



Zagrożenia związane z prowadzeniem służbowych profili w mediach społecznościowych



Kradzież tożsamości i przejęcie profilu

Przejęcie profilu służbowego może prowadzić do wykorzystania go do nielegalnych działań, w tym do oszustw finansowych, publikowania linków rozpowszechniających złośliwe oprogramowanie lub nieprawdziwe treści czy dezinformację.



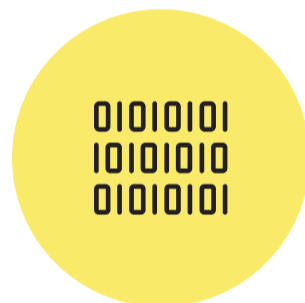
Naruszenie poufności danych

Udostępnianie poufnych informacji firmowych, przypadkowe lub celowe, może prowadzić do poważnych strat finansowych i reputacyjnych.



Brak kontroli nad treściami

Niewłaściwe treści publikowane na służbowych profilach mogą zaszkodzić wizerunkowi organizacji, wywołując negatywne reakcje klientów i partnerów biznesowych.



Przeciążenie informacyjne

Nadmiar informacji i nieprzemyślane publikacje mogą prowadzić do pominięcia ważnych wiadomości i zamieszania informacyjnego w organizacji.



Jak zadbać o bezpieczeństwo profili służbowych w social mediach?

- 1 Używaj silnych i unikalnych haseł.
- 2 Włącz weryfikację dwuetapową (2FA).
- 3 Przeprowadzaj szkolenia pracowników z zakresu cyberbezpieczeństwa i ochrony danych.
- 4 Regularnie monitoruj aktywność na profilach służbowych.
- 5 Ogranicz dostęp do zarządzania profilem tylko dla wybranych pracowników.
- 6 Stosuj polityki i procedury dotyczące korzystania z mediów społecznościowych.