

Bezpieczeństwo konta menedżera Google Ads (MCC)

Jedno przejęcie logowanie do MCC daje dostęp do wszystkich podpiętych kont klientów naraz. Ta lista zamyka najczęstsze drogi ataku: phishing, współdzielone loginy i niekontrolowane dostępy.

LOGOWANIE

- ☐ **Każda osoba ma własne konto Google w domenie firmowej.**
Bez współdzielonych loginów - klucze dostępu z nimi nie działają.
- ☐ **Wszyscy administratorzy MCC mają po dwa klucze:** passkey i zapasowy klucz sprzętowy FIDO2.
Nowy klucz zarejestruj co najmniej 48 godzin przed wrażliwą akcją.
- ☐ **Przełącznik „Wymagaj kluczy dostępu przy wrażliwych akcjach” włączony** - dopiero gdy wszyscy administratorzy mają działające klucze.
Po włączeniu nie da się go wyłączyć.
- ☐ **Administratorzy MCC rozważyli Program ochrony zaawansowanej Google.**

DOSTĘPY

- ☐ **Administratorów jest tylu, ilu trzeba, i wiadomo, kto zatwierdza wnioski** (Multi-Party Approval).
Wniosek wygasa po 20 dniach, wsparcie Google go nie zatwierdzi.
- ☐ **Dozwolone domeny e-mail ustawione w MCC.**
- ☐ **Zaproszenia i prośby o połączenie kont weryfikowane w panelu MCC**, nie przez link z maila.
- ☐ **Nowy „klient” sprawdzony przed kliknięciem czegokolwiek:** domena, strona firmy, osoba kontaktowa.
- ☐ **Co kwartał przegląd** użytkowników, kont podrzędnych i aplikacji z dostępem do kont Google.

WCZESNE OSTRZEGANIE I REAKCJA

- ☐ **Alerty o nowych kampaniach i skokach wydatków** na wszystkich kontach klientów.
- ☐ **Spisana procedura „pierwszej godziny”** z kontaktami do Google i do klientów.

Po przejęciu: zgłoś je w formularzu Google, odzyskaj konto Google, wstrzymaj (nie usuwaj) obce kampanie, usuń obcy dostęp, dokumentuj. Zwrot jest możliwy po odzyskaniu konta i włączeniu weryfikacji dwuetapowej.