Các phương pháp hay nhất về bảo mật cho tài khoản quản trị viên

Vai trò quản trị viên · https://gcs.vn/kho-tai-nguyen/google-workspace-admin-center/cac-phuong-phap-hay-nhat-ve-bao-mat-cho-tai-khoan-quan-tri-vien/

Thực hiện theo các phương pháp hay nhất này để cải thiện tính bảo mật cho tài khoản quản trị viên của bạn và mở rộng ra là cho toàn bộ doanh nghiệp của bạn.

Để biết thêm các phương pháp hay nhất về bảo mật, hãy xem Danh sách kiểm tra bảo mật .

Bảo vệ tài khoản quản trị viên

Yêu cầu Xác minh hai bước cho tài khoản quản trị viên

Nếu ai đó có được mật khẩu quản trị, Xác minh hai bước (2SV) giúp bảo vệ tài khoản khỏi truy cập trái phép. Điều này đặc biệt quan trọng đối với super admin sử dụng 2SV vì tài khoản của họ kiểm soát quyền truy cập vào tất cả dữ liệu doanh nghiệp và nhân viên trong tổ chức.

Bảo vệ doanh nghiệp của bạn bằng Xác minh hai bước

Sử dụng các phím bảo mật cho Xác minh hai bước

Có một số phương pháp Xác minh hai bước, bao gồm các phím bảo mật, Google prompt, Google Authenticator và mã dự phòng. Các phím bảo mật là các thiết bị phần cứng nhỏ được sử dụng cho xác thực yếu tố thứ hai. Chúng giúp chống lại các mối đe dọa phishing và là hình thức 2SV an toàn nhất.

Bảo vệ doanh nghiệp của bạn bằng Xác minh hai bước - Phím bảo mật

Không chia sẻ các tài khoản quản trị viên giữa người dùng

Cung cấp cho mỗi quản trị viên một tài khoản quản trị riêng và dễ nhận biết. Nếu nhiều người sử dụng cùng một tài khoản quản trị để đăng nhập vào Bảng điều khiển quản trị, ví dụ như admin@example.com, bạn không thể xác định được quản trị viên nào chịu trách nhiệm cho các hoạt động cụ thể trong nhật ký kiểm tra.

Phòng chống cuộc tấn công mục tiêu

Bạn có thể áp dụng nhiều khuyến nghị trong bài viết này cùng lúc bằng cách đăng ký tài khoản super admin và các tài khoản nhạy cảm khác vào Chương trình Bảo vệ Nâng cao.

Bảo vệ người dùng với Chương trình Bảo vệ Nâng cao

Quản lý tài khoản quản trị viên cấp cao

Thiết lập nhiều tài khoản quản trị viên cấp cao

Tổ chức của bạn nên có nhiều hơn một tài khoản super admin, mỗi tài khoản do một cá nhân riêng quản lý (tránh việc chia sẻ tài khoản quản trị). Nếu một tài khoản bị mất hoặc bị xâm nhập, một super admin khác có thể thực hiện các nhiệm vụ cần thiết trong khi tài khoản kia được khôi phục.

Không sử dụng tài khoản quản trị viên cấp cao cho các hoạt động hàng ngày

Cung cấp cho mỗi super admin 2 tài khoản: tài khoản super admin riêng và một tài khoản riêng để sử dụng trong các hoạt động hàng ngày. Người dùng chỉ nên đăng nhập vào tài khoản super admin để thực hiện các nhiệm vụ super admin, chẳng hạn như thiết lập Xác minh hai bước (2SV), quản lý thanh toán và giấy phép người dùng, hoặc giúp đỡ một quản trị viên khác khôi phục tài khoản của họ.

Các super admin nên sử dụng một tài khoản riêng, không phải là tài khoản quản trị, cho các hoạt động hàng ngày.

Ví dụ: Nếu Maria và James là super admin, họ nên có một tài khoản quản trị riêng và một tài khoản người dùng, như sau:

- admin-maria@example.com, maria@example.com
- admin-james@example.com, james@example.com

Đảm bảo bạn nhận được các thông báo quan trọng từ quản trị viên

Nếu bạn không thường xuyên đăng nhập bằng tài khoản quản trị chính của mình, bạn có thể bỏ qua các thông báo dịch vụ bắt buộc quan trọng từ Google. Để đảm bảo bạn nhận được các thông báo này, hãy thiết lập một địa chỉ email thứ cấp để gửi thông báo này đến một tài khoản mà bạn sử dụng thường xuyên.

Gửi thông báo thanh toán và tài khoản cho các quản trị viên khác

Không giữ kết nối với tài khoản quản trị viên cấp cao

Giữ kết nối với tài khoản super admin khi bạn không thực hiện các nhiệm vụ quản trị cụ thể có thể tăng nguy cơ bị tấn công lừa đảo. Super admin nên đăng nhập vào khi cần để thực hiện các nhiệm vụ cụ thể, sau đó đăng xuất.

