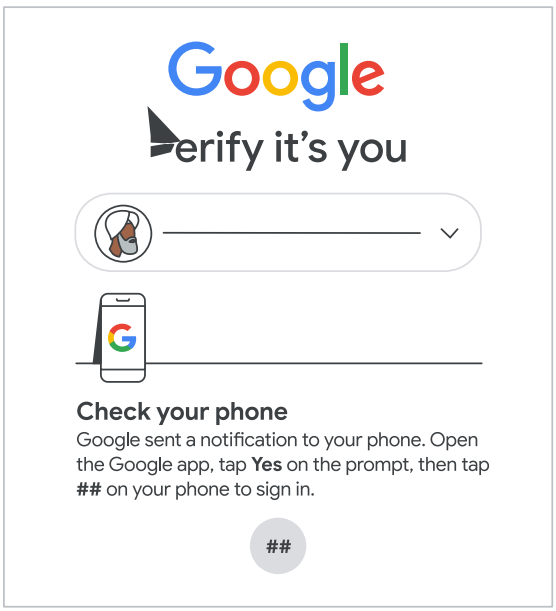
Các loại thử thách đăng nhập

Người dùng xác nhận danh tính của họ với thiết bị di động của họ

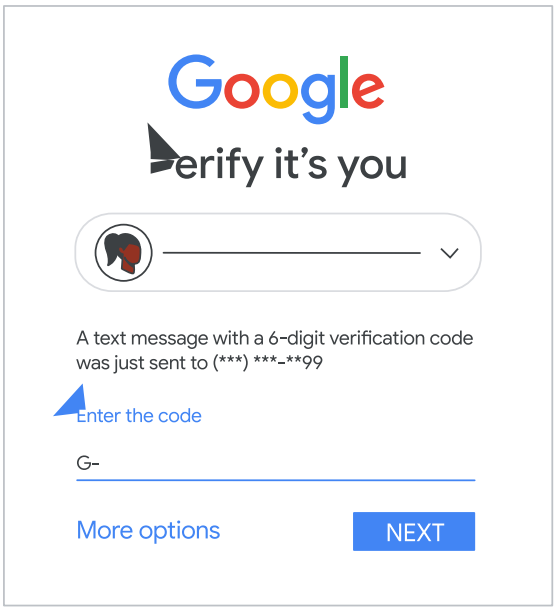
Người dùng chọn cách xác minh danh tính của họ



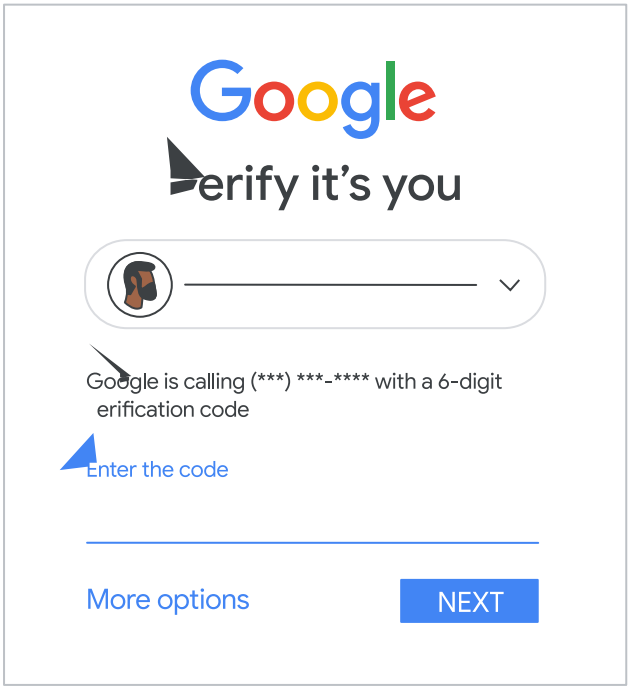
Google sử dụng ứng dụng được cài đặt trên điện thoại của người dùng để xác nhận danh tính của họ



