Jak chronić dane i prywatność w social mediach?

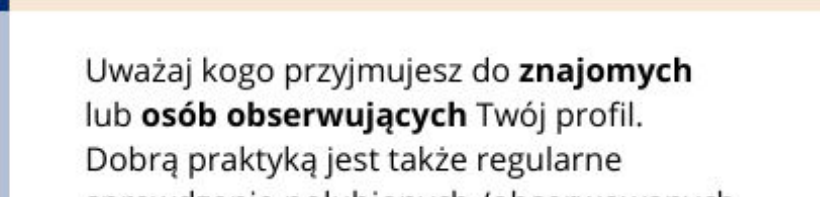
ZAKŁADANIE KONTA

Zapoznaj się z **polityką prywatności** i sprawdź, w jaki sposób Twoje dane będą przetwarzane i jak chronione.

Zastanów się czy chcesz posługiwać się swoim **prawdziwym imieniem i nazwiskiem**.

Pomyśl o użyciu **osobnego adresu e-mail** (takiego, którym nie posługujesz się na co dzień) i staraj się **nie podawać numeru telefonu**.

Nie podawaj więcej informacji niż wymaga tego portal. Pomiń wszystkie pytania dodatkowe.



Stwórz **silne hasło** (zawierające m.in. wielkie i małe litery, cyfry, znaki specjalne) i jeśli to możliwe – włącz **uwierzytelnianie dwuskładnikowe**.

W przypadku pytań dotyczących odzyskiwania hasła **nie podawaj odpowiedzi łatwych do odgadnięcia** lub **ze skończoną liczbą odpowiedzi.**

KORZYSTANIE Z SOCIAL MEDIÓW

Rozważ zablokowanie **plików cookie innych firm** i zainstalowanie **rozszerzenia blokującego śledzenie** informacji o użytkowniku.

Włącz **powiadomienia dotyczące bezpieczeństwa konta** (push, e-mailiowe lub telefoniczne).

Publikuj posty odpowiedzialne i zwracaj uwagę na to, co i kto znajduje się na zdjęciach. Dbaj również o **prywatność partnerów biznesowych**.

Zmień **ustawienia prywatności** (weryfikuj informacje udostępniane na Twoim profilu).

populacji korzysta z social mediów

Wyłącz ustawienia dotyczące załączania **danych lokalizacyjnych** i nie umieszczaj informacji o tym, **gdzie aktualnie przebywasz.**

Uważaj kogo przyjmujesz do **znajomych** lub **osób obserwujących** Twój profil. Dobrą praktyką jest także regularne sprawdzanie polubionych /obserwowanych kont i profili.

Nie odpisuj na wiadomości użytkowników, których nie znasz i nie klikaj w przesłane przez nich linki oraz nie wykonuj działań, o które poproszono Cię w wiadomości.

Zachowaj ostrożność przy klikaniu w reklamy, w udostępnianie w postach linki oraz przy pobieraniu aplikacji i wtyczek.

co trzecia osoba korzysta z mediów społecznościowych na potrzeby pracy

Regularnie **sprawdzaj ostatnie sesje i logowania** na swoim koncie.

Okresowo **przeglądaj aplikacje**, które mają dostęp do Twojego konta.

Cyklicznie sprawdzaj czy polityka prywatności serwisu, z którego korzystasz, nie została zmieniona.

Zapoznawaj się z ustawieniami grup, do których dołączasz.

Pamiętaj o **aktualizowaniu portali**.

Traktuj wszystko, czym dzielisz się w Internecie jako informacje publicznie, dostępne dla każdego. **Zastanów się dwa razy zanim coś opublikujesz**.

Jeśli prowadzisz firmę powinieneś wdrożyć **system zarządzania bezpieczeństwem informacji** oraz regularnie **szkolić pracowników** z zakresu ochrony danych i cyberzagrożeń.

Twoja firma potrzebuje wsparcia w zarządzaniu bezpieczeństwem informacji? Napisz do nas: kontakt@resilia.pl

Opracowanie na podstawie artykułu **"Prywatność, bezpieczeństwo danych i social media. Co warto wiedzieć?"** powstałego w ramach Europejskiego Miesiąca Cyberbezpieczeństwa.