Sử dụng các tài khoản không phải super admin cho các nhiệm vụ quản trị hàng ngày

Chỉ sử dụng tài khoản super admin khi cần thiết. Phân công các nhiệm vụ quản trị cho các tài khoản người dùng với vai trò quản trị hạn chế. Sử dụng nguyên tắc ít đặc quyền, cho phép mỗi người dùng truy cập vào tài nguyên và công cụ cần thiết cho nhiệm vụ thông thường của họ. Ví dụ, bạn có thể cấp quyền quản trị cho một người dùng để tạo tài khoản người dùng và đặt lại mật khẩu, nhưng không cho phép họ xóa tài khoản người dùng.

Về vai trò quản trị viên

Theo dõi hoạt động trên tài khoản quản trị

Thiết lập cảnh báo qua email cho quản trị viên

Theo dõi hoạt động quản trị và phát hiện các nguy cơ bảo mật tiềm ẩn bằng cách thiết lập cảnh báo qua email cho một số sự kiện cụ thể, chẳng hạn như các cố gắng đăng nhập đáng ngờ, thiết bị di động bị xâm phạm, hoặc các thay đổi bởi người quản trị khác.

Khi bạn bật cảnh báo cho một hoạt động nào đó, bạn sẽ nhận được một email mỗi khi hoạt động đó xảy ra.

Cảnh báo qua email cho quản trị viên và quy tắc được xác định sẵn trong hệ thống

Xem lại nhật ký quản trị

Sử dụng nhật ký kiểm tra quản trị để xem lịch sử các nhiệm vụ được thực hiện trong bảng điều khiển quản trị Google, bao gồm người quản trị thực hiện nhiệm vụ, ngày thực hiện và địa chỉ IP mà người quản trị đã đăng nhập.

Hoạt động từ super admin sẽ hiển thị trong cột **Mô tả Sự kiện** là **_SEED_ADMIN_ROLE**, tiếp theo là tên người dùng.

Nhật ký kiểm tra quản trị viên

Chuẩn bị khôi phục tài khoản quản trị viên

Add recovery options to admin accounts

Quản trị viên nên thêm các tùy chọn khôi phục vào tài khoản quản trị viên của họ.

Nếu quản trị viên quên mật khẩu, họ có thể nhấp vào nút Cần trợ giúp? trên trang đăng nhập và Google sẽ gửi mật khẩu mới qua điện thoại, tin nhắn hoặc email. Để làm điều đó, Google cần có số điện thoại và địa chỉ email khôi phục cho tài khoản.

Thêm thông tin khôi phục tài khoản vào tài khoản quản trị viên của bạn

Giữ thông tin trên tay để thiết lập lại mật khẩu

Nếu một quản trị viên cấp cao không thể đặt lại mật khẩu của họ bằng các tùy chọn khôi phục email hoặc điện thoại và một quản trị viên cấp cao khác không có mặt để đặt lại mật khẩu, thì họ có thể sử dụng trình hướng dẫn khôi phục.

Để xác minh danh tính, Google đặt câu hỏi về tài khoản của tổ chức:

- Ngày tạo tài khoản.
- Địa chỉ email phụ ban đầu được liên kết với tài khoản (email được sử dụng để đăng ký).
- Số đơn đặt hàng trên Google được liên kết với tài khoản (nếu có).
- Số tài khoản người dùng được tạo.

  Địa chỉ thanh toán được liên kết với tài khoản.
- Loại thẻ tín dụng được sử dụng và 4 chữ số cuối của nó.

  Google cũng yêu cầu quản trị viên xác minh quyền sở hữu DNS của miền, vì vậy quản trị viên cần có thông tin xác thực để chỉnh sửa cài đặt DNS của miền với công ty đăng ký của họ.

Đặt lại mật khẩu quản trị viên–Nếu không có tùy chọn email và điện thoại

Đăng ký khóa bảo mật dự phòng

Quản trị viên nên đăng ký nhiều khóa bảo mật cho tài khoản quản trị viên của mình và lưu trữ khóa đó ở nơi an toàn. Nếu khóa bảo mật chính của họ bị mất hoặc bị đánh cắp, họ vẫn có thể đăng nhập vào tài khoản của mình.

Thêm khóa bảo mật vào tài khoản của bạn

Lưu mã dự phòng trước thời hạn

Nếu quản trị viên mất khóa bảo mật hoặc điện thoại (nơi họ nhận được mã xác minh 2SV hoặc lời nhắc của Google), họ có thể sử dụng mã dự phòng để đăng nhập.

Quản trị viên nên tạo và in mã dự phòng trong trường hợp cần thiết. Giữ mã dự phòng ở một vị trí an toàn.

Tạo và in mã dự phòng

Chủ đề liên quan

- Đặt người dùng làm quản trị viên
- Vai trò quản trị viên cho doanh nghiệp
- Danh sách kiểm tra bảo mật dành cho doanh nghiệp vừa và lớn (hơn 100 người dùng)
- Danh sách kiểm tra bảo mật dành cho doanh nghiệp nhỏ (1-100 người dùng)