Google gửi tin nhắn văn bản kèm theo mã xác minh

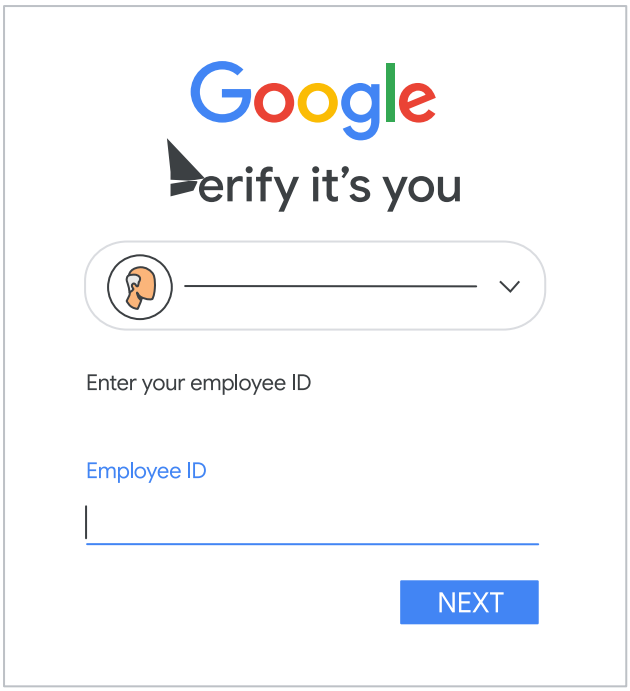


Google gọi đến số điện thoại của người dùng và cung cấp mã xác minh



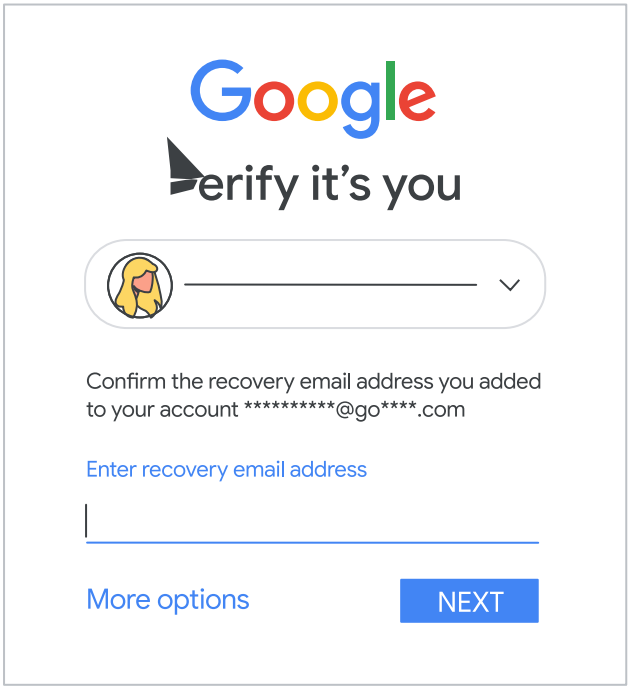
Người dùng nhập ID nhân viên của họ

Nếu bạn đã thêm ID nhân viên làm thử thách đăng nhập thì người dùng có thể sử dụng ID này để xác nhận danh tính của họ.



User enters their recovery email

Người dùng có thể nhập địa chỉ email khôi phục làm thử thách đăng nhập.



Thử thách xác minh đó là bạn đối với các hành động nhạy cảm

Nếu người dùng Google Workspace thực hiện một hành động nhạy cảm thì đôi khi người dùng đó sẽ phải đối mặt với thử thách xác minh danh tính của bạn. Nếu người dùng không thể nhập thông tin được yêu cầu, Google sẽ không cho phép thực hiện hành động nhạy cảm.

'Hành động nhạy cảm bị chặn'

Đối với hầu hết người dùng phải đối mặt với thử thách xác minh đó là bạn đối với một hành động nhạy cảm, một cửa sổ sẽ hiển thị với tiêu đề Hành **động nhạy cảm bị chặn** . Người dùng được hướng dẫn thử lại từ thiết bị họ thường sử dụng (như điện thoại hoặc máy tính xách tay) hoặc từ vị trí mà họ thường đăng nhập.

'Không thể hoàn thành hành động này ngay bây giờ'

Vì một số người dùng có thiết bị hoặc khóa bảo mật mới được thêm vào tài khoản của họ nên họ không thể xác minh danh tính ngay lập tức trước thách thức bảo mật. Đối với những người dùng này, một cửa sổ được hiển thị với tiêu đề **Không thể hoàn thành hành động này ngay bây giờ** . Những người dùng này có thể xác minh danh tính của họ sau khi thiết bị, số điện thoại hoặc khóa bảo mật đã được liên kết với tài khoản của họ trong ít nhất 7 ngày.

