Warto wiedzieć...

dzięki kilku kliknięciom możemy ograniczyć swoją widoczność w sieci – część II

Facebook. Sprawdźmy razem ustawienia prywatności

Poprzez konfigurację ustawień prywatności jesteś w stanie ograniczyć swą widoczność w sieci tak, by publikowane przez Ciebie posty oraz informacje o Tobie i Twoich znajomych dostępne były wyłącznie dla wybranych odbiorców. Niezależnie od urządzenia, z którego logujesz się do *Facebooka*, zwróć uwagę na zagadnienie personalizacji ustawień.

Oto zbiór 20 najważniejszych wskazówek dotyczących ustawień prywatności, które warto sprawdzić na *Facebooku*, w celu zwiększenia bezpieczeństwa i poczucia prywatności:

1. Sprawdź, co i komu udostępniasz

Weryfikuj ustawienia prywatności, by mieć pewność, że udostępniasz materiały tylko wskazanym przez siebie odbiorcom. Określ, kto będzie mógł oglądać Twoje posty, kontaktować się z Tobą lub wyszukiwać profil poprzez podany adres e-mail i numer telefonu.

2. Ukryj listy znajomych

Lista Twoich znajomych jest domyślnie dostępna dla wszystkich osób korzystających z *Facebooka*. Można ją jednak ukryć:

> ***Ustawienia –> Prywatność –> Kto może zobaczyć Twoją listę znajomych?***

3. Ogranicz widoczność swojego profilu z zewnątrz

Jeśli nie chcesz, by inne przeglądarki i wyszukiwarki internetowe podawały link do Twojego profilu – wyłącz tę opcję w ustawieniach:

> ***Ustawienia –> Prywatność –> Jak można Cię znaleźć i nawiązać kontakt?***

4. Zwracajmy uwagę, co udostępniamy w *relacji* i kto może ją zobaczyć

Relacje pozwalają udostępniać nam teksty, zdjęcia oraz filmy przez 24 godziny. Wszystkie treści w relacji widoczne są w aplikacji *Facebook*. Przed publikacją treści warto określić, komu chcesz je udostępniać.

5. Zarządzaj swoim profilem

Ogranicz widoczność podstawowych danych na profilu: daty urodzenia, numeru telefonu, adresu e-mail, miejsca zamieszkania. Stosuj sprawdzoną zasadę „im mniej danych osobowych, tym lepiej".

Pamiętaj! Na urządzeniach mobilnych bezpieczniej zalogować się do *Facebooka* za pomocą przeglądarki internetowej z zainstalowanymi wtyczkami. Aplikacje mobilne m.in. *Facebook* i *Messenger*, żądają dostępu do znacznie większej ilości danych z urządzenia, np. kontaktów z książki adresowej czy możliwości dostępu do aparatu.

6. Nie udostępniaj danych wrażliwych

Publikowanie informacji, które powinny być szczególnie chronione – poglądów politycznych, informacji o zdrowiu i nałogach, preferencji seksualnych, przekonań religijnych – może narazić Cię na bardzo poważne konsekwencje. Jeśli to możliwe, rezygnuj z ich podawania.

7. Zarządzaj ustawieniami lokalizacji

Nie warto zezwalać portalowi na śledzenie Twojej lokalizacji w celu tworzenia historii miejsc, które odwiedzamy. Zarządzajmy dostępem *Facebooka* do usług, które pozwalają na precyzyjne określenie lokalizacji urządzenia przy użyciu wybranych opcji, a także zarządzanie historią miejsc Twojego pobytu.

8. Kontroluj ustawienia dotyczące rozpoznawania twarzy

Przy pomocy technologii rozpoznawania twarzy portal analizuje zdjęcia i filmy użytkowników. Na tej podstawie tworzony jest szablon, dzięki któremu nasza twarz jest rozpoznawana w postach innych użytkowników. Jeśli wyłączymy funkcję rozpoznawania twarzy, portal nie będzie wykorzystywać jej do proponowania innym, by oznaczali nas na zdjęciach.

9. Twój *dziennik aktywności* na portalu

Wzmacniaj poczucie kontroli nad treściami, które sam publikujesz. Ograniczaj grono osób, dla których opublikowane informacje będą dostępne. Portal zapamiętuje każdą Twoją aktywność: komentarze, *lajki*, obejrzane filmy i *relacje*, gry, zapytania w wyszukiwarce serwisu. Sprawdź ustawienia dotyczące *dziennika aktywności*.

10. Ograniczaj widoczność Twoich postów, stron i osób, które obserwujesz

Weryfikuj ustawienia prywatności, by mieć pewność, że udostępniasz materiały tylko wskazanym przez siebie odbiorcom. Określ, kto będzie mógł oglądać Twoje posty, kontaktować się z Tobą lub wyszukiwać profil poprzez podany adres e-mail i numer telefonu;

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć...

dzięki kilku kliknięciom możemy ograniczyć swoją widoczność w sieci – część II

Facebook. Sprawdźmy razem ustawienia prywatności

11. Zdecyduj, kto będzie mógł publikować na Twojej tablicy i oznaczać Cię w postach

Korzystaj z możliwości akceptowania wybranych postów, które zostaną opublikowanie na Twojej tablicy lub postów, w których nas oznaczono za pomocą funkcji Zatwierdzanie na osi czasu. Posty te nadal będą widoczne tylko na tablicy osoby, która Cię oznaczyła, i dla osób, którym udostępnia ona swoje wpisy.

