Bảo vệ doanh nghiệp bằng xác minh hai bước

Truy cập và đồng bộ hóa · https://gcs.vn/kho-tai-nguyen/google-workspace-admin-center/bao-ve-doanh-nghiep-bang-xac-minh-hai-buoc/

Các bài viết này dành cho quản trị viên Google Workspace *.* Người dùng Google Workspace *nên chuyển đến* phần Bật xác minh 2 bước .

Xác minh 2 bước đặt thêm một rào cản giữa doanh nghiệp của bạn và tội phạm mạng đang cố lấy cắp tên người dùng và mật khẩu để truy cập dữ liệu doanh nghiệp. Bật Xác minh 2 bước là hành động quan trọng nhất mà bạn có thể thực hiện để bảo vệ doanh nghiệp của mình.

Xác minh 2 bước là gì?

Với Xác minh 2 bước, người dùng của bạn đăng nhập vào tài khoản của họ theo hai bước bằng thông tin họ biết (mật khẩu) và thông tin họ có (điện thoại hoặc Khóa bảo mật). Tìm hiểu cách thức hoạt động

Embedded media: https://www.youtube.com/embed/z_GEd0vLiXo?start=16&feature=oembed

Các doanh nghiệp nhỏ có cần Xác minh 2 bước không?

Tội phạm mạng nhắm mục tiêu vào các doanh nghiệp thuộc *mọi quy mô* . Nếu tin tặc xâm nhập vào tài khoản quản trị viên của bạn, họ có thể xem email, tài liệu, bảng tính, hồ sơ tài chính của bạn, v.v.

Tin tặc có thể đánh cắp hoặc đoán mật khẩu, nhưng chúng không thể sao chép thứ mà chỉ bạn mới có.

Phương pháp xác minh 2 bước

Khi bạn thiết lập Xác minh 2 bước, bạn chọn bước xác minh thứ hai cho người dùng của mình.

Khóa bảo mật



Khóa bảo mật là hình thức Xác minh 2 bước an toàn nhất và bảo vệ khỏi các mối đe dọa lừa đảo. Các loại khóa bảo mật:

- Khóa bảo mật phần cứng hoặc Khóa bảo mật Titan .
- Khóa bảo mật tích hợp trong điện thoại của bạn (có sẵn trên điện thoại chạy Android 7+ hoặc iOS 10+).

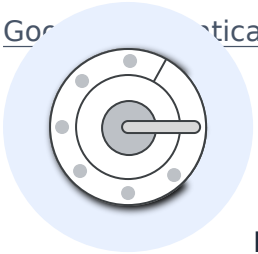
Khi người dùng đăng nhập vào Tài khoản Google của họ, thiết bị của họ sẽ phát hiện ra rằng tài khoản đó có khóa bảo mật. Đối với bước xác minh thứ hai, người dùng đăng nhập bằng khóa bảo mật của họ. Người dùng kết nối khóa bảo mật với thiết bị của họ bằng USB, Bluetooth hoặc NFC (Giao tiếp trường gần), tùy thuộc vào loại khóa. Tìm hiểu thêm về khóa bảo mật

Lời oogle



Người dùng có thể thiết lập thiết bị di động Android hoặc Apple của mình để nhận lời nhắc đăng nhập. Khi họ đăng nhập vào Tài khoản Google trên máy tính, họ sẽ nhận được thông báo “Đang cố đăng nhập?” lời nhắc trên thiết bị di động của họ. Họ chỉ cần xác nhận bằng cách chạm vào thiết bị di động của mình. Đăng nhập theo cách này bổ sung tính bảo mật của Xác minh 2 bước và nhanh hơn nhập mã xác minh. Tìm hiểu thêm về lời nhắc trên điện thoại

Go ticator và các trình tạo mã xác minh khác



Người dùng tạo mã xác minh một lần trên mã thông báo phần cứng (thiết bị phần cứng nhỏ) hoặc ứng dụng trên thiết bị di động của họ, chẳng hạn như Google Authenticator. Người dùng nhập mã để đăng nhập vào máy tính của họ và các thiết bị khác, bao gồm cả thiết bị di động. Google Authenticator và các ứng dụng khác không cần kết nối internet để tạo mã.Xác minh 2 bước hỗ trợ mã thông báo phần mềm và phần cứng sử dụng tiêu chuẩn TOTP (Mật khẩu một lần dựa trên thời gian).

Mã dự phòng



Nếu người dùng không có thiết bị di động hoặc làm việc ở khu vực mà họ không thể mang theo thiết bị di động, thì họ có thể sử dụng mã dự phòng cho Xác minh 2 bước. Người dùng có thể tạo mã xác minh dự phòng và in chúng trước thời hạn.

Tin [illegible]ản hoặc cuộc gọi điện thoại



Google gửi mã Xác minh 2 bước tới thiết bị di động trong tin nhắn văn bản hoặc cuộc gọi thoại.

Lưu ý: Xác minh 2 bước bằng số điện thoại địa phương hiện không được hỗ trợ cho một số miền ở Nigeria và Bờ Biển Ngà do số lượng lớn tài khoản bị lạm dụng ở các quốc gia đó. Để biết thông tin về việc miền của bạn có đủ điều kiện hay không, vui lòng liên hệ với bộ phận Hỗ trợ.

Các phương pháp hay nhất để Xác minh 2 bước

Thực thi Xác minh 2 bước cho quản trị viên và người dùng chính

Bạn có thể thực hiện Xác minh 2 bước tùy chọn hoặc bắt buộc đối với người dùng của mình. Chúng tôi khuyên bạn nên thực thi Xác minh 2 bước cho tài khoản quản trị viên của mình và những người dùng làm việc với thông tin doanh nghiệp quan trọng nhất của bạn.

- Tài khoản quản trị viên là tài khoản mạnh nhất vì nó có thể xóa người dùng, đặt lại mật khẩu và truy cập tất cả dữ liệu của bạn.
- Người dùng làm việc với dữ liệu nhạy cảm như hồ sơ tài chính và thông tin nhân viên cũng nên sử dụng Xác minh 2 bước.

Cân nhắc sử dụng khóa bảo mật trong doanh nghiệp của bạn

Vì khóa bảo mật là phương pháp Xác minh 2 bước mạnh nhất nên hãy cân nhắc sử dụng chúng trong doanh nghiệp của bạn.

- **Khóa bảo mật** —Phương thức Xác minh 2 bước mạnh nhất và không yêu cầu người dùng nhập mã. Bạn có thể mua khóa bảo mật tương thích từ nhà bán lẻ mà bạn tin tưởng hoặc Khóa bảo

mật Titan từ Google Store. Hoặc người dùng của bạn có thể sử dụng khóa bảo mật tích hợp trong điện thoại của họ (có sẵn trên điện thoại chạy Android 7 trở lên hoặc iOS 10 trở lên).

- **Các lựa chọn thay thế cho khóa bảo mật** —Nếu bạn quyết định không sử dụng khóa bảo mật, lời nhắc của Google hoặc ứng dụng Google Authenticator là những lựa chọn thay thế phù hợp. Lời nhắc của Google cung cấp trải nghiệm người dùng tốt hơn vì người dùng chỉ cần nhấn vào thiết bị của họ khi được nhắc thay vì nhập mã xác minh.
- **Tin nhắn văn bản không được khuyến khích** —Chúng dựa vào các mạng của nhà cung cấp dịch vụ bên ngoài và có thể bị chặn.

Tiếp theo là gì?

- Bật Xác minh 2 bước bằng cách làm theo hướng dẫn trong Triển khai xác minh 2 bước