Ví dụ về hành động nhạy cảm

Dưới đây là một số ví dụ về hành động nhạy cảm:

- Vô hiệu hóa xác minh 2 bước
- Cho phép ứng dụng truy cập dữ liệu Google
- Thay đổi địa chỉ email hoặc số điện thoại khôi phục tài khoản
- Đang tải xuống dữ liệu tài khoản
- Thay đổi tên trên tài khoản

Bật thử thách đăng nhập bằng SSO

Nếu tổ chức của bạn sử dụng nhà cung cấp danh tính bên thứ ba (IdP) để xác thực người dùng đăng nhập một lần (SSO) thông qua SAML thì bạn có thể cung cấp cho những người dùng SSO này những thử thách đăng nhập dựa trên rủi ro bổ sung, tùy thuộc vào cách bạn sử dụng IdP bên thứ ba:

- Nếu đã định cấu hình cấu hình SSO cho tổ chức của mình thì bạn có thể chọn áp dụng các thử thách xác thực bổ sung hoặc Xác minh 2 bước (2SV) cho người dùng mà cấu hình đó được áp dụng. Sau khi IdP xác thực người dùng trong quá trình đăng nhập, Google có thể đưa ra các thử thách đăng nhập bổ sung hoặc áp dụng 2SV cho người dùng.**Lưu ý:** Hành vi mặc định của những người dùng này là bỏ qua các thử thách bổ sung. Để bật chúng, hãy làm theo các bước trong Thiết lập xác minh SSO sau bài viết bên dưới.
- Nếu bạn đang sử dụng hồ sơ bên thứ ba khác cho OU hoặc nhóm trong tổ chức của mình thì mọi thử thách xác thực dựa trên rủi ro và 2SV (khi được bật) **sẽ tự động được áp dụng** cho

những người dùng này.

Các trường hợp sử dụng cho các thử thách đăng nhập bổ sung với SSO

- Bạn muốn sử dụng khóa bảo mật để bảo vệ quyền truy cập vào các tài nguyên nhạy cảm do Google lưu trữ nhằm đảm bảo tối đa và IdP hiện tại của bạn không hỗ trợ khóa bảo mật.
- Bạn muốn tiết kiệm chi phí sử dụng nhà cung cấp danh tính bên thứ ba vì trong hầu hết các trường hợp, người dùng đều truy cập vào tài nguyên của Google.
- Bạn không muốn xác thực Google (Google là nhà cung cấp danh tính) nhưng muốn tận dụng tất cả các thách thức đăng nhập dựa trên rủi ro của Google.
- Bạn muốn Google bảo vệ các hành động nhạy cảm trong hệ sinh thái Google.
-

Điều gì xảy ra khi bạn áp dụng các thử thách đăng nhập bổ sung

Để triển khai suôn sẻ, hãy thông báo cho người dùng của bạn về chính sách mới và thời điểm bạn dự định áp dụng chính sách đó. Đây là những gì sẽ xảy ra khi bạn áp dụng các thử thách đăng nhập bổ sung khi đăng nhập:

- Nếu bạn hiện có các chính sách 2SV, chẳng hạn như thực thi 2SV, thì những chính sách đó sẽ được áp dụng ngay lập tức.
- Người dùng bị ảnh hưởng bởi chính sách mới và những người đã đăng ký 2SV sẽ nhận được thử thách đăng nhập 2SV khi đăng nhập.
- Dựa trên phân tích rủi ro khi đăng nhập vào Google, người dùng có thể thấy các thử thách đăng nhập dựa trên rủi ro khi đăng nhập.

Thiết lập xác minh SSO sau

1. Đăng nhập vào Bảng điều khiển dành cho quản trị viên của Google của bạn.
2. Trong Bảng điều khiển dành cho quản trị viên, đi tới Menu > **Bảo mật** > **Xác thực** > **Thử thách đăng nhập**.
3. Ở bên trái, hãy chọn đơn vị tổ chức mà bạn muốn đặt chính sách.
   Đối với tất cả người dùng, hãy chọn đơn vị tổ chức cấp cao nhất. Ban đầu, các đơn vị tổ chức kế thừa các cài đặt của tổ chức mẹ.
4. Nhấp vào **Xác minh sau SSO** .
5. Chọn **Yêu cầu người dùng xác minh bổ sung từ Google nếu hoạt động đăng nhập có vẻ đáng ngờ và luôn áp dụng chính sách Xác minh 2 bước (nếu được định cấu hình)** .
   Google tạo một mục trong nhật ký kiểm tra của Quản trị viên để cho biết sự thay đổi về chính sách. Với chính sách mới, Google có thể đưa ra các thử thách đăng nhập xác thực dựa trên rủi

ro và Xác minh 2 bước nếu chính sách này được định cấu hình. Mặc định là bỏ qua xác minh bổ sung.