12. Usuwaj historię wyszukiwań

Mamy możliwość usuwania z historii konkretnych zapytań lub całości historii. Podobnie jest w przypadku historii wydarzeń, w których oznaczyliśmy swój udział.

13. Przejrzyj strony, które lubisz

Twoje *polubienia* sprzed lat mogą do dziś być wykorzystywane przez reklamodawców. Aby sprawdzić listę *polubień*, należy wejść do Dziennika aktywności na swojej stronie profilowej. Warto przejrzeć też całą aktywność na osi czasu.

14. Ograniczaj dostęp aplikacji zewnętrznych do danych z Twojego profilu

Możesz wyłączyć dzielenie się danymi między aplikacjami – ograniczyć dostęp do listy znajomych, wieku, miejsca zamieszkania, adresu e-mail. Większość programów wymaga dostępu najczęściej do profilu publicznego zawierającego imię i nazwisko oraz zdjęcie profilowe.

15. Ograniczaj liczbę usług, do których logujesz się za pomocą danych do jednego konta

Zablokowanie możliwości logowania przez portal do aplikacji zewnętrznych oznacza również uniemożliwienie zbierania przez nie danych, a także dostarczania profilowanych reklam, sugerowanych na bazie naszych bieżących zachowań w sieci. W ten sposób nie tylko zwiększysz poziom ochrony prywatności, ale również bezpieczeństwa danych. W przypadku ich wycieku lub wykradzenia z jednej usługi, narażone będą również dane przechowywane przez pozostałe.

16. Określ, czy aplikacje, z których korzystają znajomi, mogą wykorzystywać informacje o nas

Nawet jeśli nie korzystasz z aplikacji, ale korzystają z niej Twoi znajomi, to w konsekwencji aplikacja może uzyskać dostęp do Twoich danych. Dzieje się tak w przypadku, gdy widoczność znajomych ustawiona jest jako *publiczna*. Możesz to zmienić i zdecydować, że informacje o Tobie nie mogą być wykorzystywane w aplikacjach przez inne osoby.

17. Bezpieczeństwo Twojego konta

Warto zadbać o bezpieczeństwo konta na wypadek utraty kontroli nad nim bądź urządzeniem, za pomocą którego się logujesz. Jeśli używasz wielu urządzeń jednocześnie, możesz zdalnie wylogować się z innych sesji:

> ***Ustawienia –> Bezpieczeństwo –> Miejsce logowania*** **(widnieje tam lista urządzeń i ostatnich sesji)**

Smartfon może stać się również dodatkową warstwą zabezpieczeń. Za każdym razem, przy próbie logowania z nowego urządzenia i przeglądarki, będzie trzeba potwierdzić tożsamość na urządzeniu zaufanym. To dobry i prosty sposób, by uniknąć przechwycenia konta. Zalecane jest również włączenie powiadomienia o nierozpoznanych logowaniach na Facebooku

> ***Ustawienia –> Bezpieczeństwo –> Konfiguracja dodatkowych zabezpieczeń***

18. Hasła do konta

Dostęp do konta powinien być możliwy za pomocą silnego hasła zawierającego wielkie i małe litery, cyfry oraz znaki specjalne. Warto wykorzystać również podwójny sposób weryfikacji przy logowaniu i włączyć dwuskładnikowe (dwuetapowe) uwierzytelnianie. Warto również zaszyfrować wiadomości e-mail z powiadomieniami z Facebooka, dzięki czemu tylko Ty będziesz miał do nich dostęp.

19. „Portal społecznościowy wie o nas wszystko"

Przejrzenie archiwum portalu może uświadomić nam, że stwierdzenie to jest prawdziwe. Warto jednak pamiętać o możliwości skorzystania z dostępu do danych użytkownika i przejrzeć informacje, które przetwarzane są przez portal lub pobrać kopię swoich danych (funkcja *Pobierz archiwum*). Ilość informacji o użytkowniku, jaką dysponuje *Facebook*, jest ogromna – szczególnie jeśli ten korzysta z Messengera.

20. Usuwanie konta

Usunięcie konta z portalu to długa procedura, ale po jej zakończeniu zniknie większość posiadanych o użytkowniku informacji.

Pamiętaj! Usunięcie postu lub zdjęcia z profilu na *Facebooku* nie gwarantuje, że zniknęło ono z sieci, ponieważ każdy, kto miał dostęp do opublikowanych przez nas materiałów, mógł je wcześniej skopiować lub zrobić zrzut ekranu.

Chcesz wiedzieć więcej…

Jeśli pragniesz zdobyć więcej informacji na temat zasad przetwarzania danych osobowych, sięgnij po przewodnik dotyczący prywatności i zasad dotyczących danych. Znajdziesz tam szczegółowy opis sposobu gromadzenia informacji i ich udostępniania oraz czas ich przechowywania przez aplikacje, w tym *Facebooka*, *Instagrama*, *Messengera*.

URZĄD OCHRONY DANYCH OSOBOWYCH