6. Ở dưới cùng bên phải, nhấp vào **Lưu** .

Lưu ý: Trong một số ít trường hợp, dữ liệu sự kiện trong nhật ký có thể không hiển thị cho tất cả các sự kiện. Chúng tôi đang làm việc để giải quyết vấn đề này.

FAQ

Câu hỏi bảo mật bổ sung và thử thách đăng nhập

Khi nào người dùng nhìn thấy thách thức bảo mật?

Người dùng sẽ gặp thử thách đăng nhập khi phát hiện thấy thông tin đăng nhập đáng ngờ, chẳng hạn như người dùng không tuân theo các mẫu đăng nhập mà họ đã hiển thị trước đây. Người dùng sẽ phải đối mặt với thử thách xác minh đó là bạn nếu họ gặp phải một phiên rủi ro khi thực hiện một hành động nhạy cảm.

Quan trọng: Google quyết định loại thách thức bảo mật nào phù hợp để đưa ra cho người dùng dựa trên nhiều yếu tố về bảo mật và khả năng sử dụng. Ví dụ: thử thách đăng nhập ID nhân viên không phải lúc nào cũng được hiển thị cho một người dùng cụ thể, ngay cả khi bạn đã bật tính năng này.

Với tư cách là quản trị viên, tôi có thể chọn loại thử thách đăng nhập nào để hiển thị cho người dùng của mình không?

Xác minh 2 bước (2SV) là một loại thử thách đăng nhập. Với tư cách là quản trị viên, bạn có thể thực thi thử thách đăng nhập 2SV cho người dùng của mình. Bằng cách đó, họ sẽ không nhận được một loại thử thách đăng nhập dựa trên rủi ro khác.

Nếu bạn không thực thi 2SV cho người dùng của mình hoặc nếu người dùng không bật tính năng này thì Google sẽ quyết định loại thử thách đăng nhập nào phù hợp để đưa ra cho người dùng đó. Loại thử thách đăng nhập phù hợp dựa trên nhiều yếu tố bảo mật và khả năng sử dụng. Ví dụ: thử thách đăng nhập ID nhân viên không phải lúc nào cũng hiển thị cho một người dùng cụ thể, ngay cả khi bạn đã bật tính năng này.

Người dùng có thể cập nhật thông tin khôi phục của họ không?

Đúng. Để biết chi tiết, hãy xem Thiết lập số điện thoại hoặc địa chỉ email khôi phục.

Chúng tôi sử dụng Xác minh 2 bước. Tại sao chúng ta cần thử thách đăng nhập?

Xác minh 2 bước (2SV) là một loại thử thách đăng nhập. Khi người dùng của bạn bật tính năng này, họ sẽ không gặp phải thử thách đăng nhập nào khác. Vì lý do tương tự, Báo cáo của quản trị viên hiển thị mỗi Xác minh 2 bước dưới dạng thử thách đăng nhập.

Thử thách đăng nhập hoạt động như thế nào khi tôi bật SSO?

Điều này phụ thuộc vào cách bạn đã định cấu hình SSO trong tổ chức của mình:

- **Nếu bạn đã định cấu hình cấu hình SSO cho tổ chức của mình** – Theo mặc định, thử thách đăng nhập không được bật. Tuy nhiên, bạn có thể thiết lập xác minh SSO sau để cho phép các thử thách xác thực dựa trên rủi ro bổ sung và Xác minh 2 bước (2SV) nếu được định cấu hình.
- **Nếu bạn đang sử dụng cấu hình SSO khác** thì mọi thử thách đăng nhập bổ sung (bao gồm 2SV, nếu được định cấu hình) sẽ tự động được áp dụng.

Tính năng này có sẵn trong các phiên bản Giáo dục không?

Có, tất cả các phiên bản Google Workspace đều có thêm các câu hỏi bảo mật và thử thách đăng nhập.

Khi nào Google coi nỗ lực đăng nhập là đáng ngờ?

Chúng tôi xác định liệu một lần đăng nhập có đáng ngờ hay không khi hệ thống phân tích rủi ro của chúng tôi xác định một nỗ lực nằm ngoài khuôn mẫu hành vi thông thường của người dùng. Ví dụ: người dùng có thể cố gắng đăng nhập từ một vị trí bất thường hoặc theo cách có liên quan đến lạm dụng.

Xác minh điện thoại

Nếu người dùng của tôi không có điện thoại công ty, có cách nào khác để xác minh tài khoản của họ không?

Có, có nhiều loại thử thách đăng nhập khác nhau. Tùy thuộc vào thông tin có sẵn cho tài khoản của người dùng, người dùng sẽ gặp một loại thử thách đăng nhập khác, chẳng hạn như nhập ID nhân viên hoặc địa chỉ email khôi phục. Nếu người dùng không có quyền truy cập vào điện thoại của họ, họ có thể sử dụng mã dự phòng để đăng nhập. Để biết chi tiết, hãy xem Đăng nhập bằng mã dự phòng .

Làm cách nào người dùng có thể cập nhật số điện thoại hoặc email khôi phục được liên kết với tài khoản của họ?

Người dùng có thể cập nhật thông tin khôi phục thông qua cài đặt tài khoản .

Người dùng có thể chọn xác minh các tiêu chí khác ngoài số điện thoại khôi phục của họ không?

Nếu người dùng không nhập số điện thoại khôi phục thì các loại thử thách đăng nhập khác sẽ được áp dụng, chẳng hạn như nhập địa chỉ email khôi phục hoặc sử dụng ID nhân viên của họ.

Vô hiệu hóa thử thách đăng nhập hoặc thử thách xác minh đó là bạn

Nếu người dùng không thể xác minh danh tính của họ, tôi có thể tắt tính năng đăng nhập hoặc thử thách xác minh đó là bạn không?

Có, quản trị viên có thể tắt tính năng đăng nhập hoặc xác minh danh tính của bạn trong 10 phút.

Trong một số trường hợp, người dùng được ủy quyền không thể xác minh danh tính của họ. Ví dụ: họ có thể không có tín hiệu điện thoại và không nhận được mã xác minh. Hoặc họ không thể nhớ hoặc tìm thấy ID nhân viên của mình. Nếu điều này xảy ra, với tư cách là quản trị viên cấp cao, bạn có thể tắt tính năng đăng nhập hoặc xác minh danh tính của bạn trong 10 phút để cho phép họ đăng nhập hoặc hoàn thành hành động nhạy cảm. Hãy thận trọng khi tắt các thử thách đăng nhập hoặc xác minh đó là bạn vì tài khoản kém an toàn hơn trước những kẻ xâm nhập tài khoản trong khoảng thời gian 10 phút.

Tôi có thể tắt đăng nhập hoặc tắt thử thách xác minh là bạn cho tổ chức của mình không?

Không, bạn không thể tắt tính năng này cho toàn bộ tổ chức của mình. Bạn chỉ có thể tắt nó tạm thời tùy theo từng người dùng.

Người dùng có thể tự tắt tính năng này khỏi cài đặt tài khoản của họ không?

Không, chỉ quản trị viên mới có thể tạm thời tắt các thử thách đăng nhập hoặc bảo mật.

Thử thách đăng nhập của quản trị viên

Làm cách nào quản trị viên không thể xác minh danh tính của họ có thể nhập lại tài khoản của họ?

Với tư cách là quản trị viên, bạn có thể lấy lại quyền truy cập vào tài khoản của mình bằng cách làm theo lời nhắc trên trang đăng nhập để đặt lại mật khẩu.

Nếu bạn là quản trị viên Google Workspace đang gặp sự cố khi đăng nhập vào tài khoản quản trị viên, hãy chuyển đến phần Khôi phục quyền truy cập của quản trị viên vào tài khoản của bạn để

biết hướng dẫn.

Điều gì sẽ xảy ra nếu quản trị viên cấp cao không thể xác minh danh tính của họ?

Nếu người dùng quản trị viên cấp cao không thể xác minh danh tính của họ thì quản trị viên cấp cao khác (nếu có) có thể tạm thời tắt thử thách đăng nhập cho họ, như được mô tả trong các bước ở trên.

Ngoài ra, quản trị viên cấp cao có thể bỏ qua thử thách đăng nhập bằng cách đặt lại mật khẩu của họ.

Lưu ý: Tùy chọn đặt lại mật khẩu tự động không có sẵn cho tất cả quản trị viên cấp cao. Để biết thêm thông tin về khôi phục tài khoản quản trị viên, hãy xem Thêm tùy chọn khôi phục vào tài khoản quản trị viên của bạn .